Державна служба України з надзвичайних ситуацій

Академія пожежної безпеки імені Героїв Чорнобиля

На правах рукопису

МЕЛЬНИК РУСЛАН ПАВЛОВИЧ

УДК 004.056.55:004.312.2

МЕТОДИ ТА ЗАСОБИ СИНТЕЗУ ОПЕРАЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

спеціальність 05.13.21 – системи захисту інформації

Дисертація на здобуття наукового ступеня кандидата технічних наук

Науковий керівник:
Рудницький Володимир Миколайович,
доктор технічних наук, професор

Черкаси – 2013

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ДСНС України	Державна служба України з надзвичайних ситуацій
ІТ	інформаційні технології
ISO	Міжнародна Організація по Стандартизації
IEC	Міжнародна Електротехнічна Комісія
СЛФ	спеціалізовані логічні функції
ЦЗ	цивільний захист
ТЗ	технічні засоби
ІТС	інформаційно-телекомунікаційні системи
ДНФ	диз'юнктивна нормальна форма

ВСТУП

Актуальність теми. За останні декілька десятиліть відбулися якісні зміни в процесах управління на всіх ієрархічних рівнях за рахунок інтенсивного впровадження сучасних інформаційних технологій (ІТ). Їх швидкий розвиток призвів до зростання цінності інформації як для суспільства взагалі, так і для кожної окремої людини зокрема. Водночас почала зростати небезпека втручання в роботу інформаційних систем для несанкціонованого зчитування інформації. Значення та вагомість наслідків таких втручань з часом збільшилися настільки, що навіть розвинені держави, їх промислові та фінансові структури стали заручниками своїх інформаційних технологій. Саме тому в Україні все більше уваги приділяється проблемам захисту інформації та інформаційній безпеці.

Якщо раніше проблема захисту інформації була актуальною тільки для спеціальних служб, то згодом вона стала актуальною для всіх відомств, організацій та підприємств, в тому числі й для Державної служби України з надзвичайних ситуацій (ДСНС України), де оперативність, достовірність і конфіденційність інформації має величезне значення для безпеки людей та гарантування національної безпеки в цілому. Водночас швидка ліквідація надзвичайних ситуацій з найменшими витратами сил і засобів має особливе значення для фізичного й морального стану населення, а також економіки самої країни. В будь-якому випадку всі ці стратегічні та тактичні дії супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер.

Інформація існує в різних формах, незалежно від того, знаємо ми про неї чи ні. Її можна зберігати на комп'ютерах, передавати локальними й глобальними інформаційними мережами, друкувати чи записувати на різні носії, а також озвучувати в розмовах. З погляду інформаційної безпеки всі види інформації, включаючи паперову документацію, бази даних і знань, магнітні плівки й стрічки, аудіо-записи та відеофільми, дискети й диски,

лекції та розмови, а також будь-які інші способи її представлення та зберігання, які можуть використовуватися зацікавленими особами для передачі знань та ідей, вимагають належного захисту від неавторизованих претендентів на неї.

Сучасні темпи розвитку ІТ вимагають від структурних підрозділів ДСНС України високого рівня захисту конфіденційної інформації. Колективне використання інформаційних ресурсів потребує відповідного захисту дисків і каталогів, окремих папок і файлів, а також усіх локальних і глобальних мереж від несанкціонованого втручання інформаційних зловмисників, вірусів і небезпечних програм.

Тому важливою проблемою є постійне підвищення якості систем захисту інформації. Одним із основних напрямків розвитку систем захисту інформації є криптографічний захист.

Важливий внесок у розвиток криптології та захисту інформації внесли такі вітчизняні та зарубіжні науковці, як О. В. Гомонай, І. Д. Горбенко, А. А. Молдовян, О. Г. Корченко, Г. Ф. Конахович, В. В. Бараннік, О. К. Юдін, В. А. Лужецький, А. О. Семенов, В. К. Усенко, В. М. Рудницький, Є. В. Васіліу, Ж. Брассар, Д. М. Голубчіков, К. Шеннон, У. Збінден, І. Чанг, Б. Шнайер, М. Хеллман, Ч. Г. Беннет та ін.

Проте в сфері захисту інформації залишається цілий ряд задач і проблем, вирішення яких має важливе науково-технічне й загальнодержавне значення. Однією з таких задач є підвищення якості систем захисту інформації на основі використання операцій розширеного матричного криптографічного перетворення для інформаційних систем ДСНС України. Одним із шляхів вдосконалення існуючих криптографічних систем захисту інформації та розробки нових криптографічних алгоритмів є розширення спектра операцій, на основі яких вони будуються.

Виходячи з цього, тема дисертаційної роботи «Методи та засоби синтезу операцій розширеного матричного криптографічного перетворення» є актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до Постанови Президії Національної академії наук України від 25.02.2009 р. № 55 «Про основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009 – 2013 рр.» (п. 1.2.7.1. Розробка методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії; п. 1.2.7.2. Розробка методів підвищення продуктивності систем асиметричної криптографії), а також відповідно до «Концепції наукового забезпечення діяльності Міністерства надзвичайних ситуацій України» і «Концепції наукової діяльності Академії пожежної безпеки імені Героїв Чорнобиля МНС України на 2010 – 2015 роки». Результати дисертаційної роботи включені в НДР «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579), «Криптографічне кодування: методи та засоби реалізації (частина 2)» (ДР № 0113U001475), в яких автор брав участь як відповідальний виконавець.

Мета і задачі дослідження. Метою дисертаційної роботи є підвищення якості систем захисту інформації на основі використання операцій розширеного матричного криптографічного перетворення для захисту конфіденційної інформації.

Поставлена мета передбачає вирішення таких задач:

1. На основі аналізу існуючих методів та засобів захисту інформації та результатів обчислювального експерименту визначити нову групу операцій криптографічного перетворення, яка забезпечить підвищення якості систем захисту інформації.

2. Розробити метод синтезу елементарних функцій розширеного матричного перетворення.

3. Розробити методи синтезу операцій криптографічного перетворення інформації на основі розширеного матричного перетворення.

4. Розробити методи підвищення якості систем криптографічного захисту інформації на основі використання операцій розширеного матричного перетворення.

Об'єктом дослідження є процеси захисту інформації, яка зберігається, обробляється та передається в комп'ютерних системах і мережах.

Предмет дослідження – методи та засоби синтезу операцій розширеного матричного криптографічного перетворення для підвищення якості систем захисту інформації.

Методи дослідження. У процесі синтезу елементарних функцій та операцій криптографічного перетворення використовується математичний апарат теорії інформації, систем числення, методів дискретної математики. Розробка принципів, методів і алгоритмів синтезу операцій оберненого криптографічного перетворення згідно з запропонованим підходом базується на положеннях теорії логіки, криптографії та комп'ютерного моделювання. При розробці дискретних пристроїв застосовуються методи синтезу функціональних схем на основі дискретної математики й теорії цифрових автоматів.

Наукова новизна одержаних результатів:

1. Вперше розроблено метод синтезу елементарних функцій розширеного матричного перетворення шляхом введення логічних умов обмеження, які забезпечують нелінійність перетворення, що дало змогу будувати операції розширеного матричного перетворення.

2. Вперше розроблено методи синтезу операцій розширеного матричного криптографічного перетворення інформації на основі операцій матричного перетворення шляхом побудови та перебудови функцій обмеження, що дало можливість будувати алгоритми шифрування на основі використання більшої кількості операцій перетворення та системи криптографічного захисту інформації з новими якісними характеристиками.

3. Удосконалено методи синтезу систем захисту інформації на основі додаткового використання нової групи трирозрядних логічних операцій, які

забезпечили розширення множини операцій, на основі яких будуються криптоалгоритми.

4. Набули подальшого розвитку методи синтезу систем криптографічного захисту інформації на основі використання операцій розширеного матричного перетворення, що забезпечило підвищення криптостійкості та швидкості реалізації алгоритмів залежно від задач проектування.

Практичне значення одержаних результатів:

Практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних інженерних методик, алгоритмів, моделей та варіантів функціональних схем спеціалізованих дискретних пристроїв криптографічного перетворення для систем захисту інформації.

На підставі проведених досліджень одержано такі практичні результати: розроблено варіанти реалізації на програмному та апаратному рівнях нової групи трирозрядних криптографічних операцій на основі розширеного матричного перетворення. Розширене матричне перетворення дає можливість збільшити криптостійкість від 1032 до 10150 разів пропорційно відносно потокового шифрування при зменшенні часу шифрування від 1,5 до 6 разів.

Практична цінність роботи підтверджена актами впровадження в підрозділах Державної служби України з надзвичайних ситуацій, зокрема в Територіальному Управлінні МНС України в Черкаській області та Управлінні Держтехногенбезпеки у Черкаській області; державному підприємстві НВК «Фотоприлад» та навчальних закладах: Черкаському державному технологічному університеті, Академії пожежної безпеки імені Героїв Чорнобиля, Черкаському національному університеті імені Богдана Хмельницького, Національному аерокосмічному університеті імені М. Є. Жуковського «ХАІ» (додаток А).

Особистий внесок здобувача. Результати дисертаційної роботи отримані автором самостійно. Роботи [1, 9, 14] виконані без співавторів. У

наукових працях, опублікованих у співавторстві, з питань, що стосуються цього дослідження, авторові належать: опис способів запису трирозрядних елементарних функцій та криптографічних операцій на їх основі [2]; обґрунтування доцільності дискретного представлення операцій криптографічного перетворення інформації [3]; проведення розрахунку кількості елементарних функцій для криптографічного перетворення залежно від розрядності [4]; аналіз базових спеціалізованих трирозрядних логічних функцій [5]; проведення аналізу складності пристроїв додавання з урахуванням групового перенесення, пристроїв попереднього додавання, а також сумарної складності реалізації пристроїв на основі моделювання мікроконвеєрних суматорів для систем числення [6]; розробка методу синтезу операцій оберненого криптографічного перетворення на основі елементарних функцій розширеного матричного перетворення [7]; отримання правил синтезу матриці оберненого криптографічного перетворення при наявності в прямій операції прямої, інверсної та змішаної заміни [8]; визначення способів удосконалення процесу інформування підрозділів пожежної охорони [10]; визначення критеріїв якості інформування підрозділів пожежної охорони [11]; обґрунтування доцільності застосування спеціалізованих логічних функцій у захисті оперативної інформації інформаційно-аналітичної системи МНС України [12]; проведення дослідження групи трирозрядних логічних функцій [13].

Апробація результатів дисертації. Результати дисертаційного дослідження доповідалися й обговорювалися на XX науково-технічній конференції «Системы безопасности – 2011» (Москва, 2011), міжнародній науково-практичній конференції «Теорія та практика ліквідації надзвичайних ситуацій» (Черкаси, 2011), V міжнародній науково-практичній конференції «Актуальні проблеми технічних та природничих наук у забезпеченні діяльності служби цивільного захисту» (Черкаси, 2012), XXIV міжнародній науково-практичній конференції з проблем пожежної безпеки, присвяченій 75-річчю створення інституту (Москва, 2012), міжнародній науково-

практичній конференції «Чрезвычайные ситуации: теория, практика, инновации «ЧС – 2012» (Гомель, 2012), ІІ міжнародній науково-практичній конференції «Пожежна безпека: теорія і практика» (Черкаси, 2012), І міжнародній заочній науково-практичній конференції «Информационные системы и технологии: управление и безопасность» (Тольятті-Русе, 2012).

Публікації. Основні результати дисертаційної роботи викладено в 14 друкованих працях, а саме: 5 статтях у наукових фахових виданнях України, 2 статтях у наукових фахових виданнях Російської Федерації, 1 монографії, виданій в Російській Федерації, 6 тезах доповідей на наукових конференціях та семінарах.

Структура й обсяг дисертації. Дисертація складається зі вступу, п’яти розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації становить 178 сторінок, в тому числі 149 сторінок основної частини, 12 рисунків, 7 таблиць. Список використаних джерел містить 168 найменувань.

РОЗДІЛ 1
ПРОБЛЕМА ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ ЦИВІЛЬНОГО ЗАХИСТУ В УМОВАХ РЕАЛЬНОГО ЧАСУ

1.1 Захист інформації в інформаційно-телекомунікаційній системі цивільного захисту

На сучасному етапі серед основних реальних та потенційних загроз національній безпеці України в інформаційній сфері є розголошення інформації, що становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства й держави [15]. Інформацією називається сукупність відомостей, даних про будь-які події, предмети або явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі [16]. Серед загроз, які можуть призвести до розголошення інформації, за своїми небезпечними наслідками особливе місце займають несанкціонований доступ до інформації, яка обробляється та циркулює на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах (ІТС), а також витік інформації технічними каналами.

Якщо раніше проблема захисту інформації була актуальною тільки для спеціальних служб, то згодом вона стала актуальною для всіх організацій та підприємств, в тому числі й для органів цивільного захисту (ЦЗ). Прогнозування виникнення надзвичайних ситуацій, завчасне попередження, інформування населення про наявні джерела загроз та рівень їх небезпеки – основні завдання структурних підрозділів ДСНС України. Водночас швидка ліквідація надзвичайних ситуацій з найменшими затратами сил і засобів має важливе значення для фізичного й морального стану населення, а також

економіки країни в цілому. У будь-якому випадку всі ці стратегічні та тактичні дії супроводжуються складними інформаційними процесами, більшість з яких мають конфіденційний характер [17, 18].

Впровадження сучасних інформаційних і телекомунікаційних технологій у діяльність органів ЦЗ значно підвищує оперативність, а в необхідних випадках і конфіденційність проходження управлінських рішень до кожної ланки структурних підрозділів ДСНС України, а також забезпечує результативність виконання завдань в області ЦЗ.

В той же час активний розвиток інформатизації в системі ДСНС України й обумовлене цим процесом значне зростання відомчих інформаційних активів, у тому числі конфіденційного характеру, вимагає ухвалення адекватних і своєчасних рішень по нарощуванню потенціалу системи захисту інформації в області протидії нанесення шкоди інформаційній безпеці, що зростає в міру інтенсифікації розвитку ІТ.

Під джерелами загроз інформаційним ресурсам можна розглядати потенційно можливі дії природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на конфіденційну інформацію, що зберігається в ній. Ідентифікація джерел загроз, тобто розмежування пасивних дій від активних інформаційних зловмисників характеризується таким поняттям як уразливість інформаційних ресурсів. Саме за наявності вразливості як однієї з характеристик інформаційних систем і відбувається активізація джерел загроз. Безперечно, самі джерела загроз приховані, за своєю суттю та відповідно до теорії множин – невичерпні.

Відповідно до Закону України «Про основи національної безпеки України» [19] до джерел загроз інформаційній безпеці загалом, а також інформаційним ресурсам і комунікаційним системам зокрема належить:

- розголошення інформації, яка становить державну та іншу таємницю, передбачену відповідним законодавством, а також конфіденційної інформації, що є власністю структурних підрозділів ДСНС України;

- намагання маніпулювати суспільною свідомістю шляхом поширення недостовірної, неповної або упередженої інформації щодо появи надзвичайних ситуацій будь-якого характеру, а також їх наслідків на фізичний і моральний стан населення чи довкілля;
- комп'ютерна злочинність та мережевий тероризм – глобальний і локальний;
- розкриття інформаційних ресурсів, порушення їх цілісності, спричинення збоїв у роботі комп'ютерного обладнання та мережевого устаткування.

У науковій праці [20] авторами виокремлено ті джерела загроз, що стосуються інформаційної безпеки структурних підрозділів ДСНС України відповідно до загальної класифікації джерел загроз [16, 19]:

1) за походженням джерела загроз бувають:

- природного характеру – це небезпечні геологічні, метеорологічні, гідрологічні явища, зсуви ґрунтів чи провали надр, природні пожежі та буревії, зміна стану водних ресурсів і біосфери, а також інші природні катаклізми, які спричиняють масове руйнування каналів зв'язку та комунікаційних мереж;
- техногенного характеру – транспортні аварії (катастрофи), пожежі на потенційно-небезпечних об'єктах, неспровоковані вибухи чи їх загроза, аварії на інженерних мережах і спорудах життєзабезпечення тощо, які призводять до раптового руйнування каналів зв'язку, аварій головних серверів різних систем управління;
- антропогенного характеру – вчинення зловмисниками різноманітних дій, спрямованих на руйнування інформаційних ресурсів, комунікаційних систем і програмне забезпечення тощо, які призупиняють та розлагоджують роботу різних силових структур.

До антропогенної групи за змістом дій належать: ненавмисні, викликані помилковими чи неуважними діями людини, наприклад, помилковий запуск програми, модифікація одних даних замість інших через

неуважність оператора: навмисні (інспіровані), результат роботи зловмисників, наприклад, інсталяція програм, які передають інформацію на інші комп'ютери, зараження їх вірусами, навмисна дезінформація керівництва щодо неполадок в інформаційних мережах чи системах тощо;

2) за сферами походження джерела загроз бувають [16]:

- екзогенні – джерело дестабілізації роботи інформаційної системи знаходиться поза її межами;

- ендогенні – небезпечні програми дестабілізації роботи інформаційної системи, що перебувають у самій системі;

3) за ступенем нанесення гіпотетичної шкоди інформаційній безпеці:

- загроза – явні чи потенційні дії, що ускладнюють або унеможливлюють реалізацію різних потреб у інформаційній системі та створюють небезпеку для системи управління різними силовими структурами, в тому числі й структурними підрозділами ДСНС України;

- небезпека – безпосередня дестабілізація процесу функціонування системи управління інформаційною безпекою структурних підрозділів ДСНС України;

4) за повторюваністю вчинення джерела загроз поділяються на [20]:

- повторювані – такі загрози, які мали місце раніше, можуть виникати через певний проміжок часу;

- продовжувані – неодноразова поява джерел загроз, що складаються з ряду тотожних дій, які мають спільну мету;

5) за ймовірністю реалізації джерела загроз поділяються на:

- вірогідні – такі загрози, які за збігом обставин і специфікою виконання певного комплексу умов обов'язково настануть, наприклад, попереднє оголошення атаки інформаційних ресурсів чи інформаційних систем, після чого відбувається сама атака;

- неможливі – такі загрози, які ніколи не настануть, тобто вони мають декларативний чи залякуваний характер, не підкріплені реальною чи навіть потенційною можливістю здійснити проголошені наміри;

- випадкові – такі загрози, які навіть за збігом обставин і специфікою виконання певного комплексу умов кожного разу проходять по-різному. Такі загрози аналізують за допомогою методів дослідження операцій, зокрема теорії ймовірностей чи теорії ігор, які вивчають закономірності їх появи у випадкових явищах;

6) за значенням джерела загроз бувають [19]:

- допустимі – такі загрози, які не можуть призвести до колапсу інформаційної системи, наприклад, появи вірусів, які не шкодять іншим програмам через їх фізичне знищення;

- неприпустимі – такі загрози, які в разі їх реалізації призводять до колапсу й системної дестабілізації роботи інформаційних ресурсів, призводять до змін, не сумісних із подальшим існуванням системи захисту інформації;

7) за рівнем детермінізму джерела загроз поділяються на:

- закономірні – такі загрози, які мають стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки. Наприклад, будь-який суб'єкт (силові, виробничі, комерційні чи банківські структури) системи забезпечення інформаційної безпеки піддаватиметься інформаційним атакам, якщо в ньому вона не функціонує, або функціонує на неналежному рівні;

- випадкові – такі загрози, які можуть виникати або не виникати, наприклад, спроби хакерів дестабілізувати роботу системи інформаційної безпеки деякої комерційної структури;

8) за структурою впливу джерела загроз поділяються на [20]:

- системні – загрози, що впливають одразу на всі складові елементи системи управління інформаційною безпекою, наприклад, структурні підрозділи ДСНС України;

- структурні – загрози, що впливають на окремі компоненти системи управління інформаційною безпекою;

- елементні – загрози, що впливають на окремі елементи структури інформаційної системи, мають постійний характер і можуть бути небезпечними лише за умови неефективності або не проведення їх моніторингу;

9) за характером реалізації джерела загроз поділяються на [16]:

- реальні – активізація небезпечних програм дестабілізації роботи систем інформаційної безпеки є неминучою і не обмежена часовим інтервалом і просторовою дією;

- потенційні – активізація небезпечних програм дестабілізації можлива за певних умов стану середовища функціонування системи управління інформаційною безпекою, наприклад, головного управління ДСНС України;

- здійснені – такі загрози, реалізація яких відбулася та досягнуто повної чи часткової мети;

- уявні – псевдоактивізація небезпечних програм дестабілізації роботи інформаційних систем, або ж активізація яких за деякими ознаками схожа з діями небезпечних програм (вірусів), але насправді вони не є такими;

10) за ставленням до них джерела загроз поділяються на [20]:

- об'єктивні – такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління інформаційною безпекою не відіграє вирішальної ролі через те, що об'єктивні джерела загроз існують незалежно від волі та свідомості суб'єкта. Об'єктивні джерела загроз, які не відображено в офіційних документах, називаються ненормативними загрозами;

- суб'єктивні – така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління інформаційною безпекою, джерелом загрози його системі безпеки. При цьому визначальну роль у ідентифікації тих чи інших обставин і чинників відіграє воля суб'єкта управління інформаційною безпекою, який і приймає безпосереднє рішення про надання

статусу загрозі або ідентифікації тих чи інших його дій як потенційному джерелу загрози інформаційним ресурсам чи комунікаційним системам;

11) за об'єктом впливу джерела загроз створюють небезпеку особі, суспільству та державі.

Головним призначенням класифікації джерел загроз є демонстрація багатошаровості їх видової структури. Безперечно, джерела загроз інформаційній безпеці структурних підрозділів ДСНС України постійно змінюються, удосконалюються та модифікуються. Класифікація допомагає усвідомити не лише розмаїття джерел загроз, а й наблизитися до розуміння витоків їх формування.

Основне завдання систем інформаційної безпеки – забезпечити безперебійну роботу структурних підрозділів ДСНС України, тобто уникнути нанесення збитків від потенційних джерел загроз як конфіденційній інформації, так і іншим інформаційним ресурсам шляхом їхнього передбачення, випередження чи запобігання [21, 22]. Управління інформаційною безпекою дає змогу колективно використовувати будь-яку конфіденційну інформацію та відповідні інформаційні ресурси, забезпечуючи при цьому їх ефективний захист від несанкціонованого доступу зловмисників.

Належна організація інформаційної безпеки в структурних підрозділах ДСНС України дає змогу забезпечити [23]:

- конфіденційність інформації – властивість інформації, яка вказує на те, що її не зможе отримати неавторизований користувач і (або) інформаційний процес. Інформація зберігає секретність від несанкціонованого розкриття чи перехоплення, якщо дотримуються настанов формальних процедур ознайомлення з нею;

- цілісність інформації – властивість інформації, яка полягає в тому, що її не зможе модифікувати неавторизований користувач і (або) інформаційний процес. Інформація зберігає точність та повноту, якщо дотримуються настанов формальних процедур її модифікації чи видалення;

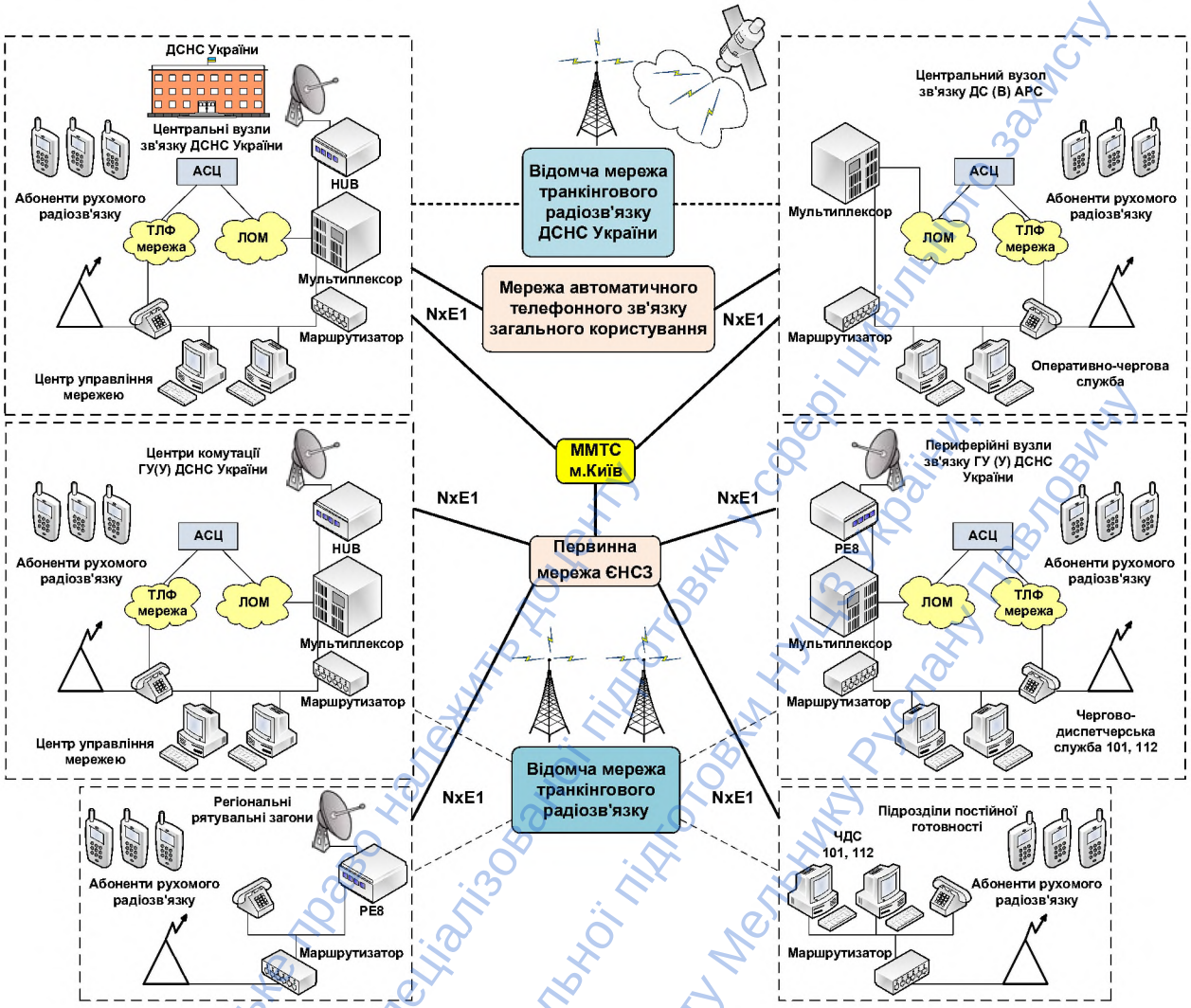

Рис. 1.1. Типова схема телекомунікаційної мережі ДСНС України

- доступність інформації (ресурсів автоматизованої інформаційної системи) – властивість інформаційної системи забезпечити доступ авторизованих користувачів до потрібної інформації та життєво важливих сервісів у міру потреби. Властивість доступності інформації здебільшого потрібна разом з її конфіденційністю та цілісністю.

Таким чином, підсумовуючи зазначене вище, можна стверджувати, що за сучасних умов у процесі забезпечення інформаційної безпеки ІТС ЦЗ, типова схема якої приведена на рис. 1.1. [24], важливо розуміти характер, природу, сутність і зміст джерел загроз і рівнів їх небезпек, вміти своєчасно їх ідентифікувати.

Тому основною задачею є підвищення якості систем захисту інформації на основі використання операцій розширеного матричного криптографічного перетворення для інформаційних систем ДСНС України.

1.2 Сучасний стан та перспективи розвитку криптографічних систем захисту інформації

Розвиток нових ІТ супроводжується такими негативними явищами, як промислове шпигунство, комп'ютерні злочини й несанкціонований доступ до секретної та конфіденційної інформації. Тому захист інформації є важливим державним завданням у будь-якій країні [25, 26]. Необхідність захисту інформації в Україні сприяла створенню Державної служби спеціального зв'язку та захисту інформації України та розвитку правової бази інформаційної безпеки.

Захист інформації повинен забезпечувати попередження завдання шкоди внаслідок втрати (розкрадання, знищення, перекручування, підробки) інформації в будь-якому її вигляді. Організація заходів захисту інформації повинна проводитися в повній відповідності до діючих законів і нормативних документів із безпеки інформації, інтересів користувачів інформації. Щоб гарантувати високий ступінь захисту інформації, необхідно постійно вирішувати складні науково-технічні завдання розробки та вдосконалення засобів її захисту.

Органи та підрозділи ДСНС України та більшість сучасних установ, організацій та підприємств незалежно від виду діяльності та форм власності не можуть успішно функціонувати, вести господарську та іншу діяльність без забезпечення системи захисту своєї інформації, що включає організаційно-нормативні заходи та технічні засоби контролю безпеки інформації при її обробці, зберіганні та передачі в автоматизованих системах [24, 27].

Захист інформації (англ. Data protection) – це сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації [16, 28-30]. Серед усього спектру методів захисту даних від несанкціонованого доступу особливе місце займають криптографічні методи [31].

Сучасні методи шифрування гарантують практично абсолютний захист даних, але завжди залишається проблема надійності їх реалізації. В даний час особливо актуальною є оцінка вже використовуваних криптоалгоритмів, класифікація яких приведена на рис. 1.2. Завдання визначення ефективності засобів захисту часто більш трудомісткі, ніж їх розробка, вимагає наявності спеціальних знань і, як правило, вищої кваліфікації, ніж завдання розробки. Ці обставини призводять до того, що на ринку з'являється безліч засобів криптографічного захисту інформації, про які ніхто нічого не знає. При цьому розробники тримають криптоалгоритм у секреті [23].

Рис.1.2. Класифікація криптографічних алгоритмів

На сьогодні залишається цілий ряд невирішених та недостатньо вивчених проблем у сфері захисту інформації. Основною задачею на сучасному етапі розвитку суспільства та його інформатизації є виконання вимоги постійного підвищення якості систем захисту інформації на основі використання нових операцій криптографічного перетворення для інформаційних систем ДСНС України.

Серед усього спектру методів захисту даних від несанкціонованого доступу особливе місце займають криптографічні методи [32, 33]. На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі та зберігання. Широке застосування комп'ютерних технологій та постійне збільшення обсягу інформаційних потоків викликає постійне зростання інтересу до криптографії [34-36].

Система криптографічного захисту інформації – сукупність органів, підрозділів, груп, діяльність яких спрямована на забезпечення криптографічного захисту інформації, та підприємств, установ і організацій, що розробляють, виробляють, експлуатують та (або) розповсюджують криптосистеми й засоби криптографічного захисту інформації.

Криптографічна система – сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та (або) передається.

Криптографічний захист інформації – вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних), з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо [31-34].

Сучасна криптографія вивчає і розвиває такі напрями:

- симетричні криптосистеми (із секретним ключем);
- несиметричні криптосистеми або асиметричні (з відкритим ключем);

• системи електронного підпису;

• системи керування ключами.

Сучасні криптографічні системи забезпечують високу стійкість зашифрованих даних за рахунок підтримки режиму таємності криптографічного ключа.

Відповідно до завдань, що виконуються із захисту інформації, можна виділити два основні класи криптографічних систем [37, 38]:

• криптосистеми, що забезпечують справжність (автентичність) інформації;

• криптосистеми, що забезпечують таємність інформації.

Такий поділ обумовлено тим, що завдання захисту секретності інформації (збереження її в таємниці) принципово відрізняється від завдання захисту дійсності (автентичності) інформації, а тому повинна вирішуватися іншими криптографічними методами.

Класифікація криптосистем відповідно до завдань, що виконуються ними із захисту інформації, представлена на рис. 1.3. [37].

Проте поряд з наведеними перевагами наявні недоліки, відповідно з якими асиметричні криптосистеми вважаються кращими [38-45]:

- головним недоліком систем з такими алгоритмами є той факт, що обидві сторони, що обмінюються інформацією, повинні домовитися про використання одного й того ж ключа, а також зберігати його в таємниці від інших;

- складність обміну ключами (для застосування необхідно вирішити проблему надійної передачі ключів кожному абоненту, оскільки потрібний секретний канал для передачі кожного ключа обом сторонам);

- складність управління ключами у великій мережі.

Однак, для компенсації недоліків симетричного шифрування в даний час широко застосовується комбінована (гібридна) криптографічна схема, де за допомогою асиметричного шифрування передається сеансовий ключ, який

використовується сторонами для обміну даними за допомогою симетричного шифрування [43-48].

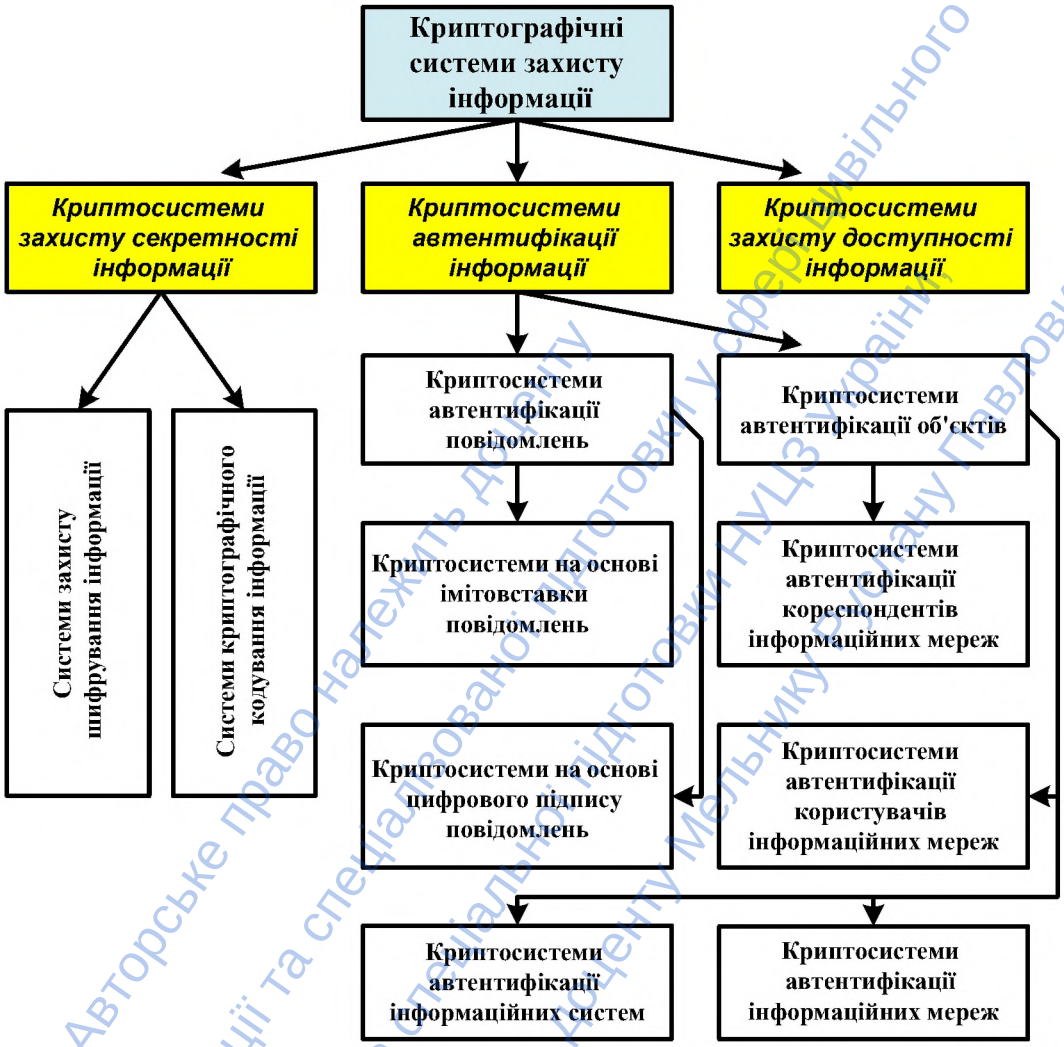

Рис.1.3. Класифікація криптографічних систем захисту інформації

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. Відомо більше десятка перевірених алгоритмів шифрування, які при використанні ключа достатньої довжини й коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу. Широко використовуються такі алгоритми шифрування, як Twofish, IDEA, RC4 та ін.

У багатьох країнах прийняті національні стандарти шифрування. У 2001 році в США прийнятий стандарт симетричного шифрування AES на основі алгоритму Rijndael з довжиною ключа 128, 192 і 256 біт. Алгоритм

AES прийшов на зміну колишньому алгоритму DES, який тепер рекомендовано використовувати тільки в режимі Triple-DES (3DES).

З розвитком комп'ютерних мереж і зростанням попиту на електронні послуги ситуація в сфері інформаційної безпеки серйозно загострилася, а питання стандартизації підходів до її вирішення стало особливо актуальним, як для розробників, так і для користувачів інформаційно-технологічними засобами [49].

Головне завдання стандартів інформаційної безпеки – створити основу для взаємодії між виробниками, споживачами та експертами по кваліфікації продуктів IT. Кожна з цих груп має свої інтереси та свої погляди на проблему інформаційної безпеки [50, 51].

Стандарт Міжнародної Організації по Стандартизації (ISO) 15408 [52-54], відомий також як «Загальні критерії оцінки безпеки інформаційних технологій» або просто «Загальні критерії», задав напрямок перегляду нормативної бази інформаційної безпеки в багатьох країнах, у тому числі й в Україні [55].

ISO/IEC 27000 – серія міжнародних стандартів, що включає стандарти з інформаційної безпеки, опубліковані спільно ISO та Міжнародною Електротехнічною Комісією (IEC). Серія містить кращі практики й рекомендації в області інформаційної безпеки для створення, розвитку та підтримки Системи Менеджменту Інформаційної Безпеки.

ISO 13335 – серія міжнародних стандартів з безпеки інформаційних технологій.

ISO/IEC 17799 – стандарт інформаційної безпеки «Інформаційні технології – Технології безпеки – Практичні правила менеджменту інформаційної безпеки». Інформаційна безпека визначається стандартом як «збереження конфіденційності (впевненості в тому, що інформація доступна тільки тому, хто уповноважений мати такий доступ), цілісності (гарантії точності й повноти інформації, методів її обробки) та доступності (гарантії в

тому, що уповноважені користувачі мають доступ до інформації та пов'язаним ресурсам)».

Законодавство України в сфері захисту інформації представлено такими нормативними документами: [16, 19, 28-31, 35, 36, 55-62].

В останні два десятиріччя швидко розвивається новий напрямок криптографічного захисту інформації – квантова криптографія, основною перевагою якої від традиційних, зокрема від методів асиметричної криптографії, що мають тільки обчислювальну стійкість, є використання специфічних властивостей квантових систем, які служать носіями інформації в протоколах квантової криптографії, дає можливість досягти при вирішенні деяких завдань захисту інформації безумовної (теоретико-інформаційної) стійкості, яка не залежить від обчислювальних та інших можливостей зловмисника.

Важливий внесок у розвиток криптології та захисту інформації внесли такі вітчизняні та зарубіжні науковці, як О. В. Гомонай, І. Д. Горбенко, А. А. Молдовян, О. Г. Корченко, Г. Ф. Конахович, В. В. Бараннік, О. К. Юдін, В. А. Лужецький, А. О. Семенов, В. К. Усенко, В. М. Рудницький, Є. В. Василіу, Ж. Брассар, Д. М. Голубчіков, К. Шеннон, У. Збінден, І. Чанг, Б. Шнайер, М. Хеллман, Ч. Г. Беннет та ін. [26, 63-85].

Питанням розроблення нових протоколів квантової криптографії з підвищеною інформаційною місткістю, аналізом атак на ці протоколи, розробленням методів підвищення стійкості протоколів до атак займається вчений Є.В. Василіу [74].

Підвищенням рівня захищеності електронних інформаційних ресурсів інформаційно-комунікаційних систем за рахунок удосконалення їх систем захисту квантовими складовими займається науковець С.О. Гнатюк [25, 64, 66].

Основним напрямком діяльності вченого О.Г. Голубничого є підвищення рівня захищеності інформації, що передається у широкосмугових телекомунікаційних системах шляхом синтезу методів та засобів

забезпечення прихованості радіосистем, які дозволяють мінімізувати їх виявлення [69].

Вирішенням важливої науково-технічної задачі підвищення швидкості доступу до конфіденційних інформаційних ресурсів на основі використання спеціалізованих логічних функцій (СЛФ) криптографічного перетворення займаються вчені наукової школи В.М. Рудницького: І.В. Миронець та В.Г. Бабенко [2-8, 72, 86].

В роботах В.Г. Бабенко вперше одержано метод підвищення швидкодії систем захисту інформації на основі застосування СЛФ шляхом використання ключа в якості команди вибору набору функцій, що дозволило збільшити довжину блоку інформації, над яким виконується криптографічне перетворення; удосконалено: методи синтезу СЛФ для криптографії на основі просторового та векторного представлення, що дозволило розширити множину СЛФ для виконання криптографічних перетворень; метод аналізу СЛФ на основі лавинного ефекту шляхом використання векторного представлення логічних функцій і таблиць мінімальних кодових відстаней по Хеммінгу, що дозволило обґрунтувати ефективність їх застосування в криптосистемах; набули подальшого розвитку: метод синтезу дискретних пристроїв для криптографічного перетворення на основі використання СЛФ шляхом поетапної мінімізації, що дозволило одержати уніфіковану модель пристрою, яка забезпечила реалізацію повної множини СЛФ; метод підвищення ефективності функціонування систем захисту інформації на основі використання запропонованих СЛФ в існуючих криптографічних алгоритмах, що дозволило забезпечити оперативність обробки інформації.

В роботах І.В. Миронець одержано модель процесу підвищення оперативності доступу до віддаленої захищеної інформації в реальному часі на основі використання логічних функцій перекодування; вперше розроблено метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання логічних функцій для криптографічного перетворення шляхом введення логічних функцій перекодування, що дало

змогу зменшити час доступу до інформації за рахунок заміни етапів «декодування–кодування»; удосконалено методи криптографічного перетворення інформації на основі логічних функцій за рахунок розробки математичних моделей та функціональних схем побудови функцій перекодування, що дало можливість розробити метод підвищення оперативності доступу до віддаленої захищеної інформації в реальному часі; набув подальшого розвитку метод оцінювання ефективності доступу до інформаційних ресурсів за рахунок урахування особливостей криптографічного перекодування, що дало змогу оцінити отримані результати.

Проте в області захисту інформації залишається цілий ряд задач і проблем, вирішення яких має важливе науково-технічне й загальнодержавне значення. Однією з таких задач є підвищення якості систем захисту інформації на основі використання операцій розширеного матричного криптографічного перетворення для інформаційних систем ДСНС України.

1.3 Аналіз методів та засобів підвищення якості криптографічних систем захисту інформації та постановка задач дослідження

Інтеграція інформаційних та обчислювальних ресурсів на основі комп'ютерних мереж є домінуючим напрямком розвитку ІТ. Зворотною стороною інтеграції є потенційна небезпека конфіденційності, цілісності та оперативності обробки інформації. Це вимагає використання спеціальних засобів захисту інформації в комп'ютерних системах та мережах. Реалізація криптографічних алгоритмів потребує додаткових затрат ресурсів комп'ютерних систем і, відповідно, знижує їх оперативність. Особливо критичним є час реалізації функцій доступу в комп'ютерних системах реального часу.

Технічною базою для створення умов розвитку систем доступу до конфіденційних інформаційних ресурсів стали досягнення інформатики й обчислювальної техніки, мікроелектроніки, телекомунікацій тощо. Наприклад, В.М. Сидельніков і С.О. Шестаков внесли пропозицію використання ряду варіантів схем на основі теоретико-кодових конструкцій, застосовуючи швидкі алгоритми декодування. Б.В. Березін, П.В. Дорошкевич досліджували схеми електронно-цифрового підпису на основі симетричних алгоритмів. А.Н. Фіонов, Б.Я. Рябко виклали основні підходи й методи сучасної криптографії для вирішення задач, які виникають при обробці, зберіганні та передачі інформації [87].

Основу забезпечення інформаційної безпеки в ІТС складають криптографічні методи та засоби захисту інформації. Слід врахувати, що найбільш надійний захист можна забезпечити тільки за допомогою комплексного підходу, тобто рішення задачі має представляти собою сукупність організаційно-технічних та криптографічних заходів.

В основі криптографічних методів лежить поняття криптографічного перетворення інформації, виробленого за певними математичними законами, з метою виключити доступ до даної інформації сторонніх користувачів, а також з метою забезпечення неможливості безконтрольної зміни інформації з боку тих же самих осіб.

Застосування криптографічних методів захисту забезпечує вирішення основних завдань інформаційної безпеки. При реалізації більшості методів криптографічного захисту виникає необхідність обміну деякою інформацією. Наприклад, автентифікація об’єктів ІТС супроводжується обміном ідентифікуючої і автентифікуючої інформації.

Створення захищеної системи – завдання комплексне, і вирішується воно шляхом застосування програмно-технічних методів і засобів, а також за допомогою організаційних заходів.

Забезпечити конфіденційність інформації користувача дозволить використання СЛФ, які можливо використовувати для підвищення оперативності доступу до конфіденційних інформаційних ресурсів [2-6, 86], на основі виконання логічних операцій криптографічного перетворення.

Метою дисертаційної роботи є підвищення якості систем захисту інформації на основі використання операцій розширеного матричного криптографічного перетворення для захисту конфіденційної інформації.

Для досягнення даної мети можна сформулювати основні етапи розробки методів та засобів синтезу операцій розширеного матричного криптографічного перетворення для захисту інформаційних ресурсів ДСНС України (рис. 1.4.).

1. Необхідно проаналізувати існуючі методи та засоби захисту інформації. Зазначений аналіз дасть змогу чітко визначити підхід до вдосконалення матричних систем криптографічного перетворення, а також вдосконалити модель процесу криптографічного перетворення на основі розширеного матричного перетворення, що дасть можливість обґрунтувати задачі дисертаційного дослідження.

2. Вдосконалена модель процесу криптографічного перетворення на основі розширеного матричного перетворення дозволить розробити метод синтезу елементарних операцій розширеного матричного перетворення, шляхом введення логічних функцій обмеження. Це, в свою чергу, дасть змогу будувати операції розширеного матричного перетворення. Для цього необхідно визначити множини трирозрядних елементарних функцій, групи елементарних функцій, провести синтез елементарних функцій розширеного матричного перетворення та аналіз форм представлення операцій криптографічного перетворення.

3. Проведений аналіз форм представлення операцій криптографічного перетворення дозволить розробити метод синтезу операцій криптографічного перетворення інформації на основі розширеного матричного перетворення,

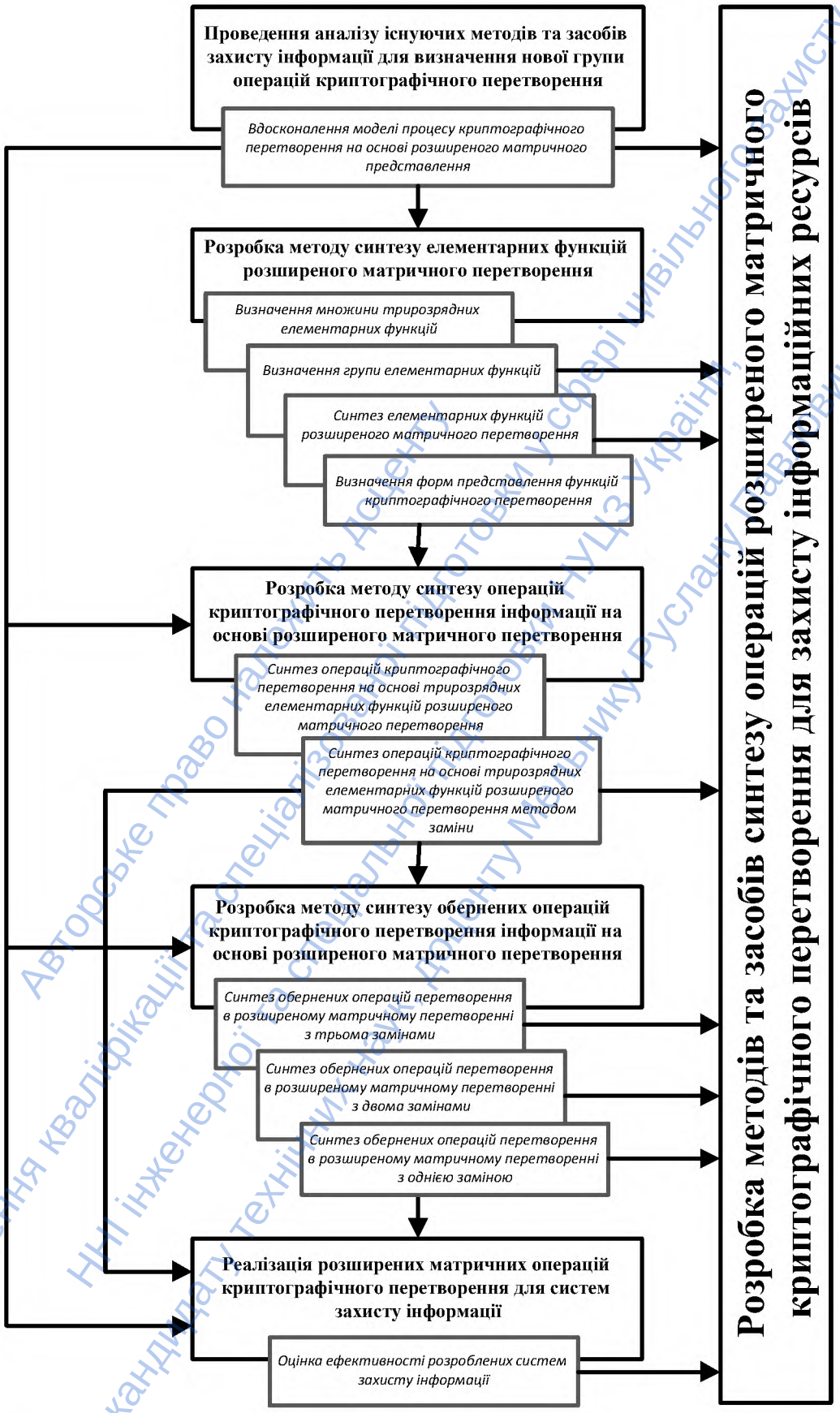

Рис. 1.4. Етапи науково-технічних досліджень та розробки методів та засобів синтезу операцій розширеного матричного криптографічного перетворення для захисту інформаційних ресурсів ДСНС України

шляхом побудови та перебудови функцій обмеження, що дасть змогу розширити кількість операцій перетворення і, як наслідок, підвищити стійкість криптоперетворення.

4. Для побудови системи захисту інформації з більшою криптостійкістю необхідно розробити метод синтезу операцій оберненого криптографічного перетворення інформації на основі розширеного матричного перетворення, шляхом побудови та перебудови функцій обмеження. Для цього необхідно провести синтез операцій оберненого криптографічного перетворення в розширеному матричному представленні з трьома, двома та однією замінами.

5. Розроблений метод синтезу систем захисту інформації на основі використання операцій розширеного матричного перетворення дозволить підвищити криптостійкість криптографічних систем на основі матричного перетворення.

Відповідно до мети та намічених етапів дослідження необхідно вирішити такі задачі дисертаційної роботи:

1. На основі аналізу існуючих методів і засобів захисту інформації та результатів обчислювального експерименту визначити нову групу операцій криптографічного перетворення, яка забезпечить підвищення якості систем захисту інформації.

2. Розробити метод синтезу елементарних функцій розширеного матричного перетворення.

3. Розробити методи синтезу операцій криптографічного перетворення інформації на основі розширеного матричного перетворення.

4. Розробити методи підвищення якості систем криптографічного захисту інформації на основі використання операцій розширеного матричного перетворення.

Висновки з розділу 1

1. Аналітичний огляд найпоширеніших сучасних методів і засобів розвитку нових тенденцій показав, що проблема підвищення інформаційної безпеки інформаційно-телекомунікаційних систем цивільного захисту є важливою та актуальною.

2. В результаті проведеного аналізу встановлено, що одним з напрямків підвищення ефективності захисту інформації в інформаційно-телекомунікаційній системі ДСНС України є впровадження операцій криптографічного перетворення.

3. В розділі сформульована та формалізована наукова задача, поетапно виокремлено питання, що потребують дослідження. Запропонований загальний підхід до вирішення задачі дисертаційного дослідження забезпечує єдність та цілеспрямованість всієї роботи.

4. Результати розділу опубліковані в [10-12].

РОЗДІЛ 2
СИНТЕЗ ТА ДОСЛІДЖЕННЯ ТРИРОЗРЯДНИХ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО ПЕРЕТВОРЕННЯ

2.1 Визначення множини трирозрядних елементарних функцій на основі проведення обчислювального експерименту

На сьогоднішній день вважається, що забезпечення безпеки інформації повинно носити комплексний характер. Пропонуються нові комплексні рішення в сфері забезпечення безпеки інформаційних ресурсів. Проте організація забезпечення безпеки інформації повинна носити не просто комплексний характер, але ще й засновуватися на всебічному аналізі можливих наслідків, при якому важливо не упустити будь-які аспекти [88].

Напрями забезпечення безпеки інформації – це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, на рівні окремої особистості.

Згідно з [89, 90] однією зі складових інженерно-технічного напрямку захисту інформації є криптографічні засоби захисту – апаратні, програмні та програмно-апаратні засоби, які реалізують захист інформації за допомогою криптографічних перетворень. А основу забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах складають саме криптографічні методи та засоби захисту інформації. Криптографічне перетворення інформації побудоване за певними математичними законами – це основа криптографічних методів, що створюються з метою виключення несанкціонованого доступу до даної інформації та її незаконного отримання.

Захист інформації розвивається в двох напрямах криптографія і кодування [90-101]. Поєднання цих двох напрямів в єдиний за рахунок перекодування під управлінням криптосистеми дозволить підвищити якість систем захисту інформації [102-111]. Поєднання цих напрямів можливе на

основі використання логічних функцій криптографічного перетворення інформації.

Інформація на цифрових носіях зберігається в двійковому коді. Мінімальна одиниця вимірювання цифрових даних – це біт або розряд інформації. Тобто будь-яке перетворення інформації на найнижчому схемотехнічному рівні теж зводиться до логічного перетворення певної кількості розрядів за визначеним алгоритмом. Зважаючи на те, що сьогодні об'єм даних, який підлягає перетворенню одночасно, досить громіздкий, то це означає, що велике значення відводиться швидкодії апаратного забезпечення, що безпосередньо реалізує перетворення інформації. Це ж саме стосується і криптографічного перетворення. Криптографічне перетворення може здійснюватись над одним, двома, трьома й більше розрядами одночасно, в залежності від алгоритму, що застосовується, та набору схемотехнічних елементів, що доступні розробнику. Крім того, кожний розряд перетворюється згідно визначених залежностей від інших розрядів відповідно.

Зважаючи на вищезазначене, введемо деякі умовні позначення та основні визначення.

Елементарні функції криптоперетворення: $f_1^{(1)}(x_1, x_2, ..., x_N)$, $f_2^{(2)}(x_1, x_2, ..., x_N)$, $f_m^{(N)}(x_1, x_2, ..., x_N)$ – функції перетворення першого, другого та N-ого розряду інформації відповідно, що являють собою дискретні логічні функції. Кожна функція відображає правило-залежність перетвореного значення розряду від всіх N початкових значень розрядів інформації.

N – кількість розрядів інформації, що бере участь у процесі криптографічного перетворення, а m – це номер функції перетворення, що застосовується, $m = \{1..M\}$, де M – загальна можлива кількість N-розрядних функцій криптографічного перетворення. $x_1, x_2, ..., x_N$ – значення першого, другого, N-ого розрядів інформації відповідно.

Відомо, що $x_1, x_2, x_N \in \{0;1\}$, а відповідно й значення дискретних логічних функцій $f_1^{(1)}, f_2^{(2)}, ..., f_m^N \in \{0;1\}$.

Криптографічні операції синтезуються на основі вибраних елементарних функцій та являють собою композицію відповідних функцій перетворення: $F_{1,2,...,m} = (f_1^{(1)}, f_2^{(2)}, ..., f_m^N)$. На основі даних елементарних функцій будуються операції криптографічного перетворення. Наприклад:

$$F^k_{30,57,106} = (f^{(1)}_{30}, f^{(2)}_{57}, f^{(3)}_{106}) \Rightarrow F^d_{45,54,106} = (f^{(1)}_{45}, f^{(2)}_{54}, f^{(3)}_{106}),$$

$$F^k_{30,89,108} = (f^{(1)}_{30}, f^{(2)}_{89}, f^{(3)}_{108}) \Rightarrow F^d_{45,106,54} = (f^{(1)}_{45}, f^{(2)}_{106}, f^{(3)}_{54}),$$

де $f^{(1)}_{30}, f^{(2)}_{57}, f^{(3)}_{106}$ – елементарні функції 1, 2, 3-го розряду відповідно; нижні індекси – номери елементарних функцій, які відповідають десятковому значенню результату їх виконання; $F^k_{30,57,106}$, $F^d_{45,54,106}$ – операції криптографічного перетворення, причому k – пряме, а d – обернене криптографічне перетворення.

Для забезпечення збору інформації про логічні функції декількох змінних, які можуть використовуватися в криптографії, та визначення їх особливостей була розроблена методика синтезу логічних функцій на основі методу перебору [112-116]. Запропонована методика стала основою для створення програмного забезпечення проведення обчислювального експерименту [116-120].

Проте на сьогоднішній день досліджені лише дворозрядні логічні функції криптографічного перетворення інформації.

Виходячи з наведених результатів, можна зробити припущення, що використання операцій криптографічного перетворення інформації більшої розрядності дозволить зменшити час криптографічної обробки інформації.

Для дослідження трирозрядних логічних функцій криптографічного перетворення інформації було вдосконалене спеціальне математичне й програмне забезпечення.

Основною задачею обчислювального експерименту є виявлення та збір інформації про логічні функції трьох змінних, які можуть бути використані для операцій криптографічного перетворення.

За результатами проведення обчислювального експерименту було знайдено 70 елементарних функцій для криптографічного перетворення інформації.

Результати обчислювального експерименту за допомогою методів мінімізації логічних функцій [115-118] були формалізовані та класифіковані за складністю та за видом представлення (прямий чи інверсний).

Класифікація формалізованих результатів обчислювального експерименту приведена в табл. 2.1.

При проведенні досліджень дворозрядних функцій криптографічного перетворення було встановлено, що операції криптографічного перетворення можуть бути поділені на групи [120]:

- базова група операцій криптографічного перетворення;
- група операцій перестановки;
- група операцій інверсії.

Для дворозрядних операцій криптографічного перетворення базова група операцій криптографічного перетворення включає в себе три операції, група операцій перестановки – дві операції, група операцій інверсії – чотири операції. Загальна кількість дворозрядних операцій криптографічного перетворення буде дорівнювати двадцяти чотирьом (добутку кількості операцій у кожній групі).

Для трирозрядних операцій криптографічного перетворення:

- група операцій перестановки складатиме: $3! = 6$;
- група операцій інверсії складатиме: $2^3 = 8$.

Для чотирирозрядних операцій криптографічного перетворення:

- група операцій перестановки складатиме: $4! = 24$;
- група операцій інверсії складатиме: $2^4 = 16$.

Таблиця 2.1

Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації

Пряма елементарна функція			Обернена елементарна функція		
Код функції		Опис функції	Код функції		Опис функції
00001111	15	$f_{15} = x_1$	11110000	240	$f_{240} = \bar{x}_1$
00110011	51	$f_{51} = x_2$	11001100	204	$f_{204} = \bar{x}_2$
01010101	85	$f_{85} = x_3$	10101010	170	$f_{170} = \bar{x}_3$
00111100	60	$f_{60} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_2$	11000011	195	$f_{195} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2$
01011010	90	$f_{90} = \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_3$	10100101	165	$f_{165} = \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_3$
01100110	102	$f_{102} = \bar{x}_2 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	10011001	153	$f_{153} = \bar{x}_2 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
00011011	27	$f_{27} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$	11100100	228	$f_{228} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$
00011101	29	$f_{29} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$	11100010	226	$f_{226} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$
00100111	39	$f_{39} = x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	11011000	216	$f_{216} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$
00101110	46	$f_{46} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$	11010001	209	$f_{209} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$
00110101	53	$f_{53} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3$	11001010	202	$f_{202} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3$
00111010	58	$f_{58} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3$	11000101	197	$f_{197} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3$
01000111	71	$f_{71} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	10111000	184	$f_{184} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3$
01001110	78	$f_{78} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$	10110001	177	$f_{177} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
01010011	83	$f_{83} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	10101100	172	$f_{172} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3$
01011100	92	$f_{92} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3$	10100011	163	$f_{163} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3$
01110010	114	$f_{114} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	10001101	141	$f_{141} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$
01110100	116	$f_{116} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	10001011	139	$f_{139} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3$
00010111	23	$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$	11101000	232	$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$
00101011	43	$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$	11010100	212	$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$
01001101	77	$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$	10110010	178	$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$
01110001	113	$f_{113} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3$	10001110	142	$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$
00011110	30	$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$	11100001	225	$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
00110110	54	$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$	11001001	201	$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
00111001	57	$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	11000110	198	$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
01001011	75	$f_{75} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10110100	180	$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
01010110	86	$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$	10101001	169	$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
01011001	89	$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10100110	166	$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$
01100011	99	$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10011100	156	$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
01100101	101	$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10011010	154	$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
01101010	106	$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10010101	149	$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
01101100	108	$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10010011	147	$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
01111000	120	$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10000111	135	$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
00101101	45	$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	11010010	210	$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
01101001	105	$f_{105} = x_1 \oplus x_2 \oplus x_3$	10010110	150	$f_{150} = x_1 \oplus x_2 \oplus x_3 \oplus 1$

Для n-розрядних операцій криптографічного перетворення:

- група операцій перестановки складатиме $n!$;
- група операцій інверсії складатиме 2^n.

Для зменшення обсягу досліджень буде доцільним зменшити кількість операцій криптографічного перетворення, виключивши групу операцій інверсії.

Якщо використовувати лише елементарні функції без інверсії, то кількість операцій криптографічного перетворення, яку необхідно дослідити, буде зменшена в 2^n раз.

Для спрощення процесу дослідження елементарні функції криптографічного перетворення було класифіковано на прямі та обернені елементарні функції на основі таких означень:

Означення 2.1. Елементарна функція називається прямою, якщо код операції знаходиться в першій половині числового ряду.

Означення 2.2. Елементарна функція називається оберненою, якщо код операції знаходиться в другій половині числового ряду.

Крім того отримані елементарні функції криптографічного перетворення було класифіковано в залежності від складності функції.

Складність елементарної функції криптографічного перетворення визначається як сума операцій диз'юнкції та кон'юнкції в мінімізованій моделі функції.

Отримані елементарні функції для криптографічного перетворення інформації мають одну спільну особливість з дворозрядними функціями. Як в трирозрядних, так і в дворозрядних функціях є однакова кількість нулів та одиниць. А таких операцій серед дворозрядних логічних функцій – 6, а серед трирозрядних – 70.

2.2 Визначення групи елементарних функцій для подальших досліджень

Проведемо детальний аналіз елементарних функцій, представлених в табл. 2.1. Класифікація трирозрядних елементарних функцій в залежності від способів їх побудови представлена на рис. 2.1.

Виходячи з аналізу математичних моделей елементарних функцій, можна виділити групу елементарних функцій, які забезпечують перестановки розрядів. Тобто на основі цих елементарних функцій будуються операції криптографічного перетворення, які забезпечують виконання перестановок розрядів інформації, що кодуємо. До цієї групи функцій відносяться:

$$f_{15} = x_1, \tag{2.1}$$

$$f_{51} = x_2, \tag{2.2}$$

$$f_{85} = x_3, \tag{2.3}$$

$$f_{240} = \bar{x}_1, \tag{2.4}$$

$$f_{204} = \bar{x}_2, \tag{2.5}$$

$$f_{170} = \bar{x}_3. \tag{2.6}$$

Необхідно відзначити, що елементарні функції (2.1) – (2.3) будуть прямими, а елементарні функції (2.4) – (2.6) будуть оберненими. Основні результати дослідження цих функцій опубліковані в [112].

Виділяється група елементарних функцій, які побудовані на основі додавання за модулем 2 (матричні функції). До цієї групи елементарних функцій відносяться:

$$f_{60} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_2, \tag{2.7}$$

$$f_{90} = \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_3, \tag{2.8}$$

$$f_{102} = \bar{x}_2 \cdot x_3 \vee x_2 \cdot \bar{x}_3, \tag{2.9}$$

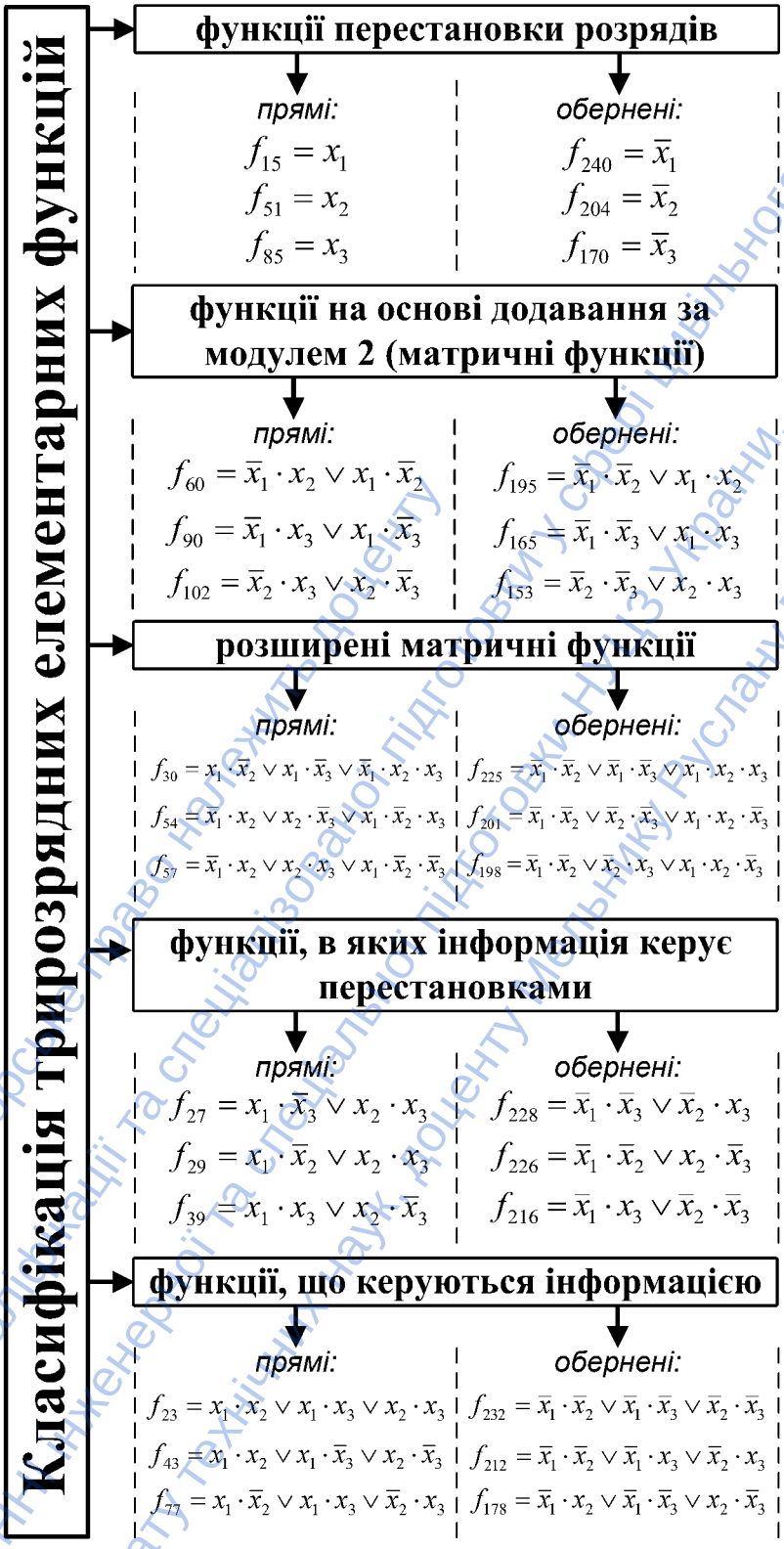

Рис. 2.1. Класифікація трирозрядних елементарних функцій

$$f_{105} = x_1 \oplus x_2 \oplus x_3, \tag{2.10}$$

$$f_{195} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2, \tag{2.11}$$

$$f_{165} = \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_3, \tag{2.12}$$

$$f_{153} = \bar{x}_2 \cdot \bar{x}_3 \vee x_2 \cdot x_3, \quad (2.13)$$

$$f_{150} = x_1 \oplus x_2 \oplus x_3 \oplus 1. \quad (2.14)$$

Елементарні функції (2.7) – (2.10) будуть прямими, а елементарні функції (2.8) – (2.14) будуть оберненими.

В ряді робіт доведено, що на основі елементарних функцій (2.1) – (2.14) будуються матричні функції криптографічного перетворення [117-119].

Наступну групу елементарних функцій представляють функції, в яких інформація керує перестановками. До цієї групи елементарних функцій відносяться:

$$f_{27} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3, \quad (2.15)$$

$$f_{29} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3, \quad (2.16)$$

$$f_{39} = x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3, \quad (2.17)$$

$$f_{46} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3, \quad (2.18)$$

$$f_{53} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3, \quad (2.19)$$

$$f_{58} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3, \quad (2.20)$$

$$f_{71} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3, \quad (2.21)$$

$$f_{78} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3, \quad (2.22)$$

$$f_{83} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3, \quad (2.23)$$

$$f_{92} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3, \quad (2.24)$$

$$f_{114} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3, \quad (2.25)$$

$$f_{116} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3, \quad (2.26)$$

$$f_{228} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3, \quad (2.27)$$

$$f_{226} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3, \quad (2.28)$$

$$f_{216} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3, \quad (2.29)$$

$$f_{209} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3, \quad (2.30)$$

$$f_{202} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3, \quad (2.31)$$

$$f_{197} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3, \quad (2.32)$$

$$f_{184} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3, \quad (2.33)$$

$$f_{177} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3, \quad (2.34)$$

$$f_{172} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3, \quad (2.35)$$

$$f_{163} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3, \quad (2.36)$$

$$f_{141} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3, \quad (2.37)$$

$$f_{139} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3. \quad (2.38)$$

Елементарні функції (2.15) – (2.26) будуть прямими, а (2.27) – (2.38) – оберненими.

На основі елементарних функцій (2.15) – (2.38) будуються функції криптографічного перетворення інформації, в яких результат перетворення залежить не лише від операції, а й від інформації, що перетворюється. Тобто інформація керує процесом перетворення на основі перестановок. Результати дослідження цих функцій опубліковані в [120].

Наступну групу елементарних функцій представляють функції, що керуються інформацією. До цієї групи елементарних функцій відносяться:

$$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3, \quad (2.39)$$

$$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3, \quad (2.40)$$

$$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3, \quad (2.41)$$

$$f_{113} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3, \quad (2.42)$$

$$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3, \quad (2.43)$$

$$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3, \quad (2.44)$$

$$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3, \quad (2.45)$$

$$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3. \quad (2.46)$$

Елементарні функції (2.39) – (2.42) будуть прямими, а (2.43) – (2.46) – оберненими.

На основі елементарних функцій (2.39) – (2.46) будуються операції криптографічного перетворення інформації, в яких керування процесом перетворення на основі перестановок залежить від значення третього розряду.

Останню групу елементарних функцій на сьогоднішній день не досліджували. До цієї групи елементарних функцій відносяться:

$$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3, \quad (2.47)$$

$$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3, \quad (2.48)$$

$$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \quad (2.49)$$

$$f_{75} = x_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3, \quad (2.50)$$

$$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3, \quad (2.51)$$

$$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \quad (2.52)$$

$$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3, \quad (2.53)$$

$$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3, \quad (2.54)$$

$$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3, \quad (2.55)$$

$$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3, \quad (2.56)$$

$$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \quad (2.57)$$

$$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3, \quad (2.58)$$

$$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3, \quad (2.59)$$

$$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3, \quad (2.60)$$

$$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3, \quad (2.61)$$

$$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \quad (2.62)$$

$$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3, \quad (2.63)$$

$$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3, \quad (2.64)$$

$$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3, \quad (2.65)$$

$$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3, \quad (2.66)$$

$$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \quad (2.67)$$

$$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \quad (2.68)$$

$$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \quad (2.69)$$

$$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3. \quad (2.70)$$

Елементарні функції (2.47) – (2.58) будуть прямими, а (2.59) – (2.70) – оберненими.

При проведенні подальших досліджень було вирішено назвати цю групу елементарних функцій, як функції розширеного матричного перетворення, тому що вони накладають додаткову умову на матричне перетворення операцій криптографічного перетворення.

2.3 Синтез елементарних функцій розширеного матричного перетворення

Для подальшого дослідження обмежимося лише прямими функціями розширеного матричного перетворення (2.47) – (2.58).

Як видно з прямих функцій розширеного матричного перетворення, лише один аргумент входить до складу всіх трьох доданків логічного додавання. Класифікуємо ці елементарні функції за даною ознакою:

- функції на основі x_1:

$$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3,$$

$$f_{75} = x_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3,$$

$$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$

$$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3;$$

- функції на основі x_2:

$$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3,$$

$$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$

$$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3,$$

$$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3;$$

- функції на основі x_3:

$$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3,$$

$$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3,$$

$$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3,$$

$$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3.$$

Розглянемо більш детально групу функцій на основі x_1. Можна зробити наступні висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_1, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому і третьому доданках x_2 має різні знаки інверсії;
- в другому і третьому доданках x_3 має різні знаки інверсії;
- в третьому доданку x_1 має інший знак інверсії, ніж в першому та другому доданках.

Розглянемо більш детально групу функцій на основі x_2. Можна зробити наступні висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому завжди присутні x_2, x_3;
- в третьому завжди присутні x_1, x_2, x_3;
- в першому і третьому доданках x_1 має різні знаки інверсії;

- в другому і третьому доданках x_3 має різні знаки інверсії;
- в третьому доданку x_2 має інший знак інверсії, ніж в першому та другому доданках.

Розглянемо більш детально групу функцій на основі x_3. Можна зробити наступні висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_2, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому і третьому доданках x_1 має різні знаки інверсії;
- в другому і третьому доданках x_2 має різні знаки інверсії;
- в третьому доданку x_3 має інший знак інверсії, ніж в першому та другому доданках.

З чотирьох варіантів елементарних функцій у трьох із них аргумент, на основі якого будується операція, представлений прямим аргументом, а в другому варіанті – інверсним.

Можливо, розподіл на прямі та обернені функції відповідно до порядку номеру функцій не зовсім коректний. Перевіримо це на основі аналізу інверсних функцій.

Як видно з інверсних функцій розширеного матричного перетворення, лише один аргумент входить до складу всіх трьох доданків логічного додавання. Класифікуємо ці елементарні функції за даною ознакою:

- функції на основі x_1:

$$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3;$$

$$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3;$$

$$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3;$$

$$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3;$$

- функції на основі x_2:

$$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3;$$

$$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3;$$

$$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3;$$

$$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3;$$

- функції на основі x_3:

$$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3;$$

$$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3;$$

$$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3;$$

$$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3.$$

Розглянемо більш детально групу функцій на основі x_1. Можна зробити наступні висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_1, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому й третьому доданках x_2 має різні знаки інверсії;
- в другому й третьому доданках x_3 має різні знаки інверсії;
- в третьому доданку x_1 має інший знак інверсії, ніж у першому та другому доданках.

Розглянемо більш детально групу функцій на основі x_2. Можна зробити наступні висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_2, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому й третьому доданках x_1 має різні знаки інверсії;

- в другому й третьому доданках x_3 має різні знаки інверсії;
- в третьому доданку x_2 має інший знак інверсії, ніж у першому та другому доданках.

Розглянемо більш детально групу функцій на основі x_3. Можна зробити наступні висновки:

- в першому доданку завжди присутні x_1, x_2;
- в другому доданку завжди присутні x_2, x_3;
- в третьому доданку завжди присутні x_1, x_2, x_3;
- в першому й третьому доданках x_1 має різні знаки інверсії;
- в другому і третьому доданках x_2 має різні знаки інверсії;
- в третьому доданку x_3 має інший знак інверсії, ніж у першому та другому доданках.

З чотирьох варіантів елементарних функцій у трьох із них аргумент, на основі якого будується операція, представлений прямим аргументом, а в другому варіанті – інверсним.

Виходячи з результатів дослідження прямих та обернених розширених матричних елементарних функцій, для спрощення алгоритму синтезу елементарних функцій (означення 2.1 та означення 2.2) було б доцільно поміняти три прямі елементарні функції з трьома оберненими функціями.

Дана заміна елементарних функцій не призведе до зміни кількості операцій криптографічного перетворення на основі розширеного матричного перетворення, при цьому може призвести до спрощення алгоритмів побудови самих операцій криптоперетворення.

Виходячи з пропозиції формування прямих функцій в залежності від прямого значення основного аргументу, а обернених – з оберненого значення основного аргументу, формалізуємо правила отримання прямої та оберненої елементарної функції:

- пряма функція:

$$f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee \overline{x}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l, \qquad (2.71)$$

де x – пряме значення аргументу; $\overline{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\overline{\hat{x}}$ – інверсне до будь-якого значення аргументу; за умови: $i \in [1,2,3]$; $j \in [1,2,3]$; $l \in [1,2,3]$; $i \neq j \neq l$;

- обернена функція:

$$f = \overline{x}_i \cdot \hat{x}_j \vee \overline{x}_i \cdot \hat{x}_l \vee x_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l. \qquad (2.72)$$

Виходячи з формул (2.71) та (2.72), сформулюємо загальний вираз для отримання елементарних функцій криптографічного перетворення:

$$f = \hat{x}_i \cdot \hat{x}_j \vee \hat{x}_i \cdot \hat{x}_l \vee \overline{\hat{x}}_i \cdot \overline{\hat{x}}_j \cdot \overline{\hat{x}}_l, \qquad (2.73)$$

де $\hat{x}_i$ – змінні, що можуть приймати прямі або інверсні значення.

Вирази (2.71) – (2.73) можна вважати формалізованим записом методу синтезу елементарних функцій розширеного матричного перетворення для криптографічного перетворення інформації.

Вирази (2.71) – (2.73) дозволяють:

- синтезувати прямі трирозрядні елементарні функції або обернені трирозрядні елементарні функції, чи повну множину трирозрядних елементарних функцій;
- синтезувати прямі або обернені трирозрядні елементарні функції, чи повну множину елементарних функцій будь-якої розрядності;
- визначити кількість елементарних функцій будь-якої розрядності.

Розглянемо більш детально синтез елементарних функцій будь-якої розрядності.

Приклад 1. Синтез чотирирозрядних елементарних функцій розширеного матричного перетворення.

Нехай елементарна функція будується на основі першого, другого та четвертого розрядів.

На основі виразу (2.71) отримаємо:

$$f = x_1 \cdot \overline{x}_2 \vee x_1 \cdot \overline{x}_4 \vee \overline{x}_1 \cdot x_2 \cdot x_4,$$
$$f = x_1 \cdot \overline{x}_4 \vee x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_4,$$
$$f = x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_4 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_4.$$

Нехай елементарна функція будується на основі першого, третього та четвертого розрядів.

Отримаємо:

$$f = x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_4 \vee \overline{x}_1 \cdot x_3 \cdot x_4,$$
$$f = x_1 \cdot \overline{x}_4 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot \overline{x}_3 \cdot x_4,$$
$$f = x_1 \cdot \overline{x}_3 \vee x_1 \cdot x_4 \vee \overline{x}_1 \cdot x_3 \cdot \overline{x}_4.$$

Приклад 2. Синтез шестирозрядних елементарних функцій розширеного матричного перетворення.

Нехай елементарна функція будується на основі другого, четвертого та шостого розрядів.

На основі виразу (2.71) отримаємо:

$$f = x_2 \cdot \overline{x}_4 \vee x_2 \cdot \overline{x}_6 \vee \overline{x}_2 \cdot x_4 \cdot x_6,$$
$$f = x_2 \cdot \overline{x}_6 \vee x_2 \cdot x_4 \vee \overline{x}_2 \cdot \overline{x}_4 \cdot x_6,$$
$$f = x_2 \cdot \overline{x}_4 \vee x_2 \cdot x_6 \vee \overline{x}_2 \cdot x_4 \cdot \overline{x}_6.$$

Нехай елементарна функція будується на основі першого, третього та п’ятого розрядів.

Отримаємо:

$$f = x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_5 \vee \overline{x}_1 \cdot x_3 \cdot x_5,$$
$$f = x_1 \cdot \overline{x}_5 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot \overline{x}_3 \cdot x_5,$$

$$f = x_1 \cdot \bar{x}_3 \vee x_1 \cdot x_5 \vee \bar{x}_1 \cdot x_3 \cdot \bar{x}_5 .$$

Визначимо кількість елементарних функцій розширеного матричного перетворення будь-якої розрядності.

Кількість прямих елементарних функцій розширеного матричного перетворення визначається:

$$K_{П} = 12 \cdot C_n^3, \tag{2.74}$$

$$C_n^3 = \frac{n!}{3!(n-3)!}, \tag{2.75}$$

де $K_{П}$ – кількість прямих елементарних функцій, С – кількість сполучень із n по 3, n – кількість розрядів, 3 – розрядність функцій.

Кількість обернених елементарних функцій розширеного матричного перетворення визначається:

$$K_O = 12 \cdot C_n^3. \tag{2.76}$$

Загальна кількість елементарних функцій розширеного матричного перетворення визначається:

$$K_{\Sigma} = K_{П} + K_O = 24 \cdot C_n^3. \tag{2.77}$$

Результати розрахунку кількості елементарних функцій розширеного матричного перетворення в залежності від розрядності моделі криптоперетворення представлені в табл. 2.2.

Аналіз таблиці показує значний ріст кількості елементарних функцій розширеного матричного перетворення в залежності від розрядності моделі криптоперетворення.

Таблиця 2.2

Результати розрахунку кількості елементарних функцій розширеного матричного перетворення

Кількість розрядів	**3**	**4**	**5**	**6**	**7**	**8**
Кількість прямих елементарних функцій	12	48	120	240	420	672
Кількість обернених елементарних функцій	12	48	120	240	420	672
Загальна кількість елементарних функцій	24	96	240	480	840	1344

2.4 Форми представлення елементарних функцій та операцій криптографічного перетворення

Криптографічні операції синтезуються на основі вибраних елементарних функцій та представляють собою композицію відповідних функцій перетворення:

$$F_{1,2,...,m} = (f_1^{(1)}, f_2^{(2)}, ..., f_m^N). \quad (2.78)$$

Елементарні функції $f_1^{(1)}, f_2^{(2)}, ..., f_m^N$ утворюють групу. Тобто виконується властивість суперпозиції: серед множини елементарних функцій можна знайти відповідні набори пар функцій таких, що $f_1^N(f_2^N(x_1, x_2, ..., x_N)) = (x_1, x_2, ..., x_N)$.

Тобто множину елементарних функцій, з яких формуються криптографічні операції, можливо використовувати як для прямого, так і для оберненого криптографічного перетворення відповідно. Надалі будемо називати такі відповідні пари як пряма криптографічна операція

перетворення F^k та обернена криптографічна операція перетворення F^d інформації відповідно.

Так як логічні функції мають різноманітні способи запису, то й криптографічні операції теж можна зображувати по різному. Розглянемо основні способи запису трирозрядних криптографічних функцій.

В роботах [112-120] досліджувалася лише група дворозрядних криптографічних функцій. Отримані результати спонукають до проведення подальших досліджень криптографічних функцій більшої розрядності.

Як було сказано раніше, в результаті обчислювального експерименту за допомогою спеціального програмного забезпечення [121-123] було знайдено групу трирозрядних логічних функцій, на основі яких будуються операції криптографічного перетворення, які не досліджувалися раніше. Основні (прямі) елементарні функції наведені нижче в дискретному представленні:

1. 00011110 (30) – $f_{30} = x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3$;
2. 00101101 (45) – $f_{45} = x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3$;
3. 00110110 (54) – $f_{54} = \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3$;
4. 00111001 (57) – $f_{57} = \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3$;
5. 01001011 (75) – $f_{75} = x_1 \cdot \overline{x}_3 \vee x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3$;
6. 01010110 (86) – $f_{86} = \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3$;
7. 01011001 (89) – $f_{89} = \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3$;
8. 01100011 (99) – $f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3$;
9. 01100101 (101) – $f_{101} = x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3$;
10. 00111001 (106) – $f_{106} = x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3$;
11. 01101100 (108) – $f_{108} = x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3$;
12. 01111000 (120) – $f_{120} = \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3$.

На основі даних функцій будуються операції криптографічного перетворення. Наприклад:

$$F^{k}_{30,57,106} = (f^{(1)}_{30}, f^{(2)}_{57}, f^{(3)}_{106}) \Rightarrow F^{d}_{45,54,106} = (f^{(1)}_{45}, f^{(2)}_{54}, f^{(3)}_{106}) \quad (2.79)$$

$$F^{k}_{30,89,108} = (f^{(1)}_{30}, f^{(2)}_{89}, f^{(3)}_{108}) \Rightarrow F^{d}_{45,106,54} = (f^{(1)}_{45}, f^{(2)}_{106}, f^{(3)}_{54}) \quad (2.80)$$

$$F^{k}_{30,106,57} = (f^{(1)}_{30}, f^{(2)}_{106}, f^{(3)}_{57}) \Rightarrow F^{d}_{75,86,108} = (f^{(1)}_{75}, f^{(2)}_{86}, f^{(3)}_{108}) \quad (2.81)$$

Якщо розписати кожну операцію, то отримаємо розширене дискретне представлення криптографічних функцій:

1) вираз (2.79) матиме вигляд:

- операція перетворення:

$$F^{k}_{30,57,106} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{45,54,106} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix};$$

2) вираз (2.80) матиме вигляд:

- операція перетворення:

$$F^{k}_{30,89,108} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{45,106,54} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix};$$

3) вираз (2.81) матиме вигляд:

- операція перетворення:

$$F^{k}_{30,106,57} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{75,86,108} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee \cdot x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix}.$$

Для проведення досліджень може бути доцільним використання різних способів запису криптографічних функцій.

Приведемо деякі можливі способи запису елементарних функцій та криптографічних операцій на основі них.

За допомогою повної системи булевих функцій $\langle \wedge, \oplus, 1 \rangle$ можливо побудувати функції у вигляді полінома Жегалкіна:

$$P(X_1 \ldots X_n) = a \oplus a_1 X_1 \oplus a_2 X_2 \oplus \ldots \oplus a_n X_n \oplus a_{12} X_1 X_2 \oplus a_{13} X_1 X_3 \oplus \ldots \oplus a_{1\ldots n} X_1 \ldots X_n,$$
$$a \ldots a_{1\ldots n} \in \{0,1\}. \qquad (2.82)$$

Для цього потрібно використати еквівалентні перетворення диз'юнктивної нормальної форми (ДНФ). В порівнянні з ДНФ у поліномі Жегалкіна відсутні операції «АБО» та «ЗАПЕРЕЧЕННЯ».

Таким чином, поліном Жегалкіна можна отримати з ДНФ, записавши операції «АБО» та «ЗАПЕРЕЧЕННЯ» через операції «ВИКЛЮЧНЕ АБО», «І» та константу 1. Для цього застосовують наступні відношення:

$$\begin{aligned} A \vee B &= A \oplus B \oplus AB; \\ \overline{A} &= A \oplus 1. \end{aligned} \qquad (2.83)$$

Наведемо приклад перетворення ДНФ в поліном Жегалкіна:

$$XY \vee \overline{XY} = XY \oplus \overline{XY} \oplus XY\overline{XY} = XY \oplus \overline{XY} = XY \oplus (X \oplus 1)(Y \oplus 1) = XY \oplus XY \oplus X \oplus Y \oplus 1 = X \oplus Y \oplus 1. \quad (2.84)$$

При перетвореннях використані відношення:

$$\begin{aligned} &A \oplus A = 0; \\ &(A \oplus B)C = AC \oplus BC \end{aligned} \quad (2.85)$$

Отримані нами елементарні функції теж можуть мати представлення поліномами Жегалкіна:

1) 00011110 (30) – $f_{30} = x_1 \oplus x_2 \cdot x_3$;

2) 00101101 (45) – $f_{45} = x_1 \oplus x_2 \oplus x_2 \cdot x_3$;

3) 00110110 (54) – $f_{54} = x_2 \oplus x_1 \cdot x_3$;

4) 00111001 (57) – $f_{57} = x_1 \oplus x_2 \oplus x_1 \cdot x_3$;

5) 01001011 (75) – $f_{75} = x_1 \oplus x_3 \oplus x_2 \cdot x_3$;

6) 01010110 (86) – $f_{86} = x_3 \oplus x_1 \cdot x_2$;

7) 01011001 (89) – $f_{89} = x_1 \oplus x_3 \oplus x_1 \cdot x_2$;

8) 01100011 (99) – $f_{99} = x_2 \oplus x_3 \oplus x_1 \cdot x_3$;

9) 01100101 (101) – $f_{101} = x_2 \oplus x_3 \oplus x_1 \cdot x_2$;

10) 00111001 (106) – $f_{106} = x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_2$;

11) 01101100 (108) – $f_{108} = x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_3$;

12) 01111000 (120) – $f_{120} = x_1 \oplus x_2 \oplus x_3 \oplus x_2 \cdot x_3$.

Тоді можна записати й представлення криптографічних функцій поліномами Жегалкіна, яке набуде наступного виду:

- операція перетворення:

$$F^{k}_{30,57,106} = \begin{bmatrix} x_1 \oplus x_2 \cdot x_3 \\ x_1 \oplus x_2 \oplus x_1 \cdot x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_2 \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{45,54,106} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot x_3, \\ x_2 \oplus x_1 \cdot x_3, \\ x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_2 \end{bmatrix};$$

- операція перетворення:

$$F^{k}_{30,89,108} = \begin{bmatrix} x_1 \oplus x_2 \cdot x_3 \\ x_1 \oplus x_3 \oplus x_1 \cdot x_2 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_3 \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{45,106,54} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_2 \\ x_2 \oplus x_1 \cdot x_3 \end{bmatrix};$$

- операція перетворення:

$$F^{k}_{30,106,57} = \begin{bmatrix} x_1 \oplus x_2 \cdot x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_2 \\ x_1 \oplus x_2 \oplus x_1 \cdot x_3 \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{75,86,108} = \begin{bmatrix} x_1 \oplus x_3 \oplus x_2 \cdot x_3 \\ x_3 \oplus x_1 \cdot x_2 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_3 \end{bmatrix}.$$

Інше поліноміальне представлення елементарних функцій у базисі $\langle \wedge, \oplus, HE \rangle$ (модульно-дискретне представлення) матиме вигляд:

$$00011110\ (30) - f_{30} = x_1 \oplus (x_2 \cdot x_3); \tag{2.86}$$

$$00101101\ (45) - f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3); \tag{2.87}$$

$$00110110\ (54) - f_{54} = x_2 \oplus (x_1 \cdot x_3); \tag{2.88}$$

$$00111001\ (57) - f_{57} = x_2 \oplus (x_1 \cdot \bar{x}_3); \tag{2.89}$$

$$01001011\ (75) - f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3); \tag{2.90}$$

$$01010110\ (86) - f_{86} = x_3 \oplus (x_1 \cdot x_2); \tag{2.91}$$

$$01011001\ (89) - f_{89} = x_3 \oplus (x_1 \cdot \bar{x}_2); \tag{2.92}$$

$$01100011\ (99) - f_{99} = x_2 \oplus (\bar{x}_1 \cdot x_3); \tag{2.93}$$

$$01100101\ (101) - f_{101} = x_3 \oplus (\bar{x}_1 \cdot x_2); \tag{2.94}$$

$$01101100\ (108) - f_{108} = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3); \tag{2.95}$$

$$00111001\ (106) - f_{106} = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2); \tag{2.96}$$

$$01111000\ (120) - f_{120} = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3). \tag{2.97}$$

Тоді представлення криптографічних функцій буде таким:

- операція перетворення:

$$F^k_{30,57,106} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3), \\ x_2 \oplus (x_1 \cdot \bar{x}_3), \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція оберненого перетворення:

$$F^d_{45,54,106} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3), \\ x_2 \oplus (x_1 \cdot x_3), \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція перетворення:

$$F^{k}_{30,89,108} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{45,106,54} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot x_3) \end{bmatrix};$$

- операція перетворення:

$$F^{k}_{30,106,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{75,86,108} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}.$$

Крім цього, від поліноміального представлення можливо перейти до дискретно-алгебраїчного представлення основних елементарних функцій таким чином:

$$00011110\ (30) - f_{30} = \begin{cases} x_1, & якщо \quad x_2 \cdot x_3 = 0 \\ \bar{x}_1, & якщо \quad x_2 \cdot x_3 = 1 \end{cases};$$

$$00111001\ (57) - f_{57} = \begin{cases} x_2, & якщо \quad x_1 \cdot \bar{x}_3 = 0 \\ \bar{x}_2, & якщо \quad x_1 \cdot \bar{x}_3 = 1 \end{cases};$$

$$00111001\ (106) -. f_{106} = \begin{cases} \bar{x}_3, & якщо \quad \bar{x}_1 \cdot \bar{x}_2 = 0 \\ x_3, & якщо \quad \bar{x}_1 \cdot \bar{x}_2 = 1 \end{cases};$$

$$00101101\ (45) - f_{45} = \begin{cases} x_1, & якщо \quad x_2 \cdot \bar{x}_3 = 0 \\ \bar{x}_1, & якщо \quad x_2 \cdot \bar{x}_3 = 1 \end{cases};$$

$$00110110\ (54) - f_{54} = \begin{cases} x_2, & якщо \quad x_1 \cdot x_3 = 0 \\ \bar{x}_2, & якщо \quad x_1 \cdot x_3 = 1 \end{cases}.$$

Тоді представлення криптографічних функцій запишеться як вектор-система:

- операція перетворення:

$$F^k_{30,57,106} = \left[\begin{cases} x_1, & якщо \quad x_2 \cdot x_3 = 0 \\ \bar{x}_1, & якщо \quad x_2 \cdot x_3 = 1 \end{cases}, \begin{cases} x_2, & якщо \quad x_1 \cdot \bar{x}_3 = 0 \\ \bar{x}_2, & якщо \quad x_1 \cdot \bar{x}_3 = 1 \end{cases}, \begin{cases} \bar{x}_3, & якщо \quad \bar{x}_1 \cdot \bar{x}_2 = 0 \\ x_3, & якщо \quad \bar{x}_1 \cdot \bar{x}_2 = 1 \end{cases} \right];$$

- операція оберненого перетворення:

$$F^d_{45,54,106} = \left[\begin{cases} x_1, & якщо \quad x_2 \cdot \bar{x}_3 = 0 \\ \bar{x}_1, & якщо \quad x_2 \cdot \bar{x}_3 = 1 \end{cases}, \begin{cases} x_2, & якщо \quad x_1 \cdot x_3 = 0 \\ \bar{x}_2, & якщо \quad x_1 \cdot x_3 = 1 \end{cases}, \begin{cases} \bar{x}_3, & якщо \quad \bar{x}_1 \cdot \bar{x}_2 = 0 \\ x_3, & якщо \quad \bar{x}_1 \cdot \bar{x}_2 = 1 \end{cases} \right];$$

- операція перетворення:

$$F^k_{30,108,89} = \left[\begin{cases} x_1 & якщо \quad x_2 \cdot x_3 = 0 \\ \bar{x}_1 & якщо \quad x_2 \cdot x_3 = 1 \end{cases}, \begin{cases} x_2 & якщо \quad \bar{x}_1 \cdot \bar{x}_3 = 0 \\ \bar{x}_2 & якщо \quad \bar{x}_1 \cdot \bar{x}_3 = 1 \end{cases}, \begin{cases} x_3 & якщо \quad x_1 \cdot \bar{x}_2 = 0 \\ \bar{x}_3 & якщо \quad x_1 \cdot \bar{x}_2 = 1 \end{cases} \right];$$

- операція оберненого перетворення:

$$F^{d}_{75,108,86} = \begin{bmatrix} \begin{cases} x_1 & якщо \ \ \bar{x}_2 \cdot x_3 = 0 \\ \bar{x}_1 & якщо \ \ \bar{x}_2 \cdot x_3 = 1 \end{cases} \\ \begin{cases} x_2 & якщо \ \ \bar{x}_1 \cdot \bar{x}_3 = 0 \\ \bar{x}_2 & якщо \ \ \bar{x}_1 \cdot \bar{x}_3 = 1 \end{cases} \\ \begin{cases} x_3 & якщо \ \ x_1 \cdot x_2 = 0 \\ \bar{x}_3 & якщо \ \ x_1 \cdot x_2 = 1 \end{cases} \end{bmatrix};$$

- операція перетворення:

$$F^{k}_{45,54,106} = \begin{bmatrix} \begin{cases} x_1 & якщо \ \ x_2 \cdot \bar{x}_3 = 0 \\ \bar{x}_1 & якщо \ \ x_2 \cdot \bar{x}_3 = 1 \end{cases} \\ \begin{cases} x_2 & якщо \ \ x_1 \cdot x_3 = 0 \\ \bar{x}_2 & якщо \ \ x_1 \cdot x_3 = 1 \end{cases} \\ \begin{cases} x_3 & якщо \ \ \bar{x}_1 \cdot \bar{x}_2 = 0 \\ \bar{x}_3 & якщо \ \ \bar{x}_1 \cdot \bar{x}_2 = 1 \end{cases} \end{bmatrix};$$

- операція оберненого перетворення:

$$F^{d}_{30,57,106} = \begin{bmatrix} \begin{cases} x_1 & якщо \ \ x_2 \cdot x_3 = 0 \\ \bar{x}_1 & якщо \ \ x_2 \cdot x_3 = 1 \end{cases} \\ \begin{cases} x_2 & якщо \ \ x_1 \cdot \bar{x}_3 = 0 \\ \bar{x}_2 & якщо \ \ x_1 \cdot \bar{x}_3 = 1 \end{cases} \\ \begin{cases} x_3 & якщо \ \ \bar{x}_1 \cdot \bar{x}_2 = 0 \\ \bar{x}_3 & якщо \ \ \bar{x}_1 \cdot \bar{x}_2 = 1 \end{cases} \end{bmatrix}.$$

Наведене дискретно-алгебраїчне представлення елементарних функцій можна трактувати по іншому, а саме:

$$00011110\ (30) - f_{30} = \begin{cases} x_2 \cdot x_3, & якщо \ \ x_1 = 0 \\ \overline{x_2 \cdot x_3}, & якщо \ \ x_1 = 1 \end{cases};$$

$$00111001\ (57) - f_{57} = \begin{cases} x_1 \cdot \bar{x}_3, & якщо \quad x_2 = 0 \\ \overline{x_1 \cdot \bar{x}_3}, & якщо \quad x_2 = 1 \end{cases};$$

$$00101101\ (45) - f_{45} = \begin{cases} x_2 \cdot \bar{x}_3, & якщо \quad x_1 = 0 \\ \overline{x_2 \cdot \bar{x}_3}, & якщо \quad x_1 = 1 \end{cases};$$

$$00110110\ (54) - f_{54} = \begin{cases} x_1 \cdot x_3, & якщо \quad x_2 = 0 \\ \overline{x_1 \cdot x_3}, & якщо \quad x_2 = 1 \end{cases};$$

$$00111001\ (106) - f_{106} = \begin{cases} \bar{x}_1 \cdot \bar{x}_2, & якщо \quad x_3 = 0 \\ \overline{\bar{x}_1 \cdot \bar{x}_2}, & якщо \quad x_3 = 1 \end{cases}.$$

Звідси представлення криптографічних функцій перетворення відповідно:

- операція кодування:

$$F^k_{30,57,106} = \begin{bmatrix} \begin{cases} x_2 \cdot x_3, & якщо \quad x_1 = 0 \\ \overline{x_2 \cdot x_3}, & якщо \quad x_1 = 1 \end{cases} \\ \begin{cases} x_1 \cdot \bar{x}_3, & якщо \quad x_2 = 0 \\ \overline{x_1 \cdot \bar{x}_3}, & якщо \quad x_2 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot \bar{x}_2, & якщо \quad x_3 = 0 \\ \overline{\bar{x}_1 \cdot \bar{x}_2}, & якщо \quad x_3 = 1 \end{cases} \end{bmatrix};$$

- операція оберненого перетворення:

$$F^d_{45,54,106} = \begin{bmatrix} \begin{cases} x_2 \cdot \bar{x}_3, & якщо \quad x_1 = 0 \\ \overline{x_2 \cdot \bar{x}_3}, & якщо \quad x_1 = 1 \end{cases} \\ \begin{cases} x_1 \cdot x_3, & якщо \quad x_2 = 0 \\ \overline{x_1 \cdot x_3}, & якщо \quad x_2 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot \bar{x}_2, & якщо \quad x_3 = 0 \\ \overline{\bar{x}_1 \cdot \bar{x}_2}, & якщо \quad x_3 = 1 \end{cases} \end{bmatrix}.$$

Наведені представлення криптографічних функцій у перспективі дають можливість зрозуміти логіку роботи дискретних пристроїв перетворення інформації на основі криптографічних операцій. А представлені способи запису дозволяють виокремити структурні блоки для реалізації схемотехнічних рішень синтезованих криптографічних операцій.

У результаті дослідження способів запису криптографічних функцій перетворення інформації було встановлено, що всі способи запису мають право на існування і використовуються відповідно до задач дослідження.

Завдяки представленим різним способам запису криптографічних функцій перетворення інформації, виникла можливість побудови різноваріантних дискретних пристроїв на основі однотипних схемотехнічних конструкцій, що в подальшому дозволяє контролювати та обмежувати складність пристроїв.

На основі отриманих результатів можна зробити висновок, що кожному способу запису можна поставити у відповідність структурні блоки, що реалізують логічні перетворення над даними за правилом, описаним криптографічними функціями.

Висновки з розділу 2

1. На основі проведення обчислювального експерименту визначено множину трирозрядних елементарних функцій, яка забезпечує побудову операцій криптографічного перетворення, але на даний час не досліджувалася. Дана множина трирозрядних елементарних функцій на основі класифікації по складності моделей елементарних функцій була визначена як група елементарних функцій розширеного матричного перетворення.

2. Розроблено та формалізовано метод синтезу елементарних функцій розширеного матричного перетворення, який забезпечує синтез прямої,

оберненої чи повної множини елементарних функцій. Отримано залежності розрахунку потужності множин елементарних функцій розширеного матричного перетворення в залежності від кількості розрядів інформації, яка перетворюється.

3. Проведено аналіз форм представлення функцій криптографічного перетворення, на основі якого встановлено, що для проведення подальших досліджень доцільно використовувати поліноміальне та дискретно-алгебраїчне представлення, так як вони спрощують процес доведення коректності виконання криптографічних операцій.

4. Результати розділу опубліковані в [2, 3, 9, 14].

РОЗДІЛ 3
СИНТЕЗ ТА ДОСЛІДЖЕННЯ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ НА ОСНОВІ РОЗШИРЕНОГО МАТРИЧНОГО ПРЕДСТАВЛЕННЯ

3.1 Синтез операцій криптографічного перетворення на основі трирозрядних елементарних функцій розширеного матричного представлення

3.1.1 Синтез операцій криптографічного перетворення на основі обчислювального експерименту

За результатами обчислювального експерименту (додаток Б) на основі прямих трирозрядних елементарних функцій розширеного матричного перетворення були отримані операції криптографічного перетворення інформації:

пряме перетворення:

$$F^{k}_{30,57,106} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

$$F^{k}_{30,89,108} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^{k}_{30,106,57} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^{k}_{30,108,89} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix}$$

обернене перетворення:

$$F^{d}_{45,54,106} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

$$F^{d}_{45,106,54} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

$$F^{d}_{75,86,108} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee \cdot x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^{d}_{75,108,86} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee \cdot x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix}$$

пряме перетворення:

$$F^{k}_{45,54,106}=\begin{bmatrix} x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{k}_{45,89,99}=\begin{bmatrix} x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{k}_{45,99,89}=\begin{bmatrix} x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{k}_{45,106,54}=\begin{bmatrix} x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{k}_{54,45,106}=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{k}_{54,101,120}=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{k}_{54,106,45}=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{k}_{54,120,101}=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{k}_{57,30,106}=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{k}_{57,75,101}=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3 \end{bmatrix}$$

обернене перетворення:

$$F^{d}_{30,57,106}=\begin{bmatrix} x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot x_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{d}_{75,101,57}=\begin{bmatrix} x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{d}_{45,99,89}=\begin{bmatrix} x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{d}_{30,89,108}=\begin{bmatrix} x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{d}_{54,45,106}=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{d}_{106,45,54}=\begin{bmatrix} x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{d}_{86,75,108}=\begin{bmatrix} \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{d}_{108,75,86}=\begin{bmatrix} x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3 \end{bmatrix}$$

$$F^{d}_{57,30,106}=\begin{bmatrix} \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3 \end{bmatrix}$$

$$F^{d}_{99,45,89}=\begin{bmatrix} x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3 \end{bmatrix}$$

пряме перетворення:

$$F^{k}_{57,101,75}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

$$F^{k}_{57,106,89}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{75,57,101}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{75,86,108}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{75,101,57}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{75,108,86}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{86,75,108}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{86,99,120}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{86,108,75}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

$$F^{k}_{86,120,99}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

обернене перетворення:

$$F^{d}_{101,75,57}=\begin{bmatrix}x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{89,30,108}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{75,57,101}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{30,106,57}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{45,89,99}=\begin{bmatrix}x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

$$F^{d}_{30,108,89}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{54,106,45}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{106,54,45}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{86,108,75}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

$$F^{d}_{108,86,75}=\begin{bmatrix}x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

пряме перетворення:

$$F^{k}_{89,30,108}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{89,45,99}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

$$F^{k}_{89,99,45}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{89,108,30}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\end{bmatrix}$$

$$F^{k}_{99,45,89}=\begin{bmatrix}x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{99,86,120}=\begin{bmatrix}x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{99,89,45}=\begin{bmatrix}x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{99,120,86}=\begin{bmatrix}x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{101,54,120}=\begin{bmatrix}x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{101,57,75}=\begin{bmatrix}x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

обернене перетворення:

$$F^{d}_{57,106,30}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\end{bmatrix}$$

$$F^{d}_{99,89,45}=\begin{bmatrix}x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{101,57,75}=\begin{bmatrix}x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

$$F^{d}_{89,108,30}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\end{bmatrix}$$

$$F^{d}_{57,75,101}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee\cdot x_1\cdot x_2\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{106,30,57}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{89,45,99}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

$$F^{d}_{108,30,89}=\begin{bmatrix}x_1\cdot\bar{x}_2\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{d}_{106,57,30}=\begin{bmatrix}x_1\cdot\bar{x}_3\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\vee\bar{x}_1\cdot x_2\cdot x_3\end{bmatrix}$$

$$F^{d}_{89,99,45}=\begin{bmatrix}\bar{x}_1\cdot x_3\vee x_2\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot\bar{x}_2\vee x_1\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

пряме перетворення:

$$F^k_{101,75,57} = \begin{bmatrix} x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee \cdot x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^k_{101,120,54} = \begin{bmatrix} x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

$$F^k_{106,30,57} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^k_{106,45,54} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

$$F^k_{106,54,45} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \\ x_1 \cdot \overline{x}_2 \vee x_1 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^k_{106,57,30} = \begin{bmatrix} x_1 \cdot \overline{x}_3 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \end{bmatrix}$$

$$F^k_{108,30,89} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^k_{108,75,86} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee \cdot x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^k_{108,86,75} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee \cdot x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

$$F^k_{108,89,30} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \end{bmatrix}$$

обернене перетворення:

$$F^d_{57,101,75} = \begin{bmatrix} \overline{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee \cdot x_1 \cdot x_2 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

$$F^d_{108,89,30} = \begin{bmatrix} x_1 \cdot \overline{x}_2 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \end{bmatrix}$$

$$F^d_{99,86,120} = \begin{bmatrix} x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^d_{108,89,30} = \begin{bmatrix} \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \vee \overline{x}_1 \cdot x_2 \cdot x_3 \end{bmatrix}$$

$$F^d_{86,99,120} = \begin{bmatrix} \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \\ x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^d_{101,54,120} = \begin{bmatrix} x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^d_{99,120,86} = \begin{bmatrix} x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^d_{54,120,101} = \begin{bmatrix} \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \end{bmatrix}$$

$$F^d_{86,120,99} = \begin{bmatrix} \overline{x}_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ x_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee \overline{x}_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

$$F^d_{101,120,54} = \begin{bmatrix} x_1 \cdot x_3 \vee \overline{x}_2 \cdot x_3 \vee \overline{x}_1 \cdot x_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee \overline{x}_1 \cdot x_3 \vee x_1 \cdot \overline{x}_2 \cdot \overline{x}_3 \\ \overline{x}_1 \cdot x_2 \vee x_2 \cdot \overline{x}_3 \vee x_1 \cdot \overline{x}_2 \cdot x_3 \end{bmatrix}$$

пряме перетворення: **обернене перетворення:**

$$F^{k}_{120,54,101}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}\quad F^{d}_{120,99,86}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{120,86,99}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}\quad F^{d}_{120,86,99}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

$$F^{k}_{120,99,86}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee\bar{x}_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee x_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}\quad F^{d}_{120,54,101}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\end{bmatrix}$$

$$F^{k}_{120,101,54}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}\quad F^{d}_{120,101,54}=\begin{bmatrix}\bar{x}_1\cdot x_2\vee\bar{x}_1\cdot x_3\vee x_1\cdot\bar{x}_2\cdot\bar{x}_3\\ x_1\cdot x_3\vee\bar{x}_2\cdot x_3\vee\bar{x}_1\cdot x_2\cdot\bar{x}_3\\ \bar{x}_1\cdot x_2\vee x_2\cdot\bar{x}_3\vee x_1\cdot\bar{x}_2\cdot x_3\end{bmatrix}$$

В результаті обчислювального експерименту отримано 42 операції криптографічного перетворення інформації на основі прямих трирозрядних елементарних функцій розширеного матричного перетворення.

Загальна кількість операцій криптографічного перетворення (N) утворюється поєднанням базових операцій ($N_б$), операцій перестановки ($N_п$) та операцій інверсії ($N_і$):

$$N = N_б \cdot N_п \cdot N_і \tag{3.1}$$

Так як у нас отримано 42 операції криптографічного перетворення інформації на основі прямих трирозрядних елементарних функцій, то, як наслідок, відсутня група операцій, пов’язаних з інверсними операціями.

Представлена група операцій утворена поєднанням лише базових операцій та операцій перестановки. Визначимо кількість базових операцій на основі виразу (3.1):

$$N = N_б \cdot N_п \cdot N_і = N_б \cdot 3! = 48\text{, тоді } N_і = 8 \tag{3.2}$$

Щоб визначити базові операції, необхідно розсортувати та згрупувати операції криптоперетворення на основі перестановок елементарних функцій. Результати роботи представлені в табл. 3.1. В таблиці для більшої наглядності наведено лише нумерацію елементарних функцій криптоперетворення.

Таблиця 3.1

Результати дослідження операцій криптографічного перетворення (пряме, обернене) інформації на основі прямих трирозрядних елементарних функцій розширеного матричного представлення

пря-ме	обер нене	пря-ме	обер нене	пря-ме	обер нене	пря-ме	обер нене	пря-ме	обер нене	пря -ме	оберн ене
30	45	30	75	57	57	57	89	106	99	106	101
57	54	106	86	30	30	106	30	30	86	57	54
106	106	57	108	106	106	30	108	57	120	30	120
30	45	30	75	89	57	89	89	108	99	108	101
89	106	108	108	30	106	108	108	30	120	89	120
108	54	89	86	108	30	30	30	89	86	30	54
45	30	45	30	54	54	54	86	106	54	106	86
54	57	106	89	45	45	106	75	45	101	54	99
106	106	54	108	106	106	45	108	54	120	45	120
45	75	45	45	89	99	89	101	99	57	99	106
89	101	99	99	45	89	99	57	45	75	86	30
99	57	89	89	99	45	45	75	89	101	120	57
75	75	75	45	57	99	57	101	101	89	101	57
57	57	101	89	75	45	101	75	57	99	75	101
101	101	57	99	101	89	75	57	75	45	57	75
75	30	75	30	86	54	86	86	108	54	108	86
86	106	108	108	75	106	108	108	75	120	86	120
108	57	86	89	108	45	75	75	86	101	75	99
120	120	120	120	54	106	54	108	101	106	101	108
54	99	101	101	101	45	120	75	54	57	120	89
101	86	54	54	120	54	101	86	120	30	54	30
120	120	120	120	86	106	86	108	99	108	99	106
86	86	99	54	99	54	120	86	120	30	86	30
99	99	86	101	120	45	99	75	86	89	120	57

Базова група операцій формується вибором однієї функції з шести в кожному рядку. З кожного рядка табл. 3.1 вибирається лише одна базова операція.

Наприклад:

- з першого рядка виберемо операцію $F^k_{30,57,106}$:

$$F^k_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \qquad F^d_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$$

- з другого рядка виберемо операцію $F^k_{30,89,108}$:

$$F^k_{30,89,147} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix} \qquad F^d_{45,149,54} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot x_3) \end{bmatrix}$$

- з третього рядка виберемо операцію $F^k_{45,54,106}$:

$$F^k_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \qquad F^d_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$$

- з четвертого рядка виберемо операцію $F^k_{45,89,99}$:

$$F^k_{45,89,99} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \qquad F^d_{75,101,57} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}$$

- з п’ятого рядка виберемо операцію $F^k_{75,57,101}$:

$$F^k_{75,57,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} \qquad F^d_{75,57,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix}$$

- з шостого рядка виберемо операцію $F^k_{75,86,108}$:

$$F^k_{75,86,147} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix} \qquad F^d_{30,149,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$$

- з сьомого рядка виберемо операцію $F^{k}_{120,54,101}$:

$$F^{k}_{135,54,101} = \begin{bmatrix} x_1 \oplus (\overline{x}_2 \cdot \overline{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\overline{x}_1 \cdot x_2) \end{bmatrix} \qquad F^{d}_{135,99,86} = \begin{bmatrix} x_1 \oplus (\overline{x}_2 \cdot \overline{x}_3) \\ x_2 \oplus (\overline{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix}$$

- з восьмого рядка виберемо операцію $F^{k}_{120,86,99}$:

$$F^{k}_{135,86,99} = \begin{bmatrix} x_1 \oplus (\overline{x}_2 \cdot \overline{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\overline{x}_1 \cdot x_3) \end{bmatrix} \qquad F^{d}_{135,86,99} = \begin{bmatrix} x_1 \oplus (\overline{x}_2 \cdot \overline{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\overline{x}_1 \cdot x_3) \end{bmatrix}$$

Так як базова група може утворювати математичну групу операцій, то на основі обчислювального експерименту було зроблено спробу знайти базові операції. Основний принцип знаходження базових операцій полягає в наступному: якщо операції утворюють групу, то повторне перетворення не призводить до збільшення криптостійкості, тобто існує якась операція, результат якої співпадає з результатом двох попередніх операцій.

3.1.2 Синтез операцій криптографічного перетворення на основі моделі операцій розширеного матричного представлення

Для визначення базової групи операцій криптографічного перетворення проведемо аналіз результатів синтезу базових груп на основі інших елементарних функцій.

Серед останніх досліджень даної задачі особливу увагу привертає ряд публікацій. Зокрема, в [72] введено поняття вектор-функції, здійснено перехід від опису перетворення двох сусідніх байтів як відображення множини самої на себе до задання таблиці можливих значень двох логічних функцій, що дало змогу будь-яку вектор-функцію подати у вигляді перестановки. Причому наведено обґрунтування, що кожній дворозрядній логічній функції можна поставити у відповідність чотирьохелементну

перестановку. Крім цього показано, що множина дворозрядних логічних функцій з введеною операцією композиції є групою.

В [124] показана можливість еквівалентного подання логічної функції у вигляді модифікованої перестановки, сформульовано правило одержання оберненої функції з функції перетворення на основі використання теорії перестановок.

Результати, наведені в [112, 113], цікаві синтезом нових функцій, а також систематизацією повної множини логічних функцій для криптографічного перетворення.

Одним з найбільш поширених підходів до синтезу базових операцій [165-168] є їх побудова на основі дискретно-алгебраїчного представлення з вибором елементарних функцій зі збільшенням номеру основного аргументу.

На основі даного підходу виділено базові операції криптографічного перетворення:

- пряме перетворення:

$$F^{k}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \overline{x}_3) \\ x_3 \oplus (\overline{x}_1 \cdot \overline{x}_2) \end{bmatrix} \quad (3.3)$$

- обернене перетворення:

$$F^{d}_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \overline{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\overline{x}_1 \cdot \overline{x}_2) \end{bmatrix} \quad (3.4)$$

- пряме перетворення:

$$F^{k}_{30,147,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\overline{x}_1 \cdot \overline{x}_3) \\ x_3 \oplus (x_1 \cdot \overline{x}_2) \end{bmatrix} \quad (3.5)$$

- обернене перетворення:

$$F^{d}_{75,147,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} \quad (3.6)$$

- пряме перетворення:

$$F^{k}_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \quad (3.7)$$

- обернене перетворення:

$$F^{d}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \quad (3.8)$$

- пряме перетворення:

$$F^{k}_{45,99,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} \quad (3.9)$$

- обернене перетворення:

$$F^{d}_{45,99,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} \quad (3.10)$$

- пряме перетворення:

$$F^{k}_{75,57,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} \quad (3.11)$$

- обернене перетворення:

$$F^{d}_{75,57,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} \quad (3.12)$$

- пряме перетворення:

$$F^{k}_{75,147,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} \quad (3.13)$$

- обернене перетворення:

$$F^{d}_{30,147,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} \quad (3.14)$$

- пряме перетворення:

$$F^{k}_{135,54,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} \quad (3.15)$$

- обернене перетворення:

$$F^{d}_{135,99,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} \quad (3.16)$$

- пряме перетворення:

$$F^{k}_{135,99,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} \quad (3.17)$$

- обернене перетворення:

$$F^{d}_{135,54,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} \quad (3.18)$$

Розглянемо синтез операцій криптографічного перетворення на основі модульно-дискретного представлення елементарних функцій.

По аналогії з синтезом елементарних функцій в дискретному представленні (2.71-2.73) розробимо метод синтезу елементарних функцій

розширеного матричного перетворення в модульно-дискретному представленні.

Як видно з прямих функцій розширеного матричного перетворення (2.86)-(2.97), лише один аргумент входить до складу всіх трьох доданків логічного додавання. Класифікуємо ці елементарні функції за даною ознакою:

- функції на основі x_1:

$$f_{30} = x_1 \oplus (x_2 \cdot x_3);$$
$$f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3);$$
$$f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3);$$
$$f_{135} = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3).$$

У загальному вигляді елементарну функцію розширеного матричного перетворення операції на основі x_1 можна представити:

$$f = x_1 \oplus (\hat{x}_2 \cdot \hat{x}_3) \qquad (3.19)$$

де $\hat{x}$ – будь-яке значення аргументу;

- функції на основі x_2:

$$f_{54} = x_2 \oplus (x_1 \cdot x_3);$$
$$f_{57} = x_2 \oplus (x_1 \cdot \bar{x}_3);$$
$$f_{99} = x_2 \oplus (\bar{x}_1 \cdot x_3);$$
$$f_{147} = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3).$$

У загальному вигляді елементарну функцію розширеного матричного перетворення операції на основі x_2 можна представити:

$$f = x_2 \oplus (\hat{x}_1 \cdot \hat{x}_3) \qquad (3.20)$$

- функції на основі x_3:

$$f_{86} = x_3 \oplus (x_1 \cdot x_2);$$

$$f_{89} = x_3 \oplus (x_1 \cdot \bar{x}_2);$$

$$f_{101} = x_3 \oplus (\bar{x}_1 \cdot x_2);$$

$$f_{149} = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2).$$

У загальному вигляді елементарну функцію розширеного матричного перетворення операції на основі x_3 можна представити:

$$f = x_3 \oplus (\hat{x}_1 \cdot \hat{x}_2). \qquad (3.21)$$

Виходячи з виразів (3.19)-(3.21), правила отримання прямої елементарної функції будуть формалізовані виразом:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l) \qquad (3.22)$$

за умови: $i \in [1,2,3]$; $j \in [1,2,3]$; $l \in [1,2,3]$; $i \neq j \neq l$, де $\hat{x}$ – будь-яке значення аргументу.

На основі узагальнених виразів (3.19)-(3.22) можна приступити до синтезу операцій криптографічного перетворення в загальному вигляді.

Почнемо синтез з першої функції. Першою елементарною операцією повинна бути операція розширеного матричного перетворення функції на основі x_1:

$$f = x_1 \oplus (\hat{x}_2 \cdot \hat{x}_3). \qquad (3.23)$$

Друга операція на основі x_2 має в другому доданку інверсне значення x_3 другого доданку першої функції. x_1 може приймати будь-яке значення.

Виходячи з цього, друга елементарна функція матиме представлення:

$$f = x_2 \oplus (\hat{x}_1 \cdot \bar{\hat{x}}_3). \qquad (3.24)$$

Третя операція на основі x_3 має в другому доданку інверсне значення x_1 до другого доданку x_1 другої функції, x_2 приймає значення інверсне значення x_2 другого доданку першої елементарної функції.

Виходячи з цього, третя елементарна функція матиме представлення:

$$f = x_3 \oplus (\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2). \tag{3.25}$$

Виходячи з виразів (3.19), (3.24), (3.25), операція криптографічного перетворення при синтезі, починаючи з першої елементарної функції:

$$F^k = \begin{bmatrix} x_1 \oplus (\hat{x}_2 \cdot \hat{x}_3) \\ x_2 \oplus (\hat{x}_1 \cdot \bar{\hat{x}}_3) \\ x_3 \oplus (\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2) \end{bmatrix} \tag{3.26}$$

По аналогії, якщо почати синтез з другої функції отримаємо:

$$F^k = \begin{bmatrix} x_1 \oplus (\hat{x}_2 \cdot \bar{\hat{x}}_3) \\ x_2 \oplus (\hat{x}_1 \cdot \hat{x}_3) \\ x_3 \oplus (\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2) \end{bmatrix} \tag{3.27}$$

По аналогії, якщо почати синтез з третьої функції отримаємо:

$$F^k = \begin{bmatrix} x_1 \oplus (\bar{\hat{x}}_2 \cdot \bar{\hat{x}}_3) \\ x_2 \oplus (\bar{\hat{x}}_1 \cdot \hat{x}_3) \\ x_3 \oplus (\hat{x}_1 \cdot \hat{x}_2) \end{bmatrix} \tag{3.28}$$

Вирази (3.26)-(3.28) дозволяють синтезувати операції криптографічного перетворення на основі розширеного матричного представлення.

3.2 Синтез операцій криптографічного перетворення на основі елементарних функцій розширеного матричного представлення методом заміни

Множину основних елементарних функцій, з яких формуються криптографічні операції, можливо використовувати як для прямого, так і для оберненого перетворення відповідно.

Згідно методу синтезу операцій криптографічного перетворення на основі додавання за модулем два, наведеного в [119], доведено, що для синтезу трирозрядних операцій криптографічного перетворення можуть використовуватися наступні елементарні логічні функції.

Розглянемо можливість синтезу базових операцій розширеного матричного перетворення на основі даного методу.

Для синтезу базових операцій використаємо елементарні функції розширеного матричного перетворення (2.86) – (2.97).

Для представлення результатів синтезу використаємо розширене матричне перетворення, а також табличне розширене матричне представлення.

Наприклад:

$$F^{k}_{15,57,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +-- \\ 1+0 \\ --+ \end{bmatrix} \qquad (3.29)$$

В табличному розширеному матричному перетворенні кожний стовпчик відображає змінну x_1, x_2, x_3 відповідно. Знаками «+» позначено наявність першого доданку розширеного матричного перетворення. Другий доданок розширеного матричного перетворення відображається символами «1» та «0». Якщо змінна в другому доданку представлена прямим значенням, вона кодується символом «1», якщо інверсним – символом «0», якщо змінна в рядку не використовується, то це відображається символом «–».

Табличне розширене матричне представлення буде необхідне для синтезу базових операцій оберненого криптографічного перетворення при відомій операції перетворення.

Синтезуємо базові операції криптографічного перетворення, а також наведемо відповідні їм обернені операції криптографічного перетворення на основі однієї, двох та трьох замін (додаток В).

В результаті синтезу отримано 42 базові операції криптографічного перетворення на основі розширеного матричного перетворення. Кількість базових операцій співпадає з кількістю операцій, отриманих на основі обчислювального експерименту.

3.3 Синтез операцій криптографічного перетворення на основі моделі операції методом виключення

Дослідження повної множини базових операцій криптографічного перетворення дозволило сформулювати метод синтезу операцій криптографічного перетворення на основі моделі операції методом виключення, сутність якого полягає в наступному:

1. Синтез множини операцій розширеного матричного перетворення на основі виразу (3.26).

2. Розширення множини операцій за рахунок видалення доповнення з однієї або двох операцій.

3. Видалення операцій, які повторюються.

4. Розширення множини операцій за рахунок перестановки розрядів у кожній операції.

5. Розширення групи операцій за рахунок введення інверсії елементарних функцій.

Розглянемо реалізацію даного методу на прикладі.

Відповідно до виразу (3.26) буде отримано 8 операцій розширеного матричного криптографічного перетворення:

- операція 1 $$F^{k}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 2 $$F^{k}_{30,147,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 3 $$F^{k}_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 4 $$F^{k}_{45,99,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 5 $$F^{k}_{75,57,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix};$$

- операція 6 $$F^{k}_{75,147,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix};$$

- операція 7 $$F^{k}_{135,54,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix};$$

- операція 8 $$F^{k}_{135,99,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix}.$$

На основі операції 1, виключивши по одному розширенню, отримаємо:

- операція 1.1 $$F^{k}_{15,57,149} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 1.2 $$F^{k}_{30,51,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 1.3 $$F^{k}_{30,57,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}.$$

На основі операції 2, виключивши по одному розширенню, отримаємо:

- операція 2.1 $$F^{k}_{15,147,89} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 2.2 $$F^{k}_{30,51,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 2.3 $$F^{k}_{30,147,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}.$$

Аналогічно необхідно отримати всі операції на основі виключення одного розширення.

Зробивши виключення одного розширення, отримаємо операції з виключенням двох розширень:

- операція 1.1.1 $$F^{k}_{15,51,149} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 1.1.2 $$F^{k}_{15,57,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix};$$

- операція 1.2.1 $$F^{k}_{15,51,149} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix};$$

- операція 1.2.1 $$F^{k}_{30,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix}.$$

Так як операції 1.1.1 і 1.2.1 співпадають, то операція 1.2.1 повинна бути виключена з групи базових операцій розширеного матричного криптографічного перетворення, що синтезується.

З отриманих операцій за допомогою виключень двох розширень отримаємо одну операцію з виключенням трьох розширень $F^{k}_{15,51,85} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$.

В результаті синтезу отримано 42 базові операції криптографічного перетворення на основі розширеного матричного представлення. Кількість базових операцій співпадає з кількістю операцій, отриманих на основі обчислювального експерименту та операцій, синтезованих на основі елементарних функцій розширеного матричного перетворення методом заміни.

Слід відзначити, що синтез операцій криптографічного перетворення на основі моделі операції методом виключення спрощує процес синтезу, шляхом використання формалізованої моделі операції перетворення.

Висновки з розділу 3

1. За результатами обчислювального експерименту на основі прямих трирозрядних елементарних функцій розширеного матричного перетворення отримані операції криптографічного перетворення інформації та визначено принцип знаходження базових операцій.

2. На основі підходу побудови базових операцій у дискретно-алгебраїчному представленні, що базується на виборі елементарних функцій зі збільшенням номеру основного аргументу, виділено базові операції криптографічного перетворення. Розроблено метод синтезу елементарних функцій розширеного матричного перетворення в модульно-дискретному представленні та отримано вирази синтезу операцій криптографічного перетворення на основі розширеного матричного перетворення.

3. Проведено синтез базових операцій криптографічного перетворення з наведенням відповідних обернених операцій на основі однієї, двох та трьох замін. Визначено, що кількість базових операцій співпадає з кількістю операцій, отриманих на основі обчислювального експерименту. Для представлення результатів синтезу було використано розширене матричне представлення, а також табличне розширене матричне представлення.

4. Розроблено метод синтез операцій криптографічного перетворення на основі моделі операції методом виключення, який спрощує процес синтезу, шляхом використання формалізованої моделі операції перетворення.

5. Результати розділу опубліковані в [4, 13].

РОЗДІЛ 4
СИНТЕЗ ОПЕРАЦІЙ ОБЕРНЕНОГО КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО ПРЕДСТАВЛЕННЯ

4.1 Підхід до синтезу операцій оберненого криптографічного перетворення на основі функцій розширеного матричного представлення

У загальному вигляді базові операції розширеного матричного перетворення з урахуванням інверсії можна представити як суму за модулем два операцій перетворення, з яких $\vec{F}_a$, $\vec{F}_b$ – лінійні матричні перетворення, а $\vec{F}_c$ – нелінійне матричне перетворення:

$$\vec{F}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} a_{11}x_1 \oplus a_{12}x_2x_3 \oplus b_1 \\ a_{12}x_2 \oplus a_{22}x_1x_3 \oplus b_2 \\ a_{13}x_3 \oplus a_{32}x_1x_2 \oplus b_3 \end{bmatrix} = \begin{bmatrix} a_{11}x_1 \\ a_{12}x_2 \\ a_{13}x_3 \end{bmatrix} \oplus \begin{bmatrix} a_{12}x_2x_3 \\ a_{22}x_1x_3 \\ a_{32}x_1x_2 \end{bmatrix} \oplus \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \vec{F}_a\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \oplus \vec{F}_c\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \oplus \vec{F}_b\begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}, \quad (4.1)$$

де $a_{11} = a_{12} = a_{13} = 1$, $a_{i2} \in [0,1]$, $b_i \in [0,1]$, $\oplus$ – операція: сума за модулем два.

Дане представлення дає змогу спростити знаходження оберненого матричного перетворення, тому що виокремлює нелінійне матричне перетворення $\vec{F}_c$.

Отже, використовуючи матричне представлення логічних операцій перетворення як базової та інверсії, можна визначити повний набір базових логічних операцій та операцій інверсії відповідно.

Представлення (4.1) дає змогу розглядати базову операцію та операцію інверсії окремо. Крім цього, додатково можна ввести трирозрядну логічну операцію перестановки. Зрозуміло, що для трьох розрядів існує лише шість перестановок.

Використовуючи розширене матричне перетворення та застосовуючи перестановку відносно базової операції, отримаємо повний набір перестановок.

Таким чином, загальна кількість операцій, що утворюються поєднанням базової, перестановки та інверсії визначається як загальна кількість комбінацій таких операцій:

$$Count(\vec{F}_a, \vec{F}_p, \vec{F}_b,) = \vec{F}_a \times \vec{F}_p \times \vec{F}_b = 42 \times 6 \times 8 = 2016.$$

Крім цього, зрозуміло, що при поєднанні даних операцій важливе значення має їх порядок застосування. Наприклад, якщо для процесу перетворення названі операції виконувалися в заданому порядку, то для процесу оберненого перетворення потрібно їх виконувати відповідно в зворотному (рис. 4.1).

Рис. 4.1. Процес криптографічного перетворення

При поєднанні базових операцій, операцій перестановки та інверсії (матриці $\vec{F}_a$, $\vec{F}_c$, $\vec{F}_b$) операція розширеного матричного перетворення буде мати вигляд:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3 \\ a_{31}x_1 \oplus a_{32}x_2 \oplus a_{3\,3}x_3 \end{pmatrix} \oplus \begin{pmatrix} a_{11}x_2x_3 \oplus a_{12}x_1x_3 \oplus a_{13}x_1x_2 \\ a_{21}x_2x_3 \oplus a_{22}x_1x_3 \oplus a_{23}x_1x_2 \\ a_{31}x_2x_3 \oplus a_{32}x_1x_3 \oplus a_{3\,3}x_1x_2 \end{pmatrix} \oplus \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}.$$

Побудова операції оберненого перетворення проводиться шляхом побудови оберненої операції матричного перетворення та добудови матриці розширеного перетворення.

Враховуючи обмеження на операцію матричного перетворення для розширеного матричного представлення, було доведено, що, якщо $F^k = (A)$, а $F^d = \left(A^{-1}\right)$, то $A_{ij}^{-1} = A_{ji}$. Було доведено, що компланарна матриця буде оберненою матрицею.

Процес синтезу операцій оберненого криптографічного перетворення на основі елементарних функцій розширеного матричного представлення будемо досліджувати поетапно.

На першому етапі дослідимо операції перетворення, синтезовані на основі однієї заміни.

При заміні однієї операції операцією розширеного матричного представлення, операції прямого та оберненого криптографічного перетворення співпадають.

На другому етапі дослідимо операції криптоперетворення, синтезовані на основі заміни двох операцій.

При заміні двох операцій операціями розширеного матричного перетворення, операції прямого та оберненого криптографічного перетворення співпадають.

На третьому етапі дослідимо операції криптоперетворення, синтезовані на основі заміни трьох операцій.

При заміні трьох операцій операціями розширеного матричного перетворення, операції прямого та оберненого криптографічного перетворення також співпадають.

В загальному виді операції матричного криптографічного перетворення побудовані на основі додавання за модулем два будуть описані наступною моделлю:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \oplus c_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \oplus c_2 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \oplus c_n \end{pmatrix}, \tag{4.2}$$

де $a_{ij}, c_i, x_i \in [0,1]$; $i = 1..n$, n – кількість розрядів інформації, $x_1 ... x_n$ – операнди-розряди інформації відповідно; a_{ij} – коефіцієнти матриці кодування; c_i – ознака наявності групи операцій інверсії; $\oplus$ – операція «сума за mod 2».

Якщо операція криптографічного перетворення без урахування групи операцій інверсії задана виразом:

$$\vec{F}_k = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \end{pmatrix}, \tag{4.3}$$

тоді операція оберненого криптографічного перетворення буде задана виразом:

$$\vec{F}_d = \begin{pmatrix} b_{11}y_1 \oplus b_{12}y_2 \oplus ... \oplus b_{1n}y_n \\ b_{21}y_1 \oplus b_{22}y_2 \oplus ... \oplus b_{2n}y_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{n1}y_1 \oplus b_{n2}y_2 \oplus ... \oplus b_{n\,n}y_n \end{pmatrix}, \tag{4.4}$$

де b_i – коефіцієнти оберненої матриці, y_i – операнди-розряди інформації, які отримані в результаті застосування операції кодування ($y_i = \vec{F}_k(x_i)$) відповідно. Тоді результатом виконання оберненої операції повинен бути вираз, що має такий запис:

$$\vec{F}_r = \begin{pmatrix} a_{11}x_1 & & & \\ & a_{22}x_2 & & \\ . & . & . & . \\ & & & a_{nn}x_n \end{pmatrix}, \qquad (4.5)$$

де $\vec{F}_r$ – еталонна матриця або матриця-результат, $x_1 \ldots x_n$ – початкові операнди-розряди інформації; $a_{ij} = 1$ при $i = j$, тому що потрібно забезпечити невиродженість перетворення, тобто повинна виконуватись умова $a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \neq 0$, а також відсутні перестановки рядків матриці.

Розглянемо докладніше процес знаходження оберненої операції (матриці):

$$\vec{F}_d = \begin{pmatrix} b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n) \\ b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n) \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n) \end{pmatrix} = \begin{pmatrix} a_{11}x_1 & & & \\ & a_{22}x_2 & & \\ . & . & . & . \\ & & & a_{nn}x_n \end{pmatrix}, \qquad (4.6)$$

Розглянемо можливість використання даного методу для побудови обернених операцій з використанням розширеного матричного представлення.

Одним із варіантів використання розширеного матричного представлення можуть бути доповнення матричного представлення розширеним матричним представленням.

$$\vec{F}_k = \begin{bmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n \end{bmatrix} \oplus \begin{bmatrix} b_1^1 \\ b_2^1 \\ \ldots \\ b_n^1 \end{bmatrix} \oplus \begin{bmatrix} d_1(x_1 \oplus (\hat{x}_i \cdot \hat{x}_j)) \\ d_2(x_2 \oplus (\hat{x}_i \cdot \hat{x}_j)) \\ . \quad . \quad . \quad . \quad . \quad . \\ d_n(x_n \oplus (\hat{x}_i \cdot \hat{x}_j)) \end{bmatrix} \oplus \begin{bmatrix} d_1 b_1^2 \\ d_2 b_2^2 \\ \ldots \\ d_n b_n^2 \end{bmatrix} \qquad (4.7)$$

Параметри d_i, $\hat{x}_i$, $\hat{x}_j$ визначаються вимогами до базових операцій розширеного матричного перетворення залежно від прийнятого підходу до синтезу операцій розширеної базової групи.

Проведемо розрахунок кількості операцій розширеного матричного перетворення для даного прикладу.

Якщо для розширеного матричного перетворення вибирається одна матриця, то загальна кількість операцій криптоперетворення – 2016 разів.

Якщо для розширеного матричного перетворення вибирається дві матриці, то загальна кількість операцій криптоперетворення збільшиться в 2016^2 разів.

Якщо для розширеного матричного перетворення вибирається k матриць, то загальна кількість операцій криптоперетворення збільшиться в 2016^k разів, де k<n/3.

Розширене матричне перетворення дає можливість збільшити кількість операцій криптографічного перетворення та, як наслідок, підвищити криптостійкість систем захисту інформації, тому що операції матричного й розширеного матричного перетворення за результатами дослідження не утворюють однієї групи.

Розширене матричне перетворення дозволяє значно збільшити кількість операцій криптографічного перетворення та, як наслідок, підвищити криптостійкість систем захисту інформації.

4.2 Аналіз обернених операцій у розширеному матричному представленні

Наведений метод синтезу матричних операцій оберненого криптографічного перетворення характеризується тим, що він дозволив поєднати синтез обернених операцій для базових операцій та операцій перестановки.

Спробуємо за аналогією отримати аналогічний метод синтезу операцій оберненого криптографічного перетворення для розширеного матричного представлення.

Для спрощення представлення закономірностей і синтезу алгоритму оберненого криптоперетворення введемо наступні означення:

Означення 4.1. Розширення елементарної функції розширеного матричного перетворення називається прямим, якщо обидва аргументи другого доданка не мають інверсії.

Означення 4.2. Розширення елементарної функції розширеного матричного перетворення називається інверсним, якщо обидва аргументи другого доданка мають інверсії.

Означення 4.3. Розширення елементарної функції розширеного матричного перетворення називається змішаним, якщо один із аргументів другого доданка не має інверсії, а другий має інверсію.

Виберемо з базових операцій криптографічного перетворення кілька операцій із однією заміною й розглянемо перестановки елементарних функцій (додаток Д).

Відзначимо наступні закономірності для операцій криптографічного перетворення, синтезованих на основі однієї заміни.

1. Якщо пряма операція перетворення має пряме представлення розширення, то й обернена операція має пряме представлення розширення.

2. Якщо пряма операція перетворення має інверсне представлення розширення, то й обернена операція перетворення має інверсне представлення розширення.

3. Якщо пряма операція перетворення має змішане представлення розширення, то й обернена операція перетворення має змішане представлення розширення.

Представивши матрицю розширеного матричного перетворення як суму матриць за модулем 2, матриці перетворення й розширеної матриці

перетворення, знайдемо обернену матрицю перетворення для першої матриці. Відповідно до виразів (4.2) – (4.6) отримаємо:

$$\vec{F}_d = \begin{pmatrix} b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3) \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3) \oplus \\ \oplus b_{13}(a_{31}x_1 \oplus a_{32}x_2 \oplus a_{33}x_3) \\ b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3) \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3) \oplus \\ \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n) \\ b_{31}(a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3) \oplus b_{32}(a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3) \oplus \\ \oplus b_{33}(a_{31}x_1 \oplus a_{32}x_2 \oplus \ldots \oplus a_{33}x_3) \end{pmatrix} = \begin{pmatrix} a_{11}x_1 & & \\ & a_{22}x_2 & \\ & & a_{33}x_3 \end{pmatrix}. \quad (4.8)$$

1. Знайдемо перший рядок оберненої матриці перетворення:

$$b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3) \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3) \oplus \\ \oplus b_{13}(a_{31}x_1 \oplus a_{32}x_2 \oplus a_{3\,3}x_3) = a_{11}x_1 \quad .$$

Так як $x_1 = 1$, а $x_j = 0$ при $j \neq 1$, тоді b_{1i} є рішенням системи рівнянь:

$$\begin{cases} b_{11}a_{11} \oplus b_{12}a_{21} \oplus b_{13}a_{31} = 1 \\ b_{11}a_{12} \oplus b_{12}a_{22} \oplus b_{13}a_{3\,2} = 0 \\ b_{11}a_{13} \oplus b_{12}a_{23} \oplus \ldots \oplus b_{13}a_{33} = 0 \end{cases} . \quad (4.9)$$

2. Знайдемо другий рядок оберненої матриці перетворення:

$$b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3) \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3) \oplus \\ \oplus b_{23}(a_{31}x_1 \oplus a_{32}x_2 \oplus \ldots \oplus a_{3\,3}x_3) = a_{22}x_2 \quad .$$

Так як $x_2 = 1$, а $x_j = 0$ при $j \neq 2$, тоді b_{2i} є рішенням системи рівнянь:

$$\begin{cases} b_{21}a_{11} \oplus b_{22}a_{21} \oplus b_{23}a_{31} = 0 \\ b_{21}a_{12} \oplus b_{22}a_{22} \oplus b_{23}a_{3\,2} = 1 \\ b_{21}a_{13} \oplus b_{22}a_{23} \oplus b_{23}a_{3\,3} = 0 \end{cases} . \quad (4.10)$$

3. Знайдемо 3-ий рядок оберненої матриці перетворення:

$$b_{31}(a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3) \oplus b_{32}(a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3) \oplus \\ \oplus b_{33}(a_{31}x_1 \oplus a_{32}x_2 \oplus \ldots \oplus a_{3\,3}x_3) = a_{3\,3}x_3 \quad .$$

Так як $x_n = 1$, а $x_j = 0$ при $j \neq n$, тоді b_{ni} є рішенням системи рівнянь:

$$\begin{cases} b_{31}a_{11} \oplus b_{32}a_{21} \oplus b_{33}a_{31} = 0 \\ b_{31}a_{12} \oplus b_{32}a_{22} \oplus b_{33}a_{32} = 0 \\ b_{31}a_{13} \oplus b_{32}a_{23} \oplus ... \oplus b_{33}a_{33} = 1 \end{cases}. \qquad (4.11)$$

На основі рішення систем рівнянь (4.8) – (4.10) буде отримана перша обернена матриця перетворення. Застосування даного підходу й синтез першої оберненої матриці перетворення дозволили отримати наступні правила синтезу операцій оберненого криптографічного перетворення за наявності в прямій операції прямого, інверсного та змішаного розширення:

1. Якщо в матричному перетворенні елементарна операція на основі a_{ij} була розширеною, то відповідна їй елементарна операція b_{lk} за умови $k = i$, де $i, j, l, k \in \{1...3\}$, теж буде розширеною.

2. Якщо в матричному перетворенні елементарна операція на основі a_{ij} була прямою, то відповідна їй елементарна операція b_{lk} за умови $k = i$ теж буде прямою.

3. Якщо в матричному перетворенні елементарна операція на основі a_{ij} була інверсною, то відповідна їй елементарна операція b_{lk} за умови $k = i$ теж буде інверсною.

4. Якщо в матричному перетворенні елементарна операція на основі a_{ij} була змішаною, то відповідна їй елементарна операція b_{lk} за умови $k = i$ теж буде змішаною.

Аналіз таблиці показав, що знайти закономірність отримання оберненої операції перетворення за наявності змішаної операції перетворення при одній заміні не є можливим.

Проведемо аналогічні дослідження для операцій криптографічного перетворення, отриманих на основі двох замін. Для цього виберемо з базових

операцій криптографічного перетворення кілька операцій з однією заміною і розглянемо перестановки елементарних функцій (додаток Ж).

Відзначимо наступні закономірності для операцій криптографічного перетворення, синтезованих на основі двох замін.

1. Якщо пряма операція перетворення має пряме й інверсне представлення розширення, то й обернена операція перетворення має пряме й інверсне представлення розширення.

2. Якщо пряма операція має пряме та змішане представлення розширення, то й обернена операція перетворення має пряме та змішане представлення розширення.

3. Якщо пряма операція має інверсне й змішане представлення розширення, то й обернена операція перетворення має інверсне й змішане представлення розширення.

Отримані правила синтезу другої оберненої матриці перетворення для операцій криптографічного перетворення на основі двох замін співпали з правилами синтезу операцій перетворення на основі однієї заміни з поправкою, що їх необхідно застосовувати двічі до кожної розширеної елементарної операції:

1. Якщо в матричному перетворенні елементарна операція на основі a_{ij} була розширеною, то відповідна їй елементарна операція b_{lk} за умови $k = i$, де $i, j, l, k \in \{1...3\}$, теж буде розширеною.

2. Якщо в матричному перетворенні елементарна операція на основі a_{ij} була прямою, то відповідна їй елементарна операція b_{lk} за умови $k = i$ теж буде прямою.

3. Якщо в матричному перетворенні елементарна операція на основі a_{ij} була інверсною, то відповідна їй елементарна операція b_{lk} за умови $k = i$ теж буде інверсною.

4. Якщо в матричному перетворенні елементарна операція на основі a_{ij} була змішаною, то відповідна їй елементарна операція b_{lk} за умови $k = i$ теж буде змішаною.

Аналіз таблиць показав, що знайти закономірність отримання оберненої операції перетворення за наявності змішаної прямої операції перетворення при двох замінах також, як і при одній заміні, не є можливим.

Проведемо дослідження операцій розширеного матричного криптографічного перетворення, отриманих на основі трьох замін. Деякі результати суміщення базових операцій і операцій перестановки наведені в додатку З.

Відзначимо наступні закономірності для операцій криптографічного перетворення, синтезованих на основі трьох замін:

1. Якщо пряма операція криптоперетворення має пряме, інверсне й змішане представлення розширення, то й обернена операція має пряме, інверсне й змішане представлення розширення.

2. Якщо пряма операція криптоперетворення має три змішаних розширення, то й обернена операція має три змішаних розширення.

Отримані правила синтезу другої матриці оберненого криптографічного перетворення для операцій криптоперетворення на основі трьох замін співпали з правилами синтезу операцій криптоперетворення на основі однієї і двох замін з поправкою, що їх необхідно застосовувати тричі до кожної розширеної операції.

Подальші дослідження були спрямовані на встановлення правила формування розширеного подання оберненої матриці при наявності змішаного доповнення прямої операції.

Попередні дослідження показали, що найбільш складним є визначення правил формування змішаного доповнення, тому почнемо досліджувати отримання оберненої операції перетворення на основі прямої операції, яка включає пряме інверсне й змішане доповнення.

4.3 Синтез обернених операцій у розширеному матричному представленні з трьома замінами

В результаті аналізу таблиць були отримані правила синтезу другої оберненої матриці при наявності в прямій операції прямої, інверсної та змішаної заміни (Правило 4.1):

4.1.1. Якщо в матричному перетворенні розширення функції на основі a_{ij} було прямим, то відповідна їй елементарна функція b_{lk} за умови $k = i$, де $i, j, l, k \in \{1...3\}$, теж буде мати пряме розширення.

4.1.2. Якщо в матричному перетворенні розширення функції на основі a_{ij} було інверсним, то відповідна їй елементарна функція b_{lk} за умови $k = i$ також буде мати інверсне розширення.

4.1.3. Якщо в матричному перетворенні розширення функції на основі a_{ij} було змішаним, то відповідна їй елементарна функція b_{lk} за умови $k = i$ теж буде мати змішане розширення. Розстановка знаків інверсії в змішаному розширенні проводиться на основі формалізованого представлення операцій криптографічного перетворення відповідно до виразів (3.26) – (3.28), де кожна змінна має бути присутня двічі (в прямому й інверсному представленні).

Розглянемо отримані правила на прикладах.

Приклад 1. Нехай задана пряма операція криптоперетворення:

$$F^{k}_{30,149,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix} = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot x_3 \\ \bar{x}_1 \cdot \bar{x}_2 \\ x_1 \cdot \bar{x}_3 \end{bmatrix}.$$

Для першої матриці, вирішивши системи рівнянь (4.9) – (4.11), отримаємо:

$$F^{d}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \widetilde{y}_2 \cdot \widetilde{y}_3 \\ \widetilde{y}_1 \cdot \widetilde{y}_2 \\ \widetilde{y}_1 \cdot \widetilde{y}_3 \end{bmatrix},$$

де $\widetilde{y}_2$ – аргумент з невідомим значенням змінної, xx – невідомий номер операції.

Застосувавши перше та друге правило до матриці доповнення, отримаємо:

$$F^{d}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \cdot y_3 \\ \widetilde{y}_1 \cdot \widetilde{y}_2 \\ \overline{y}_1 \cdot \overline{y}_3 \end{bmatrix}.$$

На основі третього правила визначимо знаки інверсії у другому рядку матриці доповнення: y_1 повинно бути прямим, так як у третьому рядку $\overline{y}_1$, а y_2 – інверсним, так як в першому рядку y_2 пряме. Отже, отримаємо:

$$F^{d}_{30,89,147} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \cdot y_3 \\ y_1 \cdot \overline{y}_2 \\ \overline{y}_1 \cdot \overline{y}_3 \end{bmatrix} = \begin{bmatrix} y_1 \oplus (y_2 \cdot y_3) \\ y_3 \oplus (y_1 \cdot \overline{y}_2) \\ y_2 \oplus (\overline{y}_1 \cdot \overline{y}_3) \end{bmatrix}.$$

Отримана операція відповідає оберненій операції криптографічного перетворення, яку шукали.

Приклад 2. Нехай задана пряма операція криптоперетворення:

$$F^{k}_{149,45,54} = \begin{bmatrix} x_3 \oplus (\overline{x}_1 \cdot \overline{x}_2) \\ x_1 \oplus (x_2 \cdot \overline{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{x}_1 \cdot \overline{x}_2 \\ x_2 \cdot \overline{x}_3 \\ x_1 \cdot x_3 \end{bmatrix}.$$

Для першої матриці, вирішивши системи рівнянь (4.9) – (4.11), отримаємо:

$$F^{d}_{xx,xx,xx}=\begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix}\oplus\begin{bmatrix} \tilde{y}_1\cdot\tilde{y}_3 \\ \tilde{y}_1\cdot\tilde{y}_2 \\ \tilde{y}_2\cdot\tilde{y}_3 \end{bmatrix}.$$

Застосувавши перше та друге правило до матриці доповнення отримаємо:

$$F^{d}_{xx,xx,xx}=\begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix}\oplus\begin{bmatrix} \tilde{y}_1\cdot\tilde{y}_3 \\ y_1\cdot y_2 \\ \bar{y}_2\cdot\bar{y}_3 \end{bmatrix}.$$

На основі третього правила визначимо знаки інверсії у першому рядку матриці доповнення: y_1 повинно бути інверсним, так як в другому рядку y_1 пряме, а y_3 – прямим, так як в третьому рядку y_3 інверсне. Отже, отримаємо:

$$F^{d}_{99,86,135}=\begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{y}_1\cdot y_3 \\ y_1\cdot y_2 \\ \bar{y}_2\cdot\bar{y}_3 \end{bmatrix}=\begin{bmatrix} y_2\oplus(\bar{y}_1\cdot y_3) \\ y_3\oplus(y_1\cdot y_2) \\ y_1\oplus(\bar{y}_2\cdot\bar{y}_3) \end{bmatrix}.$$

Отримана операція відповідає оберненій операції криптографічного перетворення, яку шукали.

Отримані правила синтезу оберненої матриці перетворення за наявності в прямій матриці прямої, інверсної та змішаної замін, дозволили на основі додаткового аналізу таблиць отримати правила синтезу оберненої матриці перетворення за наявності в прямій матриці перетворення трьох змішаних замін.

Підхід до отримання правил синтезу оберненої матриці перетворення заснований на наступному:

1. Перехід від матриці на основі трьох змішаних замін до матриці з прямою, інверсною і змішаною замінами, зі змінних вибрати одну.

2. Знаходження оберненої матриці криптографічного перетворення.

3. Зворотний перехід до матриці з трьома змішаними замінами.

Отриманий підхід був реалізований отриманими правилами синтезу оберненої матриці криптографічного перетворення за наявності в прямій матриці трьох змішаних замін (Правило 4.2):

4.2.1. Для переходу від матриці на основі трьох змішаних замін до матриці з прямою, інверсною і змішаною замінами із змінних x_1, x_2, x_3 вибрати одну й інвертувати її в розширенні прямої матриці криптографічного перетворення.

4.2.2. Знайти обернену матрицю криптографічного перетворення на основі отриманої прямої матриці перетворення, яка включає пряму, інверсну та змішану заміни, для цього виконати наступне:

4.2.2.1. Якщо в прямій матриці криптографічного перетворення операція на основі a_{ij} була прямою, то відповідна їй операція b_{lk} за умови $k = i$, де $i, j, l, k \in \{1...3\}$ теж буде прямою.

4.2.2.2. Якщо в прямій матриці криптографічного перетворення операція на основі a_{ij} була інверсною, то відповідна їй операція b_{lk} за умови $k = i$ теж буде інверсною.

4.2.2.3. Якщо в прямій матриці криптографічного перетворення операція на основі a_{ij} була змішаною, то відповідна їй операція b_{lk} за умови $k = i$ теж буде змішаною. Розстановка знаків інверсії в змішаному розширенні проводиться на основі формалізованого представлення операцій криптографічного перетворення (виразів (3.26) – (3.28)), відповідно до яких кожна змінна у розширеному представленні має бути присутня двічі (в прямому й інверсному представленні).

4.2.3. Для забезпечення зворотного переходу до розширеної матриці з трьома змішаними замінами із змінних x_1, x_2, x_3 знайти таку, яка входить в пряме й інверсне доповнення, та інвертувати її в розширенні прямої матриці криптографічного перетворення.

Розглянемо отримані правила на прикладах.

Приклад 1. Нехай задана пряма операція криптографічного перетворення:

$$F^{k}_{45,89,99} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot \bar{x}_3 \\ x_1 \cdot \bar{x}_2 \\ \bar{x}_1 \cdot x_3 \end{bmatrix}.$$

Варіант рішення 1.

Оберемо змінну x_1 та після її інвертування отримаємо:

$$F^{k*}_{45,xx,xx} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot \bar{x}_2 \\ x_1 \cdot x_3 \end{bmatrix}.$$

Для першої матриці, вирішивши системи рівнянь (4.9) – (4.11), отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \tilde{y}_2 \cdot \tilde{y}_3 \\ \tilde{y}_1 \cdot \tilde{y}_2 \\ \tilde{y}_1 \cdot \tilde{y}_3 \end{bmatrix}.$$

Використавши правила 4.2.2.1 та 4.2.2.2 до матриці доповнення, отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \tilde{y}_2 \cdot \tilde{y}_3 \\ y_1 \cdot y_2 \\ \bar{y}_1 \cdot \bar{y}_3 \end{bmatrix}.$$

На основі правила 4.2.2.3 визначимо знаки інверсії в першому рядку матриці доповнення: y_2 повинно бути інверсним, так як у другому рядку y_2 пряме, а y_3 – прямим, так як у третьому рядку y_3 інверсне. Отже, отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \cdot y_3 \\ y_1 \cdot y_2 \\ \bar{y}_1 \cdot \bar{y}_3 \end{bmatrix}.$$

Відповідно до правила 4.2.2.3 проведемо інвертування змінної y_1, оскільки вона входить до прямого та інверсного розширення (другий і третій рядки):

$$F^{d}_{75,101,57} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \cdot y_3 \\ \bar{y}_1 \cdot y_2 \\ y_1 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_1 \oplus (\bar{y}_2 \cdot y_3) \\ y_3 \oplus (\bar{y}_1 \cdot y_2) \\ y_2 \oplus (y_1 \cdot \bar{y}_3) \end{bmatrix}.$$

Отримана операція відповідає операції оберненого перетворення, яку шукали.

Варіант рішення 2.

Оберемо змінну x_2 та після її інвертування отримаємо:

$$F^{k*}_{xx,xx,99} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{x}_2 \cdot \bar{x}_3 \\ x_1 \cdot x_2 \\ \bar{x}_1 \cdot x_3 \end{bmatrix}.$$

Для першої матриці, вирішивши системи рівнянь (4.9) – (4.11), отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \tilde{y}_2 \cdot \tilde{y}_3 \\ \tilde{y}_1 \cdot \tilde{y}_2 \\ \tilde{y}_1 \cdot \tilde{y}_3 \end{bmatrix}.$$

Використавши правила 4.2.2.1 та 4.2.2.2 до матриці доповнення, отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \cdot \bar{y}_3 \\ \tilde{y}_1 \cdot \tilde{y}_2 \\ y_1 \cdot y_3 \end{bmatrix}.$$

На основі правила 4.2.2.3 визначимо знаки інверсії в другому рядку матриці доповнення: y_1 повинно бути інверсним, так як у третьому рядку y_1

пряме, а y_2 – прямим, так як в першому рядку y_2 інверсне. Отже, отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \cdot \bar{y}_3 \\ \bar{y}_1 \cdot y_2 \\ y_1 \cdot y_3 \end{bmatrix}.$$

Відповідно до правила 4.2.2.3 проведемо інвертування змінної y_3, оскільки вона входить до прямого та інверсного розширення (перший і третій рядки):

$$F^{d}_{75,101,57} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_2 \cdot y_3 \\ \bar{y}_1 \cdot y_2 \\ y_1 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_1 \oplus (\bar{y}_2 \cdot y_3) \\ y_3 \oplus (\bar{y}_1 \cdot y_2) \\ y_2 \oplus (y_1 \cdot \bar{y}_3) \end{bmatrix}.$$

Отримана операція відповідає операції оберненого перетворення, яку шукали.

Варіант рішення 3.

Оберемо змінну x_3 та після її інвертування отримаємо:

$$F^{k*}_{xx,89,xx} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix} = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot x_3 \\ x_1 \cdot \bar{x}_2 \\ \bar{x}_1 \cdot \bar{x}_3 \end{bmatrix}.$$

Для першої матриці, вирішивши системи рівнянь (4.9) – (4.11), отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \tilde{y}_2 \cdot \tilde{y}_3 \\ \tilde{y}_1 \cdot \tilde{y}_2 \\ \tilde{y}_1 \cdot \tilde{y}_3 \end{bmatrix}.$$

Використавши правила 4.2.2.1 та 4.2.2.2 до матриці доповнення, отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \cdot y_3 \\ \bar{y}_1 \cdot \bar{y}_2 \\ \tilde{y}_1 \cdot \tilde{y}_3 \end{bmatrix}.$$

На основі правила 4.2.2.3 визначимо знаки інверсії в третьому рядку матриці доповнення: y_1 повинно бути прямим, так як у другому рядку y_1 інверсне, а y_3 – інверсним, так як у першому рядку y_3 пряме. Отже, отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \cdot y_3 \\ \overline{y}_1 \cdot \overline{y}_2 \\ y_1 \cdot \overline{y}_3 \end{bmatrix}.$$

Відповідно до правила 4.2.3 проведемо інвертування змінної y_2, оскільки вона входить до прямого та інверсного розширення (перший і другий рядки):

$$F^{d}_{75,101,57} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{y}_2 \cdot y_3 \\ \overline{y}_1 \cdot y_2 \\ y_1 \cdot \overline{y}_3 \end{bmatrix} = \begin{bmatrix} y_1 \oplus (\overline{y}_2 \cdot y_3) \\ y_3 \oplus (\overline{y}_1 \cdot y_2) \\ y_2 \oplus (y_1 \cdot \overline{y}_3) \end{bmatrix}.$$

Отримана операція відповідає операції оберненого перетворення, яку шукали.

Всі три варіанти рішення дають однаковий результат і мають однакову складність, оскільки повністю ідентичні операції, змінюються лише аргументи.

Приклад 2. Нехай задана операція перетворення:

$$F^{k}_{99,89,45} = \begin{bmatrix} x_2 \oplus (\overline{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \overline{x}_2) \\ x_1 \oplus (x_2 \cdot \overline{x}_3) \end{bmatrix} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{x}_1 \cdot x_3 \\ x_1 \cdot \overline{x}_2 \\ x_2 \cdot \overline{x}_3 \end{bmatrix}.$$

Оберемо змінну x_1 та після її інвертування отримаємо:

$$F^{k*}_{xx,xx,45} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\overline{x}_1 \cdot \overline{x}_2) \\ x_1 \oplus (x_2 \cdot \overline{x}_3) \end{bmatrix} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} x_1 \cdot x_3 \\ \overline{x}_1 \cdot \overline{x}_2 \\ x_2 \cdot \overline{x}_3 \end{bmatrix}.$$

Для першої матриці, вирішивши системи рівнянь (4.9) – (4.11), отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_3 \\ y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \widetilde{y}_1 \cdot \widetilde{y}_2 \\ \widetilde{y}_2 \cdot \widetilde{y}_3 \\ \widetilde{y}_1 \cdot \widetilde{y}_3 \end{bmatrix}.$$

Використавши правила 4.2.2.1 та 4.2.2.2 до матриці доповнення, отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_3 \\ y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \widetilde{y}_1 \cdot \widetilde{y}_2 \\ y_2 \cdot y_3 \\ \overline{y}_1 \cdot \overline{y}_3 \end{bmatrix}.$$

На основі правила 4.2.2.3 визначимо знаки інверсії в першому рядку матриці доповнення: y_1 повинно бути прямим, так як у третьому рядку y_1 інверсне, а y_2 – інверсним, так як в другому рядку y_2 пряме. Отже, отримаємо:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_3 \\ y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \cdot \overline{y}_2 \\ y_2 \cdot y_3 \\ \overline{y}_1 \cdot \overline{y}_3 \end{bmatrix}.$$

Відповідно до правила 3 проведемо інвертування змінної y_3, оскільки вона входить до прямого та інверсного розширення (другий і третій рядки):

$$F^{d}_{89,45,99} = \begin{bmatrix} y_3 \\ y_1 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \cdot \overline{y}_2 \\ y_2 \cdot \overline{y}_3 \\ \overline{y}_1 \cdot y_3 \end{bmatrix} = \begin{bmatrix} y_3 \oplus (y_1 \cdot \overline{y}_2) \\ y_3 \oplus (y_2 \cdot \overline{y}_3) \\ y_2 \oplus (\overline{y}_1 \cdot y_3) \end{bmatrix}.$$

Отримана операція відповідає операції оберненого перетворення, яку шукали.

Коректність правил 4.1 та правил 4.2 перевірена на основі обчислювального експерименту для повної множини операцій розширеного матричного представлення, отриманого на основі трьох замін.

4.4 Синтез обернених операцій у розширеному матричному представленні з двома замінами

Розглянемо можливість застосування правил 4.1 та правил 4.2 для синтезу операції оберненого перетворення на основі операції перетворення з двома замінами.

Підхід до отримання правил синтезу матриці оберненого перетворення заснований на наступному (Правило 4.3):

4.3.1. Перехід від матриці на основі двох замін до матриці з трьома замінами шляхом додаткового введення заміни, яка завжди однозначно визначається за допомогою виразів (3.26) – (3.28), відповідно до яких кожна змінна в розширеному представленні має бути присутня двічі (в прямому й інверсному представленні).

4.3.2. Знаходження матриці оберненого перетворення на основі правил 4.1. та 4.2.

4.3.3. Зворотний перехід до матриці оберненого перетворення з двома замінами, таким чином, якщо в матриці перетворення елементарна функція на основі a_{ij} була не розширеною, то відповідна їй елементарна функція b_{lk} за умови $k = i$, де $i, j, l, k \in \{1...3\}$ також буде не розширеною.

Розглянемо отримані правила на прикладах.

Приклад 1. Нехай задана операція перетворення:

$$F^{k}_{30,85,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix} = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot x_3 \\ - \quad - \\ x_1 \cdot \bar{x}_3 \end{bmatrix}.$$

Введемо додаткову третю заміну, нею може бути лише $x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2)$:

$$F^{k}_{30,xx,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix} = \begin{bmatrix} x_1 \\ x_3 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot x_3 \\ \bar{x}_1 \cdot \bar{x}_2 \\ x_1 \cdot \bar{x}_3 \end{bmatrix}.$$

Знайдемо матрицю оберненого перетворення на основі правила 4.1:

Для першої матриці, вирішивши системи рівнянь (4.9) – (4.11), отримаємо:

$$F^{d}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} \tilde{y}_2 \cdot \tilde{y}_3 \\ \tilde{y}_1 \cdot \tilde{y}_2 \\ \tilde{y}_1 \cdot \tilde{y}_3 \end{bmatrix}.$$

Використавши правила 4.1.1 та 4.1.2 до матриці доповнення, отримаємо:

$$F^{d}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \cdot y_3 \\ \tilde{y}_1 \cdot \tilde{y}_2 \\ \bar{y}_1 \cdot \bar{y}_3 \end{bmatrix}.$$

На основі правила 4.1.3 визначимо знаки інверсії в другому рядку матриці доповнення: y_1 повинно бути прямим, так як у третьому рядку $\bar{y}_1$, а y_2 – інверсним, так як у першому рядку y_2 пряме. Отже, отримаємо:

$$F^{d}_{xx,xx,xx} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \cdot y_3 \\ y_1 \cdot \bar{y}_2 \\ \bar{y}_1 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_1 \oplus (y_2 \cdot y_3) \\ y_3 \oplus (y_1 \cdot \bar{y}_2) \\ y_2 \oplus (\bar{y}_1 \cdot \bar{y}_3) \end{bmatrix}.$$

Так як змінна x_3 другого рядку матриці перетворення не мала розширення і, перетворившись в змінну y_2 матриці оберненого перетворення, перейшла в третій рядок, то відповідно до правила 4.3.3 в третьому рядку матриці оберненого перетворення повинно бути відсутнім розширення. Отже, отримаємо:

$$F^{d}_{30,89,51} = \begin{bmatrix} y_1 \\ y_3 \\ y_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \cdot y_3 \\ y_1 \cdot \bar{y}_2 \\ - \quad - \end{bmatrix} = \begin{bmatrix} y_1 \oplus (y_2 \cdot y_3) \\ y_3 \oplus (y_1 \cdot \bar{y}_2) \\ y_2 \end{bmatrix}.$$

Отримана операція відповідає операції оберненого перетворення, яку шукали.

Приклад 2. Нехай задана операція перетворення:

$$F^{k}_{89,15,99} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_1 \cdot \bar{x}_2 \\ - \quad - \\ \bar{x}_1 \cdot x_3 \end{bmatrix}.$$

Введемо додаткову третю заміну, нею може бути лише $x_1 \oplus (x_2 \cdot \bar{x}_3)$:

$$F^{k*}_{89,xx,99} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_1 \cdot \bar{x}_2 \\ x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_3 \end{bmatrix}.$$

Знайдемо матрицю оберненого перетворення на основі правила 3.4:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_1 \cdot y_3 \\ y_1 \cdot \bar{y}_2 \\ y_2 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_2 \oplus (\bar{y}_1 \cdot y_3) \\ y_3 \oplus (y_1 \cdot \bar{y}_2) \\ y_1 \oplus (y_2 \cdot \bar{y}_3) \end{bmatrix}.$$

Так як змінна x_1 другого рядку матриці перетворення не мала розширення і, перетворившись в змінну y_2 матриці, перейшла в перший рядок, то відповідно до правила 4.3.3 в першому рядку матриці оберненого перетворення повинно бути відсутнім розширення. Отже, отримаємо:

$$F^{d}_{51,89,45} = \begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} - \quad - \\ y_1 \cdot \bar{y}_2 \\ y_2 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_2 \\ y_3 \oplus (y_1 \cdot \bar{y}_2) \\ y_1 \oplus (y_2 \cdot \bar{y}_3) \end{bmatrix}.$$

Отримана операція відповідає операції оберненого перетворення, яку шукали.

Коректність правила 4.3 перевірена на основі обчислювального експерименту для повної множини операцій розширеного матричного перетворення, отриманого на основі двох замін.

4.5 Синтез обернених операцій у розширеному матричному представленні з однією заміною

Розглянемо можливість застосування правила 4.1 та правила 4.2 для синтезу операції оберненого перетворення на основі операції перетворення з однією змішаною заміною.

Підхід до отримання правил синтезу матриці оберненого перетворення заснований на введенні двох додаткових замін.

Відповідно до виразів (3.26) – (3.28) кожна змінна у розширеному представленні має бути присутня двічі (в прямому й інверсному представленні). Отже, можливі два варіанти заміни, які приведуть до:

- розширеного матричного представлення на основі прямого, інверсного й змішаного розширення;
- розширеного матричного представлення на основі трьох змішаних розширень.

Перевіримо коректність можливих варіантів введення двох замін на прикладі.

Приклад. Нехай задана операція перетворення:

$$F^{k}_{85,15,99} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} - & - \\ - & - \\ \bar{x}_1 \cdot x_3 \end{bmatrix}.$$

Введемо додаткові дві заміни.

Введеними замінами відповідно до виразів (3.26) – (3.28) можуть бути:

- $x_1 \oplus (x_2 \cdot \bar{x}_3)$ і $x_3 \oplus (x_1 \cdot \bar{x}_2)$;
- $x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3)$ і $x_3 \oplus (x_1 \cdot x_2)$.

Розглянемо варіант 1.

Перетворена операція прямого перетворення матиме вигляд:

$$F^{k*}_{xx,xx,99} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_1 \cdot \bar{x}_2 \\ x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_3 \end{bmatrix}.$$

Знайдемо матрицю оберненого перетворення на основі правила 4.4:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_1 \cdot y_3 \\ y_1 \cdot \bar{y}_2 \\ y_2 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_2 \oplus (\bar{y}_1 \cdot y_3) \\ y_3 \oplus (y_1 \cdot \bar{y}_2) \\ y_1 \oplus (y_2 \cdot \bar{y}_3) \end{bmatrix}.$$

Так як змінна x_3 першого рядка матриці перетворення не мала розширення і, перетворившись в змінну y_3 матриці оберненого перетворення перейшла у другий рядок, так як змінна x_1 другого рядку матриці перетворення не мала розширення і, перетворившись в змінну y_2 матриці оберненого перетворення перейшла в перший рядок, то відповідно до правила 4.3.3 у першому та другому рядках матриці оберненого перетворення повинно бути відсутнім розширення. Отже, отримаємо:

$$F^{d}_{51,85,45} = \begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} - & - \\ - & - \\ y_2 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_2 \\ y_3 \\ y_1 \oplus (y_2 \cdot \bar{y}_3) \end{bmatrix}.$$

Розглянемо варіант 2.

Перетворена операція прямого перетворення матиме вигляд:

$$F^{k*}_{xx,xx,99} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix} = \begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_1 \cdot x_2 \\ \bar{x}_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_3 \end{bmatrix}.$$

Знайдемо матрицю оберненого перетворення на основі правила 4.3.3:

$$F^{d*}_{xx,xx,xx} = \begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{y}_1 \cdot y_3 \\ y_1 \cdot \bar{y}_2 \\ y_2 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_2 \oplus (\bar{y}_1 \cdot \bar{y}_3) \\ y_3 \oplus (y_1 \cdot y_2) \\ y_1 \oplus (y_2 \cdot \bar{y}_3) \end{bmatrix}.$$

Так як змінна x_3 першого рядка матриці прямого перетворення не мала розширення і, перетворившись в змінну y_3 матриці оберненого перетворення перейшла у другий рядок, так як змінна x_1 другого рядку матриці перетворення не мала розширення і, перетворившись в змінну y_2 матриці оберненого перетворення перейшла в перший рядок, то відповідно до правила 4.3.3 у першому та другому рядках матриці оберненого перетворення повинно бути відсутнім розширення. Отже, отримаємо:

$$F^{d}_{51,85,45} = \begin{bmatrix} y_2 \\ y_3 \\ y_1 \end{bmatrix} \oplus \begin{bmatrix} - & - \\ - & - \\ y_2 \cdot \bar{y}_3 \end{bmatrix} = \begin{bmatrix} y_2 \\ y_3 \\ y_1 \oplus (y_2 \cdot \bar{y}_3) \end{bmatrix}.$$

Слід зазначити, що в першому та другому рядках були інверсне й пряме розширення. Проведені додаткові дослідження показали, що введення додаткової прямої та інверсної замін призводить до видалення з операції оберненого перетворення теж прямої та інверсної замін.

Розглянуті варіанти замін призводять до однакового результату, дозволяють правильно знайти операцію оберненого перетворення по заданій операції перетворення з однією змішаною заміною.

Так як правила 4.3 включають в себе правила 4.2 і їх реалізація вимагає виконання більшої кількості операцій для визначення операції оберненого перетворення, отже, доцільно застосовувати другий варіант заміни – вводити додатково пряме й інверсне розширення.

Виходячи з отриманих результатів, можна сформулювати правила синтезу операції оберненого перетворення на основі операції перетворення з однією змішаною заміною (Правила 4.4):

4.4.1. Перехід від матриці перетворення на основі однієї змішаної заміни до матриці з трьома замінами шляхом додаткового введення прямої та інверсної замін.

4.4.2. Знаходження матриці оберненого перетворення на основі правил 4.3.

4.4.3. Зворотний перехід до матриці оберненого перетворення з однією заміною шляхом видалення прямого й інверсного розширення.

Коректність правил 4.4 перевірена на основі обчислювального експерименту для повної множини операцій розширеного матричного перетворення, отриманого на основі однієї змішаної заміни.

Отримані результати дозволяють приступити до розробки методу захисту інформації на основі розширених матричних криптографічних операцій.

Висновки з розділу 4

1. Для розробки методу синтезу обернених операцій розширеного матричного перетворення запропоновано представити операцію за допомогою двох матричних перетворень: лінійного й нелінійного, що забезпечило спрощення синтезу оберненої матриці криптографічного перетворення.

2. Проведено поетапне дослідження процесу синтезу операцій оберненого криптографічного перетворення на основі елементарних функцій розширеного матричного перетворення та доведено, що розширене матричне перетворення дозволяє збільшити в 2016^k разів кількість операцій криптографічного перетворення при використанні поєднання k матриць.

3. На основі аналізу варіантів обернених операцій розширеного матричного перетворення запропоновано метод синтезу обернених операцій на основі побудови нелінійного оберненого матричного перетворення з використанням тимчасових підстановок.

4. Розробка методу синтезу обернених операцій розширеного матричного перетворення дозволила будувати системи криптографічного захисту інформації.

5. Результати розділу опубліковані в [1, 7, 8].

РОЗДІЛ 5
РЕАЛІЗАЦІЯ МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ОПЕРАЦІЙ РОЗШИРЕНОГО МАТРИЧНОГО ПЕРЕТВОРЕННЯ

5.1. Структура системи захисту інформації на основі операцій розширеного матричного криптографічного перетворення

Концепція розширеного матричного перетворення теоретично базується на експериментально доведеному факті, що операції матричного криптографічного перетворення та розширеного матричного криптографічного перетворення не утворюють групи операцій криптографічного перетворення. Як наслідок, повторне перетворення інформації операціями з іншої групи криптографічних операцій забезпечує підвищення криптографічної стійкості перетворення.

Виходячи з запропонованої концепції для забезпечення високої криптографічної стійкості, операції розширеного матричного криптографічного перетворення використовуються сумісно з операціями матричного криптографічного перетворення, і забезпечують попередню або подальшу обробку даних. Використання операцій розширеного матричного криптографічного перетворення перед та після операцій матричного перетворення неефективне, так як їх повторне використання не збільшує криптостійкості.

Отримані в попередніх розділах результати дозволяють сформулювати метод захисту інформаційних ресурсів на основі розширених матричних операцій криптографічного перетворення:

1. На основі даних пароля сформулювати первинну, не вироджену матрицю криптографічного перетворення.

2. Корекція матриці криптографічного перетворення на основі псевдовипадкової послідовності.

3. Перевірка правильності синтезу матриці криптографічного перетворення.

4. Криптографічне перетворення інформації на основі матриць криптографічного перетворення.

5. На основі псевдовипадкової послідовності будуються операції розширеного матричного криптографічного перетворення у випадково вибраній кількості.

6. Криптографічне перетворення інформації на основі розширеного матричного криптографічного перетворення.

7. Перехід до наступного циклу криптографічного перетворення (пункту 2) при наявності вхідної інформації.

При розробці методу захисту інформаційних ресурсів на основі розширених матричних операцій криптографічного перетворення взято метод захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення [116-118].

Структурна схема реалізації операцій розширеного матричного криптографічного перетворення представлена на рис. 5.1.

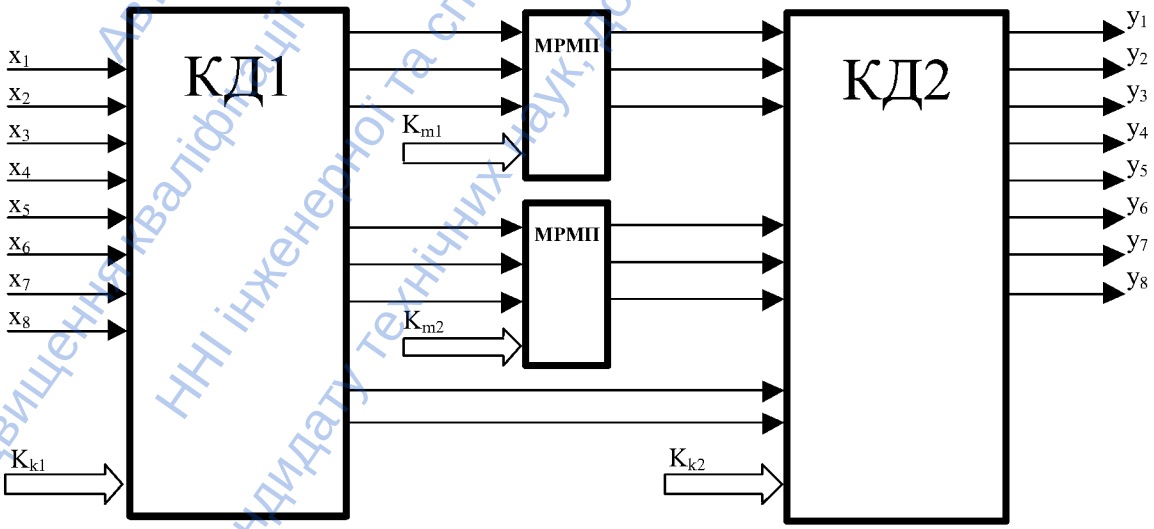

Рис. 5.1. Структурна схема реалізації операцій розширеного матричного криптографічного перетворення

На рис 5.1 позначено: КД1, КД2 – комутатори даних, які забезпечують перестановку біт або блоків даних залежно від згенерованої операції; МРМП – модулі розширеного матричного перетворення, які забезпечують виконання операцій розширеного матричного перетворення.

Функціональну схему модуля розширеного матричного криптографічного перетворення зображено на рис. 5.2.

Операція криптографічного перетворення відповідно до функціональної схеми реалізації буде виконуватися за час переключення п’яти логічних елементів.

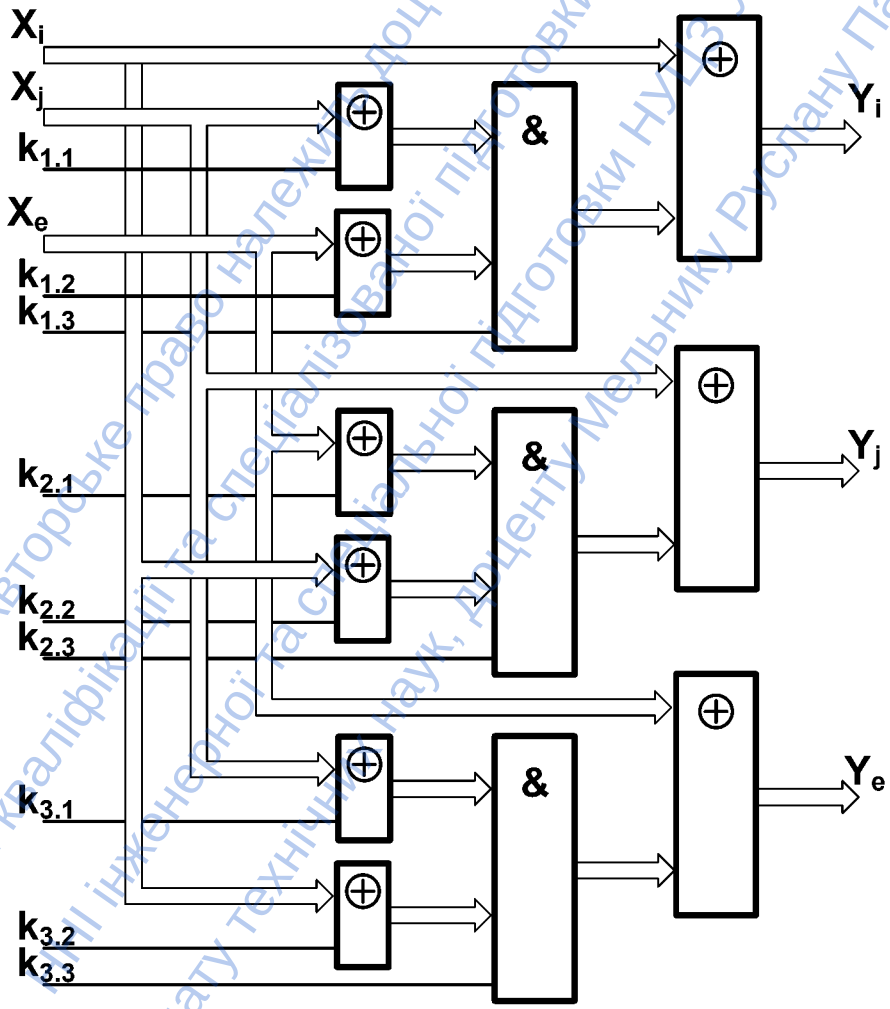

Рис. 5.2 Функціональна схема модуля розширеного матричного криптографічного перетворення

Модуль розширеного матричного криптографічного перетворення працює наступним чином: при подачі на входи X даних, а на входи K –

команд управління відповідно до матриці розширеного матричного криптографічного перетворення.

Визначимо криптографічну стійкість методу захисту інформації на основі розширених матричних операцій криптографічного перетворення на прикладі обробки 1 байта інформації.

Загальна кількість операцій, що утворюються поєднанням базової, перестановки та інверсії, визначається як загальна кількість комбінацій таких операцій:

$$Count(\vec{F}_a, \vec{F}_p, \vec{F}_b,) = \vec{F}_a \times \vec{F}_p \times \vec{F}_b = 42 \times 6 \times 8 = 2016.$$

Виходячи з запропонованої реалізації операцій розширеного матричного перетворення, кількість операцій, які можуть бути використані для шифрування інформації (St), буде визначатися:

$$St = (2016^{K_{mo}})^{Kc}, \tag{5.1}$$

де K_{mo} – кількість матричних операцій криптографічного перетворення, Kc – кількість циклів криптографічного перетворення, яка визначається як $Kc = m/n$, де m – довжина вхідної інформації, n – довжина блоку даних, який обробляється за один цикл.

Розрахунок кількості операцій для шифрування інформації залежно від кількості операцій у циклі та кількості циклів перетворення наведено в табл. 5.1.

Таблиця 5.1

Розрахунок кількості операцій для шифрування інформації

K_c / K_{mo}		**Кількість циклів**			
		1	**2**	**3**	**4**
Кількість операцій у циклі	**1**	2016	4064256	8193540096	2016^4
	2	4064256	4064256^2	4064256^3	4064256^4
	3	8193540096	8193540096^2	8193540096^3	8193540096^4

Проведемо статистичну оцінку характеристик псевдовипадкової послідовності, утвореної після виконання операцій розширеного матричного криптографічного перетворення на основі програмного пакету NIST STS.

5.2. Оцінка ефективності реалізації методу захисту інформації на основі операцій розширеного матричного криптографічного перетворення

5.2.1. Оцінка статистичних властивостей результатів шифрування на основі операцій розширеного матричного криптографічного перетворення

Оцінку методу підвищення якості систем захисту інформації здійснено на основі вимог статистичних тестів NIST STS (NIST Statistical test Suite). Даний набір тестів був запропонований в ході проведення конкурсу на новий національний стандарт США блокового шифрування. Цей набір використовувався для дослідження статистичних властивостей кандидатів на новий блоковий шифр. Сьогодні методика тестування, запропонована NIST є найбільш поширеною у розробників криптографічних засобів захисту інформації.

Порядок тестування окремої двійкової послідовності S має такий вигляд:

- висувається нульова гіпотеза H_0 – припущення того, що дана двійкова послідовність S випадкова;

- далі розраховується статистика тесту $c(S)$;

- використовуючи спеціальну функцію статистики тесту, вираховується значення вірогідності $P=f(c(S)),\ P \in [0,1]$;

- значення вірогідності P порівнюється з рівнем значення $\alpha \in [0.001, 0.01]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається. В протилежному випадку приймається альтернативна гіпотеза.

Пакет складається з 16 статистичних тестів. Однак, фізично в залежності від вхідних параметрів вираховується 189 значень вірогідності P, які можна розглядати як результат роботи окремих тестів. Опис пакету NIST STS приведено в додатку К [83].

В результаті тестування двійкової послідовності формується вектор значень вірогідності $P = \{P_1, P_2, ... P_{189}\}$. Аналіз значень P_i даного вектору дозволяє вказати конкретні дефекти випадковості тестової послідовності.

Для здійснення тестувань були обрані такі параметри:

- довжина послідовності, що тестується, n = 106 біт;
- кількість послідовностей, що тестується, m = 100;
- рівень значущості α = 0,01.

Таким чином,

- обсяг вибірки, що тестується, склав $N = 10^6 \times 100 = 108$ біт;
- кількість тестів (q) для різних довжин q = 189, таким чином, статистичний портрет генератора містить 18900 значень імовірності P.

В ідеальному випадку при m = 100 і α = 0,01 у ході тестування може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту має складати 99 %. Але це занадто жорстке правило. Тому застосовується правило на основі довірчого інтервалу для r_j. Нижня межа в цьому випадку складе значення r_{min} = 0,96015. З цих позицій аналізуються результати тестування генераторів.

Перевіримо на основі пакету тестів NIST STS метод захисту інформаційних ресурсів на основі розширених матричних операцій криптографічного перетворення.

Розроблений метод використовує для вибору матриць криптографічного перетворення генератор псевдовипадкової послідовності. Виберемо в якості генератора псевдовипадкової послідовності вбудований в

мови високого рівня генератор (датчик) псевдовипадкової послідовності RANDOM.

Застосуємо метод захисту інформаційних ресурсів на основі розширених матричних операцій криптографічного перетворення для покращення характеристик псевдовипадкової послідовності, яка генерується датчиком RANDOM. Для вирішення задачі на основі датчика на кожному циклі коректуємо матрицю перетворення та кодуємо вихідні дані датчика.

За допомогою тестів NIST STS буде виявлено відхилення монотонності закодованої інформації.

Результати тестування датчика представлені в додатку Л, зведені результати тестування – в табл. 5.2.

Алгоритм формування послідовності для перевірки матричного датчика (на основі RANDOM) програмним пакетом NIST-STS представлено на рис 5.3.

Таблиця 5.2

Результати тестування датчика

Генератор	**Кількість тестів, у яких тестування пройшли більше 99 % послідовностей**	**Кількість тестів, у яких тестування пройшли більше 96 % послідовностей**
Генератор RANDOM-РМП	127 (68 %)	189 (100 %)

Статичний портрет програмної реалізації матричного датчика (на основі RANDOM) зображено на рис. 5.4.

Результати тестування показали, що генератор RANDOM-РМП пройшов комплексний контроль за методикою NIST-STS.

Для оцінки якості перетворення будь-яких даних розробимо алгоритм реалізації методу захисту інформації на основі розширених матричних операцій криптографічного перетворення, який поєднує матричне та розширене матричне криптографічне перетворення. Даний алгоритм представлений на рис. 5.5.

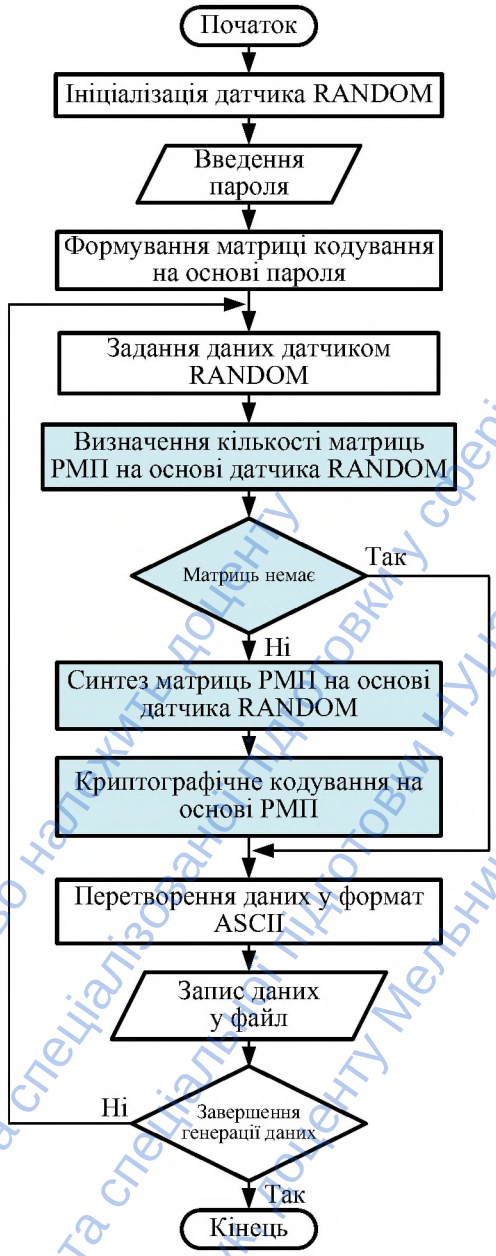

Рис. 5.3. Алгоритм формування послідовності псевдовипадкових чисел на основі розширеного матричного криптографічного перетворення

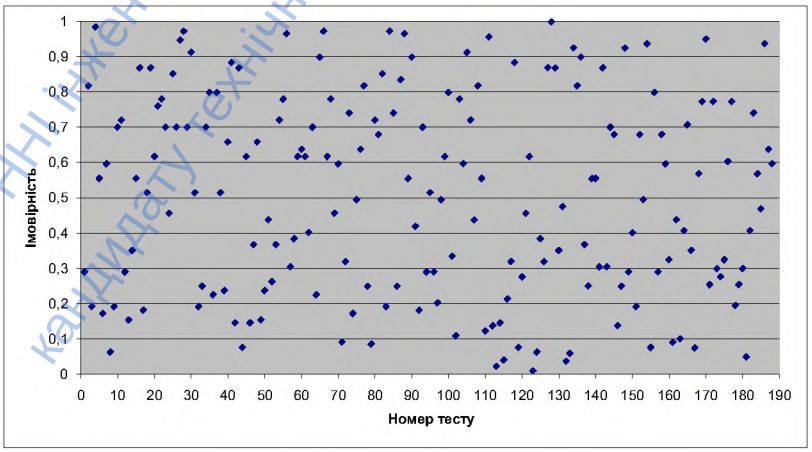

Рис. 5.4. Статистичний портрет програмної реалізації матричного датчика (на основі RANDOM)

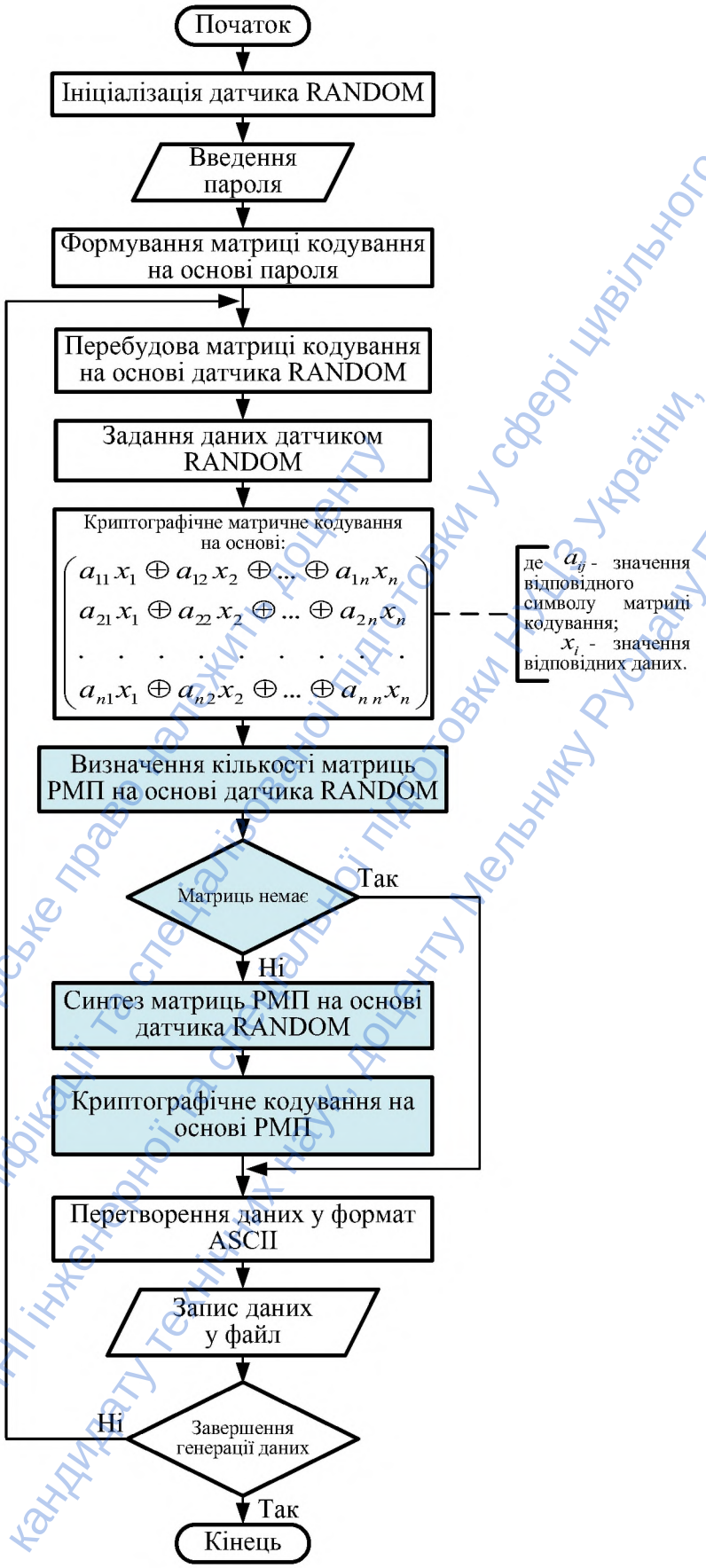

Рис. 5.5. Алгоритм формування послідовності, який поєднує матричне та розширене матричне криптографічне перетворення

Для перевірки якості роботи запропонованого алгоритму перетворимо невипадково монотонно зростаючу послідовність з циклом повторення 64 байти на основі операцій РМП. Чи будуть виявлені дані монотонності після перетворення тестування тестів NIST-STS? Результати тестування псевдовипадкової монотонно зростаючої послідовності з циклом повторення 64 байти, отриманої при реалізації методу захисту інформації на основі розширених матричних операцій криптографічного перетворення, представлені в додатку М, зведені результати тестування – в табл. 5.3.

Даний алгоритм може бути застосований для перетворення будь-яких даних. Наприклад, для перетворення текстової документації бібліотек (художня література).

Таблиця 5.3

Результати тестування

Генератор	**Кількість тестів, у яких тестування пройшли більше 99 % послідовностей**	**Кількість тестів, у яких тестування пройшли більше 96 % послідовностей**
Криптографічне перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти на основі операцій РМП	132 (70 %)	189 (100 %)

Результати тестування показали, що метод захисту інформації на основі розширених матричних операцій криптографічного перетворення пройшов комплексний контроль за методикою NIST-STS.

Перевіримо статистичні властивості результатів розширеного матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів, а саме художньої літератури в текстовому форматі.

Статичний портрет програмної реалізації алгоритму модифікованого розширеного матричного криптографічного перетворення тестового файлу зображено на рис. 5.6.

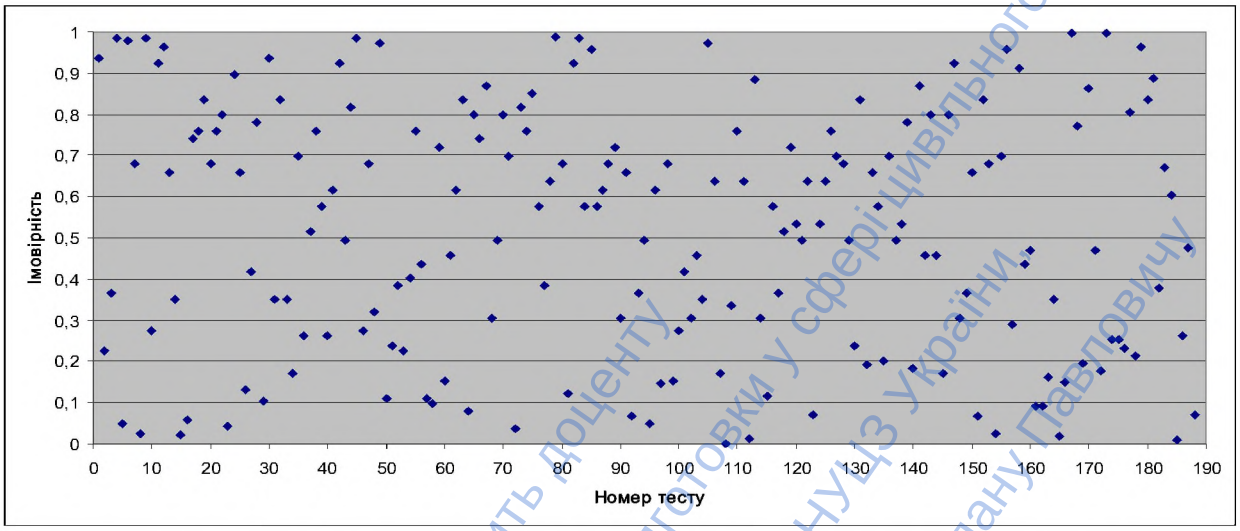

Рис. 5.6. Статистичний портрет програмної реалізації методу захисту інформації на основі розширених матричних операцій криптографічного перетворення

Результати тестування розширеного матричного криптографічного перетворення (даних) за модифікованим алгоритмом розширеного матричного перетворення текстового файлу програмним пакетом NIST-STS представлені в додатку Н, зведені – в табл. 5.4.

Таблиця 5.4

Результати тестування

Генератор	**Кількість тестів, у яких тестування пройшли більше 99 % послідовностей**	**Кількість тестів, у яких тестування пройшли більше 96 % послідовностей**
Криптографічне перетворення текстового файлу на основі операцій РМП	127 (68 %)	189 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS.

5.2.2 Оцінка криптостійкості та швидкості реалізації криптографічного захисту інформації на основі розширеного матричного перетворення

Всі проведені дослідження показали ефективність використання методу розширеного матричного криптографічного перетворення, який забезпечує підвищення криптостійкості закодованої інформації в 2016^{Kc} разів, де Kc – кількість циклів криптографічного перетворення. Ця криптостійкість розраховувалася теоретично, при цьому не враховувалася її залежність від довжини пароля.

Реалізація операцій розширеного матричного криптографічного перетворення відповідає вимогам програмного пакета статистичного тестування NIST STS.

Практичне використання операцій розширеного матричного криптографічного перетворення, виходячи з проведених досліджень, проводиться на основі гамуючої послідовності.

Застосуємо метод підвищення швидкості шифрування, сутність якого полягає у використанні гамуючої послідовності як послідовного набору команд виконання випадково вибраної підмножини операцій криптоперетворення. Необхідно відзначити, що криптостійкість (z) використання цього методу визначається як $z = z_г \cdot z_о$, де $z_г$ – криптостійкість гамуючої послідовності, $z_о$ – криптостійкість послідовностей операцій криптоперетворення.

Криптостійкість і швидкість шифрування визначаються параметрами: n_k – розрядність команди виконання послідовностей операцій криптоперетворення, $K_{оп}$ – кількість операцій у послідовності, яка реалізує команду.

Підмножина випадково вибраних операцій для реалізації методу визначається як $П_о = 2^{n_k} \cdot K_{оп}$. Практична криптостійкість залежить від розрядності пароля $R_П = (2^{n_k} \cdot K_{оп}) \log_2 2016$ і буде пропорційною величині $z_о = 2^{R_П}$.

Наприклад, якщо $n_k = 4$, а $K_{оп} = 4$, тоді $П_о = 64$, $R_П = 64 \cdot \log_2 2016 = 704$ і $z_о = 2^{704}$, що є прийнятним значенням, тому що загальна криптостійкість збільшиться в 2^{704} разів пропорційно.

Оскільки операції криптоперетворення можуть виконуватися паралельно, то час криптоперетворення буде визначатися лише часом формування n_k розрядів гамуючої послідовності. Тоді збільшення швидкості криптографічного перетворення інформації буде визначатися відношенням розрядності інформації, яка шифрується на основі операцій розширеного матричного перетворення під управлінням гамуючої послідовності, до кількості розрядів, над якими виконано гамування. Для нашого прикладу коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{3 \cdot K_{оп}}{n_k} = 3$.

Наприклад, якщо $n_k = 4$, а $K_{оп} = 2$, тоді $П_о = 32$, $R_П = 32 \cdot \log_2 2016 = 352$ і $z_о = 2^{352}$, що є прийнятним значенням, так як загальна криптостійкість збільшиться в 2^{352} разів пропорційно.

Для даного прикладу коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{3 \cdot K_{оп}}{n_k} = 1{,}5$.

Наприклад, якщо $n_k = 3$, а $K_{оп} = 6$, тоді $П_о = 48$, $R_П = 48 \cdot \log_2 2016 = 528$ і $z_о = 2^{528}$, що є прийнятним значенням, так як загальна криптостійкість збільшиться в 2^{528} разів пропорційно.

Для даного прикладу коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{3 \cdot K_{on}}{n_k} = 6$.

Як видно з прикладів розширене матричне перетворення залежно від параметрів n_k і K_{on} дає змогу збільшити криптостійкість від 10^{32} до 10^{150} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування в 1,5 до 6 разів.

Висновки з розділу 5

1. Запропонована структура системи захисту інформації на основі розширених матричних операцій криптографічного перетворення за модулем два та розроблені функціональні моделі пристроїв для їх апаратної реалізації.

2. На основі виконаної програмної реалізації методу захисту інформації проведено тестування згенерованих псевдовипадкових послідовностей програмним пакетом тестів NIST STS. Аналіз результатів тестування дозволив зробити висновок, що запропонований метод розширеного матричного криптографічного перетворення придатний для використання в системах захисту інформаційних ресурсів ДСНС України.

3. Розширене матричне перетворення в залежності від параметрів n_k і K_{on} дозволяє збільшити криптостійкість від 10^{32} до 10^{150} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування від 1,5 до 6 разів.

4. Результати розділу опубліковані в [5, 6].

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну задачу підвищення якості систем захисту інформації на основі використання нових операцій криптографічного перетворення для інформаційних систем ДСНС України:

1. В результаті аналізу існуючих методів і засобів захисту інформації та результатів обчислювального експерименту визначено групу логічних операцій, які забезпечать розширення множини операцій криптографічного перетворення для підвищення якості криптоалгоритмів. Підвищення криптостійкості систем захисту інформації базується на тому, що операції розширеного матричного перетворення не утворюють однієї групи з іншими операціями.

2. Розроблено метод синтезу елементарних функцій розширеного матричного перетворення шляхом введення логічних умов обмеження, які забезпечують нелінійність перетворення, що дало можливість отримати повну множину операцій розширеного матричного перетворення.

3. Розроблено методи синтезу операцій прямого та оберненого розширеного матричного криптографічного перетворення інформації на основі матричного перетворення шляхом побудови та перебудови функцій обмеження, що дало змогу синтезувати ці операції на основі поєднання елементарних функцій. Запропоновано використання синтезованих операцій в алгоритмах криптоперетворення, що дало можливість будувати алгоритми шифрування на основі використання більшої кількості операцій перетворення, а також будувати системи криптографічного захисту інформації з новими якісними характеристиками.

4. Набули подальшого розвитку методи підвищення якості систем криптографічного захисту інформації на основі використання операцій розширеного матричного перетворення. Оцінка якісних показників показала, що використання отриманих операцій забезпечує підвищення криптостійкості

та швидкості реалізації алгоритмів криптографічного захисту інформації залежно від задач проектування.

5. Практична цінність роботи полягає в доведенні отриманих наукових результатів до конкретних інженерних методик, алгоритмів, моделей і варіантів програмної та апаратної реалізації запропонованих операцій розширеного матричного криптографічного перетворення для систем захисту інформації.

Розширене матричне перетворення залежно від параметрів n_k і $K_{оп}$ дає змогу збільшити криптостійкість від 10^{32} до 10^{150} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування від 1,5 до 6 разів.

Реалізація операцій розширеного матричного криптографічного перетворення відповідає вимогам програмного пакета статистичного тестування NIST STS.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мельник Р. П. Застосування операцій розширеного матричного криптографічного перетворення для захисту інформації // Системи обробки інформації – Х.: ХУПС ім. І. Кожедуба, 2012. – № 9 (107). – С. 163–168.

2. Бабенко В. Г. Дослідження способів запису трьохрозрядних криптографічних операцій / В. Г. Бабенко, С. В. Рудницький, Р. П. Мельник // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2012. – № 1 (21). – Т. 2. – С. 170–173.

3. Голуб С. В. Вдосконалення методу синтезу операцій криптографічного перетворення на основі дискретно-алгебраїчного представлення операцій / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький, Р. П. Мельник // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2012. – № 2 (22). – С. 163–168.

4. Бабенко В. Г. Визначення множини трирозрядних елементарних операцій криптографічного перетворення / В. Г. Бабенко, С. В. Рудницький, Р. П. Мельник // Теоретичний і науково-практичний журнал інженерної академії України «Вісник інженерної академії України». – К.: «Інтерсервіс», 2012. – № 3-4. – С. 77–79.

5. Рудницкий С. В. Криптографическое преобразование информации на основе трехразрядных логических функций / С. В. Рудницкий, Р. П. Мельник, В. В. Веретельник // Вектор науки Тольяттинского государственного университета. – 2012. – № 4. – С. 119–122.

6. Рудницкий В. Н. Синтез и анализ математических моделей сумматоров / В. Н. Рудницкий, О. Г. Мельник, С. Ю. Куницкая, Р. П. Мельник // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2011. – № 3 (19). – С. 97–99.

7. Бабенко В. Г. Синтез операций криптографического декодирования на основе элементарных операций расширенного матричного представления / В. Г. Бабенко, Р. П. Мельник, С. В. Рудницкий // Информационные системы и технологии: управление и безопасность: материалы I международной заочной научно-практической конференции. – Тольятти, 2012.

8. Эвристические алгоритмы и распределённые вычисления в прикладных задачах (выпуск 2) : коллективная монография / под ред. Б.Ф. Мельникова. – Ульяновск, 2013. – 201 с.

9. Мельник Р. П. Використання спеціалізованих логічних функцій в системах захисту інформації / Р. П. Мельник // Актуальні проблеми технічних та природничих наук у забезпеченні діяльності служби цивільного захисту: матеріали V міжнародної науково-практичної конференції. – Черкаси : АПБ ім. Героїв Чорнобиля, 2012. – С. 67–68.

10. Рудницкий В. Н. Улучшение информирования подразделений пожарной охраны о чрезвычайных ситуациях / В. Н. Рудницкий, Р. П. Мельник, О. Г. Мельник // Системы безопасности – 2011 : материалы двадцатой научно-технической конференции. – Москва : Академия ГПС МЧС России, 2011. – С. 99–100.

11. Мельник Р. П. Процес інформування підрозділів пожежної охорони та способи його вдосконалення / Р. П. Мельник, О. Г. Мельник // Теорія та практика ліквідації надзвичайних ситуацій: матеріали міжнародної науково-практичної конференції. – Черкаси: видавець Ю. Чабаненко, 2011. – С. 140–142.

12. Рудницкий В. Н. Защита оперативной информации в информационно-аналитической системе МЧС / В. Н. Рудницкий, Р. П. Мельник, О. Г. Мельник // Материалы XXIV международной научно-практической конференции по проблемам пожарной безопасности, посвященной 75-летию создания института. – Россия: г. Балашиха, 2012. – С. 83–85.

13. Рудницкий В. Н. Повышение быстродействия систем защиты информации / В. Н. Рудницкий, Р. П. Мельник, О. Г. Мельник // Чрезвычайные ситуации: теория, практика, инновации «ЧС – 2012» : сборник материалов международной научно-практической конференции. – Гомель : ГГТУ им. П.О. Сухого, 2012. – С. 224.

14. Мельник Р. П. Альтернативні способи запису спеціалізованих логічних функцій / Р. П. Мельник // Пожежна безпека: теорія і практика: матеріали II міжнародної науково-практичної конференції. – Черкаси : АПБ ім. Героїв Чорнобиля, 2012. – С. 346–349.

15. Гатчин Ю. А. Основы информационной безопасности: учебное пособие // Ю. А. Гатчин, Е. В. Климова. – СПб : СПбГУ ИТМО, 2009. – 84 с.

16. Закон України «Про інформацію» : затверджений і введений в дію Постановою Верховної Ради України № 2657-XII від 02.10.1992 р.

17. Грицюк. Ю. І. Практичні проблеми організації системи захисту інформації у структурних підрозділах Міністерства надзвичайних ситуацій України / Ю. І. Грицюк, І. О. Малець // Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту : матеріали міжнародної наукової конференції. – Євпаторія-Херсон : ХНТУ, 2010. – Т. 2. – С. 265–272.

18. Малець І. О. Впровадження інформаційних технологій в управлінську діяльність підрозділів Міністерства надзвичайних ситуацій / І. О. Малець, Ю. І. Грицюк // Науковий вісник НЛТУ України: збірник науково-технічних праць. – Львів: РВВ НЛТУ України, 2011. – Вип. 21.14. – С. 326–331.

19. Закон України «Про основи національної безпеки України» : затверджений і введений в дію Постановою Верховної Ради України № 964-IV від 19.06.2003 р.

20. Грицюк Ю. І. Проблеми захисту інформації у структурних підрозділах МНС України / Ю. І. Грицюк, Т. Є. Рак // Науковий вісник НЛТУ України: збірник науково-технічних праць. – Львів: РВВ НЛТУ України, 2011. – Вип. 21.12. – С. 330–346.

21. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях : навчальний посібник / [Задірака В. К., Кудін А. М., Людвиченко В. О., Олексюк О. С.] – Київ-Тернопіль: Вид-во «Підручники і посібники», 2007. – 272 с.

22. Богуш В. М. Інформаційна безпека : термінологічний навчальний довідник / В. М. Богуш, В. Г. Кривуца, А. М. Кудін / за ред. В. Г. Кривуци. – К. : ООО «Д.В.К.», 2004. – 508 с.

23. Технические средства и методы защиты информации : учебник для вузов / [Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. и др.]; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : ООО «Издательство Машиностроение», 2009 – 508 с.

24. Сучасні телекомунікаційні мережі у цивільному захисті : підручник / [Щербак Г. В., Мельнікова Л. І., Рубан І. В., Садовий К. В., Сумцов А. В.]
– Харків, 2007. – 255 с.

25. Гнатюк С. О. Особливості криптографічного захисту державних інформаційних ресурсів / С. О. Гнатюк, В. М. Кінзерявий, А. О. Охріменко // Науково-практичний журнал «Безпека інформації». – 2012.– № 1. – С. 68–80.

26. Сучасні системи захисту державних інформаційних ресурсів / Є. Д. Скулиш, О. Г. Корченко, Ю. І. Горбенко [та ін.] // Захист інформації. – 2011. – № 4. – С. 5–17.

27. Малець І. О. Роль та проблеми функціонування телекомунікаційних систем при надзвичайних ситуаціях / І. О. Малець // Електронний науковий архів Науково-технічної бібліотеки Національного університету «Львівська політехніка». – 2011. – Режим доступу до статті : http://ena.lp.edu.ua.

28. Закон України «Про захист інформації в автоматизованих системах» : затверджений і введений в дію Постановою Верховної Ради України № 81/94-ВР від 05.07.1994 р.

29. Указ Президента України «Про заходи щодо захисту інформаційних ресурсів держави» № 582/2000 від 10.04.2000 р.

30. Указ Президента України «Про Положення про технічний захист інформації в Україні» № 1229/99 від 27.09.1999 р.

31. Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» № 505/98 від 22.05.1998 р.

32. Венбо Мао. Современная криптография : теория и практика / Пер. с англ. – М. : Издательский дом «Вильямс», 2005. –768 с.

33. Криптографическая защита информации / [Яковлев А. В., Безбогов А. А., Родин В. В., Шамкин В. Н.] – Тамбов : изд-во ТГТУ, 2006. – 140 с.

34. Соколов В. Ю. Інформаційні системи і технології: навчальний посібник / В. Ю. Соколов. – К. : Вид-во ДУІКТ, 2010. – 138 с.

35. Наказ Державного комітету України з питань регуляторної політики та підприємництва, Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Ліцензійні умови провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації» № 8/216 від 26.01.2008 р.

36. Наказ Адміністрації Держспецзв'язку, Держспоживстандарту України «Про затвердження Правил проведення робіт із сертифікації засобів захисту інформації» № 75/91 від 25.04.2007 р.

37. Оков И. Н. Криптографические системы защиты информации / И. Н. Оков. – СПб. : ВУС, 2001. – 236 с.

38. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин; под ред. В. Ф. Шаньгина. – М. : Радио и связь, 2001. – 376 с.

39. Теория электрической связи : учебное пособие / [Васильев К. К., Глушков В. А., Дормидонтов А. В., Нестеренко А. Г.]; под общ. ред. К. К. Васильева. – Ульяновск : УлГТУ, 2008. – 452 с.

40. Основы криптографии : учебное пособие для вузов / [Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.]. – М. : Гелиос АРИ, 2001. – 480 с.

41. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М. : Горячая линия-Телеком, 2000. – 452 с.

42. Нечаев В. И. Элементы криптографии. Основы теории защиты информации / В. И. Нечаев. – М. : Высшая школа, 1999. – 109 с.

43. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А. Ю. Щербаков. – М. : Книжный мир, 2009. – 352 с.

44. Галатенко В. А. Стандарты информационной безопасности / В. А. Галатенко. – М. : Интернет-университет информационных технологий, 2006. – 264 с.

45. Средства защиты в сетях / [Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В]. – М. : Горячая Линия-Телеком, 2008. – (Информационная безопасность открытых систем: в 2 томах). – Том 2. – 560 с.

46. Вельшенбах Михаэл. Криптография на Си и С++ в действии / Михаэл Вельшенбах; под ред. П. В. Семьянова. – М. : Триумф, 2004. – 464 с.

47. Бабаш А. В. Криптография. Аспекты защиты / А. В. Бабаш, Г. П. Шанкин. – М. : Солон-Р, 2002. – 512 с.

48. Малюк А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. – М. : Горячая линия-Телеком, 2001. – 148 с.

49. Чернавский Д. С. Синергетика и информация (динамическая теория информации) / Д.С. Чернавский. – М. : Едиториал УРСС, 2004. – 288 с.

50. Угрозы, уязвимости, атаки и подходы к защите / [Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В]. – М. : Горячая Линия-Телеком, 2006. – (Информационная безопасность открытых систем: в 2 томах). – Том 1. – 536 с.

51. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. – М. : ИД «ФОРУМ» : ИНФРА-М, 2008. – 416 с.

52. ISO 15408-99 «Общие критерии оценки безопасности информационных технологий» (I ч.).

53. ISO 15408-99 «Общие критерии оценки безопасности информационных технологий» (II ч.).

54. ISO 15408-99 «Общие критерии оценки безопасности информационных технологий» (III ч.).

55. Указ Президента України «Про Доктрину інформаційної безпеки України» № 514/2009 від 08.07.2009 р.

56. Закон України «Про державну таємницю» : затверджений і введений в дію Постановою Верховної Ради України № 3855-XII від 21.01.1994 р.

57. Закон України «Про захист персональних даних» : затверджений і введений в дію Постановою Верховної Ради України № 2297-VI від 01.06.2010 р.

58. Закон України «Про доступ до публічної інформації» : затверджений і введений в дію Постановою Верховної Ради України № 2939-VI від 13.01.2011 р.

59. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про затвердження Положення про контроль за функціонуванням системи технічного захисту інформації» № 61 від 22.12.1999 р.

60. Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» № 1126 від 08.10.1997 р.

61. Постанова Кабінету Міністрів України «Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу» № 1755 від 29.10.2000 р.

62. Постанова Кабінету Міністрів України «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення» № 616 від 25.05.2011 р.

63. Горбенко І. Д. Захист інформації в інформаційно-телекомунікаційних системах / І. Д. Горбенко, Т. О. Гріненко. – Х., 2004. – 222 с.

64. Горбенко І. Д. Методи перехоплення інформації у системах квантової криптографії / І. Д. Горбенко, Є. В. Іванченко, С. В. Карпенко, С. О. Гнатюк // Науково-технічний журнал «Захист інформації». – 2011. – № 2. – С. 5–13.

65. Корченко А. Г. Построение систем защиты информации на нечетких множествах / А. Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.

66. Корченко О. Г. Квантові технології конфіденційного зв'язку / О. Г. Корченко, С. О. Гнатюк, В. М. Кінзерявий // Защита информации : сб. науч. трудов. – К. : НАУ, 2010. – Вип. 1. – С. 179–184.

67. Лужецький В. А. Альтернативні режими блокового шифрування / В. А. Лужецький, О. В. Дмитришин // Наукові праці Вінницького національного технічного університету. – 2011. – № 1. – 9 с.

68. Семенова О. О. Штучні нейрони з імпульсним представленням інформації / О. О. Семенова, А. О. Семенов, А. А. Галка, Я. М. Хонькович // Вісник Хмельницького національного університету. – 2012. – № 3. – С. 98–101.

69. Конахович Г. Ф. Оцінка ефективності систем захисту інформації в телекомунікаційних системах / Г. Ф. Конахович, О. Г. Голубничий,

О. Ю. Пузиренко // Проблеми інформатизації та управління : зб. наук. праць. – 2007. – Вип. 3 (21). – С. 75–83.

70. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К. : «МК-Прес», 2005. – 432 с.

71. Богуш В. М. Криптографічні застосування елементарної теорії чисел : навч. посібник // В. М. Богуш, В. А. Мухачов. – Державний університет інформаційно-комунікаційних технологій. – К. : ДУІКТ, 2006. – 126 с.

72. Рудницький В. М. Модель уніфікованого пристрою криптографічного перетворення інформації / В. М. Рудницький, В. Г. Бабенко // Системи управління, навігації та зв'язку : зб. наук. пр. – 2009. – Вип. 1 (9). – С. 173–177.

73. Баранник В. В. Методология создания криптографических преобразований на базе методов, исключающих избыточность / В. В. Баранник, С. А. Сидченко, В. В. Ларин // Сучасна спеціальна техніка. – К., 2009 – Вип. 4 (19). – С. 24–30.

74. Василиу Е. В. Проблемы развития и перспективы использования квантово-криптографических систем / Е. В. Василиу, П. П. Воробиенко // Наукові праці ОНАЗ ім. О. С. Попова. – 2006. – № 1. – С. 3–17.

75. Брассар Ж. Современная криптология: пер. с англ. – М. : издательско-полиграфическая фирма «Полимед», 1999. – 176 с.

76. Румянцев К. Е. Квантовая связь и криптографія : учебное пособие / К. Е. Румянцев, Д. М. Голубчиков. – Таганрог : изд-во ТТИ ЮФУ, 2009. – 122 с.

77. Gisin N. Quantum Cryptography / N. Gisin, G. Ribordy, W. Tittel, N. Zbinden // Rev. Mod. Phys. – 2002. – Т. 74. – С. 145–191.

78. Bennett C. H. Experimental Quantum Cryptography / C. H. Bennett, F. Bessette, G. Brassard // Journal of Cryptography. – 1992. – V. 5, № 1. – С. 3–28.

79. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / С.П. Кулик, Е.А. Шапиро (пер. с англ.); С.П. Кулик, Т.А. Шмаонов (ред. пер.); Д. Боумейстер и др. (ред.). – М.: Постмаркет, 2002. – С. 33–73.

80. Килин С. Я. Квантовая криптография: идеи и практика : монография / С. Я. Килин, Д. Б. Хорошко, А. П. Низовцев. – Минск, 2008. – 398 с.

81. Kaszlikowski D. Quantum cryptography based on qutrit Bell inequalities / D. Kaszlikowski, K. Chang, D.K.L. Oi, L.C. Kwek, C.H. Oh // Physical Review A. – 2003. – V. 67, № 1.

82. Шнайер, Б. Секреты и ложь: безопасность данных в цифровом мире / Б. Шнайер. – СПб. : Питер, 2003. – 368 с.

83. Diffie W. New directions in cryptography / W. Diffie, M. E. Hellman // IEEE Transactions on Information Theory. – 1976. – № 22. – Pp. 644–654.

84. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

85. Diffie W. Authentication and authenticated key exchanges / W. Diffie, P.C. van Oorschot, Wiener M. J. // Designs, Codes and cryptography. – 1992. – № 2. – Pp. 107–125.

86. Рудницький В. М. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів / В. М. Рудницький, І. В. Миронець, В. Г. Бабенко // Системи обробки інформації : зб. наук. пр. – Х. : Харк. ун-т Повітряних Сил ім. Івана Кожедуба, 2010. – Вип. 5 (86). – С. 15–19.

87. Рябко Б. Я. Основы современной криптографии для специалистов в информационных технологиях / Б. Я. Рябко, А. Н. Фионов. – М. : Научный мир, 2004. – 172 с.

88. Бетелин В. Б. Информационная (компьютерная) безопасность с точки зрения технологии программирования [Електронний ресурс] / В. Б. Бетелин, В. Б. Галатенко // Влияние информационных

технологий на национальную безопасность : материалы IV ежегодной конференции. – Москва, 2001. – Режим доступа к статье : http://images.geo.web.ru/pubd/2001/10/23/0001161428/word5.pdf.

89. Безбогов А. А. Методы и средства защиты компьютерной информации : учебное пособие / А. А. Безбогов, А. Я. Яковлев, В. Н. Шамкин.
– Тамбов: изд-во Тамб. гос. техн. ун-та, 2006. – 196 с.

90. Безбогов А. А. Криптографическая защита информации : учебное пособие / А. А. Безбогов, А. Я. Яковлев, В. Н. Шамкин. – Тамбов: изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.

91. Прикладная теория цифровых автоматов / [Самофалов К. Г., Романкевич А. М., Валуйский В. Н., Каневский Ю. С., Пиневич М. М.]. – К. : Вища шк., 1987. – 375 с.

92. Гантемахер Ф. Р. Теория матриц / Ф. Р. Гантемахер. – 4-е изд., доп. – М. : Наука, 1988. – 548 с.

93. Ланкастер П. Теория матриц / П. Ланкастер [пер. с англ. С. Д. Демушкина]. – М.: Наука, 1978. – 280 с.

94. Глушков В. М. Синтез цифровых автоматов / В. М. Глушков. – М. : Физматгиз, 1962. – 476 с.

95. Тарannиков Ю. В. О корреляционно-имунных и устойчивых булевых функциях / Ю. В. Тарannиков // Математические вопросы кибернетики; под. ред. О. Б. Лупанова. – Вып. 11. – М. : Физматлит, 2002. – С. 91–148.

96. Логачев О. А. Булевы функции в теории кодирования и криптологии / О. А. Логачев, В. В. Ященко, А. А. Сальников. – М. : МЦМНО, 2004. – 469 с.

97. Ткаченко А. С. Теория синтеза структурных кодов и отказоустойчивых систем на их основе / А. С. Ткаченко. – М. : МО России, 1993. – 71 с.

98. Баричев С. Г. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. – М. : Горячая линия – Телеком, 2002. – 175 с.

99. Варфоломеев А. А. Блочные криптосистемы. Основные свойства и методы анализа стойкости / А. А. Варфоломеев, А. Е. Жуков, А. Б. Мельников, Д. Д. Устюжанин. – М. : МИФИ, 1998. – 200 с.

100. Столлингс В. Криптография и защита сетей: принципы и практика / Вильям Столлингс. – [2-е изд.]. – М.: Вильямс, 2001. – 672 с.

101. Герасименко В. А. Защита информации в автоматизированных системах обработки данных / В. А. Герасименко. – [в 2-х кн.]. – М. : Энергоатомиздат, 1994. – 400 с.

102. Карасик И. Программные и аппаратные средства защиты информации для персональных компьютеров / И. Карасик // Компьютер-Пресс. – 1992. – № 3. – С. 37–46.

103. Спесивцев А.В. Защита информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер А.Ю.Крутяков и др. – М.: Радио и связь, 1992. – 192 с.

104. Хофман Л.Дж. Современные методы защиты информации / Л.Дж. Хофман. – М.: Сов.радио, 1980. – 264 с.

105. Yves le Roux. Technical Criteria For Security Evaluation Of Information Technology Products/ Yves le Roux // Information Security Guide. – 1990/1991.
– p.p. 59–62.

106. Конхейм А. Основы криптографии / А. Конхейм. – М.: Радио и связь, 1987. – 412 с.

107. Торокин А.А. Основы инженерно-технической защиты информации / А.А. Торокин. – М.: Ось-89, 1998. – 336 с.

108. Основы криптографии: учеб. пособие для вузов / [Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.]. – М.: Гелиос АРИ, 2001. – 480 с.

109. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. – М.: Горячая линия-Телеком, 2001. – 148 с.

110. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособие для вузов / [П.Ю. Белкин, О.О.Михальский, А.С.Першаков и др.]. – М.: Радио и связь, 2000. – 168 с.

111. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия-Телеком, 2000. – 452 с.

112. Рудницький В.М. Визначення множини логічних функцій для синтезу цифрових пристроїв систем захисту інформації / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко // Системи управління, навігації та зв'язку: Зб. наук. пр. – Київ. - 2008. – Вип. 4(8). – С. 155-157.

113. Бабенко В.Г. Технологія визначення спеціальних логічних функцій для систем захисту інформації / В.Г. Бабенко, В.М. Рудницький, Т.В. Дахно // Вісник інженерної академії України. – 2007. – Вип. 3-4. – С.64-67.

114. Бабенко В.Г. Алгоритми синтезу логічних функцій для систем захисту інформації / В.Г. Бабенко, Т.В. Дахно, В.М. Рудницький // Науково-практична конференція молодих учених та аспірантів «Інтегровані інформаційні технології та системи (ІІТС-2007)». - Київ: НАУ, 2007. – С. 46-48.

115. Рудницький В.М. Систематизація повної множини логічних функцій для криптографічного перетворення інформації / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Зб. наук. пр. «Системи обробки інформації». – Харків: ХУПС ім. І. Кожедуба. – 2011. – Випуск 8(98). – С. 184-188.

116. Рудницький В.М. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів / В.М. Рудницький, І.В. Миронець, В.Г. Бабенко // Збірник наукових праць Харківського університету Повітряних Сил – Харків: ХУПС ім. І.

Кожедуба.
– 2011. – Випуск 3(29). – С. 145-150.

117. Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного перекодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Науково-практичний журнал «Захист інформації» – К.: НАУ. – 2012. – № 3(56). – С. 50-56.

118. Рудницький В.М. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації / В.М. Рудницький, В.Г. Бабенко, С.В. Рудницький // Збірник наукових праць Харківського університету Повітряних Сил – Харків: ХУПС ім. І. Кожедуба. – 2012. – Вип. 4 (33). – С. 198–200.

119. Голуб С.В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два / С.В. Голуб, В.Г. Бабенко, С.В. Рудницький // Зб. наук. пр. «Системи обробки інформації». – Харків: ХУПС ім. І. Кожедуба. – 2012. – Випуск 3(101). – Том 1. – С. 119-122.

120. Бабенко В.Г. Синтез функцій перекодування для групи трьохрозрядних криптографічних операцій / В.Г. Бабенко, С.В. Рудницький // Наук. журн. «Системи озброєння і військова техніка». – Харків: ХУПС ім. І. Кожедуба. – 2012. – Випуск 1(29). – С. 84-87.

121. Пат. 27818 Україна, МПК H03M 13/00. Пристрій для виконання логічних операцій одної змінної в двійково-четвірковій системі числення / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко – № u 2007 08646; Заявл. 27.07.2007; Опубл. 12.11.07, Бюл. № 18.

122. Рудницький В.М. Моделювання логічного пристрою для систем захисту інформації / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко // Проблеми і перспективи розвитку банківської системи України: зб. наук. пр. – Суми: Укр. академія банківської справи НБУ, 2006. – Т. 18. – С. 185–190.

123. Пат. 27818 Україна, МПК H03M 13/00. Пристрій для виконання логічних операцій одної змінної в двійково-четвірковій системі числення /

В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко – № u 2007 08646; Заявл. 27.07.2007; Опубл. 12.11.07, Бюл. № 18. – С. 4.

124. Рудницький В.М. Синтез математичних моделей пристроїв декодування інформації для криптографічних систем / В.М. Рудницький, В.Г. Бабенко // Системи обробки інформації: зб. наук. пр. – Х.: Харк. ун-т Повітряних Сил ім. Івана Кожедуба, 2009. – Вип. 2(76). – С. 124–128.

125. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика - Электроинформ, 1997. – 368 с.

126. Грушо А.А. Теоретические основы защиты информации / А.А. Грушо, Е.Е. Тимонина. – М.: Издательство Агентства "Яхтсмен", 1996. – 192 с.

127. Мафтик С. Механизмы защиты в сетях ЭВМ / С. Мафтик. – М.: Мир, 1993. – 216 с.

128. Молдовян А.А. Криптография: учебник для вузов / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов. – СПб.: Лань, 2000. – 224 с.

129. Молдовян Н.А. Скоростные блочные шифры / Н.А. Молдовян. – СПб.: СПбГУ, 1998. – 230 с.

130. Нечаев В.И. Элементы криптографии. Основы теории защиты информации / В.И. Нечаев. – М.: Высшая школа, 1999. – 109 с.

131. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. – СПб.: БХВ, 2000. – 384 с.

132. Аскеров Т.М. Защита информации и информационная безопасность: учебное пособие / Аскеров Т.М. – Под общей ред. Курбакова К.И. – М.: Рос. экон. академия, 2001. – 387 с.

133. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 352 с.

134. Петренко С.А. Политики информационной безопасности / С.А. Петренко, В.А. Курбатов. – М.: Компания АйТи, 2006. – 400 с.

135. Галатенко В.А. Стандарты информационной безопасности / В.А. Галатенко. – М.: Интернет-университет информационных технологий, 2006. – 264 с.

136. Петренко С.А. Управление информационными рисками / С.А. Петренко. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

137. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК Пресс, 2008. – 544 с.

138. Лепехин А.Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. – А.Н. Лепехин. – М.: Тесей, 2008. – 176 с.

139. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты / Ю. Родичев. – СПб.: Питер, 2008. – 272 с.

140. Скотт Бармен. Разработка правил информационной безопасности / Бармен Скотт. – М.: Вильямс, 2002. – 208 с.

141. Угрозы, уязвимости, атаки и подходы к защите / [Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В]. – М.: Горячая Линия-Телеком, 2006. – (Информационная безопасность открытых систем: в 2 томах). – Том 1. – 536 с.

142. Средства защиты в сетях [Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В]. – М.: Горячая Линия-Телеком, 2008. – (Информационная безопасность открытых систем: в 2 томах). – Том 2. – 560 с.

143. Стратонович Р.Л. Теория информации / Р.Л. Стратонович. – М.: Сов. радио, 1975. – 424 с.

144. Урсул А.Д. Природа информации / А.Д. Урсул. – М.: Политиздат, 1968. – 288 с.

145. Урсул А.Д. Проблема информации в современной науке / А.Д. Урсул. – М.: Наука, 1975. – 288 с.

146. Чернавский Д.С. Синергетика и информация (динамическая теория информации) / Д.С. Чернавский. – М.: Едиториал УРСС, 2004. – 288 с.

147. Вельшенбах Михаэл. Криптография на Си и С++ в действии / Михаэл Вельшенбах. – Под редакцией П.В. Семьянова. – М.: Триумф, 2004. – 464 с.

148. Бабаш А.В. Криптография. Аспекты защиты / А.В. Бабаш, Г.П. Шанкин. – М.: Солон-Р, 2002. – 512 с.

149. Чмора А.П. Современная прикладная криптография / А.П. Чмора. – [2-е изд., стер.]. – М.: Гелиос АРВ, 2002. – 256 с.

150. Саломаа А. Криптография с открытым ключом / Арто Саломаа; [пер. с англ. И.А. Вихлянцева; под ред. А.Е. Андреева и А.А. Болотова]. – М.: Мир, 1995. – 318 с.

151. Коблиц Нил. Курс теории чисел и криптографии / Нил Коблиц. – М.: ТВП, 2001. – 254 с.

152. Введение в криптографию / [Ященко В.В.,Варновский Н.П.,Нестеренко Ю.В. и др.]; под общ. ред. В. В. Ященко. – [3-е изд., испр.]. – СПб.: Питер, 2001. – 288 с.

153. Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. – СПб.: БХВ-Петербург, 2004. – 446 с.

154. Молдовян Н.А. Проблематика и методы криптографии (монография) / Н.А. Молдовян – СПб.: СПбГУ,1998. – 212 с.

155. Хаггарти Р. Дискретная математика для программистов: учеб. пособие для вузов / Р. Хаггарти; пер. с англ.; под ред. С.А. Кулешова; с доп. А.А. Ковалева. – М.: Техносфера, 2003. – 320 с. – (Мир программирования).

156. Новиков Ф.А. Дискретная математика для программистов:учеб. Пособие / Ф.А. Новиков и др. – СПб. :Питер, 2003. – 304 с.

157. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography / Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. – CRC Press, 1997. – 816 p.

158. Кан Дэвид. Взломщики кодов / Дэвид Кан. – М.: Центрполиграф, 2000. – 473 с.

159. Кобринский Н.Е. Введение в теорию конечных автоматов / Н.Е. Кобринский, Б.А. Трахтенброт. – М.: Гос. издательство физ.-мат. Литературы, 1962. – 405 с.

160. Фомичев В.М. Дискретная математика и криптология. Курс лекций / В.М. Фомичев. – М.: Диалог-МИФИ, 2003. - 400 с.

161. Х.К.А. ван Тилборг. Основы Криптологии. Профессиональное руководство и интерактивный учебник / Х.К.А. ван Тилборг. – М.: Мир, 2006. – 471 с.

162. Алгоритмы: построение и анализ / [Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Штайн]. – [2-е изд.]. – М.: Вильямс, 2006. – 1296 с.

163. Колмогоров А.Н. Теория информации и теория алгоритмов / А.Н. Колмогоров. – М.: Наука, 1987. – 304 с.

164. Объектно-ориентированный анализ и проектирование с примерами приложений / [Гради Буч, Роберт А. Максимчук, Майкл У. Энгл, Бобби Дж. Янг, Джим Коналлен, Келли А. Хьюстон]. – [3-е изд.]. – М.: Диалектика-Вильямс, 2009. – 720 с.

165. Липаев В.В. Системное проектирование сложных программных средств для информационных систем / В.В. Липаев. – М.: Синтег, 2002. – 268 с.

166. Дональд Кнут. Искусство программирования. Основные алгоритмы / Дональд Кнут. – Том 1. – [3-е изд.]. – М.: Вильямс, 2006. – 720 с.

167. Марков А.А., Нагорный Н.М. Теория алгорифмов / А.А. Марков, Н.М. Нагорный. – [2-е изд.,испр. и доп.]. – М.: Фазис, 1996. – 448 с.

168. Климова Л.М. Pascal 7.0. Практическое программирование. Решение типовых задач / Л.М. Климова. – М.: Кудиц-образ, 2003. – 496 с.

Додаток А

Акти впровадження результатів дисертаційної роботи

ЗАТВЕРДЖУЮ
Начальник
Територіального управління
МНС України
у Черкаській області
генерал-майор служби
цивільного захисту

В.М. Гвоздь

«17» 12 2012 р.

АКТ

впровадження результатів дисертаційної роботи

Мельника Руслана Павловича в Територіальному управлінні

МНС України у Черкаській області

Для розробки спеціального програмного забезпечення Територіальним Управлінням МНС України у Черкаській області у напрямку підвищення рівня захисту конфіденційної інформації були використані наступні результати, отримані Мельником Русланом Павловичем, а саме:

- технологія перетворення інформації на основі спеціалізованих логічних функцій розширеного матричного перекодування;
- математичні моделі та алгоритми побудови базових операцій криптографічного перетворення інформації на основі спеціалізованих логічних функцій.

Розроблене програмне забезпечення дозволить забезпечити конфіденційність службової інформації на електронних носіях та в інформаційно-телекомунікаційній системі в цілому.

Перший заступник начальника
Територіального управління МНС України
у Черкаській області,
полковник служби
цивільного захисту

С.І. Сташенко

ЗАТВЕРДЖУЮ
Начальник Управління
Держтехногенбезпеки
у Черкаській області
полковник служби
цивільного захисту

О.Г. Капралов

«12» 12 2012 р.

АКТ

впровадження результатів дисертаційної роботи

Мельника Руслана Павловича в Управлінні Держтехногенбезпеки у Черкаській області

Для розробки спеціального програмного забезпечення використана технологія перетворення інформації на основі спеціалізованих логічних функцій розширеного матричного перекодування, отримана Мельником Русланом Павловичем.

Розроблене програмне забезпечення, завдяки математичним моделям та алгоритмам побудови базових операцій криптографічного перетворення інформації на основі спеціалізованих логічних функцій, дозволить забезпечити конфіденційність службової інформації на електронних носіях та в інформаційно-телекомунікаційній системі в цілому.

Заступник начальника
Управління Держтехногенбезпеки
у Черкаській області,
підполковник служби цивільного захисту **О.В. Євпак**

ДЕРЖАВНЕ ПІДПРИЄМСТВО
НАУКОВО-ВИРОБНИЧИЙ КОМПЛЕКС
«ФОТОПРИЛАД»
вул. Б. Вишневецького, 85, м. Черкаси, 18000
тел.:(0472) 36 03 08
факс: (0472) 37-45-31
телетайп: 147123 «Щука»
E-mail: photopribor@ic.ck.ua

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ
НАУЧНО-ПРОИЗВОДСТВЕННЫЙ
КОМПЛЕКС
«ФОТОПРИБОР»
ул. Б. Вишневецкого, 85, г. Черкассы,
Украина,18000
тел.:(0472) 36-03-08
факс: (0472) 37-45-31
телетайп: 147123 «Щука»
E-mail: photopribor@ic.ck.ua

_____ № _____
на № _____ від _____

ЗАТВЕРДЖУЮ
Генеральний директор
НВК "Фотоприлад"
_____ А.О. Бурківський
"10" 12 2012 р.

АКТ
впровадження результатів дисертаційної роботи
Мельника Руслана Павловича
в ЦКБ "Сокіл" НВК "Фотоприлад"

Для забезпечення конфіденційності та достовірності передачі команд в оптичній лінії зв'язку за допомогою виробу 1К118 були використані наступні наукові результати отримані Мельником Русланом Павловичем, а саме:

- технологія криптографічного перетворення інформації на основі спеціалізованих логічних функцій розширеного матричного перекодування;
- математичні моделі та алгоритми побудови базових операцій криптографічного перетворення інформації на основі спеціалізованих логічних функцій.

Дані наукові результати реалізовані на основі спеціалізованого модуля операційної системи.

Начальник відділу ЦКБ "Сокіл"
НВК "Фотоприлад" _____ О.Я. Хомченко

ЗАТВЕРДЖУЮ
Проректор
з навчальної роботи
Черкаського державного
технологічного університету
к.т.н., доц.
О.О. Ситник
«___» __________ 2012 р.

АКТ
впровадження результатів дисертаційної роботи
Мельника Руслана Павловича в навчальний процес
Черкаського державного технологічного університету

Комісія у складі: завідувача кафедри комп'ютерних систем д.т.н., проф. Середенка В.М., доцента кафедри комп'ютерних систем к.т.н., доц. Шадхіна В.Ю., доцента кафедри комп'ютерних систем к.т.н., доц. Єрофеєва Ю.Ф., розглянувши матеріали дисертаційного дослідження Мельника Руслана Павловича, встановила наступне:

1. При підготовці бакалаврів за напрямом 6.050102 «Комп'ютерна інженерія» та магістрів зі спеціальності 8.050102.2 «Системне програмування» в курсі лекцій з дисципліни «Система захисту інформації», а також при підготовці курсу лекцій з дисциплін «Програмні засоби захисту інформації» та «Технічні засоби захисту інформації» використовуються результати дисертаційного дослідження, а саме:

- математичні моделі та алгоритми побудови базових операцій криптографічного перетворення інформації на основі спеціалізованих логічних функцій;
- технологія перетворення інформації на основі спеціалізованих логічних функцій розширеного матричного перекодування.

2. При виконанні курсових і кваліфікаційних робіт використовуються запропоновані методики синтезу операцій криптографічного перетворення.

Завідувач кафедри КС д.т.н., проф. **В.М. Середенко**

Доцент кафедри КС, к.т.н., доц. **В.Ю. Шадхін**

Доцент кафедри КС, к.т.н., доц. **Ю.Ф. Єрофеєв**

ЗАТВЕРДЖУЮ
Ректор
Академії пожежної безпеки
імені Героїв Чорнобиля
МНС України,
к.псих.н., проф.,
генерал-майор с.ц.з.

М.А. Кришталь

«21» 12 2012 р.

АКТ
впровадження результатів дисертаційної роботи
Мельника Руслана Павловича в навчальний процес
Академії пожежної безпеки імені Героїв Чорнобиля МНС України

Комісія у складі: начальника кафедри вищої математики та інформаційних технологій, к.ф.-м.н., доц., полковника с.ц.з. Частоколенка І.П., старшого викладача кафедри, підполковника с.ц.з. Григоренка К.В., викладача кафедри Марченка А.П., розглянувши матеріали дисертаційного дослідження Мельника Руслана Павловича, встановила наступне:

1. При підготовці бакалаврів за напрямом 6.170203 та спеціалістів 7.17020301 «Пожежна безпека»в курсі лекцій з дисциплін «Інформаційне забезпечення діяльності пожежної охорони» та «Інформаційне забезпечення діяльності підрозділів МНС» використовуються результати дисертаційного дослідження, отримані Мельником Русланом Павловичем, зокрема математичні моделі та алгоритми побудови базових операцій криптографічного перетворення інформації на основі спеціалізованих логічних функцій.

2. При проведенні практичних занять з теми № 1 «Сучасні інформаційні технології оброблення даних» (дисципліна «Інформаційне забезпечення діяльності пожежної охорони») та теми № 2 «Система інформаційного забезпечення діяльності підрозділів МНС» (дисципліна «Інформаційне забезпечення діяльності підрозділів МНС») використовується технологія перетворення інформації на основі спеціалізованих логічних функцій розширеного матричного перекодування.

Начальник кафедри вищої математики та інформаційних технологій, к.ф.-м.н., доц., полковник с.ц.з. **І.П. Частоколенко**

Старший викладач кафедри вищої математики та інформаційних технологій, підполковник с.ц.з. **К.В. Григоренко**

Викладач кафедри вищої математики та інформаційних технологій **А.П. Марченко**

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Черкаського національного
університету ім. Б. Хмельницького
канд.ф.-м.н., проф.

Н.А. Тарасенкова

«24» 12 2012 р.

АКТ
впровадження результатів дисертаційної роботи
Мельника Руслана Павловича в навчальний процес
Черкаського національного університету ім. Б. Хмельницького

Основні результати дисертаційної роботи Мельника Р.П. застосовуються при викладанні дисципліни «Комп'ютерна схемотехніка та архітектура комп'ютерів» бакалаврам за напрямом 6.050101 «Комп'ютерні науки».

До лекційного курсу включені такі результати, отримані автором: математичні моделі та алгоритми побудови базових операцій криптографічного перетворення інформації на основі спеціалізованих логічних функцій та технологія перетворення інформації на основі спеціалізованих логічних функцій розширеного матричного перекодування.

Матеріал, отриманий Мельником Р.П. в дисертаційній роботі, дозволяє бакалаврам ознайомитися з методикою синтезу розширених матричних операцій криптографічного перетворення. При виконанні курсових і кваліфікаційних робіт використовуються запропоновані математичні моделі та алгоритми.

Завідувач кафедри інтелектуальних
систем прийняття рішень,
д.т.н., проф. **С.В. Голуб**

Завідувач кафедри інформаційних
систем та медичних технологій,
к.ф.-м.н., доц. **В.С. Авраменко**

Завідувач кафедри програмного
забезпечення автоматизованих систем,
декан факультету обчислювальної техніки,
інтелектуальних та управляючих систем,
к.т.н., доц. **В.І. Салапатов**

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної та навчально-виховної роботи Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ»

В.Є. Зайцев

«26» 12 2012 р.

АКТ
впровадження результатів дисертаційної роботи
Мельника Руслана Павловича
у навчальний процес Національного аерокосмічного університету
ім. М.Є. Жуковського «ХАІ»

Комісія у складі: завідувача кафедри інженерії програмного забезпечення, д.т.н., проф. Туркіна І.Б., професора кафедри інженерії програмного забезпечення, д.т.н., доц. Шостака І.В., доцента кафедри інженерії програмного забезпечення, к.т.н., доц. Мокляка М.Г., розглянувши матеріали дисертаційного дослідження Мельника Руслана Павловича, встановила: при підготовці бакалаврів за напрямом 6.050103 «Програмна інженерія» в курсі лекцій з дисципліни «Проектування виробничих експертних систем» використовуються результати дисертаційного дослідження, отримані Мельником Русланом Павловичем, зокрема математичні моделі та алгоритми побудови базових операцій криптографічного перетворення інформації на основі спеціалізованих логічних функцій та технологія перетворення інформації на основі спеціалізованих логічних функцій розширеного матричного перекодування.

Голова комісії **І.Б. Туркін**

Члени комісії:

І.В. Шостак

М.Г. Мокляк

Погоджено:
Начальник навчально-аналітичного відділу **В.В. Воронько**

Додаток Б
Результати обчислювального експерименту (вибірка)

Група R 9
0 0 0 1 1 1 1 0 30 --- 0
0 0 1 0 1 1 0 1 45 --- 1
0 0 1 1 0 1 1 0 54 --- 2
0 0 1 1 1 0 0 1 57 --- 3
0 1 0 0 1 0 1 1 75 --- 4
30 57 106 --- 45 54 106 *** 9 9 9 --- 9 9 9
30 89 108 --- 45 106 54 *** 9 9 9 --- 9 9 9
30 106 57 --- 75 86 108 *** 9 9 9 --- 9 9 9
30 108 89 --- 75 108 86 *** 9 9 9 --- 9 9 9
45 54 106 --- 30 57 106 *** 9 9 9 --- 9 9 9
45 89 99 --- 75 101 57 *** 9 9 9 --- 9 9 9
45 99 89 --- 45 99 89 *** 9 9 9 --- 9 9 9
45 106 54 --- 30 89 108 *** 9 9 9 --- 9 9 9
54 45 106 --- 54 45 106 *** 9 9 9 --- 9 9 9
54 101 120 --- 106 45 54 *** 9 9 9 --- 9 9 9
54 106 45 --- 86 75 108 *** 9 9 9 --- 9 9 9
54 120 101 --- 108 75 86 *** 9 9 9 --- 9 9 9
57 30 106 --- 57 30 106 *** 9 9 9 --- 9 9 9
57 75 101 --- 99 45 89 *** 9 9 9 --- 9 9 9
57 101 75 --- 101 75 57 *** 9 9 9 --- 9 9 9
57 106 30 --- 89 30 108 *** 9 9 9 --- 9 9 9
75 57 101 --- 75 57 101 *** 9 9 9 --- 9 9 9
75 86 108 --- 30 106 57 *** 9 9 9 --- 9 9 9
75 101 57 --- 45 89 99 *** 9 9 9 --- 9 9 9
75 108 86 --- 30 108 89 *** 9 9 9 --- 9 9 9
86 75 108 --- 54 106 45 *** 9 9 9 --- 9 9 9
86 99 120 --- 106 54 45 *** 9 9 9 --- 9 9 9
86 108 75 --- 86 108 75 *** 9 9 9 --- 9 9 9
86 120 99 --- 108 86 75 *** 9 9 9 --- 9 9 9
89 30 108 --- 57 106 30 *** 9 9 9 --- 9 9 9
89 45 99 --- 99 89 45 *** 9 9 9 --- 9 9 9
89 99 45 --- 101 57 75 *** 9 9 9 --- 9 9 9
89 108 30 --- 89 108 30 *** 9 9 9 --- 9 9 9
99 45 89 --- 57 75 101 *** 9 9 9 --- 9 9 9
99 86 120 --- 106 30 57 *** 9 9 9 --- 9 9 9
99 89 45 --- 89 45 99 *** 9 9 9 --- 9 9 9
99 120 86 --- 108 30 89 *** 9 9 9 --- 9 9 9
101 54 120 --- 106 57 30 *** 9 9 9 --- 9 9 9
101 57 75 --- 89 99 45 *** 9 9 9 --- 9 9 9
101 75 57 --- 57 101 75 *** 9 9 9 --- 9 9 9
101 120 54 --- 108 89 30 *** 9 9 9 --- 9 9 9
106 30 57 --- 99 86 120 *** 9 9 9 --- 9 9 9
106 45 54 --- 54 101 120 *** 9 9 9 --- 9 9 9
106 54 45 --- 86 99 120 *** 9 9 9 --- 9 9 9
106 57 30 --- 101 54 120 *** 9 9 9 --- 9 9 9
108 30 89 --- 99 120 86 *** 9 9 9 --- 9 9 9
108 75 86 --- 54 120 101 *** 9 9 9 --- 9 9 9
108 86 75 --- 86 120 99 *** 9 9 9 --- 9 9 9
108 89 30 --- 101 120 54 *** 9 9 9 --- 9 9 9
120 54 101 --- 120 99 86 *** 9 9 9 --- 9 9 9
120 86 99 --- 120 86 99 *** 9 9 9 --- 9 9 9
120 99 86 --- 120 54 101 *** 9 9 9 --- 9 9 9
120 101 54 --- 120 101 54 *** 9 9 9 --- 9 9 9

Група R 911
0 0 0 1 1 1 1 0 30 --- 0
0 0 1 0 1 1 0 1 45 --- 1
0 0 1 1 0 1 1 0 54 --- 2
0 0 1 1 1 0 0 1 57 --- 3
0 1 0 0 1 0 1 1 75 --- 4
0 1 0 1 0 1 1 0 86 --- 5
0 1 0 1 1 0 0 1 89 --- 6
0 1 1 0 0 0 1 1 99 --- 7
0 1 1 0 0 1 0 1 101 --- 8
0 1 1 0 1 0 0 1 105 --- 9
0 1 1 0 1 0 1 0 106 --- 10
0 1 1 0 1 1 0 0 108 --- 11
0 1 1 1 1 0 0 0 120 --- 12
0 0 0 0 0 0 0 0 0 --- 13
30 57 106 --- 45 54 106 *** 9 9 9 --- 9 9 9
30 89 108 --- 45 106 54 *** 9 9 9 --- 9 9 9
30 106 57 --- 75 86 108 *** 9 9 9 --- 9 9 9
30 108 89 --- 75 108 86 *** 9 9 9 --- 9 9 9
45 54 106 --- 30 57 106 *** 9 9 9 --- 9 9 9
45 89 99 --- 75 101 57 *** 9 9 9 --- 9 9 9
45 99 89 --- 45 99 89 *** 9 9 9 --- 9 9 9
45 106 54 --- 30 89 108 *** 9 9 9 --- 9 9 9
54 45 106 --- 54 45 106 *** 9 9 9 --- 9 9 9
54 101 120 --- 106 45 54 *** 9 9 9 --- 9 9 9
54 106 45 --- 86 75 108 *** 9 9 9 --- 9 9 9
54 120 101 --- 108 75 86 *** 9 9 9 --- 9 9 9
57 30 106 --- 57 30 106 *** 9 9 9 --- 9 9 9
57 75 101 --- 99 45 89 *** 9 9 9 --- 9 9 9
57 101 75 --- 101 75 57 *** 9 9 9 --- 9 9 9
57 106 30 --- 89 30 108 *** 9 9 9 --- 9 9 9
75 57 101 --- 75 57 101 *** 9 9 9 --- 9 9 9
75 86 108 --- 30 106 57 *** 9 9 9 --- 9 9 9
75 101 57 --- 45 89 99 *** 9 9 9 --- 9 9 9
75 108 86 --- 30 108 89 *** 9 9 9 --- 9 9 9
86 75 108 --- 54 106 45 *** 9 9 9 --- 9 9 9
86 99 120 --- 106 54 45 *** 9 9 9 --- 9 9 9
86 108 75 --- 86 108 75 *** 9 9 9 --- 9 9 9
86 120 99 --- 108 86 75 *** 9 9 9 --- 9 9 9
89 30 108 --- 57 106 30 *** 9 9 9 --- 9 9 9
89 45 99 --- 99 89 45 *** 9 9 9 --- 9 9 9
89 99 45 --- 101 57 75 *** 9 9 9 --- 9 9 9
89 108 30 --- 89 108 30 *** 9 9 9 --- 9 9 9
99 45 89 --- 57 75 101 *** 9 9 9 --- 9 9 9
99 86 120 --- 106 30 57 *** 9 9 9 --- 9 9 9
99 89 45 --- 89 45 99 *** 9 9 9 --- 9 9 9
99 120 86 --- 108 30 89 *** 9 9 9 --- 9 9 9
101 54 120 --- 106 57 30 *** 9 9 9 --- 9 9 9
101 57 75 --- 89 99 45 *** 9 9 9 --- 9 9 9
101 75 57 --- 57 101 75 *** 9 9 9 --- 9 9 9
101 120 54 --- 108 89 30 *** 9 9 9 --- 9 9 9
106 30 57 --- 99 86 120 *** 9 9 9 --- 9 9 9
106 45 54 --- 54 101 120 *** 9 9 9 --- 9 9 9
106 54 45 --- 86 99 120 *** 9 9 9 --- 9 9 9
106 57 30 --- 101 54 120 *** 9 9 9 --- 9 9 9
108 30 89 --- 99 120 86 *** 9 9 9 --- 9 9 9
108 75 86 --- 54 120 101 *** 9 9 9 --- 9 9 9
108 86 75 --- 86 120 99 *** 9 9 9 --- 9 9 9
108 89 30 --- 101 120 54 *** 9 9 9 --- 9 9 9
120 54 101 --- 120 99 86 *** 9 9 9 --- 9 9 9
120 86 99 --- 120 86 99 *** 9 9 9 --- 9 9 9
120 99 86 --- 120 54 101 *** 9 9 9 --- 9 9 9
120 101 54 --- 120 101 54 *** 9 9 9 --- 9 9 9

Додаток В

Результати синтезу базових операцій криптографічного перетворення на основі замін

Пряме перетворення	Обернене перетворення
1 заміна:	
$F^{k}_{15,51,85} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} + - - \\ - + - \\ - - + \end{bmatrix}$	$F^{d}_{15,51,85} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} + - - \\ - + - \\ - - + \end{bmatrix}$
$F^{k}_{30,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +11 \\ -+- \\ --+ \end{bmatrix}$	$F^{d}_{30,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +11 \\ -+- \\ --+ \end{bmatrix}$
$F^{k}_{45,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +10 \\ -+- \\ --+ \end{bmatrix}$	$F^{d}_{45,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +10 \\ -+- \\ --+ \end{bmatrix}$
$F^{k}_{75,51,85} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +01 \\ -+- \\ --+ \end{bmatrix}$	$F^{d}_{75,51,85} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +01 \\ -+- \\ --+ \end{bmatrix}$
$F^{k}_{135,51,85} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +00 \\ -+- \\ --+ \end{bmatrix}$	$F^{d}_{135,51,85} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} +00 \\ -+- \\ --+ \end{bmatrix}$
$F^{k}_{15,54,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} + - - \\ 1+1 \\ --+ \end{bmatrix}$	$F^{d}_{15,54,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} + - - \\ 1+1 \\ --+ \end{bmatrix}$
$F^{k}_{15,57,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} + - - \\ 1+0 \\ --+ \end{bmatrix}$	$F^{d}_{15,57,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} + - - \\ 1+0 \\ --+ \end{bmatrix}$

Пряме перетворення	Обернене перетворення
$F^k_{15,99,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +-- \\ 0+1 \\ --+ \end{bmatrix}$	$F^d_{15,99,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +-- \\ 0+1 \\ --+ \end{bmatrix}$
$F^k_{15,147,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +-- \\ 0+0 \\ --+ \end{bmatrix}$	$F^d_{15,147,85} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +-- \\ 0+0 \\ --+ \end{bmatrix}$
$F^k_{15,51,86} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ -+- \\ 1\ 1+ \end{bmatrix}$	$F^d_{15,51,86} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ -+- \\ 1\ 1+ \end{bmatrix}$
$F^k_{15,51,89} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ -+- \\ 1\ 0+ \end{bmatrix}$	$F^d_{15,51,89} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ -+- \\ 1\ 0+ \end{bmatrix}$
$F^k_{15,51,101} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ -+- \\ 01+ \end{bmatrix}$	$F^d_{15,51,101} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ -+- \\ 01+ \end{bmatrix}$
$F^k_{15,51,149} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ -+- \\ 0\ 0+ \end{bmatrix}$	$F^d_{15,51,149} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ -+- \\ 0\ 0+ \end{bmatrix}$
2 заміни:	
$F^k_{30,57,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +11 \\ 1+0 \\ --+ \end{bmatrix}$	$F^d_{30,57,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +11 \\ 1+0 \\ --+ \end{bmatrix}$
$F^k_{30,147,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +11 \\ 0+0 \\ --+ \end{bmatrix}$	$F^d_{30,147,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} = \begin{bmatrix} +11 \\ 0+0 \\ --+ \end{bmatrix}$

Пряме перетворення	**Обернене перетворення**
$F^{k}_{45,54,85}=\begin{bmatrix} x_1\oplus(x_2\cdot\bar{x}_3) \\ x_2\oplus(x_1\cdot x_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +10 \\ 1+1 \\ --+ \end{bmatrix}$	$F^{d}_{45,54,85}=\begin{bmatrix} x_1\oplus(x_2\cdot\bar{x}_3) \\ x_2\oplus(x_1\cdot x_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +10 \\ 1+1 \\ --+ \end{bmatrix}$
$F^{k}_{45,99,85}=\begin{bmatrix} x_1\oplus(x_2\cdot\bar{x}_3) \\ x_2\oplus(\bar{x}_1\cdot x_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +10 \\ 0+1 \\ --+ \end{bmatrix}$	$F^{d}_{45,99,85}=\begin{bmatrix} x_1\oplus(x_2\cdot\bar{x}_3) \\ x_2\oplus(\bar{x}_1\cdot x_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +10 \\ 0+1 \\ --+ \end{bmatrix}$
$F^{k}_{75,57,85}=\begin{bmatrix} x_1\oplus(\bar{x}_2\cdot x_3) \\ x_2\oplus(x_1\cdot\bar{x}_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +01 \\ 1+0 \\ --+ \end{bmatrix}$	$F^{d}_{75,57,85}=\begin{bmatrix} x_1\oplus(\bar{x}_2\cdot x_3) \\ x_2\oplus(x_1\cdot\bar{x}_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +01 \\ 1+0 \\ --+ \end{bmatrix}$
$F^{k}_{75,147,85}=\begin{bmatrix} x_1\oplus(\bar{x}_2\cdot x_3) \\ x_2\oplus(\bar{x}_1\cdot\bar{x}_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +01 \\ 0+0 \\ --+ \end{bmatrix}$	$F^{d}_{75,147,85}=\begin{bmatrix} x_1\oplus(\bar{x}_2\cdot x_3) \\ x_2\oplus(\bar{x}_1\cdot\bar{x}_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +01 \\ 0+0 \\ --+ \end{bmatrix}$
$F^{k}_{135,54,85}=\begin{bmatrix} x_1\oplus(\bar{x}_2\cdot\bar{x}_3) \\ x_2\oplus(x_1\cdot x_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +00 \\ 1+1 \\ --+ \end{bmatrix}$	$F^{d}_{135,54,85}=\begin{bmatrix} x_1\oplus(\bar{x}_2\cdot\bar{x}_3) \\ x_2\oplus(x_1\cdot x_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +00 \\ 1+1 \\ --+ \end{bmatrix}$
$F^{k}_{135,99,85}=\begin{bmatrix} x_1\oplus(\bar{x}_2\cdot\bar{x}_3) \\ x_2\oplus(\bar{x}_1\cdot x_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +00 \\ 0+1 \\ --+ \end{bmatrix}$	$F^{d}_{135,99,85}=\begin{bmatrix} x_1\oplus(\bar{x}_2\cdot\bar{x}_3) \\ x_2\oplus(\bar{x}_1\cdot x_3) \\ x_3 \end{bmatrix}=\begin{bmatrix} +00 \\ 0+1 \\ --+ \end{bmatrix}$
$F^{k}_{30,51,89}=\begin{bmatrix} x_1\oplus(x_2\cdot x_3) \\ x_2 \\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2) \end{bmatrix}=\begin{bmatrix} +01 \\ -+- \\ 10+ \end{bmatrix}$	$F^{d}_{30,51,89}=\begin{bmatrix} x_1\oplus(x_2\cdot x_3) \\ x_2 \\ x_3\oplus(x_1\cdot\bar{x}_2) \end{bmatrix}=\begin{bmatrix} +01 \\ -+- \\ 10+ \end{bmatrix}$
$F^{k}_{30,51,149}=\begin{bmatrix} x_1\oplus(x_2\cdot x_3) \\ x_2 \\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2) \end{bmatrix}=\begin{bmatrix} +11 \\ -+- \\ 00+ \end{bmatrix}$	$F^{d}_{30,51,149}=\begin{bmatrix} x_1\oplus(x_2\cdot x_3) \\ x_2 \\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2) \end{bmatrix}=\begin{bmatrix} +11 \\ -+- \\ 00+ \end{bmatrix}$
$F^{k}_{45,51,89}=\begin{bmatrix} x_1\oplus(x_2\cdot\bar{x}_3) \\ x_2 \\ x_3\oplus(x_1\cdot\bar{x}_2) \end{bmatrix}=\begin{bmatrix} +10 \\ -+- \\ 10+ \end{bmatrix}$	$F^{d}_{45,51,89}=\begin{bmatrix} x_1\oplus(x_2\cdot\bar{x}_3) \\ x_2 \\ x_3\oplus(x_1\cdot\bar{x}_2) \end{bmatrix}=\begin{bmatrix} +10 \\ -+- \\ 10+ \end{bmatrix}$

Пряме перетворення	Обернене перетворення
$F^{k}_{45,51,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +1\,0 \\ -+- \\ 0\,0+ \end{bmatrix}$	$F^{d}_{45,51,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +1\,0 \\ -+- \\ 0\,0+ \end{bmatrix}$
$F^{k}_{135,51,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +0\,0 \\ -+- \\ 1\,1+ \end{bmatrix}$	$F^{d}_{135,51,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +0\,0 \\ -+- \\ 1\,1+ \end{bmatrix}$
$F^{k}_{135,51,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +0\,0 \\ -+- \\ 0\,1+ \end{bmatrix}$	$F^{d}_{135,51,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +0\,0 \\ -+- \\ 0\,1+ \end{bmatrix}$
$F^{k}_{15,54,101} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 1+1 \\ 1\,0+ \end{bmatrix}$	$F^{d}_{15,54,101} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 1+1 \\ 1\,0+ \end{bmatrix}$
$F^{k}_{15,54,149} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 1+1 \\ 0\,0+ \end{bmatrix}$	$F^{d}_{15,54,149} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 1+1 \\ 0\,0+ \end{bmatrix}$
$F^{k}_{15,57,101} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 1+0 \\ 0\,1+ \end{bmatrix}$	$F^{d}_{15,57,101} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 1+0 \\ 0\,1+ \end{bmatrix}$
$F^{d}_{15,57,149} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 1+0 \\ 0\,0+ \end{bmatrix}$	$F^{d}_{15,57,149} = \begin{bmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 1+0 \\ 0\,0+ \end{bmatrix}$
$F^{k}_{15,147,86} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 0+0 \\ 1\,1+ \end{bmatrix}$	$F^{d}_{15,147,86} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 0+0 \\ 1\,1+ \end{bmatrix}$
$F^{k}_{15,147,89} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 0+0 \\ 1\,0+ \end{bmatrix}$	$F^{d}_{15,147,89} = \begin{bmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +-- \\ 0+0 \\ 1\,0+ \end{bmatrix}$

Пряме перетворення	Обернене перетворення
З заміни:	
$F^{k}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +11 \\ 1+0 \\ 0\,0+ \end{bmatrix}$	$F^{d}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +11 \\ 1+0 \\ 0\,0+ \end{bmatrix}$
$F^{k}_{30,147,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +11 \\ 0+0 \\ 1\,0+ \end{bmatrix}$	$F^{d}_{30,147,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +11 \\ 0+0 \\ 1\,0+ \end{bmatrix}$
$F^{k}_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +10 \\ 1+1 \\ 0\,0+ \end{bmatrix}$	$F^{d}_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +10 \\ 1+1 \\ 0\,0+ \end{bmatrix}$
$F^{k}_{45,99,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +10 \\ 0+1 \\ 1\,0+ \end{bmatrix}$	$F^{d}_{45,99,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix} = \begin{bmatrix} +10 \\ 0+1 \\ 1\,0+ \end{bmatrix}$
$F^{k}_{75,57,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +01 \\ 1+0 \\ 0\,1+ \end{bmatrix}$	$F^{d}_{75,57,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +01 \\ 1+0 \\ 0\,1+ \end{bmatrix}$
$F^{k}_{75,147,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +01 \\ 0+0 \\ 1\,1+ \end{bmatrix}$	$F^{d}_{75,147,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +01 \\ 0+0 \\ 1\,1+ \end{bmatrix}$
$F^{k}_{135,54,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +00 \\ 1+1 \\ 0\,1+ \end{bmatrix}$	$F^{d}_{135,54,101} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +00 \\ 1+1 \\ 0\,1+ \end{bmatrix}$
$F^{k}_{135,99,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +00 \\ 0+1 \\ 1\,1+ \end{bmatrix}$	$F^{d}_{135,99,86} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{bmatrix} = \begin{bmatrix} +00 \\ 0+1 \\ 1\,1+ \end{bmatrix}$

Додаток Д

Операції з однією заміною

Перестановка	Операція криптографічного перетворення		Операція криптографічного перетворення	
	пряма	обернена	пряма	обернена
1	$F^k_{30,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix}$	$F^d_{30,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix}$	$F^k_{135,51,85} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix}$	$F^d_{135,51,85} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix}$
2	$F^k_{30,85,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \end{bmatrix}$	$F^d_{30,85,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \end{bmatrix}$	$F^{\mathrm{k}}_{135,85,51} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \\ x_2 \end{bmatrix}$	$F^d_{135,85,51} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \\ x_2 \end{bmatrix}$
3	$F^k_{51,30,85} = \begin{bmatrix} x_2 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \end{bmatrix}$	$F^d_{54,15,85} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \\ x_3 \end{bmatrix}$	$F^k_{51,135,85} = \begin{bmatrix} x_2 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$	$F^d_{147,15,85} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \\ x_3 \end{bmatrix}$
4	$F^k_{51,85,30} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^d_{86,15,51} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \\ x_2 \end{bmatrix}$	$F^k_{51,85,135} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^d_{149,15,51} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \\ x_2 \end{bmatrix}$
5	$F^k_{85,30,51} = \begin{bmatrix} x_3 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \end{bmatrix}$	$F^d_{54,85,15} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \\ x_1 \end{bmatrix}$	$F^k_{85,135,51} = \begin{bmatrix} x_3 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \end{bmatrix}$	$F^d_{147,85,15} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \\ x_1 \end{bmatrix}$
6	$F^k_{85,51,30} = \begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^d_{86,51,15} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \\ x_1 \end{bmatrix}$	$F^k_{85,51,135} = \begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^d_{149,51,15} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \\ x_1 \end{bmatrix}$

Перестановка	Операція криптографічного перетворення		Операція криптографічного перетворення	
	пряма	обернена	пряма	обернена
1	$F^{k}_{45,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix}$	$F^{d}_{45,51,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix}$	$F^{k}_{75,51,85} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix}$	$F^{d}_{75,51,85} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix}$
2	$F^{k}_{45,85,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \\ x_2 \end{bmatrix}$	$F^{d}_{75,85,51} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \\ x_2 \end{bmatrix}$	$F^{k}_{75,85,51} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \\ x_2 \end{bmatrix}$	$F^{d}_{45,85,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \\ x_2 \end{bmatrix}$
3	$F^{k}_{51,45,85} = \begin{bmatrix} x_2 \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$	$F^{d}_{57,15,85} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \\ x_3 \end{bmatrix}$	$F^{k}_{51,75,85} = \begin{bmatrix} x_2 \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \end{bmatrix}$	$F^{d}_{99,15,85} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_1 \\ x_3 \end{bmatrix}$
4	$F^{k}_{51,85,45} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{d}_{89,15,51} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \\ x_2 \end{bmatrix}$	$F^{k}_{51,85,75} = \begin{bmatrix} x_2 \\ x_3 \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \end{bmatrix}$	$F^{d}_{101,15,51} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_1 \\ x_2 \end{bmatrix}$
5	$F^{k}_{85,45,51} = \begin{bmatrix} x_3 \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \end{bmatrix}$	$F^{d}_{99,85,15} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \\ x_1 \end{bmatrix}$	$F^{k}_{85,75,51} = \begin{bmatrix} x_3 \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \end{bmatrix}$	$F^{d}_{57,85,15} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \\ x_1 \end{bmatrix}$
6	$F^{k}_{85,51,45} = \begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{d}_{101,51,15} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_2 \\ x_1 \end{bmatrix}$	$F^{k}_{85,51,75} = \begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \end{bmatrix}$	$F^{d}_{89,51,15} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \\ x_1 \end{bmatrix}$

Додаток Ж

Операції з двома замінами

Перестановка	Операція криптографічного перетворення		Операція криптографічного перетворення	
	пряма	обернена	пряма	обернена
1	$F^{k}_{30,57,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$	$F^{d}_{30,57,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$	$F^{k}_{30,147,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$	$F^{d}_{30,147,85} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$
2	$F^{k}_{30,85,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{30,89,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \end{bmatrix}$	$F^{k}_{30,85,147} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{30,149,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \end{bmatrix}$
3	$F^{k}_{57,30,85} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \end{bmatrix}$	$F^{k}_{54,45,85} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$	$F^{k}_{147,30,85} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \end{bmatrix}$	$F^{k}_{54,135,85} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$
4	$F^{k}_{57,85,30} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{k}_{86,75,51} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \end{bmatrix}$	$F^{k}_{147,85,30} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{k}_{86,135,51} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \end{bmatrix}$
5	$F^{k}_{85,30,57} = \begin{bmatrix} x_3 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{54,101,15} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_1 \end{bmatrix}$	$F^{k}_{85,30,147} = \begin{bmatrix} x_3 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{54,149,15} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \end{bmatrix}$
6	$F^{k}_{85,57,30} = \begin{bmatrix} x_3 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{k}_{86,99,15} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_1 \end{bmatrix}$	$F^{k}_{85,147,30} = \begin{bmatrix} x_3 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{k}_{86,147,15} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \end{bmatrix}$

Перестановка	Операція криптографічного перетворення		Операція криптографічного перетворення	
	пряма	обернена	пряма	обернена
1	$F^{k}_{30,51,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{30,51,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{k}_{30,51,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{30,51,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$
2	$F^{k}_{30,149,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \end{bmatrix}$	$F^{k}_{30,85,147} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{30,89,51} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \end{bmatrix}$	$F^{d}_{30,85,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}$
3	$F^{k}_{51,30,149} = \begin{bmatrix} x_2 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{k}_{54,15,149} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{k}_{51,30,89} = \begin{bmatrix} x_2 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{54,15,101} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix}$
4	$F^{k}_{51,149,30} = \begin{bmatrix} x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{k}_{86,15,147} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{51,89,30} = \begin{bmatrix} x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{d}_{86,15,99} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix}$
5	$F^{k}_{149,30,51} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \end{bmatrix}$	$F^{k}_{54,85,135} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{89,30,51} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \end{bmatrix}$	$F^{d}_{54,85,45} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$
6	$F^{k}_{149,51,30} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{k}_{86,51,135} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{89,51,30} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{d}_{86,51,75} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \end{bmatrix}$

Додаток З

Операції з трьома замінами

Перестановка	Операція криптографічного перетворення		Операція криптографічного перетворення	
	пряма	обернена	пряма	обернена
1	$F^{k}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{\mathrm{d}}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{k}_{30,147,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{30,147,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$
2	$F^{k}_{30,149,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{\mathrm{d}}_{30,89,147} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{30,89,147} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{\mathrm{d}}_{30,149,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}$
3	$F^{k}_{57,30,149} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{54,45,149} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{k}_{147,30,89} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{54,135,101} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix}$
4	$F^{k}_{57,149,30} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{d}_{86,75,147} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{147,89,30} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{d}_{86,135,99} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix}$
5	$F^{k}_{149,30,57} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{d}_{54,101,135} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{89,30,147} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{d}_{54,149,45} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$
	$F^{k}_{149,57,30} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{d}_{86,99,135} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{89,147,30} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix}$	$F^{d}_{86,147,75} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \end{bmatrix}$

Перестановка	Операція криптографічного перетворення		Операція криптографічного перетворення	
	пряма	обернена	пряма	обернена
1	$F^{k}_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{45,54,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{k}_{45,99,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\hat{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{45,99,89} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\hat{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$
2	$F^{k}_{45,149,54} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot x_3) \end{bmatrix}$	$F^{\mathrm{d}}_{75,86,147} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{45,89,99} = \begin{bmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix}$	$F^{\mathrm{d}}_{75,101,57} = \begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix}$
3	$F^{k}_{54,45,149} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{57,30,149} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{k}_{99,45,89} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{bmatrix}$	$F^{d}_{57,75,101} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{bmatrix}$
4	$F^{k}_{54,149,45} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{d}_{89,30,147} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{99,89,45} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{d}_{89,45,99} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix}$
5	$F^{k}_{149,45,54} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \end{bmatrix}$	$F^{d}_{99,86,135} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{89,45,99} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \end{bmatrix}$	$F^{d}_{99,89,45} = \begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$
6	$F^{k}_{149,54,45} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{d}_{101,54,135} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{k}_{89,99,45} = \begin{bmatrix} x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \end{bmatrix}$	$F^{d}_{101,57,75} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \end{bmatrix}$

Додаток К

Опис пакету статичних тестів NIST STS

№	Назва статистичного тесту	Статистика тесту *c(S)*	Дефект, що виявляється у тесті
1.	Частотний або монобітний тест.	Нормалізована абсолютна сума значень елементів послідовності.	Досить велика кількість нулів або одиниць у згенерованій послідовності.
2.	Частотний тест в середині блоку.	Міра узгодженості одиниць, що виявляються в ході тесту із теоретичним сподіванням.	Відхилення частоти появи одиниць у блоці (локальне) від ідеального значення $\frac{1}{2}$.
3.	Перевірка накопичених сум.	Максимальне відхилення значень накопиченої суми елементів послідовності від початкової точки відліку .	Велика кількість одиниць або нулів на початку чи в кінці послідовності.
4.	Перевірка серій.	Загальна кількість серій на всій послідовності.	Занадто швидка або повільна зміна знаку в ході генерації досліджуваної послідовності.
5.	Перевірка максимальної довжини серії в блоці.	Міра узгодження значень максимальної довжини, що виявляються в ході тесту із теоретичним сподіванням.	Відхилення від теоретичного закону розподілу максимальної довжини серій одиниць.
6.	Перевірка рангу двійкової матриці.	Міра узгодження значень рангів різноманітних порядків, що виявляються в ході тесту із теоретичним сподіванням.	Відхилення емпіричного закону розподілу рангів матриць від теоретичного, що вказує на залежність елементів згенерованої послідовності.
7.	Спектральний аналіз на основі дискретного перетворення Фур'є.	Нормалізована різниця кількості частотних компонент, що виявляються із теоретичним сподіванням за умови перевищення граничного рівня 95%.	Виявлення трендів у двійковій послідовності.
8.	Перевірка шаблонів, які перекриваються.	Міра узгодженості кількості шаблонів, що перекриваються у ході виконання тесту із теоретичними значеннями	Велика кількість *m*-бітових серій одиниць у послідовності.
9.	Універсальний тест Маурера.	Сума логарифма відстаней між *l*-бітними шаблонами.	Можливість стиснення послідовності.
10.	Ентропійний тест.	Міра узгодженості значення джерела ентропії, що отримується в ході виконання тесту із таким, що теоретично очікується від випадкового.	Нерівномірність розподілу *m*-бітових слів у послідовності (регулярність властивостей джерела).
11.	Перевірка випадкових відхилень.	Міра узгодженості спостережуваної кількості візитів при випадковому блуканні у заданий стан в середині циклу із тим, що теоретично очікується.	Відхилення від теоретичного закону розподілу візитів в конкретний стан при випадковому блуканні.
12.	Перевірка випадкових відхилень.	Загальна кількість візитів при випадковому блуканні.	Відхилення від теоретично очікуваної кількості загальної кількості візитів при випадковому блуканні в заданий стан.
13.	Послідовний тест.	Міра узгодженості кількості всіх варіантів m-бітових шаблонів, які спостерігаються в ході виконання із тою кількістю, що очікується теоретично.	Нерівномірність розподілу m-бітових слів у послідовності.
14.	Перевірка стискання згідно алгоритму Лемпеля-Зіва.	Кількість різних слів у послідовності.	Велика ступінь стискання послідовності, що проходить тестування у порівнянні із ступенем стискання, що теоретично очікується від випадкової послідовності.
15.	Перевірка шаблонів, що не перекриваються.	Міра узгодженості кількості неперіодичних шаблонів у послідовності, що проходить тест із теоретичним значенням.	Велика кількість заданих у послідовності неперіодичних шаблонів.
16.	Перевірка лінійної складності.	Міра узгодженості спостережуваної послідовності кількості подій, котрі полягають у появі фіксованої довжини еквівалентного ЛРР для заданого блока з теоретичним.	На недостатню складність тестованої послідовності вказує відхилення емпіричного розподілу довжин еквівалентних ЛРР послідовностей фіксованої довжини від теоретичного закону розподілу випадкової послідовності.

Додаток Л

Результати тестування датчика RANDOM

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <R_RND_D1.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
9	9	14	15	8	11	6	7	10	11	0.595549	0.9800	Frequency
7	10	8	10	9	12	10	15	12	7	0.779188	0.9800	BlockFrequency
11	9	6	9	10	10	18	10	5	12	0.262249	1.0000	CumulativeSums
10	11	11	9	15	11	7	10	7	9	0.851383	1.0000	CumulativeSums
11	7	7	12	9	12	6	11	13	12	0.759756	0.9800	Runs
13	8	5	14	12	7	8	15	8	10	0.350485	0.9900	LongestRun
8	14	13	12	12	4	13	6	9	9	0.350485	0.9900	Rank
3	7	6	13	10	13	6	10	14	18	0.026948	1.0000	FFT
7	3	7	9	13	9	13	13	19	7	0.028817	0.9900	NonOverlappingTemplate
9	10	12	7	8	14	10	10	14	6	0.678686	1.0000	NonOverlappingTemplate
8	11	11	14	8	10	8	13	9	8	0.883171	0.9900	NonOverlappingTemplate
12	15	10	6	10	6	18	8	7	8	0.115387	1.0000	NonOverlappingTemplate
11	14	10	6	13	8	10	4	13	11	0.419021	0.9800	NonOverlappingTemplate
11	9	9	7	11	15	9	8	9	12	0.851383	0.9900	NonOverlappingTemplate
10	12	8	13	6	9	15	10	11	6	0.574903	1.0000	NonOverlappingTemplate
12	7	13	15	7	10	10	9	11	6	0.595549	1.0000	NonOverlappingTemplate
9	7	12	14	6	11	7	12	7	15	0.401199	0.9900	NonOverlappingTemplate
15	6	7	11	6	10	15	6	17	7	0.055361	1.0000	NonOverlappingTemplate
11	7	11	7	10	12	11	6	15	10	0.678686	1.0000	NonOverlappingTemplate
9	14	9	13	12	7	5	8	16	7	0.249284	0.9900	NonOverlappingTemplate
13	7	12	10	12	12	11	7	9	7	0.834308	0.9700	NonOverlappingTemplate
12	14	13	8	7	10	3	16	10	7	0.137282	1.0000	NonOverlappingTemplate
9	8	17	13	13	11	10	6	7	6	0.249284	1.0000	NonOverlappingTemplate
7	8	14	15	13	8	7	8	11	9	0.514124	1.0000	NonOverlappingTemplate
8	8	17	14	8	4	10	14	7	10	0.129620	0.9800	NonOverlappingTemplate
11	11	8	10	14	12	9	10	9	6	0.883171	1.0000	NonOverlappingTemplate
13	8	12	7	5	10	13	11	10	11	0.719747	0.9900	NonOverlappingTemplate
15	10	12	6	8	11	10	11	9	8	0.779188	0.9900	NonOverlappingTemplate
12	10	8	13	11	11	8	6	6	15	0.534146	1.0000	NonOverlappingTemplate
11	7	7	10	10	10	12	11	11	11	0.978072	0.9700	NonOverlappingTemplate
12	9	6	8	12	7	15	12	6	13	0.419021	0.9800	NonOverlappingTemplate
12	9	12	9	11	10	9	11	7	10	0.987896	0.9900	NonOverlappingTemplate
11	13	11	7	9	10	8	11	9	11	0.971699	1.0000	NonOverlappingTemplate
8	7	11	12	11	7	10	13	12	9	0.897763	0.9800	NonOverlappingTemplate
7	10	10	8	10	17	7	7	12	12	0.455937	0.9800	NonOverlappingTemplate
10	9	9	9	12	12	12	8	9	10	0.991468	0.9900	NonOverlappingTemplate
10	10	8	8	6	10	9	11	16	12	0.678686	1.0000	NonOverlappingTemplate
10	10	10	4	10	12	4	20	9	11	0.037566	1.0000	NonOverlappingTemplate
8	22	14	5	11	7	9	4	8	12	0.003712	0.9900	NonOverlappingTemplate
13	10	10	5	10	7	9	10	13	13	0.719747	0.9800	NonOverlappingTemplate
6	9	13	13	9	8	8	7	10	17	0.334538	0.9800	NonOverlappingTemplate
11	7	5	13	10	12	12	8	14	8	0.574903	1.0000	NonOverlappingTemplate
12	10	9	10	9	15	7	7	7	14	0.595549	0.9900	NonOverlappingTemplate
11	14	14	9	8	9	6	9	8	12	0.699313	0.9900	NonOverlappingTemplate
11	7	8	7	13	18	9	3	12	12	0.080519	1.0000	NonOverlappingTemplate
10	13	7	15	14	5	8	11	12	5	0.224821	1.0000	NonOverlappingTemplate
11	5	14	13	8	11	8	12	8	10	0.657933	0.9800	NonOverlappingTemplate
12	9	15	7	13	8	6	14	4	12	0.191687	0.9900	NonOverlappingTemplate
14	11	15	6	9	10	11	7	6	11	0.474986	0.9900	NonOverlappingTemplate
12	12	7	15	5	7	11	6	16	9	0.162606	0.9800	NonOverlappingTemplate
14	9	10	9	13	7	9	13	11	5	0.616305	1.0000	NonOverlappingTemplate
13	7	19	7	9	10	5	11	8	11	0.122325	0.9700	NonOverlappingTemplate
8	8	13	10	10	5	12	20	2	12	0.010988	1.0000	NonOverlappingTemplate
9	12	6	9	13	11	8	8	9	15	0.678686	1.0000	NonOverlappingTemplate
12	5	12	11	11	8	8	9	11	13	0.798139	0.9800	NonOverlappingTemplate
12	14	11	9	15	5	2	7	13	12	0.071177	0.9800	NonOverlappingTemplate
15	7	13	9	7	15	7	12	7	8	0.319084	0.9900	NonOverlappingTemplate
9	6	11	9	16	11	10	8	8	12	0.657933	0.9800	NonOverlappingTemplate
8	9	11	15	16	10	8	7	9	7	0.437274	0.9900	NonOverlappingTemplate
11	6	15	11	9	8	11	9	8	12	0.759756	0.9900	NonOverlappingTemplate

13	11	13	9	12	6	8	11	11	6	0.719747	1.0000	NonOverlappingTemplate
14	8	11	10	11	7	9	7	11	12	0.867692	0.9800	NonOverlappingTemplate
12	13	4	6	11	12	10	9	12	11	0.574903	0.9900	NonOverlappingTemplate
6	7	12	12	9	10	15	11	10	8	0.699313	1.0000	NonOverlappingTemplate
9	9	8	11	14	6	9	11	11	12	0.867692	1.0000	NonOverlappingTemplate
7	9	13	7	12	14	8	11	5	14	0.401199	0.9900	NonOverlappingTemplate
13	7	11	13	5	7	11	13	13	7	0.437274	1.0000	NonOverlappingTemplate
10	6	4	5	12	14	12	9	15	13	0.137282	0.9700	NonOverlappingTemplate
8	19	9	12	16	6	11	7	5	7	0.028817	0.9800	NonOverlappingTemplate
13	12	13	8	10	9	8	5	13	9	0.678686	0.9800	NonOverlappingTemplate
14	10	13	7	11	9	10	8	8	10	0.883171	0.9900	NonOverlappingTemplate
7	12	8	7	11	15	10	10	11	9	0.798139	1.0000	NonOverlappingTemplate
11	5	11	9	8	11	16	13	10	6	0.401199	0.9800	NonOverlappingTemplate
12	8	6	9	9	11	9	16	10	10	0.699313	0.9600	NonOverlappingTemplate
11	15	7	7	15	10	10	8	8	9	0.554420	0.9600	NonOverlappingTemplate
16	10	8	9	12	10	10	8	7	10	0.759756	0.9900	NonOverlappingTemplate
12	7	11	13	10	11	9	9	7	11	0.935716	1.0000	NonOverlappingTemplate
12	8	14	5	9	13	9	9	11	10	0.719747	0.9900	NonOverlappingTemplate
12	8	14	7	9	11	10	8	7	14	0.699313	0.9800	NonOverlappingTemplate
12	16	6	5	10	13	13	7	8	10	0.262249	1.0000	NonOverlappingTemplate
10	13	11	15	11	8	5	16	2	9	0.055361	0.9700	NonOverlappingTemplate
14	16	6	7	10	6	8	11	12	10	0.334538	0.9800	NonOverlappingTemplate
7	3	7	9	13	9	13	13	19	7	0.028817	0.9900	NonOverlappingTemplate
8	9	8	8	8	16	11	7	8	17	0.236810	0.9900	NonOverlappingTemplate
10	9	12	13	8	12	11	9	6	10	0.911413	1.0000	NonOverlappingTemplate
10	7	11	12	13	14	5	8	12	8	0.574903	0.9900	NonOverlappingTemplate
9	13	10	5	7	9	8	13	14	12	0.554420	1.0000	NonOverlappingTemplate
9	13	11	8	9	13	9	9	9	10	0.971699	0.9800	NonOverlappingTemplate
6	14	9	9	10	14	4	12	8	14	0.275709	1.0000	NonOverlappingTemplate
13	14	11	7	9	11	10	9	8	8	0.867692	0.9900	NonOverlappingTemplate
10	8	6	12	10	10	12	11	11	10	0.964295	0.9900	NonOverlappingTemplate
9	12	13	7	9	10	8	15	8	9	0.759756	0.9900	NonOverlappingTemplate
9	7	9	15	10	10	11	11	8	10	0.897763	0.9900	NonOverlappingTemplate
11	8	7	9	10	16	14	12	4	9	0.289667	0.9700	NonOverlappingTemplate
14	8	12	6	8	12	12	7	11	10	0.719747	0.9800	NonOverlappingTemplate
10	8	5	6	11	17	8	13	7	15	0.115387	0.9800	NonOverlappingTemplate
8	9	6	8	7	14	13	9	14	12	0.534146	0.9900	NonOverlappingTemplate
12	14	5	10	8	11	10	15	8	7	0.455937	0.9700	NonOverlappingTemplate
4	13	10	7	10	8	14	10	8	16	0.249284	0.9900	NonOverlappingTemplate
11	4	11	13	11	6	15	10	12	7	0.334538	0.9900	NonOverlappingTemplate
4	9	12	7	8	11	13	14	9	13	0.437274	1.0000	NonOverlappingTemplate
9	14	15	7	6	8	13	14	5	9	0.202268	0.9900	NonOverlappingTemplate
12	16	9	9	9	9	7	10	8	11	0.759756	1.0000	NonOverlappingTemplate
8	18	11	9	15	7	9	12	9	2	0.042808	0.9900	NonOverlappingTemplate
8	12	12	8	9	11	7	10	13	10	0.935716	0.9900	NonOverlappingTemplate
12	11	7	8	10	12	10	12	11	7	0.935716	1.0000	NonOverlappingTemplate
9	15	13	9	7	14	8	8	11	6	0.474986	0.9900	NonOverlappingTemplate
12	5	12	8	11	4	10	18	11	9	0.122325	1.0000	NonOverlappingTemplate
12	7	14	14	12	12	3	7	7	12	0.191687	0.9800	NonOverlappingTemplate
12	7	11	12	5	10	14	16	7	6	0.213309	1.0000	NonOverlappingTemplate
12	11	8	5	9	6	10	12	14	13	0.534146	1.0000	NonOverlappingTemplate
11	8	8	17	7	10	9	9	10	11	0.637119	0.9900	NonOverlappingTemplate
13	5	6	14	8	14	6	14	13	7	0.137282	0.9900	NonOverlappingTemplate
8	4	14	7	11	10	13	14	12	7	0.319084	1.0000	NonOverlappingTemplate
14	10	10	8	14	8	4	9	13	10	0.474986	0.9800	NonOverlappingTemplate
10	19	7	10	11	9	10	7	11	6	0.224821	1.0000	NonOverlappingTemplate
14	5	15	4	11	15	9	10	4	13	0.042808	1.0000	NonOverlappingTemplate
10	6	14	7	14	12	8	11	9	9	0.657933	0.9900	NonOverlappingTemplate
11	10	8	5	6	8	7	15	17	13	0.115387	0.9800	NonOverlappingTemplate
10	3	11	14	9	7	11	9	11	15	0.319084	0.9900	NonOverlappingTemplate
9	10	11	8	14	9	3	15	9	12	0.334538	0.9900	NonOverlappingTemplate
13	12	11	6	8	7	19	10	8	6	0.108791	1.0000	NonOverlappingTemplate
5	16	14	9	9	6	9	10	8	14	0.236810	0.9900	NonOverlappingTemplate
9	7	9	11	10	13	8	12	10	11	0.964295	1.0000	NonOverlappingTemplate
7	14	11	9	10	9	14	8	9	9	0.834308	0.9900	NonOverlappingTemplate
13	15	12	9	9	4	13	7	5	13	0.171867	0.9900	NonOverlappingTemplate
12	10	8	14	9	17	9	9	8	4	0.236810	1.0000	NonOverlappingTemplate
17	9	7	12	13	13	9	9	4	7	0.171867	0.9800	NonOverlappingTemplate
3	14	11	8	16	7	10	10	12	9	0.213309	0.9900	NonOverlappingTemplate
12	6	14	9	8	5	16	13	12	5	0.122325	0.9800	NonOverlappingTemplate
11	11	8	8	9	12	12	8	12	9	0.971699	1.0000	NonOverlappingTemplate

7	8	7	8	16	5	12	16	9	12	0.153763	0.9900	NonOverlappingTemplate
11	13	10	6	10	9	11	8	11	11	0.946308	1.0000	NonOverlappingTemplate
10	15	12	9	5	6	10	12	9	12	0.534146	0.9900	NonOverlappingTemplate
8	8	7	5	12	12	10	11	12	15	0.534146	1.0000	NonOverlappingTemplate
11	13	9	14	9	9	5	7	11	12	0.657933	0.9900	NonOverlappingTemplate
14	7	10	7	15	6	9	10	9	13	0.474986	0.9900	NonOverlappingTemplate
9	7	9	7	12	15	16	8	11	6	0.304126	0.9700	NonOverlappingTemplate
4	10	15	12	8	16	10	1	14	10	0.016717	1.0000	NonOverlappingTemplate
10	15	3	11	11	8	9	9	14	10	0.366918	0.9900	NonOverlappingTemplate
14	8	8	11	11	11	15	7	6	9	0.554420	0.9700	NonOverlappingTemplate
10	8	7	9	11	12	8	15	10	10	0.851383	0.9800	NonOverlappingTemplate
9	7	12	8	6	14	16	13	10	5	0.213309	0.9800	NonOverlappingTemplate
9	9	16	12	10	10	13	6	6	9	0.494392	0.9700	NonOverlappingTemplate
11	9	11	14	8	8	10	7	13	9	0.867692	0.9900	NonOverlappingTemplate
6	11	12	3	10	16	10	11	9	12	0.262249	1.0000	NonOverlappingTemplate
10	13	9	15	10	10	7	9	7	10	0.798139	1.0000	NonOverlappingTemplate
10	12	9	14	11	11	10	7	10	6	0.851383	1.0000	NonOverlappingTemplate
11	21	2	13	9	8	13	10	10	3	0.002203	0.9700	NonOverlappingTemplate
8	6	8	17	11	8	5	12	13	12	0.213309	0.9900	NonOverlappingTemplate
9	16	7	8	19	10	12	6	7	6	0.040108	0.9900	NonOverlappingTemplate
10	8	11	9	9	8	12	14	11	8	0.935716	1.0000	NonOverlappingTemplate
15	13	13	6	5	9	10	10	13	6	0.275709	0.9700	NonOverlappingTemplate
3	8	8	15	9	16	13	9	13	6	0.080519	1.0000	NonOverlappingTemplate
11	10	12	8	10	9	17	7	9	7	0.554420	0.9900	NonOverlappingTemplate
14	16	6	7	10	6	8	11	12	10	0.334538	0.9800	NonOverlappingTemplate
14	7	13	17	8	8	9	9	6	9	0.275709	0.9700	OverlappingTemplate
10	9	14	8	15	10	9	11	4	10	0.494392	1.0000	Universal
9	12	8	7	11	15	11	8	9	10	0.834308	1.0000	ApproximateEntropy
6	5	6	2	3	2	9	11	5	8	0.048716	1.0000	RandomExcursions
4	1	3	8	3	4	7	6	14	7	0.002971	0.9825	RandomExcursions
5	5	6	2	5	5	8	9	4	8	0.437274	1.0000	RandomExcursions
4	7	6	7	5	8	5	3	7	5	0.798139	1.0000	RandomExcursions
5	8	8	12	5	1	3	4	7	4	0.028817	1.0000	RandomExcursions
5	4	6	6	6	8	4	4	8	6	0.834308	0.9825	RandomExcursions
5	3	6	7	11	7	2	7	2	7	0.090936	0.9825	RandomExcursions
4	5	5	4	7	7	9	5	8	3	0.554420	0.9649	RandomExcursions
5	6	7	7	3	5	6	5	6	7	0.924076	1.0000	RandomExcursionsVariant
6	5	5	6	6	4	6	7	6	6	0.987896	1.0000	RandomExcursionsVariant
5	8	4	3	4	10	3	6	7	7	0.304126	1.0000	RandomExcursionsVariant
6	6	3	4	8	4	8	6	7	5	0.719747	0.9825	RandomExcursionsVariant
7	6	2	5	5	3	10	8	4	7	0.249284	0.9825	RandomExcursionsVariant
8	3	5	7	6	3	5	9	4	7	0.474986	1.0000	RandomExcursionsVariant
8	5	5	5	9	5	9	7	1	3	0.162606	0.9825	RandomExcursionsVariant
7	3	9	7	6	6	4	5	5	5	0.719747	0.9825	RandomExcursionsVariant
6	6	7	5	3	3	5	8	7	7	0.719747	0.9825	RandomExcursionsVariant
9	7	7	4	4	7	2	6	6	5	0.514124	0.9649	RandomExcursionsVariant
4	6	5	7	7	7	2	4	10	5	0.366918	0.9825	RandomExcursionsVariant
4	5	5	6	4	7	5	14	4	3	0.028817	0.9825	RandomExcursionsVariant
2	6	9	4	5	2	5	7	7	10	0.129620	0.9825	RandomExcursionsVariant
3	6	7	4	3	7	5	7	9	6	0.554420	0.9825	RandomExcursionsVariant
5	5	5	7	6	5	6	4	8	6	0.946308	1.0000	RandomExcursionsVariant
7	5	5	5	9	1	9	5	6	5	0.304126	1.0000	RandomExcursionsVariant
7	3	6	10	3	6	1	7	9	5	0.090936	1.0000	RandomExcursionsVariant
5	5	7	7	7	2	2	6	8	8	0.366918	1.0000	RandomExcursionsVariant
12	9	5	6	13	13	10	12	10	10	0.657933	0.9900	Serial
12	15	8	11	10	8	6	10	11	9	0.779188	0.9900	Serial
13	9	10	14	9	3	14	9	10	9	0.401199	0.9900	LinearComplexity

- -

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 0.960150 for a sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately 0.950463 for a sample size = 57 binary sequences.

For further guidelines construct a probability table using the MAPLE program provided in the addendum section of the documentation.

- -

Додаток М

Результати тестування псевдовипадкової послідовності, отриманої при реалізації методу захисту інформації на основі розширених матричних операцій криптографічного перетворення

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <R_KOD_2.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
12	13	7	8	8	4	12	13	15	8	0.289667	0.9900	Frequency
8	8	12	11	7	14	12	10	7	11	0.816537	1.0000	BlockFrequency
11	17	5	8	6	11	8	14	8	12	0.191687	1.0000	CumulativeSums
12	8	11	12	9	9	10	8	9	12	0.983453	1.0000	CumulativeSums
14	6	10	11	14	10	12	10	6	7	0.554420	0.9900	Runs
12	9	9	15	4	14	14	8	10	5	0.171867	0.9900	LongestRun
6	11	11	12	11	9	6	14	13	7	0.595549	1.0000	Rank
3	3	11	9	14	14	13	8	14	11	0.062821	0.9900	FFT
17	14	12	8	9	6	8	5	12	9	0.191687	0.9700	NonOverlappingTemplate
14	9	13	11	9	10	5	11	7	11	0.699313	1.0000	NonOverlappingTemplate
12	11	9	7	12	13	12	5	8	11	0.719747	1.0000	NonOverlappingTemplate
8	11	10	9	15	7	7	15	13	5	0.289667	0.9800	NonOverlappingTemplate
12	15	11	8	2	12	6	9	12	13	0.153763	0.9800	NonOverlappingTemplate
10	7	13	14	3	10	12	8	13	10	0.350485	1.0000	NonOverlappingTemplate
11	11	14	9	11	12	11	10	8	3	0.554420	1.0000	NonOverlappingTemplate
7	11	11	12	9	14	11	7	8	10	0.867692	0.9900	NonOverlappingTemplate
13	5	7	14	10	7	7	10	17	10	0.181557	0.9900	NonOverlappingTemplate
13	13	11	12	9	6	12	12	5	7	0.514124	1.0000	NonOverlappingTemplate
10	12	11	8	8	7	8	10	14	12	0.867692	0.9800	NonOverlappingTemplate
11	10	7	10	17	8	8	11	10	8	0.616305	0.9900	NonOverlappingTemplate
11	13	8	10	7	12	7	12	13	7	0.759756	1.0000	NonOverlappingTemplate
8	9	14	14	11	8	10	8	7	11	0.779188	0.9900	NonOverlappingTemplate
14	12	10	6	8	6	12	10	10	12	0.699313	0.9700	NonOverlappingTemplate
10	12	8	15	9	4	11	12	7	12	0.455937	0.9800	NonOverlappingTemplate
8	5	12	10	12	9	10	11	13	10	0.851383	0.9900	NonOverlappingTemplate
8	9	13	12	10	14	11	5	8	10	0.699313	0.9900	NonOverlappingTemplate
11	11	13	10	10	8	11	9	11	6	0.946308	0.9900	NonOverlappingTemplate
10	9	7	12	10	12	9	8	11	12	0.971699	1.0000	NonOverlappingTemplate
14	14	8	10	9	6	7	10	11	11	0.699313	0.9900	NonOverlappingTemplate
12	6	9	10	11	10	10	9	9	14	0.911413	0.9900	NonOverlappingTemplate
9	5	10	11	11	13	14	8	6	13	0.514124	0.9800	NonOverlappingTemplate
6	9	15	6	10	7	10	17	8	12	0.191687	0.9900	NonOverlappingTemplate
12	10	6	13	4	12	6	12	15	10	0.249284	0.9800	NonOverlappingTemplate
7	11	14	14	8	8	12	9	10	7	0.699313	1.0000	NonOverlappingTemplate
9	12	7	12	10	9	13	9	6	13	0.798139	0.9900	NonOverlappingTemplate
13	13	9	10	7	11	16	8	3	10	0.224821	0.9900	NonOverlappingTemplate
11	11	7	12	10	12	7	14	7	9	0.798139	0.9800	NonOverlappingTemplate
4	8	9	12	9	13	15	11	9	10	0.514124	1.0000	NonOverlappingTemplate
7	9	18	8	9	11	5	13	11	9	0.236810	0.9900	NonOverlappingTemplate
8	8	7	10	14	12	8	15	9	9	0.657933	1.0000	NonOverlappingTemplate
12	6	12	11	8	10	13	11	9	8	0.883171	0.9800	NonOverlappingTemplate
6	13	9	8	17	15	11	6	8	7	0.145326	0.9800	NonOverlappingTemplate
9	9	11	10	9	12	13	12	5	10	0.867692	0.9900	NonOverlappingTemplate
15	14	5	9	8	5	15	13	5	11	0.075719	0.9700	NonOverlappingTemplate
14	9	4	12	8	9	11	12	9	12	0.616305	0.9900	NonOverlappingTemplate
7	10	11	5	15	8	17	9	6	12	0.145326	0.9900	NonOverlappingTemplate
17	9	11	4	7	10	11	11	10	10	0.366918	1.0000	NonOverlappingTemplate
8	8	6	11	13	14	9	7	12	12	0.657933	1.0000	NonOverlappingTemplate
10	15	12	12	3	4	9	13	10	12	0.153763	0.9800	NonOverlappingTemplate
10	14	8	7	12	6	15	5	14	9	0.236810	0.9900	NonOverlappingTemplate
10	10	14	11	10	16	9	6	6	8	0.437274	0.9900	NonOverlappingTemplate
9	8	14	7	15	6	15	6	10	10	0.262249	0.9900	NonOverlappingTemplate
8	11	11	11	14	13	4	11	5	12	0.366918	0.9800	NonOverlappingTemplate
12	11	12	6	7	8	14	8	12	10	0.719747	0.9900	NonOverlappingTemplate
11	9	11	15	11	6	11	9	7	10	0.779188	0.9800	NonOverlappingTemplate
8	9	12	9	11	13	8	11	8	11	0.964295	1.0000	NonOverlappingTemplate
12	11	8	9	16	10	14	4	8	8	0.304126	1.0000	NonOverlappingTemplate
8	8	13	9	10	15	14	9	10	4	0.383827	1.0000	NonOverlappingTemplate

12	5	8	12	8	7	10	13	13	12	0.616305	1.0000	NonOverlappingTemplate
11	14	10	12	11	11	7	5	12	7	0.637119	1.0000	NonOverlappingTemplate
10	14	12	10	9	11	7	6	14	7	0.616305	0.9900	NonOverlappingTemplate
11	12	13	7	9	14	12	10	9	3	0.401199	0.9900	NonOverlappingTemplate
12	7	9	9	10	6	13	14	8	12	0.699313	0.9800	NonOverlappingTemplate
6	15	6	11	9	13	15	10	10	5	0.224821	0.9900	NonOverlappingTemplate
13	11	14	8	10	10	9	9	9	7	0.897763	1.0000	NonOverlappingTemplate
10	11	12	9	7	12	10	12	9	8	0.971699	0.9800	NonOverlappingTemplate
9	11	10	11	5	13	15	7	9	10	0.616305	0.9900	NonOverlappingTemplate
10	10	14	11	7	10	7	8	14	9	0.779188	1.0000	NonOverlappingTemplate
10	9	12	16	13	8	8	8	11	5	0.455937	0.9900	NonOverlappingTemplate
12	7	10	15	9	9	14	7	10	7	0.595549	1.0000	NonOverlappingTemplate
11	9	9	16	8	3	7	8	16	13	0.090936	1.0000	NonOverlappingTemplate
7	11	13	7	16	12	11	11	7	5	0.319084	1.0000	NonOverlappingTemplate
11	10	13	12	9	8	7	6	14	10	0.739918	1.0000	NonOverlappingTemplate
9	17	9	7	15	11	8	5	12	7	0.171867	1.0000	NonOverlappingTemplate
13	10	8	14	7	4	10	13	11	10	0.494392	0.9900	NonOverlappingTemplate
13	9	11	6	13	13	12	9	6	8	0.637119	0.9900	NonOverlappingTemplate
6	11	8	9	10	9	10	15	10	12	0.816537	0.9700	NonOverlappingTemplate
8	17	6	7	11	7	12	12	7	13	0.249284	0.9800	NonOverlappingTemplate
13	12	7	6	12	10	4	11	7	18	0.085587	0.9800	NonOverlappingTemplate
10	10	9	10	6	7	11	15	9	13	0.719747	0.9700	NonOverlappingTemplate
9	4	8	9	12	13	13	10	11	11	0.678686	0.9900	NonOverlappingTemplate
12	11	10	15	8	10	8	9	7	10	0.851383	0.9900	NonOverlappingTemplate
17	14	12	8	9	6	8	5	12	9	0.191687	0.9700	NonOverlappingTemplate
6	10	11	13	11	10	10	9	10	10	0.971699	1.0000	NonOverlappingTemplate
12	9	12	11	9	12	6	7	8	14	0.739918	0.9700	NonOverlappingTemplate
11	13	2	10	12	7	10	11	9	15	0.249284	0.9800	NonOverlappingTemplate
11	13	5	10	10	11	13	8	9	10	0.834308	0.9900	NonOverlappingTemplate
9	9	11	12	9	8	14	9	9	10	0.964295	1.0000	NonOverlappingTemplate
4	7	11	10	12	14	12	10	8	12	0.554420	1.0000	NonOverlappingTemplate
14	11	9	12	7	10	9	7	10	11	0.897763	0.9900	NonOverlappingTemplate
5	11	6	11	7	9	15	13	12	11	0.419021	0.9900	NonOverlappingTemplate
11	8	6	14	3	9	12	9	13	15	0.181557	1.0000	NonOverlappingTemplate
7	12	8	14	11	5	10	10	12	11	0.699313	0.9900	NonOverlappingTemplate
18	9	14	10	9	6	8	9	8	9	0.289667	0.9900	NonOverlappingTemplate
11	14	12	5	10	14	6	8	10	10	0.514124	1.0000	NonOverlappingTemplate
10	7	16	8	10	11	16	8	7	7	0.289667	0.9900	NonOverlappingTemplate
9	9	19	5	8	11	12	10	9	8	0.202268	0.9800	NonOverlappingTemplate
12	10	12	10	9	7	15	12	4	9	0.494392	0.9900	NonOverlappingTemplate
8	10	12	6	11	12	13	7	14	7	0.616305	1.0000	NonOverlappingTemplate
10	9	13	15	8	9	7	10	8	11	0.798139	0.9900	NonOverlappingTemplate
14	7	8	7	6	13	9	16	9	11	0.334538	0.9800	NonOverlappingTemplate
8	12	9	18	11	8	11	11	2	10	0.108791	0.9900	NonOverlappingTemplate
12	8	11	12	11	9	4	11	12	10	0.779188	0.9900	NonOverlappingTemplate
10	16	12	7	6	8	10	9	10	12	0.595549	0.9900	NonOverlappingTemplate
10	8	12	9	11	14	10	8	7	11	0.911413	0.9900	NonOverlappingTemplate
13	12	10	5	13	8	11	7	10	11	0.719747	0.9900	NonOverlappingTemplate
9	10	8	12	6	14	6	15	12	8	0.437274	0.9700	NonOverlappingTemplate
12	7	8	11	10	11	8	14	12	7	0.816537	0.9800	NonOverlappingTemplate
14	11	8	4	10	8	11	10	14	10	0.554420	0.9900	NonOverlappingTemplate
10	7	12	12	5	16	12	10	13	3	0.122325	0.9800	NonOverlappingTemplate
11	9	12	10	10	13	10	9	10	6	0.955835	0.9800	NonOverlappingTemplate
12	11	11	12	9	7	18	10	6	4	0.137282	0.9900	NonOverlappingTemplate
4	14	5	11	16	11	9	8	17	5	0.021999	1.0000	NonOverlappingTemplate
9	6	5	10	9	11	14	17	13	6	0.145326	0.9900	NonOverlappingTemplate
11	9	3	8	6	12	10	20	11	10	0.040108	0.9900	NonOverlappingTemplate
5	6	11	8	10	10	10	18	13	9	0.213309	1.0000	NonOverlappingTemplate
4	12	12	13	8	6	8	15	11	11	0.319084	1.0000	NonOverlappingTemplate
12	11	9	10	12	13	6	10	10	7	0.883171	0.9800	NonOverlappingTemplate
18	14	9	9	12	9	12	4	5	8	0.075719	0.9800	NonOverlappingTemplate
5	11	15	7	10	9	14	14	9	6	0.275709	1.0000	NonOverlappingTemplate
13	12	15	4	10	12	9	8	8	9	0.455937	0.9800	NonOverlappingTemplate
15	9	8	11	14	6	7	10	10	10	0.616305	0.9800	NonOverlappingTemplate
9	5	10	6	21	16	9	9	9	6	0.009535	0.9900	NonOverlappingTemplate
16	16	11	10	11	5	7	7	4	13	0.062821	0.9900	NonOverlappingTemplate
12	15	9	8	8	6	7	8	15	12	0.383827	1.0000	NonOverlappingTemplate
11	16	9	9	5	8	11	15	9	7	0.319084	0.9700	NonOverlappingTemplate
10	9	13	13	9	9	11	6	8	12	0.867692	0.9900	NonOverlappingTemplate
9	9	11	8	11	11	12	10	9	10	0.997823	1.0000	NonOverlappingTemplate
12	8	12	10	10	12	8	13	9	6	0.867692	1.0000	NonOverlappingTemplate

11	9	13	7	10	17	7	7	7	12	0.350485	0.9800	NonOverlappingTemplate
13	7	11	8	7	10	15	7	14	8	0.474986	0.9700	NonOverlappingTemplate
17	15	11	9	12	8	9	12	2	5	0.037566	0.9900	NonOverlappingTemplate
6	8	9	14	5	16	9	16	12	5	0.058984	1.0000	NonOverlappingTemplate
10	13	11	13	9	9	9	6	10	10	0.924076	0.9900	NonOverlappingTemplate
9	9	10	8	10	12	9	6	14	13	0.816537	0.9900	NonOverlappingTemplate
14	9	11	13	9	8	9	10	10	7	0.897763	0.9800	NonOverlappingTemplate
13	9	7	14	12	9	7	13	4	12	0.366918	0.9900	NonOverlappingTemplate
12	16	9	11	9	7	4	14	7	11	0.249284	1.0000	NonOverlappingTemplate
9	9	9	14	13	8	8	9	6	15	0.554420	0.9900	NonOverlappingTemplate
15	9	9	10	11	8	15	9	8	6	0.554420	0.9900	NonOverlappingTemplate
9	7	9	14	13	10	10	16	5	7	0.304126	1.0000	NonOverlappingTemplate
6	11	9	9	11	10	10	10	9	15	0.867692	1.0000	NonOverlappingTemplate
9	11	14	12	5	11	11	15	6	6	0.304126	1.0000	NonOverlappingTemplate
9	13	12	13	11	10	6	6	8	12	0.699313	0.9900	NonOverlappingTemplate
9	12	8	11	6	9	15	12	11	7	0.678686	0.9800	NonOverlappingTemplate
15	10	12	13	7	6	8	3	14	12	0.137282	0.9900	NonOverlappingTemplate
17	7	7	11	10	10	13	10	4	11	0.249284	0.9900	NonOverlappingTemplate
13	6	12	9	9	9	9	12	11	10	0.924076	1.0000	NonOverlappingTemplate
6	10	5	12	11	13	10	6	11	16	0.289667	1.0000	NonOverlappingTemplate
11	5	9	14	7	14	9	14	7	10	0.401199	0.9900	NonOverlappingTemplate
7	15	8	15	3	9	10	11	9	13	0.191687	1.0000	NonOverlappingTemplate
12	11	12	6	14	12	6	10	9	8	0.678686	0.9800	NonOverlappingTemplate
6	11	9	12	10	14	6	8	9	15	0.494392	0.9900	NonOverlappingTemplate
10	8	13	10	9	12	11	12	8	7	0.935716	0.9900	NonOverlappingTemplate
11	16	10	5	7	17	6	10	6	12	0.075719	1.0000	NonOverlappingTemplate
12	11	10	15	7	11	8	9	7	10	0.798139	0.9900	NonOverlappingTemplate
8	8	10	9	15	16	10	7	12	5	0.289667	1.0000	OverlappingTemplate
7	11	16	10	11	8	9	7	12	9	0.678686	0.9900	Universal
9	10	5	12	14	13	6	9	11	11	0.595549	0.9900	ApproximateEntropy
7	4	5	9	8	2	7	11	5	6	0.324180	0.9688	RandomExcursions
4	7	6	2	6	11	9	11	3	5	0.090936	1.0000	RandomExcursions
3	9	5	9	2	7	7	8	6	8	0.437274	1.0000	RandomExcursions
3	10	11	4	7	10	6	5	2	6	0.100508	0.9844	RandomExcursions
5	7	4	11	8	5	9	7	5	3	0.407091	0.9844	RandomExcursions
8	6	6	5	8	6	2	8	6	9	0.706149	0.9844	RandomExcursions
12	5	6	5	7	8	4	8	3	6	0.350485	0.9688	RandomExcursions
3	11	6	4	3	9	8	3	11	6	0.074177	0.9844	RandomExcursions
8	7	10	7	5	7	2	5	8	5	0.568055	0.9688	RandomExcursionsVariant
7	8	8	6	8	4	4	6	4	9	0.772760	0.9844	RandomExcursionsVariant
7	8	7	6	3	6	6	8	7	6	0.949602	1.0000	RandomExcursionsVariant
7	10	4	4	5	6	5	12	4	7	0.253551	1.0000	RandomExcursionsVariant
9	3	7	5	6	8	7	4	7	8	0.772760	1.0000	RandomExcursionsVariant
10	4	4	10	6	9	5	5	8	3	0.299251	0.9844	RandomExcursionsVariant
6	7	7	13	4	7	4	7	4	5	0.275709	0.9844	RandomExcursionsVariant
6	6	10	8	10	4	5	2	8	5	0.324180	0.9844	RandomExcursionsVariant
8	7	6	7	6	5	8	10	5	2	0.602458	0.9844	RandomExcursionsVariant
7	10	9	5	6	5	5	6	4	7	0.772760	1.0000	RandomExcursionsVariant
7	11	7	6	5	2	6	4	11	5	0.195163	1.0000	RandomExcursionsVariant
12	3	6	7	6	6	7	2	7	8	0.253551	0.9844	RandomExcursionsVariant
10	6	7	9	3	4	4	4	7	10	0.299251	0.9844	RandomExcursionsVariant
12	6	8	2	6	6	10	5	8	1	0.048716	0.9844	RandomExcursionsVariant
9	9	4	9	7	3	9	5	5	4	0.407091	1.0000	RandomExcursionsVariant
7	8	8	10	4	5	6	7	4	5	0.739918	1.0000	RandomExcursionsVariant
9	3	10	8	6	8	5	5	5	5	0.568055	1.0000	RandomExcursionsVariant
8	4	10	7	8	3	6	5	9	4	0.468595	1.0000	RandomExcursionsVariant
9	9	10	11	10	6	11	10	10	14	0.935716	0.9900	Serial
13	8	9	7	9	11	7	8	14	14	0.637119	0.9900	Serial
13	10	7	12	12	12	9	5	13	7	0.595549	0.9700	LinearComplexity

- -

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 0.960150 for a sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately 0.952688 for a sample size = 64 binary sequences.

For further guidelines construct a probability table using the MAPLE program provided in the addendum section of the documentation.

- -

Додаток Н

Результати тестування даних за модифікованим алгоритмом розширеного матричного кодування текстового файлу

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <KOD_TX2.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
9	12	8	10	10	13	12	11	7	8	0.935716	1.0000	Frequency
15	4	10	11	9	11	14	5	8	13	0.224821	1.0000	BlockFrequency
7	10	8	15	13	11	4	8	13	11	0.366918	1.0000	CumulativeSums
10	12	9	10	9	13	7	10	10	10	0.983453	0.9900	CumulativeSums
14	5	9	12	19	10	6	9	5	11	0.048716	0.9900	Runs
11	13	9	11	8	8	10	12	9	9	0.978072	0.9800	LongestRun
8	10	9	7	13	11	12	13	12	5	0.678686	0.9900	Rank
1	10	6	11	8	7	16	14	12	15	0.023545	1.0000	FFT
9	11	11	10	10	7	12	12	8	10	0.983453	0.9800	NonOverlappingTemplate
9	14	5	11	10	9	6	7	14	15	0.275709	0.9900	NonOverlappingTemplate
8	13	8	9	12	11	13	9	8	9	0.924076	0.9800	NonOverlappingTemplate
12	11	11	8	7	12	9	8	11	11	0.964295	1.0000	NonOverlappingTemplate
15	8	11	6	8	12	10	12	7	11	0.657933	0.9900	NonOverlappingTemplate
12	12	15	9	10	6	5	14	7	10	0.350485	0.9700	NonOverlappingTemplate
17	11	6	15	6	4	4	12	13	12	0.020548	0.9900	NonOverlappingTemplate
13	16	6	5	12	4	16	9	9	10	0.058984	0.9900	NonOverlappingTemplate
9	10	15	9	14	7	8	8	10	10	0.739918	0.9900	NonOverlappingTemplate
8	11	9	11	6	11	8	15	12	9	0.759756	1.0000	NonOverlappingTemplate
8	9	13	14	9	8	13	8	9	9	0.834308	1.0000	NonOverlappingTemplate
7	9	11	12	10	11	7	16	8	9	0.678686	0.9800	NonOverlappingTemplate
11	6	12	13	10	11	7	7	10	13	0.759756	0.9700	NonOverlappingTemplate
8	9	10	10	14	6	12	13	8	10	0.798139	0.9900	NonOverlappingTemplate
8	13	11	10	17	7	9	3	16	6	0.042808	0.9800	NonOverlappingTemplate
11	9	12	10	10	10	5	11	13	9	0.897763	0.9800	NonOverlappingTemplate
6	10	8	15	8	9	13	11	12	8	0.657933	1.0000	NonOverlappingTemplate
11	13	11	12	8	3	7	16	13	6	0.129620	1.0000	NonOverlappingTemplate
7	6	9	9	9	13	7	16	11	13	0.419021	0.9900	NonOverlappingTemplate
7	12	10	11	7	12	12	6	13	10	0.779188	1.0000	NonOverlappingTemplate
7	10	12	18	4	13	12	8	6	10	0.102526	1.0000	NonOverlappingTemplate
9	14	9	9	11	9	12	7	9	11	0.935716	0.9800	NonOverlappingTemplate
7	13	9	8	5	11	10	9	17	11	0.350485	0.9900	NonOverlappingTemplate
11	12	10	13	8	12	8	8	6	12	0.834308	0.9900	NonOverlappingTemplate
9	7	6	12	8	16	7	14	12	9	0.350485	0.9800	NonOverlappingTemplate
10	8	10	8	5	9	10	13	8	19	0.171867	0.9800	NonOverlappingTemplate
11	9	9	7	8	9	15	7	13	12	0.699313	1.0000	NonOverlappingTemplate
7	11	19	9	12	7	9	8	9	9	0.262249	1.0000	NonOverlappingTemplate
8	7	9	13	7	10	7	14	10	15	0.514124	1.0000	NonOverlappingTemplate
9	10	13	9	9	12	7	14	11	6	0.759756	0.9700	NonOverlappingTemplate
11	10	12	8	8	7	13	14	12	5	0.574903	1.0000	NonOverlappingTemplate
9	7	9	6	17	11	10	9	7	15	0.262249	0.9900	NonOverlappingTemplate
9	12	5	6	11	12	14	9	12	10	0.616305	0.9900	NonOverlappingTemplate
9	15	8	9	10	10	11	8	11	9	0.924076	0.9900	NonOverlappingTemplate
7	13	7	5	11	12	10	15	11	9	0.494392	0.9800	NonOverlappingTemplate
8	8	11	14	8	6	11	12	11	11	0.816537	0.9900	NonOverlappingTemplate
12	12	7	8	10	10	9	11	10	11	0.983453	0.9900	NonOverlappingTemplate
7	6	17	9	7	11	8	14	12	9	0.275709	1.0000	NonOverlappingTemplate
8	15	11	6	11	7	10	13	9	10	0.678686	1.0000	NonOverlappingTemplate
10	13	8	15	10	7	10	12	3	12	0.319084	0.9900	NonOverlappingTemplate
10	10	12	11	7	8	9	12	12	9	0.971699	0.9900	NonOverlappingTemplate
5	10	8	8	11	14	12	3	15	14	0.108791	0.9800	NonOverlappingTemplate
13	13	4	16	10	11	8	8	6	11	0.236810	0.9800	NonOverlappingTemplate
14	11	10	7	16	8	9	6	12	7	0.383827	0.9800	NonOverlappingTemplate
14	5	9	9	8	17	8	7	13	10	0.224821	1.0000	NonOverlappingTemplate
13	8	6	12	7	6	9	15	11	13	0.401199	0.9900	NonOverlappingTemplate
9	6	11	10	8	10	10	10	10	16	0.759756	1.0000	NonOverlappingTemplate
12	6	7	14	7	15	11	7	10	11	0.437274	0.9700	NonOverlappingTemplate
8	12	13	10	16	2	14	9	9	7	0.108791	0.9800	NonOverlappingTemplate
4	14	9	10	5	8	14	17	10	9	0.096578	0.9900	NonOverlappingTemplate
12	14	13	8	8	10	10	10	10	5	0.719747	1.0000	NonOverlappingTemplate

10	15	11	17	6	9	8	12	6	6	0.153763	0.9800	NonOverlappingTemplate
13	8	12	12	7	13	14	8	5	8	0.455937	0.9800	NonOverlappingTemplate
8	8	11	13	12	7	15	6	10	10	0.616305	1.0000	NonOverlappingTemplate
8	9	9	6	11	15	10	11	10	11	0.834308	1.0000	NonOverlappingTemplate
14	14	7	6	13	13	5	8	5	15	0.080519	0.9900	NonOverlappingTemplate
8	12	10	9	9	13	5	11	10	13	0.798139	1.0000	NonOverlappingTemplate
9	12	5	10	10	14	13	8	10	9	0.739918	1.0000	NonOverlappingTemplate
9	8	15	11	10	10	11	8	7	11	0.867692	0.9900	NonOverlappingTemplate
10	9	11	17	6	8	7	7	14	11	0.304126	0.9900	NonOverlappingTemplate
11	6	12	14	7	12	13	5	10	10	0.494392	0.9800	NonOverlappingTemplate
14	10	12	8	6	12	8	8	11	11	0.798139	1.0000	NonOverlappingTemplate
5	13	8	7	10	12	12	10	10	13	0.699313	1.0000	NonOverlappingTemplate
19	5	10	11	8	6	13	14	5	9	0.037566	0.9600	NonOverlappingTemplate
5	10	8	9	10	13	12	10	10	13	0.816537	0.9800	NonOverlappingTemplate
10	10	8	11	11	13	14	9	5	9	0.759756	0.9900	NonOverlappingTemplate
9	12	9	14	7	10	8	10	13	8	0.851383	0.9800	NonOverlappingTemplate
6	12	5	9	12	14	10	9	10	13	0.574903	1.0000	NonOverlappingTemplate
9	6	14	11	9	8	8	17	10	8	0.383827	0.9700	NonOverlappingTemplate
14	11	10	10	11	11	5	13	9	6	0.637119	0.9900	NonOverlappingTemplate
10	11	13	11	8	10	9	11	8	9	0.987896	0.9900	NonOverlappingTemplate
12	10	6	12	10	6	12	12	7	13	0.678686	0.9600	NonOverlappingTemplate
5	15	14	11	6	14	10	9	4	12	0.122325	1.0000	NonOverlappingTemplate
9	12	13	11	12	9	7	11	8	8	0.924076	1.0000	NonOverlappingTemplate
9	11	10	11	10	7	12	12	8	10	0.983453	0.9800	NonOverlappingTemplate
13	12	10	9	11	8	8	14	11	4	0.574903	0.9900	NonOverlappingTemplate
10	9	10	8	13	11	8	10	8	13	0.955835	0.9900	NonOverlappingTemplate
10	13	11	10	8	13	3	10	10	12	0.574903	0.9900	NonOverlappingTemplate
11	9	11	11	14	4	8	8	12	12	0.616305	0.9800	NonOverlappingTemplate
8	14	10	7	9	9	13	9	14	7	0.678686	1.0000	NonOverlappingTemplate
11	5	12	12	9	10	11	7	14	9	0.719747	0.9700	NonOverlappingTemplate
6	13	16	10	14	10	7	6	8	10	0.304126	0.9900	NonOverlappingTemplate
13	11	13	9	9	9	4	9	10	13	0.657933	1.0000	NonOverlappingTemplate
17	16	8	8	8	9	7	9	4	14	0.066882	0.9900	NonOverlappingTemplate
15	4	14	9	11	11	6	10	9	11	0.366918	1.0000	NonOverlappingTemplate
10	10	14	6	9	13	7	14	6	11	0.494392	0.9900	NonOverlappingTemplate
18	11	8	12	9	6	10	14	2	10	0.048716	0.9700	NonOverlappingTemplate
12	9	8	8	15	12	6	11	12	7	0.616305	0.9800	NonOverlappingTemplate
12	8	8	10	6	19	8	6	12	11	0.145326	0.9800	NonOverlappingTemplate
9	10	15	9	9	6	7	10	12	13	0.678686	1.0000	NonOverlappingTemplate
8	4	11	14	16	12	7	13	6	9	0.153763	0.9800	NonOverlappingTemplate
12	8	9	17	9	9	7	5	14	10	0.275709	0.9800	NonOverlappingTemplate
7	10	16	10	10	7	10	7	8	15	0.419021	0.9900	NonOverlappingTemplate
7	8	14	13	11	13	5	14	9	6	0.304126	1.0000	NonOverlappingTemplate
9	16	8	7	8	12	12	6	13	9	0.455937	0.9900	NonOverlappingTemplate
12	9	5	14	7	9	13	9	15	7	0.350485	1.0000	NonOverlappingTemplate
9	12	12	9	8	11	10	7	12	10	0.971699	0.9900	NonOverlappingTemplate
11	11	8	7	11	12	10	5	10	15	0.637119	0.9800	NonOverlappingTemplate
6	5	8	14	9	12	10	17	7	12	0.171867	1.0000	NonOverlappingTemplate
17	13	7	9	3	2	17	12	4	16	0.000347	0.9800	NonOverlappingTemplate
14	3	9	10	12	8	11	15	9	9	0.334538	0.9800	NonOverlappingTemplate
14	8	7	7	13	9	11	11	8	12	0.759756	0.9700	NonOverlappingTemplate
7	14	7	12	8	8	12	14	10	8	0.637119	0.9900	NonOverlappingTemplate
10	10	3	17	17	6	14	5	8	10	0.013569	0.9800	NonOverlappingTemplate
8	13	9	14	8	8	8	11	11	10	0.883171	0.9900	NonOverlappingTemplate
7	9	18	7	8	13	9	9	12	8	0.304126	0.9900	NonOverlappingTemplate
17	5	14	6	12	12	12	6	8	8	0.115387	0.9600	NonOverlappingTemplate
12	9	10	12	15	11	8	10	4	9	0.574903	1.0000	NonOverlappingTemplate
3	12	10	11	15	9	12	9	12	7	0.366918	1.0000	NonOverlappingTemplate
15	6	8	12	12	9	8	14	8	8	0.514124	0.9600	NonOverlappingTemplate
10	8	14	6	8	9	12	13	8	12	0.719747	1.0000	NonOverlappingTemplate
10	9	16	8	9	12	5	11	12	8	0.534146	0.9900	NonOverlappingTemplate
11	5	10	11	12	5	9	11	11	15	0.494392	0.9900	NonOverlappingTemplate
9	14	11	13	8	11	13	6	8	7	0.637119	1.0000	NonOverlappingTemplate
10	9	8	8	11	10	9	21	9	5	0.071177	0.9900	NonOverlappingTemplate
12	10	8	5	15	6	11	10	11	12	0.534146	0.9900	NonOverlappingTemplate
10	9	10	7	14	7	10	7	11	15	0.637119	0.9900	NonOverlappingTemplate
11	13	13	6	13	9	10	7	10	8	0.759756	0.9900	NonOverlappingTemplate
9	11	12	6	8	12	10	13	6	13	0.699313	0.9900	NonOverlappingTemplate
11	11	9	11	8	9	16	11	6	8	0.678686	0.9900	NonOverlappingTemplate
14	5	12	7	11	8	14	9	8	12	0.494392	1.0000	NonOverlappingTemplate
7	13	8	16	15	5	8	10	10	8	0.236810	0.9900	NonOverlappingTemplate

12	12	7	7	7	12	11	10	13	9	0.834308	0.9900	NonOverlappingTemplate
7	8	11	4	16	9	9	14	14	8	0.191687	0.9900	NonOverlappingTemplate
7	14	7	9	13	12	9	13	7	9	0.657933	1.0000	NonOverlappingTemplate
5	10	11	9	14	15	8	10	8	10	0.574903	1.0000	NonOverlappingTemplate
7	12	13	11	7	5	14	7	8	16	0.202268	1.0000	NonOverlappingTemplate
8	14	12	12	7	7	8	11	8	13	0.699313	0.9800	NonOverlappingTemplate
9	8	8	6	13	13	14	10	6	13	0.494392	0.9900	NonOverlappingTemplate
11	14	8	7	8	14	9	7	8	14	0.534146	0.9900	NonOverlappingTemplate
11	8	7	9	12	9	11	11	7	15	0.779188	0.9900	NonOverlappingTemplate
10	12	5	10	12	10	18	10	8	5	0.181557	0.9900	NonOverlappingTemplate
13	8	7	8	9	13	12	9	9	12	0.867692	0.9800	NonOverlappingTemplate
12	8	10	11	13	14	11	4	6	11	0.455937	0.9800	NonOverlappingTemplate
12	13	13	5	10	10	11	8	9	9	0.798139	1.0000	NonOverlappingTemplate
8	12	15	7	6	6	10	13	12	11	0.455937	0.9900	NonOverlappingTemplate
6	12	5	10	12	11	4	15	14	11	0.171867	1.0000	NonOverlappingTemplate
13	9	8	11	11	10	13	6	7	12	0.798139	0.9900	NonOverlappingTemplate
11	8	11	8	13	10	13	10	7	9	0.924076	0.9900	NonOverlappingTemplate
11	3	13	13	12	6	11	12	7	12	0.304126	1.0000	NonOverlappingTemplate
8	15	11	5	15	10	12	7	9	8	0.366918	0.9900	NonOverlappingTemplate
9	8	11	16	7	13	8	10	10	8	0.657933	0.9900	NonOverlappingTemplate
8	12	13	17	2	8	14	7	10	9	0.066882	0.9900	NonOverlappingTemplate
11	15	8	11	9	11	9	6	10	10	0.834308	0.9800	NonOverlappingTemplate
12	14	13	7	9	6	11	10	7	11	0.678686	0.9900	NonOverlappingTemplate
14	15	7	15	15	9	3	8	10	4	0.025193	1.0000	NonOverlappingTemplate
7	15	11	8	9	10	14	8	8	10	0.699313	1.0000	NonOverlappingTemplate
10	11	12	12	12	9	7	11	8	8	0.955835	1.0000	NonOverlappingTemplate
6	6	11	15	10	8	15	6	12	11	0.289667	0.9900	OverlappingTemplate
11	10	13	8	10	12	6	9	12	9	0.911413	1.0000	Universal
15	10	13	12	8	5	8	13	7	9	0.437274	1.0000	ApproximateEntropy
9	9	5	9	4	7	7	5	2	5	0.468595	0.9677	RandomExcursions
3	4	4	7	14	8	6	4	6	6	0.090936	0.9839	RandomExcursions
7	5	4	11	11	4	2	5	4	9	0.090936	1.0000	RandomExcursions
1	5	5	11	8	7	8	4	4	9	0.162606	1.0000	RandomExcursions
6	3	3	8	6	9	8	3	10	6	0.350485	0.9839	RandomExcursions
11	7	5	0	9	0	7	7	7	9	0.017912	0.9677	RandomExcursions
9	2	7	6	6	6	11	1	8	6	0.148094	0.9839	RandomExcursions
7	6	6	5	5	7	5	7	7	7	0.998205	1.0000	RandomExcursions
6	7	6	4	5	5	6	11	7	5	0.772760	0.9839	RandomExcursionsVariant
7	3	8	5	6	6	1	11	6	9	0.195163	0.9839	RandomExcursionsVariant
6	6	9	6	4	4	9	6	5	7	0.862344	0.9839	RandomExcursionsVariant
7	7	6	4	12	6	4	5	7	4	0.468595	0.9839	RandomExcursionsVariant
11	3	4	11	7	6	7	5	3	5	0.178278	0.9677	RandomExcursionsVariant
8	7	6	6	7	6	6	6	6	4	0.995711	0.9839	RandomExcursionsVariant
9	7	2	5	7	5	8	5	3	11	0.253551	1.0000	RandomExcursionsVariant
9	3	6	5	3	11	7	3	8	7	0.253551	0.9839	RandomExcursionsVariant
4	7	9	5	6	2	11	3	8	7	0.232760	1.0000	RandomExcursionsVariant
4	9	7	6	4	6	7	4	9	6	0.804337	0.9677	RandomExcursionsVariant
6	4	6	6	13	7	8	3	5	4	0.213309	0.9839	RandomExcursionsVariant
7	5	5	8	7	5	7	6	8	4	0.964295	0.9839	RandomExcursionsVariant
7	3	7	7	6	5	6	4	9	8	0.834308	0.9839	RandomExcursionsVariant
5	5	7	9	4	4	8	6	7	7	0.888137	1.0000	RandomExcursionsVariant
4	4	8	5	10	4	4	5	10	8	0.378138	1.0000	RandomExcursionsVariant
6	3	5	8	4	10	5	7	6	8	0.671779	1.0000	RandomExcursionsVariant
6	2	4	8	7	8	7	9	7	4	0.602458	1.0000	RandomExcursionsVariant
6	1	8	3	8	7	15	5	3	6	0.007880	1.0000	RandomExcursionsVariant
6	6	12	8	12	10	8	10	10	18	0.262249	1.0000	Serial
10	6	10	12	14	9	5	8	12	14	0.474986	1.0000	Serial
8	11	7	14	5	5	11	13	18	8	0.071177	1.0000	LinearComplexity

- -

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 0.960150 for a sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately 0.952091 for a sample size = 62 binary sequences.

For further guidelines construct a probability table using the MAPLE program provided in the addendum section of the documentation.

- -