ВІДГУК

офіційного опонента на дисертаційну роботу

Фауре Еміля Віталійовича

«Методологія захисту інформації на основі факторіального кодування даних»,

представлену на здобуття наукового ступеня

доктора технічних наук

за спеціальністю 05.13.21 – системи захисту інформації

Актуальність теми дисертаційної роботи.

Криптосистеми на основі кодових конструкцій з надмірністю, експлуатують перетворення кодових слів повідомлення у кодові слова перешкодостійкого коду з використанням замаскованої матриці, що породжує код з додаванням довільного вектору помилок. Криптографічна стійкість алгоритму ґрунтується на складності декодування повних лінійних кодів (загальна задача декодування є NP-складною) і на даний момент не існує квантового алгоритму її вирішення. Початкова конструкція на основі двійкових кодів Гоппи була запропонована Робертом Мак-Елісом у 1978 році. У подальшому надано декілько модернізацій такої схеми. Для симетричних криптосистем породжуючий багаточлен кода Гоппи задається ключовим словом. Для маскування кодових слів пропонується використання вектору помилок та скорочення коду. Для асиметричних криптосистем пропонується швидкісний алгоритм Нідеррайтера (криптоалгоритм McNie). Рівень безпеки криптосистеми системи McEliece залишається дуже стабільним і стійким незважаючи на безліч теоретичних атак протягом більше 40 років. Автентичні параметри McEliece були спроектовані тільки для рівня безпеки 2^{64}, система легко масштабується до дуже великих параметрів, гарантується захист проти атак з використанням квантових обчислень. Недоліком класичної криптосистеми McEliece є великий розмір ключа. Запропоновані поліпшення, наприклад, застосування 4 квазі-циклічних LRPC кодів над полем призводить до розміру ключа в 2775 біт для 128 бітного рівня безпеки. Криптоалгоритм McNie залишається безпечним проти структурних атак і атак підміни.

Використання блокових лінійних кодів має ряд недоліків: велика складність перетворень при шифруванні та розшифруванні, великий розмір ключових даних (до декількох сотень тисяч бітів), уразливість до нав'язування хибних повідомлень через властивість лінійності кодів. У той час, як у ряді застосувань необхідно забезпечити високу швидкодію крипто алгоритмів, скоротити вимоги до продуктивності обчислювальних засобів, підвищити

показники достовірності, а також зменшити обсяг внесеної надлишковості та збільшити ефективну швидкість передавання інформації. Розв'язання цього протиріччя можливо на основі побудови криптографічних перетворень з факторіальним кодуванням даних. Використання групи перестановки при кодуванні приводить до складності задачі крипто аналізу, що визначається як проблема «слова», що забезпечує стійкість до квантового криптоаналізу.

Дисертаційна робота Фауре Еміля Віталійовича «Методологія захисту інформації на основі факторіального кодування даних» присвячена розробці методології захисту інформації на основі побудови симетричних криптосистем шифрування з використанням надмірних кодів в класі груп перестановок.

Актуальність дисертаційної роботи визначається необхідністю розробки методів захисту інформації стійких до квантового криптоаналізу та підтверджується науково-дослідними роботами «Синтез операцій криптографічного перетворення із заданими характеристиками» (державний реєстраційний номер 0116U008714), держбюджетної науково-дослідної теми «Розробка мобільного високоефективного ультразвукового хірургічного інструменту для військової та цивільної медицини» (державний реєстраційний номер 0117U007474), в яких автор був виконавцем.

Метою дисертаційної роботи є підвищення криптографічної стійкості симетричного шифрування на основі криптосистеми з надмірним факторіальним кодуванням в класі груп перестановок. Для досягнення поставленной мети сформульовано основні задачі дослідження, які в роботі послідовно розв'язано. У результаті це дозволило дисертанту розробити методологію захисту інформації на основі факторіального кодування даних для застосування в блокових симетричних перетвореннях.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Ступінь обґрунтованості нових положень, висновків і рекомендацій у дисертації обумовлена коректністю застосування методів перешкодостійкого кодування, теорії груп перестановки, теорії чисел, теорії графів, теорії ймовірностей і математичної статистики, теорії статистичного та кореляційного аналізу для розробки методів формування випадкової послідовності перестановок на основі використання факторіальної системи числення, роздільного та нероздільного факторіального кодування, математичну модель процесу декодування факторіальних кодів, методів формування псевдовипадкової послідовності на основі лінійного конгруентного методу,

симетричного криптографічного захисту інформації на основі операції гамування, побудови комбінаційного генератора з комбінаційною функцією модульного підсумовування, оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел.

Достовірність основних положень та висновків підтверджено тестуванням розроблених методів на основі застосування програмних засобів.

Ідентичність змісту автореферату й основних положень дисертації

У авторефераті дисертації з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертації. Структура дисертації відповідає вимогам, які ставляться до докторських дисертацій. Дисертаційна робота складається з анотації, вступу, шести розділів, висновків, додатків і списку використаних джерел (355 найменувань). Повний об'єм дисертації складає 477 сторінок, у тому числі 312 сторінок основного тексту. Робота містить 104 таблиці та 80 рисунків.

У першому оглядовому розділі виконано аналіз існуючих підходів, методів і засобів, що реалізують сумісний захист інформації від помилок каналу зв'язку, несанкціонованого доступу та/або модифікації даних, а також методів формування й оцінювання псевдовипадкових послідовностей.

На основі проведеного аналізу сформульовано задачі дисертаційного дослідження.

У другому розділі розроблено метод формування випадкових послідовностей перестановок на основі факторіальної системи числення, методів захисту інформації від нав'язування хибних даних і помилок каналу зв'язку на основі роздільного факторіального кодування, а також математичної моделі процесу декодування роздільних факторіальних кодів.

Метод формування випадкових послідовностей перестановок на основі ФСЧ дозволяє формувати відтворювану непередбачувану послідовність перестановок, виключити необхідність приведення випадкового числа до потрібного діапазону, зменшити розрядність додаткового генератора псевдовипадкових чисел, а також підвищити швидкість формування перестановок порівняно з алгоритмом Фішера-Йєтса.

Розроблені принципи роздільного факторіального кодування інформації дозволяють розширити науково-технічну базу методів і засобів контролю цілісності інформації під час її зберігання та передавання. Виявлення помилок, внесених каналом зв`язку, і виявлення факту несанкціонованої модифікації інформації – забезпечується за рахунок використання завадостійкого

факторіального коду, в процесі формування перевірної частини якого використовується множина змінних констант, що використовується в якості ключа.

У третьому розділі розроблено метод нероздільного факторіального кодування з відновленням та математичної моделі процесу декодування нероздільних факторіальних кодів.

Методи нероздільного факторіального кодування інформації (метод факторіального кодування з відновленням даних за перестановкою, метод факторіального кодування з відновленням даних за перестановкою з доповненням, метод нероздільного факторіального кодування з декількома контрольними сумами, метод факторіального кодування з відновленням даних за перестановкою з заданим числом інверсій, метод факторіального кодування з відновленням даних за перестановкою та виправленням помилок) дозволяють забезпечити захист інформації від несанкціонованого читання та помилок каналу зв'язку, властивість самосинхронізації коду та підвищити достовірність інформації в умовах обмежень пропускної здатності каналів зв'язку.

У четвертому розділі запропоновано вдосконалення методу формування псевдовипадкових послідовностей на основі конкатенації зв'язних компонентів графа станів лінійного конгруентного генератора для генерації елементів перетворення інформації в процесі факторіального кодування, а також удосконаленням методу симетричного криптографічного захисту інформації для забезпечення її конфіденційності.

На основі теорії монад і їх графів побудовано типові структури графа станів ЛКГ. Виконано узагальнення проаналізованих структур, представлено типові графи ЛКГ. Виконано дослідження впливу параметрів ЛКГ на його топологію.

Метод формування ПВП на основі лінійного конгруентного методу за рахунок конкатенації не тільки відокремлених і непересічних циклів у графі станів ЛКГ, а й передциклів (дерев), якщо вони в ньому містяться, дозволяє формувати ПВП рівномірно розподілених чисел незалежно від топології графа станів ЛКГ та, як наслідок, мінімізувати часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення максимального періоду.

Метод двоконтурного криптографічного перетворення дозволяє об'єднати переваги потокових і блокових шифрів: довжина ключа скінченна, трек помилки не перевищує довжини блоку, винесення ключа блокується,

рандомізація інформаційного масиву не вимагається, а також забезпечується підвищення криптографічної стійкості перетворення до статистичного криптоаналізу.

У п'ятому розділі виконано аналіз статистичних властивостей комбінаційного методу формування псевдовипадкових послідовностей на основі підсумовування за модулем.

Теоретично обґрунтовано принципи побудови комбінаційного генератора, який використовує підсумовування за модулем в якості комбінаційної функції, для чого визначено закон розподілу чисел на виході комбінаційного генератора, що містить групу первинних генераторів випадкових чисел як з необмеженими, так і з обмеженими періодами, а також циклічно повторюваних перестановок. Це дозволило обґрунтувати загальні вимоги до первинних послідовностей і комбінаційної функції для забезпечення рівномірного розподілу чисел у заданому діапазоні, а також розробити методику вибору параметрів первинних генераторів.

У шостому розділі запропоновано метод і критерії кореляційного аналізу часових рядів для тестування псевдовипадкових послідовностей з метою оцінювання їх статистичних відхилень, а також надано опис методології захисту інформації в телекомунікаційних системах і мережах на основі факторіального кодування даних.

Розроблені метод, критерії та методики оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел дозволяють виявити статистичні властивості, притаманні послідовностям, породженим природними джерелами випадкових чисел, і не притаманні штучно згенерованим ПВП. Застосування розроблених методів і критеріїв дозволило виявити статистичні відхилення для деяких генераторів ПВП.

Для основних положень дисертації та змісту автореферату характерна повна ідентичність.

Наукове та практичне значення результатів дисертаційної роботи

У дисертаційній роботі вирішено наукову проблему створення методології захисту інформації на основі факторіального кодування даних з необхідними статистичними, структурними властивостями кодових послідовностей. Розроблена методологія дозволяє забезпечити підтримку процесів створення систем захисту інформації від помилок каналу зв'язку, несанкціонованої модифікації та/або несанкціонованого доступу.

Наукова новизна отриманих результатів дисертаційної роботи, на мою думку полягає в наступному:

1. Удосконалено метод формування випадкової послідовності перестановок на основі використання ФСЧ. Метод базується на введенні додаткового генератора випадкових чисел (ГВЧ), символи якого підсумовуються з модифікованим синдромом попередньої перестановки та визначають синдром наступної перестановки. Це дозволяє зменшити обсяг внутрішньої пам'яті додаткового ГВЧ не менш ніж на кількість біт, що дорівнює логарифму двійковому від порядку генерованих перестановок, уникнути порушення рівномірності їх розподілу та підвищити швидкість їх формування.

2. Вперше розроблено методи роздільного факторіального кодування інформації, які реалізують єдину процедуру завадостійкого кодування та захисту від нав'язування хибних даних шляхом використання перестановки в якості перевірної частини кодового слова. Це дозволяє забезпечити контроль цілісності інформації та підвищити її достовірність під час передавання в телекомунікаційних системах з обмеженою пропускною здатністю каналів зв'язку.

3. Вперше розроблено методи нероздільного факторіального кодування інформації, які реалізують єдину процедуру завадостійкого кодування та шифрування шляхом бієктивного перетворення інформаційної послідовності в перестановку чисел заданого порядку. Це дозволяє забезпечити захист інформації від помилок каналу зв'язку та несанкціонованого доступу, а також підвищити її достовірність під час передавання в телекомунікаційних системах з обмеженою пропускною здатністю каналів зв'язку.

4. Вперше розроблено математичну модель процесу декодування факторіальних кодів під час передавання даних симетричним двійковим каналом з незалежними бітовими помилками. Це дозволяє оцінити показники достовірності передавання інформації в результаті застосування факторіального кодування та підтвердити його переваги порівняно з іншими методами завадостійкого кодування.

5. Удосконалено метод формування ПВП)на основі лінійного конгруентного методу. Для цього розроблено модель узагальненого графа станів ЛКГ, представлено кожну зв'язну компоненту графа у вигляді циклів, оснащених добутками дерев, передбачено конкатенацію в графі станів ЛКГ не лише відособлених непересічних циклів, а і передциклів (дерев). Це дозволяє

формувати ПВП рівномірно розподілених чисел максимального періоду незалежно від топології графа станів ЛКГ, мінімізувати часові витрати на вибір параметрів ЛКГ та збільшити розмір простору їх допустимих значень для досягнення максимального періоду в число разів, що дорівнює відношенню потужності алфавіту ЛКГ до її функції Ейлера.

6. Удосконалено метод симетричного криптографічного захисту інформації на основі операції гамування. Метод базується на введенні другого контуру шифрування та використання в ньому принципів конкатенації зв'язних компонентів у графі станів ЛКГ. Це дозволяє виключити можливість винесення гами, зменшити ймовірність зламу шифру методом повного перебору ключового простору та підвищити стійкість до статистичного криптоаналізу;

7. Уперше теоретично обґрунтовано принципи побудови комбінаційного генератора з комбінаційною функцією підсумовування за деяким модулем слів, отриманих від групи первинних генераторів рівномірно розподілених випадкових чисел. Для цього визначено закон розподілу чисел на виході комбінаційного генератора. Це дозволило сформувати загальні вимоги до первинних послідовностей і комбінаційної функції для забезпечення необхідних статистичних властивостей послідовності чисел.

8. Вперше розроблено метод оцінювання послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел. Для цього досліджено закон розподілу знаків емпіричної автокореляційної функції відносно кількості символів в перекритих частинах відрізків, на які розбивається послідовність чисел, і визначено допустимий «поріг» перекриття, нижче якого спостерігається рівномірний розподіл знаків автокореляційної функції. Це дозволяє виявити статистичні властивості, притаманні послідовностям, породженим природними джерелами дискретного білого шуму.

Практичне значення результатів дисертації полягає у наступному:

1. Розроблено алгоритм формування випадкової послідовності перестановок порядку M, що забезпечують можливість його практичної реалізації та дозволяють уникнути приведення випадкових чисел до діапазону зі змінною верхньою межею, зменшити розрядність внутрішнього стану додаткового генератору випадкових чисел не менш ніж на $\log_2 M$ біт, а також підвищити у рази швидкість формування перестановок порівняно з алгоритмом Фішера-Йєтса.

2. Розроблено алгоритми кодування та декодування факторіальних кодів (повного факторіального коду, комбінованого факторіального коду, роздільного

та нероздільного факторіальних кодів з декількома контрольними сумами, факторіального коду з відновленням даних за перестановкою, факторіального коду з заданим числом інверсій, факторіального коду з виявленням і виправленням помилок, що дозволяє забезпечити енергетичний виграш та захист інформації.

3. Розроблено алгоритм формування псевдовипадкових послідовностей перестановок на основі лінійного конгруентного генератора з будь-яким типом графа його станів, що дозволяє мінімізувати часові витрати на вибір параметрів лінійного конгруентного генератора , збільшити розмір простору їх допустимих значень та періоду псевдовипадкових послідовностей, збільшити в рази швидкість роботи в порівнянні генератора псевдовипадкових чисел LFIB78 із застосуванням алгоритму Фішера-Йєтса.

4. Розроблено алгоритм роботи пристрою двоконтурного криптографічного перетворення даних, що забезпечує підвищену криптографічну стійкість до атаки повного перебору.

5. Розроблено методику вибору параметрів первинних генераторів перестановок для комбінаційного генератора з комбінаційною функцією підсумовування за модулем M , що дозволяє забезпечити рівномірний розподіл сформованої послідовності на множині цілих чисел потужності M та проходження пакетів статистичного тестування ПВП NIST STS, Diehard, TestU01.

6. Розроблено критерії та методики перевірки послідовностей рівномірно розподілених випадкових і псевдовипадкових чисел, що можуть бути використані під час оцінювання випадкових послідовностей, у тому числі сумісно з пакетами статистичного тестування. Застосування розроблених критеріїв дозволило виявити статистичні відхилення для деяких генераторів псевдовипадкових послідовностей, які успішно проходять усі автокореляційні тести пакету TestU01, а також для реалізації квантового ГВЧ.

Результати дисертаційного дослідження впроваджено в ДП «НДІ «Акорд» (система дистанційного зв'язку, контролю та управління віддаленими об'єктами, м. Черкаси), ТОВ «Діджитал Мастер» (імітатор модуля керування метеорологічним локатором «Буран-А» авіаційного тренажера КТС-148, м. Київ); Департаменті освіти та гуманітарної політики Черкаської міської ради (система обліку кадрів, м. Черкаси), а також використані в навчальному процесі Черкаського державного технологічного університету, Черкаського інституту пожежної безпеки імені Героїв Чорнобиля та Національного аерокосмічного

університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

Повнота викладу результатів дисертаційної роботи в опублікованих працях та їх апробація

Результати дослідження опубліковані у 80 наукових працях – двох розділах у двох колективних монографіях, 33 статтях, 12 патентах України, 33 тезах доповідей на наукових конференціях. Кількість та якість праць, опублікованих за матеріалами дисертаційного дослідження, відповідають встановленим вимогам МОН України. Перераховані публікації в достатній мірі відображують основні наукові та практичні результати дисертаційної роботи.

З праць, опублікованих у співавторстві, здобувачем використано лише ті результати, які отримано ним самостійно.

Зауваження

1. У дисертації не представлена формалізація цілі в якій визначаються показники оцінки розроблених рішень та параметри, що оптимізуються. Часткові показники які використовуються, наприклад, енергетична ефективність коду, мають обмеження щодо використання. Для систем передачі з перезапитом базовою характеристикою є ймовірність визначення помилок (навмисних чи ненавмисних) і вона впливає на зменшення швидкодії каналу передачі даних. Якщо оцінюється криптографічна властивість системи, основною характеристикою є ймовірність нав'язування повідомлень.

2. В роботі не надано чисельних прикладів, щодо факторіального кодування та декодування. Це ускладнює розуміння розроблених алгоритмів та співставлення з відомими кодовими алгоритмами та оцінками.

3. Одним з основних показників криптографічних перетворень є стійкість до атак. У роботі зроблені оцінки тільки до атаки переборного типу. Не показані атаки інших типів: на алгоритм, по кодової відстані, з відкритим текстом.

4. Формулювання вимог до повного факторіального коду (стор. 105) в частині забезпечення імітостійкості та достовірності: «повинен забезпечувати захист інформації від нав'язування хибних даних і помилок, що вносяться каналом зв'язку» не конкретизовані та легко здійсненні будь-яким загальновідомим методом (наприклад, введенням контрольної суми). Якби додатково вказувалося обсяги введеної надлишковості для кожного з видів захисту, вимоги до показників достовірності та імітостійкості, то це б відсікало всі типові рішення. Аналогічно вимоги до рівня колізій мали б бути більш конкретизовані та роз'яснені.

5. Для факторіального коду з відновленням даних і виправленням

помилок (стор. 196-207) не визначено процедуру вибору сигнально-кодової конструкції максимальної потужності, яка дозволяє виправляти задану кратність помилок.

6. Під час висвітлення результатів дослідження швидкості роботи пристроїв формування послідовностей перестановок (стор. 104, 243) не вказано архітектуру та показники продуктивності засобу, на якому реалізовано генератори перестановок.

7. За результатами роботи чітко не визначені пропозиції щодо параметрів вибору параметрів криптографічних перетворень в класі факторіальних кодів на групі перестановки, які забезпечують сучасні вимоги криптографічної стійкості.

Висновки

Дисертаційна робота Фауре Еміля Віталійовича «Методологія захисту інформації на основі факторіального кодування даних» за своїм змістом відповідає паспорту спеціальності 05.13.21 – системи захисту інформації.

Зазначені недоліки не є суттєвими та критичними і не впливають на загальну позитивну оцінку здобувача. У цілому дисертаційна робота Фауре Еміля Віталійовича є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати для вирішення задач комплексного захисту інформації в телекомунікаційних системах загального та спеціального призначення.

Вважаю, що дисертаційна робота «Методологія захисту інформації на основі факторіального кодування даних» повністю відповідає вимогам «Порядку присудження наукових ступенів», затвердженого Постановою КМ України від 24.07.2013р. №567 (із змінами, внесеними згідно з Постановами КМ України №656 від 19.08.2015, №1159 від 30.12.2015 №567 від 27.07.2016р.), а її автор Фауре Еміль Віталійович, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
завідувач кафедри безпеки інформаційних технологій
Харківського національного університету радіоелектроніки,
доктор технічних наук, професор Г.З. Халімов

Підпис Халімова Г.З.
Засвідчую
Учений секретар І.В. Магдаліна