УДК 004.056.55

О. О. Кузнецов[1], Р. В. Олійников[1], Ю. І. Горбенко[1],
А. І. Пушкарьов[2], О. В. Дирда[2], І. Д. Горбенко[1]
[1]ПАТ "Інститут інформаційних технологій"
[2]Департамент криптографічного захисту інформації Державної
служби спеціального зв'язку та захисту інформації

ОБҐРУНТУВАННЯ ВИМОГ, ПОБУДУВАННЯ ТА АНАЛІЗ ПЕРСПЕКТИВНИХ СИМЕТРИЧНИХ КРИПТОПЕРЕТВОРЕНЬ НА ОСНОВІ БЛОЧНИХ ШИФРІВ

Досліджено теоретичні та практичні аспекти аналізу та синтезу перспективних симетричних криптосистем. Проаналізовано вимоги, які ставлять до перспективних симетричних шифрів, зокрема щодо криптографічної стійкості, швидкодії та обсягів пам'яті. Досліджено принципи синтезу сучасних блокових симетричних криптоперетворень, викладено основні результати проведених досліджень.

Ключові слова: криптографічний захист інформації, блокове симетричне криптографічне перетворення, режими застосування алгоритмів шифрування.

REQUIREMENTS JUSTIFICATION, CONSTRUCTION AND ANALYSIS OF PERSPECTIVE SYMMETRIC CRYPTOGRAPHICAL TRANSFORMATIONS ON THE BASE OF BLOCK CIPHER CODES

Theoretical and practical aspects of analysis and synthesis of perspective symmetric cryptosystems have been developed. Analysis of requirements for perspective symmetric cipher, in particular for cryptoresistability, operating speed and memory volume has been performed. Principles of synthesis of the modern block symmetric cryptographical transformations have been investigated, main results of the performed investigations have been presented.

Key words: cryptographic information protection, block symmetric cryptographical transformations, application regimes of encryption algorithms.

Вступ

Доктриною інформаційної безпеки України, затвердженою Указом Президента України від 08.07.2009 р. № 514, визначено реальні та потенційні загрози інформаційній безпеці України, до яких, зокрема, зараховано несанкціонований доступ до інформаційних ресурсів, зокрема внаслідок використання іноземних інформаційних технологій [1–7].

Щоб забезпечити інформаційну безпеку України, Адміністрація Держспецзв'язку ініціювала розроблення вітчизняного криптографічного алгоритму блокового симетричного шифру (БСШ). Безумовно, прийняття національного стандарту БСШ сприятиме підвищенню рівня інформаційної безпеки України [8, 9].

Серед переваг прийняття національного стандарту – впровадження в Україні сучасного криптографічного БСШ, застосування якого допоможе забезпечити необхідну захищеність інформації та інформаційних ресурсів у частині послуг конфіденційності та цілісності, зокрема з

обмеженим доступом, а також здійснювати захищену обробку інформації з підвищеною швидкодією в інформаційно-телекомунікаційних системах (ІТС).

Мета статті – викласти теоретичні та практичні аспекти побудування та аналізу перспективного БСШ з урахуванням зростання вимог, а також порівняльного аналізу отриманих результатів з відомими, зокрема складності шифрування.

Аналіз вимог, які ставляться до перспективних симетричних криптосистем

Згідно з нинішніми поглядами блокові симетричні криптоперетворення та розроблені на їх основі БСШ є основним криптографічним механізмом забезпечення конфіденційності та цілісності, а також захисту інформації та інформаційних ресурсів від НСД. Іншою важливою властивістю БСШ є можливість забезпечення достатньо високої швидкодії шифрування та розгортання ключа [9].

Для досягнення поставленої мети спочатку проаналізуємо вимоги, які ставлять до перспективних симетричних криптоперетворень, зокрема БСШ, зокрема загальних вимог щодо криптографічної стійкості та спеціальних вимог, які визначають певні параметри криптографічного перетворення у визнаних на практиці та закріплених у міжнародних стандартах режимах роботи БСШ.

Загальні вимоги до криптографічної стійкості

У сучасних ІТС з криптографічним захистом інформації та інформаційних ресурсів довжина повідомлення, що захищається з використанням БСШ, значно перевищує довжину ключа шифрування, тобто ентропія джерела повідомлень істотно перевищує ентропію джерела ключа. У цьому випадку відносно БСШ не виконується критерій безумовної стійкості [9] і в таких умовах доцільне введення поліноміального критерію, що припускає наявність обмежень для обчислювальних ресурсів зловмисника й часу, протягом якого шифр залишається стійким. Такий поліноміальний критерій приводить до практичного критерію стійкості – неможливості реалізації атаки на шифр в умовах сучасної обчислювальної бази, зокрема з урахуванням постійного збільшення потужності засобів обчислювальної техніки та появи квантових комп’ютерів, упродовж тривалого строку.

З урахуванням результатів проведених досліджень основні вимоги до проекту національного БСШ [9, 10, 39], в частині його криптографічної стійкості, такі.

1. Криптографічна стійкість шифру залежить від складності реалізації атаки на БСШ. Показниками складності криптоаналізу, як правило, слугують [9, 13, 15].

Часовий – математичне сподівання часу (безпечний час), необхідного для реалізації атаки на доступних / перспективних обчислювальних засобах.

Просторової складності – обсяг пам'яті, що необхідний для виконання криптографічного аналізу.

Мінімально необхідна для успішної реалізації атаки кількість пар зашифротекст/ відкритий текст чи кількість пар відкритий текст/ шифротекст.

Попередній аналіз дає підстави зробити висновок, що якщо хоча б щодо одного із зазначених показників реалізація атаки на практиці неможлива зі значним запасом стійкості, то алгоритм шифрування можна вважати стійким.

2. Як правило, початкову оцінку стійкості необхідно здійснювати стосовно силових атак: на БСШ, атак на словник, створення колізій тощо. За умови забезпечення необхідного рівня стійкості БСШ до силових атак можна переходити до оцінки стійкості БСШГ відносно аналітичних атак.

3. Результати аналізу показали: відносно сучасних БСШ як критерії оцінки стійкості до аналітичних атак рекомендується застосовувати [9, 15]:

− потужність множини шифрованих/відкритих текстів, необхідних для виконання криптоаналітичної атаки, повинна перевищувати потужність множини допустимих шифрованих/відкритих текстів;

− складність будь-якої аналітичної атаки повинна перевищувати складність силової атаки або дорівнювати їй;

− для реалізації аналітичної атаки необхідна кількість групових операцій шифрування повинна бути не меншою, ніж за повного перебирання ключів;

− обсяг пам'яті, необхідний для зберігання проміжних результатів у разі здійснення аналітичної атаки, повинен бути не меншим, ніж за реалізації атаки на словник на повний шифр;

− з огляду на можливість удосконалювання криптоаналітичних методів необхідно використовувати критерій “запасу стійкості” до аналітичних атак, згідно з яким складність атаки на весь алгоритм повинна істотно перевищувати складність силових атак. Як правило, цей критерій розглядає версію БСШ алгоритму шифрування зі зменшеною кількістю циклів, що є уразливим проти криптографічного аналізу (за цих умов різниця в кількості циклів визначає запас стійкості алгоритму до конкретної криптоаналітичної атаки, причому чим більша різниця, тим стійкіший алгоритм);

− для оцінки криптографічної стійкості загальної конструкції шифру можна використати ще один критерій, що розглядає можливість усунення яких-небудь операцій або заміни їх менш складними операціями (наприклад, на деяких наборах вхідних даних операція додавання за модулем 232 близька або еквівалентна до операції додавання за модулем 2. За цих умов повноцикловий варіант спрощеного шифру повинен залишатися стійким до аналітичних атак.

4. Необхідно також ураховувати, що більшість сучасних аналітичних атак, насамперед, таких як диференціальний і лінійний криптоаналіз, є статистичними [9, 39]. Під час криптоаналізу для одержання ключа виконується велика кількість шифрувань і на підставі шифротекстів формуються варіанти підключів (циклових ключів). Під час обробки доволі великої вибірки шифротекстів, сформованих на одному ключі, правильне значення ключових бітів трапляється частіше від інших варіантів. Очевидно, що ймовірність знаходження правильної пари (що дає коректне значення ключа) залежить від статистичних властивостей шифру, і для збільшення складності криптоаналізу властивості криптограми повинні бути близькі до властивостей випадкової послідовності. Тому необхідною (але не достатньою) умовою стійкості шифру до аналітичних атак є забезпечення належних статистичних властивостей вихідної послідовності (шифротекстів).

5. З'ясовано [39], що для захисту БСШ від алгебраїчних атак необхідно, щоб не існувало способу практичної побудови системи рівнянь, що зв'язують відкритий текст, криптограму й ключ шифрування, або не існувало способу розв’язання таких систем у поліноміальний час.

6. Розробляючи засоби блокового шифрування, необхідно враховувати можливість організації атак на реалізацію (зміна температурного режиму електронного пристрою, вхідної напруги, поява іонізуючого випромінювання, замірювання споживаних струмів, часу виконання тощо). Такі атаки можуть бути ефективні проти всіх криптографічних алгоритмів, і захист від них під час проектування засобів криптографічного захисту інформації потребує вже інженерних рішень.

7. Загалом можна сформулювати також вимоги відносно стійкості сучасних БСШ:

− забезпечення стійкості до силових атак, наприклад за часовим або просторовим критерієм стосовно зберігання проміжних результатів обсягу пам'яті;

− відсутність способів побудови або розв’язання системи рівнянь, що зв'язує відкритий текст, криптограму й ключ шифрування;

− неможливість реалізації відомих аналітичних атак на шифр або їхня складність повинна бути вищою від складності реалізації силових атак (наприклад, один з таких критеріїв: потужність необхідної множини відкритих/зашифрованих повідомлень; необхідна кількість операцій шифрування; обсяг пам'яті, потрібний для зберігання проміжних результатів);

− наявність “запасу стійкості” шифру (додаткових циклів шифрування), що забезпечує безпечне використання алгоритму у випадку вдосконалювання криптоаналітичних атак;

− стійкість спрощеного варіанта шифру, у якому деякі операції вилучені або замінені простішими;

− забезпечення “належних” статистичних властивостей вихідної послідовності шифру (криптограми або гами, що шифрує), за яких криптограми й гами шифрування практично не відрізняються за властивостями від випадкової послідовності.

8. Крім необхідного рівня криптографічної стійкості, до БСШ ставиться вимога забезпечення високого рівня продуктивності (складності зашифрування, розшифрування та розгортання ключа).

Зважаючи на значні обсяги інформації, що обробляються в ІТС, ця вимога є надзвичайно важливою та критичною для ефективного функціонування всієї ІТС. Також під час розроблення систем із застосуванням БСШ, крім перерахованих вимог, необхідно враховувати вартість реалізації засобів шифрування та експлуатації відповідних засобів.

9. Попередній аналіз підтвердив, що зазначені вимоги, по суті, доволі суперечливі: наприклад, у більшості сучасних алгоритмів зростання криптографічної стійкості вимагає додаткових циклів шифрування, що веде до зниження продуктивності. Проте алгоритми-фіналісти міжнародних криптографічних конкурсів, таких як AES, NESSIE, CryptRec [30–32] та інших, свідчать про можливості досягнення раціональних показників, близьких до оптимальних.

Спеціальні вимоги до перспективного БСШ

Проведений аналіз спеціальних вимог [9, 10, 39], які визначають певні параметри криптографічного перетворення, дав змогу сформулювати такі обмеження та вимоги до перспективного БСШ.

1. Захищеність алгоритму від криптоаналітичних атак. Основними методами криптографічного аналізу є: диференціальний криптоаналіз, розширення для диференціального криптоаналізу, пошук найкращої диференціальної характеристики, лінійний криптоаналіз; інтерполяційне вторгнення; вторгнення із частковим угадуванням ключа; вторгнення з використанням зв'язаного ключа; вторгнення на основі обробки збоїв; пошук лазівок та потенційні атаки тощо.

2. Статистична безпека криптографічного алгоритму в плані нерозрізнюваності гам шифрування та шифротекстів від істинно випадкових [9].

3. Особливості конструкції та відкритість структури. Криптоалгоритм повинен мати зрозумілу, легку для аналізу структуру й ґрунтуватися на надійному математичному апараті.

4. Стійкість до модифікації, коли всіх кандидатів перевіряють на стійкість до різноманітних модифікацій: стійкість до криптоаналітичних атак у разі зменшення кількості циклів, скорочення компонентів, використовуваних алгоритмом тощо.

5. Обчислювальна складність (швидкість) за шифрування/розшифрування. Складність програмної, апаратної й програмно-апаратної реалізації повинна оцінюватися обсягом пам'яті як для програмної, так і для апаратної реалізації, зокрема за програмної реалізації – кількістю необхідної оперативної пам'яті, розміром вихідного коду, швидкістю роботи програми на різних платформах за реалізації на відомих мовах програмування. За апаратної оцінюється кількістю вентилів і швидкістю в Мб/с.

6. Універсальність криптографічного алгоритму: можливість роботи з різними довжинами початкових ключів та інформаційних блоків; безпека реалізації на різних платформах і додатках; можливість використання криптографічного алгоритму в необхідних обґрунтованих режимах роботи БСШ.

7. Загальні вимоги до БСШ повинен визначати замовник у вигляді конкретних параметрів криптоалгоритму. Їх сутність така.

8. Параметри криптоалгоритму:

- криптоалгоритм повинен будуватись на основі БСШ;
- обов’язкові розміри блока даних – 128, 256 та 512 бітів;
- обов’язкові розміри разового (сеансу) ключа – 128, 256, 512 бітів.

9. Принципи побудови:

- здатність протистояти відомим методам криптографічного аналізу та мати запас стійкості з урахуванням тенденцій розвитку засобів електронної обчислювальної техніки та криптографічної науки;
- криптографічні перетворення, що застосовуються, повинні ґрунтуватись на надійній та прозорій математичній базі та не мати вбудованих лазівок;
- швидкодія криптоалгоритму повинна бути не меншою, ніж швидкодія чинного державного стандарту шифрування.

10. Реалізація криптоалгоритму:

- криптоалгоритм повинен бути орієнтованим для можливості реалізації на 32- або 64-розрядних процесорах;
- зазначені в криптоалгоритмі операції повинні мати ефективну програмну та апаратну реалізацію;
- необхідний для роботи обсяг пам’яті має враховувати можливість реалізації криптоалгоритму у мікропристроях;
- давати змогу паралельного виконання декількох операцій (за можливості).

11. Ключова система:

- наявність ключа сеансу;
- криптоалгоритм може передбачати наявність довгострокового ключа;
- довжина синхронізуючої посилки – не менше ніж 64 бітів.

12. Ефективність криптографічного захисту із застосуванням БСШ залежить не тільки від властивостей БСШ, але і від способів його використання, тобто властивості криптографічного перетворення безпосередньо залежать від режиму застосування блокового симетричного шифрування. В криптоалгоритмі повинні бути передбачені такі режими роботи [41]:

- режим простої заміни, який є обов’язковою складовою для всіх інших режимів застосування блокового симетричного шифрування. Це найпростіший з погляду реалізації режим електронної кодової книги, який полягає у забезпеченні конфіденційності окремих блоків відкритого тексту з їх шифруванням за введеним секретним ключем;
- режим гамування, призначений для забезпечення конфіденційності з швидким шифруванням блоків відкритого тексту із можливістю застосування паралельних обчислень. Він полягає у шифруванні набору вхідних блоків, які є виходом лічильника, та у додаванні їх (блоків гами) до блоків відкритого тексту;
- режим гамування зі зворотним зв'язком, який призначено для забезпечення конфіденційності шифруванням потоку даних з розмноженням помилок і унеможливленням маніпуляцій із окремими блоками відкритого тексту;
- режим зчеплення шифроблоків, який призначено для забезпечення конфіденційності, де процес шифрування побудовано як об'єднання блоків відкритого тексту з попередніми блоками зашифрованого тексту;
- режим вироблення імітовставки, оснований на використанні режиму зчеплення шифроблоків із додатковим додаванням ключа до останнього шифроблока. Сформована у такий спосіб імітовставка призначена для забезпечення автентичності й цілісності інформації;
- режим гамування зі зворотним зв’язком по шифрогамі, призначений для забезпечення конфіденційності. Цей режим основано на шифруванні вектора ініціалізації (синхропосилки) для генерації послідовності вихідних блоків (шифрогами), які додаються до звичайного тексту, щоб сформувати зашифрований текст і навпаки, до шифротексту для його розшифрування;
- режим імітовставки із гамуванням та без гамування – Galois/Counter Mode and Galois Message Authentication Code (GCM and GMAC), який призначений для забезпечення конфіденційності та цілісності інформації;
- режим індексованої заміни (XEX-based Tweakable CodeBook mode with Ciphertext Stealing – XTS), який призначений для забезпечення конфіденційності даних передусім у разі їх зберігання на певних фізичних носіях (вінчестерах, оптичних дисках тощо);
- режим шифрування ключа (Key Wrapping – KW), який полягає в багаторазовому застосуванні функції шифрування до масиву ключових даних, що “обгортаються” шифром і надійно захищаються за певною схемою “обгортки”. Правило “обгортання” задається специфікацією режиму Key Wrapping.

13. Досвід і результати виконання проектів AES, NESSIE, з урахуванням також національних вимог до БСШ, дають змогу запропонувати класифікацію БСШ за стійкістю у вигляді таких умов [9, 39]:

- надвисокої стійкості, коли довжини блока інформації й довжина вихідного ключа не менше за 512 бітів;

− високої стійкості, коли довжина блока інформації й довжина ключа не менші, ніж 256 бітів;

− нормального рівня стійкості, коли довжина блока інформації й довжина ключа не менше ніж 128 бітів;

− задовільний рівень стійкості, коли довжина блока інформації не менш ніж 64 бітів, а довжина ключа – не менше ніж 128 бітів.

На наш погляд, наведені вимоги є необхідними, але не достатніми.

Аналіз принципів синтезу сучасних блокових симетричних шифрів

Історія створення БСШ розпочинається з представлення фірмою IBM в 1974 р. алгоритму блокового симетричного шифрування DES (Data Encryption Standard) [11, 12]. Алгоритм DES надала фірма IBM у відповідь на звернення Національного бюро стандартів США до спеціалістів з питанням про алгоритми для стандарту шифрування в державних та приватних установах. Одна із вимог полягала в тому, що алгоритм повинен бути опублікований без ризику відносно його стійкості. Розробка фірми IBM була основана на її попередньому шифрі Lucifer з 128-бітним ключем [13]. В алгоритмі IBM запропонувала ключ з довжиною 48*16 бітів, відповідно 48 бітів на кожному із 16 циклів. У 1977 р. алгоритм БСШ DES опубліковано як федеральний стандарт США, який набрав чинності в липні того самого року [11]. Цю дату можна вважати початком створення та застосування БСШ DES у відкритому вигляді. Майже одразу після прийняття стандарт DES став об’єктом полеміки.

Основним недоліком вважалась мала довжина секретного ключа – 56 бітів. Справді, вже на той час за потужності множини 256 ключів (приблизно 1016.86) явною була можливість здійснення силової атаки, яка була близькою до межі можливості її реалізувати. Діффі та Геллман опублікували проект спеціалізованої багатопроцесорної обчислювальної машини вартістю близько $ 20 млн, яка могла б розкрити DES приблизно за 12 годин [14, 15]. Зауважимо, що в DES, на момент його створення, були вдало реалізовані накопичені до того моменту теоретичні й практичні здобутки щодо побудови симетричних шифрів. Уже одразу після прийняття протягом наступних двадцяти років БСШ DES детально вивчали й досліджували, і якраз поява багатьох методів криптоаналізу була пов'язана з DES. Конструкція алгоритму шифрування виявилася настільки вдалою, що продовжила розвиватись в інших відомих криптографічних алгоритмах – передусім ГОСТ 28147–89 [16], FEAL [17] і деяких інших менш відомих криптографічних алгоритмах, розроблених в 80-ті роки XX ст. Надалі для усунення такого недоліку, як мала довжина ключа, було запропоновано збільшити довжину ключа в три рази та застосовувати трикратне шифрування, яке є порівняно ефективним та застосовується донині.

Практично до початку 90-х років у закордонному відкритому друку практично не було фундаментальних робіт, що стосувались блокових симетричних шифрів. На початку 90-х років критика алгоритму DES почала посилюватися. У відкритій закордонній пресі з'явився ряд фундаментальних робіт, у яких вирішувались завдання криптоаналізу БСШ. Це насамперед лінійний криптоаналіз Матсуі [18] і диференціальний криптоаналіз Біхама й Шаміра [19–21], а також розширення зазначених атак. У вказаних роботах також критикують схему формування циклових підключів БСШ DES, відтак простоту схеми розгортання ключів, описано існування 4 слабких і 12 наполовину слабких ключів, а також властивість інвертування, що дозволяє скоротити пряме перебирання усіх ключів з 2^{56} до 2^{55}. Серед офіційних документів, що стосувались DES та його модифікації DEA, необхідно відзначити публікацію в 1981 р. федерального стандарту DES [12]. Якраз у ній описано слабкі й наполовину слабкі ключі, для чого було використано поняття двоїстих ключів. Детальніше вивчено слабкі й наполовину слабкі ключі у роботах Мура, Сімонса [22] та Коперсміта [23].

Згодом з’явились роботи [24–28], що були присвячені аналізу схем розгортання ключів у БСШ. Фундаментальною роботою можна вважати публікацію Біхама [29]. В цій роботі вперше описана атака на схему розгортання ключів типу “зв'язані ключі”, яка могла бути застосованою до БСШ DES і LOKI. Однак цей метод криптоаналізу з атакою на схему розгортання ключів мав радше

теоретичну, ніж практичну цінність, і не становив порівняно з диференціальним та лінійним криптоаналізом циклової функції шифру реальної загрози для БСШ.

Далі пошук нових рішень торкнувся вдосконалювання криптографічних перетворень циклової функції. З'явилась низка нових криптографічних алгоритмів. На найбільшу увагу серед них заслуговує алгоритм PES, що став основою розроблення Європейського стандарту IDEA, а також алгоритми RC5 та SAFER. Особливістю вказаних шифрів є те, що схеми розгортання ключів нових БСШ формують циклові підключі, аналогічно, як і у БСШ DES. По суті, вони являють собою алгоритми вибору певних бітів із секретного ключа. Згодом на названі шифри були розроблені ефективні методи криптоаналізу через схеми розгортання ключів.

Так, аналіз схеми розгортання ключів алгоритму IDEA дозволив Даемену [30] виявити кілька класів слабких ключів. Найбільший із цих слабких класів становить множину 251 ключів, причому належність ключа, що застосовується, до цього класу, можна перевірити двома шифруваннями й виконанням невеликої кількості додаткових обчислень. Якщо ключ належить цьому класу, то його можна відновити після 16 зашифрувань відкритих текстів з підібраною різницею, а також близько 216 групових операцій і 217 шифрувань перевірки ключа. У зазначеній вище роботі Даемен запропонував незначну модифікацію процедури розгортання ключа IDEA, що дозволило усунути знайдені ним слабкі ключі.

Схема розгортання ключів БСШ SAFER K-64 виявилася уразливою до атаки на зв'язані ключі, що запропонував Біхам [19]. Це пояснюється тим, що схема розгортання ключів має недостатній лавиноутворювальний ефект і генерує всі циклові ключі за однаковим алгоритмом. Ці дослідження описано в роботах Л. Кнудсена [31]. Загалом розвиток запропонованої оригінальної схеми криптоалгоритму продовжено у криптоалгоритмах SAFER SK-128, SAFER+ і SAFER++ [32, 33].

У роботі Кнудсена, Мейера [31] описана диференціальна атака на RC5, а також визначено множину слабких ключів, для яких ця атака стає ще ефективнішою. Криптоалгоритм розвинено в RC6 [34] зі змінами в схемі розгортання ключів.

До кінця 90-х років з'явились нові ефективні методи криптоаналізу схем розгортання ключів БСШ, основані на використанні як диференціального, так і лінійного методів криптоаналізу. Принципово необхідно виділити диференціальний криптоаналіз на зв'язаних ключах [19], атаку ковзання і її розширення [35]. Особливістю таких атак, порівняно з атаками на циклову функцію БСШ (наприклад, диференціальним і лінійним криптоаналізом), є більша ефективність, що полягає в слабкій залежності від кількості ітерацій, що використовуються в шифрі.

Загальною рекомендацією є пропозиція уникати лінійних алгоритмів під час формування циклових підключів, а також щоби процес вироблення підключів був важкооборотним [9, 39], зв'язок між цикловими підключами повинен бути складним з погляду складності аналізу.

Подальший аналіз показав, що до кінця 90-х склалась ситуація, коли в несекретних державних і комерційних установах продовжувалось використання морально та технічно застарілих шифрів. Водночас швидкий розвиток обчислювальної техніки й безлічі різних, високоефективних методів криптоаналізу блокових симетричних шифрів стали для них потенційними загрозами. Крім того, криптографічні алгоритми, що були розроблені, не підтвердили необхідного рівня безпеки, щоб стати заміною прийнятих стандартів шифрування даних (наприклад, Skipjack). Вказане привело до однієї із найважливіших подій у сфері прикладної криптографії – оголошення міжнародного конкурсу AES (Advanced Encryption Standard) [36]. У січні 1997 р. NIST США оголосив про початок конкурсу на новий стандарт шифрування XXI століття, спрямованого на вибір на конкурсній основі нового стандарту блокового симетричного шифрування. У результаті виконання цього проекту за результатами голосування переможцем був оголошений алгоритм Rijndael [37], згодом на його основі у звуженій версії був прийнятий федеральний стандарт США FIPS-197, який нині широко застосовують у США та у світі.

У проекті AES уперше зібрано воєдино безліч різних криптографічних алгоритмів з різною архітектурою й цілеспрямовано, детально проаналізовано. Фактично визначено вимоги, які повинні задовольняти перспективні БСШ. В процесі проведення конкурсу також визначено нові вимоги до схем розгортання ключів. У представлених на конкурс БСШ схеми розгортання ключів суттєво

відрізняються від DES-подібних. Крім того, відсутність основоположних принципів проектування схем розгортання ключів привела до того, що розроблювачі шифрів керуються суб'єктивним розумінням побудови схем розгортання ключів. У підсумку більшість шифрів виявилися уразливими до атак на схеми розгортання ключів. Так, у проекті AES брали участь БСШ Deal, Rijndael, SAFER+, DFC, MAGENTA, CRYPTON, HPC, LOKI97, MARS, RC6, Serpent, Twofish, CAST, E2, FROG. Але більшість із названих БСШ були уразливі до атак на схеми розгортання ключів, зокрема: SAFER+, CRYPTON, DFC, FROG, HPC, MAGENTA. Для інших БСШ атаки на схеми розгортання ключів були реалізовані на неповну кількість ітерацій, але виявилися найефективнішими порівняно з атаками на циклову функцію алгоритму. Так, прикладом може слугувати БСШ Rijndael, для якого знайдена дев'ятициклова атака на зв'язаних ключах (версія алгоритму з довжиною ключа $l_k = 128$ й кількістю ітерацій $r = 12$) і розширена Square-атака на семицикловий варіант алгоритму.

За аналогією з проектом AES розгорнуто та виконано аналогічні проекти у Європі (NESSIE) і Японії (CRYPTREC). Проект NESSIE розпочатий в 2000 р. під егідою Європейської комісії. Основними завданнями проекту NESSIE був відбір кращих десяти криптографічних примітивів.

Для криптоалгоритмів нормального й високого рівня безпеки склалася така ситуація: Noekeon, Hierocrypt-L3 і SHACAL-1 уразливі до атак зв'язані ключі й ковзання. Серед БСШ, на які виявлено атаки, зв'язані зі схемою розгортання ключів, але не на повноциклову версію, відзначимо криптоалгоритм Rijndael [37]. Переможцями конкурсу серед криптоалгоритмів нормального й високого рівня безпеки були оголошені Camellia, Rijndael і SHACAL-256. На всі інші криптопримітиви практично знайдено аналітичні атаки, ефективніші від "грубої" сили або такі, що не забезпечували необхідної швидкості шифрування.

Зазначимо, що вперше ставилися вимоги не тільки високої криптостійкості, але і якісних характеристик (наприклад швидкості). Результати досліджень також показали, що криптоалгоритми Grandcru і SC2000 мають низькі показники швидкості, внаслідок чого вони не пройшли в другий тур. Найшвидшими серед алгоритмів є БСШ RC6 і Rijndael, які позитивно оцінені ще під час проведення конкурсу AES.

За результатами подальших досліджень існуючих та перспективних БСШ прийнято міжнародний стандарт відносно блокових симетричних шифрів, що увійшли в міжнародний стандарт ISO/IEC 18033 – 3 [38]. Перелік та деякі характеристики БСШ стандарту наведено у табл. 1.

Таблиця 1

Характеристики БСШ з ISO/IEC 18033

Довжина блока	Назва алгоритму	Довжина ключа
64 бітів	TDEA	128 або 192 бітів
	MISTY1	128 бітів
	CAST-128	
128 бітів	AES	128, 192 або 256 бітів
	Camellia	
	SEED (5.3)	128 бітів

Згідно з прийнятою у проекті NESSIE класифікацією до БСШ задовільного рівня стійкості належать шифри, у яких довжина блока lб = 64 бітів, а довжина ключа lк = 128 бітів. Основними БСШ, що можна зарахувати до задовільного рівня стійкості, є БСШ ГОСТ 28147 – 89, TDEA, MISTY1 та CAST – 128. Важливо також визначитись з БСШ DES та DEA, у межах цієї класифікації їх зарахуємо до БСШ незадовільного рівня стійкості, оскільки їх уже не рекомендують застосовувати.

До БСШ нормального рівня стійкості належать шифри, у яких довжина блока lб = 128 бітів, а довжина ключа lк = 128 бітів. Основними БСШ, що належать до нормального рівня стійкості, є БСШ FIPS 197(AES), Camellia та S0EEDx ї.

До БСШ високого рівня стійкості можна відносити шифри FIPS 197(AES), Camellia, Калина, Мухомор тощо, у яких довжина блока дорівнює або не менша за 128 бітів і не більша за 256 бітів, а довжина ключа дорівнює або не менша за 256 бітів.

Важливою подією для України є підготовка та проведення національного конкурсу на кращий проект національного стандарту БСШ, який розпочався 15 жовтня 2006 р. і закінчений, про суті, в травні 2010 р. На конкурс в ініціативному порядку подано чотири кандидати в установленій формі – Калина, Лабіринт, ADE та Мухомор шифри. По суті два шифри, тобто Калина і ADE, є тією чи іншою мірою удосконаленням шифру з SPN-структурою, Лабіринт – ланцюга Файстеля, а Мухомор – IDEA структури. Специфікації та результати досліджень вказаних шифрів представлені також в низці видань. Результатом конкурсу є формування колективів, здатних виконувати складні завдання розроблення та дослідження перспективних БСШ, а також розробка та освоєння науково-методичного забезпечення в сфері синтезу та аналізу БСШ. Цей досвід уже використано для гармонізації в Україні міжнародного стандарту ISO/IEC 18033 – 3 [38] та інших стандартів.

Вимоги, поставлені до перспективного БСШ в національному конкурсі, відрізняються від Nessie вимог тим, що у національному конкурсі ще введено надвисокий рівень безпеки (гарантій), коли lб≥256 бітів, а довжина ключа lк≥512 бітів.

До БСШ надвисокого рівня стійкості зарахуємо шифри БСШ SHACAL-2, “Калина”, “Мухомор”, Threefish, у яких довжина блока дорівнює або не менша за 256 і не більша за 512 бітів, а довжина ключа дорівнює або більша за 512 бітів.

Проведені дослідження принципів синтезу симетричних криптоперетворень показали, що нині необхідно виділити три методологічних підходи до побудови перспективних БСШ [9]. По суті, вони уже представлені кандидатами на стандарт БСШ Європейської програми NESSIE.

Перший пов’язаний з використанням SPN структур. Загальна структура – SPN, square-type, байт – байт-орієнтований шифр. На основі таких структур були розроблені та здобули визнання БСШ Rijndael та його звужена версія AES (FIPS – 197) [9, 37], що побудовані на основі попередньої розробки авторів – шифру Square. Цей напрям був достатньо досліджений і за їх результатами запропоновано кандидат національного стандарту БСШ “Калина” [39].

У процесі досліджень звернуто увагу на БСШ, що мають IDEA подібну структуру. Відомо, що де-факто Європейський стандарт IDEA пройшов тривале випробовування часом й досі забезпечує задекларований рівень стійкості. На початку XXI ст. Паскаль Юнод та Серж Воденей запропонували проект удосконаленого БСШ, що отримав назву FOX [40]. Алгоритм IDEA NXT (раніше відомий як FOX), являє собою блоковий симетричний шифр, що розробили Паскаль Юнод і Серж Воденей з лабораторії EPFL. Задуманий у період між 2001 і 2003 рр., проект спочатку називався FOX і був опублікований в 2003 р. У травні 2005 р. він був анонсований компанією MediaCrypt за назвою IDEA NXT. IDEA NXT є нащадком алгоритму IDEA і використовує розширену схему Лея-Массея, відому своєю стійкістю до криптоаналізу [9, 40]. Він є власністю швейцарської компанії MediaCrypt, якій належать права на поширення IDEA і яка є власником патентів на IDEA NXT. Шифр IDEA NXT являє собою сім’ю різних модифікацій шифрів з різними розмірами блоків і розмірами ключів: Standard NXT64 (64-бітовий блок, 128-бітовий ключ, 12 раундів) і Standard NXT128 (128-бітовий блок, bits, 256-бітовий ключ, 12 раундів). Можуть бути також побудовані версії Standard (з розміром ключа від 0 до 256 бітів, кількістю раундів від 2 до 255). А також можуть завантажуватися індивідуальні таблиці (sbox, матриця перестановок – permutation matrix), що заміняють стандартну таблицю.

В основу реалізації третього методологічного підходу покладено уже добре випробувану фейстельподібну схему [11, 12, 15–22]. Вона реалізована у випробуваних часом стандартах БСШ DES, DEA, TDEA, ГОСТ 28147–89, а також в MISTY1, Cammellia. Сьогодні стандарти БСШ, що мають фейстельподібну структуру, ще часто застосовуються на практиці та не втратили перспективу застосування, можливо, з деяким удосконаленням.

Отже, аналіз принципів проектування сучасних шифрів показав, що однією із найпоширеніших та найпотужніших сучасних концепцій проектування блокових симетричних шифрів є стратегія широкого сліду, що будується на основі матричного множення в розширених

полях. Її застосували розробники AES, що дало змогу обґрунтувати значення окремих показників ефективності БСШ, зокрема отримати просту специфікацію шифру, легку в аналізі із застосуванням прозорого та надійного математичного апарату. Вважається, що одним з додаткових проектних рішень у перспективних розробках має стати використання циклової функції з високими динамічними характеристиками переходу до сталих (стаціонарних) значень максимумів повних диференціалів і лінійних корпусів.

Під час проведення досліджень обґрунтовано загальну структуру, таблиці підстановки, блоки лінійного перетворення та схему вироблення підключів перспективного алгоритму блокового симетричного криптоперетворення “Калина”. Як нелінійні елементи шифру використані випадково сформовані таблиці підстановок, відібрані за критеріями стійкості до диференціального, лінійного криптоаналізу та ступеня нелінійності булевих функцій. Це дає змогу досягти високих показників захисту проти диференціального та лінійного криптоаналізу і водночас захиститися від потенційної можливості алгебраїчної атаки на такі шифри, як Rijndael, Camellia та ін. Як блок лінійного перетворення запропоновано використовувати добре перевірене МДВ [24, 25, 38] (перетворення, основане на використанні лінійних блокових кодів з максимально досяжною кодовою відстанню), що дозволяє досягти верхньої межі мінімальної “кількості гілок” за будь-якої (відмінної від нуля) вхідної різниці. Поширений вигляд вибраного перетворення дозволяє досягти вищих показників “кількості гілок” порівняно з БСШ Rijndael (9 проти 5). Завдяки використанню 64-бітного МДВ-коду забезпечується повна залежність кожного біта від входу вже на двох циклах шифрування, незалежно від розміру блока. Характеристики кращі, ніж у Rijndael 256/256, де потрібно більше циклів для поширення різниці на весь блок. В БСШ “Калина” ключова інформація вводиться за декількома метриками гамування, внаслідок чого криптографічний алгоритм переходить до класу немарковських шифрів і визначення ймовірності диференціальних (лінійних) характеристик має експонентний характер відносно складності, що робить проведення диференціального (лінійного) криптоаналізу за вибраними відповідно параметрами практично неможливим.

Отже, запропоновані удосконалення шифру Rijndael, реалізовані в шифрі “Калина”, дозволяють перекрити виявлені потенційні вразливості, які є в шифрі Rijndael, та зробити кандидат у національний стандарт блокового симетричного шифрування стійким відносно усіх відомих криптоаналітичних атак. Вказаний висновок підтверджено в роботах, що виконані в процесі експертизи та досліджень поданих на національний конкурс кандидатів.

Порівняльний аналіз сучасних БСШ за стійкістю

Відповідно до сформульованих вимог до блокових симетричних криптоперетворень, перспективні БСШ повинні забезпечувати стійкість до всіх відомих криптоаналітичних атак за ефективної програмної, апаратної та програмно-апаратної реалізації засобів захисту інформації. Проведемо порівняльний аналіз сучасних БСШ за критерієм криптографічної стійкості та за показниками швидкодії, обсягу пам’яті.

Порівняльний аналіз БСШ за критерієм криптографічної стійкості

Виконуючи порівняльний аналіз існуючих БСШ, необхідно визначити набір умов та вихідних даних, що використовуються для реалізації атаки. Зрозуміло, що криптоаналітик буде застосовувати найефективніший метод криптоаналізу, щоб мінімізувати матеріально-технічні ресурси, потрібні для успішного здійснення атаки. Визначається і потім застосовується найефективніший метод. Тобто, як правило, такий метод передбачає найменші фінансові і/або просторово-часові витрати порівняно з іншими методами аналізу.

Отже, ефективність методу криптоаналізу визначається можливістю застосування цієї атаки до БСШ для одержання секретного ключа або відкритого повідомлення зі складністю, меншою, ніж складність силової атаки. У зв’язку з цим оцінка ефективності методу криптоаналізу симетричного шифру може бути виконана тільки стосовно конкретного алгоритму або класу шифрів, що

використовують однакові принципи їх побудування. Але, незважаючи на вказане, базові принципи проведення криптоаналізу можна застосувати і для алгоритмів, що використовують різні принципи побудови. Ступінь застосовності різних методів проведення атаки відносно шифрів, що використовують різні принципи побудови, визначає універсальність методу криптоаналізу.

Оцінюючи криптографічну стійкість, необхідно враховувати, що деяка модифікація або доповнення алгоритму виконання криптоаналізу можуть істотно змінити складність проведення атаки. Так, використання 2R-атаки в диференційному криптоаналізі DES дало змогу зменшити складність і зробити цю атаку ефективнішою, ніж пряме перебирання ключів.

Тому, оцінюючи ефективність методу криптоаналізу, необхідно враховувати такі фактори:

− рівень доступності відкритих повідомлень для криптоаналітика;

− умови проведення атаки – можливість вибору значень на входах шифратора і/або залежностей між ними;

− перелік алгоритмів, відносно яких може бути застосований метод криптоаналізу;

− можливості вибору криптоаналітиком значень відкритих повідомлень;

− можливість та необхідність наявності у криптоаналітика фізичного доступу до обладнання;

− мінімальна складність виконання проведення атаки на повний шифр;

− універсальність методу криптоаналізу, тобто можливість його застосування до поширених шифрів.

Також необхідно враховувати, що універсальність, мінімальні вимоги до умов проведення атаки й низька складність збільшують ефективність методу криптоаналізу. Своєю чергою, необхідність наявності відкритих текстів, їх вибору або завдання залежності між секретними ключами знижує ефективність. Також вимога наявності фізичного доступу до обладнання істотно звужує спектр застосування методу криптоаналізу і, відповідно, також знижує його ефективність.

Як найефективніші методи криптоаналізу для більшості сучасних симетричних блокових алгоритмів, можна виділити диференційний криптоаналіз, лінійний криптоаналіз та алгебраїчні методи. Щодо алгоритму шифрування AES [37] додатково можна виділити інтегральний криптоаналіз і атаку з використанням нездійсненних диференціалів.

Нині БСШ AES (Rijndael, FIPS 197) став визнаним у світі БСШ, він стандартизований на міжнародному рівні і рекомендований міжнародним стандартом ISO/IEC 18033-3 як шифр, що забезпечує нормальний або високий рівні стійкості. Тому, використовуючи отримані результати досліджень, зробимо відносно БСШ AES деякі оцінки. Це необхідно для того, щоби показати, що уже в БСШ “Калина” потенційні вразливості AES перекриті.

Загалом щодо AES можна зробити такі висновки [9]:

1. Аналіз результатів дослідження стійкості алгоритму AES (FIPS 197), отриманих у ході виконання проектів AES і NESSIE, а також результати його випробовування часом показали, що він забезпечує необхідний рівень стійкості.

2. Для розв’язання задач криптоаналізу до алгоритму FIPS 197 можуть бути застосовані передусім такі атаки: атаки “грубої сили”, диференційний та лінійний криптоаналіз, атаки усічених і здійсненних диференціалів, бумеранг-атака, інтерполяційна атака й атака лінійних сум, атака диференціалів вищих порядків та інтегральний криптоаналіз.

3. Проведені теоретичні й експериментальні дослідження стійкості Fips 197 показали, що зазначені у пункті 1 висновків атаки можуть бути реалізовані зі складністю, яка порівнюється зі складністю атаки “груба сила”, тільки на зменшеній кількості циклів алгоритму. Так, можна реалізувати зі складністю меншої складності атаки “груба сила” відповідно: диференційний криптоаналіз – для трьох циклів, лінійний криптоаналіз – для трьох циклів, усічених диференціалів – для трьох циклів, неможливих диференціалів – для п’яти циклів, бумеранг-атака – для чотирьох циклів, диференціалів вищих порядків – для трьох циклів, інтерполяційна атака – для чотирьох циклів, інтегральний криптоаналіз – для шести циклів.

4. Аналіз даних табл. 2 дає підстави зробити висновок про стійкість алгоритму FIPS - 197 проти розглянутих криптоаналітичних атак. І більше, можна говорити про наявність визначеного запасу стійкості для алгоритму із заданою кількістю циклів перетворення – 10, 12 і 14, залежно від

довжини ключа – 128, 192 і 256 бітів відповідно. Наявність цього запасу дає змогу сподіватися, що алгоритм FIPS 197 буде залишатися безпечним протягом визначеного часу в майбутньому. І навіть більше, в БСШ Rijndael є можливості збільшення довжин шифрованих блоків до 192 та 256 бітів, що робить його стійкішим, ніж FIPS 197.

Таблиця 2

Аналіз криптостійкості алгоритму FIPS 197

Види криптоатак	Мінімальна кількість циклів, за якої шифр стійкий			Показники відомих атак на AES (Rijndael-128)		
	Rijndael-128	Rijndael-192	Rijndael-256	Максимальна кількість циклів	Обчисл. ресурси	Пам'ять
Диференційна	4	7	8	3	254	мало
Лінійна	4	7	8			
Усіч. дифер.	4	5	7	3	28	мало
Немож. дифер.	6	6	6	5	236	224
Бумеранг	5	6	7			
Диф. вищ. пор.	4	4	4			
Інтерполяційна	5	5	5			
Інтегральна	7	7	7	6	272	232

Одним із основних безумовних критеріїв оцінки БСШ є критерій захищеності шифру від усіх відомих і потенційно можливих криптоаналітичних атак. Він є безумовним у тому сенсі, що якщо алгоритм шифрування не задовольняє вимоги цього критерію, то алгоритм шифрування відкидається і не розглядається як претендент. Алгоритм шифрування вважається стійким, якщо всі відомі криптоаналітичні атаки мають більшу складність, ніж складність атаки типу "груба сила".

Важливим умовним критерієм є реальна захищеність від відомих криптоаналітичних атак за зменшеної кількості циклів. Річ у тім, що відповідно до безумовного критерію шифри Rijndael, Shacal-2 і Camellia на повній кількості циклів є стійкими проти всіх відомих атак. Тому одним із критеріїв порівняльної оцінки шифрів є порівняння за мінімумом циклів, за якого жоден з методів криптоаналізу не має складність, меншу, ніж складність атаки типу "груба сила". Тому важливими є задачі оцінки криптографічної стійкості алгоритму симетричного шифрування Rijndael (FIPS 197) проти відомих криптоаналітичних атак, зокрема з оцінкою мінімальної кількості циклів, за якої забезпечується стійкість.

Аналіз робіт [11–40] показав, що вже розроблено більше ніж 10 методик виконання криптоаналізу блокових симетричних шифрів, які можна застосувати й до алгоритму Rijndael.

Серед криптоаналітичних атак для обов'язкового розгляду вибрано атаки "грубої сили", диференційний та лінійний криптоаналіз, атаку усічених диференціалів, атаку нездійсненних диференціалів, бумеранг-атаку, інтерполяційну атаку, атаку лінійних сум, атаку диференціалів вищих порядків та інтегральний криптоаналіз.

На наш погляд, для виконання оцінки стійкості відносно кожної із цих атак спочатку необхідно провести огляд відомих методів, що дають змогу виконати оцінку стійкості шифру AES до цієї атаки. Потім, зважаючи на можливості реалізації на практиці й точність одержуваної оцінки необхідно вибрати найефективнішу методику виконання оцінки стійкості та застосувати її для аналізованого шифру. Крім цього, з метою вивчення найефективніших методів криптоаналізу необхідно реалізувати їх для шифру AES зі зменшеною кількістю циклів.

Більшість атак "грубої сили" можна застосувати до будь-якого блокового шифру, і складність цих атак залежить тільки від довжини блока n або довжини ключа k і не залежить від структури алгоритму.

Атака повного перебору ключів є найпростішим способом пошуку ключа шифрування. Складність такої атаки залежить від довжини ключа і, як відомо, не менша, ніж $2k - 1$ шифрувань за

допомогою досліджуваного шифру. Для забезпечення захищеності від цієї атаки у шифрах використовують ключі великого розміру. Оскільки мінімальна довжина ключа шифру AES становить 128 бітів, то вичерпний пошук ключа вимагає 2128 шифрувань і на практиці нездійсненний.

До словникової атаки уразливі шифри з недостатньою довжиною блока. Для виконання атаки потрібна таблиця розміром 2n блоків, а для побудови такої таблиці необхідно 2n шифрувань. Мінімальна довжина блока розглянутого шифру – 128 бітів, отже, атака зі словником 2128 також на практиці нездійсненна.

Далі вважатимемо, що алгоритм захищений від деякої криптоаналітичної атаки, якщо її реалізація перевищує або дорівнює складності атаки "грубої сили". Найбільш відомими і потужними методами виконання атак на БСШ є запропоновані на початку 90-х диференційний криптоаналіз та лінійний криптоаналіз [18 – 21].

Відомі чотири критерії стійкості n-бітового шифру до цих криптоатак:

– точний критерій – максимальне значення ймовірностей диференціалів і шаблонів лінійної апроксимації нижче ніж 2–n;

– теоретичний критерій – верхні межі значень ймовірностей диференціалів і шаблонів лінійної апроксимації нижчі, ніж 2–n;

– евристичний критерій – максимальні ймовірності диференційних та лінійних характеристик нижчі, ніж 2–n;

практичний критерій – верхні границі ймовірностей диференційних та лінійних характеристик нижчі за 2–n.

Ідеальним варіантом, з погляду перевірки можливості виконання диференційного або лінійного криптоаналізу, є перевірка точного критерію. Створення теоретично стійкого SPN-шифру на основі відомих теорем поєднано з доволі твердими вимогами до використовуваного в кожному циклі перетворення, що призводить до уповільнення процедури шифрування.

Перевірка евристичного критерію застосовна для шифрів з невеликим розміром блока (не більше ніж 64 біти), наприклад DES, FEAL, і потребує при цьому значних обчислювальних ресурсів. Для шифру Rijndael, розмір блока якого не менше ніж 128 бітів, розглянутий алгоритм вимагає занадто великих обчислювальних ресурсів, що майже неможливо реалізувати на практиці.

Підсумком оцінки стійкості шифру Rijndael до атак ДК і ЛК є висновок про те, що шифр відповідає практичному критерію стійкості до лінійного та диференційного криптоаналізу.

Разом з тим попередній аналіз показує, що Rijndael (FIPS 197) мають потенційні вразливості, зокрема:

– виявлено декілька нових властивостей компонентів і всього алгоритму, наприклад лінійна збитковість підстановки (S-блока);

– наявність можливості алгебраїчного подання циклової функції з усіма операціями в одному полі;

– можливість побудови системи рівнянь, які описують увесь шифр за допомогою ланцюгових дробів;

– можливість побудови перевизначеної системи рівнянь для усього шифру.

Але, незважаючи на вказані потенційні вразливості, використання кожної із них для аналізу всього алгоритму невідоме. Практичне використання вказаних особливостей відносно всього алгоритму невідоме. І навіть більше, немає математичного апарату для розв'язання спеціальних систем рівнянь у вигляді ланцюгових дробів.

Загалом вказане свідчить про те, що на основі SPN може бути побудований стійкий шифр.

Порівняльний аналіз сучасних БСШ щодо швидкодії та обсягу пам'яті

Однією з основних характеристик криптографічного примітиву також є його продуктивність з програмною реалізацією для універсальної платформи. Вища продуктивність за аналогічного або вищого рівня криптографічної стійкості є важливою перевагою алгоритму.

Проведемо порівняльний аналіз швидкодії та обсягу необхідної пам’яті для реалізації сучасних БСШ та обґрунтуємо вибір найвдалішого рішення.

Під час тестування продуктивності блокового шифру враховано такі фактори:

− варіативність часу виконання шифрування залежно від потенційної активності інших процесів / потоків у операційній системі загального призначення;

− залежність швидкості перетворення від наявності даних у кеші процесора;

− можливість істотного уповільнення процесу шифрування за необхідності використання файла віртуальної пам'яті операційної системи.

Варіативність часу виконання зменшувалася за рахунок багаторазового (не менше ніж 100 тис. разів) вимірювання часу шифрування і подальшого усереднення результатів.

Забезпечення продуктивності алгоритму шифрування, близької до реальних умов (обробка мережевого трафіку, дискового введення / виводу тощо), здійснювалося за рахунок обробки блока оперативної пам'яті в кілька десятків мегабайт. Таке значення гарантує відсутність даних у кеші й необхідність їх завантаження з ОЗП, що дає змогу отримати швидкісні характеристики, відповідні прикладному застосуванню шифру.

Водночас розмір оброблюваного блока дорівнює декільком десяткам мегабайтів, не вимагає використання файла віртуальної пам'яті операційної системи (в умовах відсутності інших додатків, які активно використовують ОЗП), що забезпечує тестування продуктивності тільки в межах процесора й оперативної пам'яті, без значно повільнішої дискової підсистеми.

Порівняння продуктивності здійснено для алгоритмів “Калина”, ГОСТ 28147 89 (чинний стандарт, рекомендований до застосування в Україні, і використовуваний в Росії), СТБ 34.101.31-2011 (Бел-Т, стандарт Республіки Білорусь) і AES (національний стандарт США і найпоширеніший алгоритм у світі). Теоретичний розрахунок кількості необхідних процесорних інструкцій для обробки одного байта даних наведено в табл. 3.

Водночас, сучасні процесори дають змогу апаратно оптимізувати продуктивність за рахунок перекодування і переупорядкування інструкцій, використовувати їх паралельне виконання всередині одного потоку тощо. Крім того, дуже велике значення має блок оптимізації компілятора, що дозволяє значно підвищити продуктивність за рахунок розгортання циклів (відсутності скидання конвеєра за умовного переходу) тощо. Тому без детального знання внутрішньої архітектури процесора, доступної тільки компаніям-розробникам (Intel, AMD й ін.), і особливостей оптимізаторів компіляторів, оцінити реальну продуктивність можна тільки за допомогою експериментальних вимірювань.

Таблиця 3

Теоретичний розрахунок кількості необхідних процесорних інструкцій для обробки одного байта різними шифрами

	Симетричний блоковий шифр			
	Калина (128/128)	ГОСТ 28147-89	СТБ 34.101.31-2011	AES
Кількість операцій на 1 байт	40,375	72	40,5	45,375

Вимірювання продуктивності блокових шифрів проводилися на таких програмно-апаратних платформах:

– Intel Core i5 / Windows Server 2008 R2 x64 з компілятором Visual C + + 2008;

– Intel Core 2 Duo E8500 / Linux (64 біт) з компілятором GCC останньої версії.

Для вимірювання швидкодії були взяті найбільш швидкодіючі реалізації блокових шифрів мовою C / C ++: AES – з криптографічної бібліотеки OpenSSL; ГОСТ 28147-89 – з бібліотеки АТ “ІІТ”; “Калина” – авторська реалізація. Дані щодо виміряної продуктивності наведено в табл. 4.

Отже, продуктивність перспективного блокового шифру “Калина” на 64-бітовій платформі значно вища, ніж у чинного в Україні та Росії стандарту ГОСТ 28147-89, а також стандарту Республіки Білорусь СТБ 34.101.31-2011. На цій платформі “Калина” має також перевагу в продуктивності та порівняно з алгоритмом AES з аналогічною довжиною ключа (забезпечуючи водночас значно більший запас криптографічної стійкості).

Таблиця 4

Продуктивність блокових шифрів, Мбіт/с

Платформа	Симетричний блоковий шифр								
	K128/128	K128/256	K-256/256	K-256/512	K-512/512	AES-128	AES-256	ГОСТ	СТБ
Win2008Srv	1538,31	1098,17	1256,23	977,61	995,72	1483,26	1095,19	376,3	609,18
Linux	1828,57	1291,72	1219,05	948,15	948,15	1667,95	1254,01	492,31	753,5

Проведемо порівняльні дослідження обсягів пам'яті, які необхідно виділити в обчислювальній системі для реалізації відповідних алгоритмів блокового симетричного шифрування.

Попередній аналіз показує, що для збільшення продуктивності комп'ютерів, тимчасового зберігання вмісту оперативної пам'яті, прискорення обміну між процесором і постійним запам'ятовувальним пристроєм у сучасних високошвидкісних обчислювальних системах застосовується принцип ієрархічності пам'яті, який полягає в послідовному збільшенні обсягів запам'ятовувальних пристроїв (із певним зменшенням швидкодії) впродовж "віддалення" від центрального процесорного пристрою. Найшвидшою та, відповідно, найдорожчою та найменшою за обсягом пам'яттю є внутрішня пам'ять процесора (регістри, організовані в регістровий файл і кеш процесора). Щоб максимізувати швидкість реалізації криптографічних алгоритмів, бажано максимально застосовувати можливості саме цієї пам'яті, бо в цьому випадку швидкість обчислень буде оптимізовано відповідно до певної конфігурації системи.

Проведені дослідження показали, що більшість провідних світових виробників сучасних процесорів виготовляють різні за призначенням та за технічними характеристиками вироби, які відрізняються як обсягом кешу другого та третього рівнів, так і тактовою частотою і відповідною тепловою потужністю. Однак за обсягом кеш-пам'яті першого рівня практично всі сучасні процесори мають однакові обмеження обсягу кеш-пам'яті 1-го рівня, що становлять 64 кБайт.

Отже, загальні вимоги до сучасних криптоалгоритмів стосовно обсягу пам'яті передбачають обмеження в 64 кБайт, тобто розмір таблиць передобчислювань для швидкої реалізації шифрів не повинен перевищувати обсяг пам'яті кешу першого рівня. Це є основною вимогою до обсягу пам'яті перспективного блокового симетричного шифру, бо у разі виконання встановлених вимог всі таблиці передобчислень можуть бути поміщені в кеш першого рівня і продуктивність реалізації буде максимальною.

Обсяг таблиць передобчислень визначається такими рівняннями:

мінімальний обсяг пам'яті

$$V_{min} = k \cdot 2^t \cdot s; \quad (1)$$

обсяг пам'яті, необхідний для досягнення максимальної швидкодії

$$V_{max} = 2^t \cdot s^2, \quad (2)$$

де k – кількість нелінійних вузлів замість (S-блоків), які необхідно зберігати в пам'яті; t – розрядність входу S-блока, бітів; s – розрядність МДР-матриці, байтів.

Із застосуванням наведених формул підрахуємо обсяг таблиць передобчислень та порівняємо його із обсягом кеш-пам'яті першого рівня більшості сучасних процесорів (обмеження в 64 кБайт).

Маємо такі показники:

для блокового симетричного шифру AES

$$V_{min} = k \cdot 2^t \cdot s = 1024; \quad (3)$$

$$V_{max} = 2^t \cdot s^2 = 4096, \quad (4)$$

для блокового симетричного шифру "Калина-2"

$$V_{min} = k \cdot 2^t \cdot s = 8192; \quad (5)$$

$$V_{max} = 2^t \cdot s^2 = 16384, \quad (6)$$

для блокового симетричного шифру “Кузнечик”

$$V_{min} = k \cdot 2^t \cdot s = 4096, \quad (7)$$

$$V_{max} = 2^t \cdot s^2 = 65536. \quad (8)$$

Отже, як показують проведені дослідження блокові симетричні шифри AES та “Калина” відповідають обмеженням на обсяг пам’яті кешу першого рівня, тобто їх практична реалізація дозволяє максимально застосовувати можливості цієї найшвидшої пам'яті й швидкість обчислень буде оптимізовано відповідно до певної конфігурації системи. Особливості побудови перспективного блокового шифру РФ “Кузнечик” такі, що обсяг пам’яті, необхідний для досягнення максимальної швидкодії, лежить на верхній межі обсягу пам’яті кешу першого рівня. Практично це означає, що під час обробки (шифрування) дані витіснятимуть таблиці передобчислень з необхідністю їх повторного завантаження, і це призводитиме до зниження продуктивності.

Отримані результати дають підстави зробити висновки [39], що продуктивність перспективного блокового шифру “Калина” на 64-бітовій платформі значно вища, ніж у чинного в Україні та Росії стандарту ГОСТ 28147-89, а також стандарту Республіки Білорусь СТБ 34.101.31-2011. На цій платформі “Калина” має також перевагу в продуктивності й порівняно з алгоритмом AES з аналогічною довжиною ключа (водночас забезпечуючи значно більший запас криптографічної стійкості).

Також проведені порівняльні дослідження показали, що блокові симетричні шифри AES та “Калина” відповідають обмеженням на обсяг пам’яті кешу першого рівня сучасних процесорів. Практична реалізація цих шифрів дасть змогу максимально застосовувати можливості цієї найшвидшої кеш-пам'яті й застосовувані обчислення будуть оптимізовані відповідно до певної конфігурації системи.

Висновки

Сучасний алгоритм симетричного блокового криптографічного перетворення повинен відповідати обґрунтованому переліку вимог, а саме: забезпечення гарантованого рівня стійкості; високої продуктивності за програмної, програмно-апаратної та апаратної реалізації; порівняно простої та прийнятної за вартістю реалізації засобів КЗІ.

Наведений аналіз принципів проектування сучасних шифрів показав, що однією із найпоширеніших та найпотужніших сучасних концепцій проектування блокових симетричних шифрів є стратегія широкого сліду, основана на матричному множенні в розширених полях. Її застосували розробники AES, що дало змогу обґрунтувати значення окремих показників ефективності БСШ, зокрема отримати просту специфікацію шифру, легку в аналізі із застосуванням прозорого та надійного математичного апарату.

Під час проведення досліджень було проаналізовано принципи проектування перспективного блокового симетричного алгоритму, обґрунтовано загальну структуру, таблиці підстановки, блоки лінійного перетворення та схему вироблення підключів шифру. Як нелінійні елементи шифру використані випадково сформовані таблиці підстановок, що відібрані за критеріями стійкості до диференціального, лінійного криптоаналізу та ступеня нелінійності булевих функцій. Це дає змогу досягти високих показників захисту проти диференціального та лінійного криптоаналізу і водночас з тим захиститися від потенційної можливості алгебраїчної атаки. Отже, запропоновані удосконалення шифру Rijndael, реалізовані в шифрі Калина, дозволяють перекрити виявлені потенційні вразливості, наявні в шифрі Rijndael, та зробити кандидат у національний стандарт блокового симетричного шифрування стійким відносно усіх відомих криптоаналітичних атак.

1. Указ Президента України від 08.07.2009 р. № 514 “Про Доктрину інформаційної безпеки України”. 2. Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженого Указом Президента України від 22.05.98 р. № 505. 3. Закон України “Про основи

національної безпеки України" від 19.06.2003 р. № 964-IV. 4. Закон України "Про інформацію" від 02.10.1992 р. № 2657-XII. 5. Закон України "Про електронний цифровий підпис" від 22.05.2003 р. № 852-IV. 6. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.1994 р. № 80/94-ВР. 7. Закон України "Про Національну систему конфіденційного зв'язку" від 10.01.2002 р. № 2919-III 8. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. – Харків: Форт, 2010. – 593 с. 9. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: монографія. – Харків, ХНУРЕ, Форт, 2012. – 868 с. 10. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20.07.2007 р. № 141, зареєстроване в Міністерстві юстиції України 30 липня 2007 р. за № 862/14129. 11. FIPS 46, "Data encryption standard", Federal Information Processing Standards Publication 46, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977 (revised as FIPS 46-1:1988; FIPS 46-2:1993). 12. FIPS 81. DES modes of operation. Federal Information Processing Standards Publication 81, U.S. Department of Commerce / National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1980. 13. Хоффман Л. Современные методы защиты информации / пер. с англ. – М. Сов. радио, 1980. – 264 с. 14. W. Diffie, M.E. Hellman Exhaustive cryptanalysis of the NBS Data Encryption Standard Computer. – 10 (1977).– P. 74–84. 15. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2002. – 797 с. 16. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР. 17. K. Kusuda and T. Matsumoto Optimization of time-memory trade-off cryptanalysis and its application to DES, FEAL-32, and Skipjack' //IEICE Transactions on Fundamentals of Electronics. – 1996. – P. 35–48. 18. M. Matsui. Linear Cryptanalysis Method for DES Cipher, EUROCRYPT'93, pp. W112-W123, May 1993. 19. E. Biham, A. Shamir Differential cryptanalysis of DES-like cryptosystems //Advances in Cryptology. – CRYPTO '90 (LNCS 537) 1990. – P. 2–21. 20. E. Biham, A. Shamir Differential Cryptanalysis of the Data Encryption Standard // SpringeríVerlag, New York. – 1993. 21. Biham, A. Shamir Differential cryptanalysis of the full 16-round DES // Advances in Cryptology. – CRYPTO '92 (LNCS 740). – 1993. – P. 487–496. 22. J.H. Moore and G.J. Simmons Cycle structure of the DES for keys having palindromic (or antipalindromic) sequences of round keys // Advances in Cryptology – CRYPTO '86.– 1987.– P. 9–32. 23. D. Coppersmith The real reason for Rivest's phenomenon //Advances in Cryptology – CRYPTO '85 (LNCS 218).– 1986.– P. 535–536. 24. Daemen, R. Govaerts, J. Van Weak keys for IDEA // Advances in Cryptology. – CRYPTO '93 (LNCS 773). – 1994. – P. 224–231. 25. E. Biham New types of cryptanalytic attacks using related keys // Advances in Cryptology. – Proceedings Eurocrypt'93. – LNCS 765. – 1993. – P. 398–409. 26. X. Lai, J.L. Massey. Hash Function Based on Block Ciphers // Workshop on the Theory and Applications of Cryptographic Techniques. EUROCRYPT'92. – 1992. – P. 53–66. 27. L.R. Knudsen Practically secure Feistel ciphers // Fast Software Encryption. – 1994. – P. 211–221. 28. R. Winternitz Producing One–Way Hash Function from DES // Advances in Cryptology: Proceedings of Crypto 83, Plenum Press. – 1984. – P. 203–207. 29. E. Biham New types of cryptanalytic attacks using related keys // Advances in Cryptology.– Proceedings Eurocrypt'93. – LNCS 765. – 1993. – P. 398–409. 30. J. Daemen, R. Govaerts, J. Van Weak keys for IDEA // Advances in Cryptology.– CRYPTO '93 (LNCS 773). – 1994. – P. 224–231. 31. L.R. Knudsen Block Ciphers – Analysis, Design and Applications. – PhD thesis. – Computer Science Department, Aarhus University, Denmark. – 1994. 32. L.R. Knudsen A key-schedule weakness in SAFER-K64 // Advances in Cryptology. – Proceedings Crypto'95. – LNCS 963. – 1995. – P. 274–286. 33. D.R. Stinson Cryptography: Theory and Practice. CRC Press, Boca Raton, Florida. – 1995. 34. B. S. Kaliski J. R. and Y. L. Yin On differential and linear cryptanalysis of the RC5 encryption algorithm // Advances in Cryptology. – CRYPTO '95 (LNCS 963). – 1995. – P. 171–184. 35. C. Harpes and J. L. Massey Partitioning Cryptanalysis // Fast Software Encryption. – 4th International Workshop, FSE'97. – Volume 1267 of Lecture Notes in Computer Science. – P. 13–27. 36. J. Daemen. Annex to AES Proposal Rijndael. http://www.nist.gov/aes 37. National Institute of Standards and Technology, FIPS 197: "Advanced Encryption Standard." Nov. 2001. http://www.nist.gov/aes 38. ISO/IEC 18033-3:2006 Information technology – Security techniques –

Encryption algorithms – Part 3: Block ciphers. 39. Горбенко И. Д., Долгов В. И., Олейников Р. В, Руженцев В. И., Михайленко М. С., Горбенко Ю. И., Тоцкий А. С., Казмина С. В. Перспективный блочный шифр "Калина" – основные положения и спецификация // Прикладная радиоэлектроника, 2007, №2. 40. IDEA NXT Technical Description, MediaCrypt, W W W. M E D I A C R Y P T. C O M, 2005 Надійшла до редколегії 2014 41. ISO/IEC 10116. Information technology – Security techniques – Modes of operation for an n-bit block cipher.

УДК 681.3

С. А. Лупенко, Н. Р. Шаблій, А. М. Лупенко
Тернопільський національний технічний університет імені Івана Пулюя

КОМПАРАТИВНИЙ АНАЛІЗ МОДЕЛЕЙ, МЕТОДІВ ТА ЗАСОБІВ АУТЕНТИФІКАЦІЇ ОСОБИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗА ЇЇ КЛАВІАТУРНИМ ПОЧЕРКОМ

Проаналізовано моделі, методи та засоби аутентифікації користувачів комп'ютерів за їх клавіатурним почерком. Виявлено недоліки наявних математичних моделей та методів опрацювання даних клавіатурного почерку. Сформульовано актуальні завдання подальших наукових досліджень у цій сфері інформаційної безпеки.

Ключові слова: біометрична аутентифікація, клавіатурний почерк, математичне моделювання.

COMPARATIVE ANALYSIS OF MODELS, METHODS AND TOOLS OF PERSONAL AUTHENTICATION IN INFORMATIONAL SYSTEMS AFTER KEYBOARD RHYTHM

The article analyzes the models, methods and means of authentication of computer users by their handwriting keyboard. Identified deficiencies of existing mathematical models and methods of data processing keyboard writing. Formulated topical problems of further research in the field of information security.

Key words: biometric authentication, computer handwriting, mathematical model.

Вступ

Інтенсивний розвиток засобів телекомунікацій, локальних та глобальних комп'ютерних мереж стимулює в останнє десятиліття інтенсивний розвиток технологій зберігання та опрацювання даних з використанням віддалених ресурсів – GRID та хмарних технологій, що, своєю чергою, призводить до того, що проблеми захисту інформації у цих системах виходять на перше місце. Захист інформації – це комплекс заходів, спрямованих на запобігання несанкціонованому витоку, модифікації та видаленню інформації, здійснюваним із застосуванням технічних, зокрема програмних, засобів. Враховуючи різноманіття потенційних інформаційних загроз, складність їх структури і функцій, а також участь людини в технологічному процесі опрацювання інформації, збереження і конфіденційності останньої можна досягти, лише створивши комплексну систему захисту інформації.