decoding. Assessment the strength is offered, including quantum cryptanalysis, and evaluating performance in comparison with the known cryptosystems.

Key words: *code-based cryptosystems, post-quantum period, algebraic coding.*

Одержано 23.03.2017

УДК 681.3.06

К. Є. Лисицький, аспірант

Харківський національний університет імені В. Н. Каразіна, м. Харків

ОПТИМІЗАЦІЯ ПЕРСПЕКТИВНИХ АЛГОРИТМІВ СИМЕТРИЧНОГО БЛОЧНОГО ПЕРЕТВОРЕННЯ ПО КРИТЕРІЯМ ШВИДКОДІЇ І СТІЙКОСТІ

Розглядаються принципи побудови шифру Rijndael, застосовані розробниками, що дозволили цього шифру зайняти лідируючі позиції в технологіях проектування та розробки блокових симетричних шифрів. Як друга прогресивна розробка відзначається шифр IDEA NXT. Наводяться результати аналізу перспективності рішень, прийнятих у цих розробках. Відзначається, що, незважаючи на їх новизну і досягнуті високі показники ефективності розглянутих рішень, дослідження, проведені останнім часом, свідчать про можливості їх подальшого поліпшення, про можливості побудови більш досконалої конструкції шифрувального перетворення. Ці можливості враховані в запропонованій новій концепції проектування блочних симетричних шифрів, що будується на ряді висунутих положень. Її реалізація демонструється на прикладі розробки однієї з нових конструкцій шифру і його модифікації, побудованих на основі використання принципів керованих підстановлювальних перетворень. Запропоновані конструкція за простотою і прозорістю рішень, за показниками доказової стійкості до атак диференціального і лінійного криптоаналізу, а також за показниками продуктивності не поступаються визнаному лідеру технологій блочного симетричного шифрування шифру Rijndael (AES), а по динаміці приходу шифру до стану випадкової підстановки вони перевершують практично всі відомі рішення.

Ключові слова: *технології проектування і розробки блочних симетричних шифрів, матричне лінійне перетворення, ефективність шифруючого перетворення, нова концепція проектування і розробки БСШ, лінійне перетворення з керуючими підстановками, випадкові підстановки, динамічні показники приходу шифру до випадкової підстановки.*

Розглядаються конструкції двох сучасних розробок з побудови блочних симетричних шифрів: шифр Rijndael і шифр IDEA NXT. Розглядаються також свіжі розробки — шифри Мухомор, Калина-2 і бі-

лоруський шифр. Наводяться результати аналізу перспективності рішень, прийнятих в цих розробках.

На основі аналізу цих розробок визначається стан сучасних технологій проектування БСШ (орієнтуючись на найбільш прогресивні з них) наступними основними положеннями.

1. Вважається, що показники стійкості шифрів до атак диференціального і лінійного криптоаналізу безпосередньо пов'язані зі значеннями диференціальних і лінійних ймовірностей входять до шифрів нелінійних перетворень (*S*-блоків). Тому в криптографічній літературі вже давно і інтенсивно розвивається науковий напрям досліджень, пов'язаний з розробкою і пошуком *S*-блоків з поліпшеними криптографічними показниками.

2. Найбільш прогресивні рішення з побудови БСШ пов'язані з реалізацією ітеративної багатоциклічної процедури з використанням лінійного перетворення, що реалізує стратегію широкого сліду (Rijndael, IDEA NXT, Лабіринт, Камелія, Калина, Мухомор, Grand Cru, Кузнечік і ін.).

3. Практика побудови блокових шифрів визначила число використовуваних циклів шифрування (запас стійкості), в 3–4 рази перевищує глибину лавинного ефекту (число циклів, необхідне для приходу шифру до стану випадкової підстановки).

4. Застосовані в відомих шифри конструкції циклових перетворень забезпечують прихід шифрів до стану випадкової підстановки за мінімальне число циклів, що перевершує два-три (виняток становить алгоритм блочного шифрування з білоруського стандарту).

5. Досягнуті показники по швидкодії шифрів характеризуються граничним значенням питомих витрат XOR операцій (тактів), що припадають на один *S*-блок, з урахуванням процедур введення циклових підключів, близьким до одиниці (без урахування витрат на виконання процедури розгортання ключів).

6. У всіх шифри останніх розробок використовуються схеми розгортання ключів 2-го або 3-го типу, які представляються сильно ускладненими. Існуюча концепція побудови схем розгортання ключів орієнтована на реалізацію процедур, що наближаються за своїми властивостями до додаткового шифрувальні перетворення.

Відмічається, що, незважаючи на новизну й досягнуті високі показники ефективності розглянутих рішень, дослідження, проведені в останній час, свідчать про можливість їх подальшого покращення, про можливість побудування більш досконалих конструкцій шифруючих перетворень. Ці можливості враховані у новій концепції проектування блочних симетричних шифрів, що пропонується в роботі, основним змістом котрої є побудування перших циклів шифрів таким чином, щоб активізувалися майже усі їх *S*-блоки.

Проведені до теперішнього часу результати досліджень дозволяють сформулювати вихідні положення цієї концепції у вигляді наступних положень.

1. Всі сучасні ітеративні шифри незалежно від використовуваних в них S-блоків (підстановлювальних перетворень) на полноцикловій довжині за комбінаторними показниками, а також за диференціальними та лінійними показників стають випадковими підстановками.

2. Підстановлювальні перетворення впливають лише на динаміку переходу шифру до стану випадкової підстановки.

3. Динамічні показники приходу шифру до випадкової підстановці визначаються мінімальним числом активних *S*-блоків, що припадають на перші цикли перетворень, при цьому мінімальне число активних *S*-блоків першого циклу в більшості відомих конструкцій блокових симетричних шифрів дорівнює одному. Лінійні перетворення, що будується на основі МДР перетворень, не забезпечують активізацію всіх *S*-блоків другого і третього циклів.

4. Гранична кількість розгалужень (коли один *S*-блок активізує всі наступні *S*-блоки циклу) може бути реалізовано на основі конструкції лінійного перетворення, в якій забезпечується принцип послідовної активізації *S*-блоків циклової функції одного за іншим.

5. Для отримання шифрувального перетворення, яке стає випадковою підстановкою з другого або навіть з першого циклу необхідно перші два циклу будувати зі збільшеним по відношенню до традиційних підходів числом *S*-блоків кожної з цих циклових функцій, наступні цикли можуть бути побудовані, використовуючи стандартні (відомі) методи.

6. Конструкція циклової функції має дозволяти зробити участь всіх байтів входу до шифру в активізації *S*-блоків збалансованим в тому сенсі, що після двох, а в граничному випадку одного циклів перетворень все байти входу мають проходити набір активних *S*-блоків, що перевищує за кількістю їх мінімальне припустиме число.

7. Схеми розгортання ключів можуть бути побудовані з використання істотно спрощених підходів. Основна вимога до схем розгортання ключів це відсутність самоподібності в послідовності циклових підключів.

Для реалізації цього походу запропоновано використовувати три методи:

1) застосування на першому циклі замість прийнятого у відомих розробках паралельного запуску *S*-блоків циклової функції вхідними блоками даних операції послідовного їх запуску одного за іншим;
2) використання в першому циклі збільшеного числа S-блоків, що забезпечує при активізації всього їх безлічі граничні для шифру значення максимальних диференціальних і лінійних ймовірностей;
3) введення додаткового змішуючого перетворення на вході шифру.

Пропонується три методи побудування перших циклів шифрів, які демонструють реалізацію нової концепції проектування БСШ з підвищеною стійкістю і швидкодією.

При розробці першого рішення в основу покладені наступні критерії:

1) шифр має приходити до випадкової підстановки за мінімально можливе число циклів (у даному випадку за один-два цикли);
2) конструкція циклової функції має допускати конвеєрну обробку даних;
3) обчислювальна складність виконання операцій зашифрування і розшифрування має бути вища, ніж у відомих конструкцій шифрів з таким же розміром бітового входу;
4) схема розгортання ключів має бути простою й швидкодіючою. Основна вимога до цієї схеми – відсутність самоподібності циклових підключів.

Перша конструкція — це шифр з керованими підстановками ШУП-1, який дозволяє за рахунок додатного змішуванням сегментів даних на вході шифру, а також використання принципу послідовного запуску *S*-блоків активізувати вже на першому циклі шифрування майже всі 32 *S*-блоки циклової функції і при цьому на інших циклах шифрування шифр дозволяє здійснити конвеєрну обробку даних. Перетворення, що пропонується забезпечує приход до стану випадкової підстановки за два цикли, а за рахунок конвеєрної обробки даних дозволяє підвищити продуктивність майже у три рази.

Ми далі в умовах обмеженого обсягу матеріалу наводимо результати експериментів лише за оцінкою ефективності пропонованого рішення. У таблиці наведені результати обчислювального експерименту за визначенням закону розподілу числа *S*-блоків першого циклу, що активізуються в %. Підрахунок кількості *S*-блоків, що активізуються, проводився для кожного з 32-ох байт, при цьому для кожної різниці з множини 2^8 бітових сегментів перебиралися всі можливі пари сегментів. Як випливає з представлених результатів, на першому циклі з великою ймовірністю активізуються всі 32-а *S*-блоки. Такою ефективністю переперемішування не володіє жоден з відомих шифрів.

Таблиця

Закон розподілу числа S-блоків першого циклу, що активізуються в %

Кількість активних *S*-блоків першого циклу	**Частка від загального числа переходів**
0	0,0039
1	0
. . .	. . .
27	0
28	0,0000057

Продовження таблиці

29	0,000279
30	0,0070
31	0,1094
32	0,879

Друга конструкція — шифр ШУП-2 є розвитком першої пропозиції, і вона заснована на збільшенні кількості *S*-блоків першого циклу у два рази. При цьому активізується для 256-бітного шифру близько 64-х *S*-блоків цього циклу. Це дозволяє шифру стати випадковою підстановкою вже на першому циклі.

Третя пропозиція стосується використанню додатної операції змішування блоків даних на вході першого циклу вже існуючих БСШ, що дозволяє збільшити мінімальну кількість *S*-блоків першого циклу, що активізуються. Застосування цієї пропозиції до шифру Rijndael дозволяє суттєво підвищити показники випадковості цього шифру. Зокрема, удосконалений шифр гарантовано приходить до стану випадкової підстановки за два-три цикли як за диференціальними так і за лінійними показниками. Він за своїми криптографічними показниками перевершує новий український стандарт.

Четверта пропозиція стосується використанню додатної операції змішування блоків даних на вході першого циклу шифру Калина-2 (нового стандарту БСШ України).

Зокрема, представлені пропозиції щодо вдосконалення шифру Калина дозволяють використовувати в шифрі як вузли заміни випадкові *S*-блоки без зниження показників стійкості. Придатними для побудови вузлів заміни в цьому випадку є більше половини всієї множини байтових підстановок. Це більше 2^{1683} вузлів заміни. Якщо в шифрі використовуються різні підстановки, то їх ансамбль оцінюється числом 2^{6736} для чотирьох різних *S*-блоків і 2^{13464} для 8-ми різних підстановок.

Конструкції, що пропонуються за простотою і прозорістю рішень, за показниками доказової стійкості до атак диференціального і лінійного криптоаналізу, а також за показниками продуктивності за рахунок зменшення числа циклів шифрування перевищують визнаного лідера технологій блочного симетричного шифрування шифр Rijndael (AES), а за динамікою приходу шифрів до стану випадкової підстановки (мінімальному числу *S*-блоків першого циклу, що активізуються) вони перевершують практично усі відомі рішення.

Оригінальність запропонованих рішень підтверджена патентами [1, 2].

Список використаних джерел:

1. Пат. 111547 Україна, МПК (2016.01) G09C 1/00 H04L 9/06 (2006.01). Спосіб криптографічного перетворення двійкових даних (варіанти). Горбенко І. Д., Долгов В. І., Лисицька І. В. та інші (Україна); заявник АО ІІТ м. Харків. № a201500942; заявл. 06.02.2015; опубл. 10.05.2016, Бюл. № 9. 20 с.

2. Пат. 111448 Україна, МПК H04L 29/14 (2006.01) H04L 9/14 (2006.01) H04L 9/06 (2006.01). Спосіб криптографічного перетворення двійкових даних. Горбенко І. Д., Долгов В. І., Лисицька І. В. та інші (Україна); заявник АО ІІТ м. Харків. № a201503976; заявл. 25.04.2015; опубл. 25.04.2016, Бюл. № 8. 20 с.

The principles of construction Rijndael cipher, used by developers that allow this cipher take a leading position in technology design and development of block symmetric ciphers. As a second progressive development marked cipher IDEA NXT. The results of the analysis of the prospects of the decisions taken in these developments. It is noted that in spite of their novelty and achieved high performance solutions considered, studies conducted in recent years indicate the possibility of further improvement, the possibility of building a better design encryption transformation. These features included in the proposed new design concept of block symmetric cipher that is based on a number of provisions put forward. Its implementation is demonstrated by the example of the development of a new cipher designs and modifications, based on the principles of controlled use pidstanovlyuvalnyh change. The design of the simplicity and transparency of decisions in terms of evidence-based resistance to attack by differential and linear cryptanalysis, and in terms of performance is not inferior to the acknowledged leader of technology block symmetric encryption cipher Rijndael (AES), and the dynamics coming cipher to a state of random permutation they are superior to almost all known solutions.

Key words: *technology design and development of block symmetric ciphers, linear matrix conversion efficiency encrypting conversion, the new concept of design and development BSSH linear transformation of keruyemymy substitutions, random substitution cipher dynamic performance coming to vypadkovoi substitution.*

Одержано 24.02.2017

УДК 004.04:004.056.5

Н. О. Маслова, канд. техн. наук, доцент

Донецький національний технічний університет, м. Покровськ

ЗАСТОСУВАННЯ ЗАДАЧІ РОЗПОДІЛУ РЕСУРСІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Проаналізовано застосування задач розподілу ресурсів в системах захисту інформації та методів їх вирішення; описано програмне забезпечення, яке дозволяє проводити експериментальні дослідження з вибору ефективного за часом алгоритму.

Ключові слова: *розподіл ресурсів, захист інформації, метод, програмний продукт.*

Вступ. Задача розподілу ресурсів — одна з найважливіших задач прикладного спрямування кібернетики, що використовується для вирішення безлічі практичних проблем. Це задачі розподілу грошових коштів; матеріальних запасів; водних потоків; мережевих ресурсів. Розподі-

