УДК 004.056.55

ДОСЛІДЖЕННЯ ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЕРСПЕКТИВНИХ ПОТОКОВИХ ШИФРІВ

С.С. ТІМОХІН, І.Д. ГОРБЕНКО

Потокові симетричні шифри відіграють важливу роль для захисту інформації, для якої висуваються значні вимоги до рівня стійкості та швидкості обробки в режимі он-лайн. Апаратно орієнтовані потокові шифри мають забезпечувати достатній рівень стійкості, швидкодії та бути компактними при апаратній реалізації. Нелінійні регістри зсуву є одним з підходів побудови апаратних шифрів, що є на сьогодні мало дослідженим і вимагає уваги.

Ключові слова: потокове шифрування, нелінійні регістри зсуву.

ВСТУП

Симетричні криптографічні примітиви шифрування поділяються на потокові на блокові шифри. Основні принципи побудови та аналізу безпеки блокових симетричних шифрів (БСШ) є добре вивченими та дослідженими, на відміну від потокових симетричних шифрів (ПСШ). Теоретично, БСШ можуть надійно виступати як потоковий шифр (генерування гами) у режимі OFB та CFB [3], тому виникає питання про доцільність розробки, вивчення та дослідження методів побудови, оцінки безпеки та аналізу ПСШ. Практично ж, потокові симетричні шифри використовуються у тих випадках, де використання класичних блокових шифрів є неефективним. Наприклад, у режими реального часу, коли швидкість роботи системи є одним з основних критеріїв її ефективності. У такому випадку, спеціально розроблені ПСШ працюють набагато швидше, ніж БСШ у режимах OFB та CFB. Тому, під час розробки таких шифрів, до них висувають жорсткі вимоги щодо швидкодії при програмній реалізації та розміру (а, відповідно, і вартості).

Найбільшим поштовхом для розвитку ПСШ був проект eSTREAM (2004 – 2008 рр.), після того, як були знайдені уразливості в актуальних ПСШ (наприклад, SNOW). Метою цього проекту була розробка швидких та ефективних програмних шифрів і невеликих та надійних апаратних шифрів. На сайті проекту можна знайти роботи, присвячені ПСШ, що проходили відбір за двома критеріями: програмні та апаратні шифри. Кращими програмними шифрами було обрано HC, Rabbit, Salsa, Sosemanuk та кращими апаратними шифрами було обрано Grain, Trivium та Mickey.

1. СТИСЛІ ВІДОМОСТІ ПРО ПОТОКОВІ ШИФРИ

Відомо, що шифром з абсолютною стійкістю є шифр Вернама (One-time Pad). Недоліком цього шифру є те, що довжина ключа має бути не меншою, ніж довжина повідомлення. Зберігати такий ключ дуже важко, тому інженери намагаються розробити деякий генератор гами, що відповідав би певним вимогам, та розгортав би з невеликого ключа та вектора ініціалізації досить велику псевдовипадкову послідовність. Шифр Вернама можна записати у вигляді (1)

$$E:\{0,1\}\times\{0,1\}\to\{0,1\},(m,k)\to m\oplus k\,, \qquad (1)$$

де m та k є відкритий текст та ключовий потік відповідно. Процедури шифрування (2) та розшифрування (3) можна записати у вигляді

$$E_{k_i}(m_i)=m_i\oplus k_i=c_i\,, \qquad (2)$$

$$D_{k_i}(m_i)=c_i\oplus k_i=m_i\,. \qquad (3)$$

ПСШ генерує n-бітову послідовність, базуючись на внутрішньому стані генератора. Техніка генерування гами може бути різна, деякі реалізації можуть ефективно працювати на 8-, 16-, 32- або 64-бітових архітектурах, або навіть за умови певної особливої апаратної реалізації.

Вимоги. Ключовий потік, тобто гама, що генерується, генератор псевдовипадкових чисел має задовольняти такі вимоги [1]:

1. Мати заданий період, тобто $l_G\ge l_d$, де l_d є мінімальне допустиме значення періоду.
2. Гама повинна мати складний закон її формування, інакше вона може бути визначена під час криптоаналізу.
3. Відновлюваність гами у часі і просторі, тобто можливість її точного відтворення.
4. Мінімальна або сприйнятна складність реалізації функції генерації гами.
5. Допустима величина перекриття шифруючої гами, під якою розуміють імовірність з'явлення однієї і тієї ж гами в просторі або часі, як на одній, так і у різних станцій.

Швидкість. Швидкодія шифрів (генерація гами) обчислювалась на комп'ютері з процесором Intel Core i7-3630QM з тактовою частотою 2.4 ГГц. Код написаний C++ та скомпільований за допомогою компілятора MinGW gcc-g++ версії 4.8.1-4. У таблиці не наводиться швидкодія апаратно орієнтованих шифрів, оскільки їх програмна модель є дуже повільною 2–13 Мбіт/с. Оцінка швидкодії даних шифрів є доречною за наявності апаратної реалізації.

Безпека. Усі шифри, що проходили відбір під час проекту eSTREAM, потрапили під детальний аналіз та дослідження. Деякі шифри були взламані ще під час проекту, але помилки були

Таблиця 1

Порівняння параметрів та швидкодії програмно орієнтованих шифрів

Назва шифру	Розмір ключа (біт)	Розмір вектора ініціалізації (біт)	Швидкодія генерування (Мбіт/с)	Швидкодія процесу ініціалізації (мкс)
HC128	128	128 біт	2521	16,9
Rabbit	128	64	1764	1,7
Salsa20	128	64	2006	0,8
Sosemanuk	256	128	1610	15,8

виправлені та випущені нові версії шифрів. Так, наприклад, початкова версія апаратно орієнтованого шифру Grain мала уразливість, що давала можливість здійснити атаку та разкрити секретний ключ зі складністю 2^{40} [7].

Станом на сьогодні, багато шифрів залишаються стійкими та не існує атаки зі складністю, меншою за повний перебір ключа. Такі програмні шифри, як HC, Rabbit, Sosemanuk, Salsa20/7 та вище, апаратні шифри Grain, Mickey, Trivium залишаються надійними та рекомендованими до використання.

2. НЕЛІНІЙНІ РЕГІСТРИ ЗСУВУ

Одним з перспективних і мало досліджених методів побудови апаратних генераторів псевдовипадкових послідовностей є використання нелінійних регістрів зсуву зі зворотним зв'язком (NLFSR). NLFSR є узагальненням лінійного регістру зсуву зі зворотним зв'язком (FLSR), у яких поточний стан є нелінійною функцією від попереднього стану. Така зацікавленість NLFSR викликана тим, що вони спроможні генерувати великі псевдовипадкові послідовності, що будуть важко розкриті, використовуючи існуючі методи криптоаналізу. Відомо [1], що для того, щоб виявити функцію зворотного зв'язку для LFSR методом Берлекемпа-Мессі, необхідно перехопити лише 2n бітів послідовності. Для того, щоб заплутати криптоаналітика, були розроблені алгоритми для підвищення лінійної складності послідовностей: наприклад, використання проріджуючих генераторів, нелінійні комбінації NLFSR або нелінійні фільтри [4].

Брюс Шнайер ще у 1994 році [5] писав, що нелінійні регістри зсуву є дуже цікавими з точки зору побудови потокових симетричних шифрів, але вони не мають достатнього математичного апарату для описання та аналізу. Для послідовностей, що генеруються за допомогою NLFSR, є характерні такі проблеми:

– у вихідній послідовності можуть бути зсуви, наприклад, одиниць більше ніж нулів;

– максимальний період може бути менший ніж очікувалось;

– період для різних початкових станів може бути різним;

– послідовність може деякий час виглядати як випадкова, а потім зводитись до якого-небудь єдиного значення.

На сьогоднішній день нелінійні регістри зсуву використовуються у декількох алгоритмах потокового шифрування, таких як Achterbahn, Grain, Trivium [4], причому останні є фіналістами eSTREAM. Але навіть ці NLFSR не є ідеальними. Розглянемо NLFSR потокового шифру Grain [3]. Оскільки у попередній версії шифру була виявлена атака, яка дозволяла знайти секретний ключ за $O(2^{40})$, виявивши лінійну функцію, що могла з ймовірністю більшою за S передбачити наступний біт. Для посилення стійкості шифру, автори змінили нелінійну функцію зворотного зв'язку, що на сьогоднішній день використовує 13 бітів 80-бітового регістру та має рівень нелінійності 11. Якщо заповнити його тільки одиницями, тоді він починає генерувати 0 і ніколи не виходить з цього стану. Тобто, він зводиться до певного єдиного значення. Зазвичай, конструкція шифру включає в себе лінійний регістр, що подає на вхід NLFSR свій молодший біт і дозволяє вивести регістр із-за циклювання. Таким чином, важливим є пошук методу побудови нелінійного регістру зсуву, що не мав би в собі вищезазначених вад. Тобто, для побудови NLFSR висуваються такі вимоги:

– рівномірність розподілу вихідних значень;

– генерація послідовності максимальної довжини (послідовність де Бруійна);

– відсутність підциклів;

– відсутність зациклювань.

На цю тему проводилося дуже багато досліджень [2, 4, 6. 7]. У роботі [7] був запропонований метод, що дозволяє побудувати нелінійний регістр зсуву зі зворотним зв'язком, що генеруватиме послідовність максимальної довжини. На рис. 1 показана узагальнена структура регістру

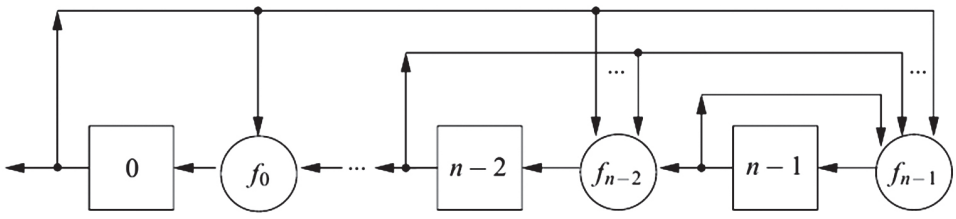

Рис. 1. Узагальнена структура регістру зсуву

зсуву, де 0 ... n-1 є поточним станом регістру зсуву, а f_i є функцією оновлення значення i. Існує теорема, що дозволяє побудувати нелінійний регістр зсуву, використовуючи простий незвідний поліном.

Теорема. Нехай N є нелінійний регістр зсуву розміру n та функції зворотного зв'язку задані у вигляді:

$$\begin{gathered} f_{n-1}(x_0,x_1,...,x_{n-2}) = \\ = x_0 + f_L(x_0,x_1,...,x_{n-2}) + f_N(x_0,x_1,...,x_{n-2}) \\ f_{n-2}(x_0,x_1,...,x_{n-3},x_{n-1}) = x_{n-1} + f_N(x_0,x_1,...,x_{n-3}) \\ f_{n-3}(x_{n-2}) = x_{n-2} \\ ... \\ f_0(x_1) = x_1, \end{gathered} \quad (4)$$

де а f_N є довільною нелінійною функцією, а f_L – лінійною булевою функцією виду (5), що побудована за допомогою простого незвідного полінома, тоді регістр має період 2^n-1.

$$f_L(x_1,x_2,...x_{n-2}) = c_1x_1 + c_2x_2 + ... + c_{n-2}x_{n-2}. \quad (5)$$

Доведення цієї теореми можна знайти у роботі [7]. Була проведена робота з дослідження цього методу генерації нелінійних регістрів зсуву. Дійсно, згенерована послідовність має максимальний період. Для тестування обирались незвідні поліноми різної довжини, як нелінійна функція була обрана функція виду:

$$\begin{gathered} f_N(x_0,x_1,...x_k) = x_0x_1 + x_0x_2 + ... + x_0x_k + x_1x_2 + ... + \\ + x_{k-1}x_k + x_0x_1x_2 + ... + x_0x_1...x_k, \end{gathered} \quad (6)$$

де k змінювалося у межах [2, 25].

Будувалися послідовності, які потім тестувалися за допомогою стандарту NIST 800-22 [2]. Дані послідовності проходили усі тести, окрім тесту на лінійну складність. У табл. 2 наведено результати тестування послідовностей, що генерувалися за допомогою даної методики. Параметри тесту обиралися стандартними.

З даної таблиці видно, що дані послідовності не мають достатньої лінійної складності, адже розподіл параметра C повністю сконцентрований у першому інтервалі і не відповідає необхідному розподілу ймовірностей. Іншими словами, дана послідовність не є достатньо складною для використання. Причиною тому є те, що даний генератор генерує ту ж саму лінійну послідовність, що й LFSR. Наприклад, у табл. 3 наведено дві послідовності, згенеровні за допомогою LFSR та NLFSR, побудовані за допомогою полінома (4, 1, 0) та функції нелінійного зсуву (7).

$$f_N = x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3. \quad (7)$$

Таблиця 3

Послідовності, побудовані за допомогою нелінійних та лінійних регістрів зсуву

Регістр	Послідовність
LFSR	0b0011010111100010
NLFSR	0b0001001101011110

З таблиці можна помітити, що це є одна і та сама послідовність, тільки зсунута одна відносно одної. Саме це стало причиною того, що послідовність не проходить тест NIST, адже існує лінійний поліном, за допомогою якого можна побудувати дану послідовність.

ВИСНОВКИ

Таким чином, основним вибором критеріїв ефективності потокового шифру є їх швидкодія, час генерування гами та ініціалізації. Вищезгадані шифри є надійними з точки зору безпеки і ефективними з точки зору швидкодії. Тим не менш, продовжується активне дослідження потокових шифрів, пошук ефективних способів і методів побудови шифрів та їх аналізу. Привабливими з точки зору криптоаналізу є шифри HC, адже він є подібним до RC4, який на сьогоднішній день є зламаним, шифр Trivium є дуже простим, на перший погляд, але тим не менш, жодної ефективної атаки на нього зроблено не було.

Найбільш цікавим з точки зору дослідження, на мою думку, є шифр Grain, адже він має у своєму складі нелінійний регістр зсуву, для яких досі не існує математичних методів оцінки та дослідження їх властивостей.

Питання побудови достатньо ефективного та надійного нелінійного регістру зсуву зі зворотним зв'язком досі залишається відкритим. Генератори, побудовані за допомогою вищезазначеної теореми є поштовхом для дослідження та побудови їх властивостей, але їх ще зарано використовувати в ході побудови сучасних потокових шифрів. Задача стоїть у необхідності знаходження функції нелінійного зворотного зв'язку, тоді до неї необхідно висунути певні вимоги, задовольняючи які, послідовність би мала необхідну лінійну складність.

Література

[1] Горбенко І.Д. Прикладна криптологія: теорія, практика, застосування. – Х.: Форт, 2012. – 867 с.

[2] A statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (NIST 800-22) – Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, 2010. – 131 p.

Таблиця 2

Результати тестування послідовностей за допомогою NIST 800-22

Поліноми \ k	3							10						
	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_0	C_1	C_2	C_3	C_4	C_5	C_6
(46, 5, 3, 2, 1, 0)	2000	0	0	0	0	0	0	2000	0	0	0	0	0	0
(47, 5, 0)	2000	0	0	0	0	0	0	2000	0	0	0	0	0	0
(66, 9, 8, 6, 0)	2000	0	0	0	0	0	0	2000	0	0	0	0	0	0

[3] A Stream Cipher for Constrained Environments / Martin Hell, Thomas Johansson and Willi Meier // eStream. – 2008. – P. 14. – Режим доступу: http://cr.yp.to/streamciphers/grain/desc.pdf

[4] Mattsson J. Stream Cipher Design – Stockholm: Master of Science Thesis, 2006. – 62 p.

[5] Шнайер Б. Прикладная криптология. М.: Диалектика, 1994. – 432 с.

[6] A Scalable Method for Constructing Galois NLFSRs with Period 2n –1 using Cross-Join Pairs / E. Dubrova // Royal Institute of Technology (KTH). – 2011. – P. 13. – Режим доступу: http://eprint.iacr.org/2011/632.pdf

[7] Distinguishing Attack on Grain / Shahram Khazaei, Mehdi Hassanzadeh, Mohammad Kiaei / Raymand Information and Communication Cryptographers. – 2005. – p. 9. Режим доступу: http://cr.yp.to/streamciphers/grain/071.pdf

Поступила в редколлегию 11.07.2014

Тімохін Сергій Сергійович, студент факультету комп'ютерних наук національного університету імені В. Н. Каразіна. Наукові інтереси: криптографія, криптоаналіз, симетричне та асиметричне шифрування.

Горбенко Іван Дмитрович, фото та відомості про автора див. на стор. 216.

УДК 004.056.55

Исследование и сравнительный анализ перспективных потоковых шифров / С.С. Тимохин, И.Д. Горбенко // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 217–220.

Потоковые симметричные шифры играют важную роль для защиты информации, для которой предъявляются значительные требования к уровню стойкости и скорости обработки в режиме он-лайн. Аппаратно-ориентированные потоковые шифры должны обеспечивать достаточный уровень устойчивости, быстродействия и быть компактными при аппаратной реализации. Нелинейные регистры сдвига является одним из подходов построения аппаратных шифров, что есть на сегодня мало исследованным и требует внимания.

Ключевые слова: потоковое шифрование, нелинейные регистры сдвига.

Табл.: 3. Ил.: 1. Библиогр.: 7 назв.

UDC 004.056.55

Research and comparative analysis of perspective stream ciphers / S.S. Timohin, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 217–220.

Streaming symmetric ciphers play an important role in information security for which significant demands to the level of resistance and processing speed in the on-line mode are made. Hardware-oriented stream ciphers should provide a sufficient level of security, speed of response and be compact in hardware implementation. Non-linear shift registers are one of the approaches to building hardware codes, which is currently slightly researched and requires attention.

Keywords: streaming encryption, nonlinear shift registers.

Tab.: 3. Fig.: 1. Ref.: 7 items.