РАДІОТЕХНІКА І ТЕЛЕКОМУНІКАЦІЇ

УДК 621.391.037.372

Горохов С. М., Захарченко М. В., Басов В. Є.
Gorohov S. M., Zaharchenko N. V., Basov V. E.

ШВИДКІСНИЙ ПОТОКОВИЙ ШИФР МАЛОЇ СКЛАДНОСТІ РЕАЛІЗАЦІЇ

THE HIGH-SPEED LINE CODE OF SMALL COMPLEXITY OF REALIZATION

Анотація. Запропоновано схему побудови швидкісних шифрів, яка ґрунтується на використанні недвійкових регістрів зсуву та нелінійних перетворень.

Summary. The chart of construction of speed codes, which is based on the use of unbinary shift registers, and nonlinear transformations, is offered.

Одним із напрямів вирішення проблеми захисту дискретної інформації є її криптографічний захист. В наш час розроблено і використовується багато алгоритмів криптографічного захисту. Найбільш поширений тип шифрів – це симетричні шифри, які розподіляються на два класи. По перше – це блочні шифри, які мають дуже велику стійкість до криптоаналітичних атак, але не дуже велику швидкодію (такі, як ГОСТ 28147-89, *T-DES, IDEA, Blowfish, TwoFish, Rindael*). По-друге – це потокові шифри, які мають дещо меншу крипостійкість, але є набагато більш швидкісними (ліцензовані: SEAL, RC4; не ліцензовані *WAKE* та на ґрунті генераторів зсуву з лінійним зворотнім зв'язком (*linear feedback shift register – LFSR*)) детальний опис яких наведено, наприклад, в літературі [1]. Стосовно лінійних, квадратичних, кубічних та інших конгруентних генераторів будь-якого ступеня – вже досить давно доведено їх непридатність для використання у криптографії [2, 3, 4, 5, 6] у чистому вигляді.

Необхідність розробки стійких швидкісних шифрів в наш час пов'язано з розвитком систем умовного доступу *Conditional Access Systems* (*CAS*) для мереж ефірного та кабельного цифрового телебачення і мовлення, що ґрунтуються на стандарті *Digital Video Broadcasting (DVB)*, та системи *Digital Right Management (DRM)* в телевізійному мовленні через мережу передавання даних – *IPTV*. Один з провідних виробників устаткування умовного доступу систем кабельного цифрового телебачення для шифрування контенту *VERIMATRIX* [7] використовує криптографічний алгоритм *RC*4, як вказано на його сайті. Інші виробники, такі як *VIACCESS*[8], *IRDETO*[9], *Philips CryptoWorks*[10], *Conax AS*[11] взагалі тримають в секреті навіть ті стандартні алгоритми, які використано у них в системах. Щоб розробнику сумісної апаратури отримати технічні дані треба укласти договір про нерозповсюдження наданої інформації і в подальшому від реалізації апаратури проводити ліцензійні відрахування близько $20 на один прикінцевий пристрій мережі *IPTV – Set Top Box (STB)*. Сучасна вартість таких пристроїв складає близько $150 за один *STB*. Таким чином розробка власної системи *DRM* може суттєво (приблизно на 15%) зменшити вартість мережі мовлення і сприяти більш швидкому зростанню таких комерційних мереж.

Не зважаючи на те, що в Світі запропоновано досить багато схем поточних шифрів, саме така комбінація складових компонентів шифру раніше ніколи не була описана у відкритих джерелах, як на Україні, так і за її межами.

Мета роботи – розробка власного швидкісного поточного шифру, який дозволяє шифрувати контент в реальному часі. Розглянемо спочатку базові інженерні рішення, на яких раніше розроблялися і розробляються поточні шифри і які використано в запропонованій схемі.

Лінійний конгруентний генератор завдається виразом

$$X_i = (A \times X_{i-1} + B) \bmod M , \qquad (1)$$

де X_i і X_{i-1} – поточне та попереднє значення на виході генератора відповідно $A < M$, $B < M$. Щоб генерована послідовність мала максимальну довжину, необхідно щоб числа B та M були взаємно простими [1]. В такому випадку на виході схеми виникає псевдовипадкова послідовність усіх чисел від 0 до $(M-1)$. Такі генератори породжують послідовності чисел зі статистичними характеристиками, що дуже близькі до рівномірного закону розподілу випадкової величини, але самі по собі мають дуже незначну криптостійкість.

Шифри на грунті LSFR. Досить довгий час використовуються, як для генерації псевдовипадкових послідовностей бітів, так і у поточних криптографічних алгоритмах. Щоб генерована послідовність мала максимальну довжину треба, щоб відводи зворотних зв'язків у регістрі відповідали примітивному поліному за модулем два [1]. Апаратно такі генератори

реалізуються дуже просто, але програмна реалізація не дуже ефективна, бо потребує не менш ніж дві операції на кожен генерований біт. Тому в програмних схемах доцільніше використовувати недвійкові регистри зсуву, коли зсув виконується не бітами, а словами.

Зараз відомо декілька варіантів генераторів, які використовують недвійкові регістри зсуву. Генератори Фібоначі (або адитивні генератори) дуже ефективні, тому що на вихід потрапляють слова, а не окремі біти. Початковий стан являє собою, як правило, масив 8, 16 або 32 розрядних слів. Тоді в загальному вигляді вихід цього генератора X_i можна записати як

$$X_i = (X_{i-a} + X_{i-b} + X_{i-c} + ... + X_{i-m}) \bmod 2^n , \quad (2)$$

де n – кількість двійкових розрядів у слові регістра зсуву. В цьому випадку коефіцієнти затримки *a, b, c,...,m* повинні відповідати примітивному двійковому породжуючому поліному, а молодший біт утворити *LFSR* з максимальним періодом [12]. Такі генератори не є криптографічно безпечними, але на їх ґрунті було розроблено декілька шифрів, таких як *Fish* (на двох генераторах Фібоначі), *Pike* (на трьох генераторах Фібоначі), *Mush* (знов на двох генераторах Фібоначі), *Gifford* (на одному генераторі дещо схожому на Фібоначі) [1]. В таких шифрах ключем є початковий стан регістра. Всі зазначені шифри, за виключенням останнього, мають невелику криптостійкість за рахунок використовування не дуже великих регістрів Фібоначі. В останньому було виявлено, що поліном зворотних зв‘язків не є примітивним і тому шифр не стійкий лише після того, як шифром припинили користуватись.

Шифри на грунті регистрів зсуву з нелінійними зворотними зв‘язками (*nonlinear feedback shift register – NFSR*). Проблема аналізу таких шифрів пов’язана з тим, що не існує математичного апарата, який дозволив би провести аналіз таких послідовностей. Ось деякі проблеми, пов’язані з аналізом схем з *NFSR*:

- у вихідних послідовностях можуть бути зміщення кількості одиниць відносно кількості нулів;
- найбільший період послідовностей може виявитися меншим ніж очікувалось;
- періоди послідовностей для різних початкових значень можуть відрізнятись;
- послідовність деякий час може виглядати випадковою, а потім зациклюватись на одному, або декількох значеннях.

Перевагою використання *NFSR* у криптографії виявляється те, що не існує теорії аналізу таких регістрів і тому існує дуже обмежена кількість можливостей криптоаналізу шифрів побудованих за допомогою цих схем. У шифрах з *NFSR* нелінійна функція зворотного зв’язку може бути будь-якою.

Пропонується шифр наступного вигляду, який є однією з можливих реалізацій *NFSR*

$$X_i = (A \times (X_{i-a} \oplus X_{i-b} \oplus X_{i-c} \oplus ... \oplus X_{i-m}) + B) \bmod M , \quad (3)$$

де $\oplus$ – побітове додавання за модулем 2. Ця схема об’єднує переваги швидкодії паралельної схеми регістрів Фібоначі і лінійного конгруентного генератора. Слід зазначити, що використання саме таких функцій у зворотному зв’язку *NFSR* ніколи раніш у відкритому друку не було описано. Схему запропонованого алгоритму шифрування, який базується на використанні недвійкового регістра зсуву з нелінійним зворотнім зв’язком зображено на рис. 1.

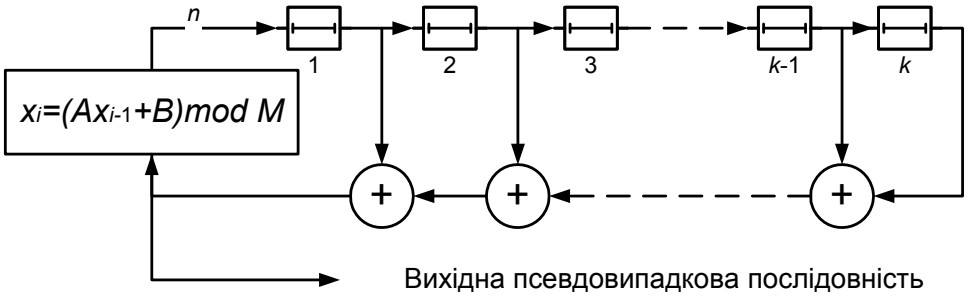

Рисунок 1 – Схема шифруючого генератора псевдовипадкової послідовності на регістрі зсуву з нелінійними зворотними зв’язками

На схемі $n = 1 + \log_2(M-1)$ – кількість двійкових розрядів, k – кількість елементів затримки в регістрі зсуву, символом $\oplus$ позначено побітові суматори за модулем 2. У цьому випадку найбільша довжина послідовності, яка не повторюється, дорівнює

$$L = M^k = 2^{k \times \log_2 M} \quad (4)$$

слів. В основу шифру закладено те, що операції в алгебраїчному кільці з двох елементів і в алгебраїчному кільці з $M > 2$ елементів є взаємно нелінійними. Таким чином комбінуючи дві різні

лінійні схеми отримаємо одну нелінійну. Якщо, як було зазначено вище, лінійний конгруентний генератор має надто малу крипостійкість, а шифруючі схеми, які ґрунтуються на двійковому регістрі зсуву довжиною k з лінійними зворотними зв'язками потребують для успіху криптоаналізу послідовність лише $2k$ бітів за алгоритмом Берлекемпа-Мессі [1, 13], то криптоаналіз шифрів, які ґрунтуються на регістрі зсуву з нелінійними зворотними зв'язками в наш час ще не розроблено [1]. Таким чином, регістр зсуву довжини k і розрядності n можна розглядати як сукупність з n ідентичних двійкових регістрів зсуву. Лінійний конгруентний генератор виконує нелінійне перетворення відносно двійкової арифметики, вихідного слова, що має заважати криптоаналізу такого шифру.

Для того, щоб схема видавала послідовність максимальної довжини, необхідно щоб для блока нелінійної функції виконувались вимоги більш жорсткі, ніж для звичайного лінійного конгруентного генератора [1], тобто значення B та M повинні бути не взаємно простими, а взагалі простими числами. В той самий час зворотні зв'язки повинні відповідати примітивному поліному для двійкових регістрів зсуву.

Було написано математичну модель на мові програмування Сі та виконано статистичну перевірку висновків. При виконанні зазначених вище вимог генератор видавав послідовність слів, що не повторюєть максимальної довжини згідно з виразом (4). Перевірка проводилась для 8, 16 та 32 розрядних регістрів зсуву, які містили від 3 до 7 елементів затримки. Перевірку було проведено для наступних примітивних за модулем 2 породжуючих поліномів: (x^2+x+1), (x^3+x+1), (x^4+x+1), (x^5+x+1), (x^6+x+1), (x^7+x+1). Коефіцієнти нелінійної функції: A = {101, 5801, 27043}, B = {139, 35401, 104711}, M = {251, 65521, 4294967291}. Ознакою кінця перевірки було повторення послідовності чисел довжиною $2 \times k$ слів.

Генератори на зразок запропонованого мають у разі програмної реалізації дуже невелику складність реалізації. Кількість операцій на одне слово на три більше, ніж кількість ненульових членів у поліномі зворотного зв'язку

$$n_t = \frac{n_b + 3}{n}, \tag{5}$$

де n_t – кількість команд на генерацію одного біта псевдо випадкової послідовності, n_b – кількість зворотних зв'язків у регістрі зсуву. Так, якщо кількість зворотних зв'язків 3, а n = 16, то треба n_t = 0,375 операцій на біт в той час, як звичайні двійкові регістри зсуву з лінійними зворотними зв'язками забезпечують ефективність три операції на біт.

Також було перевірено рівномірність розподілу псевдовипадкової послідовності. Жодному програмному архіватору не вдалося стиснути отриманий файл навіть на 0,1%, що вказує на те, що вихідна послідовність підпорядковується рівномірному закону розподілу випадкової величини і може бути криптографічно стійкою.

Наприкінці можна сказати, що запропоновано алгоритм поточного шифрування, який має дуже високу швидкодію, а його програмна реалізація потребує невеликих ресурсів. Цей шифр відноситься до класу шифрів на основі регістра зсуву з нелінійними зворотними зв'язками. З цієї причини на сьогодні у Світі ще не існує ефективних методів криптоаналізу цього класу шифрів, що його вигідно відрізняє від потокових шифрів, які грунтуються на використанні регістрів зсуву з лінійними зворотними зв'язками.

Література

1. *Брюс Шнайер*. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: Пер. с англ. – М.: Триумф, 2002. – 816 с.
2. *Reeds J.A.* Cracking random number generator // Cryptologia. – 1977. – Vol.1.– N. 1, jan. – P. 20-26
3. *Reeds J.A.* Cracking a Multiplicative Congruential Encryption Algorithm in Information Linkage Between Applead. // Mathematic and Industry, P.C.C. Wang., ed., Academic Press – 1979. – P. 467-472.
4. *Reeds J.A.* Solution of Challenge Cipher. // Cryptologia. – 1979. – Vol.3. – N. 2, apr. – P. 83-95
5. *Kravczuk H.* How to Predict Congruential Generator. // Journal of Algorithms. – 1992. – Vol. 13. – N. 4, dec. – P. 527-545.
6. *Lagarias J.C., Reeds J.A.* Unique Exploration of Polynomial Recurrences. // SIAM Jornal on Computing. – 1988. – Vol. 17. – N. 2, apr. – P. 342-362
7. http://www.verimatrix.com
8. http://www.viaccess.com
9. http://www.irdetoaccess.com
10. http://www.cryptoworks.philips.com
11. http://www.conax.com/Russian/
12. *Brent R.P.* On the Periods of Generalized 261, Fibonacci Recurrences. // Mathematic of Computation. – 1994. – Vol. 63. – N. 207, jul. – P. 394-401.
13. *Massey J.L.* Shift Register Synthesis and BCH Decoding // IEEE Transaction on Information Theory. – 1969. – vol. 15. – N. 1, jan. – P. 122-127.