УДК 621.396

О.В. Сєвєрінов

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

АНАЛІЗ МЕТОДІВ ПОБУДОВИ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

Проводиться аналіз методів генерації псевдовипадкових послідовностей для забезпечення захисту інформації в телекомунікаційних мережах. Пропонується метод, заснований на декодуванні випадкового коду, де завдання криптоаналізу зводиться до рішення теоретико-складної задачі синдромного декодування.

Ключові слова: *генератор псевдовипадкових послідовностей, лінійних регістрів зсуву зі зворотними зв'язками, генератор, заснований на проблемі декодування випадкового коду.*

Вступ

З розвитком інформаційно-телекомунікаційних мереж, збільшенням кількості їх користувачів і об'ємів інформації, що передається, все більше виникає питань по забезпеченню безпеки даних, які передаються, обробляються і зберігаються в них. Для забезпечення захисту інформації в телекомунікацій-

них мережах використовуються різні криптографічні алгоритми і протоколи. При цьому однією із задач є формування випадкових та псевдовипадкових бітових послідовностей, що є необхідною умовою генерації і формування ключових даних.

В галузі захисту інформації існує окремий напрям, пов'язаний з генерацією випадкових (псевдовипадкових) послідовностей, йде постійна робота по удосконаленню не тільки засобів генерації, але і теорії та термінології в цьому важливому напрямі, проводиться розробка теорії і практики тестування джерел інформаційно-телекомунікаційних мереж випадкових послідовностей, оцінки і вимірювання їх показників.

В даний час відомо багато різних за принципом дії генераторів, але більшість з них вимагають перевірки і удосконалення, інакше вони не задовольнятимуть сучасним вимогам і тестам на випадковість. Тому сьогодні є актуальним проведення аналізу принципів побудови джерел випадкових бітових послідовностей, які зможуть задовольнити умовам їх використання в системах захисту інформації інформаційно-телекомунікаційних мереж.

Основний матеріал досліджень

Дослідження робіт в галузі захисту інформації показали, що формування випадкових і псевдовипадкових послідовностей (ПВП) здійснюється за допомогою відповідних генераторів (ГПВП), реалізованих на основі різних відомих методів. Псевдовипадкові послідовності можуть і не бути істинно незалежними, але вони не відрізняються від дійсно випадкових послідовностей і можуть бути використані при реалізації сучасних інформаційних технологій захисту інформації. Найбільшого поширення набули ГПВП, засновані на використанні лінійних регістрів зсуву зі зворотними зв'язками (ЛРЗЗ), а також на конгруентних перетвореннях. Поряд з високими показниками швидкодії даний підхід, як правило, дозволяє формувати ПВП максимального періоду. У той же час, як показують результати досліджень, формовані псевдовипадкові числа (ПВЧ) не є криптографічно стійкими, правило їх формування легко розкривається після перехоплення зловмисником фрагмента послідовності невеликої довжини [1]. Крім того, великі випадкові числа, що генеруються з використанням бітів цієї послідовності, що йдуть підряд, є сильно корельованими і для деяких типів додатків зовсім не є випадковими. Не дивлячись на це, ЛРЗЗ часто використовуються для створення алгоритмів шифрування.

Для підвищення структурної скритності використовують [1]:

- комбінування декількох ЛРЗЗ;
- нелінійні функції в зворотному зв'язку регістра;
- нелінійну логіку і фільтрацію вмісту регістра.

Прикладом генераторів з використанням ЛРЗЗ є генератор шифруючої алгоритмів шифрування A5/1 и A5/2, що використовуються в стандарті GSM (рис. 1).

Проблема ЛРЗЗ полягає у тому, що їх програмна реалізація дуже неефективна при використанні багаточленів з великою кількістю коефіцієнтів (щільних). При використанні ж багаточленів зворотного зв'язку з малою кількістю коефіцієнтів (розріджених) полегшується криптоаналіз по кореляційних зв'язках.

Другим підходом є методи формування ПВП, засновані на використанні математичного апарату булевої алгебри і нелінійних перетворюють функцій, широко використовуваних у сучасних симетричних шифрах. Даний напрямок забезпечує високі показники стійкості ПВЧ і порівняно невисоку обчислювальну складність реалізації.

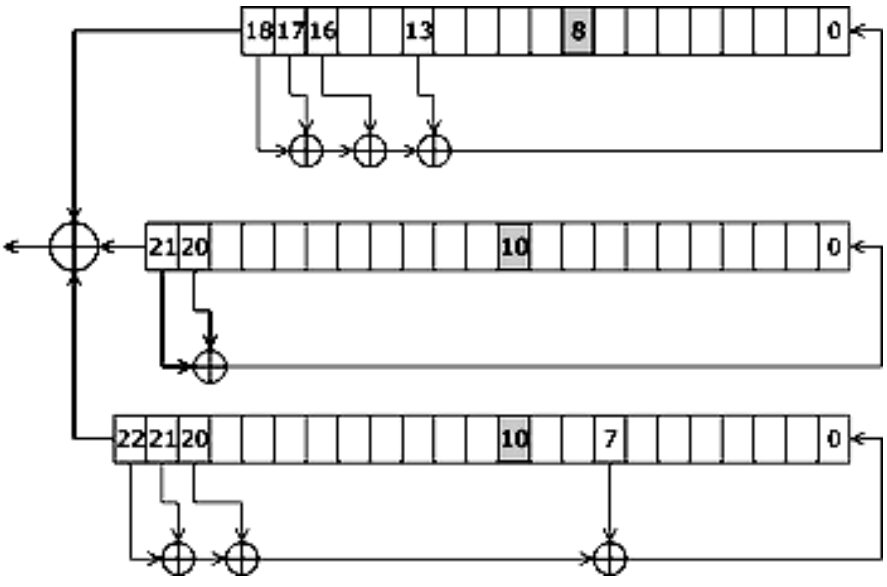

Рис. 1. Схема генератору ПВП алгоритму A5/1

На рис. 2 представлена схема генератора сеансових ключів за допомогою головного ключа [2]. Лічильник з періодом N забезпечує параметри логіки шифрування.

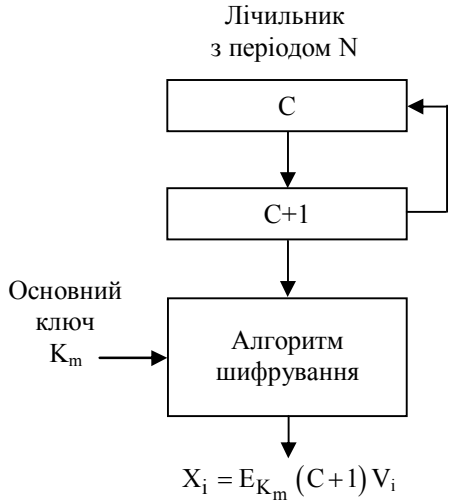

Рис. 2. Генерація псевдовипадкових чисел з використанням лічильника

Щоб зробити цей алгоритм ще більш захищеним, замість значень простого лічильника можна використовувати вихідні значення повноперіодичного генератора псевдовипадкових чисел.

Іншим підходом є використання режиму шифрування із зворотним зв'язком по виходу (OFB). Для прикладу на рис. 3 представлена схема OFB алгоритму DES, яка може служити не тільки для потокового шифрування, але і для генерації ключів.

Режим OFB володіє тією перевагою, що вплив можливих спотворень бітів при передачі даних не розповсюджується на подальші порції даних. Наприклад, якщо спотворені біти з'явилися при передачі C_1, це вплине тільки на відновлене з C_1 значення P_1, а всі подальші порції відкритого тексту через цю помилку передачі даних пошкоджені не будуть.

До основних недоліків генераторів на основі блокового шифрування можна віднести:

– нечутливість криптосхем до випадіння або вставки цілого числа блоків;

– існування проблеми останнього блоку неповної довжини.

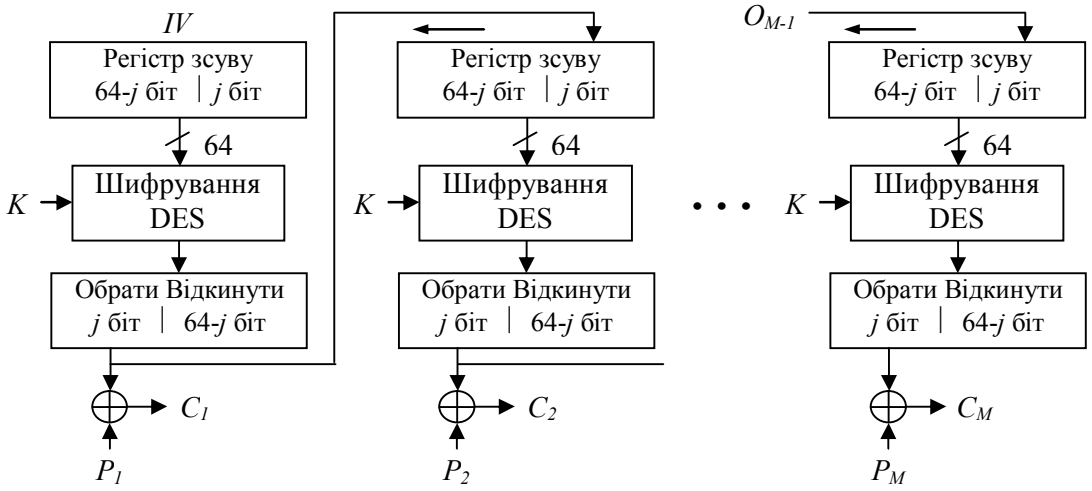

Рис. 3. Режим генерації з j-бітовим зворотним зв'язком по виходу (OFB)

Особливе місце в області формування ПВЧ займають методи, засновані на зведенні задачі криптоаналізу до вирішення деякої теоретико-складної задачі (факторизації, дискретного логарифмування). Данні методи формування ПВЧ є найбільш перспективні за показниками стійкості і, як показують проведені дослідження, володіють високими характеристиками статистичної безпеки. Генератори, які засновані на рішенні однобічних функцій, мають назву доказово стійких генераторів. До доказово стійких генераторів відносяться ГПВЧ BBS и RSA. У той же час, як показує проведений аналіз, ці алгоритми обчислювально складні в реалізації (на 3 – 4 порядки в порівнянні з симетричними криптоалгоритмами) і не дозволяють формувати ПВЧ максимального періоду.

Найбільшого розвитку сучасні механізми генерації псевдовипадкових послідовностей, в тому числі і для ключів різного призначення, в сучасних інформаційно-комунікаційних системах набули у США [3]. Основним документом, який розроблено та впроваджено національним інститутом стандартів і технологій США, є національний стандарт NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, у якому визначено декілька підходів щодо побудови генераторів псевдовипадкових послідовностей. Основними генераторами, які наведено у специфікації, є наступні [3]:

– методи детермінованого формування псевдовипадкових послідовностей, що використовують математичний апарат функцій гешування;

– методи детермінованого формування псевдовипадкових послідовностей, що використовують блокове симетричне шифрування;

– методи детермінованого формування псевдовипадкових послідовностей, що базуються на теоретико-числових задачах.

Генератори псевдовипадкових послідовностей у відповідності до стандарту NIST Special Publication 800-90A можуть бути засновані на використанні функцій гешування, які є необоротними або односторонніми функціями перетворень [2, 3]. Максимальна безпека, яку може підтримувати такий генератор, відповідає рівню безпеки застосовуваної функції гешування.

Перспективним напрямком у розвитку методів формування ПВЧ є розробка та дослідження ГПВЧ, заснованих на проблемі декодування випадкового коду. ГПВП на основі надмірних блокових кодів вперше запропоновані в роботі [4]. Даний генератор будується на використанні блокового алгебраїчного (n, k, d) коду з алгоритмами кодування і декодування, що легко реалізовуються [5]. За допомогою маскування алгебраїчного коду під випадковий код, завдання декодування для зловмисника представляється як обчислювально складне. Таким чином, не знаючи правила маскування, зловмисник змушений використовувати складний декодер випадкового коду, а весь процес кодування-декодування в цьому випадку еквівалентний односторонній криптографічній функції, складність декодування якої, в загальному випадку, зростає з експоненціальною залежністю від довжини коду та/або від його виправляючої здібності [5, 6].

Висновки

Таким чином, в ході проведеного аналізу встановлено, що для побудови стійких кодів можливо застосовувати методи, засновані на використанні односторонніх функцій, таких як факторизація числа і дискретне логарифмування. Це дозволяє будувати доказово стійки ГПВЧ із зведенням завдання криптоаналізу до вирішення теоретико-складного завдання. При цьому основним недоліком генераторів, заснованих на односторонніх функціях, є висока складність, яка визначається, перш за все, великою розрядністю чисел, над якими необхідно виконувати математичні операції. Швидкодія доказово стійких генераторів на декілька порядків нижче в порівнянні з генераторами заснованих на потокових або блокових шифрах.

Одним з перспективних напрямів є методи, засновані на декодуванні випадкового коду, де завдання криптоаналізу зводиться до рішення теоретико-складної задачі синдромного декодування. Їх використання дозволяє скоротити час формування ПВЧ в порівнянні з відомими доказово стійкими генераторами.

Список літератури

1. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В.Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

2. Столингс В. Криптография и защита сетей: принципы и практика / В. Столингс. – М.: Вильямс, 2001. – 672 с.

3. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. [Електронний ресурс]. – January 2012. – Режим доступу до ресурсу: http://csrc.nist.gov/ publications/nistpubs/800-90A/SP800-90A.pdf.

4. Fisher Jean-Dernard. An efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding / Jean-Dernard Fisher, Stern Jacques // EUROCRYPT'96 Proceeding, LNCS 1070. – P. 245-255.

5. Берлекэмп Э.Р. Алгебраическая теория кодирования: Пер. с англ. / Э.Р. Берлекэмп. – М.: Мир, 1971.– 477 с.

6. Сидельников В.М. Криптография и теория кодирования / В.М. Сидельников // Материалы конференции «Московский университет и развитие криптографии в России». – М.: МГУ, 2002. – С. 22.

Надійшла до редколегії 2.09.2013

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

АНАЛИЗ МЕТОДОВ ПОСТРОЕНИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А.В. Северинов

Проводится анализ методов генерации псевдослучайных последовательностей для обеспечения защиты информации в телекоммуникационных сетях. Предлагается метод, основанный на декодировании случайного кода, где задача криптоанализа сводится к решению теоретико-сложной задачи синдромного декодирования.

Ключевые слова: *генератор псевдослучайных последовательностей, линейных регистров сдвига с обратными связками, генератор, основанный на проблеме декодирования случайного кода.*

ANALYSIS METHODS FOR CONSTRUCTING PSEUDORANDOM SEQUENCE GENERATORS

O.V. Severinov

The analysis methods for generating pseudo-random sequences for data protection in telecommunication networks. The method is based on the decoding of random code where cryptanalysis problem is reduced to the solution of theoretical and Challenger syndrome decoding.

Keywords: *pseudorandom sequence generator, linear shift registers with reverse copulas, generator, based on the problem of decoding of random code .*