Література

1. Домарев В. В. Безопасность информационных технологий. Системный подход / Домарев В. В. – К. : ДиаСофт, 2006. – 904 с.

2. Домарев В. В. Защита информации и безопасность компьютерных систем / Домарев В. В. – К. : ДиаСофт, 1999. – 480 с.

3. Борисов А. Н. Принятие решения на основе нечетких моделей: примеры использования / Борисов А. Н., Крумберг О. А., Федоров И. П. – Рига : Знание, 1990. – 184 с.

4. Поспелов Д. А. Нечеткие множества в моделях управления и искусственного интеллекта / Поспелов Д. А. – М. : Наука, 1986. – 312 с.

5. Ротштейн А. П. Интеллектуальные технологии идентификации / Ротштейн А. П. – Винница : Универсум-Винница, 1999. – 320 с.

✧ ✧ ✧ ✧ ✧ ✧ ✧

УДК 621.396

Д. І. Прокопович-Ткаченко, аспірант
Академії митної служби України

МЕТОД ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ МАКСИМАЛЬНОГО ПЕРІОДУ З ВИКОРИСТАННЯМ ПЕРЕТВОРЕНЬ НА ЕЛІПТИЧНИХ КРИВИХ

Досліджуються методи формування псевдовипадкових послідовностей, зокрема методи, які використовують модульні перетворення та перетворення у групі точок еліптичної кривої. Встановлено недоліки досліджуваних генераторів, зокрема виявлено певні вади періодичних властивостей формованих послідовностей. Розробляється удосконалений метод, який за допомогою додаткового введення рекурентного перетворення дозволяє формувати послідовності псевдовипадкових чисел максимального періоду. Запропоновано структурну схему генератора, який практично реалізує розроблений метод та дозволяє формувати псевдовипадкові послідовності максимального періоду з використанням перетворень у групі точок еліптичної кривої.

Исследуются методы формирования псевдослучайных последовательностей на основе модульных преобразований и преобразований в группе точек эллиптической кривой. Выявлены недостатки периодических свойств исследуемых генераторов, показано, что периоды формируемых последовательностей ниже максимального. Разрабатывается усовершенствованный метод, который за счет дополнительного введения рекуррентного преобразования позволяет формировать последовательности псевдослучайных чисел максимального периода. Предложена структурная схема генератора, который практически реализует разработанный метод и позволяет формировать псевдослучайные последовательности максимального периода на основе преобразований в группе точек эллиптической кривой.

The methods of forming pseudorandom sequences including methods that use modular transformation and the transformation of points of an elliptic curve are studied. Disadvantages of studied generators including some imperfections periodic properties of molded sequences are found. Improved method that allows generating a sequence of pseudorandom number of maximum period by additional input recurrent transformations is developed. Block diagram of the generator which practically implements developed method and allow to form the pseudorandom sequences of maximum period using the change in the point of an elliptic curve is suggested.

Ключові слова. Псевдовипадкові послідовності, еліптична крива, група точок, рекурентні перетворення, максимальний період.

Вступ. Серед сучасних науково-технічних проблем у галузі інформаційних технологій особливу увагу привертає завдання криптографічного захисту інформації для забезпечення безпеки усіх складових процесу збору, обробки та передачі даних [1, 2]. Більшість сучасних механізмів криптографічного захисту інформації використовує певні процедури рандомізації, зокрема методи та обчислювальні алгоритми формування псевдовипадкових послідовностей [1–12]. Проте в існуючих генераторах є певні недоліки, зокрема формовані псевдовипадкові послідовності не завжди мають максимальний період, тобто періодичні властивості формованих послідовностей можуть не задовольняти сучасні вимоги. Як приклад генератори псевдовипадкових послідовностей будуються з використанням модульних перетворень або перетворень у групі точок еліптичної кривої [3–12]. Тому дослідження існуючих і розробка нових методів та розрахункових алгоритмів формування псевдовипадкових послідовностей максимального періоду – це важливе та актуальне науково-технічне завдання.

Відомі методи формування псевдовипадкових послідовностей із використанням модульних перетворень та перетворень у групі точок еліптичної кривої. Найефективнішими з погляду нерозрізнюваності формованих послідовностей із реалізацією випадкового процесу є методи, з використанням модульних перетворень або перетворень у групі точок еліптичної кривої [3–12]. Наприклад, відомий метод Блюм–Блюм–Шуба [3, 4] ґрунтується на тому, що ключова послідовність подається у вигляді вектора x_0, який ініціалізує початкове значення аргументу функції $f(x) = x^2 \bmod n$ модульного піднесення до квадрата.

У якості модуля n обирається добуток великих простих чисел p і q, які тотожні трьом за модулем чотири, тобто: $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$, $n = p \times q$ (ціле число Блюма).

Наступне значення аргументу функції розраховується за допомогою модульного піднесення до квадрата, а вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення цієї функції:

$$x_i = f(x_{i-1}) = x_{i-1}^{\,2} \bmod n.$$

Задача до вирахування примітивних квадратних коренів за модулем числа n обчислювально еквівалентна до задачі розкладання цього числа на множники, тобто відомої задачі факторизації [1, 2]. Тому цей метод формування послідовностей псевдовипадкових чисел криптографічно стійкий. Але його недолік у тому, що він не дозволяє формувати послідовності максимального періоду, що суттєво зменшує ефективність та обмежує можливості щодо практичного використання. Так, наприклад, у працях [5, 6] йдеться про те, що довжина періоду формованих послідовностей може на декілька порядків бути меншою за максимальну. У дослідженнях [7, 8] запропоновано удосконалений метод, в якому за рахунок додаткового введення рекурентного перетворення, що реалізується, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, вдається виконати завдання формування псевдовипадкових послідовностей максимального періоду.

Найперспективнішими вважаються генератори псевдовипадкових послідовностей, які будуються з використанням перетворень у групі точок еліптичної кривої [9–12]. Як приклад можна навести стандартизований в ISO/IEC 18031:2005 генератор псевдовипадкових послідовностей [9]. У ньому пропонують використовувати скалярне множення точок еліптичної кривої для формування внутрішніх станів та окремих елементів вихідної послідовності. У праці [10] розглянуто рекомендації стандарту NIST SP 800-90 з формування псевдовипадкових послідовностей, особливості застосування генераторів, правила вибору окремих параметрів тощо.

Ключова послідовність генератора подається у вигляді вектора x_0, який ініціалізує початкове значення аргументу функції скалярного добутку точки еліптичної кривої:

$$f(x) = x \times P, \quad (1)$$

де P – базова точка еліптичної кривої, яка належить групі точок EC_n порядку n (у якості P обирається елемент групи EC_n з якомога більшим порядком).

Кожне наступне значення x_i обчислюється за допомогою скалярного множення x_{i-1} на базову точку $Q_i = x_{i-1} \times P$ та перетворення координат отриманої точки, тобто $x_i = \varphi(Q_i) = \varphi(f(x_{i-1})) = \varphi(f(x_{i-1}) \times P)$. Вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції скалярного добутку x_i. Задача вирахування функції $f(x)^{-1}$, яка є зворотною до функції скалярного добутку точки еліптичної кривої $f(x) = x \times P$, тобто вирахування деякого значення x_{i-1} за відомим значенням x_i, є задачею дискретного логарифмування в групі точок еліптичної кривої. Щодо її розв'язання нині ще невідомо ефективних алгоритмів вирахування дискретних логарифмів для базових точок великого порядку, тому цей спосіб формування послідовностей псевдовипадкових чисел криптографічно стійкий.

Недоліком даного методу є те, що він не дозволяє формувати послідовності псевдовипадкових чисел максимального періоду, що суттєво зменшує його ефективність та обмежує можливості практичного використання. Наприклад, у працях [11, 12] зазначено, що застосовані операції скалярного множення точок еліптичної кривої та відображення $\varphi(Q)$ координат отриманої точки для формування псевдовипадкових чисел не забезпечують максимальний період формованих послідовностей. Дійсно, порядок m групи точок еліптичних кривих обмежено виразом:

$$p + 1 - 2\sqrt{p} \le m \le p + 1 + 2\sqrt{p},$$

де p – порядок простого скінченного поля $GF(p)$, над яким розглядається еліптична крива.

Тобто можуть виникати такі випадки, коли порядок групи точок може бути вищий за порядок скінченного поля, над яким формуються значення функції $\varphi(x)$. Фактично це означає, що для деяких елементів групи, наприклад, для деяких точок Q_i і Q_j, $Q_i \neq Q_j$ функція $\varphi(x)$ поверне тотожні значення. Відповідно виконуватиметься рівність $x_j = x_i$ для деяких $i \neq j$, де $x_i = \varphi(Q_i)$ і $x_j = \varphi(Q_j)$, тобто значення реальних періодів формованих послідовностей будуть нижчі за максимальний період [11, 12].

Постановка завдання. Мета дослідження – розробити метод формування послідовностей псевдовипадкових чисел, який за рахунок додаткового введення рекурентного перетворення разом із використанням перетворень у групі точок еліптичної кривої дозволить формувати псевдовипадкові послідовності максимального періоду, що підвищить його ефективність та розширить можливості щодо практичного використання.

Удосконалений метод формування псевдовипадкових послідовностей з використанням перетворень у групі точок еліптичної кривої. Поставлена задача розв'язується шляхом додаткового введення рекурентних перетворень із формуванням послідовності максимального періоду, що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками.

Сутність удосконаленого методу формування псевдовипадкових послідовностей із використанням перетворень у групі точок еліптичної кривої полягає в тому, що ключова послідовність подається у вигляді вектора x_0, який ініціалізує початкове значення рекурентного перетворення $L(x)$ та початкове значення аргументу функції скалярного добутку точки еліптичної кривої (1).

Рекурентне перетворення $L(x)$ обирається таким чином, щоб отримана послідовність чисел $y_i = L(x_i)$ мала максимальний період. Перетворення $L(x)$ може реалізуватися, наприклад, за допомогою лінійних рекурентних регістрів із оберненими зв'язками [2].

Кожне наступне значення x_i обчислюється шляхом додавання значень x_{i-1} і $y_{i-1} = L(x_{i-1})$ та скалярного множення значення $(x_{i-1} + y_{i-1})$ на базову точку P:

$$Q_i = (x_{i-1} + y_{i-1}) \times P, \tag{2}$$

а також на перетворення $\varphi(Q)$ координат отриманої точки Q_j, $Q_i \in EC_n$, яке виконується за допомогою відповідного алгоритму (наприклад, x_i може дорівнювати значенню однієї з координат точки Q_i), тобто

$$x_i = \varphi\ Q_i\ = \varphi\ f\ x_{i-1} + y_{i-1}\ = \varphi\ x_{i-1} + L\ x_{i-1}\ \times P\ . \tag{3}$$

Вихідні елементи послідовності псевдовипадкових чисел формуються шляхом зчитування значення функції скалярного добутку, тобто шуканою послідовністю біт довжини m буде послідовність

$$b_0\ \ b_1\ \ b_2\ \ \ldots\ \ b_i\ \ \ldots\ \ b_{m-1},\ i = \overline{0, (n-1)},$$

де b_i – молодший біт числа x_i.

Пропонований метод криптографічно стійкий, оскільки задача обчислення функції $f(x)^{-1}$ обернена до функції скалярного добутку точки еліптичної кривої $f(x) = x \times P$, тобто вирахування деякого значення $(x_{i-1} + y_{i-1})$ у (3) за відомим значенням x_i є задачею дискретного логарифмування в групі точок еліптичної кривої. За рахунок додаткового введення рекурентного перетворення, що реалізується, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками, вдається формувати послідовності псевдовипадкових чисел максимального періоду, що підвищує ефективність та розширює можливості практичного використання цього методу.

Структурну схему пристрою, який реалізує пропонований удосконалений метод формування псевдовипадкових послідовностей, подано на рис. 1.

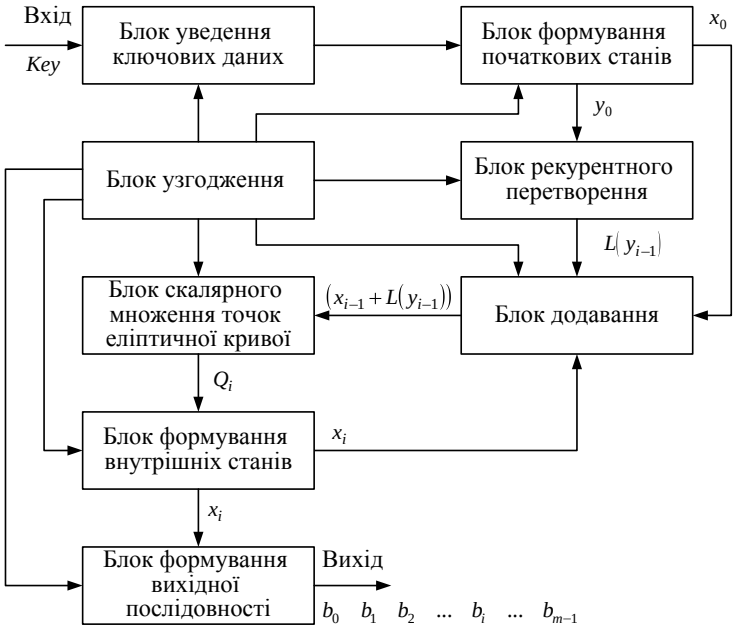

Рис. 1. Структурна схема пристрою формування псевдовипадкових послідовностей максимального періоду з використанням перетворень у групі точок еліптичної кривої

Пристрій має вхід, вихід, блок введення ключових даних, блок формування початкових станів, блок скалярного множення точок еліптичної кривої, блок формування внутрішніх станів, блок формування вихідної послідовності, блок узгодження та додатково введені блок рекурентного перетворення й блок додавання.

Елементи пристрою поєднано таким чином: вхід пристрою підключено до входу блоку введення ключових даних, вихід якого підключено до входу блоку формування початкових станів, виходи блоку формування початкових станів – до входу блоку рекурентного перетворення та до входу блоку додавання, вихід блоку рекурентного перетворення – до входу блоку додавання, вихід якого підключено до входу блоку скалярного множення точок еліптичної кривої, вихід блоку скалярного множення точок еліптичної кривої – до входу блоку формування внутрішніх станів, вихід якого підключено до входу блоку формування вихідної послідовності та до входу блоку додавання. Виходом пристрою є вихід блоку формування вихідної послідовності, а окремі виходи блоку узгодження підключено до окремих входів блоків уведення ключових даних, формування початкових станів, скалярного множення точок еліптичної кривої, формування внутрішніх станів, формування вихідної послідовності, рекурентного перетворення та блоку додавання відповідно.

Принципи роботи пропонованого пристрою: до блоку введення ключових даних вводиться послідовність даних *Key*, яка виконує роль секретного ключа. Вона передається у блок формування початкових станів, який призначено для формування початкового значення x_0 аргументу функції скалярного добутку точки еліптичної кривої (1) та рекурентного перетворення $L(x)$.

Сформований початковий стан x_0 подається на вхід блоку рекурентного перетворення. Результат рекурентного перетворення $y_{i-1} = L(x_{i-1})$ (на першій ітерації $i = j$), як і сформований початковий стан x_0, подається на вхід блоку додавання.

У блоці додавання обчислюється значення $(x_{i-1} + L(x_{i-1})$. Отриманий результат подається на вхід блоку скалярного множення точок еліптичної кривої.

У блоці скалярного множення точок еліптичної кривої розраховується значення (2), яке подається на вхід блоку формування внутрішніх станів.

У блоці формування внутрішніх станів виконується функціональне перетворення (3), виходом якого є нове значення внутрішнього стану x_i, яке подається на вхід блоку формування вихідної послідовності та на вхід додавання.

У блоці формування вихідної послідовності зі значення x_i зчитується найменш значущий біт даних (біт парності), який подається на вихід пристрою як елемент псевдовипадкової послідовності.

Наступна ітерація роботи пристрою починається поданням з виходу блоку формування внутрішніх станів значення x_i на вхід блоку додавання та з виходу блоку рекурентного перетворення значення y_i, після чого описані вище операції повторюються.

Блок узгодження призначено для покращання роботи окремих блоків пристрою та управління процесом формування псевдовипадкової послідовності. Пристрій зупиняє свою роботу за командою блоку узгодження (зупинку можна здійснити на кожному кроці).

Отже, реалізація даного пристрою дозволяє формувати псевдовипадкові послідовності максимального періоду з використанням перетворень у групі точок еліптичної кривої.

Висновки. Проведені дослідження показали, що відомі генератори псевдовипадкових послідовностей, які побудовано з використанням модульних перетворень та перетворень на еліптичних кривих, не задовольняють вимоги щодо періодичності формованих послідовностей. Пропонований удосконалений метод завдяки додатковому введенню рекурентного перетворення сприяє уникненню цього недоліку. Його практична реалізація дозволяє формувати псевдовипадкові послідовності максимального періоду з використанням перетворень у групі точок еліптичної кривої.

Таким чином, пропоноване рішення підвищує ефективність та розширює можливості практичного використання відповідного генератора псевдовипадкових послідовностей із використанням перетворень на еліптичних кривих. *Перспективним напрямком подальших досліджень* є експериментальна перевірка властивостей такого генератора, обґрунтування практичних рекомендацій щодо його реалізації та застосування.

Література

1. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity and Encryption. – April 19, 2004. – Version 0.15 (beta), Springer-Verlag. – 829 p.
2. Alfred J. Menezes Handbook of Applied Cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. – CRC Press, 1997. – 794 p.
3. Blum M. How to generate cryptographically strong sequences of pseudo-random bits / M. Blum, S. Micali // SIAM Journal on Computing. – 1984. – Vol. 13. – P. 850–864.
4. Blum L. A simple unpredictable pseudorandom number generator / L. Blum, M. Blum, M. Shub // SIAM Journal on Computing. – 1986. – Vol. 15. – P. 364–383.
5. Кузнецов О. О. Дослідження періодичних властивостей генератора псевдовипадкових послідовностей RSA / О. О. Кузнецов, Ю. М. Рябуха // Проблеми й перспективи розвитку ІТ-індустрії : тези доповідей 1-ї Міжнародної науково-практичної конференції 18–19 листопада 2009 р. – Харків, 2009. – С. 168–170.
6. Стасев Ю. В. Дослідження ефективності генераторів псевдовипадкових послідовностей / Стасев Ю. В., Кузнецов О. О., Рябуха Ю. М. // Новітні технології – для захисту повітряного простору : Сьома наукова конференція Харківського університету Повітряних сил імені Івана Кожедуба, 13–14 квітня 2011 року : тези доповідей. – Х. : ХУПС ім. І. Кожедуба. – 2011. – С. 151.
7. Кузнецов О. О. Формування псевдовипадкових послідовностей максимального періоду із використанням модулярних перетворень / О. О. Кузнецов, В. Ю. Ковтун, Ю. М. Рябуха // Системи обробки інформації. – Харків : ХУПС. – 2007. – Вип. 5 (63). – С. 137–141.
8. Патент на корисну модель 39674 Україна, МПК G09C1/00 Спосіб формування послідовностей псевдовипадкових чисел / О. О. Кузнецов, С. П. Євсєєв, Ю. М. Рябуха, Р. В. Корольов, В. А. Пудов. – № u 2008 10863; заявл. 03.09.2008, Опубл. 10.03.2009. Бюл. № 5. – 4 с.
9. ISO/IEC 18031:2005 Information technology – Security techniques – Random bit generation.
10. Barker E. Recommendation for random number generation using deterministic random bit generators [Електронний ресурс] / E. Barker, J. Kelsey // National Institute of Standards and Technology. – January 2012. – 124 p. – Режим доступу : http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf.
11. Кузнецов О. О. Методи формування псевдовипадкових послідовностей із застосуванням криптографічних перетворень на еліптичних і гіпереліптичних кривих / О. О. Кузнецов, В. Ю. Ковтун, Ю. В. Рябуха // Компьютерное моделирование в наукоемких технологиях : Труды научно-технической конференции с международным участием. – Ч. 2. – 18–21 травня 2010 р. – Х. : ХНУ ім. В. Н. Каразіна. – 2010. – С. 142–144.
12. Сорока Л. С. Дослідження генераторів псевдовипадкових послідовностей на еліптичних кривих / Л. С. Сорока, О. О. Кузнецов, Д. І. Прокопович-Ткаченко // Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку : збірник тез доповідей науково-практичної конференції Академії внутрішніх військ МВС України 21–22 березня 2012 року. – Х. : Академія внутрішніх військ МВС України, 2012. – С. 47–49.