УДК 004.056

Д.І. Прокопович-Ткаченко

Академія митної служби України, Дніпропетровськ

ПРИСКОРЕНЕ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ МАКСИМАЛЬНОГО ПЕРІОДУ ІЗ ПЕРЕТВОРЕННЯМИ НА ЕЛІПТИЧНИХ КРИВИХ

Досліджуються методи формування псевдовипадкових послідовностей для побудови механізмів підвищення безпеки інформаційних систем і технологій. Розглядається генератор псевдовипадкових послідовностей із застосуванням перетворень у групі точок еліптичних кривих (відповідно до стандарту NIST SP 800-90), показано його недоліки щодо періодичних властивостей формованих послідовностей. Досліджується удосконалений метод, який за рахунок додаткового введення рекурентного перетворення дозволяє формувати послідовності псевдовипадкових чисел максимального періоду. Пропонується реалізувати удосконалений метод у спрощеному варіанті для прискореного формування псевдовипадкових послідовностей.

Ключові слова: *безпека, інформаційна система, генератор, псевдовипадкова послідовність.*

Вступ

Проведені дослідження показали [1 – 3], що застосування криптографічних перетворень у групі точок еліптичних кривих дозволяє будувати ефективні генератори псевдовипадкових послідовностей для покращення показників ефективності телекомунікаційних систем та мереж, зокрема для вдосконалення методів та моделей підвищення безпеки у різних механізмах захисту інформації. Відповідно до цього, аналіз, розробка та дослідження криптографічно стійких генераторів псевдовипадкових послідовностей на еліптичних кривих є перспективним напрямком досліджень.

Проведені в [4] дослідження відомого генератору псевдовипадкових послідовностей на еліптичних кривих, який описано у стандарті NIST SP 800-90, дозволили встановити наступні недоліки: циклову функцію генератору, що забезпечує максимальний період формованої псевдовипадкової послідовності внутрішніх станів та відповідних точок еліптичних кривих невизначено; формування псевдовипадкової послідовності біт із послідовності точок еліптичної кривої шляхом вибірки блоку найменш значуших бітів та їх канкатенації не задовільняє вимогам статистичної розрізненості з рівномірно розподіленою послідовністю. Таким чином, відомий генератор псевдовипадкових послідовностей на еліпичних кривих (NIST SP 800-90) не задовільняє в повній мірі висуваємим вимогам.

При проведенні досліджень було розроблено удосконалений метод, який, за рахунок додаткового введення рекурентних перетворень дозволяє формувати послідовності псевдовипадкових чисел максимального періоду, що підвищує ефективність та розширює можливості практичного використання. Розроблений метод заснований на зведенні задачі знаходження таємного ключа до вирішення теоретико-складної задачі дискретного логарифмування у групі точок еліптичної кривої і дозволяє формувати псевдовипадкові послідовності максимального періоду.

В даній роботі поставлена задача реалізувати запропонований метод формування псевдовипадкових послідовностей у спрощеному варіанті, що дозволить прискорено формувати псевдовипадкові послідовності із застосуванням лише одного скалярного множення на фіксовану (базову) точку еліптичної кривої.

1. Відомий метод формування ПВП на еліптичних кривих

Метод формування ПВП із використанням перетворень на еліптичних кривих, який запропоновано в рекомендаціях NIST SP 800-90, засновано на застосуванні двох скалярних множень точок еліптичної кривої та відображенні відповідних x-координат отриманих результатів у ненульове ціле значення [3].

Перше скалярне множення на фіксовану (базову) точку P виконується для формування проміжного стану s_i, яке циклічно оновлюється на кожній ітерації при функціонуванні відповідного генератору. Таким чином значення стану s_i залежить від значення попереднього стану s_{i-1} (на попередній ітерації) та від значення базової точки P: $s_i = \phi(x(s_{i-1}P))$, де $x(A)$ - є x-координатою точки A, $\phi(x)$ - функція відображення елементів поля у ненульові цілі числа. Початкове значення параметру s_0 формується із використанням процедури ініціалізації, яка включає введення секретного ключа (*Key*), що задає початкову ентропію (невизначеність), та хешування введеного ключа із форматуванням отриманого результату до визначеної довжини бітів. Отримане таким значення Seed засіює (ініціює) початкове значення параметру: $s_0 = \text{Seed}$.

Друге скалярне множення на фіксовану (базову) точку Q виконується для формування проміжного стану r_i, яке після відповідного перетворення і задає значення формованих псевдовипадкових бітів. Значення параметру r_i залежить від сформованого у результаті першого скалярного множення параметра s_i та від значення базової точки Q: $r_i = \phi(x(s_iQ))$.

Отримане таким чином значення r_i є вихідним для формування псевдовипадкових бітів, які формуються шляхом зчитування блоку з найменш значущих (правих) бітів числа r_i. ПВП формується шляхом конкатенації зчитаних бітів формованих чисел r_i. Значення фіксованих (базових) точок задаються у вигляді констант і під час формування ПВП не змінюються.

Структурну схему генератору ПВП із використанням перетворень на еліптичних кривих відповідно до рекомендацій стандарту NIST SP 800-90 наведено на рис. 1.

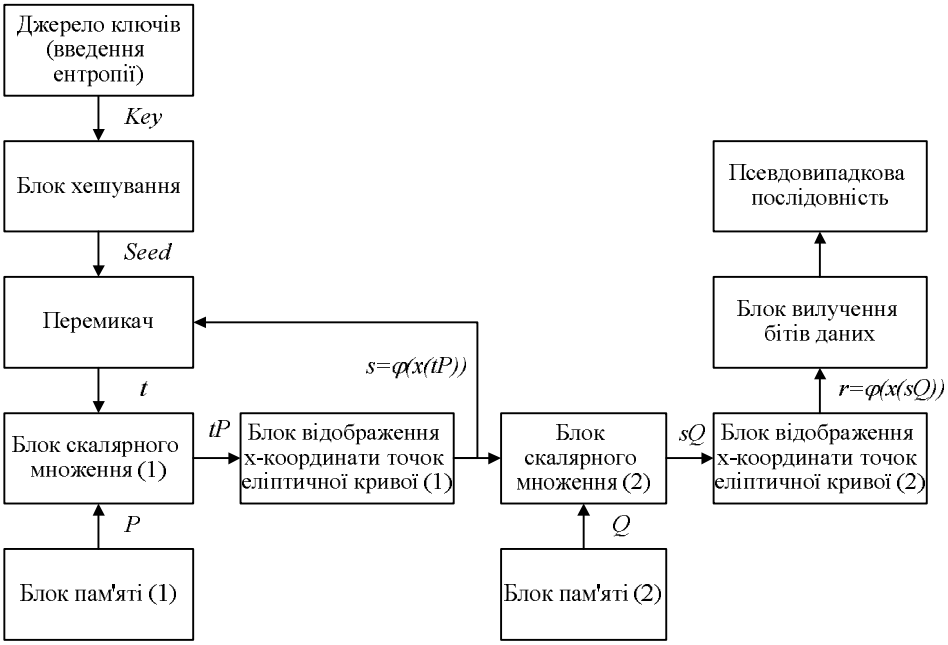

Рис. 1. Структурна схема генератору ПВП із використанням перетворень на еліптичних кривих (відповідно до рекомендацій NIST SP 800-90)

В роботі [4] проведено дослідження періодичних властивостей розглянутого генератору ПВП, зокрема проведено порівняння отримуваних довжин періодів послідовностей із максимальним періодом, який можна отримати для заданої довжини ключів та групи точок еліптичної кривої.

За максимальний період формованих ПВП, приймемо значення [4]

$$L_{max} = \min(L_{max}(K), L_{max}(S), k), \qquad (1)$$

де $L_{max}(K) = 2^{l_K} - 1$, l_K – довжина секретного ключа (бітів); $L_{max}(S) = 2^{l_S} - 1$, $l_S = \log_2(\text{Seed})$ - бітова довжина значення Seed; k – порядок точки *P* еліптичної кривої.

Максимального періоду формовані послідовності досягнуть у випадку, коли елементи послідовності

$$r_0, r_1, \ldots, r_{i-1}, r_i, \ldots r_{i+1}, \ldots, r_{L-1}, r_0, r_1, \ldots, \qquad (2)$$

будуть приймати кожне із

$$\min(2^{l_K} - 1, 2^{l_S} - 1, k)$$

ненульових значень.

Фактично це означає, що застосована функція $\phi(x)$ відображення елементів поля у ненульові цілі числа на кожній і-й ітерації для кожної сформованої точки $s_{i-1}P$ повинна формувати унікальне ціле число. Але це неможливо за визначенням. Дійсно, порядок m групи H_{EC} точок еліптичних кривих, які застосовуються для криптографічних додатків, зокрема і у передбачених рекомендаціями стандарту NIST SP 800-90 випадках, обмежений виразом:

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

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

Тобто за визначенням групи точок еліптичної кривої можуть виникати випадки, коли порядок групи точок може бути вищим за порядок кінцевого поля, над яким формуються значення функції $\phi(x)$. Фактично це означає, що для деяких елементів групи H_{EC}, наприклад, для точок P_i і P_j, $P_i \ne P_j$ функція $\phi(x)$ поверне тотожні значення. В розглянутому випадку застосовування арифметики еліптичних кривих у генераторі псевдовипадкових чисел це буде означати рівність значень станів $s_i = s_j$ для деяких $i \ne j$, де $s_i = \phi(x(s_{i-1}P)) = \phi(x(P_i))$ і $s_j = \phi(x(s_{j-1}P)) = \phi(x(P_j))$,

причому $|i - j| < L_{max}$. Тобто значення реальних періодів L формованих послідовностей станів (2) будуть нижчі за максимальний період (1).

Таким чином, за введеним у рекомендаціях стандарту NIST SP 800-90 правилом формування ПВП із застосуванням арифметики еліптичних кривих не буде отримано максимальні періоди послідовностей. Крім того, як показують проведені експериментальні дослідження [4], реальні періоди послідовностей будуть значно менші за максимальні.

2. Удосконалений метод формування ПВП максимального періоду із використанням перетворень на еліптичних кривих

Поставлена задача забезпечення максимального періоду формованих ПВП вирішується в [5] за рахунок додаткового введення у розглянутий вище генератор певних рекурентних перетворень. Структурну схему удосконаленого генератору ПВП із використанням перетворень на еліптичних кривих наведено на рис. 2.

Перше скалярне множення на фіксовану (базову) точку P, як і у генераторі, що відповідає рекомендаціям NIST SP 800-90, виконується для формування проміжного стану s_i, яке циклічно оновлюється на кожній ітерації при функціонуванні відповідного генератору. Але принциповою відмінністю є процес формування цього проміжного стану. Для забезпечення максимального періоду послідовностей $\dots s_{i-1}$, s_i, $\dots s_{i+1} \dots$ в удосконаленому методі пропонується використовувати рекурентне перетворення, яке ініціюється введеним секретним ключем (*Key*).

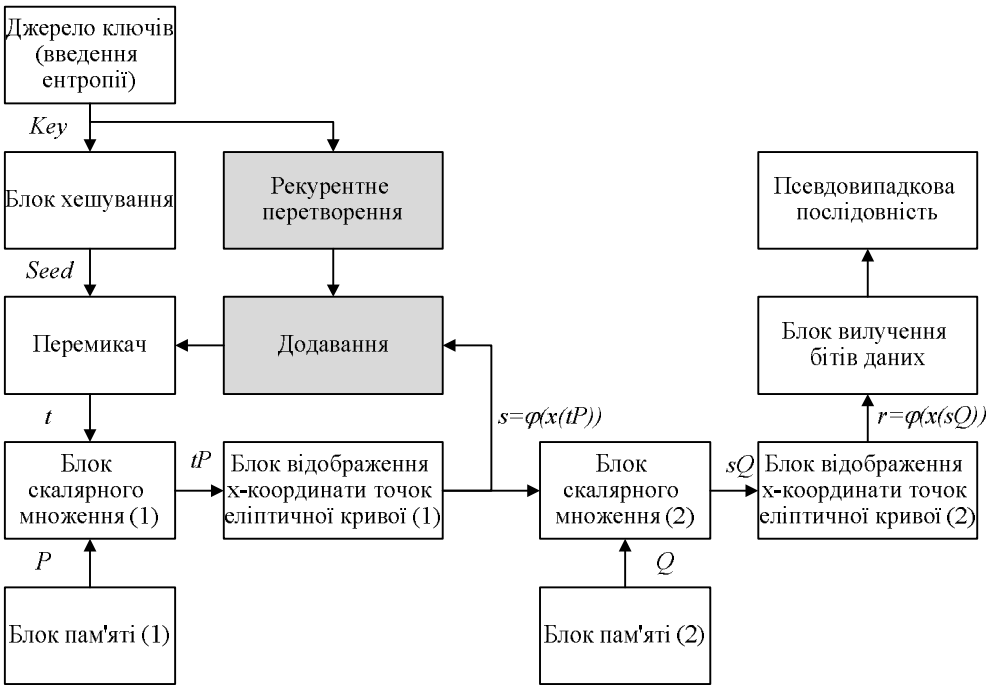

Рис. 2. Структурна схема удосконаленого генератору ПВП із використанням перетворень на еліптичних кривих

Таким чином кожне наступне значення стану s_i залежить не тільки від значення попереднього стану s_{i-1} (на попередній ітерації) та від значення базової точки P, але і від результату виконання рекурентного перетворення (позначимо його через $LRR(y)$), тобто:

$$s_i = \phi(x((s_{i-1} + LRR(y))P)),$$

де $x(A)$ - є x-координатою точки A, $\phi(x)$ - функція відображення елементів поля у ненульові цілі числа.

Сутність запропонованого удосконаленого методу формування послідовностей псевдовипадкових чисел полягає в тому, що ключова послідовність подається у вигляді вектору x_0, який ініціалізує початкове значення аргументу функції скалярного добутку точки еліптичної кривої $f(x) = x \cdot P$, де P - точка еліптичної кривої (загальносистемний параметр), яка належить групі точок EC_n порядку n, та початкове значення y_0 рекурентного перетворення L(y), що реалізуються, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками.

Наступне значення x_i аргументу функції $f(x)$ обчислюється за допомогою рекурентного перетворення (що реалізується, наприклад, за допомогою лінійних рекурентних регістрів зі зворотними зв'язками), за допомогою пристроїв скалярного множення x_{i-1} на базову точку P

$$P'_i = \left(x_{i-1} + L\left(y_{i-1}\right)\right) \cdot P,$$

та перетворення $\phi\left(P'_i\right)$ координат отриманої точки $P'_i \in EC_n$ за допомогою відповідних пристроїв (наприклад, x_i може дорівнюватися значенню однієї з координат точки P'_i), тобто

$$x_i = \phi\left(P'_i\right) = \phi\left(f\left(x_{i-1} + L\left(y_{i-1}\right)\right)\right) =$$
$$= \phi\left(\left(x_{i-1} + L\left(y_{i-1}\right)\right) \cdot P\right).$$

Отримані значення x_i подаються у вигляді аргументу функції скалярного добутку точки еліптичної кривої

$$f'\left(x\right) = x \cdot Q,$$

де Q - точка еліптичної кривої (загальносистемний параметр), яка належить групі точок EC_n порядку n.

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

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

де b_i - молодший біт числа z_i,

$$z_i = \phi\left(f'\left(x_i\right)\right) = \phi\left(x_i \cdot Q\right).$$

Формалізовано формування ПВП при застосуванні лінійних рекурентних регістрів (позначимо їх через LRR) можна подати у такий спосіб.

Секретний ключ: Key;

Константи: P, Q - точки ЕК порядку n;

Початковий стан: x_0 = Key, y_0 = Key ;

Циклова функція:

$$\phi(f(x + LRR(y))) = \phi((x + LRR(y))P), \quad (3)$$

$$LRR(y = \{u_1, u_2, \ldots, u_m\}): u_i = -\sum_j a_j u_{i-j} + u_i$$

де: $\{u_1, u_2, \ldots, u_m\}$ – стан LRR, $\{a_1, a_2, \ldots, a_m\}$ – коефіцієнти, які задають функцію зворотного зв'язку LRR, $\phi(P'_i)$ - перетворення координат точки $P'_i \in EC_n$ (наприклад, зчитування значення однієї з координат точки P'_i).

Формована ПВП $(b_0, b_1, \ldots, b_i, \ldots)$,

де b_i – найменш значущій біт (біт парності) числа z_i,

$$z_i = \phi(f'(\phi((x_{i-1} + LRR(y_{i-1}))P))) =$$
$$\phi(\phi((x_{i-1} + LRR(y_{i-1}))P)Q);$$
$$y_i = LRR(y_{i-1}).$$

За рахунок додаткового введення рекурентних перетворень, що реалізуються, 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.

3. Прискорене формування псевдовипадкових послідовностей максимального періоду та пропозиції щодо його реалізації

Запропонований метод формування псевдовипадкових послідовностей із використанням перетворень у групі точок еліптичної кривої можна реалізувати у спрощеному варіанті через подання вихідних елементів послідовності псевдовипадкових чисел шляхом зчитування значення функції скалярного добутку за допомогою відповідних пристроїв, тобто шуканою послідовністю біт довжини m буде послідовність

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

де b_i - молодший біт числа x_i,

$$x_i = \phi\left(P'_i\right) = \phi\left(f\left(x_{i-1} + L\left(y_{i-1}\right)\right)\right) =$$
$$= \phi\left(\left(x_{i-1} + L\left(y_{i-1}\right)\right) \cdot P\right).$$

Точка еліптичної кривої Q як загальносистемний параметр при цьому не використовується як і функція скалярного добутку $f'\left(x\right) = x \cdot Q$.

Структурна схема прискореного генератору псевдовипадкових послідовностей із використанням перетворень на еліптичних кривих наведено на рис. 3.

В пропонованому методі прискореного формування псевдовипадкових послідовностей застосовується лише одне скалярне множення на фіксовану (базову) точку P. Це головна відмінність від дослідженого вище удосконаленого генератора і саме за рахунок скорочення операцій скалярного множення точок еліптичної кривої досягається прискорене формування псевдовипадкових послідовностей.

Формування проміжного стану s_i, яке циклічно оновлюється на кожній ітерації при функціонуванні відповідного генератору, виконується із застосуванням рекурентних перевореннь, що забезпечують максимальний період відповідних послідовностей $\ldots s_{i-1}$, s_i, $\ldots s_{i+1} \ldots$. Тобто, кожне наступне значення s_i залежить не тільки від значення попереднього стану s_{i-1}, але й від $LRR(y)$, тобто:

$$s_i = \phi(x((s_{i-1} + LRR(y))P)),$$

де $x(A)$ є x-координатою точки A, $\phi(x)$ - функція відображення елементів поля у ненульові цілі числа.

Початкове значення параметру s_0 формується за розглянутою вище схемою.

Друге скалярне множення на фіксовану (базову) точку Q не виконується, тобто послідовність станів $\ldots r_{i-1}$, r_i, $r_{i+1}, \ldots$ не обчислюється.

Вихідним для формування псевдовипадкових бітів є сформоване значення s_i, тобто окремі біти псевдовипадкової послідовності формуються шляхом зчитування блоку з найменш значущих (правих) бітів числа s_i. Псевдовипадкова послідовність фор-

мується шляхом конкатенації зчитаних бітів формованих чисел s_i. Значення точки P задаються у вигляді константи і не змінюються під час формування псевдовипадкової послідовності.

Періодичні властивості станів … s_{i-1}, s_i, s_{i+1},…. визначаються періодичними властивостями додатково введеного рекурентного перетворення LRR(y). Схематично цей вплив наведено на рис. 4.

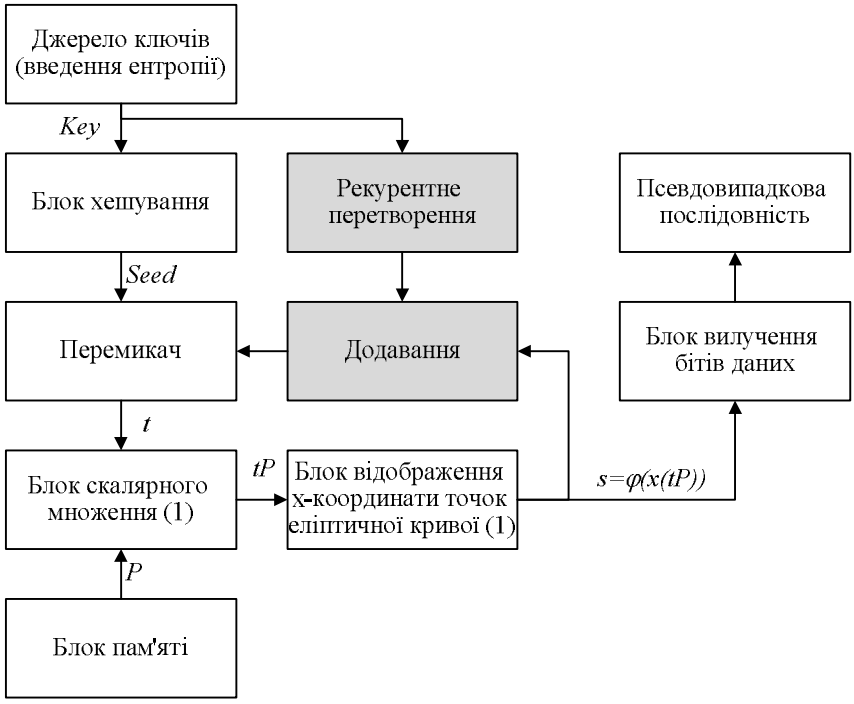

Рис. 3. Структурна схема прискореного генератору
псевдовипадкових послідовностей із використанням перетворень на еліптичних кривих

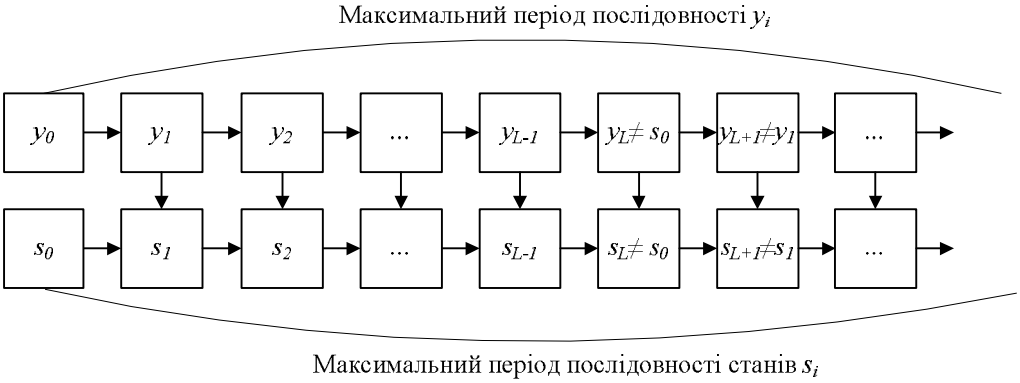

Рис. 4. Схема формування послідовностей станів прискореного генератору
з максимальним періодом псевдовипадкових послідовностей

Формалізовано спрощене (прискорене) формування псевдовипадкових послідовностей при застосуванні лінійних рекурентних регістрів (позначимо їх через LRR) можна подати у такий спосіб.

Секретний ключ: Key;

Константи: P - точка ЕК порядку n;

Початковий стан: $x_0 = Key$, $y_0 = Key$;

Циклова функція визначається виразом (3).

Формована псевдовипадкова послідовність:

$$(b_0, b_1, \ldots, b_i, \ldots)$$

де b_i – найменш значущій біт (біт парності) числа z_i,

$z_i = \phi((x_{i-1} + LRR(y_{i-1}))P)$, $y_i = LRR(y_{i-1})$.

Пристрій прискореного формування псевдовипадкових послідовностей реалізується як показано на рис. 5, тобто без другого блоку скалярного множення точок еліптичної кривої та без другого блоку формування внутрішніх станів. При цьому значення x_{i+1} з першого блоку формування початкових станів подається як на блок додавання так і на блок формування вихідної послідовності замість значення z_{i+1}. Решта послідовність операцій тотожна розглянутій вище.

Запропонований пристрій (рис. 5) формування послідовностей псевдовипадкових чисел містить вхід, вихід, блок вводу ключових даних, блок формування початкових станів, блок скалярного мно-

ження точок еліптичної кривої, блок формування внутрішніх станів, блок формування вихідної послідовності, блок узгодження та додатково введені блок рекурентного перетворення та блок додавання.

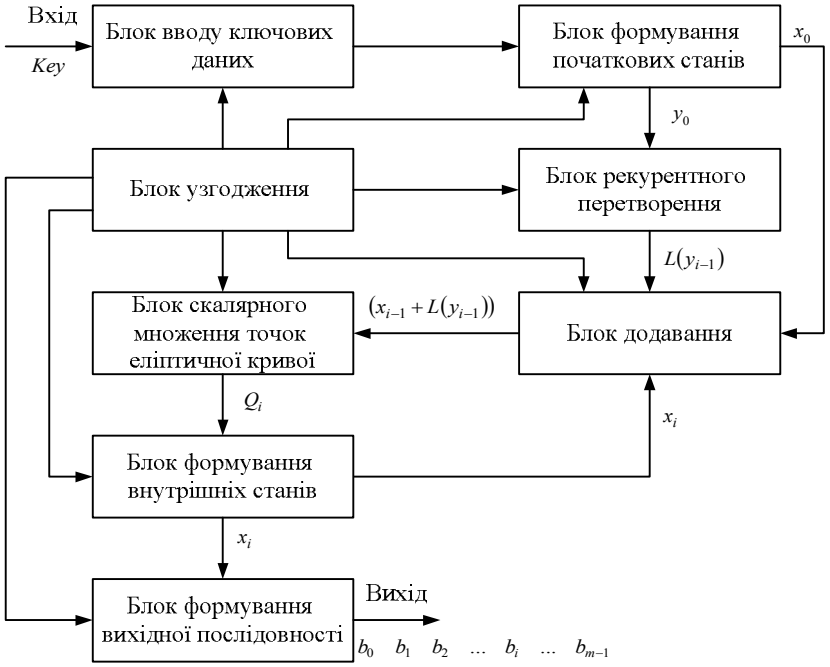

Рис. 5. Структурна схема пристрою спрощеного формування псевдовипадкових послідовностей максимального періоду із використанням перетворень у групі точок еліптичної кривої

Елементи пристрою з'єднанні таким чином.

Вхід пристрою підключено до входу блоку вводу ключових даних, вихід якого підключено до входу блоку формування початкових станів, виходи блоку формування початкових станів підключено до входу блоку рекурентного перетворення та до входу блоку додавання, вихід блоку рекурентного перетворення підключено до входу блоку додавання, вихід якого підключено до входу блоку скалярного множення точок еліптичної кривої, вихід блоку скалярного множення точок еліптичної кривої підключено до входу блоку формування внутрішніх станів, вихід якого підключено до входу боку 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 блоку вводу ключових даних, блоку формування початкових станів, блоку скалярного множення точок еліптичної кривої, блоку формування внутрішніх станів, блоку формування вихідної послідовності, блоку рекурентного перетворення та блоку додавання, відповідно.

Робота запропонованого пристрою полягає в наступному. В блок вводу ключових даних вводиться послідовність Key, яка виступає у якості секретного ключа. Вона передається у блок формування початкових станів, який призначений для формування початкового значення x_0 аргументу функції скалярного добутку точки еліптичної кривої $f(x) = x \cdot P$ 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 $i = 1$) як і сформований початковий стан x_0 подається на вхід блоку додавання. У блоку додавання обчислюється значення $(x_{i-1} + L(x_{i-1}))$, отриманий результат подається на вхід блоку скалярного множення точок еліптичної кривої. У блоку скалярного множення точок еліптичної кривої розраховується значення

$$Q_i = (x_{i-1} + L(x_{i-1})) \cdot P,$$

яке подається на вхід блоку формування внутрішніх станів.

В блоку формування внутрішніх станів виконується функціональне перетворення

$$x_i = \phi(Q_i) = \phi(f(x_{i-1} + y_{i-1})) = \phi((x_{i-1} + L(x_{i-1})) \cdot P),$$

виходом якого є нове значення внутрішнього стану x_i, яке подається на вхід блоку формування вихідної послідовності та на вхід додавання.

В блоку формування вихідної послідовності зі значення x_i зчитується найменш значущій біт даних (біт парності), який подається на вихід пристрою як елемент псевдовипадкової послідовності.

Наступна ітерація роботи пристрою починається з подання 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 призначений для погодження роботи окремих блоків пристрою та управління процесом формування псевдовипадкової послідовності. Пристрій зупиняє свою роботу за командою блоку узгодження (зупинку можна здійснити на кожному кроці).

Таким чином, розроблений метод заснований на зведенні задачі знаходження таємного ключа до вирішення теоретико-складної задачі дискретного логарифмування у групі точок еліптичної кривої і дозволяє формувати псевдовипадкові послідовності максимального періоду.

Висновки

Запропонований метод формування псевдовипадкових послідовностей із використанням перетворень на еліптичних кривих забезпечує формування максимального періоду послідовностей внутрішніх станів і відповідних точок еліптичної кривої. Для його практичного використання обґрунтовано пропозиції щодо реалізації пристрою (генератору), в який додатково введені (по відношенню до методу-прототипу, який обрано відповідно до специфікації стандарту NIST SP 800-90) блок рекурентного перетворення та блок додавання.

Запропонований метод можна реалізувати у спрощеному варіанті, при цьому для прискореного формування псевдовипадкових послідовностей застосовується лише одне скалярне множення на фіксовану (базову) точку еліптичної кривої. Саме за рахунок скорочення операцій скалярного множення точок еліптичної кривої досягається прискорене формування псевдовипадкових послідовностей.

Таким чином, запропоновані методи та засоби формування псевдовипадкових послідовностей задовольняють сучасним вимогам, що висуваються до механізмів захисту інформації телекомунікаційних систем та мереж. В той же час, як показали проведені дослідження, використання більш складних алгебраїчних кривих (гіпереліптичних, значення роду яких $g > 1$) є більш ефективним за співвідношенню криптографічна стійкість/складність обчислення. Відповідно, *перспективним напрямком подальших досліджень* слід вважати використання перетворень на гіпереліптичних кривих для побудови методів та засобів формування псевдовипадкових послідовностей, обґрунтування пропозицій щодо їхньої реалізації для забезпечення безпеки телекомунікаційних систем та мереж.

Список літератури

1. *Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.*
2. *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.*
3. *Barker E. Recommendation for random number generation using deterministic random bit generators / E. Barker, J. Kelsey, National Institute of Standards and Technology, January 2012, 124 p. – Attached to: http://csrc.nist.gov/ publications/nistpubs/800-90A/SP800-90A.pdf.*
4. *Сорока Л.С. Властивості генераторів псевдовипадкових послідовностей на еліптичних кривих / Л.С. Сорока, О.О. Кузнецов, Д.І. Прокопович-Ткаченко // Вісник Академії митної служби України. Серія: «Технічні науки». – 2012. – № 1 (47). – С. 5-15.*

Надійшла до редколегії 30.01.2013

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський національний університет радіоелектроніки, Харків.

УСКОРЕННОЕ ФОРМИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ МАКСИМАЛЬНОГО ПЕРИОДА С ПРЕОБРАЗОВАНИЯМИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Д.И. Прокопович-Ткаченко

Исследуются методы формирования псевдослучайных последовательностей для построения механизмов повышения безопасности информационных систем и технологий. Рассматривается генератор псевдослучайных последовательностей с применением преобразований в группе точек эллиптических кривых (в соответствии со стандартом NIST SP 800-90), показаны его недостатки относительно периодических свойств формуемых последовательностей. Исследуется усовершенствованный метод, который за счет дополнительного введения рекуррентного преобразования позволяет формировать последовательности псевдослучайных чисел максимального периода. Предлагается реализовать усовершенствованный метод в упрощенном варианте для ускоренного формирования псевдослучайных последовательностей.

Ключевые слова: *безопасность, информационная система, генератор, псевдослучайная последовательность.*

FORMING OF PSEUDOCASUAL SEQUENCES OF MAXIMAL PERIOD A SPEED-UP WITH TRANSFORMATIONS ON ELLIPTIC CURVES

D.I. Prokopovich-Tkachenko

The methods of forming of pseudocasual sequences are probed for the construction of mechanisms of increase of safety of the informative systems and technologies. The generator of pseudocasual sequences is examined with application of transformations to the group of points of elliptic curves (in accordance with the standard of NIST SP 800-90), his failings are rotined in relation to periodic properties of mouldable sequences. The improved method which due to additional introduction of recurrent transformation allows to form the sequences of pseudocasual numbers of maximal period is probed. It is suggested to realize the improved method in the simplified variant for the speed-up forming of pseudocasual sequences.

Keywords: *safety, informative system, generator, pseudocasual sequence.*