УДК 621.396

Л. С. Сорока, доктор технічних наук, ректор Академії митної служби України
О. О. Кузнецов, доктор технічних наук, начальник кафедри АСУ Харківського університету Повітряних сил ім. І. Кожедуба
Д. І. Прокопович-Ткаченко, аспірант Академії митної служби України

ВЛАСТИВОСТІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ЕЛІПТИЧНИХ КРИВИХ

Розглядаються методи формування псевдовипадкових послідовностей для криптографічних застосувань, зокрема для побудови механізмів забезпечення безпеки інформаційних систем і технологій. Досліджуються властивості генератора псевдовипадкових послідовностей з використанням перетворень у групі точок еліптичних кривих (відповідно до стандарту NIST SP 800-90). Установлено певні недоліки досліджуваного генератора щодо періодичних властивостей формованих послідовностей, зокрема показано, що періоди формованих послідовностей значно менші за максимальні.

Рассматриваются методы формирования псевдослучайных последовательностей для криптографических приложений, в частности для построения механизмов обеспечения безопасности информационных систем и технологий. Исследуются свойства генератора псевдослучайных последовательностей с использованием преобразований в группе точек эллиптических кривых (в соответствии со стандартом NIST SP 800-90). Определены некоторые недостатки исследуемого генератора относительно периодических свойств формируемых последовательностей, в частности показано, что периоды формируемых последовательностей значительно меньше максимальных.

There are considered the methods of pseudorandom sequences formation for cryptographic applications, in particular for the construction of mechanisms of providing security of information systems and technologies. There are analyzed the properties of pseudorandom sequence generator with the use of transformations in the group of points of elliptic curves (according to the standard NIST SP 800-90). There are determined certain defects of studied generator related to periodic properties of the formed sequences, in particular this indicates that periods of formed sequences are considerably smaller than the maximum ones.

Ключові слова. Псевдовипадкові послідовності, генератор, еліптичні криві.

Вступ. Перспективний напрямок у розвитку механізмів забезпечення безпеки митних інформаційних систем і технологій – розробка методів формування псевдовипадкових послідовностей та дослідження властивостей відповідних генераторів [1–3]. Це особливо важливо для реалізації процедур електронного декларування.

Генератори псевдовипадкових чисел – це технічні пристрої, які призначені для вироблення послідовностей псевдовипадкових чисел, що задовольняють певні статистичні властивості. Вони належать до найрозвиненіших методів криптографічного перетворення і застосовуються в більшості сучасних механізмів захисту інформації [1–2]. Найвдаліші в цьому сенсі методи формування псевдовипадкових послідовностей, стійкість яких базується на зведенні завдання відновлення секретних ключових даних (або правила формування послідовностей) до виконання добре відомого і надзвичайно складного математичного завдання з теорії чисел, наприклад завдання факторизації, дискретного логарифмування тощо [1–3].

Постановка завдання. Цю працю присвячено дослідженню властивостей генераторів псевдовипадкових послідовностей з використанням перетворень на еліптичних кривих.

Результати дослідження. *Перетворення у групі точок еліптичної кривої.* Розглянемо математичні перетворення у групі точок еліптичної кривої, які лежать в основі побудови генераторів псевдовипадкових чисел [1–5].

Нехай задано просте число $p > 3$. Тоді *еліптичною кривою E*, визначеною над кінцевим простим полем *GF (p)*, називається множина пар чисел (x, y), $x, y \in GF(p)$, що задовольняють тотожності:

$$y^2 \equiv x^3 + ax + b \pmod{p}, \qquad (1)$$

де $a, b \in F_p$ і виконано умову $4a^3 + 27b^2 \neq 0 \pmod{p}$.

Пари (x, y), що задовольняють тотожності (1), називаються *точками еліптичної кривої E*, числа x і y, відповідно, – x- і y-*координатами* точки.

Точки еліптичної кривої позначатимемо $Q(x, y)$, $P(x, y)$ або просто Q, P. Дві точки еліптичної кривої рівні, якщо рівні їх відповідні x- та y-координати.

На множині всіх точок еліптичної кривої E введемо *операцію додавання*, яку позначатимемо знаком “+”.

Для двох довільних точок $P_1\ (x_1, y_1)$ та $P_2\ (x_2, y_2)$ еліптичної кривої E розглянемо декілька варіантів.

Нехай координати точок P_1 і P_2 задовольняють умову $x_1 \neq x_2$. У цьому випадку їх сумою називатимемо точку $P_3\ (x_3, y_3)$, координати якої визначаються рівняннями

$$\begin{cases} x_3 \equiv \left(\lambda^2 - x_1 - x_2\right) \bmod (p) \\ y_3 \equiv \left(\lambda\left(x_1 - x_2\right) - y_1\right) \bmod (p), \end{cases} \tag{2}$$

де

$$\lambda \equiv \left(\frac{y_2 - y_1}{x_2 - x_1}\right) \bmod (p).$$

Геометричну інтерпретацію операції додавання точок еліптичної кривої подано на рис. 1. Результат додавання – це точка $P_3\ (x_3, y_3)$, яка симетрична відносно осі абсцис (з оберненою y-координатою) до точки $-P_3\ (x_3, -y_3)$ перетину прямої лінії, що проходить через визначені точки $P_1\ (x_1, y_1)$ і $P_2\ (x_2, y_2)$, та еліптичної кривої.

Якщо виконано рівність $x_1 = x_2$ та $y_1 = y_2 \neq 0$, тоді координати точки P_3 визначимо таким чином (операція подвоєння точки):

$$\begin{cases} x_3 \equiv \left(\lambda^2 - 2x_1\right) \bmod (p) \\ y_3 \equiv \left(\lambda\left(x_1 - x_3\right) - y_1\right) \bmod (p), \end{cases} \tag{3}$$

де

$$\lambda \equiv \left(\frac{3x_1^2 + a}{2y_1}\right) \bmod (p).$$

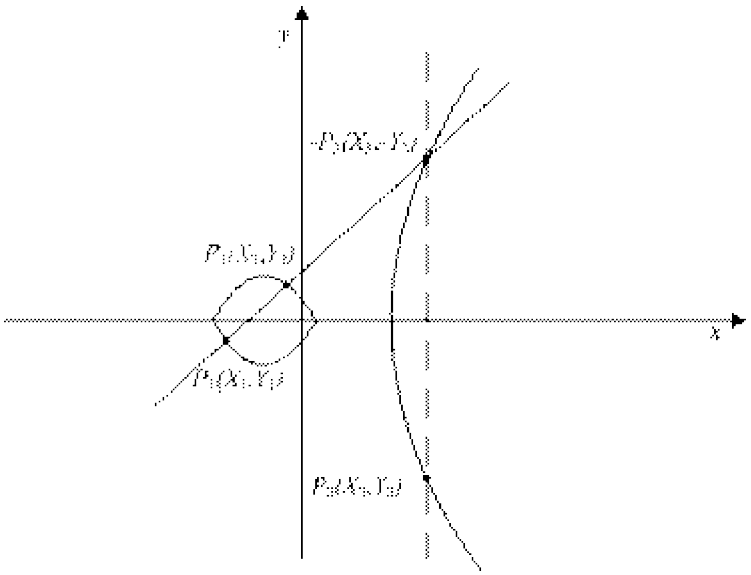

Рис. 1. Додавання точок еліптичної кривої

На рис. 2 наведено графічну інтерпретацію такого додавання. Фактично маємо збіг точок $P_1\ (x_1, y_1)$ та $P_2\ (x_2, y_2)$, тобто операцію додавання слід інтерпретувати як подвоєння точки $P_1\ (x_1, y_1) = P_2\ (x_2, y_2)$. Результатом подвоєння є точка $P_3\ (x_3, y_3)$, яка симетрична відносно осі абсцис (з оберненою y-координатою) до точки $-P_3\ (x_3, -y_3)$ перетину прямої лінії, що є дотичною в точці $P_1\ (x_1, y_1) = P_2\ (x_2, y_2)$, та еліптичної кривої.

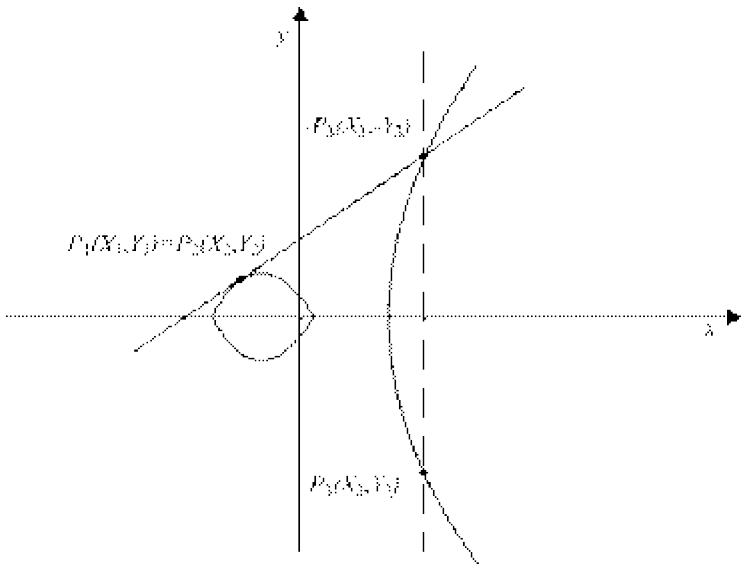

Рис. 2. Подвоєння точок еліптичної кривої

У разі, коли виконано умову $x_1 = x_2$ та $y_1 = - y_2$ (mod p), суму точок P_1 та P_2 називатимемо *нульовою точкою O*, не визначаючи її *x*- і *y*-координати. У цьому випадку точка P_2 називається *запереченням* точки P_1. Для нульової точки *O* виконано рівність

$$P + O = O + P = P, \tag{4}$$

де *P* – довільна точка еліптичної кривої *E*.

Щодо введеної операції додавання множина всіх точок еліптичної кривої *E*, разом з нульовою точкою, утворюють кінцеву абелеву (комутативну) групу H_{EC} порядку *m*, для якої виконано нерівність:

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

Точка *Q* називається точкою кратності *k*, або просто кратною точкою еліптичної кривої *E,* якщо для деякої точки *P* виконано рівність:

$$Q = \underbrace{P + P + \ldots + P}_{k \text{ разів}} = kP \tag{5}$$

Операція, яку визначено формулою (5), має назву скалярного множення точок еліптичної кривої, де *k* – скаляр, на який формально множиться точка *P*. Точка *P* має порядок *k*, якщо її скалярне множення на *k* дорівнює нульовій точці *O*, тобто якщо $kP = O$.

Розглянуті перетворення в групі точок еліптичних кривих використовуються під час побудови криптосистем з відкритим ключем [2–4]. В основі обґрунтування їх стійкості лежить зведення завдання криптоаналізу до виконання теоретично складного завдання дискретного логарифмування в групі точок еліптичної кривої.

Скористаємося поняттям дискретного логарифма, введеного в [4, 5]. Нехай *H* – кінцева група, *g* і *y* – елементи цієї групи. Будь-яке ціле *x,* таке, що $g^x = y$, називається дискретним логарифмом *y* за основою *g*. Кожен елемент $y \in H$ має дискретний логарифм за основою *g* тоді і тільки тоді, коли *H* є циклічною групою з твірною *g*. У загальному випадку відомі алгоритми для обчислення дискретних логарифмів у групах порядку *m* мають приблизно однакову складність відносно *m*, як і для алгоритмів факторизації.

Стосовно групи точок еліптичної кривої використовують таке поняття дискретного логарифма на кривій [4, 5]. Нехай H_{EC} – кінцева група точок еліптичної кривої, P_i і P_j – елементи цієї групи. Будь-яке ціле *x* таке, що $xP_i = P_j$, називається дискретним логарифмом на еліптичній кривій. Криптостійкість алгоритмів, побудованих на еліптичних кривих, обґрунтовується складністю знаходження дискретного логарифма і полягає у визначенні *x* за відомими точками P_i і P_j.

Розглянуті перетворення на еліптичних кривих зазвичай застосовуються для побудови криптографічних протоколів з несиметричними ключами, зокрема в механізмах цифрового підпису тощо. В опублікованих рекомендаціях Національного інституту стандартів і технологій (National Institute of Standards and Technology – NIST) Сполучених Штатів Америки NIST SP 800-90 визначено конкретні механізми з формування псевдовипадкових послідовностей, у тому числі із застосуванням математичних перетворень на еліптичних кривих [3]. Розглянемо сутність запропонованого підходу, проведемо дослідження властивостей відповідних генераторів псевдовипадкових послідовностей.

Метод формування псевдовипадкових послідовностей на еліптичних кривих. Метод формування псевдовипадкових послідовностей з використанням перетворень на еліптичних кривих, який запропоновано в рекомендаціях NIST SP 800-90, базується на застосуванні двох скалярних множень точок еліптичної кривої та

відображенні відповідних x-координат отриманих результатів у ненульове ціле значення.

Перше скалярне множення на фіксовану (базову) точку P виконується для формування проміжного стану S_i, яке циклічно оновлюється на кожній ітерації під час функціонування відповідного генератора. Таким чином, значення стану S_i залежить від значення попереднього стану S_{i-1} (на попередній ітерації) та від значення базової точки P:

$$s_i = \varphi(x(s_{i-1}P)), \tag{6}$$

де $x(A)$ – x-координата точки A, $\varphi(x)$ – функція відображення елементів поля в ненульові цілі числа.

Початкове значення параметра s_0 формується з використанням процедури ініціалізації, яка включає введення секретного ключа (*Key*), що задає початкову ентропію (невизначеність), та хешування введеного ключа з форматуванням отриманого результату до визначеної довжини бітів. Отримане таким чином значення *Seed* задає (ініціює) початкове значення параметра: $s_0 = Seed$.

Друге скалярне множення на фіксовану (базову) точку Q виконується для формування проміжного стану v_i, яке після відповідного перетворення і задає значення формованих псевдовипадкових бітів. Значення параметра v_i залежить від сформованого в результаті першого скалярного множення параметра s_i та від значення базової точки Q:

$$r_i = \varphi(x(s_iQ)). \tag{7}$$

Отримане таким чином значення r_i є вихідним для формування псевдовипадкових бітів шляхом зчитування блоку з найменш значущих (правих) бітів числа r_i. Псевдовипадкова послідовність формується через конкатенацію зчитаних бітів формованих чисел r_i.

Значення фіксованих (базових) точок задаються у вигляді констант і під час формування псевдовипадкової послідовності не змінюються.

Структурну схему генератора псевдовипадкових послідовностей з використанням перетворень на еліптичних кривих, відповідно до розглянутих рекомендацій стандарту NIST SP 800-90, наведено на рис. 3.

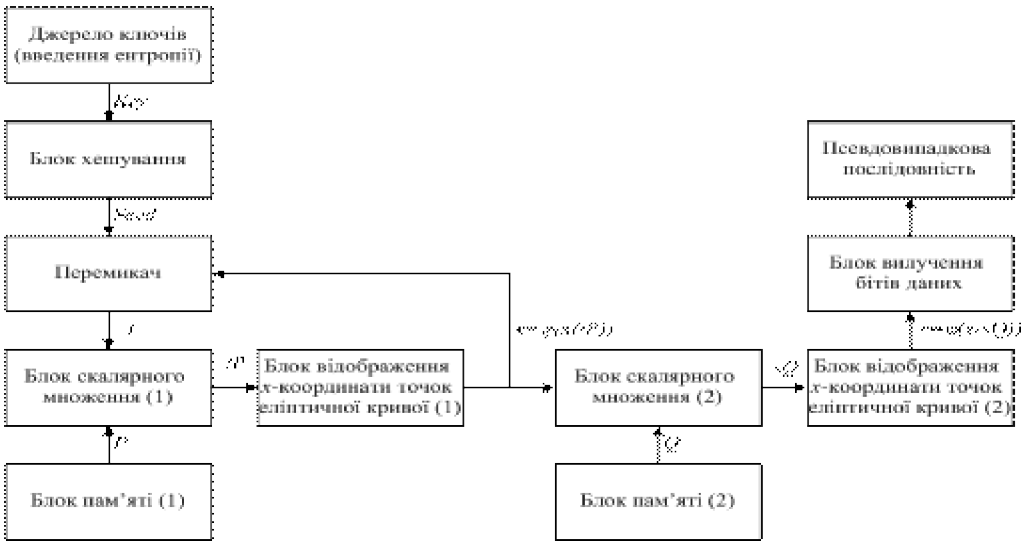

Рис. 3. Структурна схема генератора псевдовипадкових послідовностей з використанням перетворень на еліптичних кривих (відповідно до рекомендацій NIST SP 800-90)

Таким чином, розглянутий метод формування псевдовипадкових послідовностей застосовує перетворення у групі точок еліптичної кривої для формування проміжних станів s_i і r_i. Причому зворотна дія, тобто формування s_{i-1} за відомим s_i та/або формування s_i і відомим r_i пов'язана з виконанням теоретично складного завдання дискретного логарифмування у групі точок еліптичної кривої. Схему формування проміжних станів генератора подано на рис. 4.

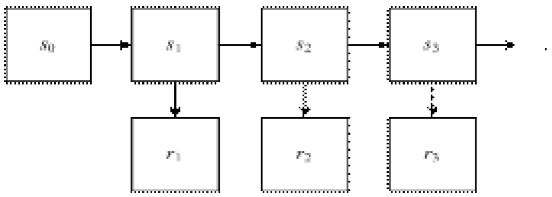

Рис. 4. Схема формування проміжних станів генератора

Як видно з рис. 4, послідовність станів $\ldots s_{i-1}, s_i, \ldots s_{i+1} \ldots$ формується з початкового значення $s_0 = Seed$, яке, у свою чергу, формується з даних секретного ключа. Кожне наступне значення s_i залежить від попереднього значення s_{i-1} і формується за допомогою скалярного множення базової точки еліптичної кривої за формулою (6).

Окремі біти псевдовипадкової послідовності формуються шляхом зчитування бітів послідовності чисел …