УДК 681.3.06

*Т. А. ГРИНЕНКО, Ю. И. ГОРБЕНКО, С. Ю. ОРЛОВА*

# МЕТОД ФОРМИРОВАНИЯ И СВОЙСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

**Введение**

Известно, что требуемый уровень криптографической защиты информации может быть обеспечен при условии, что ключи, параметры и пароли порождаются в системе случайно, равновероятно и независимо [1,2]. Для решения этих задач используются генераторы случайных и псевдослучайных последовательностей (ПСП). При программной и программно-аппаратной реализации криптографических средств в большинстве случаев практически невозможно или весьма сложно использовать чисто случайные процессы. Весьма сложно, а в ряде случаев и невозможно, использовать случайные реализации, когда последовательности большого периода должны однозначно восстанавливаться в пространстве и времени на различных объектах. В этом случае используют псевдослучайные последовательности с требуемыми свойствами. Так, для применения в криптографии ПСП должны обладать рядом свойств "случайности" их появления, иметь требуемый период повторения, высокую (требуемую) структурную скрытность законов формирования и др. [2]. Важной оперативно-технической характеристикой является вычислительная сложность формирования ПСП, которая может оцениваться, например, скоростью формирования символов в ПСП. В литературе эти требования интегрированы в понятии криптографически сильного генератора (КСГ). По определению Яо [4] КСГ можно считать такой генератор, в котором выходную последовательность генератора невозможно отличить от чисто случайной. Более точно криптографически сильным называют такой генератор, у которого никаким полиномиальным тестом невозможно определить, порождена ли его выходная последовательность псевдослучайным алгоритмом или выбрана случайно и равновероятно из множества всех последовательностей длины $l$.

Второе определение КГС основано на понятии непредсказуемости закона формирования символов и, в общем, звучит как требование невозможности предсказать никаким полиномиальным алгоритмом следующий бит последовательности на выходе генератора, если известны все предыдущие биты. Не останавливаясь на подробном анализе известных результатов в области КСГ, отметим, что общим подходом к созданию КСГ должно быть требование экспоненциальной сложности криптоанализа ПСП (в смысле определения закона её формирования). Поэтому поиск КСГ нужно вести с использованием преобразований, которые обладают экспоненциальной сложностью задач криптоанализа. К классу таких преобразований относятся преобразования на эллиптических кривых.

В 90-е годы разработан математический аппарат и созданы криптографические системы, преобразования в которых осуществляются в группах на эллиптических кривых [6]. В то же время в доступной литературе только указывается, буквально в виде термина, на возможность построения генератора ПСП на эллиптических кривых, но нет практических предложений и исследования свойств, формируемых таким образом ПСП. Целью настоящей статьи и является разработка и исследование свойств ПСП, формируемых с использованием генератора на эллиптических кривых.

## 1. Метод формирования псевдослучайных чисел на эллиптических кривых

Метод формирования базируется на рекуррентном вычислении и преобразовании псевдослучайных последовательностей и чисел на эллиптических кривых в полях Галуа [6].

Эллиптическая кривая (ЭК) над простым полем $GF(p)$, где $p$ – простое число, определяется множеством точек $P_i = (x_i, y_i)$.

Будем полагать, что координаты $x_i$ и $y_i$ принимают значения над простым полем $GF(p)$, т.е. в интервале $[1, p\text{-}1]$. Причём, каждая точка этой кривой удовлетворяет уравнению [6]:

$$y_q^2 = (x_q^3 + ax_q + b) \bmod p \qquad (1)$$

Кроме того, за счёт выбора параметров кривой выполняется условие:

$$4a^3 + 27b^3 \neq 0 (\bmod\ p) \qquad (2)$$

Суть метода формирования псевдослучайных чисел заключается в следующем. В качестве начального значения принимается случайное или псевдослучайное число $a_0 \in [1, P\text{-}1]$. Назовём его раз-

мерностью пространства внутренних состояний $l_0$. Правило формирования ПСП на эллиптической кривой представим в виде:

$$a_i = a_{i-1} * G(\text{mod } p), \qquad i = 1,2,\ldots,n \tag{3}$$

где $G$ - базовая точка эллиптической кривой (2) порядка $n$; $p$ – простое число; $a_0$ – случайное начальное состояние генератора (число); знак "*" означает операцию скалярного умножения, соответственно.

Если точка $G$ имеет порядок $n$, то максимальный период повторения будет равным $n$. Значение $G$ выбирается случайно из полного множества $\{G\}$.

При правильном выборе параметров $a$ и $b$ эллиптической кривой порядок эллиптической кривой $u_{ЭК}$ может изменяться для простого поля $GF(p)$ в интервале $p-2\sqrt{p+1} \le u_{ЭК} < p+ +2\sqrt{p+1}$ и зависит от значений $a$ и $b$.

Для конкретно выбранной базовой точки порядок эллиптической кривой моет быть связан с порядком базовой точки соотношением:

$$u_{эк} = h \cdot n, \tag{4}$$

причём, $h$ предпочтительно выбирать равным 2, 4, 8.

Соотношение (4) реализует скалярное умножение, его можно записать в виде:

$$a_i = (\underbrace{G + G + G + \ldots + G}_{a_{i-1}}) \bmod p \tag{5}$$

Поскольку $G$ - это точка на эллиптической кривой, то она имеет две координаты – $\{x_G, y_G\}$. Значение $a_i$, в общем случае, также принимает значение на эллиптической кривой, то есть имеет две координаты $(x_{ai}, y_{ai})$. В связи с тем, что $a_{i-1}$ должно быть числом, его будем формировать как:

$$a_{i-1} := \psi(a_{i-1}). \tag{6}$$

В простом случае:

$$a_{i-1} := x(a_{i-1}) \qquad \text{или} \qquad a_{i-1} := y(a_{i-1}). \tag{7}$$

В более сложном случае:

$$a_{i-1} := \psi(x_{ai-1}, y_{ai-1}), \tag{8}$$

где $\psi$ - функция нелинейного отображения, например, хеш-функция.

Таким образом, $a_{i-1}$ всегда будет целым числом.

Анализ (5) показывает, что оно имеет большую сложность, если его рассчитать выполнением операции сложения. Расчет в (5) можно свести к удвоению точки G и сложению двух различных точек.

Пусть точка имеет вид $G(x_1, y_1)$. Тогда удвоение:

$$G + G = 2(x_1, y_1) = (x_3, y_3). \tag{9}$$

Здесь координаты $(x_3, y_3)$ результирующей точки вычисляются следующим образом:

$$x_3 = \lambda^2 - 2x_1;\ y_3 = \lambda(x_1 - x_3) - y_1;\ \lambda = \frac{3x_1^2 + a}{2y_1}. \tag{10}$$

При сложении точек $G_1$ и $G_2$ имеем:

$$G_1 + G_2 = (x_1, y_1) + (x_2, y_2) = (x_3, y_3), \tag{11}$$

в этом случае:

$$x_3 = \lambda^2 - x_1 - x_2;\ y_3 = \lambda(x_1 - x_3) - y_1;\ \lambda = \frac{y_2 - y_1}{x_2 - x_1}. \tag{12}$$

Все операции в (10) и (12) выполняются по модулю $p$. Комбинируя операции удвоения и сложения, найдем скалярное произведение (5), то есть, $a_i=(x_{ai}, y_{ai})$.

В случае, когда нужно обеспечить меньшую вычислительную сложность формирования ПСП, а она для правила (3) хотя и носит полиномиальный характер, но остаётся ещё значительной, правило (3) можно реализовать в виде операций рекуррентного сложения точек на эллиптической кривой. Тогда:

$$G_i = (G_{i-1} + G_k) \bmod p, \tag{13}$$

где $G_k$ – есть ключевая точка (ключ) на эллиптической кривой, или

$$G_i = (2G_{i-1}) \bmod p. \tag{14}$$

где $G_0$ – базовая точка на эллиптической кривой.

**2. Разработка алгоритма формирования псевдослучайных чисел на эллиптической кривой**

Анализ показывает, что для реализации генератора ПСП на эллиптических кривых необходимо сформировать общесистемные параметры – простое число $p$ требуемой величины, и базовую точку $G$ порядка $n$. Это вполне разрешимая задача и требует отдельного рассмотрения. Здесь мы выберем из [7] стандартные общесистемные параметры.

*Входные данные:* параметры эллиптической кривой, т.е. простое число $p$, длиной 192 бита, параметры кривой $a$ и $b$, а также базовая точка $G$ порядка $n$ с коэффициентом связи $h$.

*Выходные данные:* последовательность $a_n$, полученная посредством применения функции выделения координаты $x$ точки $G$: $\psi=\psi(x)$, и последовательность $a_j$, полученная посредством применения хеш-функции MD5: $\psi=\psi(x,y)$.

**Алгоритм.**

1. Согласно [8] параметры области случайной эллиптической кривой над $F_p$ определены вектором T=(p,a,b,G,n,h), где конечное поле $F_p$ определено как:

$p$= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF = $2^{192}$-$2^{64}$-1

Кривая $E: y^2=x^3+ax+b$ над $F_p$ определяется как:

$a$= FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFC
$b$= 64210519 E59C80E7 0FA7E9AB 72243049 FEB8DEEC C146B9B1

Базовая точка:

$G$= 04 188DA0E B03090F6 7CBF20EB 43A18800 F4FF0AFD 82FF1012
07192B95 FFC8DA78 631011ED 6B24CDD5 73F977A1 1E794811

Порядок $n$ точки $G$ и кофактор (коэффициент связи) $h$:

$n$= FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831
$h$= 01

2. Начальное значение $a_0$, целое 192-битное число, выбираем случайным образом.
3. Определяем длину последовательности *count*.
4. Открываем файл *gen.out* для записи выходной последовательности $a_i$ и файл *genhash.out* для записи выходной последовательности $a_j$.
5. Расчёт выходной последовательности:

Для $k$ от 0 до *count* выполнять:

5.1. $a_k=a_0*G(mod\ p)=(x_{a_0}, y_{a_0})$

5.2. $a_i := x_{a_0}$;

5.3. Запись $a_i$ в *gen.out*.

5.4. $a_i := Hash(x,y)$;

5.5. Запись $a_j$ в *genhash.out*.

Результатом данного алгоритма будут две выходные последовательности, записанные в соответствующие файлы. Длина каждого отдельного числа последовательности, полученной в результате

выделения координаты $x$ полученной точки, равна 192 битам. Длина чисел второй последовательности равна 128 битам.

В процессе разработки программного модуля была использована библиотека многократной точности, разработанная на кафедре БИТ ХТУРЭ.

### 3. Анализ генератора псевдослучайных чисел на эллиптической кривой

Результаты исследования генератора псевдослучайных чисел на эллиптической кривой показали, что выходные последовательности, сформированные с помощью такого генератора, обладают гарантированной длиной периода равной порядку $n$ базовой точки $G$. В данной работе рассматривались последовательности, длина периода которых равна

FFFFFFFF FFFFFFFF FFFFFFFF 99DEF836 146BC9B1 B4D22831.

При этом модуль преобразований остаётся равным 192 битам.

Для проверки статистических свойств последовательностей использовались критерии $\chi^2$-Пирсона, Колмогорова и Мизеса, а также программный комплекс, реализующий проверку последовательностей при помощи теста Маурэра [9]. Результаты исследований приведены в табл. 1-4.

В табл. 1 приведены результаты тестирования выходной последовательности $a_i$ ГПСЧ на ЭК, сформированной с использованием функции выделения координаты $x$ полученных точек, по критериям $\chi^2$-Пирсона, Колмогорова и Мизеса. Причём, в указанной таблице приведены средние значения вероятности для критериев $\chi^2$-Пирсона и Колмогорова и средние значения критерия Мизеса, вычисленные по некоторому количеству выборок для каждого указанного в таблице объёма. Количество выборок определённого объёма зависит от длины файла, например, если файл длиной 12288 байт, то количество выборок объёмом 5120 байт будет равной двум и объёмом 10240 байт - одной выборке. В процессе тестирования использовался файл длиной 48432 байта.

Таблица 1

| Последовательность | Объём выборки | $P(\chi^2)$ | | | | $P(D_n\sqrt{n} < \lambda_a)$ | $\omega^2$ |
|---|---|---|---|---|---|---|---|
| | | 1-мерный | 2-мерный | 3-мерный | 4-мерный | | |
| $a_i$ | 5120 | 0,182 | 0,182 | 0,111 | 0,182 | 0,1 | 0,043 |
| | 10240 | 0,077 | 0,077 | 0,054 | 0,077 | 0,514 | 0,1 |
| | 20480 | 0,14 | 0,14 | 0,103 | 0,14 | 0,814 | 0,114 |
| | 40960 | 0,33 | 0,33 | 0,212 | 0,33 | 0,886 | 0,171 |

Все значения, приведённые в табл. 1, не должны превышать 0.95. Из таблицы следует, что все последовательности $a_i$, сформированные генератором на эллиптической кривой, удовлетворяют требованиям независимости, равновероятности и однородности.

Таблица 2

| Последовательность | Номер выборки | $X_u$ | $Z_u$ |
|---|---|---|---|
| $a_i$ | 1 | 3.317838 | 1.088926 |
| | 2 | 3.302538 | -1.430245 |
| | 3 | 3.311281 | 0.009319 |
| | 4 | 3.309282 | -0.319836 |
| | 5 | 3.309543 | -0.276801 |
| | 6 | 3.314171 | 0.485174 |

В табл. 2 приведены значения $X_u$ и $Z_u$ вычисленные в результате проверки последовательности $a_i$ при помощи универсального теста Маурэра. При этом значение параметра $L$ было равно 4.

Значения $Z_u$, приведённые в табл. 2, должны попадать в интервал от –2,32638 до 2,32638. Это означает, что последовательность $a_i$ практически не сжимаемая, а значит, удовлетворяет свойствам случайности и принадлежит равномерному закону распределения.

Аналогично, в табл. 3-4 приведены результаты тестирования выходной последовательности $a_i$, сформированной ГПСЧ на ЭК с применением хэш-функции, по критериям $\chi^2$-Пирсона, Колмогорова и Мизеса (табл. 3), и универсального теста Маурэра ($L$=4) (табл. 4). В процессе тестирования использовался файл длиной 32768 байт.

Таблица 3

| Последовательность | Объём выборки | $P(\chi^2)$ | | | | $P(D_n\sqrt{n} < \lambda_a)$ | $\omega^2$ |
|---|---|---|---|---|---|---|---|
| | | 1-мерный | 2-мерный | 3-мерный | 4-мерный | | |
| $a_j$ | 5120 | 0,173 | 0,173 | 0,289 | 0,173 | 0,743 | 0,2 |
| | 10240 | 0,489 | 0,489 | 0,112 | 0,489 | 0,743 | 0,171 |
| | 20480 | 0,438 | 0,438 | 0,173 | 0,438 | 0,743 | 0,1 |

Все значения, приведённые в табл. 3, не должны превышать 0.95.

Так же как и данные, приведённые в табл. 2, значения $Z_u$, приведённые в табл. 4, должны попадать в интервал от –2,32638 до 2,32638. Анализ представленных результатов показывает, что последовательности, сформированные по рекуррентному правилу (3) и последующим хешированием, также удовлетворяют необходимым требованиям.

Таблица 4

| Последовательность | Номер выборки | $X_u$ | $Z_u$ |
|---|---|---|---|
| $a_j$ | 1 | 3,302240 | -1,479258 |
| | 2 | 3,312920 | 0,279148 |
| | 3 | 3,306862 | -0,718212 |
| | 4 | 3,319351 | 1,338085 |

Кроме того, исследование предложенных последовательностей при помощи статистических тестов показало, что применение хеш-функции в виде правила (8) при одинаковом количестве испытаний в большинстве случаев даёт лучшие результаты, чем при применении правила выделения (7).

**Заключение**

С учётом того, что рассматриваемые ПСП сформированы с помощью ГПСЧ на ЭК, и при преобразованиях используются такие сложно обратимые операции как сложение или скалярное умножение на эллиптических кривых, можно высказать предположение, что формируемые последовательности относятся к классу криптографически сильных.

Применение функции нелинейного отображения $\psi = \psi(x, y)$ значительно увеличивает структурную скрытность ПСП и, как показано ниже, улучшает значения статистических критериев, однако, вычислительная сложность при этом несколько увеличивается, но остаётся приемлемой.

С учётом того, что порядок точек $G$ на ЭК заведомо большой ($2^{192}$), можно утверждать, что вероятность перекрытия выходной последовательности есть достаточно малая величина.

Выборки из последовательностей, сформированных по правилам (6) и (7), являются случайными, равновероятными и независимыми.

С учётом сказанного можно утверждать, что генераторы ПСП на ЭК могут найти применение в криптографических и других приложениях. Кроме того, авторы понимают необходимость проведения более глубоких исследований по рассматриваемой проблеме.

**Список литературы:** 1. *Кнут Д.* Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. М.: Мир, 1977. 387 с. 2. *Шеннон К.Э.* Теория связи в секретных системах // Работы по теории информации. М.: ИЛ, 1963. 3. *Blum M., Micali S.* How to generate cryptographically strong sequences of pseudo-random bits // SIAM Journal of Computing, 13(4):850-864, 1984. 4. *Andrew C. Yao.* Theory and applications of trapdoor functions. In Proceedings of the 23rd Annual Symposium on Foundation of Computer Science, pages 80-91, IEEE Computer Society, 1982. 5. *Завадская Л.А., Фраль А.И.* Криптографически сильные генераторы псевдослучайных последовательностей // Безопасность информации: №1. С.7-11, 1997. 6. *Бондаренко М.Ф., Горбенко И.Д., Качко Е.Г.* Сущность и результаты исследований свойств перспективных стандартов цифровой подписи X9.62 –1998 и распределения ключей X9.63 – 1999 на эллиптических кривых // Радиотехника. 2000. Вып. 114. С.15-24. 7. ANSI X9.62 –1998: Certificate Managment. 8. *Simon Blake-Wilson, Minghula Qu.* Guidelines for Efficient Cryptography. Recommended Elliptic Curve Domain Parameters. Version 0.4. 1999. 9. *Menezes A., P. van Oorschot, and Vanstone S.* Handbook of Applied Cryptography. Chapter 5. Pseudo-random Bits and Sequences, CRC Press, 1997.

*Харьковский государственный технический университет радиоэлектроники*

*Поступила в редколлегию 14.02.2001*