УДК 681.3.06:519.248.681

Т.А. ГРИНЕНКО, С.И. ЗБИТНЕВ, Д.В. МЯЛКОВСКИЙ

МЕТОДЫ ФОРМИРОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В ГРУППАХ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Введение

Выходные данные генераторов случайных (ГСЧ) и псевдослучайных чисел (ГПСЧ) используются во многих криптографических приложениях, например, при генерации ключей, общесистемных параметров и др. В соответствии с требованиями криптографических приложений эти генераторы должны удовлетворять ряду сложных и противоречивых требований. На наш взгляд, этим требованиям в значительной мере могут удовлетворять ГПСЧ, реализованные на основе использования преобразований в группах точек эллиптических кривых. Метод и конкретные алгоритмы построения ГПСЧ в группах точек эллиптических кривых рассмотрены в [1].

В общем случае для построения генератора псевдослучайной последовательности (ПСП) используется односторонняя функция. Для построения таких односторонних функций используются функции, сложность которых основывается на сложности дискретного логарифма [2] или на сложности факторизации большого числа [3].

В данной статье мы рассмотрим ГПСП, основывающийся на сложности дискретного логарифма в группах точек эллиптической кривой. В случае Блюм – Микали сложность дискретного логарифма заключается [4] в сложности нахождения целого a, такого что $y \equiv g^a \pmod p$. В нашем случае сложность дискретного логарифма на эллиптической кривой заключается в сложности нахождения целого d из сравнения $Q = d \times G \pmod q$, где Q, $G \in E(\mathrm{F}_q)$ и являются известными.

Математический аппарат в группе точек эллиптической кривой (ЭК) получил широкое признание и находит применение при реализации цифровых подписей для направленного шифрования и в ряде состоятельных протоколов управления ключами. В [1] предложен конкретный метод и алгоритмы построения ПСП в группах точек ЭК над простым полем $GF(P)$. Представляет интерес решение этой задачи на общий случай расширенного поля в различных представлениях ЭК и с различными реализациями алгоритмов построения ПСП. Кроме того, необходимо провести более глубокие исследования статистических характеристик различных реализаций, а также сравнительного анализа различных методов и алгоритмов построения ПСП, их сравнения с уже ставшим классическим BBS-генератором [5].

Существует несколько методов построения ПСП в группах точек ЭК [1].

1. Методы построения ПСП в группах точек ЭК

Пусть даны эллиптические кривые: E_A

$$y^2 + xy = x^3 + ax^2 + b \pmod{f(x), 2}, \tag{1}$$

определенная в аффинных координатах и E_P

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6 \pmod{f(x), 2}, \tag{2}$$

определенная в проективных координатах. Пусть дана базовая точка G с координатами $(x, y) \in E_A$ или $(X, Y, Z) \in E_P$. Рассмотрим два метода построения ПСП:

$$Z_i = Z_{i-1} + G, \text{ где } Z_i, Z_{i-1} \in E; \tag{3}$$

$$Z_i = a \times Z_{i-1}, \text{ где } Z_i, Z_{i-1} \in E. \tag{4}$$

В первом случае мы получаем последовательность значений Z_i путем многократного суммирования точки Z_{i-1} и базовой точки G, а во втором – путем скалярного умножения точки Z_{i-1} на число a. Во втором случае возникает вопрос выбора a, оно может быть константой либо получаться из другого ГПСП, в нашем случае $a=\pi(Z_{i-1})$, где π – функция преобразования x/X-координаты в число. Таким образом, мы получаем $Z_i=\pi(Z_{i-1})\times Z_{i-1}$.

Для обоих методов построение ПСП можно выполнить несколькими способами. Основными из них, на наш взгляд, являются:

$$Num(Z_i)=X_i\,||\,Y_i\,||\,Z_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{5.1}$$

$$Num(Z_i)=X_i\,||\,Y_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{5.2}$$

$$Num(Z_i)=X_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{5.3}$$

$$Num(Z_i)=x_i\,||\,y_i, \text{ если } Z_i(x_i,y_i)\in E_A, \tag{5.4}$$

$$Num(Z_i)=x_i, \text{ если } Z_i(x_i,y_i)\in E_A. \tag{5.5}$$

В выражениях (5.1)-(5.5) знак $||$ – конкатенация значений координат точек ЭК, а $Num(Z_i)$ – обозначение способа формирования ПСП.

Проведенный анализ показал, что сложность (скорость) функционирования ГПСП зависит от выбранного метода и способа формирования ПСП. Минимальная сложность достигается для метода (3) и способа формирования ПСП (5.1). В этом случае за один шаг ГПСП формируется псевдослучайное число трехкратной длины.

Координаты точки имеют корреляционную функцию, соответствующую уравнению эллиптической кривой, что может привести к корреляции значений ПСП. Проведенный анализ показал, что декорреляцию можно осуществить посредством вычисления значений хэш-функций от текущего числа $Num(Z_i)$.

С учетом (3) и (4), а также пяти способов формирования чисел (5.1)-(5.5) проведены исследования следующих конкретных алгоритмов формирования ПСП:

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=X_i\,||\,Y_i\,||\,Z_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.1}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=X_i\,||\,Y_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.2}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=X_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.3}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=x_i\,||\,y_i, \text{ если } Z_i(x_i,y_i)\in E_A, \tag{6.4}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=x_i, \text{ если } Z_i(x_i,y_i)\in E_A, \tag{6.5}$$

$$Z_i=\pi(Z_{i-1})\times Z_{i-1},\ Num(Z_i)=X_i\,||\,Y_i\,||\,Z_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.6}$$

$$Z_i=\pi(Z_{i-1})\times Z_{i-1},\ Num(Z_i)=X_i\,||\,Y_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.7}$$

$$Z_i=\pi(Z_{i-1})\times Z_{i-1},\ Num(Z_i)=X_i, \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.8}$$

$$Z_i=\pi(Z_{i-1})\times Z_{i-1},\ Num(Z_i)=x_i\,||\,y_i, \text{ если } Z_i(x_i,y_i)\in E_A, \tag{6.9}$$

$$Z_i=\pi(Z_{i-1})\times Z_{i-1},\ Num(Z_i)=x_i, \text{ если } Z_i(x_i,y_i)\in E_A, \tag{6.10}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=H(X_i\,||\,Y_i\,||\,Z_i), \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.11}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=H(X_i\,||\,Y_i), \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.12}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=H(X_i), \text{ если } Z_i(X_i,Y_i,Z_i)\in E_P, \tag{6.13}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=H(x_i\,||\,y_i), \text{ если } Z_i(x_i,y_i)\in E_A, \tag{6.14}$$

$$Z_i=Z_{i-1}+G,\ Num(Z_i)=H(x_i), \text{ если } Z_i(x_i,y_i)\in E_A, \tag{6.15}$$

$$Z_i = \pi(Z_{i-1}) \times Z_{i-1},\ \ Num(Z_i) = H(X_i \| Y_i \| Z_i), \text{ если } Z_i(X_i, Y_i, Z_i) \in E_P, \quad (6.16)$$

$$Z_i = \pi(Z_{i-1}) \times Z_{i-1},\ \ Num(Z_i) = H(X_i \| Y_i), \text{ если } Z_i(X_i, Y_i, Z_i) \in E_P, \quad (6.17)$$

$$Z_i = \pi(Z_{i-1}) \times Z_{i-1},\ \ Num(Z_i) = H(X_i), \text{ если } Z_i(X_i, Y_i, Z_i) \in E_P, \quad (6.18)$$

$$Z_i = \pi(Z_{i-1}) \times Z_{i-1},\ \ Num(Z_i) = H(x_i \| y_i), \text{ если } Z_i(x_i, y_i) \in E_A, \quad (6.19)$$

$$Z_i = \pi(Z_{i-1}) \times Z_{i-1},\ \ Num(Z_i) = H(x_i), \text{ если } Z_i(x_i, y_i) \in E_A. \quad (6.20)$$

2. Экспериментальные исследования свойств ПСП

Для сравнения ПСП были выбраны эллиптическая кривая E над полем $F_{2^{191}}$, примитивный полином $f(x) = 0x\,800000000000000000000000000000000000000000000201$, параметры ЭК $a = 0x\,2866537B676752636A68F56554E12640276B649EF7526267$, $b = 0x\,2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC$, базовая точка G с координатами $x/X = 0x\,36B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D$, $y/Y = 0x\,765BE73433B3F95E332932E70EA245CA2418EA0EF98018FB$, $Z = 1$, порядок базовой точки $n = 0x\,400000000000000000000004a20e90c39067c893bbb9a5$, кофактор $k = 2$.

Для тестирования генератора ПСЧ на эллиптических кривых использовалась методика NIST STS [6], рекомендованная Национальным институтом по стандартизации и технологиям США, разработанная для статистического тестирования алгоритмов-кандидатов на AES (NIST SP 800-22). Пакет NIST STS включает в себя 16 статистических тестов. Эти тесты используются для проверки гипотезы о случайности двоичных последовательностей произвольной длины, порождаемых ГСЧ или ГПСЧ. По совокупности результатов всех тестов принимается решение о том, будет ли заданная последовательность нулей и единиц «случайной» или нет.

Рассмотрим двоичную последовательность $S = \{s_1, s_2, \ldots, s_n\}$, $s_i \in \{0,1\}$ произвольной длины n бит. Для фиксированного значения n сформируем множество из m двоичных последовательностей, т.е. сформируем выборку объемом $N = m \times n$. Каждую последовательность подвергаем тестированию с использованием пакета NIST STS. В результате тестирования сформируем статистический портрет генератора $P_{ij} \in [0,1]$, $i = \overline{1,m}, j = \overline{1,q}$ (m – количество тестируемых двоичных последовательностей, q – количество статистических тестов). По полученному статистическому портрету определяем долю последовательностей, прошедших каждый статистический тест. Для этого задаем уровень значимости $\alpha \in [0{,}001; 0{,}01]$ и осуществляем подсчет значений вероятности P, превышающих заданный уровень α для каждого из q тестов. В результате сформируем вектор коэффициентов $R = \{r_1, r_2, \ldots r_q\}$, элементы которого характеризуют в процентном соотношении прохождение последовательности S_i всех статистических тестов. Далее осуществляем статистический анализ статистического портрета. Полученные значения вероятностей $P_{ij} \in [0,1]$ должны подчиняться равномерному закону распределения на интервале [0,1]. Наконец, принимаем окончательное решение – прошел ли генератор статистическое тестирование пакетом NIST STS или нет.

С использованием методики NIST STS было осуществлено тестирование 20 ПСП (алгоритмы (6.1)-(6.20), а также проведено сравнение свойств этих ПСП со свойствами ПСП генератора псевдослучайных чисел BBS [6] (тестовая выборка, рекомендованная NIST).

Для осуществления тестирования были выбраны следующие параметры:

1. Длина тестируемой последовательности $n = 10^6$ бит.

2. Количество тестируемых последовательностей m = 100. Таким образом, объем тестируемой выборки составил $N = 10^6 \times 100 = 10^8$ бит.

3. Уровень значимости α = 0,01

4. Количество тестов q = 189. Таким образом, статистический портрет генератора содержит 18900 значений вероятности P.

В идеальном случае при m = 100 и α = 0,01 может быть отвергнута только одна последовательность из ста, т.е. коэффициент прохождения каждого теста должен составлять 99%. Но это слишком жесткое правило. Поэтому и применяется правило на основе доверительного интервала для r_j. Нижняя граница в этом случае составит значение $r_{\min}$ = 0,96015. С этих позиций проанализируем результаты тестирования ПСП, представленные на диаграммах (рис. 1-7).

В табл. 1 приводятся данные по прохождению ПСП тестов по Правилу 1 [6].

Таблица 1

Генератор	Количество тестов, в которых тестирование прошли более 99% последовательностей	Количество тестов, в которых тестирование прошли более 96% последовательностей
BBS	134 (70,8%)	189 (100%)
6.1	119 (63%)	175 (92,6%)
6.2	126 (66,7%)	171 (90,5%)
6.4	128 (67,7%)	181 (95,8%)
6.5	137 (72,5%)	187 (98,9%)
6.9	118 (62,4%)	180 (95,2%)
6.10	123 (65,1%)	187 (98,9%)
6.11	139 (73,5%)	187 (98,9%)
6.12	141 (74,6%)	188 (99,5%)
6.13	138 (73%)	189 (100%)
6.14	134 (70,9%)	189 (100%)
6.15	124 (65,6%)	187 (98,9%)
6.16	126 (66,7%)	188 (99,5%)
6.17	146 (77,2%)	188 (99,5%)
6.18	131 (69,3%)	189 (100%)
6.19	121 (64%)	187 (98,9%)
6.20	127 (67,2%)	188 (99,5%)

Генераторы (6.13), (6.14), (6.18) прошли все тесты. Генератор BBS прошел все тесты. Если применять жесткий критерий, т.е. когда может быть отброшена лишь одна последовательность из ста, то лучший результат показал генератор (6.13), он имеет лучшие характеристики, чем BBS. Генератор (6.14) имеет такую же статистику, как и BBS.

В табл. 2 представлены сводные результаты по прохождению генераторами тестов по Правилу 2 [6].

Таблица 2

Генератор	Количество тестов, в которых значение вероятности $P \le 0,01$	Количество тестов, у которых значение вероятности $P \le 0,001$
BBS	0	0
6.1	19	16
6.2	28	18
6.4	21	14
6.5	4	2
6.9	11	7
6.10	6	4
6.11	2	0
6.12	5	0
6.13	2	0
6.14	3	2
6.15	1	0
6.16	1	0
6.17	4	0
6.18	2	0
6.19	2	1
6.20	2	1

В таблице значения вероятности P сравниваются с уровнями значимости $\alpha = 0{,}01$ и $\alpha = 0{,}001$, т.к. это достаточно малые значения.

Для (6.13) малые значения вероятности P получены:

- для неперыкрывающихся шаблонов $P = 0{,}008879$,
- для проверки случайных отклонений $P = 0{,}004301$.

Однако эти значения не совпадают с отрицательными выводами по правилу один.

Для (6.14) малые значения вероятности P получены:

- для последовательного теста $P = 0{,}009535$,
- для проверки случайных отклонений $P = 0{,}005166$,
- для проверки случайных отклонений (вариант) $P = 0{,}004045$,
- для неперыкрывающихся шаблонов $P = 0{,}00017$ и $P = 0{,}000082$.

Для (6.18) малые значения вероятности P получены:

- для неперыкрывающихся шаблонов $P = 0{,}007160$ и $P = 0{,}001112$.

Однако эти значения не совпадают с отрицательными выводами по правилу один.

На рис. 1-7 представлены статистические портреты некоторых генераторов ПСП с указанием их параметров и способов формирования.

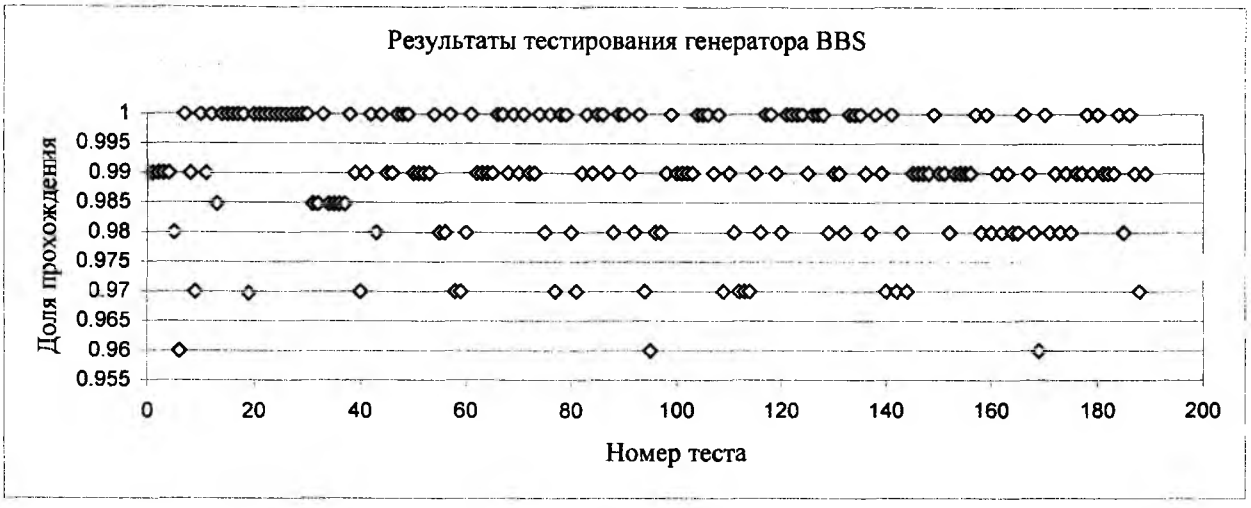

Рис. 1

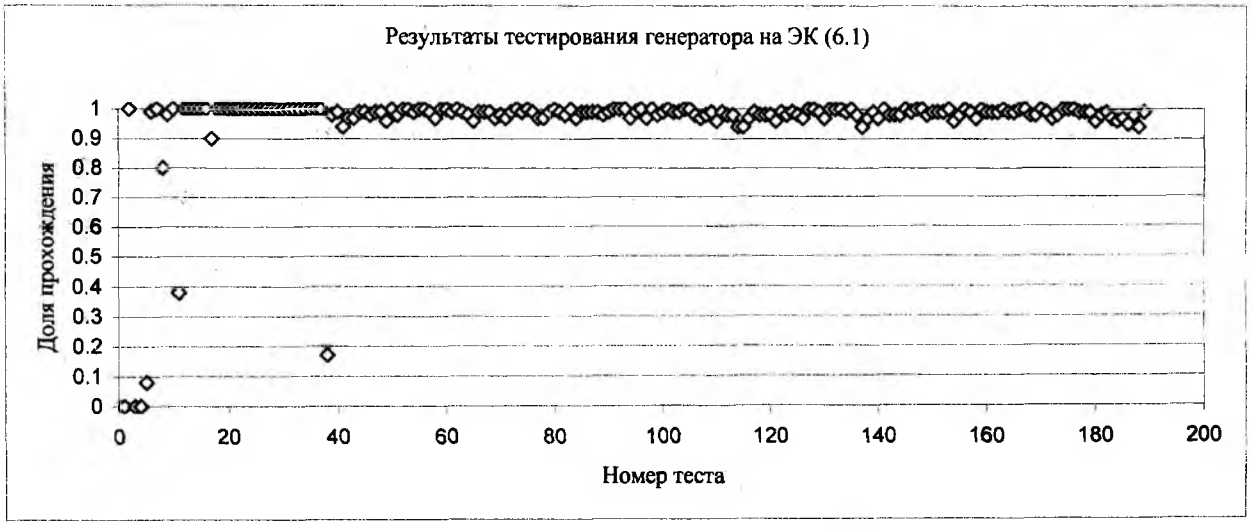

Рис.2

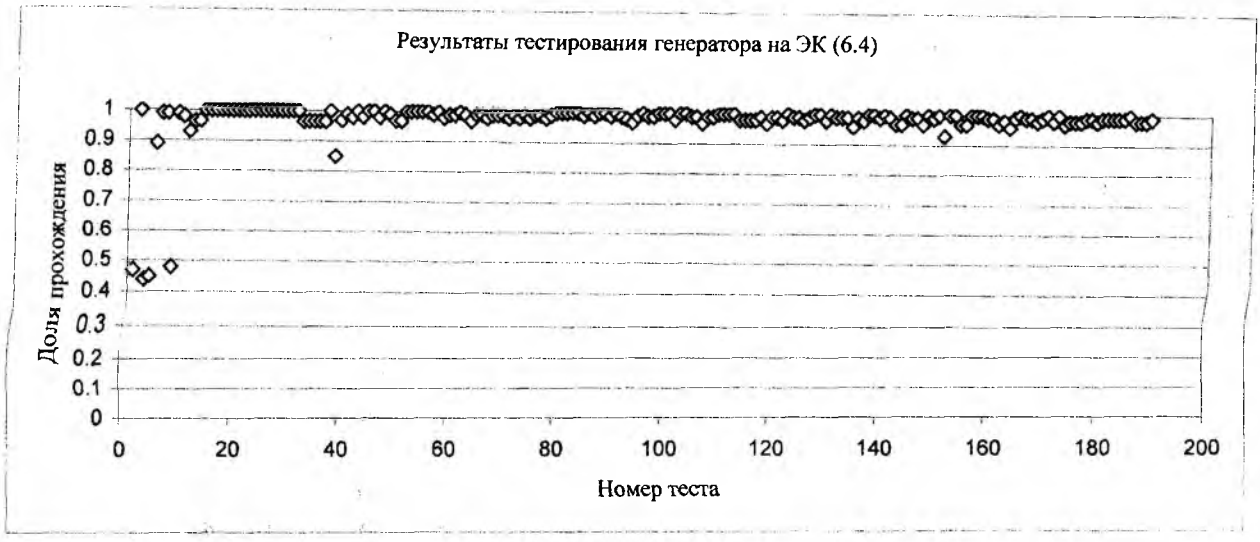

Рис.3

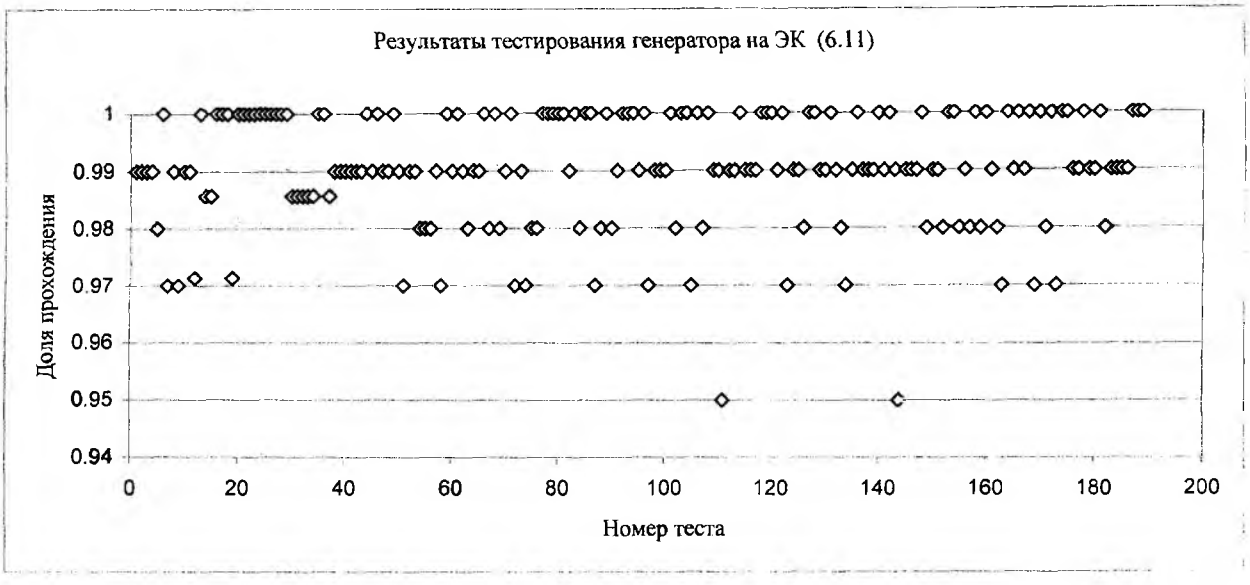

Рис.4

Рис.5

Рис.6

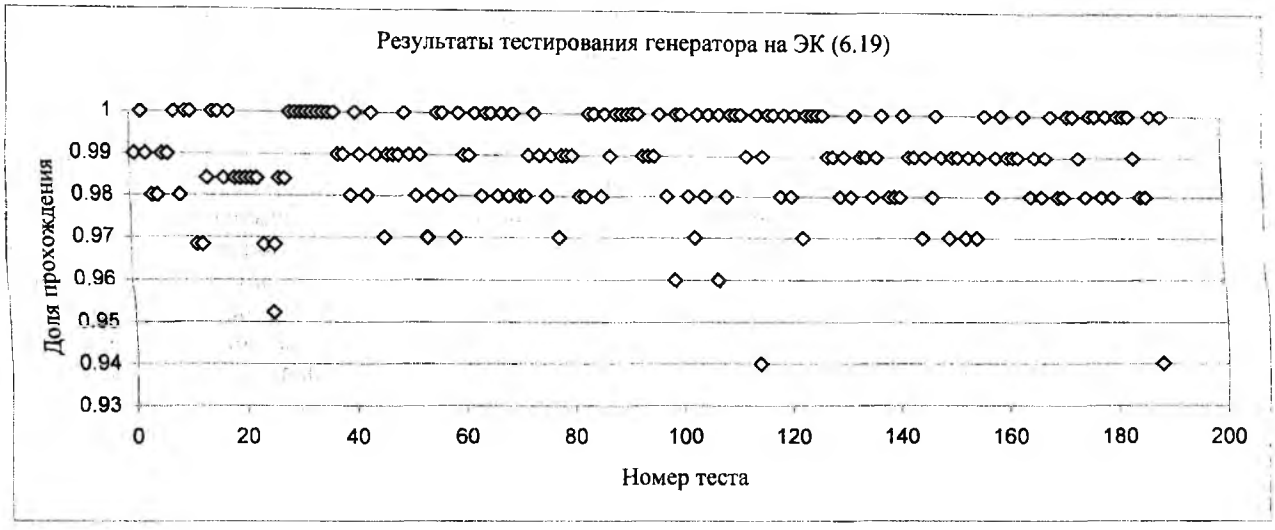

Рис.7

В табл.3 приведены результаты экспериментальной оценки скорости формирования ПСП для различных алгоритмов.

Таблица 3

Генератор	Количество полученных битов за секунду
6.1	57 600 000
6.2	38 400 000
6.3	19 200 000
6.4	93 203
6.5	46 601
6.6	15 368
6.7	10 245
6.8	5 122
6.9	390
6.10	195
6.11	12 800 000
6.12	12 800 000
6.13	12 800 000
6.14	63 366
6.15	63 366
6.16	6 835
6.17	6 835
6.18	6 835

Окончание табл. 3

6.19	258
6.20	258

Наибольшую скорость обеспечивают генераторы (6.1), (6.2), (6.3), (6.11), (6.12), (6.13). В тоже время у генератора (6.13) и лучшие статистические характеристики случайности.

Заключение

Применение математического аппарата групп точек позволяет построить различные генераторы ПСП. Основными методами формирования ПСП являются методы, основанные на операциях сложения и умножения в группах точек эллиптических кривых.

Результаты статистического тестирования предложенных алгоритмов с использованием методики NIST SP 800-22 показали, что лучшими являются генераторы (6.13), (6.14) и (6.18). Причем наилучшим является генератор (6.13), характеристики которого даже лучше, чем у принятого в качестве классического BBS генератора.

Генератор ПСП, построенный по алгоритму (6.13), кроме вполне приемлемых статистических характеристик, обеспечивает приемлемую сложность (скорость) формирования псевдослучайных чисел. Так на ПЭВМ Celeron 600 скорость составляет порядка 12 800 000 бит./с.

Список литературы: 1. *Гриненко Т.А., Горбенко Ю.И., Орлова С.Ю.* Метод формирования и свойства псевдослучайных последовательностей на эллиптических кривых // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С. 119-123. 2. *Leonard Adleman.* A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In Proceeding of the 20th Annual Symposium on Foundation of Computer Science, page 55-60, IEEE Computer Society, 1979. 3. *Werner Alexi, Benny Chor, Oded Goldreich, and Claus P.Schnorr.* RSA and Rabin functins: Certain parts are as hard as the whole. To appear, SIAM Journal of Computing. 4. *Manuel Blum and Silvio Micali.* How to generate cryptographically strong sequences of psevdo-random bits. SIAM Journal of Computing, 13 (4): 850-864, 1984. 5. *Alfred Menezes, et. al.* Handbook af Applied Cryptography – CRC Press, 1997. 6. *Потий А.В., Орлова С.Ю., Гриненко Т.А.* Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вип. 2. С. 206-214.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 29.04.2002