УДК 512.624.95 + 517.772

к.т.н. Чевардин В. Е. (ВІТІ НТУУ „КПІ”)
Шевченко В. С. (ВІТІ НТУУ „КПІ”)

АНАЛИЗ СВОЙСТВ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Проведен анализ генераторов псевдослучайных последовательностей построенных на основе преобразований в группе точек эллиптической кривой. В рассмотренных генераторах в качестве итерационной функции использовалось двойное скалярное умножение точек кривой. В статье обращен взгляд на надежность принятой в стандарте функции генерации внутренних состояний генератора. Вводится новое понятие точки вырожденности, которая обуславливает зацикливание генератора. В статье представлены результаты анализа параметров кривых, которые потенциально могут привести к зацикливанию генератора, а также оценены мощности множеств точек вырожденности.

Чевардін В.Є., Шевченко В.С. Аналіз властивостей генераторів псевдовипадкових послідовностей на еліптичних кривих. *Проведено аналіз генераторів псевдовипадкових послідовностей побудованих на основі перетворень в групі точок еліптичної кривої. В розглянутих генераторах в якості ітераційної функції використовувалось подвійне скалярне множення точок кривої. В статі погляд повернуто на надійність прийнятої в стандарті операції генерації внутрішніх станів генератора. Введено нове поняття точки виродженості, яка обумовлює зациклення генератору. В статті представлені результати аналізу параметрів кривих, які потенційно можуть привести до зациклення генератору, а також оцінені потужності множин точок виродженості.*

V. Chevardin, V. Shevchenko Analysis of properties of pseudorandom bit generators based on elliptic curves. *The analysis of random bit generators based on elliptic curve transformations was made. Scalar multiplication of points was using for iteration function of these generators. In this article attention concentrated about dependability of standard function of making of internal state of generator. Here was used new term - the degenerating point, that produce cycle of generator. New results of analyzes of curve parameters, which can produce to cycle, and new estimates of number of this points and their classes was made.*

Ключевые слова: *генератор псевдослучайных последовательностей, эллиптическая кривая.*

Вступление

Ни для кого не секрет, что генераторы псевдослучайных последовательностей (ПСП) играют важную роль для построения современных криптографических систем. Немало внимания в последние годы уделено генераторам ПСП на основе эллиптических кривых (ЭК), криптографическая стойкость которых считается эквивалентной сложности дискретного логарифмирования в группе точек ЭК [1 – 6, 8, 9]. Некоторые из этих результатов легли в основу стандартизованного алгоритма генерации ПСП на основе двойного скалярного умножения точек кривой [9]. Несмотря на это имеются достаточно серьезные замечания в адрес данного стандарта, ряд замечаний генераторов этого класса рассмотрены в работах [5, 10, 11]. Уязвимыми местами заложенного в стандарт подхода являются: итерационная функция преобразования точки кривой в блок бит, которая позволяет при определенных условиях восстанавливать точки кривой по соответствующему блоку бит, фиксированные точки кривой, которые, в свою очередь, могут быть „закладками”, позволяющими при перехвате части ПСП получать за полиномиальное время последующие биты ПСП. Тем не менее, выявленные недостатки стандарта не затрагивают самой природы криптографического преобразования, заложенного в основу генератора, которое также не лишено недостатков. В связи с чем, целью данной работы является попытка осуществить новый взгляд на особенности итерационного преобразования над точками кривой в генераторах ПСП на эллиптических кривых.

1. Необходимые элементы теории эллиптических кривых

Широко известной формой ЭК является кривая в нормальной форме Вейерштрасса (1).

$$y^2 + a_1xy + a_3y = x^3 + a_4x^2 + a_2x + a_0, \text{ где } a_i \in F_q. \qquad (1)$$

Однако несложными преобразованиями удается перейти от кривой (1) к более компактной форме – канонической форме кривой (2).

$$y^2 = x^3 + ax^2 + bx + c, \text{ где } a, b, c \in F_q. \quad (2)$$

В свою очередь, от формы (2) для случаев $q \neq 2, 3$ удается перейти к форме (3), которая и является одной из широко используемых в криптографии. Основные теоретические положения, касающиеся операций над точками эллиптической кривой, переход от нормальной формы кривой к канонической, изоморфные трансформации несингулярных кривых детально рассмотрены в работах [11 – 13]. Мы в данной работе обратимся к несуперсингулярным эллиптическим кривым над $F_q, q \neq 2, 3$.

Пусть гладкая ЭК в аффинной системе координат [13] задана уравнением (3) в канонической форме над конечным полем характеристики $p \neq 2, 3$, E_p – циклическая подгруппа точек ЭК достаточно большого порядка, $ordE_p = n$.

$$EC: y^2 = x^3 + ax + b \pmod p, \text{ где } a, b \in F_p. \quad (3)$$

Точки кривой представлены двумя координатами $\{X, Y\} \in F_p$, удовлетворяющими уравнению (3) вместе с точкой на бесконечности. Применяя метод секущих Диофанта для точек кривой (3), можно получить криптографическую операцию – операцию скалярного умножения точки $P = (X, Y)$ на скаляр $k < n$, т.е. $R = k * P = \underbrace{P + P + ... + P}_{k \text{ раз}}$. Сегодня задача вычисления числа k по двум известным точкам $R, P \in \langle P \rangle$ (задача дискретного логарифмирования в группе точек ЭК) считается вычислительно сложной (теоретико-сложностной). В отличии от широко известных алгоритмов электронной цифровой подписи, генерации общих секретных ключей, поточного шифрования операция скалярного произведения точки кривой в структурах генераторов ПСП несколько отличается. Рассмотрим на примере генератора Dual_EC_DRBG свойства итерационной функции, генерирующей внутренние состояния данного генератора.

2. Генератор на основе двойного скалярного произведения точек ЭК

Структура генераторов на основе двойного скалярного произведения, требования к параметрам кривой и к точкам были детально рассмотрены в работах [7, 9, 12]. Опираясь на известные результаты, представим функцию генерации Dual_EC_DRBG выражением (4).

$$b_i = extr\left[t_i * Q\right] = extr\left[\left(X_\psi[t_{i-1} * P] \bmod n\right) * Q\right], \quad (4)$$

где X_ψ – X-координата точки, которая представлена целым числом;

t_i – целое число, результат функции $f(X, Y)$, в данном случае $f(X, Y) = X_\psi[P_i]$;

$t_0 = HDF(entropy, nonce, ID)$.

Последовательность внутренних состояний генератора: $t_1, ..., t_n$ формируется по следующему правилу: $t_i = X_\psi[t_{i-1} * P] \bmod n$, где $t_1 = X_\psi[t_0 * P]$, $t_0 = seed$, P – базовая точка кривой, которая генерируется случайным образом. Последовательность внутренних состояний, порожденных функцией (4) для конкретного начального состояния (базовой точки P), может содержать как все, так и часть точек подгруппы $\langle P \rangle$. Это зависит от свойств преобразования $t_i = X[t_{i-1} * P] (\bmod n)$. Другими словами, если во время генерации внутреннее состояние генератора (X-координата точки кривой) повторяется, это приводит к зацикливанию генератора с периодом k. Период k не превосходит значения $n / 2$, но существуют такие случаи, когда период k существенно меньше значения $n / 2$. Поиск и доказательство криптографически стойких функций, для которых k не меньше порядка

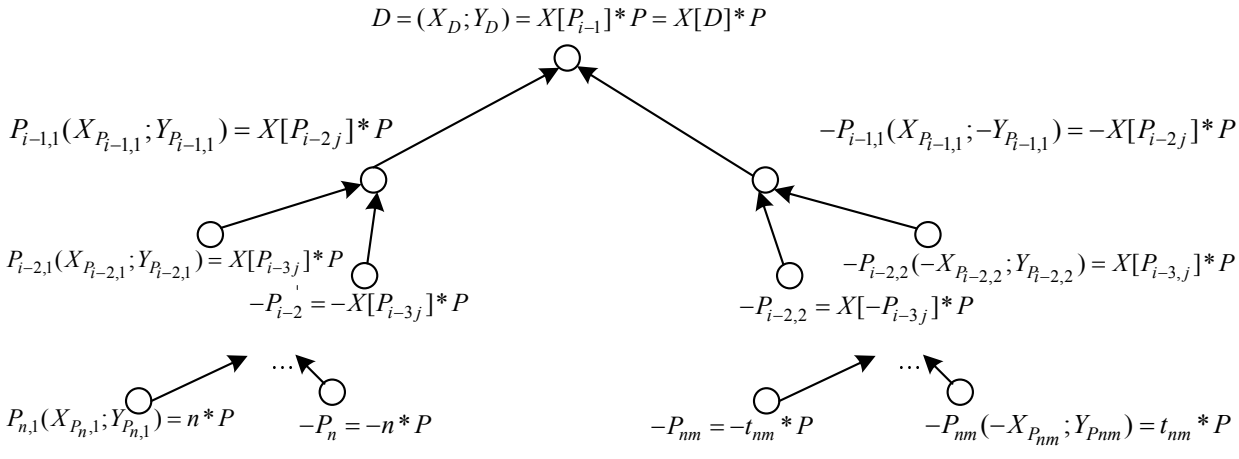
абелевой группы, используемой для построения итерационной функции, позволит обеспечить доказуемую стойкость генераторов ПВП этого класса. Рассмотрим причины возможных уменьшений периода *k*.

Определение 1. Для генератора ПСП, построенного на основе циклической группы точек эллиптической кривой (1) с параметрами $\{a,b,p,P,Q\}$ результатом работы является последовательность внутренних состояний (точек кривой), период которой определяется расстоянием от базовой точки *P* до точки вырожденности $P_i = D$, удовлетворяющей уравнению (5).

$$D = X[D]^* P. \qquad (5)$$

В случае установки внутреннего состояния в точку *D* генератор приходит к зацикливанию, т.е. число точек полученных при выполнении итерационной операции (4) из точки *P* до момента получения точки *D* определяет период генератора ПВП.

Представим этапы обработки точек (внутренних состояний генератора) в виде графа (рис. 1).



Ри

с 1. Маршруты формирования точки *D*

Полученная цепочка скалярных значений дает возможность выделить подмножество скалярных значений, которые за различное число итераций приведут генератор к зацикливанию с периодом *k*. Исключив из числа допустимых скалярных значений скаляры, которые приводят за $<< n/2$ шагов в точку *D*, получим возможность избавиться от зацикливаний малого периода, а следовательно исключим потенциальную уязвимость генератора ПВП. С другой стороны, исключив базовые точки, приводящие в точки вырожденности, из числа допустимых точек N_E также можем избежать зацикливаний малого периода. Оценим число таких точек в циклической группе.

3. Оценка числа точек вырожденности для ЭК.

Рассмотрим примеры генерации ПСП на основе функции (4).

Пример 1. ЭК задана уравнением: $y^2 = x^3 + 1 \pmod 5$, $p \equiv -1 \pmod 3$, $ordE = 6$, $\Delta \neq 0$, $j = 0$ точки имеют порядок $\#P(0,\pm 1) = 3$, $\#P(2,\pm 2) = 6$, $\#P(4,0) = 2$. Проверка всех точек показала, что две точки $(0, \pm 1)$ приводят к зацикливанию с периодом 1: $\pm 2P(0,1) = \pm P(0,1)$.

Пример 2. ЭК задана уравнением: $y^2 = x^3 + x + 1 \pmod 7$, для которой $\Delta = -(4a^3 + 27b^2) = 4$, $j = 12^3 4a^3 / 4a^3 + 27b^2 = 1$. Точками кривой являются точки: $\#P(0,\pm 1) = 5$, $\#P(2,\pm 2) = 5$. Проверка всех точек показала, что две точки $\pm(0,1)$ приводят к зацикливанию с периодом 2: $2\pm P(0;1) = \pm P(2;5)$.

Пример 3. Пусть кривая задана уравнением $y^2 = x^3 + x + 5 (\mathrm{mod}\, 23)$, $\Delta \neq 0$, $j \neq 0,12^3$. Кривая имеет 22 точки, из которых к точкам вырожденности приводят следующие 6 точек: $18P(4,\pm 2) = P(18,\pm 6)$, $3P(10,\pm 7) = P(3,\pm 9)$.

Рассмотрим кривую $y^2 = x^3 + ax + b (\mathrm{mod}\, p)$. Результаты поиска точек вырожденности для кривой $y^2 = x^3 + ax + b (\mathrm{mod}\, p)$ представлены в табл. 1.

Таблица 1.

Точки вырожденности для кривой $y^2 = x^3 - 3x + b (\mathrm{mod}\, p)$

p	7	17	23	31	43
N_E	6	23	18	28	51
a	-3	-3	-3	-3	-3
b	3	3	17	13	23
j	5	15	14	28	6
*D= t*P*	(3;0)= 3±(1;1)	±(4;15)=4±(3;2) ±(8;7)=8±(4;2) ±(3;2)=3±(7;6) ±(11;14)=11±(8;7) ±(9;12)=9±(13;6) ±(15;16)=15±(14;6) ±(7;11)=7±(15;1)	±(5;9)= 5±(6;10) ±(11;2)= 11±(15;9)	±(9;23)= 9±(6;5) ±(11;3)= 11±(7;5)	±(12;9)=12±(2;5) ±(7;42)=7±(3;16) ±(6;36)=6±(7;1) ±(23;34)=23±(10;2) ±(27;19)=27±(11;17) ±(11;17)=11±(28;2) ±(8;9)=8±(41;8) ±(2;38)=2±(42;5)

Таким образом, любая ЭК обладает точками вырожденности. Очевидно, что с ростом характеристики поля число точек, приводящих к зацикливанию малого периода растет. Проведем эксперимент с определением числа точек вырожденности и оценим относительное число точек вырожденности и время поиска таких точек (табл. 2). Для этих целей будем использовать вычислительный комплекс с параметрами: Intel Core 2 Duo E7500 2,93GHz (x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3), память: 2048MB DDR2-800 (400 MHz), а также программную реализацию генератора ПСП разработанную на основе библиотеки MIRACLE.

Таблица 2.

Точки вырожденности для кривой $y^2 = x^3 - 3x + b$ из стандарта [9] над F_p

log(p)	11	12	13	14	15	16
p	2039	4093	8191	16381	32749	65521
N_E	2053	4219	8059	16447	32911	65011
a	389	1	2077	-3	3	17
b	1776	1378	3696	4585	24313	50583
N_D	1318	2656	5128	10326	20824	40880
N_D/N_E	0,64	0,62	0,63	0,62	0,63	0,63

Из табл. 2. видно, что число точек вырожденности составляет около 0,62 от числа точек циклической группы, т. е. число точек вырожденности для циклической группы кривой является соизмеримым с ее порядком.

Для кривой $y^2 = x^3 - 3x + 1466405953$ над полем характеристики $p = 4294967291$ с $N_E = 4295095643$ первой по возрастанию X-координаты точкой, приводящей к точке вырожденности $X[D] = 2656154384$, является точка с $\mathrm{X[P]} = 1$. Время ее поиска простым перебором составило 16698 сек. Для этой же самой кривой точка с $\mathrm{X[P]} = 28690697$ приводит в точку с $\mathrm{X[P]} = 17$, $\mathrm{X[17*P]} = 17$. Проведем эксперимент.

Експеримент. Пусть задана кривая $E_p : y^2 = (x^3 + ax + b) \bmod p$. Для простых

характеристик поля: 31, 47, 67, 131, 257 получим генераторы на основе (4). Для каждой точки $P_i \in E_p$, $1 < i < (n-1)/2$, изменяя значения $1 \le t_0 < n$ получим возможные непериодические последовательности точек (рис. 2), lb – длина блока на выходе генератора.

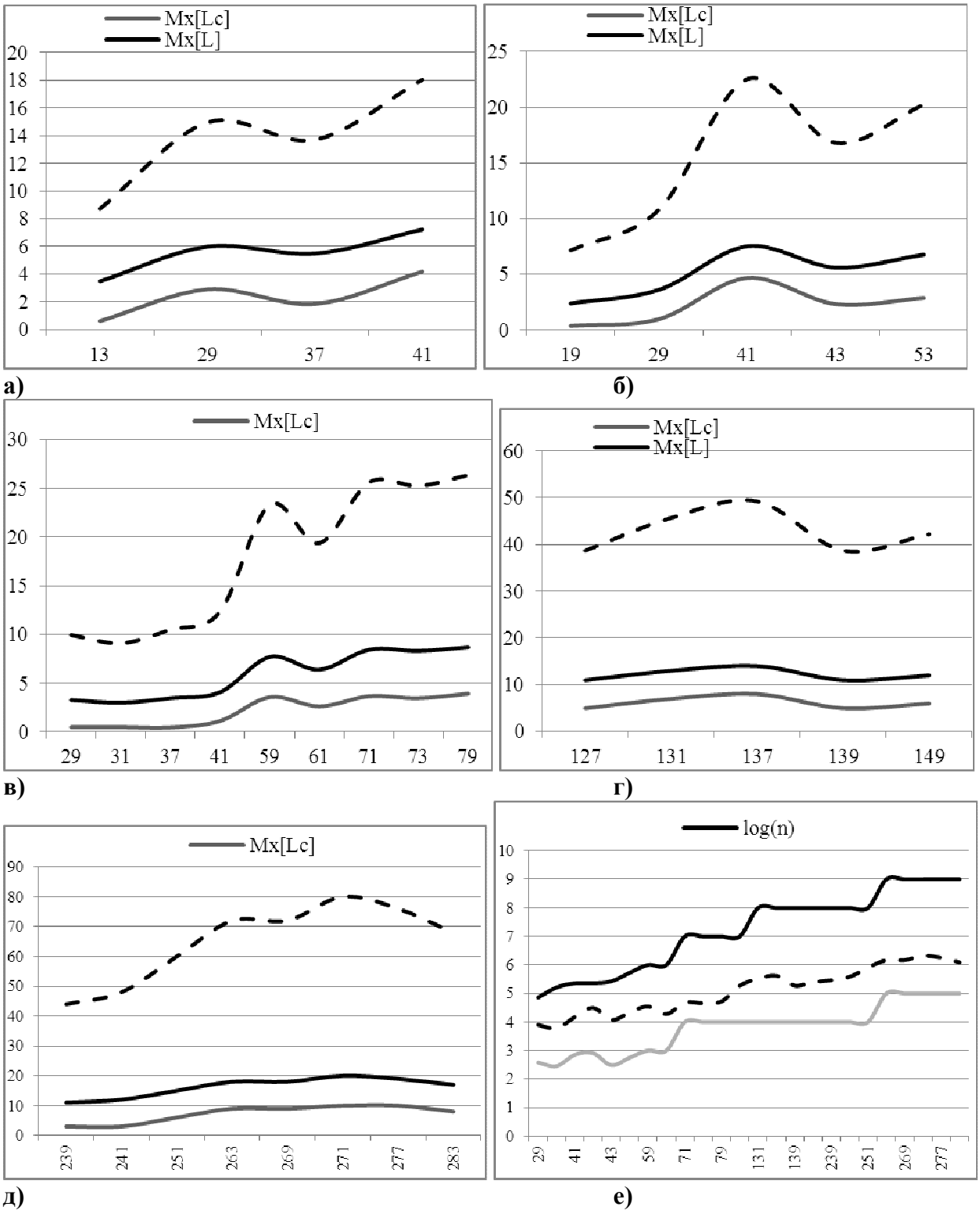


Рис. 2. а) Mx[Lc], Mx[L], p=31; б) Mx[Lc], Mx[L], p=47; в) Mx[Lc], Mx[L], p=67; г) Mx[Lc], Mx[L], p=131; д) Mx[Lc], Mx[L], p=257; е) log(n), log(L).

Определим соответствующие значения периода зацикливания[1] Lc и периода последовательности точек[2] L. Для каждой точки $P_i \in E_p$ определим средние значения $Mx[Lc]$ и $Mx[L]$.

Полученные результаты показали рост значений $Mx[Lc]$ и $Mx[L]$ з увеличением порядка циклической группы точек.

Увеличение $Mx[L]$ наблюдается при сближении порядка группы точек и значения характеристики поля Галуа (рис. 2а – 2д). Среднее значение периода L_{cp} для полученных результатов равняется значению $Mx[L]$ в случае $lb = 1$.

Если предположить, что зависимость (рис. 2е) сохраняется для полей с $\log(p) > 160$, то для кривых Е-256, $\log(p) = 256$ длина $Mx[L]$ составит $\log(L) = 128$ при $lb = 1$. Пунктирные линии на рисунках показывают значения характеристик генератора для случая использования в качестве выходного блока $\log(p)/2$ бит X-координаты точки.

Выводы

Полученные результаты позволяют утверждать о существовании еще одной уязвимости стандарта [9], а также всех существующих методов генерации ПСП на основе скалярного преобразования точки (1).

Получены результаты оценки отношения точек, приводящих к точкам вырожденности к порядку циклической группы, в том числе на основе экспериментальных исследований. Исключение точек вырожденности из числа внутренних состояний генератора ПСП позволит избежать бреши в генераторах этого класса.

Следует заметить, что, на сегодняшний день, поиск точек вырожденности для рекомендованных кривых над полями с характеристикой 2^{256} является вычислительно сложной задачей. Тем не менее, с ростом вычислительной мощности данная задача может быть решена в ближайшее время.

Решение вскрытого недостатка генераторов на ЭК позволит повысить стойкость к восстановлению и предсказанию псевдослучайных последовательностей на выходе генераторов на ЭК, а также позволит теоретически доказать период ПСП для генераторов этого класса, что является на сегодняшний день нерешенной задачей для ряда генераторов этого класса.

Включение в список требований к параметрам генераторов на ЭК дополнительной процедуры проверки базовых параметров кривой (базовой точки) на сводимость к точкам вырожденности позволит повысить криптографическую стойкость генераторов этого класса. Дальнейшие исследования будут посвящены поиску способов определения точек вырожденности на кривой с уменьшенными вычислительными затратами.

ЛИТЕРАТУРА

1. Kaliski Jr. A pseudo-random bit generator based on elliptic logarithms / B. S. Kaliski Jr. // Advances in Cryptology: Proceedings of Crypto '86 (Lecture Notes in Computer Science, vol. 263), Springer-Verlag, New York, 1987, pp. 84 – 103.

2. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo, L. Levin, and M. Luby // Proceedings of the 21st Annual ACM Symposium on Theory of Computing, ACM, New York, 1989, pp. 12 – 24.

[1] Число точек, которые повторяются циклически во время генерации внутреннего состояния функцией (4).

[2] Число точек, которые повторяются циклически во время генерации внутреннего состояния функцией (4), вместе с точками, которые получаются до начала периодической последовательности точек.

3. Burton S. One-Way Permutations on Elliptic Curves / Burton S. Kaliski, Jr. // Journal of Cryptology (1991) International Association for Cryptologic Research. 1991. - P. 187 – 199.

4. Beelen P. Pseudorandom sequences from elliptic curves / Beelen P., Doumen J. // Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer-Verlag, Berlin, 2002, 37 – 52.

5. Shparlinski I. E. On the Naor-Reingold pseudo-random function from elliptic curves, Applicable Algebra in Engineering, Communication and Computing 11 (2000), pp. 27 – 34.

6. Lange T. Certain exponential sums and random walks on elliptic curves / Lange T., Shparlinski I. E. // Canadian Jornal of Mathematics 57. – 2005. – pp. 338 – 350.

7. Gjøsteen K. Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005 / Kristian Gjøsteen // March 16, 2006.

8. Горбенко І.Д. Метод побудування випадкових бітів на основі спарювання точок еліптичних кривих / Горбенко І.Д., Шапочка Н.В., Погребняк К.А. // Журнал "Прикладная радиоэлектроника" 2010 №3. Харьков – 2010, сс. 386 – 394.

9. NIST Special Publication 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) / Elaine Barker, John Kelsey // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – March 2007.

10. Schoenmakers B. Cryptanalysis of the Dual Elliptic Curve Pseudorandom sequences from elliptic curves / Schoenmakers B., Sidorenko A. // 29 may 2006.

11. Зайцева Н. Ю. Атака розпізнавання на генератори псевдовипадкових послідовностей на основі еліптичних кривих / Зайцева Н. Ю., Завадська Л. О. // Теоретичні і прикладні проблеми фізики, математики та інформатики. – Збірка тез доповідей. ВПІ ВПК «Політехніка» - Київ – 2012. – С. 238 – 239.

12. Бессалов А. В., Чевардин В. Е. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций ЭК// Прикладная радиоэлектроника: научно-технический журнал – 2012. – Том 11. №2. – С. 234 – 237.

13. Бессалов А. В., Телиженко А. Б. Криптосистемы на эллиптических кривых: Учеб. Пособие. – К.: ІВЦ «Видавництво «Політехніка»», 2004. – 224 с.