УДК 681.3.06:519.248.681

И. Д. ГОРБЕНКО, д-р техн. наук, С. И. ЗБИТНЕВ, А. А. ПОЛЯКОВ

КРИПТОАНАЛИЗ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ В ГРУППАХ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ МЕТОДОМ ПОЛЛАРДА.

Введение

В последние годы для криптографических преобразований начали использоваться эллиптические кривые (ЭК) над полем Галуа $GF(p^n)$, где p – простое, а n – целое. Появились рабочие версии стандарта цифровой подписи X9.62[1] и протоколов Диффи – Хелмана X9.63[2], которые, по мнению разработчиков и специалистов, имеют ряд преимуществ и разрешают ряд противоречий, которые в последние годы явно появились в криптографии с открытыми ключами и открытым распространением ключей. Суть противоречий заключается в том, что в условиях интенсивного развития и создание нового математического аппарата, а также высокопроизводительных систем и средств криптоанализа, для обеспечения требуемого уровня стойкости необходимо непрерывно увеличивать длины параметров (модулей) преобразований и ключей, на сегодня до единиц тысяч и более битов. Это противоречие присуще криптографическим преобразованиям в кольцах и полях. Уменьшение длин параметров и ключей, по мнению специалистов, может быть достигнуть за счет использование при криптографических преобразованиях групп точек на эллиптической кривой над полем Галуа $GF(2^m)$ и $GF(p^n)$ [3]. Использование преобразований в группах точек на ЭК предположительно позволяет реализовать вероятно-стойкие или по другой терминологии доказуемо стойкие криптоалгоритмы. При этом доказательство стойкости в наиболее общем случае сводят к доказательству сложности решение дискретного сравнения в группе точек ЭК над полем Галуа $GF(p^n)$

$$Q = d \cdot G(\mathrm{mod}\, f(x), p), \tag{1}$$

относительно d, где G – базовая точка на ЭК порядка n, d – личный ключ (целое число, $1 \le d \le n-1$). Q – открытый ключ, $f(x)$ – примитивный полином, p – простое число.

Более частной является задача Диффи – Хелмана, которое формируется в следующем виде. Известны открытые ключи

$$Q_1 = d_1 G(\mathrm{mod}\, f(x), p) \text{ и } Q_2 = d_2 G(\mathrm{mod}\, f(x), p).$$

Необходимо найти значение общего секрета.

$$K_{21} = K_{21} = d_1 d_2 G(\mathrm{mod}\, f(x), p). \tag{2}$$

На сегодня известно несколько методов решения сравнений вида (1). Получили распространения методы Полларда ρ [4] и λ – метод.

Целью настоящей статьи является разработка математического аппарата и алгоритмов криптоанализа с использованием метода ρ – Полларда. Основной причиной выбора этого метода является возможность эффективного распараллеливания процесса решения сравнения вида (1) и по взглядам на сегодняшний день меньшая по сравнению с другими методами сложность.

1. Математическая постановка задачи

Пусть задана супернесингулярная ЭК над полем $GF(2^m)$ в аффинном представлении

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

где a и b – параметры ЭК.

Она определена множеством точек $(x, y) \in GF(2^m) \times GF(2^m)$, a и $b \in GF(2^m)$, $b \neq 0(\mathrm{mod}\, f(x), 2)$. Точки на ЭК, включая точку бесконечности O, образуют группу с операцией сложения.

Если точка $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ принадлежат эллиптической кривой, т.е. $P_i \in E(GF(2^m))$, то для каждой из них существует обратная точка, соответственно $-P_1 = (x_1, x_1 + y_1)$ и

$-P_2=(x_2,x_2+y_2)$, а также точка $P_3=(x_3,y_3)$, такая что $P_1+P_2=P_3$. Координаты точки $P_3=(x_3,y_3)$ определяются с использованием соотношений

$$x_3=\lambda^2+\lambda+x_1+x_2+a \pmod{f(x),2}; \tag{4}$$

$$y_3=\lambda(x_1+x_3)+x_3+y_1 \pmod{f(x),2}; \tag{5}$$

$$\lambda=\begin{cases}\dfrac{y_1+y_2}{x_1+x_2}\pmod{f(x),2}, & \text{если} \quad P_1\neq P_2;\\ \dfrac{x_1^2+y_1}{x_1}\pmod{f(x),2}, & \text{если} \quad P_1=P_2,\end{cases} \tag{6}$$

скалярное умножение определяется для нескольких точек $G\in E(GF(2^m))$ как

$$d\cdot G\pmod{f(x),2}=\underbrace{G+G+G+\ldots+G}_{d\text{ раз}}\pmod{f(x),2}. \tag{7}$$

Операция (7) реализуется за счет применения операций сложения $(P_1\neq P_2)$ или удвоения $(P_1=P_2)$.

Точка G имеет порядок n на ЭК, если

$$n\cdot G\pmod{f(x),2}=O; \tag{8}$$

где O – точка на бесконечности (ноль).

Важнейшей задачей при выполнении операций (4) – (8) является минимизация сложности. К сожалению продуктивных методов и алгоритмов выполнения аффинных преобразований, особенно в (6), где требуется выполнять деление по модулю, неизвестно или нет. При выполнении криптоанализа задача минимизация сложности вычислений (4) – (8) становиться особенно актуальной и требует особого внимания.

Одним из возможных методов уменьшения сложности преобразований при решении задач вида (1) и (2) является использование проективного представления точек на эллиптической кривой и выполнение операций (4) – (8) в проективном базисе. Существует ряд проблемных вопросов реализации проективного представления вычислений при криптоанализе.

При переходе от аффинного представления к проективному используют следующее преобразование [3]

$$x=\frac{X}{Z^2};\ y=\frac{Y}{Z^3}.$$

При этом точка в аффинном представлении $Q_{afin}=(x,y)$ отображается в точку проективного представления $Q_{project}=(x,y,1)$, а обратный переход выполняется в виде $Q_{afin}=\left(\dfrac{x}{z^2},\dfrac{y}{z^3}\right)$.

Проективным аналогом сравнения (3) является сравнение

$$Y^2+XYZ=X^3+aX^2Z^2+bZ^6\pmod{f(x),2}. \tag{9}$$

Если $P_1=(X_1,Y_1,Z_1)$ и $P_2=(X_2,Y_2,Z_2)$ и $P_1\neq P_2$, то суммой двух точек P_1+P_2 является точка $P_3=(X_3,Y_3,Z_3)$, координаты которой определяются с использованием формул [3] по модулю $(f(x),2)$.

$$X_3=SU; \tag{10}$$

$$Y_3=T(U+S^2X_1Z_2)+S^3Y_1Z_2+SU; \tag{11}$$

$$Z_3=S^3Z_1Z_2, \tag{12}$$

где $S=X_2Z_1+X_2Z_2;\ T=Y_2Z_1+Y_1Z_2;\ U=(T^2+TS+aS^2)Z_1Z_2+S^3.$ (13)

Для случая, когда $P_1 = P_2$ с использованием формул

$$X_3 = ST; \tag{14}$$

$$Y_3 = X^4 S + T\left(S + YZ + X^2\right); \tag{15}$$

$$Z_3 = S^3, \tag{16}$$

где $S = XZ;\ T = bZ^4 + X^4$. (17)

Причем математические операции в (14) – (17) выполняется по модулю $\left(f(x),2\right)$.

Подробные сведения, методы и алгоритмы выполнение операций сложения и удвоения точек эллиптической кривой приведены в [3].

2. Характеристики известных методов криптоанализа

Основными среди известных методов решения сравнения вида (1) являются методы Полларда ρ и λ – метод [4]. Сложность ρ – Полларда метода можно оценить с использованием соотношения [4]

$$I_\rho = \sqrt{\frac{\pi n}{2}}, \tag{18}$$

где n – порядок базовой точки на эллиптической кривой. В [4] показано, что ρ – Поллард метод может быть ускорен в $\sqrt{2}$ раза, в этом случае

$$I_\rho{}' = \sqrt{\frac{\pi n}{4}}. \tag{19}$$

Одним из преимуществ методов ρ – Полларда является то, что он допускает распараллеливание на r независимых процессов. В этом случае сложность реализации каждого из процессов можно оценить как

$$I_{\rho_1} = \frac{\sqrt{\frac{\pi n}{2}}}{r} = \sqrt{\frac{\pi n}{2r^2}}; \tag{20}$$

$$I_{\rho_1}{}' = \frac{\sqrt{\frac{\pi n}{4}}}{r} = \sqrt{\frac{\pi n}{4r^2}}. \tag{21}$$

Сложность при использовании метода λ – Полларда может быть оценена как [2]

$$I_\lambda = 2\sqrt{n}; \tag{22}$$

а при распараллеливании

$$I_{\lambda_1} = \frac{2\sqrt{n}}{r}. \tag{23}$$

В (18) – (23) сложность оценивается количеством операций сложений на эллиптической кривой.

Проведем сравнительный анализ по сложности названных методов. Для этого найдем отношение

$$\frac{I_\lambda}{I_\rho} = \frac{2\sqrt{n}}{\sqrt{\frac{\pi n}{2}}} = \frac{2\sqrt{2}}{\sqrt{\pi}} = \frac{\sqrt{8}}{\sqrt{\pi}} \approx 1.558. \tag{24}$$

Из отношения (24) вытекает, что λ – метод более сложен чем даже не оптимизированный ρ – метод. Поэтому в дальнейшем сосредоточим внимание на методах ρ – Полларда.

3. Алгоритм решения сравнения по основе ρ – метода Полларда

Непосредственно из (1) следует, что используя ρ – метод необходимо найти число d, такое что $1 \le d \le n-1$. Будем формировать последовательность предполагаемых решений d_i сравнения (1), используя функцию $f(Z_i)$, $i = 0,1,3,...,n$, которая в соответствии с ρ – методом обеспечивает (может обеспечивать) нахождение пары значений $f(Z_i)$ и $f(Z_j)$, таких, что

$$f(Z_i) = f(Z_j), \ (i \ne j). \tag{25}$$

Одним из предпочтительных представлений точек Z_i является

$$Z_i = A_i G + B_i Q, \tag{26}$$

где G – базовая точка на эллиптической кривой, а Q – открытый ключ [3].

Выберем случайным образом два числа A_0 и $B_0 \in [0, n-1]$, но так чтобы одновременно A_0 и B_0 не были равны нулю.

$$f(Z_0) = A_0 G + B_0 Q. \tag{27}$$

Далее будем искать значения $f(Z_i)$ и $f(Z_j)$, удовлетворяющие условию (25). В этом случае получим, что

$$A_j G + B_j Q \equiv A_i G + B_i Q (\mathrm{mod}\, f(x), p), \ (i \ne j). \tag{28}$$

где наличие $f(x)$ и p означает, что кривая рассматривается над полем $GF(p^m)$, m – порядок расширения поля. После преобразований (28) имеем

$$(B_i - B_j) Q = (A_j - A_i) G (\mathrm{mod}\, f(x), p), \ (i \ne j),$$

или

$$Q = \frac{A_j - A_i}{B_i - B_j} G (\mathrm{mod}\, f(x), p), \ (B_i \ne B_j), \tag{29}$$

сравнивая (1) и (29) имеем, что

$$d = \frac{A_j - A_i}{B_i - B_j} (\mathrm{mod} n), \ (B_i \ne B_j). \tag{30}$$

Выясним, каким образом нужно формировать пары коэффициентов (A_i, B_i) для всех $i \le n$. Наиболее простым алгоритмом формирования коэффициентов является следующим [4].

Разобьем точки на ЭК на три равных множества S_1, S_2 и S_3 и вычислим рекуррентно по правилу

$$Z_{i+1} = f(Z_i) = \begin{cases} 2Z_i, & если \quad Z_i^x \in S_1; \\ Z_i + G, & если \quad Z_i^x \in S_2; \\ Z_i + Q, & если \quad Z_i^x \in S_3; \end{cases} \tag{31}$$

где Z_i^x означает x – координату точки на ЭК.

Значение Z_0 формируется по (27), в простейшем случае $Z_i = G$ или $Z_i = Q$, или $Z_i = G + Q$. Выполняя последовательно вычисления по правилу (31) мы, по существу, будем изменять и коэффициенты A_i, B_i. Найдя Z_i и Z_j, удовлетворяющие условию (25), мы получим решение в виде (30).

Пример 1. Пусть имеется точка $G=(13,7)$, которая принадлежит кривой

$$y^2 = x^3 + x + 1 (\mathrm{mod}\, 23)$$

и $Q=(17,20)$. Можно показать, что G имеет порядок $n=7$. Необходимо решить сравнение (1) вида

$$(17,20) = d(13,17) (\mathrm{mod}\, 23),\ d \in [1, n-1].$$

Разобьем $p-1=22$ на три области $S_1 \in [0,7]$, $S_2 \in [8,15]$, $S_3 \in [16,22]$ и выберем $Z_0 = G = (13,7)$.

Вычислим последовательность Z_{i+1} используя (31). Поскольку $Z_0^{\,x} \in S_2$, то $Z_1 = Z_0 + G = (13,7) + (13,7) = (5,4)$. Далее $Z_1^{\,x} \in S_1$, поэтому $Z_2 = 2Z_1 = 2(5,4) = (17,20)$. $Z_2 \in S_3$, поэтому $Z_3 = Z_2 + Q = (17,20) + (17,20) = (13,7)$.

Мы получили значения Z_3 такое, что

$$Z_3 = Z_0.$$

Теперь необходимо определить пары коэффициентов (A_i, B_i) и (A_j, B_j), для которых выполняется условие (28). Результаты вычислений приведены в табл. 1.

Таблица 1

Шаг	Z_i	A_i	B_i	$A_iG + B_iQ$
0	$(13,7)$	1	0	$1\cdot(13,7) + 0\cdot(17,20)$
1	$(5,7)$	2	0	$2\cdot(13,7) + 0\cdot(17,20)$
2	$(17,20)$	4	0	$4\cdot(13,7) + 0\cdot(17,20)$
3	$(13,7)$	4	1	$4\cdot(13,7) + 1\cdot(17,20)$

Из таблицы определяем, что

$$A_0 = 1;\ B_0 = 0;\ A_3 = 4;\ B_3 = 1.$$

По правилу (30) имеем

$$d = \frac{1-4}{1-0} (\mathrm{mod}\, 7) = -3 (\mathrm{mod}\, 7) = 4.$$

Проверкой убедимся, что $d = 4$ является решением примера.

Алгоритм (31) при больших значениях n становится не эффективным. Как показали исследования, он может быть улучшен [4], если все множество точек эллиптической кривой, включая точку бесконечности, разбивать на $r > 3$ не пересекающихся множеств. В этом случае функция $f(Z_i)$ задается в виде

$$Z_{i+1} = f(Z_i) = \begin{cases} (Z_i + c_1 G + d_1 Q), & \text{если} \quad Z_i \in S_1; \\ (Z_i + c_2 G + d_2 Q), & \text{если} \quad Z_i \in S_2; \\ \ldots\ldots\ldots\ldots & \ldots\ldots \quad \ldots\ldots\ldots \\ (Z_i + c_r G + d_r Q), & \text{если} \quad Z_i \in S_r; \end{cases} \qquad (32)$$

где c_v, d_v – случайные целые числа из интервала $[0, n-1]$.

Установлено [4], что при использовании итерационных формул вида (32) можно уменьшить сложность (стоимость времени) процедуры криптоанализа. Кроме того, применение правил (32) позволяет эффективно распараллелить процесс нахождения коэффициентов A_i и B_i, для которых выполняется условие (28), по крайней мере, на r процессов.

Если числа c_v и d_v выбирать таким образом, чтобы пересечения значений Z_i в областях не было, то и каждую область, можно разбить на необходимое число подобластей, Это позволяет распараллелить задачу на необходимое количество независимых процессов. Результаты работы каждого из процессов в виде троек чисел (Z_i, A_i, B_i) заносятся в общую базу данных. Центральный процессор осуществляет параллельный поиск значений

$$Z_i = Z_j,\ (i \neq j),$$

и после этого с использованием выражения (30) вычисляют личный ключ d.

На практике процесс нахождения d может быть ускорен, если воспользоваться взаимосвязью основной и обратной точек. Если существует точка $P=(x,y)$, то обратной точкой, над полем $GF(2^m)$, является $(-P)=(x,x+y)$. Это означает, что у основной и обратной точек координаты x одинаковые. Поэтому для алгоритма (32) необходимо искать только точки у которых x – координаты одинаковые. В этом случае возможны два исхода:

1) координаты y у обеих точек одинаковы;
2) координаты y у обеих точек разные.

В первом случае решение находится так же как уже описывалось выше. Во втором случае правило неприменимо. Но если учесть, что основная и обратная точки связаны соотношением

$$Z_j + Z_k = O, \tag{33}$$

то истинные значения координат точек, для которых совпадают обе координаты точек, можно пересчитать используя то, что [4]

$$A_k + A_j = n \text{ и } B_k + B_j = n.$$

Получим, что

$$A_j = n - A_k \text{ и } B_j = n - B_k,$$

где положено, что A_k и B_k – коэффициенты точки у которой не совпадают y координаты. Использование отмеченного свойства позволяет уменьшить сложность нахождения личного ключа не менее чем в 2 раза

4. Примеры нахождения личного ключа на ЭК над полем $GF(2^m)$.

Пусть имеется ЭК $y^2+xy=x^3+ax^2+b$ над полем $GF(2^m)$ $(m=33)$, параметры ЭК: $a=571EF7A8$ и $b=39A75A68$, а полином над $GF(2^{33})$ $f(x)=200000401$. В качестве базовой выберем точку $G=(030D5A653,1B081C3F)$. Эта точка на кривой имеет порядок $n=7FFF9BEF$, открытый ключ $Q=(\text{C69A56D4,1955247BB})$.

Составим аналогично (1) уравнение

$$(\text{C69A56D4,1955247BB})=d(030D5A653,1B081C3F).$$

В таблице 2 приведены значения c_v и d_v. В таблице 3 приведены некоторые значения коэффициентов и процесс поиска коэффициентов. Он аналогичен работе при ручном поиске (пример 1).

Таблица 2

Интервал	Z_i	A_i	B_i	Интервал	Z_i	A_i	B_i
0	(0 17db318b,0 17db318b)	2ed6d0f2	7149f463	10	(1 ae1c4f64,0 ae1c4f64)	5066a455	3731287c
1	(1 1c1b66d4,0 1c1b66d4)	6bea2002	3cdba6b3	11	(1 71c072f7,1 71c072f7)	22a13b32	1d918707
2	(0 28db3c5d,1 28db3c5d)	193e7098	1c0d5e24	12	(1 77eab9f7,0 77eab9f7)	5a1feff2	299cab0
3	(0 da315ef2,0 da315ef2)	5e481b17	484d76c4	13	(1 830e176e,0 830e176e)	499d72b9	457ee43d
4	(1 a58b7411,0 a58b7411)	268c1f54	7d5a031f	14	(0 3a3b41a8,0 3a3b41a8)	ea39aa	4cca4ec3
5	(0 db9be265,1 db9be265)	1f253809	7ccc386e	15	(0 2d17b52e,1 2d17b52e)	56682364	7ed614bf
6	(0 668ecf21,1 668ecf21)	3b45f596	a890d13	16	(0 6fecbfbb,1 6fecbfbb)	668edc2d	4957ef83
7	(0 3b7b8cf6,1 3b7b8cf6)	32aedb1c	6e50fe31	17	(1 a3edec8d,0 a3edec8d)	f6a6372	1ed1cd61
8	(0 14d557ad,1 14d557ad)	7d36dc51	7632ad23	18	(0 c7420d46,0 c7420d46)	72169c9d	701e4a83
9	(0 1d5d56f4,1 1d5d56f4)	5c49e1af	7214b3be	19	(0 124f81ea,1 124f81ea)	774a4f84	39e8d702

Таблица 3

Шаг	Z_i	Применяемый интервал	A_i	B_i
1	(0 124f81ea,1 124f81ea)	Интервал=10	A[1]=774a4f84	B[1]=39e8d702
2	(0 41d32423,1 41d32423)	Интервал=7	A[2]=47b157ea	B[2]=7119ff7e
3	(1 d56a393e,0 d56a393e)	Интервал=18	A[3]=7a603306	B[3]=5f6b61c0
4	(0 efb109bf,1 efb109bf)	Интервал=11	A[4]=6c7733b4	B[4]=4f8a1054
5	(0 c4ffc7df,0 c4ffc7df)	Интервал=3	A[5]=f18d2f7	B[5]=6d1b975b
	.....	.....	.....	.....
7545	(1 ccab1475,0 ccab1475)	Интервал=17	A[7545]=2cc89bd9	B[7545]=797aa370
7546	(1 a7b63df1,1 a7b63df1)	Интервал=1	A[7546]=3c32ff4b	B[7546]=184cd4e2
7547	(1 e4592c48,0 e4592c48)	Интервал=8	A[7547]=281d835e	B[7547]=55287b95
7548	(1 6e8a5c1b,1 6e8a5c1b)	Интервал=7	A[7548]=2554c3c0	B[7548]=4b5b8cc9

Проведены эксперименты по нахождению личного ключа для ЭК над полем $GF(2^m)$ при $m=64$. Среднее время решения на одном Pentium III-800 составляет 48 мин. Отрабатываются составляющие решения сравнения (1) для $m=96$ и $m=112$. Заметим, что при решении сравнения могут возникать тупиковые ситуации.

5. Оценка сложности криптоанализа практически применяемых ЭК над $GF(2^m)$.

Группа точек ЭК является циклической группой. Поэтому потенциальные оценки сложности дискретного логарифма, которая может быть обеспечена в предельном случае, необходимо искать в общем случае как для произвольной циклической группы G. Известен метод Шенкса, при использовании которого задачу дискретного логарифма в произвольной циклической группе можно решить за $\sqrt{2^m}$ операций. Решение основывается на составление двух стеков размером $t=\sqrt{2^m}$ отсортированных по вторым компонентам [1]. Например первый стек состоит из пар $(i,\theta_e^{\,it})$, $i=\overline{0,t-1}$ и отсортирован по второму компоненту, где θ – первообразный элемент группы. Второй стек состоит из пар (α,y^j), $j=\overline{0,t-1}$ и тоже отсортирован по второй компоненте. При наличии таких стеков можно найти две пары с равными вторыми компонентами, т.е. (i,θ^{it}) и $(j,y\theta^j)$, причем $\theta^{it}=y\theta^j$, и далее

$$x=(it-j)(\bmod 2^m). \tag{34}$$

Полагая, что для решения сравнения (1) используется система, выполняющая соответственно $\gamma=10^6$ и 10^8 операций сложений на ЭК получим оценки безопасного времени $t_б$ для ρ – метода Полларда (выражение (19)). В таблице 4 приведены оценки $t_б$ для $\gamma=10^6$ (для $\gamma=10^8$ $t_б'$)операций сложения на ЭК/с, полученные с использованием выражения $t_б=\dfrac{I_\rho}{\gamma k}$, где $k=3.1\cdot10^7$ с/год (кол-во секунд в год).

Таблица 4

n	96	128	160	192	224	256	512
I_ρ (оп/с)	$249\cdot10^{12}$	$16{,}3\cdot10^{18}$	10^{25}	$70{,}2\cdot10^{27}$	$4{,}6\cdot10^{33}$	$3\cdot10^{38}$	10^{77}
$t_б$ (лет)	8,04	$5{,}2\cdot10^5$	$34{,}5\cdot10^9$	$2{,}2\cdot10^{15}$	$1{,}48\cdot10^{20}$	$9{,}72\cdot10^{24}$	$3{,}31\cdot10^{63}$
$t_б'$ (лет)	0,0804	$5{,}2\cdot10^3$	$34{,}5\cdot10^7$	$2{,}2\cdot10^{13}$	$1{,}48\cdot10^{18}$	$9{,}72\cdot10^{22}$	$3{,}31\cdot10^{61}$

Заключение

В ближайшие годы следует ожидать сосредоточение особого внимания и интеллектуальных ресурсов на решение задач криптоанализа в группах точек эллиптических кривых. По видимому основные усилия будут направлены на развитие математического аппарата решения сравнения вида (1) и (2), а также создания распараллеленых криптоаналитических систем . Если будут серьезные достижения в минимизации сложности вычислений в группах точек эллиптических кривых, то это приведет к необходимости увеличению параметров эллиптической кривой. Поэтому во внедряемых

стандартах необходимо предусматривать широкий спектр значений параметров. Так по нашим оценкам в цифровых подписях и протоколов аутентификации и управление ключами необходимо было бы предусмотреть преобразования с порядками базовых точек $n = 2^{160}, 2^{224}, 2^{256}, 2^{512}$ и более. Использование такого спектра значений порядка базовой точки с одной стороны может обеспечивать при необходимости требуемый уровень стойкости, а с другой допустимый уровень вычислительной сложности.

Список литературы: 1. *X9.62 Public Key Cryptography For The Financial Services Industry*: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998, 87 с. 2. *X9.63 Public Key Cryptography For The Financial Services Industry*: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 1999. 207 с. 3. *IEEE P1363 / D11 (Draft Version 11).* Standard Specifications for Public Key Cryptography. Annex A (Informative). Number-Theoretic Background, 1999. 91 с. 4. *Michael J. Wiener, Robert J. Zuccherato* Faster Attacks on Elliptic Curve Cryptosystems, 1998, 8 с.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 19.03.2001