УДК 681.3.06:519.248.681

В.Е. ЧЕВАРДИН

Полтавский военный институт связи, Украина

МЕТОД ИТЕРАЦИОННОГО ХЕШИРОВАНИЯ НА ОСНОВЕ ПРЕОБРАЗОВАНИЙ В ГРУППЕ ТОЧЕК НЕСИНГУЛЯРНОЙ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Представлены результаты исследований методов итерационных хеш-функций на базе модулярной арифметики и арифметики эллиптических кривых. Предложен метод Q-хеширования на базе арифметики эллиптических кривых, позволяющий получить строго универсальные классы хеширования и избежать ограничений в существующих схемах представления текста точками кривой.

хеш-функция, универсальные классы, эллиптические кривые, преобразования, группа кручения

Введение

Обеспечение безопасности информации является одной из главных проблем, стоящих перед разработчиками современных автоматизированных систем управления (АСУ). Результаты ежегодных исследований проблем информационной безопасности (Global Information Security Survey 2004′), проведенных компаниями Emst&Young и InfoWatch [1 – 3], показали, что наибольшая часть нарушений безопасности информации приходится на ее целостность (*Ц*) и аутентичность (*А*) (62%). Это объясняется доступностью для широкого круга лиц возможностей современных технологий распределенных вычислений и ресурсов ЭВМ большой вычислительной мощности, которые позволяют осуществлять криптоанализ в реальном времени. Одним из мощных механизмов обеспечения Ц и А информации являются схемы ключевого хеширования. Используемый в нашем государстве стандарт хеширования данных ГОСТ 28147-89 уступает по стойкости разработанному Европейскому стандарту IEEE 802.11i на базе шифра Rijndael, поэтому целесообразным является построение ключевых хеш-функций на базе более сильного математического аппарата. Примером такого аппарата являются эллиптические кривые.

Предложенные к использованию в 1985 г. независимо Коблицем и Миллером [4, 5] эллиптические кривые позволили решить такие проблемы, как быстрая факторизация целых, поиск конгруэнтных чисел и доказательство великой теоремы Ферма. Для современной криптографии применение эллиптических кривых позволило получить новые несимметричные системы с длиной ключа длиной 163 бита, стойкость которых соответствует стойкости RSA-подобных систем с диной ключа 1024 бита.

В связи с этим актуальным направлением исследований является применение эллиптических кривых для построения ключевых схем хеширования, что позволит существенно повысить их стойкость.

Существует несколько подходов к построению схем бесключевого хеширования и цифровой подписи на базе преобразований в группе точек эллиптической кривой [4, 6 – 9]. Основным недостатком существующих схем является сложность на этапе сопоставления текста точкой кривой. Эту задачу также необходимо решить при построении итерационной схемы хеширования. В зависимости от рассматриваемого поля и выбранной кривой текст представляется в виде точки кривой по-разному.

Способ 1. Для уравнения кривой F(x; y): $y^2 + yx = x^3 + Ax + B$, над полем F в качестве X-координаты используется $(n - k)$-разрядный текст, дополненный k двоичными разрядами так, что число

$f(x)$ – квадратичный вычет в поле F [9]. Такой способ более эффективен для эллиптических кривых над простыми полями, поскольку для нахождения k нужно вычислять значения квадратичного характера, что легко выполняется через символ Якоби в простом поле. Основным ограничением использования такого способа является его избыточность и влияние коэффициента A на скорость шифрования, что в обоих случаях сводится к росту вычислительных затрат. Второй способ отличается использованием суперсингулярных кривых вида $y^2 = x^3 + Ax + B$ над полями характеристики 3 [6 – 7] для хеширования и формирования цифровой подписи BLS с максимальным множителем стойкости к MOV – атаке, $\alpha = 6$ [11].

Способ 2. Текст в этом случае сопоставляется X-координате точки, а координата Y затем определяется из уравнения кривой – схема Map2Group, схема Map3Group отличается тем, что текст представляется координатой Y. Основным ограничением использования этого способа является существование нехешируемых текстов, что приводит к увеличению вычислительных затрат на криптопреобразования, используемые в схеме хеширования.

Таким образом, возникает противоречие между необходимостью использования стойких хеш-функций на базе эллиптических кривых и ростом вычислительных затрат на криптопреобразования, используемые в них. В работе предлагается эффективное решение сложившегося противоречия, открывающегося в отмеченном направлении.

Для исследования и разработки схем хеширования на базе арифметики эллиптических кривых рассмотрим принципы построения итерационных хеш-функций на базе модулярной арифметики и арифметику эллиптических кривых.

Для оценки стойкости схем хеширования к коллизиям введем определения и классификацию, предложенные в работах [11, 14].

Классификация схем хеширования по Вегману и Картеру

Пусть M – состояние источника последовательностей $\{0, 1\}^n$, $M \in \sum^n$, h – хеш-код (результат хеширования), $h \in \sum^r$, H – семейство функций отображения $\sum^n \to \sum^r$ размера R, $H \in \sum^R$, причем $\left| R \right| \leq \leq \varepsilon \leq 1$. Универсальный класс хеш-функций принято обозначать как ε-$U(N, n, \text{r})$, где N – мощность функций отображения, n – мощность множества входных последовательностей, r – мощность множества хеш-кодов. В соответствии с введенными определениями, если R – абелева группа, то существуют следующие классы хеш-функций:

U – семейство универсальных хеш-функций H, если для всех $M_1 \neq M_2 \in \sum^n$ $Ph \in H[h(M_1) = h(M_2)] = 1/\left| R \right|$;

ε -AU – семейство ε-почти универсальных хеш-функций H, если для всех $M_1 \neq M_2 \in \sum^n$ $P_h \in H[h(M_1) = h(M_2)] \leq \varepsilon$;

ΔU – семейство Δ-универсальных хеш-функций, если для всех $M_1 \neq M_2 \in \sum^n$ и $a \in R$, $P_h \in H[h(M_1) - h(M_2) = a] = 1/\left| R \right|$;

ε-$A\Delta U$ – семейство почти Δ-универсальных хеш-функций, если для всех $M_1 \neq M_2 \in \sum^n$ и $a \in R$, $P_h \in H[h(M_1) - h(M_2) = a] \leq \varepsilon$;

SU – семейство строго универсальных хеш-функций, если для всех $M_1 \neq M_2 \in \sum^n$ и $a, b \in R$, $P_h \in H[h(M_1) = a, h(M_2) = b] = 1/\left| R^2 \right|$;

ε-ASU – семейство почти строго универсальных хеш-функций, если для всех $M_1 \neq M_2 \in \sum^n$ и $a \in R$, $P_h \in H[h(M_1) - h(M_2) = a] \leq \varepsilon / \left| R \right|$.

Представление схем хеширования в виде универсальных классов позволяет получить для них количественную оценку стойкости к коллизиям и связать ее с размером ключевых данных.

Принципы построения схем хеширования на базе модулярной арифметики

Ключевой хеш-функцией называется итерационная схема хеширования, параметризованная секрет-

ным ключом, общий вид которой представлен в [19]. Ядром итерационной хеш-функции является цикловая функция *f*, свойства которой определяют надежность схемы хеширования, ее вычислительную стойкость, стойкость к коллизиям и вычислительную сложность.

Существует ряд модификаций и разновидностей схем на базе модулярной арифметики, которые за счет упрощения цикловой функции позволяют получить более низкие показатели вычислительной сложности схемы хеширования [11, 12, 14], что чаще всего сопровождается снижением стойкости таких схем.

Для ключевых схем хеширования на базе модулярной арифметики, предложенных в работе [14], и других RSA-подобных системах в качестве криптографического примитива использовалась операция возведения в степень по модулю простого числа. В такой схеме текст представлялся в виде большого целого числа *a*, которое затем возводилось в степень большого числа *k* (*k* – секретное число) по модулю простого *p*, $H_i = H_{i-1}^k \bmod p$. Для других представителей этого семейства использовалась либо операция возведения в квадрат либо другая операция (комбинация операций) в мультипликативной группе целых чисел, примером таких схем являются: MASH-1, MASH-2, ММН и другие схемы [12 – 14].

Цикловые функции этих схем представлены следующими выражениями:

$f_{\text{MASH-1}}$: $H_i = (((H_{i-1} y_i) A)^2 \bmod m) \mid n) \oplus H_{i-1}$, где разложение $p = vq$ (*v* и *q* – случайно выбранные числа) секретно;

$f_{\text{MASH-2}}$: $H_i = (((H_{i-1} y_i) A)^{2^8+1} \bmod m) \mid n) \oplus H_{i-1}$;

$f_{\text{ММН}}$: $g_x(m) \overset{def}{=} m \cdot x \bmod p = \sum_{i=1}^{k} m_i x_i \bmod p$, где x_i – является секретом, *p* – простым числом.

Основную часть вычислительной сложности рассмотренных цикловых функций составляют процедуры возведения в степень либо умножения по модулю простого числа, при этом сложность в отождествлении текста элементом группы, кольца либо поля целых чисел отсутствует.

Недостатком таких схем, с одной стороны, является невозможность построения строго универсальных классов хеш-функций, поэтому схемы являются доказуемо либо вычислительно стойкими. С другой стороны, для обеспечения требуемой вычислительной стойкости таких схем необходимо, чтобы длина ключа была порядка 1024 бит. Это вызывает повышение вычислительных затрат на криптопреобразования и снижает эффективность работы современных АСУ. В связи с этим, логичным шагом в развитии методов аутентификации и построении универсальных классов хеш-функций является применение арифметики в группе точек эллиптической кривой для построения ключевых итерационных хеш-функций. Рассмотрим суть скалярного произведения в группе точек эллиптической кривой и возможность его применения в схемах ключевого хеширования.

Скалярное произведение точек эллиптической кривой

Пусть *EC* – эллиптическая кривая над полем *GF*(*q*), представленная множеством точек аффинного пространства (*X*, *Y*), которая удовлетворяет общему уравнению Вейерштрасса [15]:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_5, \qquad (1)$$

где $a_i \in K, i = \overline{1, 6}$, (*K* – фиксированное алгебраическое замыкание *GF*(*q*)).

Скалярным произведением точки *Q* на скаляр *k* называется многократное сложение точки *Q* *k* раз (*kP* = *P* + *P*+ . . .+ *P* *k*-раз). Причем порядок базовой точки (мощность подгруппы, порождаемой точкой *Q*) определяет сложность криптоанализа (размерность задачи дискретного логарифмирования), по методу ρ-Полларда она составляет $\sqrt{2\pi n}$, где *n* – порядок базовой точки кривой.

Для применения аппарата эллиптических кривых в построении итерационных схем хеширования необходимо однозначно представить хешируемый текст точкой кривой, что в рассмотренных подходах 1, 2 вызывает неоднозначность либо повышение вычислительной сложности и накладывает дополнительное ограничение. Этого ограничения можно избежать с помощью представления текста M_i в виде числа s_i, где $0 < s_i < n$, n – порядок группы кручения точек кривой, а в качестве секретного параметра использовать базовую точку кривой Q (секретная базовая точка).

Схема *Q*-хеширования

Разработка схемы *Q*-хеширования

Пусть EC – произвольная эллиптическая несингулярная кривая, E_q – группа точек кривой EC, N_E – порядок группы E_q, $Q \in E_q$ – секретная базовая точка кривой, h – хеш-код, $s_i \in GF(q)$ – целое число, элемент поля $GF(q)$.

Данные M, поступающие на вход схемы хеширования, представляются в виде целых чисел: $M_i \rightarrow s_i$, где $s_i \in GF(q)$, $q = n$ – порядок базовой точки. Алгоритм итерационного Q-хеширования представлен следующими шагами:

1) устанавливаются значения: m, $GF(2^m)$, L_M – длина хешируемой последовательности;

2) задаются параметры кривой EC , $a_i \in GF(2^m)$;

3) вырабатывается секретная базовая точка Q, порядка n;

4) основной шаг криптопреобразования $f(M_i)$:

a. если $i = 0$, то $P_{i-1} = Q$;

b. вычисляется $s^x_i = (s_i + X(P_{i-1}) \bmod n) \oplus Y(P_{i-1})$;

c. выполняется скалярное умножение $s^x_i Q = P_i$;

5) координаты результирующей точки $P_t = (X_{P_t}; Y_{P_t})$ побитно складываются, результат поступает на выход, $h = (X_{P_t} \oplus Y_{P_t})$.

Основной шаг Q-хеширования представлен на рис. 1. Большая часть вычислительной сложности основного шага Q-хеширования приходится, как видно из рис. 1, на операции скалярного умножения точки эллиптической кривой (шаг 4c алгоритма Q-хеширования).

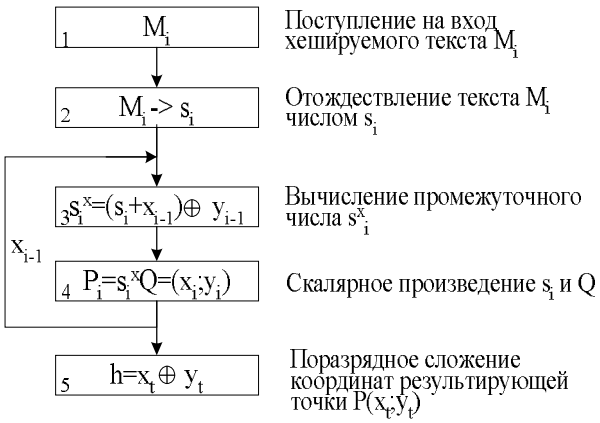

Рис. 1. Алгоритм основного шага Q-хеширования

Учитывая, что сложность задачи дискретного логарифмирования в группе точек эллиптической кривой в несколько раз превосходит сложность задачи дискретного логарифмирования в поле целых чисел, используемой в схемах [14], оценим выигрыш по вычислительным затратам Q-хеширования. В одной из наиболее удачных реализаций [16] время умножения полиномов над полем $GF(2^{163})$ на платформе Celeron 500 МГц составило 10,5 мкс, время скалярного произведения точки кривой – 13,5 мс, время возведения в степень большого числа над $GF(2^{1024})$ – 4 с. Использование этих алгоритмов и их реализаций позволяет получить выигрыш по вычислительным затратам на криптопреобразования в основном шаге Q-хеширования в 4 раза. Рассмотрим универсальные классы, которые возможно получить на базе схемы Q-хеширования.

Универсальные классы Q-хеширования

Рассмотрим вариант одноразрядовой схемы Q-хеширования, в которой текст представляется в виде одного числа s_i. Сформулируем и докажем следующую теорему.

Теорема 1. Семейство одноразрядовых функций Q-хеширования является строго универсальным

$\frac{1}{n} - SU(n,n,n)$ классом хеш-функций.

Доказательство. Пусть G_n является группой кручения точек кривой порядка n, где n – простое. Для всех точек из G_n справедливо $\forall Q \in G_n$, $s \in GF(n) \Rightarrow \{P = sQ,\ P \in G_n\}$. Существует матрица соответствий значений Q, скаляров s и функций отображения $G_n \to G_n$, $P_j^{s_i} = sQ$:

$Q_{i \setminus s_j}$	s_1	s_2		s_n
Q_1	s_1Q_1	s_1Q_2	…	s_1Q_n
Q_2	s_2Q_1	s_2Q_2	…	s_2Q_n
…	…	…	…	…
Q_n	s_nQ_1	s_nQ_2	…	s_nQ_n

Эта матрица имеет следующие свойства: в каждом столбце значение $P_j^{s_i}$ встречается один раз, в каждой строке значение $P_j^{s_i}$ также встречается один раз. Формализуем эти свойства в виде свойств, присущих строго универсальным классам хеширования:

1) для каждого $s_i \in GF(n)$ и P_i, число функций таких, что $P_i = s_iQ_j \in G_n$ равно 1;

2) для любых различных элементов $s_1, s_2 \in \{1, n\}$ и не обязательно различных $P_i \in G_n$, количество s таких, что $P_1^{s_1} = s_1Q_1$, $P_1^{s_2} = s_2Q_1$ не превышает 1.

Докажем первое свойство.

Пусть G_n – группа кручения точек EC, порядок которой n. Тогда любая точка $P_i \in G_n$ имеет такой же порядок n и является генератором группы кручения.

Зафиксируем $Q \in G_n$. При условии, что $s_i \in GF(n)$ пробегает все элементы $GF(n)$, имеем в результате скалярного умножения $P_i = s_iQ \in G_n$ всю группу кручения. Очевидно, что для каждого $s_i \in GF(n)$ и P_i, число функций таких, что $P_i = s_iQ_j \in G_n$, равно 1.

Докажем второе свойство способом от противного.

Допустим, что $s_1P = s_1P'$ и $s_2P = s_2P'$, при $P \neq P'$. Так как $\forall P_j^{s_i} \in G_n$, а G_n – группа кручения, то

$$\forall P_j^{s_i} \in G_n \{ P_j^{s_i} = s_iQ_j \},$$

где каждому s_i соответствует $P_j^{s_i}$. Учитывая, что $P \neq P' \Rightarrow s \neq s'$, выразим точки P и P'. В соответствии с этим справедливо:

$$s_1P = s_1P' \Rightarrow$$

$$\Rightarrow s_1(sQ) = s_1(s'Q);\ s_1sQ = s_1s'Q \Rightarrow s_1s = s_1s' \Rightarrow s = s'.$$

Следовательно, решение полученного уравнения существует при $s = s'$, т.е. решение существует при $P = P'$, что противоречит сделанному допущению.

Таким образом, семейство однораундовых функций Q-хеширования является $\frac{1}{n} - SU(n,n,n)$ классом хеш-функций, что и требовалось доказать.

Ограничением в использовании однораундовой схемы Q-хеширования является размер хеш-образа, равный размеру хешируемой последовательности, что ограничивает область применения такой схемы Q-хеширования.

Двухраундовая схема Q-хеширования. Согласно двухраундовой схемы Q-хеширования, хеш-образ формируется следующим образом:

$$h = s^x{}_2Q = (s_2 + X(P_1))Q = (s_2 + X((s_1 + X_Q)Q))Q, \quad (2)$$

где операция «+» обозначает сложение по модулю n.

Рассмотрим случай, когда текст M_1 представлен числами s_1, s_2, а $M_2 - s_2$, s_1.

Справедливы следующие результаты хеширования:

$$h = (s_2 + X_1)Q \text{ и } h' = (s_1 + X_2)Q.$$

Утверждение 1. Максимальная вероятность коллизий для двухраундовой схемы Q-хеширования составляет $1/n$, где n – порядок точки кручения.

Доказательство. Допустим, что для $M_1 \neq M_2$ $h = h'$. Учитывая сделанное допущение, получим следующее уравнение:

$$(s_1 + X(s_2Q))Q = (s_2 + X(s_1Q))Q.$$

Уравнение (3) имеет корни лишь в том случае, если $(s_1 + X(s_2Q))Q = (s_2 + X(s_1Q))Q$. Определим количество таких случаев. Сократим подобные члены уравнения (3), получим:

$$s_1 + X(s_2Q) = s_2 + X(s_1Q). \quad (3)$$

Исключив из рассмотрения случаи, когда $s_1 = s_2$, так как это противоречит сделанному допущению, получим условие для существования корней уравнения (3):

$$\forall s_1,\ \{s_1 = X(s_1Q)\} \Rightarrow \{s_2 = X(s_2Q)\} \Rightarrow$$
$$(s_1 + X(s_2Q))Q = (s_2 + X(s_1Q))\mathrm{Q}.$$

Решим следующее тождество:

$$s_1 + X(s_1Q) \equiv s_2 + X(s_2Q) \bmod n$$
$$\Rightarrow s_1 + X(s_1Q) \equiv 0 \bmod n$$

относительно s_1.

Данное тождество может иметь максимум одно решение:

при $s_1 < n$, $s_2 < n$, $X(s_1Q) < n$, $s_2 = X_P$,

в случае, если существует точка с координатой X_P, полученной как $P = s_2Q$.

Вероятность существования коллизии для двухраундовой схемы Q-хеширования определяется как отношение числа возможных сочетаний $s_1 + X(s_1Q)$ к числу решений уравнения (3):

$$P_{коллтах} = C_k^1 /\mathrm{d}, \quad (4)$$

где C_k^1 – биномиальный коэффициент; d – число решений уравнения (3).

Так как число возможных сочетаний s_1 и $X(s_1Q)$ равно n^2, то $P_{коллтах} = n/n^2 = 1/n$.

Таким образом, если s_1, $s_2 < n$, то для Q-хеширования $P_{коллтах} = 1/n$, где n – порядок группы кручения, что и требовалось доказать.

Обобщим полученные результаты на случай многораундовой схемы хеширования.

Многораундовая схема *Q*-хеширования. Обозначим семейство многораундовых хеш-функций Q-хеширования как Q-хеширование*. Текст в такой схеме Q-хеширования представляется последовательностью чисел $\{s_1, s_2,.., s_\delta\}$. Используя полученные результаты, сформируем и докажем следующую теорему.

Теорема 2. Семейство схем Q-хеширования* является ε-*ASU* – классом.

Доказательство. Распространим утверждение 1 на случай Q-хеширования*.

Схема Q-хеширования* имеет следующее аналитическое выражение:

$h = (s_1 + X_2(s_2 + X_3(s_3 + ..X_\delta(s_\delta + X_{\delta\text{-}1}(P_\delta + 1))\mathrm{Q}\ ))\mathrm{Q}))\mathrm{Q}))\mathrm{Q}.$

При условии, что $s_1 < n$, $s_2 < n$,.., $s_\delta < n$, $X(s_1Q) < n$, $X(s_2Q) < n$,.., $X(s_\delta Q) < n$, решение уравнения (5) существует ровно n раз. Это означает, что множество входных сообщений, как в случае представления двумя скалярами $s_1 < n$, $s_2 < n$, так и в случае $s_1 < n$, $s_2 < n$, … , $s_\delta < n$ отображается в фиксированное множество хеш-кодов, причем вероятность коллизии и в обоих случаях равна $1/n$. Следовательно, для всех $M_1 \neq M_2 \in \sum^n$ и $a \in R$,

$$P_h \in H[h(M_1) - h(M_2) = a] \leq \varepsilon / \left| \mathrm{R} \right|,$$

где $R = n$, а $\varepsilon = C_l^k = \dfrac{l!}{k!(l-k)!}$, где $l = \delta$, а $k = 2$, а в соответствии с определением ε-ASU-класса, семейство схем Q-хеширования* является ε -ASU-классом, что и требовалось доказать.

Отсюда нетрудно получить выражение для ε-ASU класса Q-хеширования*

$$\frac{C_\delta^2}{n} - ASU(n, n^\delta, n),$$

где δ – количество чисел s_i, которыми представлена последовательность M и n – порядок точки кручения эллиптической кривой.

Заключение

Разработан новый метод ключевого хеширования на базе преобразований в группе кручения точек эллиптической кривой, который позволил получить строго универсальные классы хеширования SU и ε-ASU, с размером ключевых данных, не превосходящим размер хешируемых данных. Полученная схема

позволила сократить вычислительную сложность существующих схем на базе RSA-преобразований в 4 раза. Предложенный подход к построению схемы хеширования с помощью секретной базовой точки позволил избежать существующих ограничений в схемах хеширования на базе эллиптических кривых. В дальнейших исследованиях планируется исследовать вычислительную сложность и обеспечиваемую стойкость схемы *Q*-хеширования.

Литература

1. Аволио Ф., Шипли Г. Защита информации на предприятии // Сети и системы связи. – 2000. – № 8 (58). – С. 91 – 99.
2. Шипли Г. Основы безопасности ИТ // Сети и системы связи. – 2003. – № 4. – С. 78 – 82.
3. Сереченко Д. MPLS и безопасность // Сети и системы связи. – 2004. – № 13 (119). – С. 89 – 91.
4. Miller V. Use of elliptic curves in cryptology // Odlizko A.M., editor, Advanced in Cryptology – Crypto′ 86, volume 263 of lecture Notes in Comp. sci. – Springer-Verlag. –1987. – P. 417 – 426.
5. Koblitz N. An Elliptic Curve Implementation of the Finite Field Digital Signature Algorihtm // Advances in Cryptology – Crypto ′98. Lecture Notes in Comp. sci., vol. 1462. – Springer-Verlag. – 1998. – P. 327 – 337.
6. Boneh D., Franklin M. Identity-based encryption from the Weil pairing // Advances in Cryptology, Crypto′ 2001, Lecture Notes in Comp. sci., vol. 2139. – Springer-Verlag. – 2001. – P. 213 – 229.
7. Boneh D. Lynn B., Shacham H. Short signatures from the Weil pairing // In advanced in cryptology. – AsiaCrypt′ 2001, volume 2248 of lecture Notes in Comp. sci. – Springer-Verlag. – 2002. – P. 514 – 532.
8. Ростовцев А.Г., Маховенко Е.Б. Подпись и шифрование на эллиптической кривой: анализ безопасности и безопасная реализация // Проблемы информационной безопасности. Компьютерные системы. – 2003. – № 1. – С. 64 – 73.
9. Barreto P.S.L.M., Kim Y.H., Lynn B., Scott M. Efficient algorithms for pairing-based cryptosystems. In advanced in cryptology - Crypto′ 2002, vol. 2442 of Lecture Notes in Comp. sci. – Springer-Verlag. – 2002. – P. 354 – 368.
10. Menezes A., Okamoto T. and Vanstone P. Reducing elliptic curve logarithms to logarithms in a finite field // IEEE Transactions on Information Theory. – 1993. – 39 (5). – P. 1639 – 1646.
11. Krawczyk H. LFSB-based Hashing and Authenticator // Proceedings of CRYPTO Notes in Comp. sci., vol.839. – Springer-Verlag. – 1994. – P. 129 – 139.
12. Halevi S., Krawczyk H. MMH: Software Message Authentication in the Gbit/second Rates // Extended Abstract. – March, 1997. – P. 1 – 15.
13. Кузнецов А.А., Чевардин В.Е. Метод ключевого хеширования на основе арифметики в группе точек эллиптической кривой // Системи обробки інформації. – Вип. 11 (39) – Х.: ХВУ. – 2004. – С. 108 – 115.
14. Долгов В.И., Федорченко В.Н. О некоторых подходах к построению безусловно стойких кодов аутентификации коротких сообщений // Управление и связь. – Х.: НАНУ, ПАНИ, ХВУ. – 1996. – С. 47 – 51.
15. Silverman J. The Arithmetic of Elliptic Curves // Number 106 in Graduate Texts in Mathematics. – Springer-Verlag. – 1986. – С. 281.
16. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии. – М.: МЭИ, 2000. – 100 с.

Поступила в редакцию 16.08.2005

Рецензент: канд. техн. наук, доцент С.А. Головашич, Харьковский национальный университет радиоэлектроники, Харьков.