УДК 681.3.06

Е.В. КОТУХ

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ С ОГРАНИЧЕНИЕМ ФУНКЦИОНАЛЬНОГО ПОЛЯ АЛГЕБРАИЧЕСКИХ КРИВЫХ

Построение доказуемо стойкой аутентификации на основе универсального хеширования по рациональным функциям алгебраических кривых позволяет разрешить основное противоречие между затратами ключа на аутентификацию, которые определяются размером сообщений и значением вероятности коллизии (обмана), которая определяется пространством хеш кодов. Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на границе Хассе – Вейля [1 – 3]. Вычислительная и алгоритмическая сложность хеширования зависит от размерности проективного пространства представления кривой. Проективное пространство алгебраической кривой определяется базисом линейного векторного пространства Римана – Роха для функционального поля кривой. Существуют три замечательных семейства максимальных кривых, которые связываются с Дэлигнэ – Лустига (Deligne – Lusztig) многообразием размерности $\dim = 1$. Кривая Дэлигнэ – Лустига ассоциируется с проективной специальной линейной группой (кривые Эрмита и кривые которые покрываются кривой Эрмита), с группой Сузуки (Suzuki) $Sz(q)$ (кривые Судзуки) и Ри (Ree) группой $R(q)$ [4]. В работах [3, 5] представлено универсальное хеширование по кривой Судзуки над конечным полем характеристики 2 с нечетной степенью расширения. Кривая Судзуки имеет определение в проективном пространстве P^4 и требует в два раза больше хеш вычислений по сравнению с хешированием по кривым Эрмита в P^2 для квадратичного поля. Актуальной задачей является разработка метода универсального хеширования по алгебраическим кривым с уменьшенной сложностью вычислений.

В данной работе предлагается метод универсального хеширования с ограничением функционального поля алгебраических кривых. С этой целью в разд. 1 приводятся определение и свойства универсального хеширования по рациональным функциям алгебраических кривых. В разд. 2 представлен метод универсального хеширования с ограничением функционального поля алгебраических кривых, коллизионные оценки и оценки сложности хеширования.

1. Определения и свойства универсального хеширования по рациональным функциям алгебраических кривых

Универсальное хеширование по рациональным функциям алгебраической кривой представляется определением 1 [6].

Определение 1. Пусть

χ – абсолютно неразложимая, несингулярная проективная кривая над полем F_q;

$P_1, P_2, ..., P_n$ – точки кривой χ;

P_∞ – точка на бесконечности или особая точка кривой χ;

$f_i \in F_q(\chi) \setminus \{0\}$ – рациональные функции поля рациональных функций кривой χ;

$div_\infty(f_i) = \rho_i$ значение дивизора или порядок полюса рациональной функции f_i в точке P_∞;

$f_i(P_j)$ – значение рациональной функции в точке P_j.

Хеш функция $h_{P_j}(m) \in F_q$ для сообщения $m = (m_1, ..., m_k)$, $m_i \in F_q$ в точке P_j определяется выражением

$$h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i , \qquad (1)$$

где $f_i \in F_q(\chi)$ с упорядоченными порядками полюсов $0 < \rho_1 < \rho_2 < ... < \rho_k$,.

Свойства универсального хеширования по рациональным функциям алгебраических кривых определяются утверждением 1.

Утверждение 1 [6]**.** Хеш функция $h_{P_j}(m)$ определяет универсальный хеш класс $\varepsilon - U(N, q^k, q)$, где N – число точек алгебраической кривой, q^k – объём пространства сообщений, q – объём пространства хеш кодов и вероятность коллизии определяется выражением

$$\varepsilon = \rho_k / N, \tag{2}$$

где ρ_k – значение полюса рациональной функций f_k.

Замечание 1.

1. Параметры универсального хеш класса $\varepsilon - U(N, q^k, q)$ на основе хеширования по рациональным функциям определяются свойствами алгебраической кривой. Подгруппа Вейерштрасса $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < ...\}$ определяется полюсами рациональных функций в особой точке кривой и рациональные функции упорядоченные по значениям полюсов образуют векторное линейное пространство размерности $\dim(L(G)) = \nu_\ell := \#\{(i, j) \in \mathrm{N}^2 : \rho_i + \rho_j = \rho_{\ell+1}\}$.

2. Ключевой параметр хеш функции $h_{P_j}(m)$ определяется вычислением в точке алгебраической кривой.

3. Асимптотическая граница вероятности коллизии для $\varepsilon - U(N, q^k, q)$ хеш класса построенного по рациональным функциям плоских алгебраических кривых рода g над большим алфавитом и фиксированных $k \le g$ и q, имеет вид [8]

$$1 - \frac{q^k(q-1)}{(q^k-1)q} \le P_{кол} \le \varepsilon \le \frac{\sqrt{2k}}{q} + \frac{3\sqrt{2k}}{2q\sqrt{q}}.$$

Верхняя асимптотическая граница вероятности коллизии лучше асимптотической границы для хеширования по алгебраическим кодам и уточняет границу для алгеброгеометрических кодов.

Наилучшие результаты универсального хеширования по соотношению затрат на поле вычислений, размер ключевых данных при фиксированном значении вероятности коллизии достигаются на алгебраических кривых с наибольшим отношением рода g к числу точек.

Главный результат для максимальных кривых Дэлигнэ – Лустига представлен в теоремах 1 и 2.

Теорема 1 [7]. Пусть C кривая над F_q рода g и удовлетворяются следующие условия

1. $g > (\sqrt{q} - 1)^2 / 4$

2. $\#C(F_q) = q + 2g\sqrt{q} + 1$, (то есть C является максимальной над F_q).

Тогда X является F_q изоморфной кривой Эрмита над F_q и её род $g = \sqrt{q}(\sqrt{q} - 1)/2$.

Теорема 2 [8]. Для положительного целого s заданы $q = 2q_0^2$ и $q_0 = 2^s$. Пусть X кривая над F_q рода g и удовлетворяются следующие условия:

1. $g = q_0(q - 1)$;

2. $\#X(F_q) = q^2 + 1$.

Тогда X является F_q изоморфной кривой Дэлигнэ-Лустига ассоциированной с группой Судзуки $Sz(q)$.

Размерность функционального поля кривой Эрмита определяется леммой 1.

Лемма 1. Пусть P есть рациональная точка на кривой Эрмита над полем F_q, $q = l^2$. Тогда подгруппа Вейерштрасса $H(P) = \langle l, l+1 \rangle$. Кривая Эрмита является максимальной и определяется линейной серией размерности $\dim = 2$.

Результаты по максимальным плоским кривым в конечном поле F_q, $q = l^2$ представлены в таблице.

Уравнение кривой $C(F_{l^2})$	Значение рода кривой	Полюса рациональных функций	Значение подгруппы Вейерштрасса
$y^l + y = x^{l+1}$	$g_1 = l(l-1)/2$	$(x)_\infty = l, (y)_\infty = l+1$	$\langle l, l+1 \rangle$
$y^l + y = x^{(l+1)/2}$, l нечетное	$g_2 = l(l-1)^2/4$	$(x)_\infty = l, (y)_\infty = (l+1)/2$	$\langle (l+1)/2, l \rangle$
$\sum_{i=1}^{t} y^{l/2^t} = x^{l+1}, l = 2^t$	$g_2' = l(l-2)/4$	$(x)_\infty = l/2, (y)_\infty = l+1$	$\langle l/2, l+1 \rangle$
$y^l + y = x^{(l+1)/3}, l \equiv 2(\mathrm{mod}\ 3)$	$g_3' = (l^2 - 3l + 2)/6$	$(x)_\infty = (l+1)/3, (y)_\infty = l$	$\langle (l+1)/3, l \rangle$
$\sum_{i=0}^{t-1} y^{3^t} = \omega x^{l+1}, l = 3^t,$ $\omega \in F_{l^2}, \omega^{l-1} = -1$	$g_3'' = l(l-3)/6$	$(x)_\infty = l/3, (y)_\infty = l+1$	$\langle l/3, l+1 \rangle$ $\langle 2(l+1)/3, l, l+1 \rangle$
$x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0,$ $l \equiv 2(\mathrm{mod}3)$	$g_3 = (l^2 - l + 4)/6$	$(x)_\infty = l+1, (y)_\infty = (l+1)/3,$ $(v)_\infty = l$	$\langle 2(l+1)/3, l, l+1 \rangle$
$\omega x^{(l-1)/3} - y x^{2(l-1)/3} + y^l = 0,$ $\omega \in F_{l^2}, \omega^{l-1} = -1, l \equiv 2(\mathrm{mod}3)$	$g_3' = l(l-1)/6$	$(x)_\infty = l, (y)_\infty = (l-1)/3,$ $(v)_\infty = l+1$	$\langle 2(l-1)/3, l, l+1 \rangle$
$y^l + y = (\sum_i^t x^{l/3^i})^2, l = 3^t$	$g_3' = l(l-1)/6$,	$(x)_\infty = l, (y)_\infty = 2l/3,$ $(v)_\infty = l+1$	$\langle 2l/3, l, l+1 \rangle$
$x^{2(l+1)/3} y^{(l+1)/3} + y^{2(l+1)/3} + x^{(l+1)/3} = 0$	$g_3 = (l^2 - l + 4)/6$		$\langle 2(l+1)/3, l, l+1 \rangle$

Замечание 2.

1. Алгебраические кривые $y^l + y = x^{l+1}$, $y^l + y = x^{(l+1)/2}$ и $\sum_{i=1}^{t} y^{l/2^t} = x^{l+1}, l = 2^t$ являются максимальными кривыми первого и второго рода, имеют подгруппу Вейерштрасса $H(P_\infty) = \langle \rho_1, \rho_2 \rangle$ размерности $\dim = 2$ и функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

2. Алгебраические кривые $y^l + y = x^{(l+1)/3}, l \equiv 2(\mathrm{mod}\ 3)$ и $\sum_{i=0}^{t-1} y^{3^t} = \omega x^{l+1}, l = 3^t, \omega \in F_{l^2}, \omega^{l-1} = -1$ являются максимальными кривыми третьего рода, имеют подгруппу Вейерштрасса $H(P_\infty) = \langle \rho_1, \rho_2 \rangle$ размерности $\dim = 2$ и функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

3. Максимальные кривые вида:

- $x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0, l \equiv 2(\mathrm{mod}\ 3)$,
- $\omega x^{(l-1)/3} - y x^{2(l-1)/3} + y^l = 0, \omega \in F_{l^2}, \omega^{l-1} = -1, l \equiv 2(\mathrm{mod}3)$,
- $y^l + y = (\sum_i^t x^{l/3^i})^2, l = 3^t$

имеют подгруппу Вейерштрасса $H(P_\infty)$ размерности $\dim = 3$ и функциональное поле определяется рациональными функциями вида $\{x^i \cdot y^j \cdot v^t\}$.

Кривая Дэлигнэ-Лустига, ассоциированная с группой Судзуки, определяется полной линейной серией $D = \left|(q + 2q_0 + 1)P_0\right|$ размерности $\dim = 4$ и степени $q + 2q_0 + 1$, которая выводится из энумератора зета функции. Кривая Судзуки имеет отображение на проективное пространство P^4 и подгруппу Вейерштрасса $H(P) = \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1\rangle$, $P \in X(F_q)$ [8].

Таким образом, практические алгоритмы вычисления хеш функций определяются многопараметрическими схемами вычисления по базису векторного пространства функционального поля алгебраической кривой. Сложность вычисления хеш функции определяется размерностью базисного пространства рациональных функций функционального поля. Так хеширование по кривым Судзуки над четырех мерным базисом в случае оптимизации вычислений по схеме Горнера в два раза сложнее чем хеширование по кривой Эрмита над двумерным базисом [3]. Ограничение функционального поля кривых приводит к уменьшению сложности вычислений.

2. Метод универсального хеширования с ограничением функционального поля алгебраических кривых

Определение 2. Пусть χ – абсолютно неразложимая, несингулярная проективная кривая над полем F_q с точками $P_1, P_2, ..., P_n$, особой точкой (точкой на бесконечности) P_∞ и функциональным полем $F_q(\chi) \setminus \{0\}$. Хеш функция $h_{P_j}(m)$ над конечным полем F_q для сообщения $m = (m_1, ..., m_k)$, $m_i \in F_q$ в точке P_j кривой χ определяется выражением

$$h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i , \qquad (3)$$

где $f_i \in G_q(\chi)$ – рациональные функции подмножества функционального поля $G_q(\chi) \in F_q(\chi) \setminus \{0\}$ с упорядоченными порядками полюсов $0 < \rho_1 < \rho_2 < ... < \rho_k$, $\rho_i = div_\infty(f_i)$ значение дивизора или порядок полюса рациональной функции в точке P_∞.

Замечание 3.

1. Метод универсального хеширования с ограничением функционального поля алгебраических кривых предусматривает следующий порядок действий:

- задание алгебраической кривой χ над полем F_q, вычисление точек кривой $P_1, P_2, ..., P_n$;
- вычисление функционального поля $F_q(\chi) \setminus \{0\}$ ассоциированного с алгебраической кривой χ;
- ограничение функционального поля подмножеством рациональных функций $f_i \in G_q(\chi)$ с упорядоченными порядками полюсов;
- построение алгоритма вычисления хеш функции на ограниченном подмножестве рациональных функций.

2. Ограничение функционального поля алгебраических кривых определяется решением задачи минимизации сложности вычислений при хешировании заданного числа слов данных и заданной вероятности коллизии за счет оптимизации выбора базисных функций и размерности функционального пространства.

Рассмотрим решение задачи оптимизации выбора базисных функций и размерности функционального пространства для хеширования по полю рациональных функций кривой Судзуки.

Утверждение 2. Универсальное хеширование по кривой Судзуки над F_q, $q = 2q_0^2$, $q_0 = 2^s$ с ограничением функционального поля в базисе линейного пространства $L(mP_\infty) = L(\rho_l P_\infty)$, $\rho_l \le m \le \rho_{l+1}$ рациональных функций $\{x^i \cdot y^j : iq + j(q + 2q_0) \le m\}$ определяет $U(q^2, q^k, q)$ семейство хеш функций с вероятностью коллизии

$$\varepsilon = k/(2qq_0) + s/q - s(s-1)/(4qq_0), \text{ если } \rho_{\mathrm{k}} \le 2q_0(q-1) \tag{4}$$

и сложностью хеширования

$$N_{xy} = k + s \tag{5}$$

где k – число слов данных, $s = \left| (2k + 1/4)^{1/2} - 1/2 \right|$, $\lceil \cdot \rceil$ округление к большему целому числу.

Доказательство. Кривые Судзуки S являются F_q изоморфными плоской кривой $Y^q Z^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1} Z^{q+q_0-1}$, где $q = 2q_0^2$ и $q_0 = 2^s$. Род кривой $g = q_0(q-1)$ и число F_q рациональных точек равно $q^2 + 1$. Точками кривой являются особая точка на бесконечности $P_0 = (0:1:0)$ кратности q_0 и рациональные точки $P_{a,b} = (a:b:1)$, где $a, b \in F_{q^2}$ и $b^q - b = a^{q_0}(a^q - a)$. Подгруппа Вейерштрасса функционального поля кривой содержит подгруппу $H(P_\infty) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle$. Базис пространства $L(\rho_\ell P_0)$, задается функциями вида $\{w^j \cdot v^i \cdot y^t \cdot x^r : i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + r \cdot q \le \rho_\ell\}$, что следует из подгруппы Вейерштрасса $H(P_0)$ представленной порядками полюсов функций $x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$. Порядки полюсов равны $div_\infty(x) = qP_0$, $div_\infty(y) = (q+q_0)P_0$, $div_\infty(v) = (q+2q_0)P_0$, $div_\infty(w) = (q+2q_0+1)P_0$.

Хеш функция $h_{x,y}(m) \in F_q$, для сообщения m по рациональным функциям кривой Судзуки в точке x, y определяется выражением

$$h_{x,y}(m) = \sum m_{i,j,t,r} \cdot w^j \cdot v^i \cdot y^t \cdot x^r,$$

где $m_{i,j,t,r} \in F_q$ – слова сообщения m, $i \ge 0$, $0 \le j \le 2q_0 - 1$, $0 \le t \le 1$, $0 \le r \le q_0$, $i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + rq \le \rho_k$, $x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$, ρ_k полюс подгруппы Вейерштрасса $H(P_\infty)$ [3].

Кривая Судзуки при отображении на проективное пространство P^4 представляется точками вида $P_{(a,b)} := (1:a:b:f(a,b):af(a,b)+b^2) \bigcup \pi(P_0) = (0:0:0:0:1)$, где $a, b \in F_q$ и $f(a,b) := a^{2q_0+1} + b^{2q_0}$.

Пусть $L(\rho_\ell P_0)$ определяется базисными функциями $\{x^i \cdot y^j : i \cdot q + j(q+q_0) \le \rho_\ell\}$. Для линейного пространства $L(\rho_\ell P_0)$, построенного по полному функциональному базису кривой Судзуки, имеем

$$\rho_{g+1} = 2g = 2q_0(q-1) = q + (2q_0 - 2)(q+q_0), \tag{6}$$

где g – род кривой.

Из условия (6) следует, что $i + j \le 2q_0 - 1$ и получим вычисление хеш кода по двух параметрической схеме Горнера эквивалентной схеме вычисления по кривой Эрмита

$$h_{x,y}(m) = \sum_{j=0}^{s} y^j \cdot \sum_{i=0}^{s-j} m_{i,j} \cdot x^i,$$

где $s = \left| (2k + 1/4)^{1/2} - 1/2 \right|$ – параметр от k слов данных (лемма 1 [9]).

Множество ключей определяется пространством значений x, y. Универсальное хеширование выполняется по базису $\{x^i \cdot y^j : i \cdot q + j(q + q_0) \le \rho_k\}$. Таким образом получим $U(q^2, q^k, q)$ семейство хеш функций и вероятность коллизии $\varepsilon = \rho_k / N = \rho_k / q^2$. Нетрудно показать (см. лемма 1 [9]), что $j = k - s(s-1)/2$, $i = s - j$ и $s = \left| (2k + 1/4)^{1/2} - 1/2 \right|$ при $\rho_{\text{k}} \le \rho_{g+1}$, где $\lceil \cdot \rceil$ округление к большему целому числу. Подставим соотношения i, j, s в выражение для ε и получим

$$\varepsilon = \rho_k / q^2 = (i \cdot q + j(q + q_0)) / q^2 = k/(2qq_0) + s/q - s(s-1)/(4qq_0). \qquad (7)$$

Оценка сложности универсального хеширования по базису x, y следует из оценки сложности универсального хеширования по двух параметрической схеме Горнера для кривой Эрмита (предложение 2 [9])

$$N_{xy} = k + s, \text{ если } \rho_{\text{k}} \le \rho_{g+1}, \qquad (8)$$

где $s = \left| (2k + 1/4)^{1/2} - 1/2 \right|$.

Следствие 1. Асимптотическая оценка вероятности коллизии универсального хеширования по кривой Судзуки имеет вид

$$\varepsilon \approx 1/q_0, \text{ если } k \le (2q_0 - 1)(q_0 + 1). \qquad (9)$$

Доказательство. Число хешируемых слов данных определяется числом полюсов подгруппы Вейерштрасса $\rho_{\text{k}} \le \rho_{g+1}$. Число пар $i + j \le 2q_0 - 1$ определяется как сумма арифметического ряда вида

$$k_{xy} = 1 + 2 + ... + (2q_0 - 1) + 2q_0 - 1 = (2q_0 - 1)(q_0 + 1). \qquad (10)$$

Коэффициенты i, j в (7) для $k_{xy} = (2q_0 - 1)(q_0 + 1)$ слов данных имеют значения $i = 1$, $j = 2q_0 - 2$. Окончательно получим

$$\varepsilon = \rho_k / q^2 = (q + (2q_0 - 2)(q + q_0)) / q^2 = (2q_0 - 1)/q + 1 - 2/q^2 \approx 1/q_0. \quad \Diamond$$

Замечание 2.

1. Оценка вероятности коллизии хеширования по кривой Судзуки при полном функциональном базисе для $k_{xy} = (2q_0 - 1)(q_0 + 1)$ имеет вид (см. замечание 1 [3])

$$\varepsilon = (3k_{xy})^{1/3} / q^2 = ((2q_0 - 1)(q_0 + 1))^{1/3} (q + q_0) / q^2 \approx 1.6/(q_0 q_0^{1/3}). \qquad (11)$$

Сравнение с асимптотической оценкой (9) показывает, что хеширование по двух параметрическому базису кривой Судзуки в $q_0^{1/3}$ раз проигрывает по вероятности коллизии.

2. Сложность универсального хеширования по кривым Судзуки в полном функциональном базисе определяется выражением (см. предложение [5])

$$N_{xyvw} = k + s^3/3 + s^2/2 + 2s - 1, \text{ если } s \le q_0, \qquad (12)$$

$$N_{xyvw} = k + q_0^{\,3}/3 + q_0^{\,2}/2 + (s - q_0)(2q_0 - 1) + 2s - 1, \text{ если } s > q_0, \qquad (13)$$

где $s = (3k)^{1/3}$.

Асимптотика оценки сложности универсального хеширования по кривым Судзуки следует из (12). При $s = (3k)^{1/3}$ и $s \le q_0$ получим

$$N_{xyvw} = 2k + (3\text{k})^{2/3}/2 + 2(3\text{k})^{1/3} - 1.$$

Сравнение с (8) показывает, что универсальное хеширование по базису двух рациональных функций в два раза выигрывает по сложности вычислений.

3. Зафиксируем вероятность коллизии значением $\varepsilon = \rho_{g+1} / N = 2g / q^2$. Для условия $\rho_{\text{k}} = \rho_{g+1}$ Число слов данных при хешировании по полному функциональному базису определяется родом кривой

$$k_{xyvw} = qq_0 - q_0 + 1. \qquad (14)$$

При хешировании по двух параметрическому базису функционального поля кривой Судзуки наибольшее число слов данных $\rho_{\text{k}} \le \rho_{g+1}$ определяется соотношением (5)

$$k_{xy} = (2q_0 - 1)(q_0 + 1). \qquad (15)$$

Отношение числа хешируемых слов данных при двух параметрическом хешировании к хешированию по полному базису равно

$$R = k_{xy} / k_{xyvw} = (2q_0 - 1)(q_0 + 1) / (qq_0 - q_0 + 1) \approx 1 / q_0 \qquad (16)$$

и определяет проигрыш двух параметрического хеширования при фиксированной вероятности коллизии.

Выводы

1. Универсальное хеширование с ограничением функционального поля алгебраической кривой приводит к существенному снижению сложности вычислений. При этом уменьшается число хешируемых данных. Требуется оптимизация базиса функционального поля. Эффект достигается на сложных многопараметрических кривых.

2. Уменьшение размерности функционального поля алгебраической кривой при рациональном выборе базисных функций приводит к схемам хеширования, которые вкладываются в хеширование по наилучшим плоским кривым. Так двух параметрическое хеширование по кривой Судзуки по алгоритму вычисления, асимптотическим оценкам хеширования приводит к определению хеширования по кривой Эрмита. Можно показать, что хеширование по одной базисной функции приводит к хеш функции по проективной прямой.

3. Предложен метод универсального хеширования с ограничением функционального поля алгебраической кривой, который является дальнейшим развитием метода универсального хеширования на основе скалярного произведения по рациональным функциям линейного базисного пространства и отличается от известного вычислением хеш функций по подмножеству рациональных функций функционального поля с упорядоченными порядками полюсов.

Список литературы: 1. *Халимов, Г.З.* Аутентификация с применением Эрмитовых кодов / Г.З. Халимов, А.Ю. Иохов // Вестник ХПИ. – Х., 2005. – Вып. 9. – С. 26-32. 2. *Халимов, Г.З.* Универсальное хеширование по максимальным кривым Гурвица / Г.З. Халимов // Прикладная радиоэлектроника. – 2010. – Т.9, № 3. – С.365-370. 3. *Халимов, Г.З.* Универсальное хеширование по кривым Сузуки / Г.З.Халимов, Е.В.Котух // Прикладная радиоэлектроника. –2011. – Т. 10, № 2. –С.164-170. 4. *Deligne, P.* Representations of reductive groups over finite fields / P.Deligne, Lusztig // Annatatsiya of Mathematics. – 1976. – N.103. – P.103–161. 5. *Халимов, Г.З.* Алгоритм универсального хеширования по кривой Сузуки / Г.З.Халимов, Е.В.Котух // Восточно-Европейский журнал передовых технологий. – 2011. – № 3/9 (51). – С.10-16. 6. *Халимов, Г.З.* Оценка параметров кривых Ферма для универсального хеширования в простом поле / Г.З.Халимов // Науч.-техн. конф. с междунар. участием. Компьютерное моделирование в наукоемких технологиях (часть 2). КМНТ Харьков, 18-21 мая 2010. – С.266. 7. *Fuhrmann, R.* The genus of curves over finite fields with many rational points / R.Fuhrmann, F.Torres // Manuscripta Mathematics. – 1996. – N.89. – P.103–106. 8. *Torres, F.* The Deligne-Lusztig curve associated to the Suzuki group [Электронный ресурс]/ F.Torres // arXiv:alg-geom/9706012v1 26 June 1997. 9. *Халимов, Г.З.* Универсальное хеширование по рациональным функциям кривой Эрмита / Г.З.Халимов, А.Ю.Иохов // Междунар. науч.-практ. конф. «Застосування інформаційніх технологій у підготовці та діяльності сил охорони правопорядку». Академія внутрішніх військ МВС України 17-18.03.2011. Зб. тез доповідей. – 2011. – С.48-51.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 15.09.2012