УДК 681.3.06

ОЦЕНКИ СЛОЖНОСТИ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ ПО АЛГЕБРАИЧЕСКИМ КРИВЫМ

Г.З. ХАЛИМОВ

Представлены результаты универсального хеширования по алгебраическим кривым. Получены решения для вычисления точек наилучших кривых по ключевым данным, оценки сложности вычислений, практические рекомендации применения алгебраических кривых для универсального хеширования.

Ключевые слова: универсальное хеширование, максимальные кривые.

Универсальное хеширование по алгебраическим кривым предложено в работе [1]. Наилучший результат по коллизионным оценкам достигается на максимальных кривых [2, 3]. Проблематика практической реализации универсального хеширования на основе скалярного произведения по рациональным функциям алгебраических кривых определяется сложностью построения точек алгебраических кривых по ключевым данным. Вычислительные затраты на хеширование зависят от размерности функционального поля рациональных функций. Основное противоречие универсального хеширования по алгебраическим кривым состоит в том, что для обеспечения гарантированной вероятности обмана на нижнем уровне, необходимо построить вычисления по рациональным функциям алгебраических кривых с как можно меньшим отношением значения максимального полюса рациональных функций к числу точек кривой для фиксированной длины данных. Применение максимальных кривых большого рода приводит к увеличению размерности функционального поля ассоциированного с кривой и росту сложности вычислений.

Целью статьи является оценка сложности универсального хеширования по алгебраическим кривым. В разделе 1 представлено универсальное хеширование по алгебраическим кривым. В разделе 2 приводятся наилучшие результаты универсального хеширования по максимальным кривым. В разделе 3 получены оценки сложности вычисления точек алгебраических кривых по ключевым даням.

1. УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ В ПОЛЕ РАЦИОНАЛЬНЫХ ФУНКЦИЙ

Универсальное хеширование в поле рациональных функций по точкам алгебраической кривой впервые обосновано Биербрауэром [1]. Интерпретация алгеброгеометрического подхода представлена в работах [4, 5].

Определение 1[6]. 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

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

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[4]. 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

$$\varepsilon = \rho_k / N ,$$

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 $\dim(L(G) = \nu_\ell := \{(i, j) \in N^2 : \rho_i + \rho_j = \rho_{\ell+1}\}$.

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

Интерес представляют алгебраические кривые с как можно большим отношением числа точек кривой к её роду, определенные над конечным полем F_q.

Пусть $N_q(g)$ обозначает максимальное число F_q рациональных точек, которое кривая рода

g может иметь. Кривая C рода g является оптимальной над F_q, если её число F_q рациональных точек $\#C(F_q)$ равно $N_q(g)$. Главный результат для теории определяется теоремой Хассе-Вейля.

Теорема 1 [7]. Пусть C — проективная и несингулярная, абсолютно неразложимая кривая, определенная над конечным полем F_q с q элементами. Тогда число F_q рациональных точек кривой определяется неравенством

$$N_q(g) \le 1 + q + 2\sqrt{q}g(C).$$

Для максимальных кривых над конечным полем достигается максимальное отношение числа точек кривой к роду. Основные асимптотические результаты для кривых следующие.

Пусть $N_q(g) = \max_C \#C(F_q)$ — число точек кривой C над F_q, где C пробегает все кривые рода $g(C) = g$. Асимптотическая оценка имеет вид

$$A(q) = \limsup_{g\to\infty} N_q(g)/g.$$

Используя верхнюю границу для $N_q(g) \le q + 1 + \frac{1}{2}\sqrt{(8q+1)g + 4(q^2-q)g} - g$, граница для $A(q)$ впервые была получена Ihara Y. [8]

$$A(q) \le \frac{1}{2}(\sqrt{8q+1} - 1).$$

Отметим, что из границы Хассе-Вейля прямо следует

$$A(q) \le 2\sqrt{q}.$$

Если $g > \sqrt{q}(\sqrt{q}-1)/2$, $N_q(g)$ лежит ниже границы Хассе-Вейля.

Основываясь на идее Ihara Y., Дринфельд и Влэдуц показали [9], что

$$A(q) \le \sqrt{q} - 1$$

и в случае $q = l^2$ на модулярных кривых следует равенство $A(l^2) = l - 1$.

Известна также нижняя граница Цинка для оценки $A(q^3) \ge \frac{2(q^2-1)}{q+2}$ [10].

Замечание 2. Для криптографических применений интерес представляют алгебраические кривые, определенные над конечным полем F_q с как можно большим отношением числа точек кривой к её роду.

Наилучший результат универсального хеширования достигается на максимальных кривых.

2. УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО МАКСИМАЛЬНЫМ КРИВЫМ

Главный результат для максимальных кривых представлен в теоремах 2 и 3. В таблице 1 представлены максимальные кривые над полем F_{l^2}.

Теорема 2 [11]. Пусть C кривая над F_q рода g и удовлетворяются следующие условия

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

2. $\#C(F_q) = q + 2g\sqrt{q} + 1$, ($C$ 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 3 [12]. 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 — 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 табл. 1.

Замечание 3.

1. Алгебраические кривые:

$$y^l + y = x^{l+1},$$
$$y^l + y = x^{(l+1)/2},$$
$$\sum_{i=1}^{t} y^{l/2^i} = x^{l+1},\ l = 2^t$$

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:

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

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:

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

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

4. Кривая Дэлигнэ-Лустига, ассоциированная с группой Судзуки, определяется полной линейной серией $D = |(q + 2q_0 + 1)P_0|$ размерности $\dim = 4$ и степени $q + 2q_0 + 1$, которая выводится из энумератора зета функции. Кривая

Таблица 1

Максимальные кривые над квадратичным полем F_{l^2}

Уравнение кривой $C(F_{l^2})$	Значение рода кривой	Ограничения на коэффициенты кривой	Значение подгруппы Вейерштрасса
$y^l + y = x^{l+1}$	$g_1 = l(l-1)/2$		$\langle l, l+1\rangle$
$y^l + y = x^{(l+1)/2}$	$g_2 = (l-1)^2/4$	l нечетное	$\langle (l+1)/2, l\rangle$
$\sum_{i=1}^{t} y^{l/2^i} = x^{l+1}$	$g'_2 = l(l-2)/4$	$l = 2^t$	$\langle l/2, l+1\rangle$
$y^l + y = x^{(l+1)/3}$	$g'_3 = (l^2 - 3l + 2)/6$	$l \equiv 2 \pmod 3$	$\langle (l+1)/3, l\rangle$
$\sum_{i=0}^{t-1} y^{3^i} = \omega x^{l+1}$	$g_3'' = l(l-3)/6$	$l = 3^t$, $\omega \in F_{l^2}$, $\omega^{l-1} = -1$	$\langle l/3, l+1\rangle$
$x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0$	$g_3 = (l^2 - l + 4)/6$	$l \equiv 2 \pmod 3$	$\langle 2(l+1)/3, l, l+1\rangle$
$\omega x^{(l-1)/3} - y x^{2(l-1)/3} + y^l = 0$	$g_3''' = l(l-1)/6$	$l \equiv 1 \pmod 3$, $\omega \in F_{l^2}$, $\omega^{l-1} = -1$	$\langle (2l-1)/3, l, l+1\rangle$
$y^l + y = \left(\sum_i^t x^{l/3^i}\right)^2$	$g_3''' = l(l-1)/6$	$l = 3^t$	$\langle 2l/3, l, l+1\rangle$
$x^{2(l+1)/3} y^{(l+1)/3} + y^{2(l+1)/3} + x^{(l+1)/3} = 0$	$g_3 = (l^2 - l + 4)/6$	$l \equiv 2 \pmod 3$	$\langle (2l+1)/3, l, l+1\rangle$

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].

Кривая Судзуки имеет представление

$$y^q - y = x^{q_0}(x^q - x),$$

определена над полем F_q, $q = 2q_0^2$, $q_0 = 2^s$, рода $g = q_0(q-1)$ и имеет число точек $N = q^2 + 1$.

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 $a, b \in F_q$ и $b^q - b = a^{q_0}(a^q - a)$.

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

$$div_\infty(x) = qP_0,\ div_\infty(y) = (q+q_0)P_0,$$
$$div_\infty(v) = (q+2q_0)P_0,\ div_\infty(w) = (q+2q_0+1)P_0.$$

Кривая Судзуки представляется в P^4 множеством точек вида

$$P(a,b) := (1:a:b:f(a,b):af(a,b)+b^2)$$
$$\cup\pi(P_0) = (0:0:0:0:1),$$

где $a, b \in F_q$ и $f(a,b) := a^{2q_0+1} + b^{2q_0}$.

5. Кривая Ферма вида

$$x^{(q-1)/3} + y^{(q-1)/3} + z^{(q-1)/3} = 0$$

над F_q, $q \equiv 1 \pmod 3$, является одной из лучших плоских кривых с большим числом точек

$$N = 2(q-1)^2/9.$$

3. ОЦЕНКИ СЛОЖНОСТИ ВЫЧИСЛЕНИЯ ТОЧЕК АЛГЕБРАИЧЕСКИХ КРИВЫХ ПО КЛЮЧЕВЫМ ДАННЫМ

Важный фактор практической реализации хеширования по точкам кривой состоит в вычислении точек кривой по ключевым данным.

Оценки сложности вычисления точек алгебраических кривых над полем F_q представлены в табл. 2.

Замечание 4.

1. Для хеширования над конечным полем F_q по проективной прямой значение ключа может быть прямо отождествлено с элементом поля $\alpha \in F_q$.

2. При хешировании по кривой Сузуки, как следует из уравнения $b^q - b = a^{q_0}(a^q - a)$ значения точки $P_{a,b} = (a:b:1)$, $a, b \in F_q$, могут быть выбраны независимо. Ограничения на выбор a и b определяются тем, что по алгоритму хеширования рациональные функции функционального поля кривой не должны равняться 0, т.е. $a \ne 0$, $b \ne 0$, $a^{2q_0+1} + b^{2q_0} \ne 0$, $ab^{2q_0} + a^{2q+2q_0} + b^{2q_0} \ne 0$, что уменьшает ключевое пространство до $q^2 - 4q$. Назначение $a \ne 0$, $b \ne 0$ по ключу потребует проверок $a^{2q_0+1} + b^{2q_0} \ne 0$, $ab^{2q_0} + a^{2q+2q_0} + b^{2q_0} \ne 0$. Вероятность успеха при случайном задании a и b, $a, b \in F_q$ будет определяться соотношением

$$\Pr = \left|\left\{P(a:b:1), a^{2q_0+1} + b^{2q_0} \ne 0, ab^{2q_0} + a^{2q_0+2} + b^{2q} \ne 0\right\}\right| / \left|\left\{P(a:b:1), a \ne 0, b \ne 0\right\}\right| =$$
$$(q^2 - 4q)/(q-1)^2 \approx 1 - 4/q.$$

3. Кривая Ферма $x^{(q-1)/3} + y^{(q-1)/3} + z^{(q-1)/3} = 0$ имеет большое число точек $N = 2(q-1)^2/9$ и

Таблица 2

Оценки сложности вычисления точек алгебраических кривых над полем F_q

Уравнение кривой	Число точек кривой N над полем F_q	Вычисление точек кривой $P_{a,b}=(a:b:1)$, $a,b\in F_q$	Вероятность успеха определения точки кривой
Проективная прямая	q	$a\neq 0$	1
Кривая Эрмита $y^{\sqrt{q}}+y=x^{\sqrt{q}+1}$	$q\sqrt{q}$	$b^{\sqrt{q}}+b=a^{\sqrt{q}+1}$, $a\neq 0$, $b\neq 0$, $b=\alpha^{i\cdot(q-1)+j}$, $a=\alpha^{s+t(q-1)}$, $i=\overline{0,\sqrt{q}}$, $j=\overline{0,\sqrt{q}-2}$ $t=\overline{0,\sqrt{q}}$, $\alpha^{s\cdot(\sqrt{q}+1)}=tr(b)$, $\alpha\in F_q$	$1/\sqrt{q}$
Максимальные кривые второго рода $y^{\sqrt{q}}+y=x^{(\sqrt{q}+1)/2}$	$(q-1)\sqrt{q}/2+\sqrt{q}+1$	$b^{\sqrt{q}}+b=a^{(\sqrt{q}+1)/2}$, $a\neq 0$, $b\neq 0$ $b=\alpha^{i\cdot(\sqrt{q}-1)+j}$, $a=\alpha^{2s+2t(\sqrt{q}-1)}$, $i=\overline{0,\sqrt{q}}$, $j=\overline{0,\sqrt{q}-2}$, $t=\overline{0,(\sqrt{q}+1)/2-1}$, $\alpha^{s(\sqrt{q}+1)}=tr(b)$, $\alpha\in F_q$	$1/2\sqrt{q}$
Максимальные кривые третьего рода $y^{\sqrt{q}}+y=x^{(\sqrt{q}+1)/3}$	$(q-1)\sqrt{q}/3+\sqrt{q}+1$	$b^{\sqrt{q}}+b=a^{(\sqrt{q}+1)/3}$, $a\neq 0$, $b\neq 0$ $b=\alpha^{i\cdot(\sqrt{q}-1)+j}$, $a=\alpha^{3s+3t(\sqrt{q}-1)}$, $i=\overline{0,\sqrt{q}}$, $j=\overline{0,\sqrt{q}-2}$, $t=\overline{0,(\sqrt{q}+1)/3-1}$, $\alpha^{s\cdot(\sqrt{q}+1)}=tr(b)$, $\alpha\in F_q$	$1/3\sqrt{q}$
Кривая Ферма $x^{(q-1)/3}+y^{(q-1)/3}+1=0$	$2(q-1)^2/9$	$a^{(q-1)/3}+b^{(q-1)/3}+1=0$, $a\neq 0$, $b\neq 0$,	2/9
Кривая Сузуки $y^q-y=x^{q_0}(x^q-x)$	q^2-4q	$b^q-b=a^{q_0}(a^q-a)$, $a\neq 0$, $b\neq 0$, $a^{2q_0+1}+b^{2q_0}\neq 0$, $ab^{2q_0}+a^{2q+2q_0}+b^{2q}\neq 0$	$1-4/q$

значения координат $P_{a,b}(a:b:1)$ могут быть выбраны независимо. Ограничения на выбор $a\neq 0$ и $b\neq 0$ определяются алгоритмом хеширования по рациональным функциям функционального поля кривой. Вероятность успеха при случайном выборе a и b, $a,b\in F_q$ по ключевому слову будет определяться выражением

$$\Pr=(2(q^2-1)/9-2(q-1)/3))/$$
$$(q-1)^2\approx 2/9-2/(3(q-1))\approx 2/9.$$

4. Кривая Гурвица

$$x^{2(q-1)/3}y^{(q-1)/3}+y^{2(q-1)/3}+x^{(q-1)/3}=0$$

имеет большее число точек $N=2(q-1)^2/3$. Вероятность успеха выбора точки $P_{a,b}(a:b:1)$ по ключу будет выше и равна $\Pr\approx 2/3$.

5. Точка хеширования $P_{a,b}(a:b:1)$ по кривой Эрмита определяется решением уравнения $b^{\sqrt{q}}+b=a^{\sqrt{q}+1}$, $a\neq 0$, $b\neq 0$.

Утверждение 2. Вычисление точки хеширования по кривой Эрмита определяется задачей дискретного логарифма.

Действительно $b^{\sqrt{q}}+b=tr(b)=c$, $b\in F_q$ и $c\in F_{\sqrt{q}}$. Пусть α — образующий элемент F_q и $\gamma=\alpha^{\sqrt{q}+1}$ является образующим элементом $F_{\sqrt{q}}$. Тогда $c=\gamma^s$ и $a=\alpha^s$. Решение уравнения $c=\gamma^s$ относительно показателя s имеет сложность задачи дискретного логарифма. Для переборного метода вероятность нахождения решения имеет оценку $\Pr\approx 1/\sqrt{q}$.

6. Максимальные кривые второго и третьего рода имеют в 2 и 3 раза меньше точек по сравнению с кривой Эрмита. Вычисление точек хеширования $P_{a,b}(a:b:1)$ по ключевым данным определяется задачей дискретного логарифма. Просто показать, что оценки для вероятности нахождения решения имеют значения $1/(2\sqrt{q})$ и $1/(3\sqrt{q})$ соответственно.

ВЫВОДЫ

1. Построение хеширования по алгебраическим кривым определяется вычислением точки кривой по ключевым данным. Наилучший результат достигается на плоских кривых Ферма и Гурвица с большим числом точек. Применение кривых Ферма и Гурвица снимает практическое ограничение на поле вычисления точек кривых, число точек кривых практически равняется размерности конечного поля и назначение по ключевым данным точки кривой реализуется с вероятностью близкой к единице.

2. Назначение точек кривой Судзуки по ключу имеет наибольшую вероятность успеха, требует дополнительных проверок и имеет ограничение на поле вычислений. Кривые Судзуки имеют представление в поле характеристики 2 с нечетной степенью расширения.

3. Максимальные кривые Эрмита, кривые второго и третьего рода имеют определение над квадратичным полем, наилучшие оценки вероятности коллизии для плоских алгебраических кривых, но задача вычисления значений точек кривых по ключевым данным имеет сложность решения задачи дискретного логарифма.

Литература

[1] Bierbrauer J. Authentication via algebraic-geometric codes. / Bierbrauer J. // URL http://www.math.mtu.edu/~jbierbra/ potpap.ps.

[2] Халимов Г.З. Аутентификация с применением Эрмитовых кодов. / Халимов Г.З., Иохов А.Ю. // Вестник ХПИ. – Х.: Вып. 9. – 2005. – С. 26–32.

[3] Халимов Г.З. Универсальное хеширование по максимальным кривым / Г.З.Халимов //XIII Международная научно-практическая конференция ”Безопасность информации в информационно-телекомуникационных системах”, Киев, 18-21 мая: тез. докл., 2010. – С.53.

[4] Халимов Г.З. Оценка параметров кривых Гурвица для целей универсального хеширования. Сб. трудов Первой международной научно-технической конференции “Компьютерные науки и технологии”. Белгород, Россия. 8-10 октября. Ч. 2. – 2009. – С. 118–121.

[5] Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования. Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 3. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 144–146.

[6] Халимов Г.З. Универсальное хеширование по максимальным кривым Гурвица / Халимов Г.З. // Журнал “Прикладная радиоэлектроника”. Харьков: ХНУРЭ. — 2010. — Т. 9, № 3. — С. 365–370.

[7] Weil A. Courbes algrebriques et variretres abeliennes / A.Weil // Hermann, Paris, 1971. – P.301.

[8] Ihara Y. Some remarks on the number of rational points of algebraic curves over finite fields / Y. Ihara // J. Fac. Science. Tokio. — 1981. – N. 28. – P. 721–724.

[9] Vladut S.G. Number of points of an algebraic curve / S.G. Vladut ё V.G. Drinfeld // Function Analysis. – 1983. – N. 17 (1). – P. 68–69.

[10] Giulietti M. A new family of Fq2-maximal curves / Giulietti M., Korchmaros G. // prep., 2007.

[11] Ruck H.G. A characterization of Hermitian function fields over finite fields / H.G.Ruck, H.Stichtenoth // J. reine angew. **Mathematics**. – 1994. – V. 457. – P.185–188.

[12] Torres f. The Deligne-Lusztig curve associated to the Suzuki group [Электронный ресурс]/ F.Torres // arXiv:alg-geom/9706012v1 26Jun 1997.

Поступила в редколлегию 18.03.2013

Халимов Геннадий Зайдулович, сведения об авторе см. на стр. 224.

УДК 681.3.06

Оцінки складності універсального гешування за алгебричними кривими/ Г.З. Халімов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 2. – С. 225–229.

Наведено результати універсального гешування за алгебричними кривими. Отримано рішення для обчислення точок найкращих кривих за ключовими даними, оцінки складності обчислень, практичні рекомендації щодо застосування алгебричних кривих для універсального гешування.

Ключові слова: універсальне гешування, максимальні криві.

Табл.: 02. Бібліогр.: 12 найм.

UDC 681.3.06

Estimates of complexity of universal hashing by algebraic curves / G.Z. Khalimov // Applied Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 225–229.

This paper presents the results of universal hashing by algebraic curves. Solutions for computing the best points of curves by key data, estimates of the computational complexity, practical recommendations of using algebraic curves for universal hashing are obtained.

Keywords: universal hashing, maximal curves.

Tab.: 02. Ref.: 12 items.