УДК 681.3.06

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО КРИВЫМ, АССОЦИИРОВАННЫМ С ГРУППОЙ СУДЗУКИ

Е.В. КОТУХ, Г.З. ХАЛИМОВ

Представлены результаты универсального хеширования по кривым, ассоциированным с группой Судзуки над расширениями конечного поля. Рассмотрены проективные многообразия точек кривых, поля рациональных функций. Получены сравнительные оценки вероятности коллизии универсального хеширования. Из оценки следует, что наилучший результат достигается на кривой Судзуки над полем F_q с параметрами $q = 2q_0^2$ и $q_0 = 2^s$.

Ключевые слова: универсальное хеширование, группа Судзуки, кривые Судзуки.

ВВЕДЕНИЕ

Группа Судзуки определяет многообразие алгебраических кривых, которые ассоциируются с её подгруппами. Интенсивные исследования таких кривых лежат в плоскости практических применений: схем универсального хеширования, алгебраических кодов. Основное преимущество вычислений по кривым Судзуки определяется простотой задания их точек, что нельзя сказать, например, о кривых Эрмита и других максимальных кривых. Известно, что наилучший результат универсального хеширования достигается на кривых с большим числом точек, достаточно близких к границе Хассе-Вейля. Проблематикой универсального хеширования на функциональном поле $F_q(C)$ алгебраической кривой C над конечным полем F_q является определение проективного многообразия точек кривой, поля рациональных функций и оценка параметров хеш функций.

Целью статьи является построение универсального хеширования по функциональному полю кривых, ассоциированных с подгруппами группы Судзуки. В разделе 1 приводятся определения и свойства группы Судзуки. В разделе 2 рассмотрены оценки параметров универсального хеширования по кривым Судзуки.

1. ОПРЕДЕЛЕНИЕ И СВОЙСТВА ГРУППЫ СУДЗУКИ

Семейство исключительных групп известных, как группы Судзуки, впервые представлены в [1,2]. Определения и свойства группы Судзуки $Sz(q)$ изложены в [3]. Группу $Sz(q)$ не следует путать с Судзуки 2-группой или спорадической группой Судзуки.

Замечание 1.

1. Существуют различные концептуальные определения группы Судзуки [4,5]. Явное представление группы, на основе матриц 4x4 над полями характеристики $p = 2$ дано в оригинальной работе Судзуки [1]. Параметризация группы выполнена в работах Хуберта [3] и Джонса [6 15].

Определение 1 (группа Судзуки). Пусть $a,b,\alpha,\beta \in F_q$, $q = 2^{2n+1}$ и $c,\gamma \in F_q^\times$, где $F_q^\times$ – мультипликативная группа. Определим 4×4 матрицы над F_q в виде

$$u(a,b,\alpha,\beta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \alpha a+\beta & a & 1 & 0 \\ \alpha^2 a+\alpha\beta+b & \beta & \alpha & 1 \end{pmatrix},$$

$$d(c,\gamma) = \begin{pmatrix} c\gamma & 0 & 0 & 0 \\ 0 & \gamma & 0 & 0 \\ 0 & 0 & \gamma^{-1} & 0 \\ 0 & 0 & 0 & \gamma^{-1}c^{-1} \end{pmatrix},$$

$$T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

Пусть $U(\alpha,\beta) = u(\alpha^\theta,\beta^\theta,\alpha,\beta)$ и $D(\gamma) = d(\gamma^\theta,\gamma)$, $\theta = 2^{n+1}$. Группа Судзуки имеет представление

$$Sz(q) = \begin{Bmatrix} U(\alpha,\beta)D(\gamma)TU(\alpha',\beta'): \\ \alpha,\alpha',\beta,\beta' \in F_q, \gamma \in F_q^\times \end{Bmatrix}.$$
$$\cup\left\{U(\alpha,\beta)D(\gamma): \alpha,\beta \in F_q, \gamma \in F_q^\times\right\}$$

Замечание 4.

1. Параметризация группы Судзуки по определению 1 впервые представлена в [6] и взята из работы [7]. Группа Судзуки следует из выражения для $Sz(q)$ и определяется множествами матриц 4×4 над конечным полем F_q, $q = 2^{2n+1}$ характеристики 2.

2. Свойства группы Судзуки достаточно полно исследованы в [3] с несколько отличным представлением матричных групп. Следуя работе [3] рассмотрим следующие определения.

Определение 2. Пусть $\pi(x) = x^t$, $t = 2^{m+1}$ для $\forall x \in F_q$, $q = 2^{2m+1}$, π – исключительный автоморфизм в F_q такой, что $\pi(\pi(x)) = x^2$. Для $a,b \in F_q$ и $c \in F_q^\times$ определим матрицы

$$S(a,b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & \pi(a) & 1 & 0 \\ a^2\pi(a)+ab+\pi(b) & a\pi(a)+b & a & 1 \end{pmatrix},$$

$$M(c)=\begin{pmatrix} c^{1+2^m} & 0 & 0 & 0 \\ 0 & c^{2^m} & 0 & 0 \\ 0 & 0 & c^{-2^m} & 0 \\ 0 & 0 & 0 & c^{-1-2^m} \end{pmatrix},$$

$$T=\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Замечание 2.

1. Матрицы $S(a,b)$ и $M(c)$ следуют из переопределений матриц $U(\alpha,\beta)$ и $D(\gamma)$ с заменой переменных $\alpha\to a$, $\alpha a+\beta\to b$, $\gamma\to c^{2^m}$.

Определение 3. Группа Судзуки в соответствии с выражением (1) определяется произведением матриц

$$Sz(q)=\left\langle S(a,b),M(c),T\middle|a,b\in F_q,c\in F_q^{\times}\right\rangle,$$

имеет порядок

$$\left|Sz(q)\right|=q^2(q^2+1)(q-1),$$

где три делителя попарно взаимно простые и

$$(q^2+1)=(q+t+1)(q-t+1).$$

Предложение 1 [3]**.** Для всех $a,b,a',b'\in F_q$ и $c\in F_q^{\times}$ справедливо

$$S(a,b)S(a',b')=S(a+a',b+b'+\pi(a)a'),$$

$$S(a,b)^{M(c)}=S(ca,c\pi(c)b),$$

$$M(c)M(c')=M(cc').$$

Соотношения проверяются прямыми вычислениями и следуют из свойств автоморфизма

$$\pi(\pi(a))=a^2,\ \pi(ab)=\pi(a)\pi(b)$$

$$\text{и } \pi(a+b)=\pi(a)+\pi(b),\ a,b\in F_q$$

в поле характеристики 2

Следствие 1. Для всех $a,b,a',b'\in F_q$ и $c\in F_q^{\times}$, $q=2^{2m+1}$ справедливо

$$S(a,b)^{-1}=S(a,b+\pi(a)a),$$

$$S(a,b)^{S(a',b')}=S(a,b+\pi(a)a'+\pi(a')a).$$

Предложение 2 [3]**.** Пусть,

$$\Im=\left\{S(a,b)\middle|a,b\in F_q\right\},$$

$$\mathrm{H}=\left\{M(c)\middle|c\in F_q^{\times}\right\},$$

тогда $\Im\le Sz(q)$ является 2-группой с экспонентой 4, мощности $\left|\Im\right|=q^2$ и H изоморфна циклической группе $F_q^{\times}$ порядка $q-1$.

Предложение 3 [3]. Группа $\mathrm{H}=\left\{M(c)\middle|c\in F_q^{\times}\right\}$ действием $S(a,b)^{M(c)}$ порождает группу неподвижной точки свободных автоморфизмов на $\Im=\left\{S(a,b)\middle|a,b\in F_q\right\}$ и $\Im\mathrm{H}$ является группой Фробениуса с ядром Фробениуса $\Im$.

Замечание 3.

1. Из свойства группы Фробениуса $\Im\cap H=\{1\}$ порядок группы $\Im$ H равен $q^2(q-1)$.

2. Группа Судзуки содержит подгруппы $S(a,b)$, $M(c)$, Холла и подгруппы по делителям их порядков.

2. КРИВЫЕ ДЭЛИНГЭ-ЛУСТИГА, АССОЦИИРОВАННЫЕ С ГРУППОЙ СУДЗУКИ

Кривая максимального рода над квадратичним полем F_q является кривой Эрмита. По классификации кривых Дэлигнэ-Лустига кривая Эрмита ассоциируется с проективной специальной линейной группой, покрывает максимальные плоские кривые меньшего рода в квадратичном поле и имеет наилучшую асимптотическую оценку

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

$$A(q)\approx 2\sqrt{q},$$

где $N_q(g)$ – число точек кривой рода g.

Вторая и третья группа кривых Дэлигнэ-Лустига ассоциируются с группой Судзуки $Sz(q)$ и группой Ри $R(q)$. Кривые Судзуки и Ри широко рассмотрены в [8–10]. Эти кривые являются оптимальными кривыми в том смысле, что имеют число F_q рациональных точек относительно рода достаточно близким к границе Хассе-Вейля.

Главный результат по кривым Дэлигнэ-Лустига второго типа ассоциированных с $Sz(q)$ определяется следующей теоремой.

Теорема 1. [10] 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 Сузуки $Sz(q)$.

Кривую с точностью до F_q изоморфизма, ассоциированную с подгруппой $S(a,b)$ группы Судзуки $Sz(q)$, основанную на роде, числе точек и групповом F_q автоморфизме кривой определили Хансен Дж. и Стичтенот Х. [8].

Кривая порядка q^2 из группы Судзуки порядка $q^2(q^2+1)(q-1)$, ассоциированная с подгруппой $S(a,b)$, является F_q изоморфной плоской кривой

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

Кривая Судзуки рассмотренная Хансеном Дж. и Стичтенотом Х., имеет относительно своего рода максимальное число точек. Максимальное число F_q рациональных точек кривой определяется замечательной формулой Вейля и для кривой Судзуки чуть меньше границы Хассе-Вейля. Действительно, прямая подстановка в оценку числа точек Хассе-Вейля рода кривой даёт значение

$$N_q(g)=1+q+2g\sqrt{q}=\sqrt{2}q^2-(\sqrt{2}-1)q+1$$

и имеем, что $q^2+1<\sqrt{2}q^2-(\sqrt{2}-1)q+1$.

Число F_{q^r} – рациональных точек кривой $N_{q^r}(g)$ можно определить на основе вычисления специального L полинома, который является энумератором дзета функции

$$\zeta(X,t)=\exp(\sum N_{q^r}t^r/r).$$

Известен результат Хассе-Вейля

$$\zeta(X,t)=L(X,t)/\{(1-t)(1-qt)\},$$

где $L(X,t)=\prod_{k=1}^{2g}(1-\alpha_k t)$, $L(X,t)\in Z(t)$;

$\alpha_j\alpha_{j+g}=q$, $j=1,...,g$;

$|\alpha_j|=\sqrt{q}$, $j=1,...,g$.

Следуя [6], если

$$L(X,t)=\prod_{k=1}^{2g}(1-\alpha_k t),$$

тогда число точек кривой в расширенном поле F_{q^r} определяется выражением

$$N_{q^r}(g)=q^r+1-\sum_{k=1}^{2g}\alpha_k^r.$$

Для кривой Судзуки, как показано в [9], энумератор имеет следующий вид

$$L(X,t)=(1+2q_0t+qt^2)^g.$$

Полином $L(X,t)$ имеет $2g$ корней и решения для α_k разбиваются на две группы по g одинаковых значений

$$\alpha=q_0(-1+i)\ \text{и}\ \beta=\tilde{\alpha}=q_0(-1-i).$$

Для α и β легко проверяются условия $\alpha_j\alpha_{j+g}=q$ и $|\alpha_j|=\sqrt{q}$. Для $N_{q^r}(g)$ получим результирующее выражение

$$N_{q^r}(g)=q^r+1-g(\alpha^r+\beta^r).$$

Рассмотрим основные случаи расширенного поля F_{q^r} и значения числа точек для кривой Судзуки. Подставляя в $N_{q^r}(g)$ степени расширения $r=\overline{1,4}$, получим

$$N_q(g)=q+1-g(\alpha+\beta)=q+1+2gq_0=$$
$$q+1+2q_0q_0(q-1)=q^2+1;$$
$$N_{q^2}(g)=q^2+1-g(\alpha^2+\beta^2)=$$
$$q^2+1-gq_0{}^2(-2i+2i)=q^2+1;$$
$$N_{q^3}(g)=q^3+1-g(\alpha^3+\beta^3)=$$
$$q^3+1-4gq_0{}^3=q^3+1-4q_0{}^4(q-1)=q^2+1;$$
$$N_{q^4}(g)=q^4+1-g(\alpha^4+\beta^4)=$$
$$q^4+1+8gq_0{}^4=q^4+1+2q_0(q-1)q^2.$$

Замечание 4.

1. Кривая Судзуки над полем F_q является оптимальной, по числу точек лежит близко к границе Хассе-Вейля для кривой рода $g=q_0(q-1)$.

2. Кривая Судзуки над квадратичным и кубическим полем является неоптимальной.

3. Кривая Судзуки над конечным полем степени расширения 4 является максимальной. Подстановка значения рода $g=q_0(q-1)$ в выражение Хассе-Вейля дает

$$N_{q^4}(g)=q^4+1+2q_0(q-1)q^2,$$

что равно числу точек кривой в F_{q^4}.

4. Более общий результат получен в [9], где показано, для расширений $r\equiv 0\bmod 4$ кривая Судзуки является максимальной.

Действительно

$$N_{q^{4s}}(g)=q^{4s}+1-g(\alpha^{4s}+\beta^{4s})=$$
$$q^{4s}+1+2\cdot 4^s gq_0{}^{4s}=q^{4s}+1+2q_0(q-1)q^{2s},\quad s\geq 1.$$

5. В работе [9] рассмотрена кривая Судзуки

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

с параметрами $q_0=2^s$ и $q=2q_0$.

Показано, что кривая имеет род $g=q_0(q-1)$, число точек $N_q(g)=q^2+1$ так же является F_q – изоморфной кривой Дэлигнэ-Лустига, ассоциированной с группой Судзуки $Sz(q)$. По сравнению с определением из теоремы 1, кривая определена над меньшим в q_0 раз конечным полем и содержит в $q_0{}^2$ меньше точек.

6. В работе [11] получены производные кривые по подгруппам группы Судзуки для случая $q=2q_0{}^2$ и $q_0=2^s$.

По циклической подгруппе порядка r, $r|q-1$ кривая рода $g=q_0(q-1)/r$ имеет вид

$$V^{(q-1)/r}f(U)=(1+U^{q_0})(U^{q-1}+V^{2(q-1)/r}),$$

где $f(t)=1+\sum_{i=0}^{s-1}t^{2^i(2q_0+1)-(q_0+1)}(1+t)^{2^i}$.

По подгруппе Зингера порядка $q+2q_0+1$ кривая рода $g=(q+2q_0+1)(q_0-1)/r+1$ имеет вид

$$V^{(q+2q_0+1)/r}\tilde{f}(U)=U^{q+2q_0+1}+V^{2(q+2q_0+1)/r},$$

где $\tilde{f}(t)=1+\sum_{i=0}^{s-1}t^{2^iq_0}(1+t)^{2^i(q_0+1)-q_0}+t^{q/2}$.

По подгруппе Зингера порядка $q-2q_0+1$ кривая рода $g=(q-2q_0+1)(q_0-1)/r-1$ имеет вид

$$bV^{(q-2q_0+1)/r}f(U)=$$
$$=(U^{q_0-1}+V^{2q_0-1})(U^{q-2q_0+1}+V^{2(q-2q_0+1)/r}),$$

где $b=\lambda^{q_0}+\lambda^{q_0-1}+\lambda^{-q_0}+\lambda^{-(q_0-1)}$, $\lambda\in F_{q^4}$, порядка $q-2q_0+1$.

7. В работе [11] также рассмотрены кривые, ассоциированные с подгруппами группы Судзуки порядков 2^ur, $2r$, $2s$, $4s$, где $r|(q-1)$, $s|(q\pm 2q_0+1)$.

Кривые по данным подгруппами имеют число точек соответствующими порядкам подгрупп, что меньше числа точек кривой ассоциированной с подгруппой $S(a,b)$ порядка q^2.

Замечание 5.

1. Универсальное хеширование по кривой Судзуки для случая $q_0=2^s$ и $q=2q_0{}^2$, ассоциированное с дивизором $D=|(q+2q_0+1)P_0|$ определяется на F_q рациональном морфизме $\pi:=(1:x:y:v:w)$ в P^4, где x,y,v,w определяются уравнениями [8]

$$y^q-y=x^{q_0}(x^q-x),$$
$$v:=x^{2q_0+1}+y^{2q_0},$$
$$w:=xy^{2q_0}+x^{2q+2q_0}+y^{2q},$$

и 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 определяется 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 $f(a,b) := a^{2q_0+1} + b^{2q_0}$ [12].

Хеширование по рациональным функциям кривой Судзуки определяет универсальный хеш класс $\varepsilon - U(q^2, q^k, q)$, где q^2 – число хеш функций (объём ключевого пространства), q^k – объём пространства сообщений, q – объём пространства хеш кодов. Вероятность коллизии ε определяется соотношениями

$$\varepsilon = (i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + rq)/q^2, \text{ если } k < q_0(q-1),$$

$$\varepsilon = (k + q_0(q-1))/q^2, \text{ если } k \ge q_0(q-1),$$

где $0 \le i \le q_0 - 1, 0 \le j \le q_0 - 1, 0 \le t \le 1, 0 \le r \le q-1$.

2. Пусть $k \approx \sqrt{q}(\sqrt{q}-1)/2$. Имеем, значения параметров $i \approx s$, $j = 0$, $t = 0$, $r = 0$, $s \approx \left\lceil (3k)^{1/3} \right\rceil \approx (q)^{1/3}$ и оценку вероятности коллизии

$$\varepsilon \approx q^{1/3}(q+q_0)/q^2 \approx q^{-1/6}\varepsilon_{ЭК},$$

где $\varepsilon_{ЭК} = 1/\sqrt{q} + 1/q$ – значение вероятности коллизии универсального хеширования по кривой Эрмита в квадратичном поле F_q при $k = \sqrt{q}(\sqrt{q}-1)/2$. Из оценки $\varepsilon \approx q^{-1/6}\varepsilon_{ЭК}$ следует выигрыш в $q^{1/6}$ раз по вероятности коллизии относительно хеширования по кривой Эрмита. Размер ключевых данных по сравнению с хешированием по Эрмита больше в $\sqrt{q}$.

3. Для $k = q_0(q-1)$ имеем вероятность коллизии хеширования по кривым Сузуки

$$\varepsilon = 2q_0(q-1)/q^2 \approx \sqrt{2}q^{-1/2}.$$

Подстановка $k = q_0(q-1)$ в выражение для вероятности коллизии хеширования по кривым Эрмита дает

$$\varepsilon = k/q^3 + 1/(2q) - 1/(2q^2) = \frac{1}{\sqrt{2}}\sqrt{q}(q-1)/q\sqrt{q} + 1/(2\sqrt{q}) - 1/(2q) \approx 1/\sqrt{2}.$$

4. Универсальное хеширование по кривой Судзуки для случая $q_0 = 2^s$ и $q = 2q_0$, ассоциированное с дивизором $D = |(q+2q_0+1)P_0|$ определяется на том же F_q рациональном морфизме $\pi := (1:x:y:v:w)$ в P^4 с теми же порядками полюсов как для случая кривой с параметрами $q_0 = 2^s$ и $q = 2q_0^2$. Следовательно, справедливо определение и соотношения для вероятности коллизии из п.1 замечания 5.

Для $k = q_0(q-1)$ получим оценку вероятности коллизии хеширования

$$\varepsilon = 2q_0(q-1)/q^2 \approx (4q_0^2 - 2q_0)/4q_0^2 \approx 1,$$

что хуже по сравнению с хешированием с параметрами $q_0 = 2^s$ и $q = 2q_0^2$

$$\varepsilon = 2q_0(q-1)/q^2 \approx 1/q_0.$$

5. Функциональное поле максимальной кривой Судзуки над конечным полем F_{q^4} рассмотрено в [13]. Универсальное хеширование по максимальной кривой Судзуки над конечным полем F_{q^4} вычисляется по пяти параметрическим функциям базиса $L(lD)$ в выражении

$$S := \left\{ \begin{array}{l} x^a y^b v^c w^d (x^q + x)^r \\ aq + b(q+q_0) + c(q+2q_0) + \\ \quad + d(q+2q_0+1) + rq^2 \le l(q^2+1) \\ 0 \le a \le q-1, 0 \le b \le 1, 0 \le c \le q_0 - 1, \\ 0 \le d \le q_0 - 1, 0 \le r \le l \end{array} \right\}.$$

Функциональное поле в векторном пространстве выстраивается в порядке возрастания полюсов $f = x^a y^b v^c w^d (x^q + x)^r$. Для числа слов данных $k < q(q_0 - 1)^2$ вычисления рациональных функций осуществляется по параметрам x, y, v, w.

Для крайних параметров a,b,c,d в выражении для S будет иметь значение дискретной оценки

$$\nu_\infty(f) = (q-1)q + (q+q_0) + (q_0-1)(q+2q_0) + (q_0-1)(q+2q_0+1) = q^2 + 2g - 1.$$

Для числа слов данных $k > q(q_0-1)^2$ вычисление рациональных функций следует выполнять по пяти параметрам $x, y, v, w, (x^q + x)$, что позволяет построить функциональное пространство с непрерывной последовательностью полюсов для больших значений k.

Для $k = q_0(q-1)$ получим оценку вероятности коллизии хеширования над полем F_{q^4}

$$\varepsilon = 2q_0(q-1)/q^4 \approx \frac{1}{q^2 q_0}.$$

Определение хеширования по кривой Судзуки над полем F_p с параметрами $p_0 = 2^s$, $p = 2p_0^2$ и $p \approx q^4$ для $k = q_0(q-1)$ слов данных аналогично п.2 замечания 5 и будет иметь оценку вероятности коллизии

$$\varepsilon \approx \rho_k / p^2 \approx \frac{k^{1/3}(q+q_0)}{q^8} \approx \frac{1}{q^6 q_0},$$

что существенно лучше по сравнению с хешированием в расширенном поле F_{q^4}.

ЗАКЛЮЧЕНИЕ

Кривые по подгруппам группы Судзуки имеют число точек, соответствующим порядкам подгрупп. Наилучшие параметры универсального хеширования по вероятности коллизии и затратам ключа достигаются по кривой Судзуки, ассоциированной с подгруппой $S(a,b)$ порядка q^2.

Кривая Судзуки над конечным полем четвертой степени расширения является максимальной, но имеет относительно малое значение рода и поэтому проигрывает по вероятности коллизии. Практическое применение таких кривых может быть перспективным для алгебраического кодирования.

Кривая Судзуки с параметрами $q_0 = 2^s$ и $q = 2q_0$ имеет меньшее отношение числа точек к роду, что определяет её проигрыш хешированию с параметрами $q_0 = 2^s$ и $q = 2q_0^2$.

Кривые ассоциированные с подгруппами Зингера и подгруппами меньших порядков имеют малое число точек, сложность построения и следовательно их применение лежит в плоскости простых кодовых схем.

Литература

[1] *Suzuki M.* A new type of simple groups of finite order. / M.Suzuki // Proc. Nat. Acad. Sci. U.S.A. – 1960. – V. 46. – P. 868–870.

[2] *Suzuki M.* On a class of doubly transitive groups. / M. Suzuki // Ann. of Math. – 1962. – V. (2)75. – P.105–145.

[3] *Huppert B.* Finite groups. III. / B. Huppert, N. Blackburn // Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 243, Springer-Verlag, Berlin. – 1982. – vol. 243.

[4] *Carter R.W.* Simple groups of Lie type. / R.W. Carter // Reprint of the 1972 original. Wiley Classics Library. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York. – 1989. – P.335.

[5] *Wilson R.A.* The finite simple groups. / R.A.Wilson // Graduate Texts in Mathematics 251. Springer-Verlag London, Ltd., London. – 2009. – P. 298.

[6] *Jones G.A.* Varieties and simple groups. / G.A. Jones // J. Austr. Math. Soc.-1974. – V.17. – P. 163–173.

[7] *Landazuri V.* On the minimal degrees of projective representations of the finite Chevalley groups. / V.Landazuri and G. M.Seitz // J. Algebra. – 1974. – V.32. –P. 418–443.

[8] *Hansen J.P.* Group codes on certain algebraic curves with many rational points. / J.P.Hansen, H.Stichtenoth // AAECC 1. – 1990. – P. 67–77.

[9] *Hansen J.P.* Deligne-Lusztig varieties and group codes. / J.P. Hansen // Lect. Notes Math. – 1992. – V. 1518. – P. 63–81.

[10] *Pedersen J.P.* A function field related to the Ree group. / J.P. Pedersen // Lect. Notes Math. – 1992. – V. 1518. – P. 122–131.

[11] *Giulietti M.* Quotient curves of the Suzuki curve. / M.Giulietti, G.Korchmarros, F.Torres //Acta Arith. – 2006. – no. 3. – P. 245–274.

[12] *Tits J.* Ovo¨ıdes et groupes de Suzuki. / J.Tits // Archive Mathematics. – 1962. – N.13. –P.187–198.

[13] *Eid A.* Suzuki-invariant codes from the Suzuki curve. / A.Eid, H.Hasson, A.Ksir, J.Peachey // arXiv: 1411.6215v2[math.AG] 25 Nov 2014.

Поступила в редколлегию 26.11.2015

Котух Евгений Владимирович, аспирант кафедры БИТ ХНУРЭ. Научные интересы: аутентификация данных и кодирование.

Халимов Геннадий Зайдулович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Научные интересы: методы и средства аутентификации данных.

УДК 681.3.06

Універсальне хешування по кривих, які асоційовані з групою Судзукі / Е.В. Котух, Г.З. Халімов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2015. – Том 14. – № 4. – С. 361–365.

Наведено результати універсального гешування по кривих, які асоційовані з групою Судзукі над розширеннями кінцевого поля. Розглянуто проективні розмаїття точок кривих, поля раціональних функцій. Отримано порівняльні оцінки ймовірності колізії універсального гешування. З оцінки випливає, що найкращий результат досягається на кривій Судзукі над полем F_q з параметрами $q = 2q_0^2$ і $q_0 = 2^s$.

Ключові слова: універсальне гешування, група Судзукі, криві Судзукі.

Бібліогр.: 13 найм.

UDC 681.3.06

Universal hashing by curves associated with Suzuki group / E.V. Kotukh, G.Z. Khalimov // Applied Radio Electronics: Sci. Journ. — 2015. — Vol. 14. — № 4. — P. 361–365.

The paper presents the results of universal hashing by curves associated with the Suzuki group on extensions of a finite field. A projective variety of points of the curves, fields of rational functions are considered. Comparative estimates of the probability of universal hashing collisions are obtained. The estimate has shown that the best result is achieved on the Suzuki curve over the field F_q with parameters $q = 2q_0^2$ and $q_0 = 2^s$.

Keywords: universal hashing, the Suzuki group, Suzuki curves.

Ref.: 13 items.