

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО КРИВОЙ СУЗУКИ

Г.З. ХАЛИМОВ, Е.В. КОТУХ

Представлены результаты универсального хеширования по кривой Сузуки над конечным полем. Рассмотрены проективное многообразие точек кривой, поле рациональных функций. Представлено доказательство подгруппы Вейерштрасса для рациональных функций кривой и определение универсального хеширования над функциональным полем кривой. Получены оценки вероятности коллизии универсального хеширования. Из оценки следует выигрыш в $\sqrt{2/3}k^{1/6}$ раз по вероятности коллизии к хешированию по кривой Эрмита.

Ключевые слова: универсальное хеширование, кривая Сузуки.

ВСТУПЛЕНИЕ

Максимальные кривые ассоциированные с группой Сузуки и группой Ри имеют максимально возможное значение рода и соответственно число точек. Первые оценки универсального хеширования по проективной линии, кривым Эрмита и Гурвица представлены в [1-3]. Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на 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 семейства хеш функций.

Целью статьи является решение задачи построения универсального хеширования по функциональному полю кривой Сузуки. В разделе 1 приводятся определение и свойства кривой Сузуки. В разделе 2 рассмотрено функциональное поле кривой Сузуки. В разделе 3 представлено универсальное хеширование в поле рациональных функций по кривой Сузуки и оценка параметров универсального хеширования.

1. ОПРЕДЕЛЕНИЕ И СВОЙСТВА КРИВОЙ СУЗУКИ

Кривые Сузуки S являются F_q изоморфными плоской кривой

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

где $q = 2q_0^2$ и $q_0 = 2^s$. Род кривой $g = q_0(q-1)$ и число F_q рациональных точек равно $q^2 + 1$.

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

Теорема 1. [4] 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

Делигнэ-Лустига ассоциированной с группой Сузуки $Sz(q)$.

Кривая Делигнэ-Лустига ассоциированная с группой Сузуки определяется полной линейной серией $D = |(q+2q_0+1)P_0|$ размерности $\dim = 4$ и степени $q+2q_0+1$, которая выводится из эnumератора Зета функции [6]. Отображение кривой Сузуки на проективное пространство P^4 и подгруппа Вейерштрасса $H(P)$, $P \in X(F_q)$ рассмотрены в работах [4-7].

2. ФУНКЦИОНАЛЬНОЕ ПОЛЕ КРИВОЙ СУЗУКИ

Основные результаты обобщены в утверждении 1.

Утверждение 1. F_q рациональный морфизм кривой Сузуки в P^4 есть отображение

$$\pi := (1 : x : y : v : w),$$

где x, y, v, w определяются уравнениями [5]

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

$$v := x^{2q_0+1} + y^{2q_0},$$

$$w := xy^{2q_0} + x^{2q+2q_0} + y^{2q},$$

и порядки полюсов равны

$$\operatorname{div}_\infty(x) = qP_0,$$

$$\operatorname{div}_\infty(y) = (q+q_0)P_0,$$

$$\operatorname{div}_\infty(v) = (q+2q_0)P_0,$$

$$\operatorname{div}_\infty(w) = (q+2q_0+1)P_0.$$

Кривая Сузуки может быть представлена 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 $f(a,b) := a^{2q_0+1} + b^{2q_0}$ [6].

Подгруппа Вейерштрасса $H(P)$, $P \in C(F_q)$ функционального поля кривой содержит подгруппу [5]

$$H(P) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle.$$

Доказательство. Покажем подгруппу Вейерштрасса. Для этого запишем уравнение

кривой в проективных координатах

$$Y^q Z^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1} Z^{q+q_0-1}. \quad (1)$$

На кривой C существуют особая точка на бесконечности $P_0 = (0:1:0)$ кратности q_0 и рациональные точки $P_{\alpha,0} = (\alpha:0:1)$, $P_{0,\beta} = (0:\beta:1)$, где $\alpha, \beta \in F_q$.

Пусть $\aleph$ является линией с уравнением $X=0$. Тогда $\aleph$ пересекает кривую в точках $P_{0,\beta}$ и P_0 . Число точек $P_{0,\beta}$ равно q . Линия $\aleph$ имеет только однократные пересечения в точках $P_{0,\beta}$, так как $X=0$ не является касательной в этих точках. По теореме Безу кратность пересечения линии $\aleph$ с кривой C равна $q+q_0$. Отсюда следует, что $\aleph \cdot C = \sum_{\beta \in F_q} P_{0,\beta} + q_0 P_0$.

Рассмотрим линию $\aleph$ с уравнением $Y=0$. $\aleph$ пересекает кривую C в точках $P_{\alpha,0}$ и в точке $P_{0,0} = (0:0:1)$ является касательной кратности пересечения q_0+1 , следовательно $\aleph \cdot C = \sum_{\alpha \in F_q, \alpha \neq 0} P_{\alpha,0} + (q_0+1)P_{0,0}$. Для линии $\aleph$ с уравнением $Z=0$ имеем пересечение с кривой только в одной точке $P_0 = (0:1:0)$ и $\aleph \cdot C = (q+q_0)P_0$.

Для рациональных функций $x = X/Z$ и $y = Y/Z$ получим следующие дивизоры

$$\operatorname{div}(x) = \sum_{\beta \in F_q} P_{0,\beta} + qP_0,$$

$$\operatorname{div}(y) = \sum_{\alpha \in F_q, \alpha \neq 0} P_{\alpha,0} + (q_0+1)P_{0,0} - (q+q_0)P_0,$$

соответственно $\operatorname{div}_\infty(x) = qP_0$ и $\operatorname{div}_\infty(y) = (q+q_0)P_0$ значение полюса дивизоров.

Рассмотрим уравнение $v := x^{2q_0+1} + y^{2q_0}$. Имеем

$$y = (v - x^{2q_0+1})^{1/2q_0}.$$

Подставим в $y^q - y = x^{q_0}(x^q - x)$ и после преобразований получим

$$v^q - v = x^{2q_0}(x^q - x).$$

Запишем уравнение в проективных координатах

$$V^q Z^{2q_0} - VZ^{q+2q_0-1} = X^{q+2q_0} - X^{2q_0+1} Z^{q-1}. \quad (2)$$

Уравнение (2) также как и уравнение кривой (1) имеет q^2+1 число решений в F_q .

Рассмотрим линию Ψ с уравнением $V=0$. Ψ пересекает кривую C в точках $P_{\alpha,\beta}$, $\alpha^{2q_0+1} + \beta^{2q_0} = 0$ и в точке $P_{0,0} = (0:0:1)$ является касательной кратности пересечения $2q_0+1$, следовательно

$$\Psi \cdot C = \sum_{\alpha, \beta \in F_q, \alpha^{2q_0+1} + \beta^{2q_0} = 0} P_{\alpha,\beta} + (2q_0+1)P_{0,0}.$$

Для линии $\aleph$ с уравнением $Z=0$ имеем пересечение с кривой

$$V^q Z^{2q_0} - VZ^{q+2q_0-1} = X^{q+2q_0} - X^{2q_0+1} Z^{q-1}$$

только в одной точке

$$P_0 = (0:1:0) \text{ и } \aleph \cdot C = (q+2q_0)P_0.$$

Для рациональной функций $v = V/Z$ получим дивизор

$$\operatorname{div}(v) = \sum_{\alpha \in F_q, \alpha \neq 0} P_{\alpha,0} + (2q_0+1)P_{0,0} - (q+2q_0)P_0$$

и $\operatorname{div}_\infty(v) = (q+2q_0)P_0$ значение полюса дивизора.

Определим $w := y^{2q_0}x + v^{2q_0}$. Уравнение от переменных w, y, x имеет вид

$$\begin{aligned} w^q - w &= y^{2q_0}x^q + v^{2q_0}x - y^{2q_0}x - v^{2q_0} = \\ &= y^{2q_0}(x^q - x). \end{aligned}$$

Порядок полюса функции w в точке P_0 получим с использованием следующих свойств дискретной оценки ϑ_P для рациональных функций:

а) $\vartheta_{P_0}(xy) = \vartheta_{P_0}(x) + \vartheta_{P_0}(y)$ (см. определение I.1.9 стр. 4, [7]);

б) оценка ϑ_P рациональных функций x, y в уравнении $y^q + \mu y = f(x)$ над $F_q, q = p^s$ определяется выражением (см. VI.4.1 стр. 200, [7]) $q\vartheta_{P_0}(y) = \vartheta_{P_0}(y^q + \mu y) = \vartheta_{P_0}(f(x))$.

Вычислим оценку ϑ_P для $w^q - w$

$$\vartheta_{P_0}(w^q - w) = \vartheta_{P_0}(y^{2q_0}(x^q - x)) =$$

$$\vartheta_{P_0}(y^{2q_0}) + \vartheta_{P_0}(x^q - x).$$

Так как

$$\vartheta_{P_0}(x) = \operatorname{div}_\infty(x) = q \text{ и } \vartheta_{P_0}(y) = \operatorname{div}_\infty(y) = q + q_0$$

получим

$$q\vartheta_{P_0}(w) = (q+q_0)2q_0 + q \cdot q = q(q+2q_0+1)$$

и значение полюса дивизора $\operatorname{div}_\infty(w) = q+2q_0+1$.

Отсюда следует, что подгруппа Вейерштрасса $H(P)$, $P \in C(F_q)$ функционального поля кривой содержит подгруппу

$$H(P) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle.$$

Число точек разрыва определяет род кривой $|G(P_0)| = \#(N \setminus H) = q_0(q-1)$ [5]. Линейная серия $q, q+q_0, q+2q_0, q+2q_0+1$ является полной, размерности $\dim = 4$ и определяется рациональными функциями $x, y, v, w \in F_q(C)$.

Рассмотрим представление точек кривой Сузуки.

Для $P \in C(F_q) \setminus P_0$ пусть $a := x(P)$, $b := y(P)$ и $f(a, b) := v(a, b) = a^{2q_0+1} + b^{2q_0}$.

Уравнение для $w := y^{2q_0}x + v^{2q_0}$ приводится к виду $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$. Тогда

$$w(a, b) := af(a, b) + b^2. \quad \diamond$$

Пример 1. Пусть задано F_{2^3} . Кривая Сузуки имеет вид $y^8 - y = x^2(x^8 - x)$. Число точек кривой равно $N = 65$. Точки кривой в P^4 определяются уравнениями:

$$x = a,$$

$$y = b,$$

$$v = x^5 + y^4 = a^5 + b^4,$$

$$w = x^6 + y^2 + xy^4 = a^6 + b^2 + ab^4,$$

где $b^8 - b = a^2(a^8 - a)$ и представлены в табл. 1.

Значения полюсов дивизоров $\text{div}_\infty(x) = 8P_\infty$ и $\text{div}_\infty(y) = 10P_\infty$, $\text{div}_\infty(v) = 12P_\infty$, $\text{div}_\infty(w) = 13P_\infty$. Подгруппа Вейерштрасса точек неразрыва определяется значениями полюсов $H(P_\infty) = \langle 8, 10, 12, 13 \rangle$ и имеет вид $\{0, 8, 10, 12, 13, 16, 18, 20, 21, 22, 23, 24, 25, 26, 28, \dots\}$. Точки разрыва определяются множеством $G(P_\infty) = \{1, 2, 3, 4, 5, 6, 7, 9, 11, 14, 15, 17, 19, 27\}$, их число $|G(P_\infty)| = 14$ и равняется значению рода $g = q_0(q-1) = 14$. Линейная серия 8, 10, 12, 13 является полной, определяется рациональными функциями x, y, v, w .

3. ОПРЕДЕЛЕНИЕ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ ПО КРИВОЙ СУЗУКИ

Определение 1. Хеш функция $h_{x,y}(m) \in F_q$, $q = 2q_0^2$, $q_0 = 2^s$ для сообщения m по рациональным функциям в точке x, y кривой

$$Y^q Z^{q_0} - YZ^{q+q_0-1} = X^{q+q_0} - X^{q_0+1} Z^{q+q_0-1}$$

определяется выражением

$$h_{x,y}(m) = \sum m_{i,j,t,r} \cdot w^j \cdot v^i \cdot y^t \cdot x^r, \quad (3)$$

где ρ_k полюс подгруппы Вейерштрасса $H(P_\infty)$, $m_{i,j,t,r} \in F_q$ – слова сообщения m , $i \geq 0$, $0 \leq j \leq 2q_0 - 1$, $0 \leq t \leq 1$, $0 \leq r \leq q_0$,

$$i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + rq \leq \rho_k,$$

$$x = X/Z, \quad y = Y/Z, \quad v = x^{2q_0+1} + y^{2q_0}$$

$$w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}.$$

Для теоретической оценки вероятности коллизии необходимо связать значение k с показателями i, j, t, r степеней рациональных функций w, v, y, x .

Лемма 1. Пусть $k < q_0(q-1)$. Для кривой Сузуки имеет место

$$i = p - j, \quad j = \Delta - t \cdot q_0 - 1, \quad r = s - s_2 + d \cdot q_0,$$

$$t = t_1 \bmod 2,$$

где

$$s' = \left\lceil (3k)^{1/3} \right\rceil, \quad \Sigma = s'(s'+1)(2s'+1)/6, \quad s = s' + \lfloor k/\Sigma \rfloor,$$

$$s_1 = s - q_0 - 1, \quad \Sigma_{s-1} = s(s-1)(2s-1)/6 -$$

$$s_1(s_1-1)(2s_1-1)/3 - s_1(s_1-1), \quad k' = k - \Sigma_{s-1},$$

$$k_1 = \lceil k'/2 \rceil, \quad d = \lfloor s_2/(s-t) \rfloor, \quad k_2 = k_1 + s_1(s_1+1)/2,$$

$$s_2 = \left\lceil (2k_2 + 1/4)^{1/2} - 1/2 \right\rceil,$$

$$s_3 = s_2 - q_0 - 1, \quad \Delta = k' - 2k_3, \quad t_1 = \lfloor \Delta/q_0 \rfloor,$$

$$k_3 = (s_2 - 1)s_2/2 - (s_1 - 1)(s_1 + 1)/2 - s_3(s_3 + 1)/2$$

$$p = s_2 - (s_2 - t)d,$$

$\lceil \cdot \rceil$ – округление к большему целому числу,
 $\lfloor \cdot \rfloor$ – округление к меньшему целому числу,
 $\lceil \cdot \rceil$ – округление к ближайшему целому числу.

Доказательство. Аддитивная подгруппа Вейерштрасса $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < \dots\}$ кривой

Таблица 1

Точки кривой $y^8 - y = x^2(x^8 - x)$ над F_{2^3}

	P ₀	P ₁	P ₂	P ₃	P ₄	P ₅	P ₆	P ₇	P ₈	P ₉	P ₁₀	P ₁₁	P ₁₂	P ₁₃	P ₁₄	P ₁₅	P ₁₆
z	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x	0	0	1	α^1	α^2	α^3	α^4	α^5	α^6	0	1	α^1	α^2	α^3	α^4	α^5	α^6
v	1	0	1	α^5	α^3	α^1	α^6	α^4	α^2	1	0	α^4	α^1	α^3	α^2	α^5	α^6
w	1	0	1	α^6	α^5	α^4	α^2	α^1	1	1	α^4	α^1	α^2	α^2		α^1	α^3
	P ₁₇	P ₁₈	P ₁₉	P ₂₀	P ₂₁	P ₂₂	P ₂₃	P ₂₄	P ₂₅	P ₂₆	P ₂₇	P ₂₈	P ₂₉	P ₃₀	P ₃₁	P ₃₂	P ₃₃
z	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	α^1	α^1	α^1	α^1	α^1	α^1	α^1	α^1	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^3
x	0	1	α^1	α^2	α^3	α^4	α^5	α^6	0	1	α^1	α^2	α^3	α^4	α^5	α^6	0
v	α^4	α^5	1	α^6	α^2	α^3	0	α^1	α^1	α^3	α^6	1	0	α^5	α^2	α^4	α^5
w	α^2	α^3	α^4	α^4	α^3	α^6	α^2	α^6	α^5	α^1	α^4	α^1	α^4	α^1	α^5	α^6	α^6
	P ₃₄	P ₃₅	P ₃₆	P ₃₇	P ₃₈	P ₃₉	P ₄₀	P ₄₁	P ₄₂	P ₄₃	P ₄₄	P ₄₅	P ₄₆	P ₄₇	P ₄₈	P ₄₉	P ₅₀
z	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
y	α^3	α^3	α^3	α^3	α^3	α^3	α^3	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α^4	α^5	α^5
x	1	α^1	α^2	α^3	α^4	α^5	α^6	0	1	α^1	α^2	α^3	α^4	α^5	α^6	0	1
v	α^4	0	α^2	α^6	α^1	1	α^3	α^2	α^6	α^3	α^5	α^4	1	α^1	0	α^6	α^2
w	α^3	α^6	α^3	1	α^1	α^1	1	α^1	α^5	α^2	α^3	α^3	α^2	α^5	α^1	α^3	α^5
	P ₅₁	P ₅₂	P ₅₃	P ₅₄	P ₅₅	P ₅₆	P ₅₇	P ₅₈	P ₅₉	P ₆₀	P ₆₁	P ₆₂	P ₆₃	P ₆₄			
z	1	1	1	1	1	1	1	1	1	1	1	1	1	1			
y	α^5	α^5	α^5	α^5	α^5	α^5	α^6	α^6	α^6	α^6	α^6	α^6	α^6	α^6			
x	α^1	α^2	α^3	α^4	α^5	α^6	0	1	α^1	α^2	α^3	α^4	α^5	α^6			
v	α^1	α^4	α^5	0	α^3	1	α^3	α^1	α^2	0	1	α^4	α^6	α^5			
w	α^5	α^4	1	α^3	1	α^4	α^5	α^6	α^2	α^5	α^2	α^6	1	1			

$y^q - y = x^{q_0}(x^q - x)$ определяется значениями полюсов, $\phi = q$, $\omega = q + q_0$, $\eta = q + 2q_0$ и $\gamma = q + 2q_0 + 1$

Рассмотрим пример кривой $y^{32} - y = x^4(x^{32} - x)$ над полем F_{2^5} , число точек кривой $N = q^2 + 1 = 1025$ и род $g = q_0(q - 1) = 124$. Размещение полюсов подгруппы Вейерштрасса $H(P) = \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1 \rangle$ для кривой Сузуки над F_q , $q_0 = 2^2$, $q = 2^5$, $q + q_0 = 36$, $q + 2q_0 = 40$, $q + 2q_0 + 1 = 41$ имеет вид, представленный в табл. 2.

Полюса подгруппы Вейерштрасса

$$H(P_\infty) = \langle 32, 36, 40, 41 \rangle$$

в соответствии с таблицей 2 делятся на два слоя. Отличием второго слоя от первого является то, что наряду с комбинаций полюсов 32, 40, 41 функций x, v, w учитывается полюс со значением 36 рациональной функции y . Каждый слой состоит из уровней с нарастающим числом строк. Число уровней для $k < q_0(q - 1) = 124$ равно $2q_0 - 1 = 7$.

Число полюсов на каждом уровне определяется следующим выражением. Пусть s – номер уровня и $s \leq q_0 = 4$. Тогда в первом слое имеем $\Sigma_1 = s(s + 1)/2$, во втором $\Sigma_2 = s(s - 1)/2$ и результирующее число полюсов на уровне s будет равно $\Sigma = s(s + 1)/2 + s(s - 1)/2 = s^2$. Рассмотрим случай $s > q_0 = 4$. Заметим, что можно использовать выражение для суммы s членов арифметической прогрессии с вычитанием недостающих элементов ряда $1, 2, \dots, s - q_0 - 1$. В каждом слое таких наборов по два и результирующее выражение для суммы полюсов на уровне s будет равно $\Sigma = s^2 - 2s_1(s_1 + 1)$, где $s_1 = s - q_0 - 1$. Суммарное число полюсов на всех уровнях $1, 2, \dots, s$ определяется выражением

$$\Sigma_s = \sum_{i=1}^s i^2 - 2 \sum_{j=1}^{s_1} j^2 - 2 \sum_{j=1}^{s_1} j = s(s+1)(2s+1)/6 - s_1(s_1+1)(2s_1+1)/3 - s_1(s_1+1). \quad (4)$$

Таблица 2

Полюса подгруппы Вейерштрасса $H(P_\infty) = \langle 32, 36, 40, 41 \rangle$

Полюса второго слоя				Полюса первого слоя				№
							$\rho_0=0$	1
			$\rho_2=36$				$\rho_1=32$	
						$\rho_4=41$	$\rho_3=40$	2
			$\rho_6=68$				$\rho_5=64$	
		$\rho_{10}=77$	$\rho_9=76$			$\rho_8=73$	$\rho_7=72$	
					$\rho_{13}=82$	$\rho_{12}=81$	$\rho_{11}=80$	3
			$\rho_{15}=100$				$\rho_{14}=96$	
		$\rho_{19}=109$	$\rho_{18}=108$			$\rho_{17}=105$	$\rho_{16}=104$	
	$\rho_{25}=118$	$\rho_{24}=117$	$\rho_{23}=116$		$\rho_{22}=114$	$\rho_{21}=113$	$\rho_{20}=112$	
				$\rho_{29}=123$	$\rho_{28}=122$	$\rho_{27}=121$	$\rho_{26}=120$	4
			$\rho_{31}=132$				$\rho_{30}=128$	
		$\rho_{35}=141$	$\rho_{34}=140$			$\rho_{33}=137$	$\rho_{32}=136$	
	$\rho_{41}=150$	$\rho_{40}=149$	$\rho_{39}=148$		$\rho_{38}=146$	$\rho_{37}=145$	$\rho_{36}=144$	
$\rho_{49}=159$	$\rho_{48}=158$	$\rho_{47}=157$	$\rho_{46}=156$	$\rho_{45}=155$	$\rho_{44}=154$	$\rho_{43}=153$	$\rho_{42}=152$	
			$\rho_{54}=164$	$\rho_{53}=163$	$\rho_{52}=162$	$\rho_{51}=161$	$\rho_{50}=160$	5
		$\rho_{58}=173$	$\rho_{57}=172$			$\rho_{56}=169$	$\rho_{55}=168$	
	$\rho_{64}=182$	$\rho_{63}=181$	$\rho_{62}=180$		$\rho_{61}=178$	$\rho_{60}=177$	$\rho_{59}=176$	
$\rho_{72}=191$	$\rho_{71}=190$	$\rho_{70}=189$	$\rho_{69}=188$	$\rho_{68}=187$	$\rho_{67}=186$	$\rho_{66}=185$	$\rho_{65}=184$	
$\rho_{80}=199$	$\rho_{79}=198$	$\rho_{78}=197$	$\rho_{77}=196$	$\rho_{76}=195$	$\rho_{75}=194$	$\rho_{74}=193$	$\rho_{73}=192$	
		$\rho_{86}=205$	$\rho_{85}=204$	$\rho_{84}=203$	$\rho_{83}=202$	$\rho_{82}=201$	$\rho_{81}=200$	6
	$\rho_{92}=214$	$\rho_{91}=213$	$\rho_{90}=212$		$\rho_{89}=210$	$\rho_{88}=209$	$\rho_{87}=208$	
$\rho_{100}=223$	$\rho_{99}=222$	$\rho_{98}=221$	$\rho_{97}=220$	$\rho_{96}=219$	$\rho_{95}=218$	$\rho_{94}=217$	$\rho_{93}=216$	
$\rho_{108}=231$	$\rho_{107}=230$	$\rho_{106}=229$	$\rho_{105}=228$	$\rho_{104}=227$	$\rho_{103}=226$	$\rho_{102}=225$	$\rho_{101}=224$	
$\rho_{116}=239$	$\rho_{115}=238$	$\rho_{114}=237$	$\rho_{113}=236$	$\rho_{112}=235$	$\rho_{111}=234$	$\rho_{110}=233$	$\rho_{109}=232$	
	$\rho_{123}=246$	$\rho_{122}=245$	$\rho_{121}=244$	$\rho_{120}=243$	$\rho_{119}=242$	$\rho_{118}=241$	$\rho_{117}=240$	7
$\rho_{131}=255$	$\rho_{130}=254$	$\rho_{129}=253$	$\rho_{128}=252$	$\rho_{127}=251$	$\rho_{126}=250$	$\rho_{125}=249$	$\rho_{124}=248$	
$\rho_{139}=263$	$\rho_{138}=262$	$\rho_{137}=261$	$\rho_{136}=260$	$\rho_{135}=259$	$\rho_{134}=258$	$\rho_{133}=257$	$\rho_{132}=256$	
$\rho_{147}=271$	$\rho_{146}=270$	$\rho_{145}=269$	$\rho_{144}=268$	$\rho_{143}=267$	$\rho_{142}=266$	$\rho_{141}=265$	$\rho_{140}=264$	
$\rho_{155}=279$	$\rho_{154}=278$	$\rho_{153}=277$	$\rho_{152}=276$	$\rho_{151}=275$	$\rho_{150}=274$	$\rho_{149}=273$	$\rho_{148}=272$	
$\rho_{163}=287$	$\rho_{162}=286$	$\rho_{161}=285$	$\rho_{160}=284$	$\rho_{159}=283$	$\rho_{158}=282$	$\rho_{157}=281$	$\rho_{156}=280$	8

Размещение полюсов ρ_k в порядке возрастания в подгруппе $H(P_\infty) = \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1 \rangle$, с учетом полюсов рациональных функций представлено в табл. 3.

Значение k определяется выражением

$$k = s(s-1)(2s-1)/6 + s_2(s_2-1) - s_1(s_1-1) - s_3(s_3-1) + t_1 q_0 + j + 1. \quad (5)$$

Здесь s – значение уровня, на котором располагается полюс ρ_k , s_2 – номер строки расположения полюса на уровне s , s_1 – номер строки дополнения до полного арифметического ряда s строк, s_3 – номер строки расположения полюсов, которые необходимо вычесть из суммы полного арифметического ряда s строк, t_1 , число строк размера q_0 уровня s , j – месторасположение полюса в последней строке уровня s .

Для вычисления значений показателей i, j, t, r степеней рациональных функций w, v, y, x соответствующих заданному k следует определить уровень, на котором находится полюс ρ_k , строку расположения полюса на уровне, месторасположения ρ_k в этой строке и принадлежность к первому или второму слою полюсов.

Не трудно показать, что значение уровня, на котором находится полюс ρ_k , вычисляется по формулам:

- $s' = \lceil (3k)^{1/3} \rceil$ – округление к ближайшему целому,

- $\Sigma = s'(s'+1)(2s'+1)/6$ – сумма числа полюсов уровней $1 \div s'$,

- $s = s' + \lfloor k/\Sigma \rfloor$ – уточнение значения уровня, $\lfloor \cdot \rfloor$ – округление к наименьшему целому.

Результат следует из кубической зависимости k от s . Для вычисления строки расположения полюса ρ_k на уровне s следует учесть, что число полюсов по строкам на уровне определяется арифметическим рядом. Результирующие выражения имеют вид:

- $s_1 = s - q_0 - 1$ – значение числа строк дополнения,

$$\Sigma_{s-1} = \sum_{i=1}^{s-1} i^2 - 2 \sum_{j=1}^{s_1-1} j^2 - 2 \sum_{j=1}^{s_1-1} j =$$

$$= s(s-1)(2s-1)/6 - s_1(s_1-1)(2s_1-1)/3 - s_1(s_1-1) -$$

число полюсов на уровнях $1, \dots, s-1$,

- $k' = k - \Sigma_{s-1}$ – число полюсов на уровне s ,

- $k_1 = \lceil k'/2 \rceil$ – число полюсов на уровне s для одного слоя,

- $k_2 = k_1 + s_1(s_1+1)/2$ – дополнение числа полюсов на уровне s за счет s_1 строк,

- $s_2 = \lceil (2k_2 + 1/4)^{1/2} - 1/2 \rceil$ – значение строки расположения полюса.

Число строк t_1 размера q_0 на уровне s определяется выражениями:

- $s_3 = s_2 - q_0 - 1$ – число строк расположения полюсов, которые необходимо вычесть из суммы полного арифметического ряда,

Таблица 3

Размещение полюсов подгруппы Вейерштрасса $H(P_\infty) = \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1 \rangle$

№	Полюса первого слоя				Полюса второго слоя			
1	$\rho_0=0$							
	$\rho_1=\theta=\phi$				$\rho_2=\theta+\theta_0=\omega$			
2	$\rho_3=\theta+2\theta_0=\eta$	$\rho_4=\theta+2\theta_0+1=\gamma$						
	$\rho_5=2\phi$				$\rho_6=\omega+\phi$			
	$\rho_7=\eta+\phi$	$\rho_8=\gamma+\phi$			$\rho_9=\eta+\omega$	$\rho_{10}=\gamma+\omega$		
3	$\rho_{11}=2\eta$	$\rho_{12}=\gamma+\eta$	$\rho_{13}=2\gamma$					
	$\rho_{14}=3\phi$				$\rho_{15}=\omega+2\phi$			
	$\rho_{16}=\eta+2\phi$	$\rho_{17}=\gamma+2\phi$			$\rho_{18}=\eta+\omega+\phi$	$\rho_{19}=\gamma+\omega+\phi$		
	$\rho_{20}=2\eta+\phi$	$\rho_{21}=\gamma+\eta+\phi$	$\rho_{22}=2\gamma+\phi$		$\rho_{23}=2\eta+\omega$	$\rho_{24}=\gamma+\eta+\omega$	$\rho_{25}=2\gamma+\omega$	
4	$\rho_{26}=3\eta$	$\rho_{27}=\gamma+2\eta$	$\rho_{28}=2\gamma+\eta$	$\rho_{29}=3\gamma$				
	$\rho_{30}=4\phi$				$\rho_{31}=\omega+3\phi$			
	$\rho_{32}=\eta+3\phi$	$\rho_{33}=\gamma+3\phi$			$\rho_{34}=\eta+\omega+2\phi$	$\rho_{35}=\gamma+\omega+2\phi$		
	$\rho_{36}=2\eta+2\phi$	$\rho_{37}=\gamma+\eta+2\phi$	$\rho_{38}=2\gamma+2\phi$		$\rho_{39}=2\eta+\omega+\phi$	$\rho_{40}=\gamma+\eta+\omega+\phi$	$\rho_{41}=2\gamma+\omega+\phi$	
	$\rho_{42}=3\eta+\phi$	$\rho_{43}=\gamma+2\eta+\phi$	$\rho_{44}=2\gamma+\eta+\phi$	$\rho_{45}=3\gamma+\phi$	$\rho_{46}=3\eta+\omega$	$\rho_{47}=\gamma+2\eta+\omega$	$\rho_{48}=2\gamma+\eta+\omega$	$\rho_{49}=3\gamma+\omega$
5	$\rho_{50}=4\eta$	$\rho_{51}=\gamma+3\eta$	$\rho_{52}=2\gamma+2\eta$	$\rho_{53}=3\gamma+\eta$	$\rho_{54}=4\gamma$			
	$\rho_{55}=\eta+4\phi$	$\rho_{56}=\gamma+4\phi$			$\rho_{57}=\eta+\omega+3\phi$	$\rho_{58}=\gamma+\omega+3\phi$		
	$\rho_{59}=2\eta+3\phi$	$\rho_{60}=\gamma+\eta+3\phi$	$\rho_{61}=2\gamma+3\phi$		$\rho_{62}=2\eta+\omega+2\phi$	$\rho_{63}=\gamma+\eta+\omega+2\phi$	$\rho_{64}=2\gamma+\omega+2\phi$	
	$\rho_{65}=3\eta+2\phi$	$\rho_{66}=\gamma+2\eta+2\phi$	$\rho_{67}=2\gamma+\eta+2\phi$	$\rho_{68}=3\gamma+2\phi$	$\rho_{69}=3\eta+\omega+\phi$	$\rho_{70}=\gamma+2\eta+\omega+\phi$	$\rho_{71}=2\gamma+\eta+\omega+\phi$	$\rho_{72}=3\gamma+\omega+\phi$
	$\rho_{73}=4\eta+\phi$	$\rho_{74}=\gamma+3\eta+\phi$	$\rho_{75}=2\gamma+2\eta+\phi$	$\rho_{76}=3\gamma+\eta+\phi$	$\rho_{77}=4\eta+\omega$	$\rho_{78}=\gamma+3\eta+\omega$	$\rho_{79}=2\gamma+2\eta+\omega$	$\rho_{80}=3\gamma+\eta+\omega$
6	$\rho_{81}=5\eta$	$\rho_{82}=\gamma+4\eta$	$\rho_{83}=2\gamma+3\eta$	$\rho_{84}=3\gamma+2\eta$	$\rho_{85}=4\gamma+\eta$	$\rho_{86}=5\gamma$		
	...	...	...	...	...	...		
	$\rho_{s(s-1)(2s-1)/6+s_2(s_2-1)-s_1(s_1-1)-s_3(s_3-1)+t_1 q_0+j+1} = i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + r q$							

$$\begin{aligned} \bullet \quad k_3 &= (s_2 - 1)s_2 / 2 - (s_1 - 1)(s_1 + 1) / 2 - \\ &\quad - s_3(s_3 + 1) / 2 - \end{aligned}$$

число полюсов на уровне s для одного слоя,

- $\Delta = k' - 2k_3$ — число полюсов на строке s_2 ,
- $t_1 = \lfloor \Delta / q_0 \rfloor$ — число строк размера q_0 .

Результирующие выражения для показателей i, j, t, r степеней рациональных функций w, v, y, x определяются по формулам:

- $t = t_1 \bmod 2$ — степень y^t (определитель второго слоя),
- $j = \Delta - t \cdot q_0 - 1$ — степень w^j ,
- $d = \lfloor s_2 / (s - t) \rfloor$ — индикатор последней строки s_2 на уровне s ,
- $p = s_2 - (s_2 - t)d$ — показатель степени для строки s_2
- $i = p - j$ — степень v^i ,
- $r = s - s_2 + d \cdot q_0$ — степень x^r .

Пример 2. Пусть $y^{32} - y = x^4(x^{32} - x)$ над полем F_{2^5} , $q = 2^5$. Полюса представлены табл. 2. Вычислить значение полюса ρ_l .

Пусть $l = 113$. Имеем $k = l + 1 = 114$ и вычисления по формулам леммы 1 дают следующее.

$$\begin{aligned} s' &= \lceil (3k)^{1/3} \rceil = (3 \cdot 114)^{1/3} = 7, \\ \Sigma &= s'(s' + 1)(2s' + 1) / 6 = 7 \cdot 8 \cdot 15 / 6 = 140, \\ s &= s' + \lfloor k / \Sigma \rfloor = 7, \\ s_1 &= s - q_0 - 1 = 7 - 5 = 2, \\ \Sigma_{s-1} &= s(s-1)(2s-1) / 6 - s_1(s_1-1)(2s_1-1) / 3 - \\ &\quad - s_1(s_1-1) = 7 \cdot 6 \cdot 13 / 6 - 2 \cdot 1 \cdot 3 / 3 - 2 \cdot 1 = 87, \\ k' &= k - \Sigma_{s-1} = 114 - 87 = 27, \\ k_1 &= \lceil k' / 2 \rceil = 27 / 2 = 14, \\ k_2 &= k_1 + s_1(s_1 + 1) / 2 = 14 + 2 \cdot 3 / 2 = 17, \\ s_2 &= \lceil (2k_2 + 1 / 4)^{1/2} - 1 / 2 \rceil = \\ &\quad \lceil (2 \cdot 17 + 0.25)^{1/2} - 0.5 \rceil = 6, \\ s_3 &= s_2 - q_0 - 1 = 6 - 4 - 1 = 1, \\ k_3 &= (s_2 - 1)s_2 / 2 - s_1(s_1 + 1) / 2 - s_3(s_3 + 1) / 2 = \\ &\quad = 5 \cdot 6 / 2 - 2 \cdot 3 / 2 - 1 \cdot 2 / 2 = 11, \\ \Delta &= k' - 2k_3 = 27 - 2 \cdot 11 = 5, \\ t_1 &= \lfloor \Delta / q_0 \rfloor = \lfloor 5 / 4 \rfloor = 1, \\ t &= t_1 \bmod 2 = 1, \\ j &= \Delta - t \cdot q_0 - 1 = 5 - 5 - 1 = 0, \\ d &= \lfloor s_2 / (s - t) \rfloor = \lfloor 6 / (7 - 1) \rfloor = 1, \\ p &= s_2 - (s_2 - t)d = 6 - (6 - 1) \cdot 1 = 1, \\ i &= p - j = 1 - 0 = 1, \\ r &= s - s_2 + d \cdot q_0 = 7 - 6 + 1 \cdot 4 = 5. \end{aligned}$$

Получим значение полюса

$$\begin{aligned} \rho_{113} &= i(q + 2q_0) + j(q + 2q_0 + 1) + \\ &\quad t(q + q_0) + rq = 1 \cdot 40 + 0 \cdot 41 + 1 \cdot 36 + \\ &\quad 5 \cdot 32 = 236, \end{aligned}$$

что совпадает со значением в таблице 2.

Утверждение 2. Хеширование по рациональным функциям кривой $y^q - y = x^{q_0}(x^q - x)$, где $q = 2q_0^2$ и $q_0 = 2^s$ над полем F_q , определяет универсальный хеш класс $\varepsilon - U(q^2, q^k, q)$, где q^2 — число хеш функций (объем ключевого пространства), q^k — объем пространства сообщений, q — объем пространства хеш кодов. Вероятность коллизии ε определяется соотношениями

$$\begin{aligned} 1) \text{ если } k < q_0(q-1) \\ \varepsilon &= (i(q + 2q_0) + j(q + 2q_0 + 1) + \\ &\quad t(q + q_0) + rq) / q^2, \end{aligned} \quad (6)$$

$$\begin{aligned} 2) \text{ если } k \geq q_0(q-1) \\ \varepsilon &= (k + q_0(q-1)) / q^2, \end{aligned} \quad (7)$$

где i, j, t, r определяются леммой 1.

Доказательство. Параметры универсального класса по рациональным функциям кривой Сузуки следуют из определения кривой и числа её точек в F_q .

Вероятность коллизии ε определяется соотношением $\varepsilon = \rho_k / N$, где

$$\rho_k = i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq -$$

значение полюса рациональной функций $f_k = w^i \cdot v^j \cdot y^t \cdot x^r$, $N = q^2$ — число точек кривой.

Пусть $k < q_0(q-1)$. Параметры i, j, t, r определяются леммой 1 и по подстановке в $\varepsilon = \rho_k / N$ следует (6).

Вслучае $k = q_0(q-1)$, имеем $\rho_k = 2g = 2q_0(q-1)$ и $\varepsilon = 2g / N$, что согласуется с (7). С другой стороны $\rho_k = i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq$. Вычисления по формулам леммы 1 дают $i = q_0 - 1$, $j = 0$, $t = 0$, $r = q_0$ и прямой подстановкой получим проверку

$$\begin{aligned} \rho_k &= i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + rq = \\ &\quad (q_0 - 1)(q + 2q_0) + q_0 q = 2q_0(q - 1). \end{aligned}$$

Пусть $k > q_0(q-1)$. Заметим, что $\rho_k = k + q_0(q-1)$. Прямое вычисление $\varepsilon = \rho_k / N$ приводит к выражению (7). $\diamond$

Замечание 1.

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

$$\varepsilon \approx q^{1/3}(q + q_0) / q^2 \approx q^{-1/6} \varepsilon_{\text{ЭК}}, \quad (8)$$

где $\varepsilon_{\text{ЭК}} = 1 / \sqrt{q} + 1 / q$ — значение вероятности коллизии универсального хеширования по кривой Эрмита в квадратичном поле F_q при $k = \sqrt{q}(\sqrt{q} - 1) / 2$. Из оценки (8) следует выигрыш в $q^{1/6}$ раз по вероятности коллизии хешированию

по кривой Эрмита. Размер ключевых данных по сравнению с хешированием по Эрмита больше в $\sqrt{q}$.

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

$$\varepsilon = 2q_0(q-1)/q^2 \approx \sqrt{2}q^{-1/2}. \quad (9)$$

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

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

Следствие 1. Асимптотика вероятности коллизии универсального хеширования по кривой $y^q - y = x^{q_0}(x^q - x)$ над F_q при больших значениях размерности поля $q \rightarrow \infty$ имеет вид

$$\varepsilon_{q \rightarrow \infty} = (3k)^{1/3}/q, \quad k < g. \quad (10)$$

Доказательство. По лемме 1 определим $s \approx (3k)^{1/3}$ и значения параметров $i \approx s$, $j = 0$, $t = 0$, $r = 0$. Подставим в (6) и для больших q получим (10).

ВЫВОДЫ

Асимптотические оценки вероятности коллизии универсального хеширования по кривой Сузуки при малых значениях k определяются отношением корня кубического длины данных к размерности поля и являются наилучшими оценками для плоских максимальных кривых. Выигрыш к хешированию по кривой Эрмита составляет $\sqrt{2/3}k^{1/6}$ раз.

Литература

- [1] Bierbrauer J. Authentication via algebraic-geometric codes. / Bierbrauer J. // URL <http://www.math.mtu.edu/~jbierbra/potpar.ps>.
- [2] Халимов Г.З. Аутентификация с применением Эрмитовых кодов. / Халимов Г.З., Иохов А.Ю. // Вестник ХПИ. – Х., -2005. – Вып. 9. – С. 26-32.
- [3] Халимов Г.З. Универсальное хеширование по максимальным кривым Гурвица / Халимов Г.З. // Журнал “Прикладная радиоэлектроника”. Харьков: ХНУРЭ. – 2010. – Т.9 № 3, – С.365-370.
- [4] Torres F. The Deligne-Lusztig curve associated to the Suzuki group / Torres F. // arXiv:alg-geom/9706012v1 26Jun. – 1997.
- [5] Hansen J.P. Group codes on certain algebraic curves with many rational points / Hansen J.P.; Stichtenoth H. // AAECC 1. – 1990. – P.67–77.

- [6] Tits J. Ovoides et groupes de Suzuki / Tits J. // Arch. Math. – 1962. Vol.13, – P.187–198. 7. Stichtenoth H. Algebraic function fields and codes / Stichtenoth H. // Springer-Verlag, Berlin. – 1993.

Поступила в редколлегию 15.04.2011



Халимов Геннадий Зайдулович, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: методы и средства аутентификации данных.



Котух Евгений Владимирович, аспирант кафедры БИТ ХНУРЭ. Область научных интересов: аутентификация данных и кодирование.

УДК 681.3.06

Універсальне гешування по кривій Сузукі / Г.З. Халимов, Є.В. Котух // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 164–170.

Представлені результати універсального гешування по кривій Сузукі над кінцевим полем. Розглянуто проєктивне розмаїття точок кривої, поле раціональних функцій. Представлено доказ підгрупи Вейерштрасса для раціональних функцій кривої та визначення універсального гешування над функціональним полем кривої. Отримано оцінки ймовірності колізії універсального гешування. З оцінки слід виграти у $\sqrt{2/3}k^{1/6}$ раз за ймовірністю колізії до гешування по кривій Ерміта.

Ключові слова: універсальне хешування, криві Сузукі.

Табл. 03. Бібліогр.: 07 найм.

UDC 681.3.06

Universal hashing for Suzuki curve / G.Z. Khalimov, E.V. Kotukh // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 164–170.

The paper presents the results of universal hashing for Suzuki curve over a finite field. A projective variety of points of the curve, the field of rational functions are considered. A proof of the Weierstrass subgroup of rational curve functions and the definition of universal hashing over the function field of the curve are presented. Estimates of the collision probability of universal hashing are obtained. The winning of $\sqrt{2/3}k^{1/6}$ times on the probability of collision to the hash of the Hermite curve follows from the estimation.

Keywords: universal hashing, Suzuki curve.

Tab. 03. Ref.: 07 items.