УДК 681.3.06

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО МАКСИМАЛЬНОЙ КРИВОЙ ТРЕТЬЕГО РОДА

Г.З. ХАЛИМОВ

Харьковский национальный университет радиоэлектроники

e-mail: gennadykhalimov@mail.ru

Представлены результаты универсального хеширования по максимальной кривой вида $x^{(q+1)/d}+x^{2(q+1)/d}+y^{q+1}=0$ над конечным полем F_{q^2}. Рассмотрены проективное многообразие точек кривой, поле рациональных функций и оценки параметров семейства хеш функций.

Ключевые слова: универсальное хеширование, алгебраические кривые.

Аутентификация доказуемой стойкости реализуется методами универсального хеширования. Первые оценки универсального хеширования по проективной линии, кривым Эрмита, Гурвица и Сузуки представлены в [1-5]. Для построения хеш функций используются вычисления в поле рациональных функций $F_q(C)$ алгебраических кривых C. Свойства линейного пространства функционального поля алгебраической кривой определяются фундаментальной теоремой Римана-Роха и связываются с алгеброгеометрическими параметрами кривой. Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на границе Хассе-Вейля. Классификация максимальных кривых представлена в [6]. Кривая $x^{(q+1)/d}+x^{2(q+1)/d}+y^{q+1}=0$ в квадратичном поле F_{q^2} в случае $d=3$ является третьей по значению рода после кривой Эрмита.

Целью статьи является определение проективного многообразия точек кривой $x^{(q+1)/d}+x^{2(q+1)/d}+y^{q+1}=0$, поля рациональных функций и оценки параметров семейства хеш функций. В разделе 1 приводятся определение универсального хеширования по точкам алгебраической кривой и функциональное поле кривой. В разделе 2 представлены коллизионные свойства универсального хеширования, в разделе 3 – практический алгоритм вычисления хеш функции.

1. Определение универсального хеширования по кривой $x^{(q+1)/d}+x^{2(q+1)/d}+y^{q+1}=0$

Известные результаты [6]:

- Уравнение кривой в проективном пространстве P^2

$$F(X,Y,Z)=X^{(q+1)/d}Z^{(d-1)(q+1)/d}+X^{2(q+1)/d}Z^{(d-2)(q+1)/d}+Y^{q+1},$$

и в аффинном пространстве над F_{q^2}

$$x^{(q+1)/d}+x^{2(q+1)/d}+y^{q+1}=0.$$

- Кривая имеет $(q+1)^2+(q+1)(q-2)q/d$ F_{q^2}-рациональных точек, род $g=(q+1)(q-2)/2d+1$ и достигает границы Хассе-Вейля.
- Точками кривой являются особые точки: $P_\infty=(1:0:0)$ и $P_{0,0}=(0:0:1)$, простые точки $P_{a,b}=(a:b:1)$, где $a,b\in F_{q^2}$ и $a^{(q+1)/d}+a^{2(q+1)/d}=-b^{q+1}$.

- Подгруппа Вейерштрасса функционального поля кривой содержит подгруппу $H(P_\infty)=\langle 2(q+1)/d, q, q+1\rangle$.

Утверждение 1. Базис пространства $L(\rho_\ell P_\infty)$ функционального поля кривой $X^{(q+1)/d}Z^{(d-1)(q+1)/d}+X^{2(q+1)/d}Z^{(d-2)(q+1)/d}+Y^{q+1}$, задается функциями вида $\{v^i\cdot x^j\cdot y^t : iq+j(q+1)+t2(q+1)/d\le\rho_\ell\}$, где $x=X/Z$, $y=Y/Z$ и $div_\infty(v)=q$.

Доказательство. Кривой принадлежат особые точки $P_\infty=(1:0:0)$ кратности $(d-2)(q+1)/d$, $P_{0,0}=(0:0:1)$ кратности $(q+1)/d$ и $(q+1)/d$ простых точек $P_{\beta,0}=(\beta:0:1)$, $\beta\in F_{q^2}$. Частные производные имеют вид

$$F_X=(q+1)/d\cdot X^{(q+1)/d-1}Z^{(d-1)(q+1)/d},\ F_Y=(q+1)Y^q,$$
$$F_Z=(d-1)(q+1)/d\cdot X^{(q+1)/d}Z^{(d-1)(q+1)/d-1}+(d-2)(q+1)/d\cdot X^{2(q+1)/d}Z^{(d-2)(q+1)/d-1}$$

и $F_X=0$, $F_Y=0$, $F_Z=0$ в точках $P_\infty=(1:0:0)$ и $P_{0,0}=(0:0:1)$. Максимальный порядок, при котором частные производные не равны нулю, определяет кратность особых точек. Как следует из выражений для частных производных, точки $P_\infty=(1:0:0)$ и $P_{0,0}=(0:0:1)$ имеют кратности $(d-2)(q+1)/d$ и $(q+1)/d$. Точки $P_\infty=(1:0:0)$, $P_{0,0}=(0:0:1)$ и $P_{\beta,0}=(\beta:0:1)$ являются точками пересечения линии $\Re: Y=0$ с кривой $F(X,Y,Z)$. По теореме Безу кратность пересечения линии $\Re$ с кривой равна $q+1$, следовательно, имеем $(q+1)/d$ простых точек $P_{\beta,0}=(\beta:0:1)$ и $\Re\cdot F(X,Y,Z)=\sum_{\beta\in F_i}P_{\beta,0}+(q+1)/dP_{0,0}+(d-2)(q+1)/dP_\infty$.

Пусть $\aleph$ является линией с уравнением $X=0$. Тогда $\aleph$ пересекает кривую в одной точке $P_{0,0}$ и $\aleph\cdot F(X,Y,Z)=(q+1)P_{0,0}$.

Для линии $\Im$ с уравнением $Z=0$ справедливо пересечение кривой в точке $P_\infty=(1:0:0)$ и имеем $\Im\cdot F(X,Y,Z)_1=(q+1)P_\infty$. Для рациональных функций $x=X/Z$ и $y=Y/Z$ имеем следующие дивизоры

$$div(x)=(q+1)P_{0,0}-(q+1)P_\infty,\ div(y)=\sum_{\beta\in F_i}P_{\beta,0}+(q+1)/dP_{0,0}-2(q+1)/dP_\infty,$$

соответственно $div_\infty(x)=(q+1)P_\infty$ и $div_\infty(y)=2(q+1)/dP_\infty$ – значения полюсов дивизоров.

Функциональное поле кривой $X^{(q+1)/d}Z^{(d-1)(q+1)/d}+X^{2(q+1)/d}Z^{(d-2)(q+1)/d}+Y^{q+1}$ по рациональным функциям $x=X/Z$ и $y=Y/Z$ является не полным. Подгруппа Вейерштрасса точек не разрыва определяется значениями полюсов рациональных функций x и y, которые кратны $(q+1)/d$. Для полноты $H(P_\infty)$, аддитивную подгруппу следует дополнить значением полюса $div_\infty(v)=qP_\infty$ рациональной функции $v=f(X,Y,Z)$. Отсюда следует базис пространства $L(\rho_\ell P_\infty)$ функционального поля кривой в виде $\{v^i\cdot x^j\cdot y^t : iq+j(q+1)+t2(q+1)/d\le\rho_\ell\}$. ◊

Замечание 1.

1. Пусть $d=3$, $q=2(\mathrm{mod}3)$ и F_{q^2}. Имеем кривую $x^{(q+1)/3}+x^{2(q+1)/3}+y^{q+1}=0$ третьего рода $g_3=(q^2-q+4)/6$.

2. Кривая $x^{(q+1)/3}+x^{2(q+1)/3}+y^{q+1}=0$ в поле характеристики $p=2$ определена над F_{q^2}, для $q=2^{2t+1}$, $t=1,2,\ldots$.

3. Число точек кривой следует из подстановки рода в уравнение Хассе-Вейля для числа точек максимальных кривых.

4. Оценки дивизоров рациональных функции $x = X/Z$, $y = Y/Z$ пространства $L(\rho_t P_\infty)$ функционального поля кривой представлены в утверждении 1 впервые. Задача определения функции v с порядком полюса равным q требует решения.

5. Линейная серия $2(q+1)/d, q, q+1$ имеет размерность $\dim = 3$.

Определение 1. Хеш функция $h_{x,y}(m) \in F_{q^2}$ для сообщения m по рациональным функциям в точке x, y кривой $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$ определяется выражением

$$h_{x,y}(m) = \sum_{i,j,t} m_{i,j,t} \cdot v^i \cdot x^j \cdot y^t, \qquad (1)$$

где $i \geq 0, 0 \leq j \leq (q+1)/3 - 1, 0 \leq t \leq 2, iq + j(q+1) + t \cdot 2(q+1)/3 \leq \rho_k$, ρ_k полюс подгруппы Вейерштрасса $H(P_\infty)$ для k слова сообщения, $m_{i,j,t} \in F_{q^2}$ – слова сообщения m.

Замечание 2.

1. Хеш функция $h_{x,y}(m) \in F_{q^2}$ определена для кривой третьего рода наибольшего для данного вида кривых.

2. Индексация рациональных функций x, v и y в выражении (1) учитывает отношение порядков полюсов функций и справедливость такой индексации показана в лемме 1 и предложении 1.

Пример 1. Пусть задано F_{3^4}. Кривая $x^2 z^8 + x^4 z^6 + y^{10} = 0$ имеет род $g = 8$ и $d = 5$. Число точек кривой в P^2 равно $N = (q+1)^2 + (q+1)(q-2)q/d = 226$. Значения полюсов дивизоров рациональных функций равны $div_\infty(x) = 10P_\infty$, $div_\infty(y) = 4P_\infty$ и $div_\infty(v) = 9P_\infty$. Подгруппа Вейерштрасса точек не разрыва определяется значениями полюсов $H(P_\infty) = \langle 4,9,10 \rangle$ и имеет вид $\{0,4,8,9,10,12,13,14,16,17,...\}$. Точки разрыва определяются множеством $G(P_\infty) = \{1,2,3,5,6,7,11,15\}$, их число $|G(P_\infty)| = 8$ и равняется значению рода $g = (q+1)(q-2)/2d + 1 = 8$. Линейная серия $4,9,10$ является полной.

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

Лемма 1. Пусть $d = 3$ и $k < (q^2 - q + 4)/6$, тогда для кривой третьего рода $i = s' - j - 1$, $j = k'' - s'(s'-1)/2 - 1$, $t = s - s' + 1$, $s = \lfloor (2k' + 1/4)^{1/2} - 1/2 \rfloor$, $s' = \lfloor (2k'' + 1/4)^{1/2} - 1/2 \rfloor$, $k' = \lceil k/3 \rceil$, $k'' = k - 3(s-1)s/2 + (s-1)(s-2)/2$, где $\lceil \cdot \rceil$ – округление к большему целому числу.

Доказательство. Аддитивная подгруппа Вейерштрасса $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < ...\}$ кривой $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$ определяется значениями полюсов $\rho_1 = 2(q+1)/3$, $\rho_2 = q$ и $\rho_3 = q+1$.

Рассмотрим пример кривой $x^{11} + x^{22} + y^{33} = 0$ над полем $F_{2^{10}}$, $q = 2^5$. Размещение полюсов рациональных функций базисного пространства $L(\rho_t P_\infty)$ подгруппы Вейерштрасса $H(P_\infty) = \langle 22,32,33 \rangle$ представлено в табл. 1. Полюса подгруппы Вейерштрасса $H(P_\infty) = \langle 22,32,33 \rangle$ делятся на уровни, каждый представляется тремя строками с возрастающими по порядку полюсами.

Рассмотрим третий уровень. Значения полюсов первой строки третьего уровня определяются полюсами рациональных функций третьей строки первого уровня, т.е. функциями x и v, и полюсом функции y^2.

Таблица 1

Размещение полюсов подгруппы Вейерштрасса $H(P_\infty)=\langle 22,32,33\rangle$

Значения полюсов					Номер уровня
				ρ_0=0	**0**
				ρ_1=22	
			ρ_3=33	ρ_2=32	**1**
				ρ_4=44	
			ρ_6=55	ρ_5=54	
		ρ_9=66	ρ_8=65	ρ_7=64	**2**
			ρ_{11}=77	ρ_{10}=76	
		ρ_{14}=88	ρ_{13}=87	ρ_{12}=86	
	ρ_{18}=99	ρ_{17}=98	ρ_{16}=97	ρ_{15}=96	**3**
		ρ_{21}=110	ρ_{20}=109	ρ_{19}=108	
	ρ_{25}=121	ρ_{24}=120	ρ_{23}=119	ρ_{22}=118	
ρ_{30}=132	ρ_{29}=131	ρ_{28}=130	ρ_{27}=129	ρ_{26}=128	**4**
…	…	…	…	…	

Таким образом, первая строка третьего уровня определяется полюсами функций $v\cdot y^2$ и $x\cdot y^2$, по возрастанию. Для второй строки третьего уровня получим полюса функций $v^2\cdot y$, $v\cdot x\cdot y$ и $x^2\cdot y$. Третья строка третьего уровня определяется полюсами функций v^3, $v^2\cdot x$, $v\cdot x^2$ и x^3.

Для i-уровня получим полюса следующих функций:

- $v^{s-2}\cdot y^2$, $v^{s-3}\cdot x\cdot y^2$,..., $x^{s-2}\cdot y^2$ – 1-я строка;
- $v^{s-1}\cdot y$, $v^{s-2}\cdot x\cdot y$,..., $x^{s-1}\cdot y$ – 2-я строка;
- v^s, $v^{s-1}\cdot x$,..., x^s – 3-я строка.

Число полюсов на каждом уровне кратно $d=3$. Число уровней равно $(q+1)/3=11$.

В общем случае размещение полюсов ρ_t в порядке возрастания в подгруппе $H(P_\infty)$ для кривой $x^{(q+1)/3}+x^{2(q+1)/3}+y^{q+1}=0$ представлено в табл. 2.

Таблица 2

Размещение полюсов подгруппы Вейерштрасса $H(P_\infty)=\langle 2(q+1)/3,q,q+1\rangle$

Значения полюсов				Номер уровня
			ρ_0=0	0
			$\rho_1=\varphi=2(q+1)/3$	
		$\rho_3=\eta=q+1$	$\rho_2=\gamma=q$	1
			$\rho_4=2\varphi$	
		$\rho_6=\eta+\varphi$	$\rho_5=\gamma+\varphi$	
	$\rho_9=2\eta$	$\rho_7=\eta+\gamma$	$\rho_7=2\gamma$	2
		$\rho_{11}=\eta+2\varphi$	$\rho_{10}=\gamma+2\varphi$	
	$\rho_{14}=\eta+\varphi$	$\rho_{13}=\eta+\gamma+\varphi$	$\rho_{12}=2\gamma+\varphi$	
$\rho_{18}=3\eta$	$\rho_{16}=2\eta+\gamma$	$\rho_{16}=\eta+2\gamma$	$\rho_{15}=3\gamma$	3
…	…	…	…	
	$\rho_{3(s-1)s/2+(2-t)(s-1)+(2-t)(2-t-1)/2+i+1}=iq+j(q+1)+2t(q+1)/3$			s

Значение k определяется выражением

$$k = 3(s-1)s/2 + (2-t)(s-1) + (2-t)(2-t-1)/2 + i + 1. \qquad (2)$$

Нормировка k по 3 даёт $k' = \lceil k/3 \rceil = (s-1)s/2$ и $s = \left| (2k'+1/4)^{1/2} - 1/2 \right|$. Для определения строки t размещения полюса ρ_k на уровне s выполним дополнение арифметического ряда членами $1,2,\ldots,s-2$. Далее имеем $k - 3(s-1)s/2 + (s-1)(s-2)/2 = k''$ и вычисление $s' = \left| (2k''+1/4)^{1/2} - 1/2 \right|$ даёт $t = s - s' + 1$. Индекс j следует из выражения $j = k'' - s'(s'-1)/2 - 1$ и $i = s' - j - 1$.

◊

Пример 3. Пусть кривая $x^{11} + x^{22} + y^{33} = 0$ определена над $F_{2^{10}}$, $q = 2^5$. Полюса представлены таблицей 1. Вычислить значение полюса ρ_k.

Пусть $k = 15$. Имеем

$k' = \lceil k/3 \rceil = \lceil 15/3 \rceil = 5$, $s = \left| (2k'+1/4)^{1/2} - 1/2 \right| = \left| (2\cdot 5 + 0.25)^{1/2} - 0.5 \right| = 3$,

$k'' = k - 3(s-1)s/2 + (s-1)(s-2)/2 = 15 - 9 + 1 = 7$,

$s' = \left| (2k''+1/4)^{1/2} - 1/2 \right| = \left| (2\cdot 7 + 0/25)^{1/2} - 0.5 \right| = 4$,

$t = s - s' + 1 = 3 - 4 + 1 = 0$, $j = k'' - s'(s'-1)/2 - 1 = 7 - 4(4-1)/2 - 1 = 0$,

$i = s' - j - 1 = 4 - 0 - 1 = 3$.

Получим значение полюса $\rho_{15} = iq + j(q+1) + t\cdot 2(q+1)/3 = 3\cdot 16 = 48$, что совпадает со значением в табл. 1.

Замечание 3. Для случая кривых с $d > 3$ соотношения между значением k и показателями i, j, t степеней рациональных функций v, x, y являются более сложными. Общего решения для показателей степеней i, j, t для произвольного значения d не существует. Рассмотрим кривую $x^4 z^{16} + x^8 z^{12} + y^{20} = 0$ над полем F_{19^2}, $d = 5$. Значения полюсов подгруппы Вейерштрасса $H(P_\infty) = \langle 8,19,20 \rangle$ представлены в табл. 3.

Таблица 3

Размещение полюсов подгруппы Вейерштрасса $H(P_\infty) = \langle 8,19,20 \rangle$

Значения полюсов			Номер уровня
		ρ_0=0	0
		ρ_1=4	0’
		ρ_2=8	
	ρ_4=10	ρ_3=9	1
		ρ_5=12	
	ρ_7=14	ρ_6=13	1’
		ρ_8=16	
		ρ_9=17	
ρ_{12}=20	ρ_{11}=19	ρ_{10}=18	2
		ρ_{13}=21	
ρ_{16}=24	ρ_{15}=23	ρ_{14}=22	2’
		ρ_{17}=25	
		ρ_{18}=26	
ρ_{21}=29	ρ_{20}=28	ρ_{19}=27	3
		ρ_{22}=30	
ρ_{25}=33	ρ_{24}=32	ρ_{23}=31	3’
…	…	…	

На каждом уровне имеется два подуровня. Если для случая $d = 3$ полюса уровней образуют геометрическую фигуру трапецию, тогда при $d = 5$ имеем фигуру в виде усеченной пирамиды. Это усложняет подсчет числа полюсов на уровнях $H(P_\infty)$.

2. Оценка параметров универсального хеширования.

Утверждение 1. Хеширование по рациональным функциям кривой $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$ над полем F_{q^2}, определяет универсальный хеш класс $\varepsilon - U((q^3 + 2q^2 + 4q + 3)/3, q^{2k}, q^2)$, где $(q^3 + 2q^2 + 4q + 3)/3$ – число хеш функций (объём ключевого пространства), q^{2k} – объём пространства сообщений, q^2 – объём пространства хеш кодов. Вероятность коллизии ε определяется соотношениями

$$\varepsilon = (3iq + 3j(q+1) + t \cdot 2(q+1))/(q^3 + 2q^2 + 4q + 3), \text{ если } k < \left(q^2 - q + 4\right)/6, \quad (3)$$

$$\varepsilon = 3(k + \left(q^2 - q + 4\right)/6)/(q^3 + 2q^2 + 4q + 3), \text{ если } k \geq \left(q^2 - q + 4\right)/6, \quad (4)$$

где $i = s' - j - 1$, $j = k'' - s'(s'-1)/2 - 1$, $t = s - s' + 1$, $s = \left|(2k' + 1/4)^{1/2} - 1/2\right|$, $s' = \left|(2k'' + 1/4)^{1/2} - 1/2\right|$, $k' = \lceil k/3 \rceil$, $k'' = k - 3(s-1)s/2 + (s-1)(s-2)/2$.

Доказательство. Параметры универсального класса по рациональным функциям кривой $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$ следуют из определения кривой и числа её точек в F_{q^2}.

Вероятность коллизии ε определяется соотношением $\varepsilon = \rho_k / N$, где $\rho_k = iq + j(q+1) + t2(q+1)/3$ – значение полюса рациональной функции $f_k = v^i \cdot x^j \cdot y^t$, i, j, t определяются по лемме 1, $N = (q^3 + 2q^2 + 4q + 3)/3$ – число точек кривой.

Пусть $k < \left(q^2 - q + 4\right)/6$. По лемме 1 имеем $i = s' - j - 1$, $j = k'' - s'(s'-1)/2 - 1$, $t = s - s' + 1$, $s = \left|(2k/3 + 1/4)^{1/2} - 1/2\right|$, $s' = \left|(2k'' + 1/4)^{1/2} - 1/2\right|$ $k'' = k - 3(s-1)s/2 + (s-1)(s-2)/2$.

В случае $k = \left(q^2 - q + 4\right)/6$, имеем $\rho_k = 2g = (q^2 - q + 4)/3$ и $\varepsilon = 2g/N$ что согласуется с (4). С другой стороны $\rho_k = iq + j(q+1) + t2(q+1)/3$ и подстановка $t = 2$, $j = 0$, $i = (q+1)/3 - 2$ дает проверку

$$\rho_k = iq + j(q+1) + t2(q+1)/3 = (q+1)q/3 - 2q + 4(q+1)/3 = (q^2 - q + 4)/3.$$

Пусть $k > \left(q^2 - q + 4\right)/6$. Заметим, что $\rho_k = k + \left(q^2 - q + 4\right)/6$. Прямое вычисление $\varepsilon = \rho_k / N$ дает выражение (4). ◊

Пример 4. Пусть кривая $x^{11} + x^{22} + y^{33} = 0$ определена над $F_{2^{10}}$, $q = 2^5$. Пусть $k = (q^2 - q + 4)/6 = 166$. Имеем

$k' = \lceil k/3 \rceil = \lceil 166/3 \rceil = 56$, $s = \left|(2k' + 0.25)^{1/2} - 1/2\right| = \left|(2 \cdot 56 + 0.25)^{1/2} - 0.5\right| = 11$,

$k'' = k - 3(s-1)s/2 + (s-1)(s-2)/2 = 166 - 165 + 45 = 46$,

$s' = \left|(2k'' + 0.25)^{1/2} - 1/2\right| = \left|(2 \cdot 46 + 0{,}25)^{1/2} - 0.5\right| = 10$,

$t = s - s' + 1 = 11 - 10 + 1 = 2$, $j = k'' - s'(s'-1)/2 - 1 = 46 - 10(10-1)/2 - 1 = 0$,

$i = s' - j - 1 = 10 - 0 - 1 = 9$.

Тогда $\rho_{166} = k + \left(q^2 - q + 4\right)/6 = 332$ и $\varepsilon = \rho_k / N \approx 0.028$.

Замечание 4.

1. Выражения для вероятности коллизии для универсального хеширования по рациональным функциям кривой $x^{(q+1)/3}+x^{2(q+1)/3}+y^{q+1}=0$ представлены впервые.

2. Пусть $k=q(q-1)/2$. Подстановка в (4) дает

$$\varepsilon=3(q(q-1)/2+(q^2-q+4)/6)/(q^3+2q^2+4q+3)\approx 2\varepsilon_{ЭК}, \quad (5)$$

где $\varepsilon_{ЭК}=1/q+1/q^2$ – значение вероятности коллизии универсального хеширования по кривой Эрмита при $k=q(q-1)/2$ [3]. Из оценки (5) следует проигрыш в 2 раза по вероятности коллизии хешированию по кривой Эрмита. Размер ключевых данных $N=(q^3+2q^2+4q+3)/3$ по сравнению с хешированием по Эрмита меньше почти в 3 раза. Это приводит к уменьшению в 3 раза максимально возможного числа хешируемых слов.

3. Для $k<(q^2-q+4)/6$ отличие по вероятности коллизии хеширования по кривым $x^{(q+1)/3}+x^{2(q+1)/3}+y^{q+1}=0$ и Эрмита будет несущественным. Действительно размер ключевых данных уменьшается в 3 раза, но для одного и того же k, значение полюса ρ_k в силу нормировки $k'=\lceil k/3\rceil$ приблизительно в 3 раза меньше по сравнению с хешированием по кривой Эрмита.

3. Практический алгоритм вычисления хеш кода.

Предложение 1. Сложность универсального хеширования по кривым $x^{(q+1)/3}+x^{2(q+1)/3}+y^{q+1}=0$ в F_{q^2} определяется выражением

$$N_{опер}=k+s+3, \text{ если } k<(q^2-q+4)/6, \quad (6)$$

$$N_{опер}=k+(q+1)/3+3, \text{ если } k\ge(q^2-q+4)/6, \quad (7)$$

где $s=\left|(2k'+1/4)^{1/2}-1/2\right|$, $k'=\lceil k/3\rceil$.

Доказательство. Универсальное хеширование определяется выражением (1). Базис пространства $L(\rho_k P_\infty)$, задается функциями вида $\{v^i\cdot x^j\cdot y^t : iq+j(q+1)+t2(q+1)/d\le\rho_k\}$. Размещение полюсов подгруппы Вейерштрасса $H(P_\infty)=\langle 2(q+1)/3, q, q+1\rangle$ определяется табл. 2.

Пусть $k<(q^2-q+4)/6$. Члены суммы в выражении $h_{x,y}(m)$ можно представить трёхмерным массивом $H_{x,v,y}$ по возрастанию полюсов рациональных функций $x^j\cdot v^i\cdot y^t$ в виде табл. 4.

Таблица 4

Рациональные функции $x^j\cdot v^i\cdot y^t$ в выражении $h_{x,y}(m)$

1	2	3	4	5	6	7
					$x^0v^0y^0m_{0,0,0}$	**0**
					$x^0v^0y^1m_{0,0,1}$	
				$x^1v^0y^0m_{1,0,0}$	$x^0v^1y^0m_{0,1,0}$	**1**
					$x^0v^0y^2m_{0,0,2}$	
				$x^1v^0y^1m_{1,0,1}$	$x^0v^1y^1m_{0,1,1}$	

Окончание табл. 4

1	2	3	4	5	6	7
			$x^2v^0y^0m_{2,0,0}$	$x^1v^1y^0m_{1,1,0}$	$x^0v^2y^0m_{0,2,0}$	**2**
				$x^1v^0y^2m_{1,0,2}$	$x^0v^1y^2m_{0,1,2}$	
			$x^2v^0y^1m_{2,0,1}$	$x^1v^1y^1m_{1,1,1}$	$x^0v^2y^1m_{0,2,1}$	
		$x^3v^0y^0m_{3,0,0}$	$x^2v^1y^0m_{2,1,0}$	$x^1v^2y^0m_{1,2,0}$	$x^0v^3y^0m_{0,3,0}$	**3**
		$x^{s-2-i}v^iy^1m_{s-2-i,i}$	…	$x^1v^{s-3}y^2m_{1,s-3,2}$	$x^0v^{s-2}y^2m_{0,s-2,2}$	
		$x^{s-1-i}v^iy^1m_{s-1-i,i,1}$	…	$x^1v^{s-2}y^1m_{1,s-2,1}$	$x^0v^{s-1}y^1m_{0,s-1,1}$	
$x^sv^0y^0m_{s,0,0}$	…	$x^{s-i}v^iy^0m_{s-i,i,0}$	…	$x^1v^{s-1}y^0m_{1,s-1,0}$	$x^0v^sy^0m_{0,s,0}$	s

где $s=\left|(2k'+1/4)^{1/2}-1/2\right|$, $k'=\lceil k/3\rceil$.

Сумма элементов матрицы даёт значение $h_{x,y}(m)$. Группировка слагаемых по строкам и столбцам матрицы приводит к следующему порядку вычислений

$$h_{x,y}(m)=y^0(x^0v^0m_{0,0,0}+x^1v^0m_{1,0,0}+x^0v^1m_{0,1,0}+\ldots+x^sv^0m_{s,0,0}+x^{s-1}v^1m_{s-1,1,0}+\ldots+x^0v^sm_{0,s,0})+$$
$$y^1(x^0v^0m_{0,0,1}+x^1v^0m_{1,0,1}+x^0v^1m_{0,1,1}+\ldots+x^{s-1}v^0m_{s-1,0,1}+x^{s-2}v^1m_{s-2,1,1}+\ldots+x^0v^{s-1}m_{0,s-1,1})+\ldots$$

$$+y^2(x^0v^0m_{0,0,2}+x^1v^0m_{1,0,2}+x^0v^1m_{0,1,2}+\ldots+x^{s-2}v^0m_{s-2,0,2}+x^{s-2}v^1m_{s-2,1,2}+\ldots+x^0v^{s-2}m_{0,s-2,2}.$$

Выражения в скобках определяется схемой вычисления Горнера для $h_{x,y}(m)$. Окончательное выражение будет иметь вид

$$h_{x,y}(m)=\sum_{t=0}^{2}y^t\cdot\sum_{j=0}^{s-t}x^j\sum_{i=0}^{s-t-j}m_{j,i,t}v^i, \qquad (8)$$

где $s=\left|(2k'+1/4)^{1/2}-1/2\right|$, $k'=\lceil k/3\rceil$.

Выражение (8) определяет, что $h_{x,y}(m)$ можно вычислить по схеме Горнера, последовательно для трёх сумм. Сложность хеширования составит $N_{опер}=k+s+3$ операций умножений и сложений в F_{q^2}.

Пусть $k\geq\left(q^2-q+4\right)/6$. Параметр s первой суммы в выражении $h_{x,y}(m)$ (8) определяется значением $s=(q+1)/3$. Сложность вычисления внутренней суммы в (8) составит k операций, а внешних – $(q+1)/3$ и 3 операций умножений и сложений в F_{q^2}, что определяет (7). ◊

Замечание 5.

1. Результаты предложения 1 являются новыми и представлены впервые.

2. Асимптотика оценки сложности универсального хеширования по кривым $x^{(q+1)/3}+x^{2(q+1)/3}+y^{q+1}=0$ при $k<\left(q^2-q+4\right)/6$ определяется $N_{опер}=k+(k/3)^{1/2}+3$, так как $s=\left|(2k'+1/4)^{1/2}-1/2\right|$, $k'=\lceil k/3\rceil$. Результат совпадает с оценкой сложности

хеширования по кривой третьего рода $y^{3^{l-1}} + y^{3^{l-2}} + ... + y = \omega x^{3^l+1}$, $g_3 = q(q-3)/6$ в поле характеристики $p = 3$ и лучше, чем при хешировании по кривым Эрмита ($N_{опер}(HC) = k + k^{1/2}$ (см. [3]).

Выводы. Универсальное хеширование по кривой $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$ третьего рода определено над полем характеристики 2, хорошо согласуется с битовым представлением данных, несколько уступает по вероятности коллизии хешированию по кривым Эрмита и имеет меньшую сложность вычисления. Задача определения рациональной функции порядка q для построения базиса функционального пространства кривой требует решения.

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 алгеброгеометрических кодов. / Халимов Г.З.,. Кузнецов А.А. //Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2001. – Вып. 120.- С. 103-109.

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

4. Халимов Г.З. Оценка параметров кривых Гурвица для целей универсального хеширования. / Халимов Г.З. // Сборник трудов I Международной научно-технической конференции "Компьютерные науки и технологии" (Белгород, Россия, 8-10 октября 2009). – 2009. –.Ч. 2. – С. 118-121.

5. Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования / Халимов Г.З.//Материалы XI Международной научно-практической конференции «Информационная безопасность» (Таганрог, Россия, 23-25 июня 2010), ТТИ ЮФУ. – 2010. – Ч. 3. – С. 144-146.

6. Cossidente A. Curves of large genus covered by the Hermitian curve / Cossidente A., Korchmaros G. and Torres F. // Commutative Algebra. – 2000. – Vol. 28, No. 10. – P. 4707–4728.

UNIVERSAL HASHING ON MAXIMUM CURVE OF THE THIRD GENUS

G.Z. KHALIMOV

Kharkiv National University of Radio Electronics

e-mail: gennadykhalimov@mail.ru

Presents the results of universal hashing on the maximum curve of the form $x^{(q+1)/d} + x^{2(q+1)/d} + y^{q+1} = 0$ defined over finite field F_{q^2}. Consider a projective variety of points of the curve, the field of rational functions and estimate the parameters of a family of hash functions.

Key words: universal hashing, algebraic curves.