УДК 681.3.06

Г. З. ХАЛИМОВ, канд. техн. наук

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО РАЦИОНАЛЬНЫМ ФУНКЦИЯМ МАКСИМАЛЬНОЙ КРИВОЙ ТРЕТЬЕГО РОДА

Для построения хеш функций используются вычисления в функциональном поле алгебраических кривых. Свойства линейного пространства по рациональным функциям алгебраической кривой определяются фундаментальной теоремой Римана – Роха и связываются с алгеброгеометрическими параметрами кривой. Первые оценки универсального хеширования по проективной линии, кривым Эрмита, Гурвица и Сузуки представлены в [1 – 4]. Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на границе Хассе – Вейля. Классификация максимальных кривых представлена в [5]. Кривая $\omega x^{(q-1)/d} - yx^{2(q-1)/d} + y^q = 0$ в квадратичном поле F_{q^2} в случае $d = 3$, $q = 1(\mathrm{mod}3)$ является третьей по значению рода после кривой Эрмита.

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

1. Функциональное поле кривой $\omega x^{(q-1)/d} - yx^{2(q-1)/d} + y^q = 0$

Известные результаты [5]:

- Уравнение кривой в проективном пространстве P^2

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

- и в аффинном пространстве над F_{q^2}

$$\omega x^{(q-1)/d} - yx^{2(q-1)/d} + y^q = 0,$$

где $q \equiv 1(\mathrm{mod}3)$, $\omega \in F_{q^2}$, $\omega^{q-1} = -1$.

- Кривая имеет род $g = q(q-1)/2d$, число F_{q^2}-рациональных точек равно $q^2(q-1)/d + q^2 - (q-1)/d - 1$ и достигает границы Хассе – Вейля.

- Точками кривой являются особые точки: $P_\infty = (1:0:0)$, $P_{0,0} = (0:0:1)$ и простые точки $P_{a,b} = (a:b:1)$, где $a,b \in F_{q^2}$ и $\omega a^{(q-1)/d} - ba^{2(q-1)/d} + b^q = 0$.

- Подгруппа Вейерштрасса функционального поля кривой третьего рода содержит подгруппу $H(P_\infty) = \langle (2q+1)/3, q, q+1 \rangle$.

Замечание 1.

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

2. Кривая $\omega x^{(q-1)/d} - yx^{2(q-1)/d} + y^q = 0$ в поле характеристики $p = 2$ определена над F_{q^2}, для $q = 2^{2t}$, $t = 1,2,...$ и приводится к виду $x^{(q-1)/d} + yx^{2(q-1)/d} + y^q = 0$.

3. В поле характеристики $p=2$ имеем $\omega=1$. В случае $p\neq 2$, $\alpha^{(q^2-1)/2}=-1$, $\omega=\alpha^{(q+1)/2}$, где $\alpha\in F_{q^2}$ порядка q^2-1.

4. Число точек кривой определяется выражением Хассе – Вейля для максимальных кривых. Исследования точек $P_{0,0}=(0:0:1)$ и $P_\infty=(1:0:0)$ показывают следующее. Кратность особой точки $P_{0,0}=(0:0:1)$ равна $(q-1)/d$. Это следует из оценки частных производных F_X, F_Y, F_Z. Точка на бесконечности $P_\infty=(1:0:0)$ имеет коэффициент ветвления 2. Из выражения Хассе – Вейля для числа точек максимальной кривой вычтем особые точки с учетом их кратности и получим число точек кривой $P_{a,b}=(a:b:1)$, $a,b\neq 0, a,b\in F_{q^2}$

$$N=q^2(q-1)/d+q^2-(q-1)/d-1. \tag{1}$$

5. Подгруппа Вейерштрасса функционального поля кривой третьего рода $g_3=q(q-1)/6$ и $d=3$ имеет размерность $\dim=3$, содержит подгруппу $H(P_\infty)=\langle(2q+1)/3,q,q+1\rangle$ [5].

6. Для произвольного $d>3$, $q\equiv 1(\mathrm{mod}\,d)$ подгруппа Вейерштрасса принимает значения

$$H(P_\infty)=\langle(2(q-1)/d+1,q-1,q\rangle \tag{2}$$

или

$$H(P_\infty)=\langle(2(q-1)/d+1,q-2,q\rangle, \tag{3}$$

если $((2(q-1)/d+1)n=q-1$. Этот результат является новым.

Пример 1. Пусть $q=7$ и задано F_{7^2}. Кривая $\alpha^4x^2z^5+\alpha^{24}x^4yz^2+y^7=0$ имеет род $g=7$ и $d=3$. Это случай кривой третьего рода. Выражение Хассе – Вейля определяет число точек кривой в P^2 $N=q^2+2gq+1=148$. Точные вычисления точек $P_{a,b}=(a:b:1)$, $a,b\neq 0, a,b\in F_{7^2}$ приводят к значению $N=144$, без двух особых точек $P_{0,0}, P_\infty$, что совпадает с выражением (1). Подгруппа Вейерштрасса точек неразрыва определяется значениями полюсов $H(P_\infty)=\langle 5,7,8\rangle$ и имеет вид $\{0,5,7,8,10,12,13,14,...\}$. Точки разрыва определяются множеством $G(P_\infty)=\{1,2,3,4,6,9,11\}$, их число $|G(P_\infty)|=7$ и равняется значению рода $g=q(q-1)/2d=7$. Линейная серия 5,7,8 является полной.

Пример 2. Пусть $q=2^4$. Делители $q-1=3\cdot 5$. Рассмотрим кривую $x^3z^{13}+x^6yz^9+y^{16}=0$ над F_{2^8}, $d=5$. Род кривой $g=24$. Число точек кривой в P^2 по формуле Хассе – Вейля $N=1025$. Точные вычисления числа F_{q^2} рациональных точек приводят к значению $N=1020$, что совпадает с выражением (1). Подгруппа Вейерштрасса точек неразрыва определяется выражением (2) $H(P_\infty)=\langle 7,15,16\rangle$ и имеет вид $\{0,7,14,15,16,21,22,23,248,19,30,31,32,35,36,37,38,39,42,43,44,45,46,47,48,...\}$. Число точек разрыва $|G(P_\infty)|=24$ и равняется значению рода. Линейная серия 5,15,16 является полной.

Пример 3. Пусть $q=11$. Делители $q-1=2\cdot 5$. Рассмотрим кривую $\alpha^6x^2z^9+\alpha^{60}x^4yz^6+y^{11}=0$ над F_{11^2}, $d=5$. Род кривой $g=11$. Число точек кривой в P^2 по формуле Хассе – Вейля $N=364$. Точные вычисления числа F_{q^2} рациональных точек приводят к значению $N=360$, что совпадает с выражением (1). Подгруппа

Вейерштрасса точек неразрыва определяется выражением (3) $H(P_\infty)=\langle 5,9,11\rangle$, так как $((2(q-1)/5+1)2=q-1$ и имеет вид $\{0,5,9,10,11,14,15,16,18,19,20,21,23,24,...\}$. Число точек разрыва $|G(P_\infty)|=11$ и равняется значению рода. Линейная серия 5,9,11 является полной.

Утверждение 1. Базис пространства $L(\rho_\ell P_\infty)$ функционального поля кривой

$$\omega X^{(q-1)/3}Z^{(2q+1)/3}-X^{2(q-1)/3}YZ^{(q-1)/3}+Y^q$$

задается функциями вида $\{x^i\cdot v^j\cdot y^t : iq+j(q+1)+t(2q+1)/3\le\rho_\ell\}$, где $x=X/Z$, $y=Y/Z$ и $div_\infty(v)=q+1$.

Доказательство. Кривая $F(X,Y,Z)=\omega X^{(q-1)/3}Z^{(2q+1)/3}+YX^{2(q-1)/3}Z^{(q-1)/3}+Y^q$ является F_{q^2} изоморфной кривой Эрмита (§2 [5]). Это кривая третьего рода и $g_3<(q-1)^2/4$. Размерность линейной серии подгруппы Вейерштрасса функционального поля кривой в этом случае равна $\dim=3$ и первые три положительных числа подгруппы Вейерштрасса $H(P)$, $P\in F(X,Y,Z)$ удовлетворяют условию (§5 [5])

$$m_1(P)<m_2(P)\le q<m_3(P). \tag{4}$$

Над полем F_{q^2} справедливо $m_2(P)=q$ и $m_1(P)\ge q/2$. Вычисления R. Fuhrmann ([6] предложение 1.5) определяют основную подгруппу в виде $\langle m,q,q+1\rangle$, а предложение 5.1 [5] устанавливает $m_1(P)=(2q+1)/3$, $q\equiv 1(\mathrm{mod}\,3)$.

Пусть $\aleph$ является линией с уравнением $X=0$. Тогда $\aleph$ пересекает кривую в одной точке $P_{0,0}$ и $\aleph\cdot F(X,Y,Z)=qP_{0,0}$. Для линии $\Im$ с уравнением $Z=0$ справедливо пересечение кривой в точке $P_\infty=(1:0:0)$; $\Im\cdot F(X,Y,Z)_1=qP_\infty$. Для рациональной функций $x=X/Z$ имеем дивизор $div(x)=qP_{0,0}-qP_\infty$. Полюс рациональной функций $x=X/Z$ определяет значение $m_2(P)=q$. Рациональная функция $y=Y/Z$ не может иметь полюс $div_\infty(y)=(q+1)P_\infty$, так как такое распределение полюсов соответствует кривой Эрмита. Следовательно, имеем $div_\infty(y)=(2q+1)/3P_\infty$ и $m_1(P)=(2q+1)/3$.

Размерность линейной серии подгруппы Вейерштрасса $\dim=3$ и функциональное поле $x=X/Z$ и $y=Y/Z$ следует дополнить функцией $v=f(X,Y,Z)$ с полюсом $div_\infty(v)=(q+1)P_\infty$.◊

Замечание 2. Задача определения функции v с порядком полюса, равным $q+1$, требует решения. Оценки дивизоров рациональных функции $x=X/Z$, $y=Y/Z$ пространства $L(\rho_\ell P_\infty)$ функционального поля кривой представлены в утверждении 1 впервые.

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

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

$$h_{x,y}(m)=\sum_{i,j,t} m_{i,j,t}\cdot x^i\cdot v^j\cdot y^t, \tag{5}$$

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

Замечание 3.

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

2. Индексация рациональных функций x, v и y в выражении (5) учитывает отношение порядков полюсов функций и справедливость такой индексации показана в лемме 1 и предложении 1.

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

Доказательство. Аддитивная подгруппа Вейерштрасса $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < \ldots\}$ кривой $\omega X^{(q-1)/3} Z^{(2q+1)/3} - X^{2(q-1)/3} Y Z^{(q-1)/3} + Y^q$ определяется значениями полюсов $\rho_1 = (2q+1)/3$, $\rho_2 = q$ и $\rho_3 = q+1$. Рассмотрим пример кривой $x^5 + x^{10} y + y^{16} = 0$ над полем F_{2^8}, $q = 2^4$. Размещение полюсов рациональных функций базисного пространства $L(\rho_\ell P_\infty)$ подгруппы Вейерштрасса $H(P_\infty) = \langle 11, 16, 17 \rangle$ имеет следующий вид (табл. 1).

Таблица 1

Значения полюсов подгруппы Вейерштрасса $H(P_\infty) = \langle 22, 32, 33 \rangle$						Номер уровня
					ρ_0=0	0
					ρ_1=11	
				ρ_3=17	ρ_2=16	1
					ρ_4=22	
				ρ_6=28	ρ_5=27	
			ρ_9=34	ρ_8=33	ρ_7=32	2
				ρ_{11}=39	ρ_{10}=38	
			ρ_{14}=45	ρ_{13}=44	ρ_{12}=43	
		ρ_{18}=51	ρ_{17}=50	ρ_{16}=49	ρ_{15}=48	3
			ρ_{21}=56	ρ_{20}=55	ρ_{19}=54	
		ρ_{25}=62	ρ_{24}=61	ρ_{23}=60	ρ_{22}=59	
	ρ_{30}=68	ρ_{29}=67	ρ_{28}=66	ρ_{27}=65	ρ_{26}=64	4
		ρ_{34}=73	ρ_{33}=72	ρ_{32}=71	ρ_{31}=70	
	ρ_{39}=79	ρ_{38}=78	ρ_{37}=77	ρ_{36}=76	ρ_{35}=75	
ρ_{45}=85	ρ_{44}=84	ρ_{43}=83	ρ_{42}=82	ρ_{41}=81	ρ_{40}=80	5
	...	...	...	...	...	

Полюса подгруппы Вейерштрасса $H(P_\infty) = \langle 11, 16, 17 \rangle$ в табл. 1 делятся на строки и уровни, число уровней $(q-1)/3 = 5$.

В общем случае размещение полюсов ρ_ℓ в порядке возрастания в подгруппе $H(P_\infty)$ для кривой $\omega X^{(q-1)/3} Z^{(2q+1)/3} - X^{2(q-1)/3} Y Z^{(q-1)/3} + Y^q$ представлено в табл. 2.

Так как $\rho_1 = (2q+1)/d$, имеем

$$\rho_{3(s-1)s/2 + (2-t)(s-1) + (2-t)(2-t-1)/2 + i + 1} = iq + j(q+1) + t \cdot (2q+1)/3.$$

Значение k определяется выражением

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

Таблица 2

Значения полюсов подгруппы Вейерштрасса $H(P_\infty) = \langle (2q+1)/3, q, q+1 \rangle$				Номер уровня
			$\rho_0=0$	0
			$\rho_1=\phi=(2q+1)/3$	
		$\rho_3=\eta=q+1$	$\rho_2=\gamma=q$	1
			$\rho_4=2\phi$	
		$\rho_6=\eta+\phi$	$\rho_5=\gamma+\phi$	
	$\rho_9=2\eta$	$\rho_7=\eta+\gamma$	$\rho_7=2\gamma$	2
		$\rho_{11}=\eta+2\phi$	$\rho_{10}=\gamma+2\phi$	
	$\rho_{14}=\eta+\phi$	$\rho_{13}=\eta+\gamma+\phi$	$\rho_{12}=2\gamma+\phi$	
$\rho_{18}=3\eta$	$\rho_{16}=2\eta+\gamma$	$\rho_{16}=\eta+2\gamma$	$\rho_{15}=3\gamma$	3
...	...	...	...	
	$\rho_{3(s-1)s/2+(2-t)(s-1)+(2-t)(2-t-1)/2+i+1}=iq+j(q+1)+t(2q+1)/3$			s

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 $1,2,...,s-2$.

Далее имеем $k - 3(s-1)s/2 + (s-1)(s-2)/2 = k''$ и вычисление $s' = \left| (2k''+1/4)^{1/2} - 1/2 \right|$ дает $t = s - s' + 1$. Индекс j следует из выражения $j = k'' - s'(s'-1)/2 - 1$ и $i = s' - j - 1$.

Замечание 4. Для случая кривых с $d > 3$ соотношения между значением k и показателями i, j, t степеней рациональных функций x, v, y являются более сложными. Как и в случае с кривой $x^{(q+1)/d} + x^{2(q+1)/d} + y^{q+1} = 0$ общего решения для показателей степеней i, j, t для $d > 3$ не существует.

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

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

$$\varepsilon = 3(k + q(q-1)/6)/(q^3+2q^2-q-2), \text{ если } k \geq q(q-1)/6, \quad (7)$$

где i, j, t, определяются по лемме 1.

Доказательство. Параметры универсального класса следуют из определения кривой и числа ее точек в F_{q^2}. Пусть $k < q(q-1)/6$. Вероятность коллизии ε определяется соотношением $\varepsilon = \rho_k / N$, где $\rho_k = iq + j(q+1) + t(2q+1)/3$ – значение полюса рациональной функції $f_k = x^i \cdot v^j \cdot y^t$, i, j, t определяются по лемме 1, $N = (q^3+2q^2-q-2)/3$ – число точек кривой и подстановка дает (6). В случае $k = q(q-1)/6$, имеем $\rho_k = 2g = q(q-1)/3$ и $\varepsilon = 2g/N$, что согласуется с (7). С другой стороны, $\rho_k = iq + j(q+1) + t(2q+1)/3$ и подстановка $t = 0$, $j = 0$, $i = (q-1)/3$ дает проверку $\rho_k = iq + j(q+1) + t(2q+1)/3 = q(q-1)q/3$.

Пусть $k > q(q-1)/6$. Заметим, что $\rho_k = k + q(q-1)/6$. Прямое вычисление $\varepsilon = \rho_k / N$ дает выражение (7). ◊

Пример 4. Пусть кривая $x^5 + x^{10}y + y^{16} = 0$ определена над F_{2^8}, $q = 2^4$. Пусть $k = q(q-1)/6 = 40$. Имеем:

$k' = \lceil k/3 \rceil = \lceil 40/3 \rceil = 14$,

$s = \left| (2k'+0.25)^{1/2} - 1/2 \right| = \left| (2 \cdot 14 + 0.25)^{1/2} - 0.5 \right| = 5$,

$k'' = k - 3(s-1)s/2 + (s-1)(s-2)/2 = 40 - 30 + 6 = 16$,

$s' = \left| (2k''+0.25)^{1/2} - 1/2 \right| = \left| (2 \cdot 16 + 0{,}25)^{1/2} - 0.5 \right| = 6$,

$t = s - s' + 1 = 5 - 6 + 1 = 0$,

$j = k'' - s'(s'-1)/2 - 1 = 16 - 6(6-1)/2 - 1 = 0$,

$i = s' - j - 1 = 6 - 0 - 1 = 5$.

Тогда $\rho_{40} = k + q(q-1)/6 = 80$ и $\varepsilon = \rho_k / N \approx 0.052$.

Замечание 5.

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

2. Пусть $k = q(q-1)/2$. Подстановка в (7) дает

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

где $\varepsilon_{ЭК} = 1/q + 1/q^2$ – значение вероятности коллизии универсального хеширования по кривой Эрмита при $k = q(q-1)/2$ (см. [3]). Из оценки (8) следует проигрыш в два раза по вероятности коллизии хешированию по кривой Эрмита. Размер ключевых данных $N = (q^3 + 2q^2 - q - 2)/3$ по сравнению с хешированием по Эрмита меньше почти в три раза. Это приводит и к уменьшению в три раза максимально возможного числа слов хешируемых данных.

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

3. Практический алгоритм вычисления хеш кода

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

$$N_{опер} = k + s + 3, \text{ если } k < q(q-1)/6, \qquad (9)$$

$$N_{опер} = k + (q-1)/3 + 3, \text{ если } k \geq q(q-1)/6, \qquad (10)$$

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

Доказательство. Универсальное хеширование определяется выражением

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

где $i \geq 0, 0 \leq j \leq (q-1)/3, 0 \leq t \leq 2, iq + j(q+1) + t \cdot (2q+1)/3 \leq \rho_k$.

Базис пространства $L(\rho_k P_\infty)$, задается функциями вида

$$\{v^i \cdot x^j \cdot y^t : iq + j(q+1) + t(2q+1)/d \leq \rho_k\}.$$

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

Пусть $k < q(q-1)/6$. Члены суммы в выражении $h_{x,y}(m)$ можно представить трехмерным массивом $H_{x,y,v}$ по возрастанию полюсов рациональных функций $x^i \cdot v^j \cdot y^t$ в виде табл. 3:

Таблица 3

Рациональные функции $x^i \cdot v^j \cdot y^t$ в выражении $h_{x,y}(m)$						Номер уровня
					$v^0x^0y^0m_{0,0,0}$	**0**
					$v^0x^0y^1m_{0,0,1}$	
				$v^1x^0y^0m_{1,0,0}$	$v^0x^1y^0m_{0,1,0}$	**1**
					$v^0x^0y^2m_{0,0,2}$	
				$v^1x^0y^1m_{1,0,1}$	$v^0x^1y^1m_{0,1,1}$	
			$v^2x^0y^0m_{2,0,0}$	$v^1x^1y^0m_{1,1,0}$	$v^0x^2y^0m_{0,2,0}$	**2**
				$v^1x^0y^2m_{1,0,2}$	$v^0x^1y^2m_{0,1,2}$	
			$v^2x^0y^1m_{2,0,1}$	$v^1x^1y^1m_{1,1,1}$	$v^0x^2y^1m_{0,2,1}$	
		$v^3x^0y^0m_{3,0,0}$	$v^2x^1y^0m_{2,1,0}$	$v^1x^2y^0m_{1,2,0}$	$v^0x^3y^0m_{0,3,0}$	**3**
		...	...	...	...	...
		$v^{s-i}x^{i-2}y^2m_{s-i,i-2,2}$	...	$v^1x^{s-3}y^2m_{1,s-3,2}$	$v^0x^{s-2}y^2m_{0,s-2,2}$	
		$v^{s-i}x^{i-1}y^1m_{s-i,i-1,1}$	...	$v^1x^{s-2}y^1m_{1,s-2,1}$	$v^0x^{s-1}y^1m_{0,s-1,1}$	
$v^sx^0y^0m_{s,0,0}$	...	$v^{s-i}x^iy^0m_{s-i,i,0}$	...	$v^1x^{s-1}y^0m_{1,s-1,0}$	$v^0x^sy^0m_{0,s,0}$	**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:

$$h_{x,y}(m) = \sum_{t=0}^{2} y^t \cdot \sum_{j=0}^{s-t} v^j \sum_{i=0}^{s-t-j} m_{j,i,t} x^i. \qquad (11)$$

Выражение (11) 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 $k \geq q(q-1)/6$. Параметр s первой суммы в выражении $h_{x,y}(m)$ (11) определяется значением $s = (q-1)/3$. Сложность вычисления внутренней суммы в (11) составит k операций, а внешних – $(q-1)/3$ и 3 операций умножений и сложений в F_{q^2} по схеме Горнера. ◊

Замечание 6.

1. Результаты предложения 1 являются новыми и представлены впервые.

2. Асимптотика оценки сложности универсального хеширования по кривым $\alpha^{(q+1)/2}x^{(q-1)/3} + \alpha^{(q^2-1)/2}x^{2(q-1)/3}y + y^q = 0$ при $k < q(q-1)/6$ определяется $N_{опер} = k + (2k/3)^{1/2} + 3$, 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 $y^{3^{t-1}} + y^{3^{t-2}} + \ldots + y = \omega x^{3^t+1}$,

$g_3 = q(q-3)/6$ в поле характеристики $p=3$ и по кривой $x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$, и лучше, чем при хешировании по кривым Эрмита $N_{опер}(HC) = k + \sqrt{2}k^{1/2}$ (см. [3]).

Следствие 1. Асимптотика вероятности коллизии универсального хеширования по кривой $\alpha^{(q+1)/2}x^{(q-1)/3} + \alpha^{(q^2-1)/2}x^{2(q-1)/3}y + y^q = 0$ при больших значениях размерности поля $q \to \infty$ имеет вид

$$\varepsilon_{q\to\infty} = \sqrt{6}k^{1/2}/q^2,\ k < g. \qquad (12)$$

Доказательство. В выражении (11) для $h_{x,y}(m)$ определим $t=0$, $j=s$ и $i=0$. Подставим в (6) $s = \left|(2k/3+1/4)^{1/2} - 1/2\right|$ и для больших q получим (12).◊

Выводы

1. Наилучшей максимальной кривой $\omega x^{(q-1)/d} - yx^{2(q-1)/d} + y^q = 0$ над F_{q^2} является кривая третьего рода $d=3$. С ростом d уменьшается род и число точек кривой.

2. Асимптотические оценки вероятности коллизии универсального хеширования по кривой $\alpha^{(q+1)/2}x^{(q-1)/3} + \alpha^{(q^2-1)/2}x^{2(q-1)/3}y + y^q = 0$ при малых значениях k определяются отношением корня квадратного длины данных к размерности поля и совпадают с оценками для максимальных кривых третьего рода. Проигрыш хешированию по кривой Эрмита составляет $\sqrt{3}$ раз.

3. Практический алгоритм вычисления хеш кода по кривой $\alpha^{(q+1)/2}x^{(q-1)/3} + \alpha^{(q^2-1)/2}x^{2(q-1)/3}y + y^q = 0$ определяется схемой вычисления Горнера по рациональным функциям $x = X/Z$, $y = Y/Z$, v со сложностью $N_{опер} = k + (2k/3)^{1/2} + 3$. Это сложнее, чем хеширование по кривым третьего рода $y^q + y = x^{(q+1)/3}$ и $\sum_{i=1}^{t} y^{q/3^i} + \omega x^{q+1} = 0$, для которых базисное пространство определяется функциями $x = X/Z$, $y = Y/Z$. Относительное увеличение сложности вычислений по сравнению с хешированием по проективной прямой является несущественным $N_{опер}(FC)/N_{опер}(PS) = 1 + \sqrt{2/3}k^{-1/2}$.

Список литературы: 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 алгебро-геометрических кодов / Халимов Г.З.,. Кузнецов А.А. // Радиотехника. – 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.* Универсальное хеширование по максимальным кривым Гурвица / Халимов Г.З. // Прикладная радиоэлектроника. – Харьков : ХНУРЭ, 2010. – Т.9 № 3. – С.365-370. 5. *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. 4707–4728.6. *Fuhrmann R.* On maximal curves/ Fuhrmann R., Garcia A. and Torres F. // J. Number Theory. – 1997. – Vol. 67, No. 1. – P. 29–51.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 11.02.2011