УДК 681.3.06

Г.З. ХАЛИМОВ

Харьковский национальный университет радиоэлектроники, Украина

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО МАКСИМАЛЬНОЙ КРИВОЙ ВТОРОГО РОДА

Представлены результаты универсального хеширования по максимальной кривой $y^q + y = x^d$ *над конечным полем* F_{q^2}. *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 проигрыш в* $((q+1)/d+1)/2$ *раз по вероятности коллизии хешированию по кривой Эрмита и проигрыш по размеру ключевых данных в* $(q+1)/d$ *раз. Предложен эффективный алгоритм вычисления хеш-функции.*

Ключевые слова: *универсальное хеширование, алгебраические кривые.*

Введение

Проблематика построения схем универсального хеширования на основе алгеброгеометрического представления заключается в выборе алгебраических кривых и связанных с ними функциональных полей. Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на границе Хассе-Вейля. Классификация максимальных кривых представлена в [1]. Кривая $y^q + y = x^d$ в квадратичном поле F_{q^2} в случае $d = (q+1)/2$ является второй по значению рода после кривой Эрмита. Первые оценки универсального хеширования по проективной линии, кривым Эрмита, Гурвица и Сузуки представлены в [2-5]. 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.

Целью статьи является определение проективного многообразия точек кривой $y^q + y = x^d$, поля рациональных функций, оценки параметров семейства хеш функций и практического алгоритма вычислений. 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 $y^q + y = x^d$

Известные результаты.

Уравнение кривой в проективном пространстве P^2

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

и в аффинном пространстве

$$y^q + y = x^d,$$

где d делит $q+1$.

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

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

Подгруппа Вейерштрасса $H(P_\infty)$ в точке P_∞ образуется порядками полюсов $\mathrm{div}_\infty(x) = qP_\infty$ и $\mathrm{div}_\infty(y) = dP_\infty$, и $H(P_\infty) = \{\rho_0 = 0 < \rho_1 < ...\}$ (теорема 1).

Базис пространства $L(\rho_\ell P_\infty)$, задается функциями вида $\{x^i \cdot y^j : iq + jd \le \rho_\ell\}$, что следует из подгруппы Вейерштрасса $H(P_\infty)$ представленной порядками полюсов функций $x = X/Z$ и $y = Y/Z$).

Теорема 1. Пусть C_1 - кривая задана над F_{l^2} уравнением вида $y^l + y = x^m$, где m - делитель $l+1$. Кривая C_1 является максимальной, рода

$g=(m-1)(l-1)/2$. Подгруппа Вейерштрасса $H(P)$, $P\in C_1\left(F_{l^2}\right)$ функционального поля кривой содержит подгруппу $H(P)=\langle m,l\rangle$.

Доказательство. Отметим, что существует сюръективный морфизм кривой Эрмита на кривую C_1 $\phi: C\to C_1, (a,b)\to\left(a^n b\right)$, где $n=(l+1)/m$. Кривая Эрмита покрывает C_1, и C_1 является максимальной. Можно прямо показать максимальность C_1. Действительно пусть T является мультипликативной подгруппой поля F_{l^2} порядка $|T|=(l-1)\cdot m$ и $a\in T\cup\{0\}$, если $a^m\in F_l$. Так как $b^l+b=a^m$ для аффинной точки $(a,b)\in C_1$ и b^l+b есть след расширения F_{l^2}/F_l число точек кривой будет равно

$$\#C_1(F_q)=1+[l+m(l-1)]\cdot 1.$$

С другой стороны так же имеем

$$1+[l+m(l-1)]\cdot 1=1+l^2+2l(l-1)(m-1)/2,$$

где $(l-1)(m-1)/2$ значение рода кривой.

Чтобы показать подгруппу Вейерштрасса $H(P)=\langle m,l+1\rangle$, рассмотрим проективную плоскую кривую C_1 над конечным полем F_{l^2}

$$F(X,Y,Z)=Y^l+YZ^{l-1}-X^mZ^{l-m}.$$

На кривой существуют точка на бесконечности $P_0=(1:0:0)$ и точки $P_{0,\beta}=(0:\beta:1)$, $\beta\in F_l$.

Пусть $\aleph$ является линией с уравнением $X=0$. Тогда $\aleph$ пересекает кривую C_1 в точках $P_{0,\beta}$. Число точек $P_{0,\beta}$ равно l размерности подполя F_l. По теореме Безу кратность пересечения линии $\aleph$ с кривой C_1 равна l. Отсюда следует, что линия $\aleph$ имеет только однократные пересечения в точках $P_{0,\beta}$ с кривой C_1 и $\aleph\cdot C=\sum_{\beta\in F_l}P_{0,\beta}$.

Рассмотрим линию $\Re$ с уравнением $Y=0$. $\Re$ пересекает кривую C_1 в точках $P_{0,0}=(0:0:1)$ и $P_0=(1:0:0)$. Линия $\Re: Y=0$ является касательной к кривой C_1 в точке $P_{0,0}=(0:0:1)$. Частные производные кривой C_1 имеют следующий вид $F_X=mX^{m-1}Z^{l-m}$, $F_Y=lY^{l-1}+Z^{l-1}=Z^{l-1}$, $F_Z=(l-1)YZ^{l-2}-(l-m)X^mZ^{l-m-1}$. В точке $P_{0,0}=(0:0:1)$ получим, что $F_X=0$, $F_Y=1$, $F_Z=0$ и действительно уравнение касательной $d_PF=\Re$. Кратность пересечения $\Re$ с C_1 в $P_{0,0}=(0:0:1)$ определяется порядком частных производных когда $d_P^{(n)}F\neq\Re$. Дифференцируя частные производные кривой C_1 последовательно m раз получим

$$F_X^{(m)}=m(m-1)(m-2)...2\cdot 1\cdot Z^{l-m},$$

$$F_Y^{(m)}=l(l-1)(l-2)...(l-m+1)Y^{l-m},$$

$$F_Z^{(m)}=(l-1)(l-2)...(l-m)YZ^{l-m-1}-$$

$$-(l-m)(l-m-1)(l-2m+1)X^mZ^{l-2m}.$$

В точке $P_{0,0}=(0:0:1)$ имеем $F_X=1$, $F_Y=0$, $F_Z=0$ и $d_P^{(m)}F\neq\Re$. Тогда $\Re\cdot C_1=mP_{0,0}+(1-m)P_0$.

Линия $\Im$ с уравнением $Z=0$ пересекает C_1 только в одной точке $P_0=(1:0:0)$ и по теореме Безу получим пересечение $\Im\cdot C_1=lP_0$. Для рациональных функций $x=X/Z$ и $y=Y/Z$ имеем следующие дивизоры

$$\mathrm{div}(x)=\sum_{\beta\in F_l}P_{0,\beta}-lP_0,\ \mathrm{div}(y)=mP_{0,0}-mP_0,$$

соответственно $\mathrm{div}_\infty(x)=lP_0$ и $\mathrm{div}_\infty(y)=mP_0$ - значения полюсов дивизоров. Подгруппа Вейерштрасса точек не разрыва определяется значениями этих полюсов $H(P_0)=\langle m,l\rangle$.

Множество точек не разрыва кривой $H(P_0)$ определяется последовательностью

$$\{0,m,2m,3m,...;l,$$

$$m+l,2m+l,3m+l,...;2l,m+2l,2m+2l,3m+2l,...\}.$$

Пусть $(l+1)/m=n$. Число точек разрыва будет равно

$$|G(P_0)|=(1-n)+(1-2n)+...+(1-(m-1)n)=$$

$$(l-1)(m-1)/2,$$

что определяет род кривой. Можно заключить, что линейная серия m,l является полной, определяется рациональными функциями $x,y\in F_q(C)$.

Замечание 1.

1. Результаты по кривой $y^l+y=x^m$ являются хорошо известными. Их обобщение в теореме представлено впервые.

2. Доказательство несингулярности кривой представлено в [1].

3. Доказательство максимальности кривой взято из [6].

4. Доказательство для подгруппы Вейерштрасса является новым.

Следствие 1. Пусть $d=(q+1)/2$. Имеем кривую $y^q+y=x^{(q+1)/2}$ второго рода $g_2=(q-1)^2/4$ в поле F_{q^2} нечетной характеристики и $H(P)=\langle(q+1)/2,q\rangle$.

Следствие 2. Пусть $d=(q+1)/3$. Имеем кривую $y^q+y=x^{(q+1)/3}$ третьего рода $g_3=\left(q^2-3q+2\right)/6$ в поле F_{q^2} четной характеристики и $H(P)=\langle (q+1)/3, q\rangle$. Кривые $y^q+y=x^{(q+1)/3}$ определены над $GF(2^{2r+1})$.

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

$$h_{x,y}(m)=\sum_{0\le i\le d-1,\, j\ge 0,\, i\cdot q+j\cdot d\le \rho_k} m_{i,j}\cdot x^i\cdot y^j, \qquad (1)$$

где ρ_k полюс подгруппы Вейерштрасса $H(P_\infty)$ для k - го слова, $m_{i,j}\in F_{q^2}$ -слова сообщения m.

Пример 1. Пусть задано F_{5^2}. Кривая второго рода имеет вид $y^5+y+\alpha^{12}x^3=0$. Точки кривой представлены в табл. 1.

Таблица 1

Точки кривой $y^5+y+\alpha^{12}x^3=0$

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
z	0	1	1	1	1	1	1	1	1
y	0	0	1	1	1	α^1	α^1	α^1	α^2
x	1	0	α^2	α^{10}	α^{18}	1	α^8	α^{16}	α^2
	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}	P_{17}
z	1	1	1	1	1	1	1	1	1
y	α^2	α^2	α^3	α^4	α^4	α^4	α^5	α^5	α^5
x	α^{10}	α^{18}	0	1	α^8	α^{16}	1	α^8	α^{16}
	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}	P_{25}	P_{26}
z	1	1	1	1	1	1	1	1	1
y	α^6	α^6	α^6	α^7	α^7	α^7	α^8	α^8	α^8
x	α^4	α^{12}	α^{20}	α^2	α^{10}	α^{18}	α^4	α^{12}	α^{20}
	P_{27}	P_{28}	P_{29}	P_{30}	P_{31}	P_{32}	P_{33}	P_{34}	P_{35}
z	1	1	1	1	1	1	1	1	1
y	α^9	α^{10}	α^{10}	α^{10}	α^{11}	α^{11}	α^{11}	α^{12}	α^{12}
x	0	α^2	α^{10}	α^{18}	α^2	α^{10}	α^{18}	α^6	α^{14}
	P_{36}	P_{37}	P_{38}	P_{39}	P_{40}	P_{41}	P_{42}	P_{43}	P_{44}
z	1	1	1	1	0	1	1	1	1
y	α^{12}	α^{13}	α^{13}	α^{13}	α^{14}	α^{14}	α^{14}	α^{15}	α^{16}
x	α^{22}	α^4	α^{12}	α^{20}	α^6	α^{14}	α^{22}	0	α^4
	P_{45}	P_{46}	P_{47}	P_{48}	P_{49}	P_{50}	P_{51}	P_{52}	P_{53}
z	1	1	1	1	1	1	1	1	1
y	α^{16}	α^{16}	α^{17}	α^{17}	α^{17}	α^{18}	α^{18}	α^{18}	α^{19}
x	α^{12}	α^{20}	α^4	α^{12}	α^{20}	1	α^8	α^{16}	α^6
	P_{54}	P_{55}	P_{56}	P_{57}	P_{58}	P_{59}	P_{60}	P_{61}	P_{62}
z	1	1	1	1	1	1	1	1	1
y	α^{19}	α^{19}	α^{20}	α^{21}	α^{20}	α^{20}	α^{22}	α^{22}	α^{22}
x	α^{14}	α^{22}	1	α^8	α^{16}	0	α^6	α^{14}	α^{22}
	P_{63}	P_{64}	P_{65}						
z	1	1	1						
y	α^{23}	α^{23}	α^{23}						
x	α^6	α^{14}	α^{22}						

Число точек кривой равно $[d(q-1)+1]\cdot q+1=66$.

Значения полюсов дивизоров $div_\infty(x)=5P_\infty$ и $div_\infty(y)=3P_\infty$. Подгруппа Вейерштрасса точек не разрыва определяется значениями полюсов $H(P_\infty)=\langle 3,5\rangle$ и имеет вид $\{0,3,5,6,8,9,10,11,.....\}$. Точки разрыва определяются множеством $G(P_\infty)=\{1,2,4,7\}$, их число $|G(P_\infty)|=4$ и равняется значению рода $g=(d-1)(q-1)/2=2\cdot 4/2=4$. Линейная серия $3,5$ является полной, определяется рациональными функциями $x,y\in F_{5^2}(C)$.

Пример 2. Пусть задано F_{2^6}, $q=2^3$. Кривая третьего рода имеет вид $y^8+y+x^3=0$. Число точек кривой равно $[d(q-1)+1]\cdot q+1=(3\cdot 7+1)\cdot 8+1=177$ и соответствует прямому вычислению. Значения полюсов дивизоров $div_\infty(x)=8P_\infty$ и $div_\infty(y)=3P_\infty$. Подгруппа Вейерштрасса точек не разрыва определяется значениями полюсов $H(P_\infty)=\langle 3,8\rangle$ и имеет вид $\{0,3,6,8,9,11,12,14,15,16,17,.....\}$. Точки разрыва определяются множеством $G(P_\infty)=\{1,2,4,5,7,10,13\}$, их число $|G(P_\infty)|=7$ и равняется значению рода $g=(d-1)(q-1)/2=2\cdot 7/2=7$. Линейная серия $3,7$ также является полной.

2. Оценка параметров универсального хеширования

Для теоретической оценки вероятности коллизии необходимо связать значение k с показателями i,j степеней рациональных функций $x^i\cdot y^j$.

Лемма 1. Пусть $k<(d-1)(q-1)/2$, и $d=(q+1)/m$, тогда $i=m(s-1)s/2+s-1-k+ts$, $j=(s-1-i)m+t$, $s=\left\lceil (2k/m+1/4)^{1/2}-1/2\right\rceil$, $t=\lfloor (k-m(s-1)s/2)/s\rfloor$, где $\lceil\cdot\rceil$ - округление к большему целому числу, $\lfloor\cdot\rfloor$ - округление к меньшему целому числу.

Доказательство. Аддитивная подгруппа Вейерштрасса $H(P_\infty)=\{\rho_0=0<\rho_1<...\}$ кривой $y^q+y=x^d$ определяется значениями полюсов $\rho_1=q$ и $\rho_2=d$. Размещение ρ_k в порядке возрастания в подгруппе $H(P_\infty)$ представлено в табл. 2.

Таблица 2

Размещение полюсов подгруппы Вейерштрасса $H(P_\infty)=\langle d,q\rangle$

Уро вень	Значение полюсов				
0	$\rho_0=0$				
	$\rho_1=d$				
	$\rho_2=2d$				
	...				
1	$\rho_{m+1}=md$	$\rho_m=q$			
	$\rho_{m+3}=(m+1)d$	$\rho_{m+2}=q+d$			
	...	...			
2	$\rho_{3m+2}=2md$	$\rho_{3m+1}=q+md$	$\rho_{3m}=2q$		
	$\rho_{3m+4}=(2m+1)d$	$\rho_{3m+4}=q+(m+1)d$	$\rho_{3m+3}=2q+d$		
...	...	...	...	...	...
s-1	$\rho_{m(s-1)s/2+s-1}=$ $=(s-1)md$	...	$\rho_{m(s-1)s/2+2}=$ $=(s-3)q+2md$	$\rho_{m(s-1)s/2+1}=$ $=(s-2)q+md$	$\rho_{m(s-1)s/2}=$ $=(s-1)q$
	$\rho_{m(s-1)s/2+2s-1}=$ $=((s-1)m+1)d$	...	$\rho_{m(s-1)s/2+s+2}=$ $=(s-3)q+(2m+1)d$	$\rho_{m(s-1)s/2+s+1}=$ $=(s-2)q+(m+1)d$	$\rho_{m(s-1)s/2+s}=$ $=(s-1)q+d$
	...	$\rho_{m(s-1)s/2+s-1-i+ts}=$ $=iq+((s-1-i)m+t)d$ ...	...	...	...

Значение k определяется выражением

$$k=m(s-1)s/2+s-1-i+ts. \qquad (2)$$

Нормировка k по m даёт $k'=\lceil k/m\rceil=(s-1)s/2$ и

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

Далее имеем $k-m(s-1)s/2=s-1-i+ts$ и вычисление $\lfloor (k-m(s-1)s/2)/s\rfloor=t$. Индекс i следует из выражения (2) $i=m(s-1)s/2+s-1-k+ts$ и $j=(s-1-i)m+t$.

Пример 3. Пусть кривая $y^{11}+y=x^6$ определена над F_{11^2}. Вычислить значение полюса ρ_k, $k=15$. Построим таблицу полюсов.

Имеем

$m=(q+1)/d=12/6=2$,

$k'=\lceil k/m\rceil=\lceil 15/2\rceil=8$,

$s=\left\lceil (2k'+1/4)^{1/2}-1/2\right\rceil=\left\lceil (2\cdot 8+0.25)^{1/2}-0.5\right\rceil=4$,

$t=\lfloor (k-m\cdot s(s-1)/2)/s\rfloor=\lfloor (15-2\cdot 4\cdot 3/2)/4\rfloor=0$,

$i=m(s-1)s/2+s-1-k+ts=0$,

$j=(s-1-i)m+t=(4-1-0)\cdot 2+0=6$,

$\rho_k=iq+jd=6\cdot 6=36$.

Пусть $k=17$. Получим

$k'=\lceil k/m\rceil=\lceil 17/2\rceil=9$,

$s=\left\lceil (2k'+1/4)^{1/2}-1/2\right\rceil=\left\lceil (2\cdot 9+0.25)^{1/2}-0.5\right\rceil=4$,

$t=\lfloor (k-m\cdot s(s-1)/2)/s\rfloor=\lfloor (17-2\cdot 4\cdot 3/2)/4\rfloor=1$,

$i=m(s-1)s/2+s-1-k+ts=2$,

$j=(s-1-i)m+t=(4-1-2)\cdot 2+1=3$,

$\rho_k=iq+jd=2\cdot 11+3\cdot 6=40$.

Полученные результаты соответствуют значениям полюсов в табл. 3.

Таблица 3

Размещение полюсов подгруппы Вейерштрасса $H(P_\infty)=\langle 6,11\rangle$

Уро-вень	Значение полюсов				
0	ρ_0=0				
	ρ_1=6				
1	ρ_3=12	ρ_2=11			
	ρ_5=18	ρ_4=17			
2	ρ_8=24	ρ_7=23	ρ_6=22		
	ρ_{11}=30	ρ_{10}=29	ρ_9=28		
3	ρ_{15}=36	ρ_{14}=35	ρ_{13}=34	ρ_{12}=33	
	ρ_{19}=42	ρ_{18}=41	ρ_{17}=40	ρ_{16}=39	
4	ρ_{24}=48	ρ_{23}=47	ρ_{22}=46	ρ_{21}=45	ρ_{20}=44
	ρ_{29}=54	ρ_{28}=53	ρ_{27}=54	ρ_{26}=51	ρ_{25}=50
	...	...	...	...	...

Утверждение 2. Хеширование по рациональным функциям кривой $y^q+y=x^d$ над полем F_{q^2} определяет универсальный хеш-класс $\varepsilon-U(q^2+(d-1)(q-1)q,q^{2k},q^2)$, где $d=(q+1)/m$,

$q^2+(d-1)(q-1)q$ - число хеш-функций (объём ключевого пространства), q^{2k} - объём пространства сообщений, q^2 - объём пространства хеш-кодов. Вероятность коллизии ε определяется соотношениями

$$\varepsilon = (iq+jd)/(q^2+(d-1)(q-1)q), \qquad (3)$$

если $k<(d-1)(q-1)/2$, и

$$\varepsilon = (k+(d-1)(q-1)/2)/(q^2+(d-1)(q-1)q), \qquad (4)$$

если $k\ge(d-1)(q-1)/2$, где i,j определяются леммой 1.

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

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

Пусть $k<(d-1)(q-1)/2$. По лемме 1 имеем $i=m(s-1)s/2+s-1-k+ts$, $j=(s-1-i)m+t$, где $s=\left\lceil(2k/m+1/4)^{1/2}-1/2\right\rceil$ и $t=\lfloor(k-m(s-1)s/2)/s\rfloor$. В случае $k=(d-1)(q-1)/2$, имеем $i=d-2$, $j=m-1$ и $\rho_k=(d-2)q+((q+1)/d-1)d=(d-1)(q-1)=2g$. Подстановка ρ_k в $\varepsilon=\rho_k/N$, приводит к выражению $\varepsilon=1/(q+q^2/(d-1)(q-1))$, что согласуется с (4). Пусть $k>q(q-1)/2$. Заметим, что $\rho_k=k+(d-1)(q-1)/2$. Прямое вычисление $\varepsilon=\rho_k/N$ дает выражение (4).

Замечание 3.

1. Результаты утверждения 2 представлены впервые.

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

$$\varepsilon=(q+d-1)(q-1)/(2q^2+2(d-1)(q-1)q).$$

С учётом $d=(q+1)/m$ получим

$$\varepsilon\approx\frac{(m+1)}{2}\varepsilon_{ЭК}=\frac{(q+d+1)}{2d}\varepsilon_{ЭК}, \qquad (5)$$

где $\varepsilon_{ЭК}=1/q+1/q^2$ - значение вероятности коллизии универсального хеширования по кривой Эрмита при $k=q(q-1)/2$ (см. [4]).

Из оценки (5) следует проигрыш в $(m+1)/2$ раз по вероятности коллизии хешированию по кривой Эрмита. Размер ключевых данных $N=(q^3+(m-1)q)/m$, что приводит к уменьшению в m раз слов хешируемых данных.

3. Для кривой второго рода $y^q+y=x^{(q+1)/2}$ имеем увеличение $\varepsilon\approx\frac{3}{2}\varepsilon_{ЭК}$.

4. Для кривой третьего рода $y^q+y=x^{(q+1)/3}$ получим $\varepsilon\approx 2\varepsilon_{ЭК}$.

5. Для $k<(d-1)(q-1)/2$ отличие по вероятности коллизии хеширования по кривым $y^q+y=x^d$ и Эрмита будет несущественным. Действительно размер ключевых данных $N=(q^3+(m-1)q)/m$ уменьшается в m раз, но для одного и того же k, значение полюса ρ_k в m раз меньше по сравнению с хешированием по кривой Эрмита.

3. Практический алгоритм вычисления хеш-кода

Практический алгоритм вычисления хеш кода определяется предложением 1.

Предложение 1. Сложность универсального хеширования по кривым $y^q+y=x^d$ в F_{q^2} для k слов данных определяется выражением

$$N_{опер}=k+s, \text{ если } k<(d-1)(q-1)/2, \qquad (6)$$

$$N_{опер}=k+q, \text{ если } k\ge(d-1)(q-1)/2, \qquad (7)$$

где $s=\left\lceil(2k/m+1/4)^{1/2}-1/2\right\rceil, m=(q-1)/d$.

Доказательство. Универсальное хеширование определяется выражением

$$h_{x,y}(m)=\sum_{0\le i\le d-1,\,j\ge 0,\,i\cdot q+j\cdot d\le\rho_k} m_{i,j}\cdot x^i\cdot y^j.$$

Базис пространства $L(\rho_k P_\infty)$, задается функциями вида $\{x^i\cdot y^j : iq+jd\le\rho_k\}$. Размещение полюсов подгруппы Вейерштрасса $H(P_\infty)=\langle d,q\rangle$ определяется табл. 1.

Пусть $k<(d-1)(q-1)/2$. Члены суммы в выражении $h_{x,y}(m)$ можно представить двумерным массивом $H_{x,y}$ по возрастанию полюсов рациональных функций $x^i\cdot y^j$ в виде табл. 4. Сумма элементов матрицы даёт значение $h_{x,y}(m)$. Группировка слагаемых по столбцам матрицы приводит к следующему порядку вычислений

$$h_{x,y}(m)=\sum_{i=0}^{s-1}x^i\cdot\sum_{j=0}^{m(s-1-i)+t+ind}m_{i,j}\cdot y^j \qquad (8)$$

Таблица 4

Члены суммы в выражении $h_{x,y}(m)$ с учетом возрастания полюсов рациональных функций $x^i \cdot y^j$

Уровень	Значения рациональных функций с учетом возрастания полюсов				
0	$x^0y^0m_{0,0}$				
	$x^0y^1m_{0,1}$				
	$x^0y^2m_{0,2}$				
	...				
1	$x^0y^mm_{0,m}$	$x^1y^0m_{1,0}$			
	$x^0y^{m+1}m_{0,m+1}$	$x^1y^1m_{1,1}$			
	...	...			
2	$x^0y^{2m}m_{0,2m}$	$x^1y^mm_{1,m}$	$x^2y^0m_{2,0}$		
	$x^0y^{2m+1}m_{0,2m+1}$	$x^1y^{m+1}m_{1,m+1}$	$x^2y^1m_{2,1}$		
...	...	...	...	...	
s-1	$x^0y^{m(s-1)}m_{0,m(s-1)}$	...	$x^{s-3}y^{2m}m_{s-3,2m}$	$x^{s-2}y^mm_{s-2,m}$	$x^{s-1}y^0m_{s-1,0}$
	$x^0y^{m(s-1)+1}m_{0,m(s-1)+1}$	...	$x^{s-3}y^{2m+1}m_{s-3,2m+1}$	$x^{s-2}y^{m+1}m_{s-2,m+1}$	$x^{s-1}y^1m_{s-1,1}$
	...	$x^{s-1-i}y^{m(s-1-i)+t}m_{s-1-i,m(s-1-i)+t}$	...	...	...

где $ind = 0$, если $s - i \le (k - m(s-1)s/2) \bmod s$ (слагаемое $h_{x,y}(m)$ присутствует в последней строке матрицы $H_{x,y}$) и $ind = -1$, если $s - i > (k - m(s-1)s/2) \bmod s$ (слагаемое $h_{x,y}(m)$ не присутствует в последней строке матрицы $H_{x,y}$). Параметры s, t определяются леммой 1.

Выражение (8) определяет, что $h_{x,y}(m)$ можно вычислить по схеме Горнера, сначала для внутренней суммы, затем для внешней и сложность хеширования составит $N_{опер} = k + s$ операций умножений и сложений в F_{q^2}.

Пусть $k \ge (d-1)(q-1)/2$. Параметр s первой суммы в выражении $h_{x,y}(m)$ (8) определяется значением $s = d$. Параметр i в выражении (8) имеет верхнее значение $d-1$. Сложность вычисления внутренней суммы в (8) составит k операций, а внешней - q операций умножений и сложений в F_{q^2} по схеме Горнера.

Значения точек кривой $y^q + y = x^d$ определяются предложением 2.

Предложение 2. Пусть кривая $y^q + y = x^d$ задана над конечным полем F_{q^2}, $d \mid q+1$. Точки кривой $P_{a,b} = (a:b:1)$ определяются выражениями

$$b = \alpha^{i\cdot(q-1)+j},\ a = \alpha^{s(q+1)/d + t(q^2-1)/d}, \qquad (9)$$

где $i = \overline{0,q}$, $j = \overline{0,q-2}$, $t = \overline{0,d-1}$, $\alpha^{s\cdot(q+1)} = tr(b)$, $\alpha \in F_{q^2}$.

Доказательство. Пусть значения b есть решения уравнения Эрмита по координате y. Так как b пробегают все элементы поля F_{q^2}, справедливо $b = \alpha^{i\cdot(q-1)+j}$, где $i = \overline{0,q}$ и $j = \overline{0,q-2}$. Подстановка в уравнение кривой даёт

$$b^q + b = x^d.$$

Так как $b^q + b$ есть след $tr(b = \alpha^{i\cdot(q-1)+j}) \in F_q$, справедливо $tr(b) = \alpha^{s\cdot(q+1)}$, $s = \overline{0,q-2}$ и имеем решение $a = \alpha^{s(q+1)/d + t(q^2-1)/d}$, $t = \overline{0,d-1}$ для $P_{a,b} = (a:b:1)$.

Замечание 4.

1. Результаты предложений 1,2 являются новыми и представлены впервые.

2. Асимптотика оценки сложности универсального хеширования по кривым $y^q + y = x^d$ при $k < (d-1)(q-1)/2$ определяется $N_{опер} = k + (k/m)^{1/2}$, так как $s = \left\lceil (2k/m + 1/4)^{1/2} - 1/2 \right\rceil$. Это лучше, чем при хешировании по кривым Эрмита, так как $N_{опер}(HC) = k + k^{1/2}$ (см. [4]).

Выводы

Универсальное хеширование по кривой $y^q + y = x^d$ определено над полем рациональных функций $x = X/Z$, $y = Y/Z$ в проективном пространстве.

Для случая $d = (q+1)/2$ имеем универсальное хеширование по кривой второго рода над полем нечетной характеристики и при $d = (q+1)/3$ – по кривой третьего рода над полем четной характеристики.

Впервые определено хеширование по кривой и получены оценки хеширования. Оценки по вероятности коллизии показывают проигрыш в 1,5-2 раза хешированию по кривой Эрмита и проигрыш в 2-3 раза по размеру ключевых данных.

Впервые представлен практический алгоритм вычисления хешей по схеме Горнера. Выигрыш в скорости хеширования определяется значением $\approx \sqrt{2} \div \sqrt{3}$ по сравнению с кривой Эрмита. Задача эффективного вычисления точек кривой требует решения.

Литература

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

2. Bierbrauer J. Authentication via algebraic-geometric codes [Электронный ресурс] / J. Bierbrauer. – Режим доступа: http://www.math. mtu. edu/~jbierbra/ potpap.ps.

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

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

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

6. Garcia A. On curves over finite fields / A. Garcia // Seminaires&Congres. – 2005. – No.11. – P. 75-110.

Поступила в редакцию 5.03.2011

Рецензент: д-р техн. наук, проф., проф. кафедры автоматизации и компьютерно-интегрированных технологий В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков.

УНІВЕРСАЛЬНЕ ГЕШУВАННЯ ЗА МАКСИМАЛЬНОЮ КРИВОЮ ДРУГОГО РОДУ

Г.З. Халімов

Представлені результати універсального гешування за максимальною кривою $y^q + y = x^d$ над кінцевим полем F_{q^2}. Розглянуто проективне розмаїття точок кривої, поле раціональних функцій. Представлено доказ підгрупи Вейєрштрасса для раціональних функцій кривої та визначення універсального гешування над функціональним полем кривої. Отримано оцінки ймовірності колізії універсального гешування. З оцінки слідує програш у $((q+1)/d+1)/2$ рази за ймовірністю колізії гешування по кривій Ерміта і програш за розміром ключових даних в $(q+1)/d$ рази. Запропоновано ефективний алгоритм обчислення геш функції.

Ключові слова: універсальне гешування, алгебраїчні криві.

UNIVERSAL HASHING ON MAXIMAL CURVE OF THE SECOND GENUS

G.Z. Khalimov

The results of universal hashing for maximal curve $y^q + y = x^d$ over a finite field F_{q^2} are presented. The projective variety of points of the curve, the field of rational functions are considered. The proof of the Weierstrass subgroup of the rational functions of the curve and the definition of universal hashing over a function field of the curve are presented. The estimates of the collision probability of universal hashing is obtained. The loss is equal to $((q+1)/d+1)/2$ time by the probability of collision hashing Hermite curve and the loss on the size of key data is equal to $(q+1)/d$ time with assessment. An efficient algorithm for computing the hash function is proposed.

Keywords: universal hashing, algebraic curves.

Халимов Геннадий Зайдулович – канд. техн. наук, доцент кафедры безопасности информационных технологий Харьковского национального университета радиоэлектроники, Харьков, Украина, e-mail: GennadyKhalimov@mail.ru.