ЗАЩИТА ИНФОРМАЦИИ В РАДИОТЕХНИЧЕСКИХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

УДК 681.3.06

Г. З. ХАЛИМОВ, д-р техн. наук

ВЫСОКОСКОРОСТНОЕ УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО АЛГЕБРАИЧЕСКИМ КРИВЫМ

Решение задачи построения высокоскоростного хеширования определяется схемами хеш вычислений в конечных полях. Примером являются модификации алгоритма UMAC (2000 – 2005 гг.). Разрешение противоречия между требованиями стойкости к атакам на хеш функцию, сложности, скорости вычисления, характеристикам и реализациям алгоритма определяется в теории универсального хеширования по алгебраическим кривым. Наилучшие результаты универсального хеширования обеспечиваются вычислениями в простом и квадратичном конечном поле по кривым большого рода [1, 2]. Применение алгебраических кривых большого рода приводит к увеличению размерности функционального поля ассоциированного с кривой и росту сложности вычислений.

Цель статьи – оценка сложности универсального хеширования по наилучшим алгебраическим кривым с большим числом точек. В разд. 1 представлено определение и наилучшие результаты универсального хеширования по алгебраическим кривым. В разд. 2 приводятся оценки сложности вычисления хеш кодов по максимальным кривым в квадратичном поле.

1. Определение и наилучшие результаты универсального хеширования по алгебраическим кривым

Определение 1 [3]. Пусть задана абсолютно неразложимая, несингулярная проективная кривая χ над полем F_q с точками $P=\{P_1,P_2,...,P_n\}\in\chi(F_q)$. Для каждой алгебраической кривой можно определить поле рациональных функций $F_q(\chi)$. В каждой точке P_j кривой χ можно вычислить оценку ϑ_P для рациональных функций $f_i\in F_q(\chi)$, которая определяет порядок нуля или полюса функции f_i в этой точке. Хеш значение $h_{P_j}(m)\in F_q$ для сообщения $m=(m_1,...,m_k)$, $m_i\in F_q$ в точке $P_j\in F_q$ определяется выражением

$$h_{P_j}(m)=\sum_{i=1}^{k} f_i(P_j)m_i\,, \qquad (1)$$

где $f_i\in F_q(\chi)$ с упорядоченными порядками полюсов $0<\rho_1<...<\rho_k$. Хеш функция $h_{P_j}(m)$ определяет универсальный хеш класс $\varepsilon-U(N,q^k,q)$, где вероятность коллизии $\varepsilon\le\rho_k/N$, N – число точек алгебраической кривой.

Замечание 1.

1. Выражение (1) определяет хеш вычисление на основе скалярного произведения по рациональным функциям алгебраических кривых. Метод универсального хеширования определяется последовательностью следующих действий:

- определить проективное многообразие – алгебраическую кривую и её точки;
- построить линейное векторное пространство для функционального поля алгебраической кривой;
- задать хеш функцию как скалярное произведение слов данных и значений рациональных функций в точке кривой.

2. Параметры универсального хеш класса $\varepsilon-U(N,q^k,q)$ на основе хеширования по рациональным функциям определяются свойствами алгебраической кривой. Подгруппа Вейерштрасса $H(P_\infty)=\{\rho_0=0<\rho_1<...\}$ определяется полюсами рациональных функций в осо-

бой точке кривой и рациональные функции упорядоченные по значениям полюсов образуют векторное линейное пространство размерности $\dim(L(G) = \nu_\ell := \{(i, j) \in N^2 : \rho_i + \rho_j = \rho_{\ell+1}\}$.

3. Ключевой параметр хеш функции $h_{P_j}(m)$ определяется вычислением в точке алгебраической кривой.

Определение 2 [4]. Асимптотическая граница вероятности коллизии для $\varepsilon - U(N, q^k, q)$ хеш класса, построенного по рациональным функциям алгебраических кривых над большим алфавитом и фиксированных k и q, имеет вид

$$1 - \frac{q^k(q-1)}{(q^k-1)q} \le P_{кол} \le \varepsilon \le \frac{\sqrt{2k}}{q} + \frac{3\sqrt{2k}}{2q\sqrt{q}} \qquad (2)$$

Замечание 2.

1. Нижняя оценка ε определяется известной верхней границей Плоткина для кодового расстояния алгебраических кодов. Верхняя граница (2) следует из соотношения $\varepsilon \le \rho_k / N$ для максимальных плоских кривых.

2. Универсальное хеширование по рациональным функциям максимальных плоских алгебраических кривых имеет лучшие асимптотические результаты. Верхняя граница вероятности коллизии для универсального хеширования $h_{P_j}(m)$ определена в области малых значений $k \le 2g$, g-род кривой, является прямо пропорциональной корню квадратному из k.

Определение 3. Пусть $N_q(g)$ обозначает максимальное число F_q рациональных точек, которое кривая рода g может иметь. Кривая C рода g является максимальной над F_q, если число её F_q рациональных точек $\#C(F_q)$ равно $N_q(g)$.

Теорема 1 [5]. Пусть C – проективная и несингулярная, абсолютно неразложимая кривая, определенная над конечным полем F_q с q элементами. Тогда число F_q рациональных точек кривой определяется неравенством

$$N_q(g) \le 1 + q + 2\sqrt{q}g(C)$$

Замечание 3.

1. Теорема 1 (известная как теорема Хассе – Вейля) определяет, что для максимальных кривых над конечным полем достигается максимальное отношение числа точек кривой к роду.

2. Наилучший результат универсального хеширования, как следует из оценки вероятности коллизии $\varepsilon \le \rho_k / N$, достигается на максимальных кривых.

Теорема 2 [6]. Пусть C кривая над F_q рода g и удовлетворяются следующие условия

1. $g > (\sqrt{q} - 1)^2 / 4$;

2. $\#C(F_q) = q + 2g\sqrt{q} + 1$, (то есть C является максимальной над F_q).

Тогда X является F_q изоморфной кривой Эрмита над F_q и её род $g = \sqrt{q}(\sqrt{q} - 1)/2$.

Теорема 3 [7]. Для положительного целого s заданы $q = 2q_0^2$ и $q_0 = 2^s$. Пусть X кривая над F_q рода g и удовлетворяются следующие условия:

1. $g = q_0(q - 1)$;

2. $\#X(F_q) = q^2 + 1$.

Тогда X является F_q изоморфной кривой Дэлигнэ – Лустига ассоциированной с группой Судзуки $Sz(q)$.

Замечание 4. Теоремы 2 и 3 формулируют главный результат для максимальных кривых.

Известные результаты по алгебраическим кривым над полем F_q, $q = l^2$.

1. Кривая Эрмита $y^l + y = x^{l+1}$ является наилучшей максимальной плоской кривой наибольшего первого рода $g = l(l-1)/2$ и функциональное поле определяется функциями вида $\{x^i \cdot y^j\}$.

2. Алгебраические кривые:

- $y^l + y = x^{(l+1)/2}$;
- $\sum_{i=1}^{t} y^{l/2^i} = x^{l+1}$, $l = 2^t$;
- $y^l + y = x^{(l+1)/3}$, $l \equiv 2 (\mathrm{mod}\ 3)$;
- $\sum_{i=0}^{t-1} y^{3^i} = \omega x^{l+1}$, $l = 3^t$, $\omega \in F_{l^2}$ $\omega^{l-1} = -1$

являются максимальными кривыми второго и третьего рода, имеют подгруппу Вейерштрасса $H(P_\infty) = \langle \rho_1, \rho_2 \rangle$ размерности $\dim = 2$ и функциональное поле $\{x^i \cdot y^j\}$.

3. Максимальные кривые вида:

- $x^{(l+1)/3} + x^{2(l+1)/3} + y^{l+1} = 0$, $l \equiv 2 (\mathrm{mod}\ 3)$;
- $\omega x^{(l-1)/3} - y x^{2(l-1)/3} + y^l = 0$, $l \equiv 1 (\mathrm{mod}\ 3)$, $\omega \in F_{l^2}$, $\omega^{l-1} = -1$;
- $y^l + y = \left(\sum_i^t x^{l/3^i} \right)^2$, $l = 3^t$

имеют подгруппу Вейерштрасса $H(P_\infty)$ размерности $\dim = 3$ и функциональное поле определяется рациональными функциями вида $\{x^i \cdot y^j \cdot v^t\}$.

4. Кривая Дэлигнэ – Лустига, ассоциированная с группой Судзуки, определяется полной линейной серией $D = |(q + 2q_0 + 1)P_0|$ размерности $\dim = 4$ и степени $q + 2q_0 + 1$ [8].

Кривая Судзуки $y^q - y = x^{q_0}(x^q - x)$ определена над полем F_q, $q = 2q_0^2$, $q_0 = 2^s$ рода $g = q_0(q-1)$ и имеет число точек $N = q^2 + 1$. Базис пространства $L(\rho_\ell P_0)$ задается функциями вида $\{w^j \cdot v^i \cdot y^t \cdot x^r : i(q + 2q_0) + j(q + 2q_0 + 1) + t(q + q_0) + r \cdot q \le \rho_\ell\}$.

5. Кривая Ферма $x^{(q-1)/3} + y^{(q-1)/3} + z^{(q-1)/3} = 0$ над F_q, $q \equiv 1 (\mathrm{mod}\ 3)$ является кривой с большим числом точек $N = 2(q-1)^2/9$.

Замечание 5.

1. Кривая Эрмита имеет наилучшее отношение числа точек к роду кривой $N_q(g)/g$.
2. Максимальные кривые второго и третьего рода покрываются кривой Эрмита.
3. Абсолютно наилучший результат $N_q(g)/g$ достигается на кривой Судзуки.

2. Оценки сложности универсального хеширования по алгебраическим кривым

Замечание 6.

1. Сложность универсального хеширования по алгебраическим кривым определяется размерностью функционального поля ассоциированного с кривой.

2. Вычисление хеш значений $h_{P_j}(m)$ по выражению (1) определяется многопараметрическим скалярным произведением рациональных функций алгебраических кривых со словами сообщения. В конструкции с прямым вычислением $h_{P_j}(m)$ требуется m (m – размерность поля рациональных функций) умножений в конечном поле для одного значения суммы (1) с предварительным вычислением значения рациональной функции в точке кривой.

3. Хеширование по алгебраическим кривым с использованием метод вычисления хеш функций на основе многопараметрической схемы Горнера реализует наименьшую сложность вычислений [9].

Метод вычисления хеш функций на основе многопараметрической схемы Горнера основывается на определении хеш функции по алгебраической кривой, её функционального поля, соотношения между размерностью линейного пространства рациональных функций кривых и размером хешируемых данных и имеет следующую последовательность действий:

- задать хеш функцию через скалярное произведение рациональных функций функционального поля алгебраической кривой;
- определить массив рациональных функций с учетом возрастания полюсов рациональных функций и размерности функционального пространства;
- построить алгоритм вычисления хеш функций на основе многопараметрической схемы Горнера соответственно размерности функционального поля кривой.

Алгоритмы вычислений хеш функций по максимальным кривым Эрмита, Судзуки и кривым с большим числом точек Ферма и оценки сложности хеширования представлены в табл.1.

Таблица 1.

Уравнение кривой	Определение $h_{x,y}(m)$	Оценки сложности хеш вычислений
Проективная прямая $X+Y+Z=0,\ F_q$	$\sum_{i=0}^{k-1} m_i \cdot x^i$	k
Кривая Эрмита $y^q+y=x^{q+1},\ F_{q^2}$	$\sum_{j=0}^{s} y^j \cdot \sum_{i=0}^{s-j} m_{i,j} \cdot x^i$	$k+s$
Максимальные кривые $y^q+y=x^d,\ F_{q^2},$ $d\mid q+1$	$\sum_{i=0}^{s_1-1} x^i \cdot \sum_{j=0}^{m(s_1-1-i)+t+ind} m_{i,j} \cdot y^j,$ $t=\lfloor (k-m(s_1-1)s_1/2)/s_1 \rfloor,\ m=(q+1)/d,$ $ind=0,-1$	$k+s_1$
Кривая Судзуки $y^q-y=x^{q_0}(x^q-x),$ $F_q,\ q=2q_0^2,\ q_0=2^s,$	$\sum_{t=0}^{1} y^t \sum_{i=0}^{s-t} v^s \sum_{r=0}^{\min\{s-t,q_0-t\}} (x/v)^r \sum_{j=0}^{\min\{s-r,q_0-1\}} m_{t,i,r,j}(w/v)^j,$ $s=(3k)^{1/3}$	$k+s^3/3+$ $s^2/2-1$
Кривая Ферма $X^{(q-1)/3}+Y^{(q-1)/3}+Z^{(q-1)/3}=0$ $F_q,\ q\equiv 1 \pmod 3$	$\sum_{j=0}^{s} y^j \cdot \sum_{i=0}^{s-j} m_{i,j} \cdot x^i$	$k+s$

$s=\left|(2k+1/4)^{1/2}-1/2\right|,\ s_1=\left|(2k/m+1/4)^{1/2}-1/2\right|,$ $\lceil\cdot\rceil$ – округление к большему целому числу, $\lfloor\cdot\rfloor$ – округление к меньшему целому числу.

Оценки сложности вычислений по числу операций универсального хеширования по рациональным функциям алгебраических кривых для фиксированного поля вычислений представлены в табл. 2.

Таблица 2

Уравнение кривой	Оценки числа операций $N_{опер}(k)$ над F_q для k слов данных		
	$k=\sqrt{q}$	$k=q$	$k=q^{3/2}$
Проективная прямая	$q^{1/2}$	-	-
Кривая Эрмита	$q^{1/2}+\sqrt{2}q^{1/4}$	$q+\sqrt{2}q^{1/2}$	-
Максимальные кривые второго рода $y^{\sqrt{q}}+y=x^{(\sqrt{q}+1)/2}$	$q^{1/2}+q^{1/4}$	$q+q^{1/2}$	-
Максимальные кривые третьего рода $y^{\sqrt{q}}+y=x^{(\sqrt{q}+1)/3}$	$q^{1/2}+\sqrt{2/3}q^{1/4}$	$q+\sqrt{2/3}q^{1/2}$	-
Кривые Ферма с большим числом точек $X^{(q-1)/3}+Y^{(q-1)/3}+Z^{(q-1)/3}=0$	$q^{1/2}+\sqrt{2}q^{1/4}$	$q+\sqrt{2}q^{1/2}$	$q^{3/2}+\sqrt{2}q^{3/4}$
Кривая Сузуки $y^q-y=x^{q_0}(x^q-x)$	$2q^{1/2}+1.04q^{1/3}+2\sqrt[3]{3}q^{1/6}$	$2q+1.04q^{2/3}+2\sqrt[3]{3}q^{1/3}$	$2q^{3/2}+1.04q+2\sqrt[3]{3}q^{1/2}$

Замечание 7.

1. Результаты табл. 2 следуют из оценок универсального хеширования для алгоритмов быстрых вычислений Горнера по рациональным функциям алгебраических кривых.

2. Увеличение числа операций вычислений в конечном поле при универсальном хешировании по максимальным кривым по сравнению с хешированием по проективной прямой имеет зависимость, которая определяется корнем квадратным от числа слов данных. С уменьшением рода максимальной кривой уменьшаются затраты на вычисления. Хеширование по кривой Ферма $X^{(q-1)/3}+Y^{(q-1)/3}+Z^{(q-1)/3}=0$ с большим числом точек имеет одинаковую сложность с хешированием по кривой Эрмита.

3. Наибольшие затраты на вычисления имеет хеширование по кривой Сузуки. Число вычислений в конечном поле в два раз больше по сравнению с хешированием по проективной прямой.

Значения числа вычислений универсального хеширования представлены в табл. 3.

Таблица 3

Уравнение кривой	Число операций вычисления универсального хеширования для L бит данных (относительное число операций)								
	Размер поля F_q, $\log q=32$			Размер поля F_q, $\log q=64$			Размер поля F_q, $\log q=128$		
	1*Кбт*	1*Мбт*	1*Гбт*	1*Кбт*	1*Мбт*	1*Гбт*	1*Кбт*	1*Мбт*	1*Гбт*
Проективная прямая	2^8	2^{18}	2^{28}	2^7	2^{17}	2^{27}	2^6	2^{16}	2^{26}
Кривая Эрмита	$2^8+2^{4,5}$ (1,09)	$2^{18}+2^{9,5}$ (1,003)	$2^{28}+2^{14,5}$ ($1,0^48$)	2^7+2^4 (1,12)	$2^{17}+2^9$ (1,004)	$2^{27}+2^{14}$ ($1,0^31$)	$2^6+2^{3,5}$ (1,17)	$2^{16}+2^{8,5}$ (1,006)	$2^{26}+2^{13,5}$ ($1,0^32$)
Кривые второго рода	2^8+2^4 (1,06)	$2^{18}+2^9$ (1,002)	$2^{28}+2^{14}$ ($1,0^46$)	$2^7+2^{3,5}$ (1,09)	$2^{17}+2^{8,5}$ ($1,0^227$)	$2^{27}+2^{13,5}$ ($1,0^48$)	2^6+2^3 (1,125)	$2^{16}+2^8$ (1,004)	$2^{26}+2^{13}$ ($1,0^31$)
Кривые третьего рода	$2^8+2^{3,7}$ (1,05)	$2^{18}+2^{8,7}$ (1,002)	$2^{28}+2^{13,7}$ ($1,0^46$)	$2^7+2^{3,2}$ (1,07)	$2^{17}+2^{8,2}$ ($1,0^222$)	$2^{27}+2^{13,2}$ ($1,0^47$)	$2^6+2^{2,7}$ (1,1)	$2^{16}+2^{7,7}$ (1,003)	$2^{26}+2^{12,7}$ ($1,0^31$)
Кривые Ферма	$2^8+2^{4,5}$ (1,09)	$2^{18}+2^{9,5}$ (1,003)	$2^{28}+2^{14,5}$ ($1,0^48$)	2^7+2^4 (1,12)	$2^{17}+2^9$ (1,004)	$2^{27}+2^{14}$ ($1,0^31$)	$2^6+2^{3,5}$ (1,17)	$2^{16}+2^{8,5}$ (1,006)	$2^{26}+2^{13,5}$ ($1,0^32$)
Кривая Сузуки	$2^9+2^{5,4}+2^{4,19}$ (2,23)	$2^{19}+2^{12,05}+2^{7,5}$ (2,017)	$2^{29}+2^{18,7}+2^{10,86}$ (2,002)	$2^8+2^{4,7}{}^2+2^{3,86}$ (2,32)	$2^{18}+2^{11,3}{}^9+2^{7,19}$ (2,02)	$2^{28}+2^{18,0}{}^5+2^{10,53}$ (2,002)	$2^7+2^{4,05}+2^{3,53}$ (2,44)	$2^{17}+2^{10,7}{}^2+2^{6,86}$ (2,027)	$2^{27}+2^{17,3}{}^9+2^{10,19}$ (2,0025)

В скобках представлен проигрыш по числу вычислений по сравнению с проективной прямой.

Выводы

1. Оценки числа операций хеш вычислений по плоским алгебраическим кривым являются близкими, и сложность вычислений имеет тенденцию к уменьшению с ростом размерности поля вычислений при фиксированном размере данных.

2. Хеш вычисления по плоским алгебраическим кривым несколько сложнее по сравнению с вычислениями по проективной прямой. Относительное увеличение числа операций составляет порядка 5 – 17% на блоках данных малой длины ≈1*Кбт* и <<1 % для данных ≥1*Мбт*.

3. Хеш вычисления по кривой Сузуки сложнее приблизительно в два раза, по сравнению с хешированием по плоским кривым и проективной прямой.

Список литературы: 1. *Халимов Г.З.* Универсальное хеширование по алгебраическим кривым в простом поле / Г.З.Халимов // Системи управління, навігації та зв'язку / Міністерство промислової політики України, ДП «Центральний науково-дослідний інститут навігації і управління». – Київ, 2011. – Вип. 1(17). – С.156-161. 2. *Халимов Г.З.* Универсальное хеширование по рациональным функциям кривой Эрмита / Г.З.Халимов, А.Ю.Иохов // Междунар. науч.-практ. конф. «Застосування інформаційніх технологій у підготовці та діяльності сил охорони правопорядку» ; Академія внутрішніх військ МВС України 17.03.2011. Зб. тези доповідей. – 2011. – С.48-51. 3. *Халимов Г.З.* Универсальное хеширование по максимальным кривым Гурвица / Халимов Г.З. // Прикладная радиоэлектроника. – Харьков : ХНУРЭ, 2010. – Т.9. № 3, – С.365-370. 4. *Халимов Г.З.* Коллизионные оценки универсального хеширования на основе схем с алгебраическими кодами / Г.З.Халимов // Прикладная радиоэлектроника. – Харьков : ХНУРЭ, 2009. – Т. 8, Вып. 3. – С.338-342. 5. *Weil A.* Courbes alg´ebriques et vari´et´es abeliennes / A.Weil // Hermann, Paris, 1971. – P.301. 6. *Ruck H.G.* A characterization of Hermitian function fields over finite fields / H.G.Ruck, H.Stichtenoth // J. reine angew. Mathematics. – 1994. – V.457. – P.185–188. 7. *Torres f.* The Deligne-Lusztig curve associated to the Suzuki group [Электронный ресурс] / F.Torres // arXiv:alg-geom/9706012v1 26Jun 1997. 8. *Ihara Y.* Some remarks on the number of rational points of algebraic curves over finite fields / Y.Ihara // J. Fac. Science. Tokio. – 1981. -N.28. –P. 721–724. 9. *Халимов Г.З.* Аутентификация с применением эрмитовых кодов / Г.З.Халимов, А.Ю.Иохов // Вестник ХПИ. – Х. : НТУ „ХПИ", 2005. – Вып. 9. – С. 26-32.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 01.02.2013