ми физико-механическими требованиями к получаемым заготовкам. Исходный материал для раскроя и формы заготовок может иметь более сложную форму, а заготовки могут принимать произвольную ориентацию, что значительно усложняет постановку задачи раскроя и её алгоритмизацию. Программное обеспечение для решения задач раскроя материала, а также получаемые карты раскроя, которые характеризуются информацией о физических характеристиках, форме, местоположении и размерах заготовок, могут быть интегрированы в станки с ЧПУ для лазерной резки материала.

Литература

1. Стоян, Ю. Г. Основная задача геометрического проектирования [Текст] / Ю. Г. Стоян. – Х. : ИПМаш АН УССР, 1983. – 36 с.
2. Стоян, Ю. Г. Оптимизация технических систем с источниками физических полей [Текст] / Ю. Г. Стоян, В. П. Путятин. – К. : Наук. думка, 1988. – 192 с.
3. Канторович, Л. В. Рациональный раскрой промышленных материалов [Текст] / Л. В. Канторович, В А. Залгаллер. – Новосибирск : Наука, 1971. – 299 с.
4. Рвачев, В. Л. Геометрические приложения алгебры логики [Текст] / В. Л. Рвачёв. – К. : Техника, 1967. – 212 с.
5. Стоян, Ю. Г. Методы и алгоритмы размещения плоских геометрических объектов [Текст] / Ю. Г. Стоян, Н. И. Гиль. – К. : Наук. думка, 1976. – 248 с.
6. Кузьмичёв, В. Е. Законы и формулы физики [Текст] / В. Е. Кузьмичёв. – К. : Наук. думка, 1986. – 864 с.
7. Грицюк, Ю. І. Моделювання карт і оптимізація плану розкрою плитних деревних матеріалів на меблеві заготовки [Текст] / Ю. І. Грицюк – Львів : Панорама, 2004. – 524 с.

УДК 681.3.06

АЛГОРИТМ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ ПО КРИВОЙ СУЗУКИ

Г.З. Халимов
Кандидат технических наук, доцент, профессор*
E-mail: Gennadykhalimov@mail.ru
Е.В. Котух
Аспирант*
*Кафедра безопасности информационных технологий
Харьковский национальный университет радиоэлектроники
пр. Ленина, 14, Харьков, Украина
Контактный тел.: (057) 702-14-25

Представлено алгоритм універсального хешування по кривій Сузукі над кінцевим полем, який визначається схемою обчислення Горнера по чотирьох раціональних функціях. Отримано оцінки складності обчислення хеш коду

Ключові слова: універсальне хешування, алгебраїчна крива Сузукі

Представлен алгоритм универсального хеширования по кривой Сузуки над конечным полем, который определяется схемой вычисления Горнера по четырём рациональным функциям. Получены оценки сложности вычисления хеш кода

Ключевые слова: универсальное хеширование, алгебраическая кривая Сузуки

An algorithm for universal hashing on the Suzuki curve over a finite field, which is determined by calculating the Horner's scheme for the four rational functions. Obtained estimates of the complexity of computing the hash code

Key words: universal hashing, algebraic curve Suzuki

Введение

Наилучший результат универсального хеширования достигается на максимальных кривых, число точек которых лежит на границе Хассе-Вейля. Максимальные кривые ассоциированные с группой Сузуки и группой Ри имеют максимально возможное значение рода и соответственно число точек [1]. Первые оценки универсального хеширования по проективной линии, кривым Эрмита и Гурвица представлены в [2-4]. Определение универсального хеширования в функциональном поле кривой Сузуки, доказательство подгруппы Вейерштрасса для рациональных функций кривой, оценки вероятности коллизии универсального хеширования рассмотрены в [5].

Целью статьи является решение задачи построения алгоритма универсального хеширования по кривой Сузуки. В разделе 1 приводятся свойства кривой Сузуки и определение универсального хеширования по кривой. В разделе 2 представлен практический алгоритм вычисления хешей по рациональным функциям кривой Сузуки и оценки сложности вычислений.

1. Универсальное хеширование по рациональным функциям кривой Сузуки

Известные результаты

• Уравнение кривой в проективном пространстве P^2

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

и в аффинном пространстве над F_q

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

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. Кривая является максимальной и удовлетворяет границе Хассе-Вейля.

• Точками кривой являются особая точка на бесконечности $P_0 = (0:1:0)$ кратности q_0 и рациональные точки $P_{a,b} = (a:b:1)$, где $a,b \in F_{q^2}$ и $b^q - b = a^{q_0}(a^q - a)$.

• Подгруппа Вейерштрасса функционального поля кривой содержит подгруппу $H(P_\infty) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle$. Кривая Сузуки определяется полной линейной серией $D = |(q+2q_0+1)P_0|$ размерности $\dim = 4$.

• Базис пространства $L(\rho_\ell P_0)$, задается функциями вида

$$\{w^j \cdot v^i \cdot y^t \cdot x^r : i(q+2q_0) + \\ + j(q+2q_0+1) + t(q+q_0) + r \cdot q \le \rho_\ell\},$$

что следует из подгруппы Вейерштрасса $H(P_0)$ представленной порядками полюсов функций $x = X/Z$, $y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$. Порядки полюсов равны $\mathrm{div}_\infty(x) = qP_0$, $\mathrm{div}_\infty(y) = (q+q_0)P_0$, $\mathrm{div}_\infty(v) = (q+2q_0)P_0$, $\mathrm{div}_\infty(w) = (q+2q_0+1)P_0$.

• Кривая Сузуки представляется 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 $f(a,b) := a^{2q_0+1} + b^{2q_0}$.

Определение [5]. 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

$$h_{x,y}(m) = \sum m_{i,j,t,r} \cdot w^j \cdot v^i \cdot y^t \cdot x^r, \tag{1}$$

где ρ_k - полюс подгруппы Вейерштрасса $H(P_\infty)$,

$m_{i,j,t,r} \in F_q$ - слова сообщения m, $i \ge 0$,

$0 \le j \le 2q_0 - 1$, $0 \le t \le 1$, $0 \le r \le q_0$,

$i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + rq \le \rho_k$, $x = X/Z$,

$y = Y/Z$, $v = x^{2q_0+1} + y^{2q_0}$, $w := xy^{2q_0} + x^{2q+2q_0} + y^{2q}$.

Пример. 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 $b^8 - b = a^2(a^8 - a)$.

Базисное пространство кривой $y^8 - y = x^2(x^8 - x)$ определяется рациональными функциями x, y, $v = x^5 + y^4$, $w := x^6 + xy^4 + y^2$. Распределение кратности пересечения полиномов базисного пространства и $y^8 - y = x^2(x^8 - x)$ над F_{2^3} представлено в табл. 1.

Таблица 1

Распределение кратности пересечения полиномов базисного пространства и кривой $y^8 - y = x^2(x^8 - x)$

Базисное пространство	Число испытаний	Распределение кратности пресечения (значение числа точек пересечения =число опытов)		
x,y,v,w	10000	8:=767 9:=1095	12:=2074	13:=6060
x,y,v,w,x^2	10000	8:=730 9:=138 11:=2904	12:=1479 13:=3781 14:=234	15:=717 16:=17
x,y,v,w,x^2,xy	10000	8:=959 9:=10 10:=2683 11:=1192	12:=2722 13:=577 14:=1136 15:=403	16:=259 17:=21 18:=38
x,y,v,w,x^2,xy,y^2	10000	8:=864 9:=75 10:=2703 11:=897 12:=2969	13:=866 14:=970 15:=307 16:=201	17:=33 18:=108 19:=4 20:=3

Хеш вычисления в конечном поле F_{2^3} по полиномиальному базису $L(18P_\infty)$ на кривой $y^8 - y = x^2(x^8 - x)$ дают оценку вероятности коллизии $\varepsilon = m/N = 18/64 = 0.28$. Действительно число точек кривой $N = 64$ и число совпадающих хешей при вычислении по полиномиальному базису $L(18P_\infty)$ не превышает значения 18. Число слов данных равно $k = 6$. Хеш вычисления в конечном поле F_{2^3} для 6 слов данных по полиномиальному базису $L(6P_\infty)$ на проективной прямой $x + y + z = 0$ дают оценку вероятности коллизии $\varepsilon = m/N = 6/8 = 0.75$.

Связь значение k с показателями i,j,t,r степеней рациональных функций w,v,y,x определяется леммой [5].

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

$i = p - j$, $j = \Delta - t \cdot q_0 - 1$, $r = s - s_2 + d \cdot q_0$, $t = t_1 \bmod 2$,

где $s' = \left[(3k)^{1/3}\right]$, $\Sigma = s'(s'+1)(2s'+1)/6$,

$s = s' + \lfloor k/\Sigma \rfloor$, $s_1 = s - q_0 - 1$,

$\Sigma_{s-1} = s(s-1)(2s-1)/6 - s_1(s_1-1)(2s_1-1)/3 - s_1(s_1-1)$,

$k' = k - \Sigma_{s-1}$, $k_1 = \lceil k'/2 \rceil$, $d = \lfloor s_2/(s-t) \rfloor$,

$k_2 = k_1 + s_1(s_1+1)/2$, $s_2 = \left\lceil (2k_2 + 1/4)^{1/2} - 1/2 \right\rceil$,

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

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

$p = s_2 - (s_2 - t)d$, $\lceil \cdot \rceil$ - округление к большему целому числу, $\lfloor \cdot \rfloor$ - округление к меньшему целому числу, $[\cdot]$ - округление к ближайшему целому числу.

2. Практический алгоритм вычисления хеш кода

Практический алгоритм вычисления хеш кода определяется предложением.

Таблица 2

Размещение полюсов подгруппы Вейерштрасса $H(P_\infty) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle$, F_q, $q = 2^5$

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

Предложение. Сложность универсального хеширования по кривым $y^q - y = x^{q_0}(x^q - x)$, где $q = 2q_0^2$ и $q_0 = 2^s$ над полем F_q определяется выражением

$$N_{\text{опер}} = k + s^3/3 + s^2/2 + 2s - 1 \text{, если } s \le q_0 \text{,} \quad (2)$$

$$N_{\text{опер}} = k + q_0{}^3/3 + q_0{}^2/2 + (s - q_0)(2q_0 - 1) + 2s - 1 \text{, если } s > q_0 \text{,} \quad (3)$$

где $s = (3k)^{1/3}$.

Размещение полюсов подгруппы Вейерштрасса $H(P_\infty) = \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle$ имеет представление над F_q, $q_0 = 2^2, q = 2^5, q + q_0 = 36$ подобное $H(P_\infty) = \langle 32, 36, 40, 41 \rangle$ (см. табл. 2).

Пусть $k < q_0(q-1)$.

Члены суммы в выражении $h_{x,y}(m)$ представляются табл. 3 и 4 для F_q, $q = 2^5$ четырёхмерным массивом $H_{w,v,y,x}$ по возрастанию полюсов рациональных функций $w^j \cdot v^i \cdot y^t \cdot x^r$, с учетом включения функций $w^j \cdot v^i \cdot y^0 \cdot x^r$ и $w^j \cdot v^i \cdot y^1 \cdot x^r$.

Таблица 3

Члены суммы в выражении $h_{x,y}(m)$ с учетом возрастания полюсов рациональных функций $w^j \cdot v^i \cdot y^0 \cdot x^r$ над F_q, $q = 2^5$

Номера уровней s	Мономы $h_{x,y}(m)$ для рациональных функции $w^j \cdot v^i \cdot y^0 \cdot x^r$			
1	$w^0v^0y^0x^0m_{0,0,0,0}$			
	$w^0v^0y^0x^1m_{0,0,0,1}$			
2	$w^0v^1y^0x^0m_{0,1,0,0}$	$w^1v^0y^0x^0m_{1,0,0,0}$		
	$w^0v^0y^0x^2m_{0,0,0,2}$			
	$w^0v^1y^0x^1m_{0,1,0,1}$	$w^1v^0y^0x^1m_{1,0,0,1}$		
3	$w^0v^2y^0x^0m_{0,2,0,0}$	$w^1v^1y^0x^0m_{1,1,0,0}$	$w^2v^0y^0x^0m_{2,0,0,0}$	
	$w^0v^0y^0x^3m_{0,0,0,3}$			
	$w^0v^1y^0x^2m_{0,1,0,2}$	$w^1v^0y^0x^2m_{1,0,0,2}$		
	$w^0v^2y^0x^1m_{0,2,0,1}$	$w^1v^1y^0x^1m_{1,1,0,1}$	$w^2v^0y^0x^1m_{2,0,0,1}$	
4	$w^0v^3y^0x^0m_{0,3,0,0}$	$w^1v^2y^0x^0m_{1,2,0,0}$	$w^2v^1y^0x^0m_{2,1,0,0}$	$w^3v^0y^0x^0m_{3,0,0,0}$
	$w^0v^0y^0x^4m_{0,0,0,4}$			
	$w^0v^1y^0x^3m_{0,1,0,3}$	$w^1v^0y^0x^3m_{1,0,0,3}$		
	$w^0v^2y^0x^2m_{0,2,0,2}$	$w^1v^1y^0x^2m_{1,1,0,2}$	$w^2v^0y^0x^2m_{2,0,0,2}$	
	$w^0v^3y^0x^1m_{0,3,0,1}$	$w^1v^2y^0x^1m_{1,2,0,1}$	$w^2v^1y^0x^1m_{2,1,0,1}$	$w^3v^0y^0x^1m_{3,0,0,1}$
5	$w^0v^4y^0x^0m_{0,4,0,0}$	$w^1v^3y^0x^0m_{1,3,0,0}$	$w^2v^2y^0x^0m_{2,2,0,0}$	$w^3v^1y^0x^0m_{3,1,0,0}$
	$w^0v^1y^0x^4m_{0,1,0,4}$	$w^1v^0y^0x^4m_{1,0,0,4}$		
	$w^0v^2y^0x^3m_{0,2,0,3}$	$w^1v^1y^0x^3m_{1,1,0,3}$	$w^2v^0y^0x^3m_{2,0,0,3}$	
	$w^0v^3y^0x^2m_{0,3,0,2}$	$w^1v^2y^0x^2m_{1,2,0,2}$	$w^2v^1y^0x^2m_{2,1,0,2}$	$w^3v^0y^0x^2m_{3,0,0,2}$
	$w^0v^4y^0x^1m_{0,4,0,1}$	$w^1v^3y^0x^1m_{1,3,0,1}$	$w^2v^2y^0x^1m_{2,2,0,1}$	$w^3v^1y^0x^1m_{3,1,0,1}$
6	$w^0v^5y^0x^0m_{0,5,0,0}$	$w^1v^4y^0x^0m_{1,4,0,0}$	$w^2v^3y^0x^0m_{2,3,0,0}$	$w^3v^2y^0x^0m_{3,2,0,0}$
	...	...	...	...

Доказательство. Универсальное хеширование определяется выражением (1)

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

где $i \ge 0$, $0 \le j \le 2q_0 - 1$, $0 \le t \le 1$, $0 \le r \le q_0$, $i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + rq \le \rho_k$, $m_{i,j,t,r} \in F_q$ - слова сообщения m.

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

$$\{w^j \cdot v^i \cdot y^t \cdot x^r : i(q+2q_0) + j(q+2q_0+1) + t(q+q_0) + r \cdot q \le \rho_k\}.$$

Вычисление $h_{x,y}(m)$ по табл. 3 и 4 включает суммы по уровням. Вычисления по рациональным функциям $w^j \cdot v^i \cdot y^1 \cdot x^r$ отличается умножением всех коэффициентов на значение y^1. Рассмотрим вычисления для первого слоя на уровне $s = 6$. Выражение для суммы коэффициентов имеет вид

$$\Sigma_{s=6} = w^1v^0y^0x^4m_{1,0,0,4} + w^0v^1y^0x^4m_{0,1,0,4} +$$

$$w^2v^0y^0x^3m_{2,0,0,3} + w^1v^1y^0x^3m_{1,1,0,3} + w^0v^2y^0x^3m_{0,2,0,3} +$$

$$w^3v^0y^0x^2m_{3,0,0,2} + w^2v^1y^0x^2m_{2,1,0,2} + w^1v^2y^0x^2m_{1,2,0,2} +$$

Таблица 4

Члены суммы в выражении $h_{x,y}(m)$ с учетом возрастания полюсов рациональных функций $w^j \cdot v^i \cdot y^1 \cdot x^r$ над F_q, $q = 2^5$

Номера уровней s	Мономы $h_{x,y}(m)$ для рациональных функции $w^j \cdot v^i \cdot y^0 \cdot x^r$			
1				
	$w^0v^0y^1x^0m_{0,0,1,0}$			
2				
	$w^0v^0y^1x^1m_{0,0,1,1}$			
	$w^0v^1y^1x^0m_{0,1,1,0}$	$w^1v^0y^1x^0m_{1,0,1,0}$		
3				
	$w^0v^0y^1x^2m_{0,0,1,2}$			
	$w^0v^1y^1x^1m_{0,1,1,1}$	$w^1v^0y^1x^1m_{1,0,1,1}$		
	$w^0v^2y^1x^0m_{0,2,1,0}$	$w^1v^1y^1x^0m_{1,1,1,0}$	$w^2v^0y^1x^0m_{2,0,1,0}$	
4				
	$w^0v^0y^1x^3m_{0,0,1,3}$			
	$w^0v^1y^1x^2m_{0,1,1,2}$	$w^1v^0y^1x^2m_{1,0,1,2}$		
	$w^0v^2y^1x^1m_{0,2,1,1}$	$w^1v^1y^1x^1m_{1,1,1,1}$	$w^2v^0y^1x^1m_{2,0,1,1}$	
	$w^0v^3y^1x^0m_{0,3,1,0}$	$w^1v^2y^1x^0m_{1,2,1,0}$	$w^2v^1y^1x^0m_{2,1,1,0}$	$w^3v^0y^1x^0m_{3,0,1,0}$
5	$w^4v^0y^0x^0m_{4,0,0,0}$			
	$w^0v^1y^1x^3m_{0,1,1,3}$	$w^1v^0y^1x^3m_{1,0,1,3}$		
	$w^0v^2y^1x^2m_{0,2,1,2}$	$w^1v^1y^1x^2m_{1,1,1,2}$	$w^2v^0y^1x^2m_{2,0,1,2}$	
	$w^0v^3y^1x^1m_{0,3,1,1}$	$w^1v^2y^1x^1m_{1,2,1,1}$	$w^2v^1y^1x^1m_{2,1,1,1}$	$w^3v^0y^1x^1m_{3,0,1,1}$
	$w^0v^4y^1x^0m_{0,4,1,1}$	$w^1v^3y^1x^0m_{1,3,1,0}$	$w^2v^2y^1x^0m_{2,2,1,0}$	$w^3v^1y^1x^0m_{3,1,1,0}$
6	$w^4v^1y^0x^0m_{4,1,0,0}$	$w^5v^0y^0x^0m_{5,0,0,0}$		
	...	...		

$$w^0v^3y^0x^2m_{0,3,0,2} +$$

$$w^3v^1y^0x^1m_{3,1,0,1} + w^2v^2y^0x^1m_{2,2,0,1} + w^1v^3y^0x^1m_{1,3,0,1} +$$

$$w^0v^4y^0x^1m_{0,4,0,1} +$$

$$w^3v^2y^0x^0m_{3,2,0,0} + w^2v^3y^0x^0m_{2,3,0,0} + w^1v^4y^0x^0m_{1,4,0,0} +$$

$$w^0v^5y^0x^0m_{0,5,0,0} .$$

После преобразований получим

$$\Sigma_{s=6} = y^0v^5\sum_{r=0}^{4}(x/v)^r\sum_{j=0}^{\min\{5-r,3\}}(w/v)^j .$$

Обобщение для Σ_s в поле F_q, $q = 2q_0^2$, $q_0 = 2^s$ и произвольном s имеет вид

$$\Sigma_s = y^0v^{s-1}\sum_{r=0}^{\min\{s-1,q_0\}}(x/v)^r\sum_{j=0}^{\min\{s-1-r,q_0-1\}}(w/v)^j .$$

Результирующая формула $h_{x,y}(m)$ определяется выражением

$$h_{x,y}(m) = \sum_{t=0}^{1}y^t\sum_{i=0}^{s-t}v^s\sum_{r=0}^{\min\{s-t,q_0-t\}}(x/v)^r\sum_{j=0}^{\min\{s-r,q_0-1\}}(w/v)^j , \quad (4)$$

где s - число уровней для k информационных слов. Параметр s определяется по лемме. В выражении (8) значение s уменьшено на 1, так как вычисления по индексу i начинаются с 0.

Алгоритм хеширования $h_{x,y}(m)$ определяется схемой вычисления Горнера последовательно для четырёх параметров. Вычисления по внутренней сумме определяются значением $\Sigma_j = k$. Сложность вычисления по индексу r определяются числом уровней и строк на каждом уровне.

В случае $s \le q_0$ имеем

$$\Sigma_{r,s\le q_0} = \sum_{\tau=1}^{s\le q_0}\tau(\tau+1)/2 = \\ = s(s+1)(2s+1)/12 + s(s+1)/4 . \quad (5)$$

Пусть $s > q_0$. На уровнях $q_0+1, q_0+2, \ldots$ имеем q_0 умножений на x/v и получим

$$\Sigma_{r,s>q_0} = q_0(q_0+1)(2q_0+1)/12 + \\ + q_0(q_0+1)/4 + (s-q_0)q_0 . \quad (6)$$

Для вычислений по рациональным функциям $w^j \cdot v^i \cdot y^1 \cdot x^r$ в выражениях (5) и (6) следует сделать замену $s \to s-1$ и на уровнях $q_0+1, q_0+2, \ldots$ имеем q_0-1 умножений на x/v.

Сложность вычислений по индексу i в выражении (4) равна $\Sigma_i = s$, где значение s определяется леммой.

Если $s \le q_0$, результирующая оценка сложности вычислений $h_{x,y}(m)$ по схеме Горнера будет иметь вид

$$N_{опер} = \Sigma_j + \Sigma_{r,y=0} + \Sigma_{i,y=0} + \Sigma_{r,y=1} + \Sigma_{i,y=1} =$$

$$k + s(s+1)(2s+1)/12 + s(s+1)/4 +$$

$$+ s(s-1)(2s-1)/12 + s(s-1)/4 + s + s - 1 =$$

$$= k + s^3/3 + s^2/2 + 2s - 1 .$$

В случае $s > q_0$ применим (6) и получим

$$N_{опер} = k + q_0(q_0+1)(2q_0+1)/12 + q_0(q_0+1)/4 +$$

$$+ (s-q_0)q_0 + q_0(q_0-1)(2q_0-1)/12 +$$

$$+ q_0(q_0-1)/4 + (s-q_0)(q_0-1) + s + s - 1 =$$

$$= k + q_0^{\;3}/3 + q_0^{\;2}/2 + (s-q_0)(2q_0-1) + 2s - 1 .$$

Полученные выражения определяют (2) и (3).

Замечание

1. Результаты предложения являются новыми и представлены впервые.

2. Асимптотика оценки сложности универсального хеширования по кривым Сузуки следует из (3). При $s \le q_0$, где $s = (3k)^{1/3}$ число операций сложений и умножений определяется выражением

$$\begin{aligned} N_{опер} &= k + s^3/3 + s^2/2 + 2s - 1 = \\ &= 2k + (3k)^{2/3}/2 + 2(3k)^{1/3} - 1 \end{aligned} . \qquad (7)$$

3. Прямое вычисление $h_{x,y}(m)$ по формуле (1) имеет сложность $N_{опер} = 4k$, без учета возведения в степень рациональных функций базисного пространства.

4. Схема Горнера требует предварительного вычисления w/v и x/v. Выбор точки кривой по ключевым данным реализуется просто, так как решениями уравнения Сузуки являются рациональные точки $P_{a,b} = (a:b:1)$, где $a, b \in F_{q^2}$ Следует исключить точки $P_{a,0}$, $P_{0,b}$ и $P_{a,b}$ для которых $w = 0$ и $v = 0$. Число таких точек меньше $4q$. Пространство ключей равно $q^2 - 4q$.

Выводы

1. Кривая Сузуки $y^q - y = x^{q_0}(x^q - x)$ определена над полем нечетной степени расширения характеристики $p = 2$, F_q $q = 2^{2s+1}$ и является кривой с наибольшим числом точек среди плоских максимальных кривых.

2. Практический алгоритм вычисления хеш кода по рациональными функциями кривой $y^q - y = x^{q_0}(x^q - x)$ определяется схемой вычисления Горнера по четырём суммам со сложностью $N_{опер} = 2k + (3k)^{2/3}/2 + 2(3k)^{1/3} - 1$, и в 2 раза сложнее, чем хеширование по проективной прямой и по максимальным плоским кривым.

Литература

1. Torres F. The Deligne-Lusztig curve associated to the Suzuki group [Текст] / F. Torres // arXiv:alg-geom/9706012v1 26Jun. – 1997.
2. Bierbrauer J. Authentication via algebraic-geometric codes. [Текст] / J. Bierbrauer // URL http://www.math.mtu.edu/~jbierbra/potpap.ps.
3. Халимов Г.З. Аутентификация с применением Эрмитовых кодов. [Текст] / Г.З. Халимов, А.Ю. Иохов // Вестник ХПИ. – Х., -2005. –Вып. 9. – С. 26-32.
4. Халимов Г.З. Универсальное хеширование по максимальным кривым Гурвица [Текст] / Г.З. Халимов // Журнал “Прикладная радиоэлектроника”. Харьков: ХНУРЭ. - 2010. - Т.9, № 3. - С.365-370.
5. Халимов Г.З. Универсальное хеширование по кривой Сузуки [Текст] / Г.З. Халимов, Е.В. Котух // Журнал “Прикладная радиоэлектроника”. Харьков: ХНУРЭ. - 2011. - Т.10, № 2. - С.80-86.