УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО КРИВЫМ ГУРВИЦА

Халимов Г.З.
Харьковский национальный университет радиоэлектроники
61166, Харьков, пр. Ленина, каф. БИТ, тел.(057) 702-14-25,
E-mail: ivanov@kture.kharkov.ua ; факс (057) 702-14-25

Presents result research to curves for target universal hashing up to Carter-Vegman, parameters valuation algebraic curve Hurvitz.

Проблематика построения схем универсального хеширования по Картеру-Вегману на основе алгеброгеометрического кодирования в представлении Биербрауэра и Кабатинского заключается в выборе алгебраических кривых с требуемыми параметрами.

В представлении Биербрауэра и Кабатинского хеш функция $h_{P_j}(m)$ определяется как универсальный хеш класс $\varepsilon - U(N, q^k, q)$ над полем F_q, где вероятность коллизии $\varepsilon \le \frac{u_k}{N}$, N - длина алгебраического кода, u_k - значение полюса рациональной функции $f_k \in F_q(\chi)$. Как следует из алгеброгеометрической конструкции хеш-функции параметр N есть число точек алгебраической кривой. При фиксированном значении полюса u_k вероятность коллизии ε зависит обратно пропорционально от параметра N. Таким образом, целью исследований является поиск кривых с большим числом точек.

Одним из кандидатов алгебраических кривых для целей универсального хеширования является класс кривых Гурвица. Кривые Гурвица $\mathcal{H}_n$ определяются выражением $X^nY + Y^nZ + XZ^n = 0$.

Несингулярность кривых Гурвица над F_q, определяется условиями вида: n и q должны быть взаимно простыми, и $gcd(n^2-n+1,q)=1$. Кривая $\mathcal{H}_n$ имеет род $g = \frac{n^2 - n}{2}$. Существует обобщение кривых Гурвица $\mathcal{H}_{n,l}$ которое имеет вид $X^nY^l + Y^nZ^l + X^lZ^n = 0$, где $n \ge l \ge 2$ и $\Delta(n,l)=n^2-nl+l^2 \ge 2$.

Несингулярность кривых Гурвица $\mathcal{H}_{n,l}$ над F_q, определяется условием ($gcd(\Delta(n,l), char(F_q))=1$. Род кривой $\mathcal{H}_{n,l}$, равен $g = \frac{n^2 - nl + l^2 + 2 - 3\gcd(n,l)}{2}$. Между кривыми Гурвица и Ферма существует морфизм, установленный P. Carbonne, T.Henocq и обобщенный F.Torres. Кривая Гурвица $\mathcal{H}_{n,l}$ является F_q покрытой кривой Ферма $Fr_{n^2-nl+l^2}$ $U^{n^2-nl+l^2} + V^{n^2-nl+l^2} + W^{n^2-nl+l^2} = 0$.

Задачей исследований является оценка числа решений для кривой Гурвица. Число решений кривой Гурвица для произвольного конечного поля определяет следующая теорема.

Теорема 1. Пусть кривая $X^nY^l + Y^nZ^l + X^lZ^n = 0$ определена над конечным полем F_q и является несингулярной. Пусть $gcd(n,l,(q-1))=c>1$ и $\gcd\left(n^2 - nl + l^2, c(q-1)\right) = c^2 d$, тогда имеем следующую оценку для числа точек кривой Гурвица $N = tc^2 d + 3$, где $0 \le t \le q-1$.

Частные результаты по кривым Гурвица представлены следствиями 1÷3.

Следствие 1 Если $gcd(n^2-nl+l^2,q-1)=1$ и $gcd(n,l)=1$, тогда число точек несингулярной кривой Гурвица $\mathcal{H}_{n,l}$ будет равно $N = q + 2$.

Данный случай описывает кривые Гурвица $\mathcal{H}_{n,l}$ с тривиальным числом точек равным $q+2$ и родом $g=\frac{n^2-nl+l^2-1}{2}$.

Следствие 2 Если $gcd(n^2-nl+1^2,q-1)=1$ и $gcd(n,l)=c$, тогда число точек несингулярной кривой Гурвица $\mathcal{H}_{n,l}$ будет равно $N=tc^2+3$.

В данном случае род кривых Гурвица $\mathcal{H}_{n,l}$ равен $g=\frac{n^2-nl+l^2+2-3c}{2}=\frac{c(c\delta-3)}{2}+1$, где $\delta=\frac{n^2-nl+l^2}{c^2}>1$.

Следствие 3 Если $gcd(n^2-nl+1^2,q-1)=d$ и $gcd(n,l)=1$, тогда число точек несингулярной кривой Гурвица $\mathcal{H}_{n,l}$ будет равно $N=td+3$.

Данный случай кривых является наиболее интересным. Имеют место следующие полезные леммы.

Лемма 1 Пусть $n>0$ есть целое число и $\Delta(n,1)=n^2-n+1$ имеет простые делители $d>3$. Тогда $d\equiv 1 \bmod 6$.

Лемма 2 Пусть $n>1$ есть целое число и $\Delta(n,1)=n^2-n+1$. Тогда одним из делителей $\Delta(n,1)$ может быть простой делитель равный 3.

Лемма 3 Пусть $n>0$ есть целое число и $\Delta(n,1)=n^2-n+1$ имеет степенные делители d^e, $d>3$ и $d\equiv 1 \bmod 6$.

Обобщение полученных результатов на случай, когда $l\neq 1$ в параметре $\Delta(n,l)=n^2-nl+l^2$ представлено в лемме 4.

Лемма 4 Пусть $n,l>0$ есть целые взаимно простые числа, $gcd(n,l)=1$ и $\Delta(n,l)=n^2-nl+l^2$. Тогда одним из делителей $\Delta(n,1)$ может быть простой делитель равный 3, делители $d>3$ со свойством $d\equiv 1 \bmod 6$, а так же степенные делители d^e, $d>3$ и $d\equiv 1 \bmod 6$.

Параметр $\Delta(n,l)=n^2-nl+l^2$ имеет следующие свойства:

1. $\Delta(n,l)=\Delta(l,n);$ (1)
2. $\Delta(n,l)=\Delta(n,n-l);$ (2)
3. Если $\gcd(n,l)=1$ и $p>n>l$ является делителем $\Delta(n,l)$, тогда $\Delta(n,l)=\Delta(p-n,p-l)$. (3)
4. Если $\gcd(n,l)=1$ и p является делителем $\Delta(n,l)$, тогда $\Delta(n',l')$ будет иметь делители не выше $p>n>l$, где $n'=n \bmod(p)$, $l'=l \bmod(p)$.
5. $\Delta(cn,cl)=c^2\Delta(n,l).$ (4)

Рассмотрим доказательство свойства 4. Так как $n',l'<p$, тогда возьмём верхнюю оценку $n'=l'=p$. Получим $\Delta(n',l')=p^2-pp+p^2=p^2$. Отсюда следует, что один делитель p, другие не больше чем p. Доказательства свойств 1-3,5 простые.

Замечание. Если $gcd(n^2-nl+1^2,q-1)=1$ и $gcd(n,l)=c$, тогда кривая Гурвица $\mathcal{H}_{n,l}$ покрывается кривой Ферма Fr_c $X^c+Y^c+Z^c=0$, рода $g=\frac{(c-1)(c-2)}{2}$. Следует это из оценок для числа точек кривых. Род кривых Ферма Fr_c меньше рода кривых Гурвица $\mathcal{H}_{n,l}$ данного типа. Сравнение по оценке Дринфельда-Влэдуца показывает, что кривые Гурвица $\mathcal{H}_{n,l}$ для этого случая проигрывают покрывающим кривым Ферма.

Следующая теорема определяет существование нетривиальных кривых Гурвица $\mathcal{H}_{n,l}$, для случая $gcd(n^2-nl+l^2,q-1)=d$ и $gcd(n,l)=1$.

Теорема 2. Пусть задано конечное поле F_q и $n,l>0$ есть целые взаимно простые числа, $gcd(n,l)=1$. Нетривиальная кривая Гурвица $\mathcal{H}_{n,l}$ $X^nY^l+Y^nZ^l+X^lZ^n=0$ существует, если

$\gcd\left(n^2 - nl + l^2, (q-1)\right)$ содержит делители $d_i^e > 3$ такие, что $d_i \equiv 1 \bmod 6$, а так же делитель равный 3, где $e \geq 1$.

Решение обратной задачи построения нетривиальных кривых Гурвица $\mathcal{H}_{n,l}$ по делителям порядка поля F_q представлено теоремой 3.

Теорема 3. Пусть задано конечное поле F_q. Делители порядка поля $q-1$ есть числа $p_1, p_2, \ldots, p_k$, удовлетворяющие условиям $p_i \equiv 1 \bmod 6$ для всех i, кроме, может быть одного делителя равного 3. Степень n нетривиальной кривой Гурвица $\mathcal{H}_n$ $X^n Y + Y^n Z + XZ^n = 0$ определяется выражением

$$n = n_1 P_1 + n_2 P_2 + \ldots + n_k P_k \pmod{p_1 p_2 \ldots p_k}, \tag{5}$$

$$P_i = b_i \prod_{\substack{s=1 \\ s \neq i}}^{k} p_s \equiv 1 (\bmod p_i), \tag{6}$$

где $n_1, n_2, \ldots, n_k$ – образующие элементы мультипликативных подгрупп 6-го и 2-го порядков по модулям $p_1, p_2, \ldots, p_k$, а b_i – целые числа.

Решение задачи построения обобщенных кривых Гурвица $\mathcal{H}_{n,l}$ с заданным числом точек и наименьшим родом, оптимальных в этом смысле, определяется теоремой 4.

Теорема 4. Пусть задано конечное поле F_q. Делители порядка поля $q-1$ есть числа $p_1, p_2, \ldots, p_k$, удовлетворяющие условиям $p_i \equiv 1 \bmod 6$ для всех i, кроме, может быть одного делителя равного 3. Тогда существует обобщенная кривая Гурвица $\mathcal{H}_{n,l}$ $X^n Y^l + Y^n Z^l + X^l Z^n = 0$, такая что $\gcd\left(n^2 - nl + l^2, (q-1)\right) = p_1 p_2 \ldots p_k$.

Выводы. 1. По свойству покрытия, максимальные кривые Гурвица существуют, если они покрываются максимальными кривыми Ферма. В силу существования максимальных кривых Ферма можно утверждать, что существуют и максимальные кривые Гурвица. Практические вычисления в расширенных полях подтверждают это утверждение.

2. Сравнение кривых Гурвица и покрывающих кривых Ферма по параметру рода, показывает, что род кривых Гурвица меньше, чем род покрывающих кривых Ферма. Таким образом, присутствует смещение по роду и соответственно по числу точек максимальных кривых в область меньших значений. По максимальному числу точек кривые Гурвица уступают кривым Ферма.

3. Теоремы 3 и 4 являются конструктивными, позволяют для заданного поля построить все нетривиальные кривые Гурвица, с числом точек превышающим размерность поля.

4. Свойства класса универсальных хеш функций определяются родом кривых и числом их точек. Хеш функции по кривым Гурвица уступают хеш классу по кривым Ферма.