УДК 681.3.06

О.Г. ХАЛИМОВ, Е.В. АЛЕКСИ, Г.З. ХАЛИМОВ

ПОСТРОЕНИЕ НЕТРИВИАЛЬНЫХ КРИВЫХ ГУРВИЦА

Универсальное хеширование по алгебраическим кривым χ над конечным полем F_q на основе скалярного произведения по рациональным функциям линейного базисного пространства $f_i \in F_q(\chi) \setminus \{0\}$ для сообщения $m = (m_1,..., m_k)$, $m_i \in F_q$ в точке кривой P_j определяется вычислением $h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i$. Вероятность коллизии определяется отношением $\varepsilon = \rho_k / N$, где ρ_k – максимальное значение полюса рациональной функции, f_k и N – число точек алгебраической кривой [1]. Основная проблематика реализации универсального хеширования по алгебраическим кривым состоит в построении проективного многообразия с наибольшим отношением числа точек кривой к ее роду. Для случая простого поля универсальное хеширование по кривым Гурвица имеет абсолютно наилучший результат [2]. В работе [3] представлено решение задачи построения максимальных кривых Гурвица. Оценки параметров наилучших кривых Гурвица в простом, кубическом поле представлены в [2, 4]. Важной научной задачей является разработка метода построение кривых Гурвица без ограничений на показатели степени кривой над произвольным конечным полем с уменьшенной сложностью вычислений.

В данной работе предлагается метод построения кривых Гурвица минимального рода по делителям порядка конечного поля. С этой целью в разд. 1 приводятся определение и основные результаты по кривым Гурвица. В разд. 2 представлен переборный метод построения кривых Гурвица по делителям порядка конечного поля.

1. Определения и результаты по кривым Гурвица в конечном поле

Многообразие нетривиальных кривых Гурвица определяется значениями делителей порядка поля.

Утверждение 1[5]**.** Пусть F_q конечное поле и $q-1 = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, $e_i \geq 1$. Нетривиальные кривые Гурвица $H_{n,l}$, $n > l$ принадлежат одному из семейств:

a) $X^n Y + Y^n Z + X Z^n = 0$, если $\Delta(n, l=1) = n^2 - n + 1 = p_i \cdot ... \cdot p_j$;

b) $X^n Y^l + Y^n Z^l + X^l Z^n = 0$, если $\Delta(n,l) = n^2 - nl + l^2 = p_i \cdot ... \cdot p_j$;

c) $X^{cn} Y^{cl} + Y^{cn} Z^{cl} + X^{cl} Z^{cn} = 0$, если $\Delta(cn, cl) == c^2 \cdot p_i \cdot ... \cdot p_j$;

d) $X^c Y^c + Y^c Z^c + X^c Z^c = 0$, если $\Delta(c,c) = c^2$,

где делители $p_i,..., p_j$ тождественны 1 по *mod 6* кроме, делителя равного 3, все $c, p_i,..., p_j$ взяты из набора делителей порядка поля $q-1 = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ и $\gcd(n,l) > 1$.

Условия эквивалентных кривых Гурвица определяются следующими утверждениями.

Утверждение 2 [5]**.** В конечном поле F_q обобщенные кривые Гурвица $X^n Y^l + Y^n Z^l + X^l Z^n = 0$ и $X^n Y^{n-l} + Y^n Z^{n-l} + X^{n-l} Z^n = 0$, $n > l$ являются кривыми одного рода и имеют одинаковое число точек.

Утверждение 3. Кривые Гурвица $X^n Y^l + Y^n Z^l + X^l Z^n = 0$ и $X^l Y^n + Y^l Z^n + X^n Z^l = 0$ являются эквивалентными кривыми одного рода и имеют одинаковые точки с точность до перестановки координат.

Замечание 1.

1. Уравнения a) и b) утверждения 1 определяют кривые Гурвица H_n и $H_{n,l}$. Уравнения c) и d) являются производными от кривых a) и b) и определяются по делителям порядка конечного поля.

2. Утверждения 2 и 3 определяют, что можно построить кривую

$$X^l Y^n + Y^l Z^n + X^n Z^l = 0,\ n > l$$

и затем построить кривые Гурвица $X^n Y^l + Y^n Z^l + X^l Z^n = 0$ и $X^n Y^{n-l} + Y^n Z^{n-l} + X^{n-l} Z^n = 0$.

3. Утверждение 3 является очевидным.

Род кривой Гурвица определяется выражением

$$g = (n^2 - nl + l^2 + 2 - 3\gcd(n,l))/2 = (\Delta(n,l) + 2 - 3\gcd(n,l))/2. \quad (1)$$

Замечание 2.

1. Род кривой определяется делителями порядка поля, так как

$$\Delta(n,l) = n^2 - nl + l^2 = p_i \cdot \ldots \cdot p_j,$$

что впервые отмечено в [6].

2. Кривые с числом точек $N \neq q+2$ называются нетривиальными [6].

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

Теорема 1[6]**.** Пусть задано конечное поле F_q и $n,l > 0$, $\gcd(n,l) = 1$. Нетривиальная кривая Гурвица $H_{n,l}$ $X^n Y^l + Y^n Z^l + X^l Z^n = 0$ существует, если $\gcd(n^2 - nl + l^2, q-1)$ содержит делители $d_i^e > 3$ такие, что $d_i \equiv 1 \bmod 6$, а так же делитель равный 3, где $e \geq 1$.

Построение нетривиальных кривых Гурвица H_n по делителям порядка поля F_q определяется теоремой 3.

Теорема 2[6]**.** Пусть задано конечное поле F_q. Делители порядка поля $q-1$ есть числа $p_i \equiv 1 \bmod 6$, для $\forall i$ кроме, может быть одного делителя равного 3. Степень n нетривиальной кривой Гурвица $X^n Y + Y^n Z + XZ^n = 0$ определяется выражением

$$n = n_1 P_1 + n_2 P_2 + \ldots + n_k P_k \bmod p_1 \cdot p_2 \cdot \ldots \cdot p_k, \quad (2)$$

$$P_i = b_i \prod_{\substack{s=1 \\ s \neq i}}^{k} p_s \equiv 1 (\bmod p_i), \quad (3)$$

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.

Действие теоремы представлено в примере 1 [7].

Замечание 3.

1. Применение теоремы 2 приводит к кривым Гурвица H_n с разными значениям показателя степени n, в зависимости от выбора образующих элементов мультипликативных подгрупп 6-го порядка по модулям $p_1, p_2, \ldots, p_k$. Кривые H_n при различных показателях степени имеют одинаковое число точек (см. доказательство утверждения 1 [5]) и разные значения рода (см. выражение (1)).

2. Кривые H_n, построенные по делителям порядка поля, являются избыточными по роду, если в разложении $\Delta(n, l=1) = n^2 - n + 1 = p_i \cdot \ldots \cdot p_j$ содержатся делители, которые не являются делителями порядка поля.

3. Приведение к кривым наименьшего рода реализуется через обобщенные кривые Гурвица $H_{n,l}$. Вычисление показателей n и l кривых осуществляется методом последовательного перебора значений наименьшего показателя степени l и вычисления второго показателя по модулю $n' \equiv n \cdot l \bmod p_1 p_2 p_3$ с проверкой разложения на делители $\Delta(n', l)$. Алгоритм останавливается, когда выполнится условие $\Delta(n', l) = p_1 \cdot p_2 \cdot p_3$.

4. Теорема 2 не дает прямого ответа на вопрос как построить кривые Гурвица H_n по одному делителю порядка поля. В работе [7] для случая вычислений по одному делителю порядка поля показано, что можно дополнить вычисления (2), (3) еще одним делителем.

Существование обобщенных кривых с наименьшим значением параметра $\Delta(n,l) = p_1 \cdot p_2 \cdot p_3$ определяется теоремой 3 [5].

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

Выводы

1. Вычислительные затраты на приведение кривых Гурвица H_n к обобщенным кривым $H_{n,l}$ минимального рода определяются размером делителей порядка конечного поля и являются пропорциональными произведению этих делителей. Вычисления для практически важных конструкций кривых над большими полями $\approx 2^{64} \div 2^{128}$ становятся существенными.

2. Для построения обобщенной кривой минимального рода с наименьшими показателями степеней n и l следует выполнить вычисления для всех обычных кривых, построенных по теореме 2, что дополнительно увеличивает сложность вычислений.

Ниже рассматривается переборный метод построения кривых Гурвица по делителям порядка поля.

2. Переборный метод построения кривых Гурвица по делителям порядка поля

Метод построения кривых Гурвица на основе приведения к обобщенным кривым $H_{n,l}$ наименьшего рода по теоремам 2 и 3 определяется последовательным перебором значений наименьшего показателя степени l и вычислением второго показателя по модулю $n' \equiv n \cdot l \bmod p_1 \cdot p_2 \cdots p_k$ с проверкой условия $\Delta(n', l) = p_1 \cdot p_2 \cdots p_k$. Реализуется последовательный спуск от кривых избыточного рода с показателем $\Delta(n, l = 1)$ к без избыточной кривой с $\Delta(n', l) < \Delta(n, l = 1)$.

Для заданного значения $\Delta(n,l)$ пределы изменения значения показателя n определяются леммами 1 и 2 [7].

Лемма 1. Параметр $\Delta(n,l)$ лежит в диапазоне

$$n^2 - n^2/4 \le \Delta(n,l) \le n^2 - n + 1. \qquad (4)$$

Лемма 2. Показатель степени кривой Гурвица $H_{n,l}$

$$\sqrt{\Delta(n,l)} < n < 2\sqrt{\Delta(n,l)}/\sqrt{3} \qquad (5)$$

Свойства показателя $\Delta(n,l)$ представлены в предложении 1.

Предложение 1. Пусть $n > l$ и $1 \le l \le n/2$. Справедливо следующее:

$$1.\ \Delta(n, l-1) - \Delta(n,l) = n - 2l + 1; \qquad (6)$$

2. $\sum_{l=m+1}^{n/2}\Delta(n,m-1)-\Delta(n,m)=(n/2-m)^2$, если n четное; (7)

3. $\sum_{l=m+1}^{\lceil n/2\rceil}\Delta(n,m-1)-\Delta(n,m)=(\lceil n/2\rceil-m)((n-1)/2-m)$, (8)

если n нечетное, $\lceil\bullet\rceil$ – округление к большему целому.

Доказательство. Выражение (6) следует из подстановки $\Delta(n,l)=n^2-nl+l^2$.

Пусть n четное, легко заметить, что выражение (12) является суммой нечетных чисел $1+3+5+\ldots+(n-2(m+1)+1)$, откуда следует (7).

Аналогично для нечетного n, просто показать, что выражение (8) является суммой четных чисел $0+2+4+\ldots+(n-2(m+1)+1)$. ◊

Пример 1. Для $n=\overline{5,20}$, $l=\overline{1,10}$ построить кривые Гурвица.

Вычислим $\Delta(n,l)=n^2-nl+l^2$ для $n=\overline{5,20}$, $l=\overline{1,10}$ со значениями в таблице.

	Значение параметра $\Delta(n,l)=n^2-nl+l^2$									
n/l	1	2	3	4	5	6	7	8	9	10
20	381	364	349	336	325	316	309	304	301	300
19	343	327	313	301	291	283	277	273	271	271
18	307	292	279	268	259	252	247	244	243	244
17	273	259	247	237	229	223	219	217	217	219
16	241	228	217	208	201	196	193	192	193	196
15	211	199	189	181	175	171	169	169	171	175
14	183	172	163	156	151	148	147	148	151	156
13	157	147	139	133	129	127	127	129	133	139
12	133	124	117	112	109	108	109	112	117	124
11	111	103	97	93	91	91	93	97	103	111
10	91	84	79	76	75	76	79	84	91	100
9	73	67	63	61	61	63	67	73	81	
8	57	52	49	48	49	52	57	64		
7	43	39	37	37	39	43	49			
6	31	28	27	28	31	36				
5	21	19	19	21	25					

Уравнение a) утверждения 1 определяет кривые Гурвица H_n с параметром $\Delta(n,l=1)=n^2-n+1$ в первом столбце таблицы. Обобщенные кривые $H_{n,l}$ $l\geq 2$ задаются всеми остальными столбцами. Под уравнение b) утверждения 1 попадают кривые $X^nY^l+Y^nZ^l+X^lZ^n=0$ с параметром $\Delta(n,l)=n^2-nl+l^2=p_i\cdot\ldots\cdot p_j$ и для $\forall t$ делители $p_t\equiv 1 \bmod 6$ и может быть один $p_s=3$. Например, кривая $X^{16}Y^3+Y^{16}Z^3+X^3Z^{16}$ имеет $\Delta(16,3)=217=7\cdot 31$. Уравнение c) $X^{cn}Y^{cl}+Y^{cn}Z^{cl}+X^{cl}Z^{cn}=0$ является производным от кривых a) и b), и определяется по делителям порядка конечного поля. Кривая $X^{16}Y^2+Y^{16}Z^2+X^2Z^{16}$ с $\Delta(16,2)=228=4\cdot 57$ является производной от кривой $X^8Y+Y^8Z+XZ^8$ с $\Delta(8,1)=57=3\cdot 19$. Так как утверждение 2 определяют эквивалентность $X^nY^l+Y^nZ^l+X^lZ^n=0$ и $X^nY^{n-l}+Y^nZ^{n-l}+X^{n-l}Z^n=0$, все вычисления можно ограничить условием $l=\overline{1,m/2}$.

Замечание 4.

1. Значения $\Delta(n,l)=n^2-nl+l^2$ определяют кривые Гурвица над конечным полем и могут быть заданы по делителям порядка поля.

2. Представление $\Delta(n,l)=n^2-nl+l^2$ в таблице демонстрирует метод построения кривых Гурвица на основе задания значения $\Delta(n,l)$ по делителям порядка поля и нахождения степеней n и l.

Утверждения 1 – 3, леммы 1, 2 и предложение 1 определяют переборный метод построения кривых Гурвица минимального рода по заданному набору делителей порядка поля. Основными шагами являются следующие.

1. Фиксируем конечное поле F_q, разложение порядка поля $q-1$ на сомножители, в общем случае, со степенями $q-1=p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}$, $e_i\geq 1$ и набор делителей $p_i,\ldots,p_j$ которые по модулю 6 тождественны единице и, если существует, сомножитель равный 3.

2. Фиксируем делители из набора $p_i,\ldots,p_j$, для которых вычисляем искомое значение параметра $\Delta=p_i\cdot\ldots\cdot p_j$.

3. По лемме 2 фиксируем целочисленные начальное и конечное значения показателя степени кривой Гурвица $H_{n,l}$

$$\sqrt{\Delta}\leq n\leq 2\sqrt{\Delta}/\sqrt{3}.$$

4. Перебираем последовательно значение параметра n от $\lceil\sqrt{\Delta}\rceil$, где $\lceil\bullet\rceil$ округление до наибольшего целого и вычисляем $\Delta'(n,l=\lceil n/2\rceil)=\Delta'$

5. По предложению 1 для поиска искомых n и l для фиксированного четного n вычисляем

$$\begin{gathered}\Delta-\Delta'=(n/2-m)^2,\\ r=\sqrt{\Delta-\Delta'},\\ l=m=n/2-r.\end{gathered}\qquad(9)$$

Если $r=\sqrt{\Delta-\Delta'}$ - целочисленное, тогда l является искомым.

Для нечетного n имеем следующие выражения

$$\begin{gathered}\Delta-\Delta'=(\lceil n/2\rceil-m)((n-1)/2-m),\\ r=\lfloor\sqrt{\Delta-\Delta'}\rfloor,\ \lfloor\bullet\rfloor\text{-округление к наименьшему целому},\\ l=m=(n-1)/2-r.\end{gathered}\qquad(10)$$

Если $r(r+1)=\Delta-\Delta'$, тогда l является искомым.

6. Искомая кривая Гурвица минимального рода определяется первыми найденными показателями степеней n и l на пространстве значений $\sqrt{\Delta}\leq n\leq 2\sqrt{\Delta}/\sqrt{3}$, $l\leq n/2$.

Замечание 5.

1. Переборный метод построения кривых Гурвица по делителям порядка поля реализует последовательный подъем от кривых с наименьшими показателями степеней к искомым, которые соответствуют заданному значению $\Delta(n,l)$.

2. Метод не требует предварительных вычислений кривых Гурвица H_n по теореме 2.

Пример 2. Пусть $\Delta(n,l)=301=7\cdot 43$. Требуется построить кривую Гурвица $H_{n,l}$ минимального рода.

Вычислим границы для показателя n по лемме 2, получим $17<n\leq 20$.

Фиксируем $n=18$. Вычисляем по выражениям (9):

$$\begin{gathered}\Delta'(18,l=9)=243\\ \Delta-\Delta'=58,\\ r=\sqrt{\Delta-\Delta'}\approx 7{,}62,\end{gathered}$$

Так $r=\sqrt{\Delta-\Delta'}$ - не целочисленное, увеличиваем $n=19$.

Повторяем вычисления нечетного n по формулам (10):

$$\Delta'(19, l=10) = 271,$$
$$\Delta - \Delta' = 30,$$
$$r = \left\lfloor \sqrt{\Delta - \Delta'} \right\rfloor = 5,$$

Так как $r(r+1) = \Delta - \Delta'$, тогда l является искомым и определяется значением

$$l = (n-1)/2 - r = 9 - 5 = 4.$$

Получим кривую Гурвица $X^{19}Y^4 + Y^{19}Z^4 + X^4Z^{19}$ с $\Delta(19,4) = 301$.

Замечание 6.

1. Вычисления по предложенному методу позволяют найти все кривые с $\Delta(n,l) = 301 = 7 \cdot 43$. Следующая кривая имеет вид $X^{20}Y^9 + Y^{20}Z^9 + X^9Z^{20}$. По утверждению 2 получим еще две кривые Гурвица. Число кривых определяется числом делителей $\Delta(n,l)$ и числом образующих элементов мультипликативных подгрупп 6-го и 2-го порядков по модулям этих делителей.

2. Для практически применений достаточно получить первую кривую с наименьшими показателями n и l. Значения показателей степеней будут определять значения полюсов рациональных функций функционального поля ассоциированного с точками кривой и, в конечном счете, вероятность коллизии при универсальном хешировании.

Выводы

1. Предложен переборный метод построения кривых Гурвица по делителям порядка конечного поля на основе последовательного подъема от кривых с наименьшими показателями степеней к искомым, которые соответствуют заданному значению $\Delta(n,l)$, который позволяет сократить время вычисления степенных показателей кривой и получить кривую с наименьшими значениями показателей степеней n и l.

Список литературы: 1. *Халимов, Г.З.* Максимальные кривые Гурвица для целей универсального хеширования // Материалы XI Междунар. науч.-практ. конф. «Информационная безопасность». Ч. 3. – Таганрог : Изд-во ТТИ ЮФУ, 2010. – С.144-146. 2. *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. 3. *Халимов, Г.З.* Универсальное хеширование по максимальным кривым Гурвица / Г.З. Халимов // Прикладная радиоэлектроника. – Харьков : ХНУРЭ. – 2010. – Т.9, № 3. – С.365-370. 4. *Халимов, Г.З.* Кривые Гурвица с большим числом точек в расширенных конечных полях / Г.З.Халимов // Системи управління, навігації та зв'язку / Міністерство промислової політики України, ДП «Центральний науково-дослідний інститут навігації і управління». – Київ, 2011. – Вип. 2(18). – С.185-189. 5. *Халимов, Г.З.* Условия построения нетривиальных кривых Гурвица / Г.З.Халимов // Системи управління, навігації та зв'язку / Міністерство промислової політики України, ДП «Центральний науково-дослідний інститут навігації і управління» – Київ, 2010. – Вип 3(15). – С.125-129. 6. *Халимов, Г.З.* Условия существования нетривиальных кривых Гурвица / Г.З. Халимов // Системи обробки інформації МО України / Харківський університет Повітряних Сил ім. Івана Кожедуба. – 2010. – Вип. 6(87). -С. 229-233. 7. *Халимов, О.Г.* Универсальное хеширование по обобщенным кривым Гурвица / О.Г.Халимов, А.Н.Герцог // Радиотехника. – 2012. – Вып 171. – С.140-146.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 12.12.2013