# ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 681.3.06

## ПОСТРОЕНИЕ КРИВЫХ ГУРВИЦА ДЛЯ УНИВЕРСАЛЬНОГО ХЕШИРОВАНИЯ

**О.Г. ХАЛИМОВ**[1]
**А.Д. БУХАНЦОВ**[2]
**Г.З. ХАЛИМОВ**[1]

[1)]*Харьковский национальный университет радиоэлектроники*

[2)]*Белгородский государственный Национальный исследовательский университет*

*e-mail:*
*gennadykhalimov@mail.ru*
*bukhantsov@bsu.edu.ru*

Представлен метод построения кривых Гурвица по делителям порядка конечного поля на основе последовательного подъёма показателей кривых от наименьшего значения старшего показателя к искомому, что позволяет сократить время вычисления степенных показателей кривой и получить кривую с наилучшим отношением числа точек к роду кривой.

Ключевые слова: универсальное хеширование, алгебраические кривые Гурвица.

Универсальное хеширование по алгебраическим кривым $\chi$ 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 $m = (m_1,\ldots,m_k)$, $m_i \in F_q$ 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 $\rho_k$ – максимальное значение полюса рациональной функции $f_k$ и $N$ – число точек алгебраической кривой [1]. Практическое универсальное хеширование реализуется в конечных полях размерности $2^{64} \div 2^{128}$. Классическое решение задачи построения хеширования по максимальным кривым третьего рода в квадратичном поле представлено в [2]. Быстрые вычисления $h_{P_j}(m)$ в простом поле определяют проблематику построения алгебраических кривых заданного рода с большим числом точек. Для простого поля наилучший результат достигается по кривым Гурвица [3]. Основные результаты по кривым Гурвица представлены в [4–7].

Впервые оценки параметров кривых Гурвица в конечном поле получены в [4] и развиты в работах [5-8]. Решение задачи построения максимальных кривых Гурвица представлено в [1, 5, 9]. Важной научной задачей является разработка метода построение кривых Гурвица заданного рода без ограничений на показатели степени над произвольным конечным полем с уменьшенной сложностью вычислений.

Целью статьи является разработка метода построения кривых Гурвица заданного рода по делителям порядка конечного поля. С этой целью в разделе 1 приводятся основные результаты и определения по кривым Гурвица. В разделе 2 представлен метод построения кривых Гурвица на основе последовательного подъёма показателей кривых.

**1. Основные результаты по кривым Гурвица в конечном поле.**

Многообразие нетривиальных кривых Гурвица определяется значениями делителей порядка поля.

Утверждение 1[6]. Пусть $F_q$ конечное поле и $q-1=p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$, $e_i\geq 1$. Нетривиальные кривые Гурвица $H_{n,l}$, $n>l$ принадлежат одному из семейств:

a) $X^nY+Y^nZ+XZ^n=0$, если $\Delta(n,l=1)=n^2-n+1=p_i\cdot\ldots\cdot p_j$;

b) $X^nY^l+Y^nZ^l+X^lZ^n=0$, если $\Delta(n,l)=n^2-nl+l^2=p_i\cdot\ldots\cdot p_j$;

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

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

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

Замечание 1.

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

2. 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.

3. Просто показать, что кривые Гурвица $X^nY^l+Y^nZ^l+X^lZ^n=0$, $X^lY^n+Y^lZ^n+X^nZ^l=0$ и $X^nY^{n-l}+Y^nZ^{n-l}+X^{n-l}Z^n=0$, $n>l$ являются кривыми одного рода и имеют одинаковое число точек с точность до перестановки координат.

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. 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 [7].

Вычисления по кривым Гурвица для простого поля $F_q$, $q=2011$ представлены в табл. 1. Максимальных кривых в простом поле не существует, за исключением тривиального случая квадратичного уравнения.

Замечание 3. Как следует из прямых вычислений для кривых Гурвица при малом роде число точек кривых почти равняется порядку простого поля и только когда $g\geq q$ значение $N/q$ становится существенно больше единицы.

Существование обобщенных кривых с наименьшим значением параметра $\Delta(n,l)=p_1\cdot p_2\cdot p_3$ определяется теоремой 1 [6].

Теорема 1. Пусть задано конечное поле $F_q$. Делители порядка поля $q-1$ есть числа $p_1,p_2,\dots,p_k$ и $p_i\equiv 1\bmod 6$, для $\forall i$ кроме, может быть одного делителя равного 3. Тогда существует обобщенная кривая Гурвица $H_{n,l}$ $X^nY^l+Y^nZ^l+X^lZ^n=0$, такая что $\gcd(n^2-nl+l^2,(q-1))=p_1p_2\dots p_k$.

*Таблица 1*

**Параметры кривых Гурвица над простым полем $F_q$**

| $q$ | $q-1=$ $p_1 p_2 \ldots$ | $H_{n,l}\ (n,l)$ | $\Delta(n,l)=n^2-nl+l^2$ | $N$ | $g$ | $N_H$ | $N/N_H$ | $N/q$ |
|---|---|---|---|---|---|---|---|---|
| 2011 | 2·3·5·67 | (2,1) | 3=3 | 1953 | 1 | 2101 | 0,93 | 0,97 |
| | | (9,2) | 67=67 | 1544 | 33 | 4949 | 0,312 | 0,77 |
| | | (16,5) | 201=3·67 | 1611 | 100 | 10912 | 0,148 | 0,8 |
| | | (4,2) | 12=2²·3 | 2043 | 4 | 2368 | 0,863 | 1,02 |
| | | (6,3) | 27=3³ | 1947 | 10 | 2902 | 0,671 | 0,97 |
| | | (10,5) | 75=3·5² | 2403 | 31 | 4771 | 0,504 | 1,19 |
| | | (12,6) | 108=2²·3³ | 1515 | 46 | 6106 | 0,248 | 0,75 |
| | | (18,4) | 268=2²·67 | 2147 | 132 | 13760 | 0,156 | 1,07 |
| | | (20,10) | 300=2²·3·5² | 603 | 136 | 14116 | 0,043 | 0,3 |
| | | (27,6) | 603=3²·67 | 1812 | 298 | 28534 | 0,064 | 0,9 |
| | | (30,15) | 675=3³·5**2 | 2703 | 316 | 30136 | 0,09 | 1,34 |
| | | (32,10) | 804=2²·3·67 | 4023 | 400 | 37612 | 0,107 | 2 |
| | | (45,10) | 1675=5²·67 | 3353 | 831 | 75971 | 0,044 | 1,67 |
| | | (48,15) | 1809=3³·67 | 1812 | 901 | 82201 | 0,022 | 0,9 |
| | | (80,25) | 5025=3·5²·67 | 10053 | 2506 | 225046 | 0,045 | 5 |
| | | **(90,20)** | **6700=2²·5²·67** | **13403** | **3336** | **298916** | **0,045** | **6,66** |
| | | **(134,67)** | **13467=3·67²** | **26937** | **6634** | **592438** | **0,045** | **13,39** |
| | | **(160,50)** | **20100=2²·3·5²·67** | **40203** | **10036** | **895216** | **0,045** | **19,99** |
| | | **(268,134)** | **53868=2²·3·67²** | **107739** | **26734** | **2381338** | **0,045** | **53,57** |
| | | **(670,335)** | **336675=3·5²·67²** | **673353** | **167836** | **14939416** | **0,045** | **334,83** |
| | | **(1340,670)** | **1346700=2²·3·5²·67²** | **2693403** | **672346** | **59840806** | **0,045** | **1339,34** |

Прмечание: жирным шрифтом выделены кривые с параметрами отношения $N/q>1$, $N_H$ – значение границы Хассе-Вейля числа точек для кривой рода $g$.

Построение нетривиальных кривых Гурвица $H_n$ по делителям порядка поля $F_q$ определяется теоремой 2.

Теорема 2 [7]. 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 $X^nY+Y^nZ+XZ^n=0$ определяется выражением

$$n = n_1P_1 + n_2P_2 + \ldots + n_kP_k \bmod p_1 \cdot p_2 \cdot \ldots \cdot p_k, \quad (2)$$

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

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.

Пример 1. Пусть задано конечное поле $F_q$, $q=2^{32}-3713$. Среди делителей порядка поля $q-1$ есть числа $p_1=13$, $p_2=43$, $p_3=7$. Построить по делителям $p_1, p_2, p_3$ нетривиальную кривую Гурвица $H_n$.

Решение. Делители $p_1, p_2, p_3$ определяют мультипликативные подгруппы 6-го порядка так как $p_i \equiv 1 \bmod 6$, $i=\overline{1,3}$. Каждая мультипликативная подгруппа определяется двумя образующими элементам (по вычислениям из формулы Эйлера). Просто показать, что образующие элементы для подгрупп по модулям $p_i$, $i=\overline{1,3}$ принимают значения:

- $n_1 = 4$ и 10 для подгруппы по модулю $p_1 = 13$;
- $n_2 = 7$ и 37 для подгруппы по модулю $p_2 = 43$;
- $n_3 = 3$ и 5 для подгруппы по модулю $p_3 = 7$.

Вычисления по формуле (3) дадут следующие значения параметров $P_1, P_2, P_3$:

- $P_1 = b_1 p_2 p_3 = b_1 43 \cdot 7 = 7 \cdot 301 = 2107 \equiv 1 \bmod 13$;
- $P_2 = b_2 p_1 p_3 = b_2 13 \cdot 7 = 26 \cdot 91 = 2366 \equiv 1 \bmod 43$;
- $P_3 = b_3 p_1 p_2 = b_3 13 \cdot 43 = 6 \cdot 559 = 3354 \equiv 1 \bmod 7$.

Вычисления по формуле (2) по модулю $P_1 \cdot P_2 \cdot P_3 = 13 \cdot 43 \cdot 7 = 3913$ приводит к кривым Гурвица следующего вида:

- $X^{3748}Y + Y^{3748}Z + XZ^{3748} = 0$, для $n_1 = 4$, $n_2 = 7$, $n_3 = 3$;
- $X^{2630}Y + Y^{2630}Z + XZ^{2630} = 0$, для $n_1 = 4$, $n_2 = 7$, $n_3 = 5$;
- $X^{738}Y + Y^{738}Z + XZ^{738} = 0$, для $n_1 = 10$, $n_2 = 7$, $n_3 = 3$;
- $X^{381}Y + Y^{381}Z + XZ^{381} = 0$, для $n_1 = 4$, $n_2 = 37$, $n_3 = 3$;
- $X^{1284}Y + Y^{1284}Z + XZ^{1284} = 0$, для $n_1 = 10$, $n_2 = 37$, $n_3 = 3$;
- $X^{3533}Y + Y^{3533}Z + XZ^{3533} = 0$, для $n_1 = 10$, $n_2 = 7$, $n_3 = 5$;
- $X^{3176}Y + Y^{3176}Z + XZ^{3176} = 0$, для $n_1 = 4$, $n_2 = 37$, $n_3 = 5$;
- $X^{166}Y + Y^{166}Z + XZ^{166} = 0$, для $n_1 = 10$, $n_2 = 37$, $n_3 = 5$.

Замечание 4.

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 $p_1, p_2, \ldots, p_k$. При этом кривые $H_n$ при различных показателях степени имеют одинаковое число точек (см. утверждение 1 [6]) 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. Все кривые из примера 1 являются избыточными по роду, так как параметр $\Delta(n, l = 1) = n^2 - n + 1$ имеет не только заданный набор делителей $p_1 = 13$, $p_2 = 43$, $p_3 = 7$.

3. Приведение к кривым наименьшего рода реализуется через обобщенные кривые Гурвица $H_{n,l}$ по представлению теоремы 1. 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. В случае вычислений по одному делителю порядка поля можно дополнить вычисления (2), (3) еще одним делителем.

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. Метод построения кривых Гурвица на основе последовательного подъёма показателей кривых.**

Метод построения кривых Гурвица на основе приведения к обобщенным кривым $H_{n,l}$ наименьшего рода по теоремам 1 и 2 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 [10].

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

$$n^2 - n^2/4 \le \Delta(n,l) \le n^2 - n + 1. \quad (3)$$

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

$$\sqrt{\Delta(n,l)} < n < 2\sqrt{\Delta(n,l)}/\sqrt{3} \quad (4)$$

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

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

1. $\Delta(n,l-1) - \Delta(n,l) = n - 2l + 1$; (5)
2. $\sum_{l=m+1}^{n/2} \Delta(n,m-1) - \Delta(n,m) = (n/2 - m)^2$, если $n$ четное; (6)
3. $\sum_{l=m+1}^{\lceil n/2 \rceil} \Delta(n,m-1) - \Delta(n,m) = (\lceil n/2 \rceil - m)((n-1)/2 - m)$, (7)

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

Доказательство. Выражение (5) следует из подстановки $\Delta(n,l) = n^2 - nl + l^2$.

Пусть $n$ четное, легко заметить, что выражение (6) является суммой нечетных чисел $1 + 3 + 5 + \ldots + (n - 2(m+1) + 1)$, откуда следует (6).

Аналогично для нечетного $n$, просто показать, что выражение (7) является суммой четных чисел $0 + 2 + 4 + \ldots + (n - 2(m+1) + 1)$.

Пример 2. Для $n = \overline{5,20}$, $l = \overline{1,10}$ построить все кривые Гурвица.

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

Обычные кривые Гурвица $H_n$ определяются параметром $\Delta(n,l=1) = n^2 - n + 1$ в первом столбце таблицы. Обобщенные кривые $H_{n,l}$ $l \ge 2$ задаются всеми остальными столбцами. Уравнение b) утверждения 1 определяет кривые $X^n Y^l + Y^n Z^l + X^l Z^n = 0$ 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 кривые $X^nY^l + Y^nZ^l + X^lZ^n = 0$ и

$X^nY^{n-l}+Y^nZ^{n-l}+X^{n-l}Z^n=0$ являются эквивалентными (см. замечание 1), все вычисления можно ограничить условием $l=\overline{1,m/2}$.

*Таблица 2*

**Значения параметра $\Delta=n^2-nl+l^2$ для кривых Гурвица $H_{n,l}$**

| n | $\Delta=n^2-nl+l^2$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | l=1 | l=2 | l=3 | l=4 | l=5 | l=6 | l=7 | l=8 | l=9 | l=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 | | | | | |

Утверждение 1, 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

$$\begin{gathered}\Delta-\Delta'=(n/2-m)^2,\\ r=\sqrt{\Delta-\Delta'},\\ l=m=n/2-r.\end{gathered}\qquad(8)$$

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

Для нечетного $n$ имеем следующие выражения

$$\Delta-\Delta'=(\lceil n/2\rceil-m)((n-1)/2-m),$$

$r=\lfloor\sqrt{\Delta-\Delta'}\rfloor$, $\lfloor\bullet\rfloor$ -округление к наименьшему целому,

$$l=m=(n-1)/2-r.\qquad(9)$$

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 $\sqrt{\Delta} \le n \le 2\sqrt{\Delta}/\sqrt{3}$, $l \le n/2$.

Замечание 5.

1. Переборный метод построения кривых Гурвица по делителям порядка поля реализует последовательный подъём 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.

3. Для широкого класса кривых с) из утверждения 1 с показателем $\Delta(n,l) = c^2 \cdot p_i \cdot \ldots \cdot p_j$, следует предварительно понизить значение показателя $\Delta(n',l') = \Delta(n,l)/c^2$. Понижение показателя $\Delta(n,l)$ уменьшает диапазон изменения значения показателя степени $\sqrt{\Delta} \le n' \le 2\sqrt{\Delta}/\sqrt{3}$ и уменьшает число итераций вычислений. Вычисления дополняются предварительным шагом понижения показателя $\Delta$ и последним шагом подъема показателей степеней $n = c \cdot n'$, $l = c \cdot l'$.

Пример 3. Пусть $\Delta(n,l) = 316 = 4 \cdot 79$. Требуется построить кривую Гурвица $H_{n,l}$ минимального рода.

Выполним понижение значения показателя $\Delta(n',l') = \Delta(n,l)/4 = 79$.

Вычислим границы для показателя $n'$ по лемме 2, получим $9 \le n' \le 10$.

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

$$\Delta'(9, l' = 5) = 61,$$
$$\Delta - \Delta' = 18,$$
$$r = \left\lfloor \sqrt{\Delta - \Delta'} \right\rfloor = 4.$$

Так как $r(r+1) \neq \Delta - \Delta'$, тогда $n'$, $l'$ не являются искомыми, и следует увеличить $n'$.

Повторяем вычисления для четного $n'$ по формулам (8):

$$\Delta'(10, l' = 5) = 75$$
$$\Delta - \Delta' = 4,$$
$$r = \sqrt{\Delta - \Delta'} = 2.$$

Так $r = \sqrt{\Delta - \Delta'}$ - целочисленное, имеем $n' = 10$, $l' = n'/2 - r = 3$. Выполняем подъем показателей степеней $n = n' \cdot 2 = 20$, $l = l' \cdot 2 = 6$, получим искомую кривую Гурвица $X^{20}Y^6 + Y^{20}Z^6 + X^6Z^{20}$ с $\Delta(20,6) = 316$, что совпадает с результатами табл. 2.

Замечание 6.

1. Вычисления по предложенному методу позволяют найти все кривые с заданным значением $\Delta(n,l)$. Число кривых определяется числом делителей $\Delta(n,l)$ $\Delta = p_i \cdot \ldots \cdot p_j$, которые по модулю 6 тождественны единице и, если существует, сомножителем равным 3, и числом образующих элементов мультипликативных подгрупп 6-го и 2-го порядков по модулям этих делителей. В рассмотренном случае такой делитель один $p_1 = 79$ и только одна кривая имеет $\Delta(20,6) = 316$, $n > l$. Для случая $\Delta(n,l) = 301 = 7 \cdot 43$ таких кривых две: $X^{19}Y^4 + Y^{19}Z^4 + X^4Z^{19}$, $X^{20}Y^9 + Y^{20}Z^9 + X^9Z^{20}$. По замечанию 1 получим еще две кривые Гурвица.

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 счёте, алгоритм хеширования по выражению $h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i$ и вероятность коллизии универсального хеширования.

Выводы. Предложен переборный метод построения кривых Гурвица заданного рода по делителям порядка конечного поля на основе последовательного подъёма показателей кривых от наименьшего значения старшего показателя к искомому, что позволяет сократить время вычисления степенных показателей кривой и получить кривую с наилучшим отношением числа точек к роду кривой.

**Список литературы**

1. Халимов Г.З. Максимальные кривые Гурвица для целей универсального хеширования. Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 3.- Таганрог: Изд-во ТТИ ЮФУ, 2010. с.144-146.

2. Халимов Г.З. Универсальное хеширование по максимальной кривой третьего рода $x^{(q+1)/d} + x^{2(q+1)/d} + y^{q+1} = 0$ / Г.З. Халимов // Научные ведомости Белгородского государственного университета. – 2011. – №1 (96), – Вып. 17/1. – С. 137–145.

3. Халимов Г.З. Универсальное хеширование по алгебраическим кривым в простом поле / Г.З.Халимов // Журнал «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.

4. Халимов Г.З. Оценка параметров кривых Гурвица для целей универсального хеширования / Халимов Г.З.// Сб. трудов Первой международной научно-технической конференции "Компьютерные науки и технологии". Белгород, Россия. 8-10 октября 2009. -Ч.2, - С.118-121.

5. Халимов Г.З. Универсальное хеширование по максимальным кривым Гурвица / Г.З. Халимов // Журнал "Прикладная радиоэлектроника". Харьков: ХНУРЭ. – 2010. – Т.9, № 3. – С.365-370.

6. Халимов Г.З. Условия построения нетривиальных кривых Гурвица / Халимов Г.З.// Журнал «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.

7. Халимов Г.З. Условия существования нетривиальных кривых Гурвица / Халимов Г.З. // Системи обробки інформації МО України, Харківський університет Повітряних Сил ім. Івана Кожедуба. – 2010. –вип. 6(87) -С. 229-233.

8. Халимов Г.З. Кривые Гурвица с большим числом точек в расширенных конечных полях / Г.З.Халимов // Журнал «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.

9. Torres F. Plan maximal curves / F.Torres // Acta Arithmetic. – 2001. – Vol. 98, No. 2. – P. 165-179. 10. Beelen P. The Newton polygon of plane curves with many rational points. / P.Beelen, R.Pellikan //Designs, Codes and Cryptography. -2000. –N.21. –P.41–67.

10. Халимов О.Г. Универсальное хеширование по обобщенным кривым Гурвица / О.Г.Халимов, А.Н.Герцог // Журнал «Радиотехника». – Харьков, ХНУРЭ. -2012. – вып 171. – С.140-146.

## UNIVERSAL HASHING ON MAXIMUM CURVE OF THE THIRD GENUS

**O.G. KHALIMOV[1]**
**A.D.BUKHANTSOV[2]**
**G.Z. KHALIMOV[1]**

*[1] Kharkiv National University of Radio Electronics*

*[2] Belgorod National Research University*

*e-mail:*
*gennadykhalimov@mail.ru*
*bukhantsov@bsu.edu.ru*

Presented a method for constructing Hurwitz curves of given genus over divisors of the order of a finite field, based on a consistent performance curves rise from the lowest value to the highest exponent desired, thereby reducing the computation time exponents of the curve and get the curve with the best ratio of the number of points to the genus of the curve.

Keywords: universal hashing, algebraic curves Hurwitz