УДК 681.3.06

О.Г. ХАЛИМОВ, А.Н. ГЕРЦОГ

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО ОБОБЩЕННЫМ КРИВЫМ 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 $h_{P_j}(m) = \sum_{i=1}^{k} f_i(P_j) m_i$ и имеет оценку для вероятности коллизии $\varepsilon = \rho_k / N$, где ρ_k – максимальное значение полюса рациональной функции f_k и N – число точек алгебраической кривой [1]. Универсальное хеширование $h_{P_j}(m)$ обеспечивает наилучшие соотношения между вероятностью коллизии, затратами на ключевые данные, сложность вычисления при фиксированной длине сообщения и поля вычисления. Основная проблематика реализации универсального хеширования по алгебраическим кривым состоит в построении проективного многообразия с большим отношением числа точек кривой к её роду. Универсальное хеширование по кривым Гурвица реализует вычисления на большом числе точек. Для случая простого поля по сравнению с кривыми Ферма достигается абсолютно наилучший результат [2]. Основные результаты по кривым Гурвица представлены в работах [3 – 5]. В работе [3] представлено решение задачи построения максимальных кривых Гурвица. Условия существования и построения нетривиальных кривых Гурвица получены в [4, 5]. В работе [5] впервые определены все семейства нетривиальных кривых Гурвица. Оценки параметров наилучших кривых Гурвица в простом, кубическом поле представлены в [2, 6]. Здесь же рассмотрены частные случаи кривых Гурвица с большим числом точек. Важной научной задачей является разработка метода построения хороших кривых Гурвица без ограничений на показатели степени кривой над произвольным конечным полем с уменьшенной сложностью вычислений.

В данной работе предлагается метод построения кривых Гурвица с наибольшим отношением числа точек к роду на основе приведения к обобщенным кривым минимального рода с перебором значения наибольшего показателя кривой. С этой целью в разд. 1 приводятся определение и основные результаты по кривым Гурвица. В разд. 2 излагается общий метод построения нетривиальных кривых. В разд. 3 представлен метод построения кривых Гурвица на основе приведения к обобщенным кривым минимального рода по наибольшему показателю степени кривой и оценки сложности вычисления.

1. Основные результаты по кривым Гурвица в конечном поле.

Кривые Гурвица H_n определяются выражением

$$X^n Y + Y^n Z + X Z^n = 0, \tag{1}$$

и имеют частные производные $F_X = nX^{n-1}Y + Z^n$, $F_Y = nY^{n-1}Z + X^n$, $F_Z = nZ^{n-1}X + Y^n$.

Несингулярность кривых Гурвица над F_q определяется условиями [7]:

1) n и q должны быть взаимно простыми;

2) $\gcd(n^2 - n + 1, q) = 1$.

Для вычисления рода кривой Гурвица H_n используем выражение для рода кривой $X^a + X^b Y^c + Y^d = 0$ (замечание 4.3 в [8])

$$g \le 1 + \frac{1}{2}\left\{ac + bd - ad\right| - \gcd(a-b, c) - \gcd(b, c-d) - \gcd(a, d)\right\} \tag{2}$$

Если характеристика поля F_q не делит $\gcd(a-b,c), \gcd(b,c-d), \gcd(a,d)$ и $ac+bd-ad$, тогда справедливо равенство. В силу соотношения (2) для кривой Гурвица H_n выражение для рода имеет вид

$$g=(n^2-n)/2. \tag{3}$$

Существует обобщение кривых Гурвица H_{nl} вида [9]

$$X^nY^l+Y^nZ^l+X^lZ^n=0, \tag{4}$$

где $n \ge l \ge 2$, $\Delta(n,l)=n^2-nl+l^2 \ge 2$ и частные производные $F_X=nX^{n-1}Y^l+lX^{l-1}Z^n$, $F_Y=nY^{n-1}Z^l+lX^nY^{l-1}, F_Z=nZ^{n-1}X^l+lY^nZ^{l-1}$.

Несингулярность кривых Гурвица H_{nl} над F_q определяется условием [9]:

$$\gcd(\Delta(n,l), char(F_q))=1. \tag{5}$$

Род кривой H_{nl}, как следует из (2) и отмечается в [10],

$$g=(n^2-nl+l^2+2-3\gcd(n,l))/2=(\Delta(n,l)+2-3\gcd(n,l))/2. \tag{6}$$

Кривые с числом точек $N \ne q+2$ называются нетривиальными.

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

Теорема 2. [4] Пусть задано конечное поле F_q и $n,l>0$, $\gcd(n,l)=1$. Нетривиальная кривая Гурвица H_{nl} $X^nY^l+Y^nZ^l+X^lZ^n=0$ 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 также делитель равный 3, где $e \ge 1$.

2. Построение нетривиальных кривых Гурвица

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

Теорема 3 [4]. 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. Степень n нетривиальной кривой Гурвица $X^nY+Y^nZ+XZ^n=0$ определяется выражением

$$n=n_1P_1+n_2P_2+...+n_kP_k \bmod p_1 \cdot p_2 \cdot ... \cdot p_k, \tag{7}$$

$$P_i=b_i\prod_{\substack{s=1\\ s\ne i}}^{k} p_s \equiv 1 (\bmod p_i), \tag{8}$$

где $n_1, n_2, ..., n_k$ – образующие элементы мультипликативных подгрупп 6-го и 2-го порядков по модулям $p_1, p_2, ..., p_k$, 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 обра-

зующими 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 (8) 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 (7) по модулю $P_1 \cdot P_2 \cdot P_3 = 13 \cdot 43 \cdot 7 = 3913$ приводят 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 1.

1. Применение теоремы 3 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 $p_1, p_2, ..., p_k$. При этом кривые H_n при различных показателях степени имеют одинаковое число точек (см. утверждение 1 [5]) и разные значения рода (см. выражение (6)).

2. 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 $p_1 = 13$, $p_2 = 43$, $p_3 = 7$. Разложения $\Delta(n,1)$ по делителям имеет вид:

- $\Delta(3748,1) = 3748^2 - 3748 + 1 = 14043757 = 7 \cdot 13 \cdot 37 \cdot 43 \cdot 97$;
- $\Delta(2630,1) = 2630^2 - 2630 + 1 = 6914271 = 3 \cdot 7 \cdot 13 \cdot 19 \cdot 31 \cdot 43$;
- $\Delta(738,1) = 738^2 - 738 + 1 = 543907 = 7 \cdot 13 \cdot 43 \cdot 139$;
- $\Delta(381,1) = 381^2 - 381 + 1 = 144781 = 7 \cdot 13 \cdot 37 \cdot 43$;
- $\Delta(1284,1) = 1284^2 - 1284 + 1 = 1647373 = 7 \cdot 13 \cdot 37 \cdot 43 \cdot 421$;
- $\Delta(3533,1) = 3533^2 - 3533 + 1 = 12478557 = 3 \cdot 7 \cdot 13 \cdot 43 \cdot 1063$;
- $\Delta(3176,1) = 3176^2 - 3176 + 1 = 10083801 = 3 \cdot 7 \cdot 13 \cdot 43 \cdot 859$;
- $\Delta(166,1) = 166^2 - 166 + 1 = 27391 = 7^2 \cdot 13 \cdot 43$.

3. Приведение к кривым наименьшего рода реализуется через обобщенные кривые Гурвица $H_{n,l}$. Существование обобщенных кривых с наименьшим значением параметра $\Delta(n,l) = p_1 \cdot p_2 \cdot p_3$ определяется теоремой 4 [5].

Теорема 4. 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 $H_{n,l}$ $X^nY^l + Y^nZ^l + X^lZ^n = 0$, такая что $\gcd\left(n^2 - nl + l^2, (q-1)\right) = p_1 p_2 ... p_k$.

Применение теоремы дает следующие нетривиальные кривые:

- $X^{71}Y^{47} + Y^{71}Z^{47} + X^{47}Z^{71} = 0$, для $n_1 = 4$, $n_2 = 7$, $n_3 = 3$;
- $X^{64}Y^{3} + Y^{64}Z^{3} + X^{3}Z^{64} = 0$, для $n_1 = 4$, $n_2 = 7$, $n_3 = 5$;
- $X^{69}Y^{16} + Y^{69}Z^{16} + X^{16}Z^{69} = 0$, для $n_1 = 10$, $n_2 = 7$, $n_3 = 3$;
- $X^{72}Y^{31} + Y^{72}Z^{31} + X^{31}Z^{72} = 0$, для $n_1 = 4$, $n_2 = 37$, $n_3 = 3$;
- $X^{64}Y^{61} + Y^{64}Z^{61} + X^{61}Z^{64} = 0$, для $n_1 = 10$, $n_2 = 37$, $n_3 = 3$;
- $X^{72}Y^{41} + Y^{72}Z^{41} + X^{41}Z^{72} = 0$, для $n_1 = 10$, $n_2 = 7$, $n_3 = 5$;
- $X^{69}Y^{53} + Y^{69}Z^{53} + X^{53}Z^{69} = 0$, для $n_1 = 4$, $n_2 = 37$, $n_3 = 5$;
- $X^{71}Y^{24} + Y^{71}Z^{24} + X^{47}Z^{24} = 0$, для $n_1 = 10$, $n_2 = 37$, $n_3 = 5$.

Замечание 2.

1. Все кривые, рассмотренные в примере, имеют наименьшее значение рода, так как имеют одинаковое значение показателя $\Delta(n,l) = 3913$.

2. 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 $\Delta(n',l) = p_1 \cdot p_2 \cdot p_3$.

Выводы

1. Теорема 3 не дает прямого ответа на вопрос как построить кривые Гурвица H_n по одному делителю порядка поля. Например, для делителя $p_i = 19$ непосредственные вычисления показывают, что не существует обычной кривой Гурвица H_n, так как не существуют решения в целых числах для уравнения $\Delta(n,1) = 19$, но существуют решения для $\Delta(n,l) = 19$. Таким решением является $n = 5$, $l = 2$.

2. Вычислительные затраты на приведение кривых Гурвица H_n к обобщенным кривым $H_{n,l}$ определяются размером делителей порядка конечного поля и являются пропорциональными произведению этих делителей. Для практически важных конструкций кривых над большими полями $\approx 2^{64} \div 2^{128}$ вычисления становятся значительными. Ниже рассматривается метод построения кривых Гурвица на основе приведения к обобщенным кривым минимального рода.

3. Метод построения обобщенных кривых Гурвица

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 $H_{n,l}$ принадлежат одному из семейств:

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

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

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

г) $X^cY^c + Y^cZ^c + X^cZ^c = 0$, 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 эквивалентности кривых Гурвица определяются следующими утверждениями.

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

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

Утверждение 2 является очевидным.

Замечание 3.

1. Уравнения а) и б) утверждения 1 определяют кривые Гурвица H_n и $H_{n,l}$. Уравнения в) и г) являются производными от кривых а) и б) и определяются по делителям порядка конечного поля.

2. Утверждения 2 и 3 определяют: можно построить кривую $X^lY^n + Y^lZ^n + X^nZ^l = 0$ и затем построить классические кривые Гурвица $X^nY^l + Y^nZ^l + X^lZ^n = 0$ и $X^nY^{n-l} + Y^nZ^{n-l} + X^{n-l}Z^n = 0$.

Следующие леммы 1 и 2 определяют для заданного значения $\Delta(n,l)$ пределы изменения значения показателя n.

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

$$n^2 - n^2/4 \le \Delta(n,l) \le n^2 - n + 1. \tag{9}$$

Действительно минимальное значение $\Delta(n,l)$ определяется в точке $l = n/2$, так как $\left.\frac{\partial\Delta(n,l)}{\partial l}\right|_{l=n/2} = 0$ и справедливо $\Delta(n, l < n) < \Delta(n, l = 1)$.

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

$$\sqrt{\Delta(n,l)} < n < 2\sqrt{\Delta(n,l)}/\sqrt{3} \tag{10}$$

Левая часть соотношения (10) следует из выражения для $\Delta(n,l) \le n^2 - nl + l^2$ и леммы 1. Правая часть определяется выражением для минимального значения $\Delta(n, l = n/2) = 3n^2/4$. ◊

Утверждения 1 – 3 и леммы 1, 2 определяют усовершенствованный метод построения обобщенных кривых Гурвица 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 $q-1 = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, $e_i \ge 1$ и набор делителей $p_i,...,p_j$ которые по модулю 6 тождественны единице и, если существует, сомножитель равный 3.

2. Фиксируем делители из набора $p_i,...,p_j$, для которых вычисляем искомое значение параметра $\Delta' = p_i \cdot ... \cdot p_j$ и формируем набор образующих элементов мультипликативных подгрупп 6-го и 2-го порядков.

3. В соответствии с выражениями (7) и (8) вычисляем набор кривых $X^nY + Y^nZ + XZ^n$ число которых определяется комбинацией значений образующих элементов мультиплика тивных подгрупп 6-го и 2-го порядков.

4. Для каждой кривой H_n из полученного набора вычисляем $\Delta(n,1)$ и сравниваем с Δ'. Если $\Delta(n,1)=\Delta'$, тогда кривая является без избыточной по роду. Для избыточных кривых $\Delta(n,1)>\Delta'$, переходим к п.5 и 6 – построению обобщенных кривых Гурвица.

5. В соответствии с утверждением 3 уравнения $X^nY+Y^nZ+XZ^n$ из набора кривых п.3 преобразуются в уравнения $XY^l+YZ^l+X^lZ=0$, где $l=n$.

6. Перебираем последовательно значение параметра n от $\left\lceil\sqrt{\Delta'}\right\rceil$, где $\lceil\bullet\rceil$ округление до наибольшего целого и вычисляем показатель степени $m=l\cdot n \bmod \Delta'$ для обобщенной кривой $H_{n,m}$ и если $\Delta(n,m)=\Delta'$ – искомая кривая построена. Для построения всех обобщенных кривых следует выполнить вычисления для всех обычных кривых, построенных в п.3 и применить утверждение 2.

Замечание 4. Если кривая Гурвица строится по одному делителю порядка поля p_1, для вычислений следует задать еще один делитель p_2, который по модулю 6 тождественный единице или равный 3. Это не противоречит требованию теорем 3 и 4, так как параметр $\Delta(n,l)$ наряду с искомым делителем может содержать и другие делители не обязательно из делителей порядка поля.

Пример 2. Пусть $p_1=19$. Требуется построить кривую Гурвица $H_{n,l}$ минимального рода.

Зададим дополнительный делитель $p_2=3$. Значение $\Delta'=p_1$.

Образующие элементы для подгрупп по модулям p_i, $i=1,2$ принимают значения:

- $n_1=8$ и 12 для подгруппы по модулю $p_1=19$;
- $n_2=2$ для подгруппы по модулю $p_2=3$;

Вычисления по формуле (8) дадут следующие значения параметров P_1, P_2:

- $P_1=b_1p_2=b_13=13\cdot 3=39\equiv 1 \bmod 19$;
- $P_2=b_2p_1=b_219=1\cdot 19=19\equiv 1 \bmod 3$.

Для образующих $n_1=8$, $n_2=2$ по формуле (7) получим $n=n_1P_1+n_2P_2(\bmod p_1p_2)=8\cdot 39+2\cdot 19=8 \bmod 57$ и кривую Гурвица

$$X^8Y+Y^8Z+XZ^8=0. \tag{11}$$

Вычисления для образующих $n_1=12$ и $n_2=2$ приводят к $n=n_1P_1+n_2P_2(\bmod p_1p_2)=12\cdot 39+2\cdot 19=50 \bmod 57$ и

$$X^{50}Y+Y^{50}Z+XZ^{50}=0. \tag{12}$$

Кривые (11), (12) являются избыточными по роду. Для приведения к кривым минимального рода используем метод построения обобщенных кривых. По пункту 5 получим кривые:

- $XY^8+YZ^8+X^8Z=0$;
- $XY^{50}+YZ^{50}+X^{50}Z=0$.

Вычисление обобщенных кривых начинается с нижней границы для $n=\left\lceil\sqrt{\Delta'}\right\rceil=5$. Для $XY^8+YZ^8+X^8Z=0$ получим $m=l\cdot n \bmod \Delta'=8\cdot 5 \bmod 19=2$ и кривую минимального рода $X^5Y^2+Y^5Z^2+X^2Z^5=0$. Аналогично для кривой $XY^{50}+YZ^{50}+X^{50}Z=0$ получим $m=l\cdot n \bmod \Delta'=50\cdot 5 \bmod 19=3$ и обобщенную кривую минимального рода $X^5Y^3+Y^5Z^3+X^3Z^5=0$. Заметим, что обычной кривой Гурвица с $\Delta(n,1)=19$ не существует.

Предложение 1. Метод построения кривой Гурвица $H_{n,l}$ с перебором наибольшего показателя n в 7.46 раза быстрее по сравнению с перебором по наименьшему показателю l.

Действительно, по лемме 2 показатель n искомой кривой $H_{n,l}$ минимального рода лежит в интервале $\sqrt{\Delta(n,l)} < n < 2\sqrt{\Delta(n,l)}/\sqrt{3}$ и максимальное число итераций для п. 6 при вычислении кривой $H_{n,l}$: $T_n = (2-\sqrt{3})\sqrt{\Delta(n,l)}/\sqrt{3}$. В известном методе по теореме 4 [8] вычисления выполнялись по показателю l со значения $l = 2$. Лемма 2, в силу утверждения 3, определяет верхнее значение для показателя степени $l < 2\sqrt{\Delta(n,l)}/\sqrt{3}$. Максимальное число итераций при вычислении кривой $H_{n,l}$ по показателю l равно $T_l = 2\sqrt{\Delta(n,l)}/\sqrt{3}$. Число вычислений при итерациях по l в среднем будет больше числа итераций по n в $T_n / T_l = 2/(2-\sqrt{3}) \approx 7.46$ раз.

Замечание 5. Для кривых $H_{n,l}$ из примера 1 вычисления по предложенному методу в шесть раз быстрее, так как показатель n пробегает значения от $n = \left|\sqrt{\Delta'}\right| = \left|\sqrt{3913}\right| = 63$ до $n = 72$ и заканчивается за 10 шагов, а для итераций по показателю l требуется 60 шагов.

Выводы

1. Предложен метод построения кривых Гурвица на основе приведения к обобщенным кривым минимального рода с последовательным перебором наибольшего показателя кривой Гурвица, который является дальнейшим развитием метода построения кривых Гурвица по делителям порядка поля и отличается от известного введением дополнительного делителя в случае построения кривой по одному делителю порядка поля.

2. Построение кривой Гурвица $H_{n,l}$ по методу приведения к обобщенным кривым минимального рода с перебором наибольшего показателя в среднем в 7.46 раза быстрее по сравнению с перебором по наименьшему показателю степени кривой и расширяет множество кривых, так как определяет построение кривых по одному делителю порядка поля.

Список литературы: 1. *Халимов, Г.З.* Максимальные кривые Гурвица для целей универсального хеширования // Материалы XI Междунар. науч.-практ. конференции «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. – 2010. – Т.9, № 3. – С.365-370. 4. *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. 5. *Халимов, Г.З.* Условия построения нетривиальных кривых Гурвица / Халимов Г.З. // 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.* Кривые Гурвица с большим числом точек в расширенных конечных полях / Г.З.Халимов // Системи управління, навігації та зв'язку. – 2011. – Вип. 2(18). – С.185-189. 7. *Hoholdt, N.* Algebraic geometry codes / N.Hoholdt, J.H. van Lint and R.Pellican // In the Handbook of Coding Theory, (V.S. Pless, W.C. Huffman and R.A. Brualdi Eds.), Elsevier, Amsterdam. – 1998. –V. 1. –P.871-961. 8. *Pellikan, R.* The Klein quartic, the Fano plan and curves representing design / R.Pellikan // In Codes, Curves and Signals: Common Threads in Communications, (A. Vardy Ed.), Kluwer Academy Published, Dordrecht. – 1998. – P.9-20. 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.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 20.09.2012