МЕХАНИЗМЫ И МЕТОДЫ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

УДК 621.391:519.7

А. Н. АЛЕКСЕЙЧУК, д-р техн. наук, А. А. МАТИЙКО

ОЦЕНКИ ВЕРОЯТНОСТИ ОБРАТИМОСТИ СЛУЧАЙНЫХ МНОГОЧЛЕНОВ, ИСПОЛЬЗУЕМЫХ В МОДИФИЦИРОВАННОЙ ВЕРСИИ КРИПТОСИСТЕМЫ NTRU

Введение

Асимметричная система шифрования NTRU предложена в 1996 г. [1] и является первым представителем широкого класса криптосистем с одноименным названием, стойкость которых основана на сложности нахождения коротких векторов в некоторых решетках (см., например, работы [2, 3] и приведенные там ссылки).

Для задания криптосистем из этого класса используют кольцо усеченных многочленов $R_{n,q} = \mathbf{Z}_q[x]/(x^n - 1)$, где n и q – взаимно простые натуральные числа, а также натуральное число p, взаимно простое с q (обычно в качестве n выбирают простое число от 100 до 2000, а q и p полагают равными 2048 и 3 соответственно [4]). Секретным ключом криптосистемы служит пара многочленов $F(x), g(x) \in R_{n,q}$ таких, что многочлен $f(x) = 1 + pF(x)$ обратим в кольце $R_{n,q}$, а открытым ключом – многочлен $h = pg(x)(f(x))^{-1} \in R_{n,q}$.

В доступных публикациях описаны различные способы формирования многочленов $F(x)$ и $g(x)$, исходя из условий практичности и стойкости криптосистем к известным атакам. Например, в [4, 5] предлагается выбирать эти многочлены случайно равновероятно из некоторых множеств многочленов с коэффициентами 0, ± 1 и малым числом ненулевых коэффициентов. В обоснованно стойком варианте NTRU [6] $F(x)$ и $g(x)$ выбираются независимо друг от друга в соответствии с дискретным гауссовым распределением, а в [7] – случайно из некоторых множеств так называемых многочленов-произведений. Отметим, что способ формирования многочленов $F(x)$ и $g(x)$ существенно влияет на стойкость и практичность соответствующей версии криптосистемы NTRU. При этом указанный способ должен гарантировать высокую вероятность обратимости многочлена $f(x) = 1 + pF(x)$.

Цель статьи – построение оценок вероятности обратимости многочлена $f(x)$ в предположении, что коэффициенты многочлена $F(x)$ являются независимыми случайными величинами, принимающими значения ± 1 и 0 с вероятностями θ и $1 - 2\theta$ соответственно, где $\theta \in (0, 1/2)$. Эта схема формирования многочленов служит приближением к традиционной схеме [4, 5], однако является более удобной при исследовании стойкости криптосистемы к некоторым атакам. В частности, эта схема используется в [5] для (эвристической) оценки стойкости NTRU относительно так называемых атак на основе ошибок расшифрования.

Дальнейшее изложение в статье построено следующим образом. В п. 1 для простого числа n и взаимно простого с ним числа q описано строение кольца $R_{n,q}$ и приведена формула для порядка группы обратимых элементов этого кольца. В п. 2 для различных простых n и q получены точные выражения вероятностей некоторых вспомогательных событий, связанных с обратимостью случайного многочлена $f(x)$, а в п. 3 – при некоторых дополнительных ограничениях на n и q – выражения и оценки вероятности обратимости этого многочлена. Представлены также результаты численных расчетов, позволяющие

судить о значениях указанной вероятности. В заключительной части статьи сформулированы краткие выводы.

1. Строение кольца усеченных многочленов

Пусть n и q – взаимно простые натуральные числа, $n,q>1$. Обозначим $\mathbf{Z}_q$ – кольцо классов вычетов по модулю q и рассмотрим кольцо $R_{n,q}=\mathbf{Z}_q[x]/(x^n-1)$.

Напомним (см., например, [8]), что кольцом Галуа порядка p^{lm} и характеристики p^l, где p – простое, l,m – натуральные числа, называется кольцо $\mathbf{Z}_{p^l}[x]/(F(x))$, где $F(x)\in\mathbf{Z}_{p^l}[x]$ – унитарный многочлен степени m, образ которого над полем $\mathbf{Z}_p$ (получаемый в результате приведения всех коэффициентов многочлена $F(x)$ по модулю p) неприводим над этим полем. Кольцо Галуа однозначно с точностью до изоморфизма определяется своими порядком и характеристикой и обозначается $\mathbf{GR}(p^{lm},p^l)$. Порядок группы обратимых элементов этого кольца $|\mathbf{GR}(p^{lm},p^l)^*|=p^{(l-1)m}(p^m-1)$.

Утверждение 1. Пусть n – нечетное простое число, $q=q_1^{\,l_1}\cdots q_s^{\,l_s}$ – каноническое разложение числа q, m_i – показатель, которому принадлежит q_i по модулю n (то есть наименьшее натуральное число, для которого $q_i^{\,m_i}\equiv 1 \bmod n$). Тогда

$$R_{n,q}\cong\bigoplus_{i=1}^{s}R_{n,q_i^{\,l_i}}\,, \tag{1}$$

и

$$R_{n,q_i^{\,l_i}}\cong\mathbf{Z}_{q_i^{\,l_i}}\oplus\underbrace{\mathbf{GR}(q_i^{\,l_i m_i},q_i^{\,l_i})\oplus\cdots\oplus\mathbf{GR}(q_i^{\,l_i m_i},q_i^{\,l_i})}_{(n-1)/m_i},\ i\in\overline{1,s}\,. \tag{2}$$

При этом вероятность события, состоящего в том, что случайный равновероятный элемент кольца обратим,

$$p_{n,q}=\prod_{i=1}^{s}\left(1-\frac{1}{q_i}\right)\left(1-\frac{1}{q_i^{\,m_i}}\right)^{\frac{n-1}{m_i}}. \tag{3}$$

Доказательство. Согласно китайской теореме об остатках [9, с. 83], $\mathbf{Z}_n\cong\bigoplus_{i=1}^{s}\mathbf{Z}_{q_i^{\,l_i}}$, откуда следует, что

$$R_{n,q}=\mathbf{Z}_q[x]/(x^n-1)\cong\bigoplus_{i=1}^{s}\mathbf{Z}_{q_i^{\,l_i}}[x]/(x^n-1)=\bigoplus_{i=1}^{s}R_{n,q_i^{\,l_i}}\,.$$

Далее, каноническое разложение многочлена x^n-1 над полем $\mathbf{Z}_{q_i}$ имеет вид $x^n-1=(x-1)f_{1,i}(x)\cdots f_{t_i,i}(x)$, где $f_{1,i}(x),\ldots,f_{t_i,i}(x)$ – различные неприводимые многочлены степени m_i, $t_i=(n-1)/m_i$ [10, теор. 2.47]. Отсюда на основании леммы Гензеля [8, с. 152], следует, что существуют попарно взаимно простые унитарные многочлены $F_{1,i}(x),\ldots,F_{t_i,i}(x)\in\mathbf{Z}_{q_i^{\,l_i}}[x]$ такие, что в кольце $\mathbf{Z}_{q_i^{\,l_i}}[x]$ выполняется равенство $x^n-1=(x-1)F_{1,i}(x)\cdots F_{t_i,i}(x)$ и для любого $j\in\overline{1,t_i}$ образ многочлена $F_{j,i}(x)$ над полем $\mathbf{Z}_{q_i}$ равен $f_{j,i}(x)$. Следовательно, на основании китайской теоремы об остатках и определения

колец Галуа,

$$R_{n,q_i^{l_i}} \cong \mathbf{Z}_{q_i^{l_i}}[x]/(x-1) \oplus \mathbf{Z}_{q_i^{l_i}}[x]/(F_{1,i}(x)) \oplus \cdots \oplus \mathbf{Z}_{q_i^{l_i}}[x]/(F_{t_i,i}(x)) \cong$$
$$\cong \mathbf{Z}_{q_i^{l_i}} \oplus \underbrace{\mathbf{GR}(q_i^{l_i m_i}, q_i^{l_i}) \oplus \cdots \oplus \mathbf{GR}(q_i^{l_i m_i}, q_i^{l_i})}_{(n-1)/m_i}.$$

Итак, справедливы соотношения (1) и (2).

Для доказательства равенства (3) достаточно заметить, что в силу (1), (2)

$$|R_{n,q}{}^*| = \prod_{i=1}^{s} |\mathbf{Z}_{q_i^{l_i}}{}^*| \cdot |\mathbf{GR}(q_i^{l_i m_i}, q_i^{l_i})^*|^{\frac{n-1}{m_i}} =$$

$$= \prod_{i=1}^{s} q_i^{l_i-1}(q_i-1)\,(q_i^{(l_i-1)m_i}(q_i^{m_i}-1))^{\frac{n-1}{m_i}},\ |R_{n,q}| = \prod_{i=1}^{s} q_i^{l_i}\,(q_i^{l_i m_i})^{\frac{n-1}{m_i}}$$

и $p_{n,q} = |R_{n,q}{}^*| \cdot |R_{n,q}|^{-1}$.

Утверждение доказано.

Следствие 1. Пусть выполняется условие утверждения 1. Тогда:

а) если q – простое число, показатель которого по модулю n равен $n-1$, то

$$R_{n,q} \cong \mathbf{GF}(q) \oplus \mathbf{GF}(q^{n-1}),\ p_{n,q} = \left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^{n-1}}\right);$$

б) если $q = 2^l$ и 2 является примитивным элементом поля $\mathbf{Z}_n$, то

$$R_{n,q} \cong \mathbf{Z}_{2^l} \oplus \mathbf{Z}_{2^l}[x]/(\Phi_n(x)),$$

где многочлен $\Phi_n(x) = x^{n-1} + x^{n-2} + \cdots + 1$ неприводим над полем $\mathbf{Z}_2$, и

$$p_{n,q} = \frac{1}{2}\left(1-\frac{1}{2^{n-1}}\right).$$

2. Формулы для вероятностей вспомогательных событий

Пусть теперь n и q – различные простые числа, p – натуральное число, взаимно простое с q, $p < q-1$, $\xi_0, \xi_1, \ldots, \xi_{n-1}$ – независимые случайные величины, распределенные по закону

$$\mathbf{P}\{\xi_i = 1\} = \mathbf{P}\{\xi_i = -1\} = \theta,\ \mathbf{P}\{\xi_i = 0\} = 1-2\theta,\ i \in \overline{0,n-1}, \tag{4}$$

где $\theta \in (0, 1/2)$. Требуется оценить вероятность $\pi_{n,q}$ события, состоящего в том, что элемент кольца $R_{n.q}$, соответствующий многочлену $f(x) = 1 + pF(x)$, где $F(x) = \xi_0 + \xi_1 x + \ldots + \xi_{n-1}x^{n-1}$, необратим в этом кольце.

Отметим, что если q является степенью простого числа $\bar{q}$, то на основании изложенного $f(x) \in R_{n,q}{}^*$ тогда и только тогда, когда $f(x) \in R_{n,\bar{q}}{}^*$. Поэтому результаты, изложенные ниже для простого q, справедливы также в случае, когда q является степенью простого
числа.

Для нахождения оценок вероятности $\pi_{n,q}$ рассмотрим каноническое разложение

многочлена x^n-1 над полем $\mathbf{Z}_q$. Пусть m – показатель, которому принадлежит q по модулю n. Тогда $x^n-1=(x-1)f_1(x)\cdots f_t(x)$, где $f_1(x),\dots,f_t(x)$ – различные неприводимые многочлены степени m над полем $\mathbf{Z}_q$, $t=(n-1)/m$ [10, теор. 2.47]. Обозначим α_j произвольный
корень многочлена $f_j(x)$ в поле $\mathbf{GF}(q^m)$, $j\in\overline{1,t}$. Положим $\alpha_0=1$,

$$\pi_{n,q}(\alpha_j)=\mathbf{P}\{f(\alpha_j)=0\},\ j\in\overline{0,t}. \tag{5}$$

Ясно, что $f(x)\notin R_{n,q}{}^*$ тогда и только тогда, когда существует $j\in\overline{0,t}$ такое, что $f(\alpha_j)=0$. Отсюда вытекают следующие неравенства:

$$\max_{0\le j\le t}\pi_{n,q}(\alpha_j)\le\ \pi_{n,q}\le\pi_{n,q}(\alpha_0)+t\max_{1\le j\le t}\pi_{n,q}(\alpha_j). \tag{6}$$

Следующее утверждение устанавливает явные выражения параметров (5).

Утверждение 2. Для любого $j\in\overline{0,t}$ справедливо равенство

$$\pi_{n,q}(\alpha_j)=q^{-m}\sum_{x\in\mathbf{GF}(q^m)}\cos\left(\frac{2\pi\,\mathrm{Tr}(x)}{q}\right)\prod_{k=0}^{n-1}\left(1-2\theta\left(1-\cos\left(\frac{2\pi p\,\mathrm{Tr}(\alpha_j{}^k x)}{q}\right)\right)\right), \tag{7}$$

где $\mathrm{Tr}(z)=z+z^q+\cdots+z^{q^{m-1}}$ – абсолютный след элемента $z\in\mathbf{GF}(q^m)$.

Доказательство. Согласно определению

$$\pi_{n,q}(\alpha_j)=\mathbf{P}\{f(\alpha_j)=0\}=\mathbf{P}\{p\xi_0+p\xi_1\alpha_j+\dots+p\xi_{n-1}\alpha_j{}^{n-1}=-1\},$$

где $\xi_0,\xi_1,\dots,\xi_{n-1}$ – независимые случайные величины, распределенные по закону (4).

Обозначим $\chi(z)=\exp\left\{\frac{2\pi i\,\mathrm{Tr}(z)}{q}\right\}$, $z\in\mathbf{GF}(q^m)$ нетривиальный аддитивный характер поля $\mathbf{GF}(q^m)$ (где $i^2=-1$; см., например, [11]). Преобразование Фурье распределения случайной величины $\eta_k=p\xi_k\alpha_j{}^k$ имеет вид

$$\psi_k(x)=\sum_{a\in\mathbf{GF}(q^m)}\mathbf{P}\{\eta_k=a\}\chi(ax)=1-2\theta+\theta(\chi(\alpha_j{}^k px)+\chi(-\alpha_j{}^k px))=$$

$$=1-2\theta+\theta(\chi(\alpha_j{}^k px)+\overline{\chi(\alpha_j{}^k px)})=1-2\theta(1-\mathrm{Re}(\chi(\alpha_j{}^k px)))=$$

$$=1-2\theta\left(1-\cos\left(\frac{2\pi p\,\mathrm{Tr}(\alpha_j{}^k x)}{q}\right)\right),\ x\in\mathbf{GF}(q^m),\ k\in\overline{0,n-1}.$$

Отсюда, используя теорему о свертке и формулу обращения для преобразования Фурье (см., например, [11]), получим, что

$$\pi_{n,q}(\alpha_j)=q^{-m}\sum_{x\in\mathbf{GF}(q^m)}\overline{\chi(-x)}\,\psi_0(x)\cdots\psi_{n-1}(x)=$$

$$=q^{-m}\sum_{x\in\mathbf{GF}(q^m)}\exp\left\{\frac{2\pi i\,\mathrm{Tr}(x)}{q}\right\}\prod_{k=0}^{n-1}\left(1-2\theta\left(1-\cos\left(\frac{2\pi p\,\mathrm{Tr}(\alpha_j{}^k x)}{q}\right)\right)\right).$$

Поскольку $\pi_{n,q}(\alpha_j)$ – вещественное число, то полученное равенство равносильно формуле (7). Утверждение доказано.

Утверждение 2 позволяет установить связь между числами (5) и весовыми спектрами некоторых линейных кодов над полем $\mathbf{Z}_q$.

Для любого $j \in \overline{0,t}$ рассмотрим линейный код C_j, состоящий из всех слов вида $c = (c_0, c_1, \dots, c_{n-1})$, где $c_k = \mathrm{Tr}(\alpha_j{}^k x)$, $k \in \overline{0,n-1}$, а x пробегает все элементы поля $\mathbf{GF}(q^m)$. Заметим, что слова кода C_j – это отрезки длины n линейных рекуррент с неприводимым над полем $\mathbf{Z}_q$ характеристическим многочленом степени m, корнем которого является элемент α_j. При этом n равно порядку указанного многочлена, то есть является минимальным периодом каждой из этих рекуррент.

Для любых $c \in C_j$, $a \in \mathbf{Z}_q$ обозначим $\nu_a(c)$ число координат слова c, равных a.

Непосредственно из утверждения 2 вытекает следующий результат.

Следствие 2. Для любого $j \in \overline{0,t}$ выполняется равенство

$$\pi_{n,q}(\alpha_j) = q^{-m}\left(1 + \sum_{c \in C_j \setminus \{0\}} \cos\left(\frac{2\pi c_0}{q}\right) \prod_{a \in \mathbf{Z}_q} \left(1 - 2\theta\left(1 - \cos\left(\frac{2\pi p a}{q}\right)\right)\right)^{\nu_a(c)}\right), \tag{8}$$

где суммирование ведется по всем ненулевым словам $c = (c_0, c_1, \dots, c_{n-1})$ кода C_j.

В частности, если $q = 2$, то

$$\pi_{n,2}(\alpha_j) = 2^{-m}\left(1 + \sum_{c \in C_j \setminus \{0\}} (-1)^{c_0} (1 - 4\theta)^{wt(c)}\right), \tag{9}$$

где $wt(c)$ – вес Хэмминга слова c.

Наконец, полагая в формуле (7) $j = 0$, получаем такой результат.

Следствие 3. Справедливо равенство

$$\pi_{n,q}(1) = q^{-1} \sum_{k=0}^{q-1} \cos\left(\frac{2\pi k}{q}\right)\left(1 - 2\theta\left(1 - \cos\left(\frac{2\pi p k}{q}\right)\right)\right)^n . \tag{10}$$

В частности, если $q = 2$, то

$$\pi_{n,2}(1) = 2^{-1}(1 - (1 - 4\theta)^n). \tag{11}$$

3. Оценки вероятности обратимости случайного многочлена f

Получим оценки вероятности $\pi_{n,q}$ при некоторых дополнительных ограничениях на параметры m и θ.

Утверждение 3. Пусть $q = 2$, $\theta < 1/4$ и

$$d \stackrel{\text{def}}{=} \frac{2^{m-1} n}{2^m - 1} - 2^{m/2-1}\left(1 - \frac{n}{2^m - 1}\right) > 0. \tag{12}$$

Тогда

$$2^{-1}(1 - (1 - 4\theta)^n) \le \pi_{n,2} \le 2^{-1}(1 - (1 - 4\theta)^n) + \frac{n-1}{2^m m}\left(1 + 2^{m-1}(1 - 4\theta)^d\right). \tag{13}$$

В частности, если $n = 2^m - 1$ – простое число, то

$$2^{-1}(1 - (1 - 4\theta)^n) \le \pi_{n,2} \le 2^{-1}(1 - (1 - 4\theta)^n) + \frac{1}{\log(n+1)}\left(1 + \frac{n+1}{2}(1 - 4\theta)^{\frac{n+1}{2}}\right). \tag{14}$$

Доказательство. Покажем, что в условиях утверждения для любого $j \in \overline{0,t}$ выполняется следующее неравенство:

$$\pi_{n,2}(\alpha_j) \le 2^{-m}(1+2^{m-1}(1-4\theta)^d). \quad (15)$$

Тогда соотношения (13), (14) следуют непосредственно из формул (6), (11) и (15).

Для доказательства неравенства (15) воспользуемся формулой (9). Поскольку $\theta < 1/4$, то

$$\pi_{n,2}(\alpha_j) = 2^{-m}\left(1 + \sum_{c\in C_j\setminus\{0\}}(-1)^{c_0}(1-4\theta)^{wt(c)}\right) \le 2^{-m}\left(1 + \sum_{c\in C_j\setminus\{0\}:c_0=0}(1-4\theta)^{wt(c)}\right) \le$$

$$\le 2^{-m}(1+2^{m-1}(1-4\theta)^{d(C_j)}),$$

где $d(C_j)$ – минимальное расстояние кода C_j. Далее, согласно [10, теор. 8.84], справедливо неравенство $d(C_j) \ge d$, откуда на основании условия (12) следует формула (15).

Утверждение доказано.

Отметим, что условие (12) выполняется только для малых по сравнению с n значениях m (порядка $2\log(\varepsilon n)$, где $\varepsilon \in (0,1)$).

Следующее утверждение позволяет найти точное значение вероятности $\pi_{n,q}$ в случае, когда m принимает наибольшее возможное значение, равное $n-1$.

Утверждение 4. Пусть $m = n-1$. Тогда, если q нечетно, то

$$\pi_{n,q} = q^{-1}\sum_{k=0}^{q-1}\cos\left(\frac{2\pi k}{q}\right)\left(1-2\theta\left(1-\cos\left(\frac{2\pi pk}{q}\right)\right)\right)^n. \quad (16)$$

Если же $q = 2$, то

$$\pi_{n,2} = 2^{-1}(1-(1-4\theta)^n) + (1-2\theta)\theta^{n-1}. \quad (17)$$

Кроме того, если p' – элемент, обратный к p по модулю q, $p' \in \overline{0,q-1}$, и $n < \min\{p', q-p'\}$, то $\pi_{n,q} = 0$.

Доказательство. Если $m = n-1$, то $t = 1$, и многочлен $x^n - 1$ над полем $\mathbf{Z}_q$ раскладывается в произведение двух различных неприводимых сомножителей: $x-1$ и $\Phi_n(x) = x^{n-1} + x^{n-2} + \cdots + 1$. Поэтому элемент $f(x)$ кольца $R_{n,q}$ необратим тогда и только тогда, когда имеет место одно из двух взаимоисключающих условий: $f(1) = 0$; $f(x) = \Phi_n(x)$.

Пусть $f(x) = 1 + pF(x)$, где $F(x) = \xi_0 + \xi_1 x + \ldots + \xi_{n-1}x^{n-1}$, а $\xi_0, \xi_1, \ldots, \xi_{n-1}$ – независимые случайные величины, распределенные по закону (4). Тогда при нечетном q в силу неравенства $p < q-1$ имеем

$$\mathbf{P}\{f(x) = \Phi_n(x)\} = \mathbf{P}\{1 + p\xi_0 = 1,\ p\xi_1 = \ldots = p\xi_{n-1} = 1\} = 0,$$

$\pi_{n,q} = \pi_{n,q}(1)$, откуда на основании формулы (10) следует равенство (16). Если же $q = 2$, то

$$\mathbf{P}\{f(x) = \Phi_n(x)\} = \mathbf{P}\{\xi_0 = 0,\ \xi_1 = \ldots = \xi_{n-1} = 1\} = (1-2\theta)\theta^{n-1},$$

$\pi_{n,2} = \pi_{n,2}(1) + (1-2\theta)\theta^{n-1}$, откуда на основании формулы (11) следует равенство (17).

Покажем, наконец, то из условия $n < \min\{p', q-p'\}$ вытекает равенство $\pi_{n,q} = 0$. Заметим, что $p' > 1$, поскольку $n > 1$; следовательно, q – нечетное простое число и по доказанному

$$\pi_{n,q} = \pi_{n,q}(1) = \mathbf{P}\{\xi_0 + \xi_1 + \cdots + \xi_{n-1} \equiv (q-p') \bmod q\}.$$

Обозначим $\eta = \xi_0 + \xi_1 + \cdots + \xi_{n-1}$. Поскольку случайные величины $\xi_0, \xi_1, \ldots, \xi_{n-1}$ принимают значения 0, ± 1, то $|\eta| \le n$. Если $\eta \ge 0$, то в силу соотношений $0 \le \eta \le n < \min\{p', q-p'\} < q$ получаем, что $\eta \bmod q = \eta < q - p'$; следовательно, сравнение $\eta \equiv (q-p') \bmod q$ не выполняется. Если $\eta \le 0$, то в силу тех же соотношений получаем, что $-\eta \bmod q = -\eta < p'$, и сравнение $\eta \equiv (q-p') \bmod q$ также не выполняется. Таким образом, событие $\{\eta \equiv (q-p') \bmod q\}$ является невозможным и $\pi_{n,q} = \mathbf{P}\{\eta \equiv (q-p') \bmod q\} = 0$.

Утверждение доказано.

Следствие 4. Пусть выполняется условие утверждения 4, $p = 3$ и $q > 3n+1$. Тогда $\pi_{n,q} = 0$.

Доказательство. Достаточно заметить, что $p' = \dfrac{q+1}{3}$, если $q \equiv -1 \bmod 3$ и $p' = \dfrac{2q+1}{3}$, если $q \equiv 1 \bmod 3$.

Соотношения (16), (17) дают возможность изучить поведение вероятности $\pi_{n,q}$ как функции параметра θ в наиболее интересных с практической точки зрения случаях:

а) $q = 2^l$, n – нечетное простое число, 2 – примитивный элемент поля $\mathbf{Z}_n$;

б) q и n – различные нечетные простые числа, $p = 3 < q-1$, и показатель, которому принадлежит q по модулю n, равен $n-1$.

Как показано выше, в случае а) выполняется равенство $\pi_{n,q} = \pi_{n,2}$. При этом вероятность $\pi_{n,q}$ практически не отличается от $0{,}5$ при всех разумных, с практической точки зрения, значениях n и θ (другими словами, в среднем каждый второй случайно сгенерированный по указанному выше закону многочлен не обратим в кольце $R_{n.q}$, рис. 1, 2).

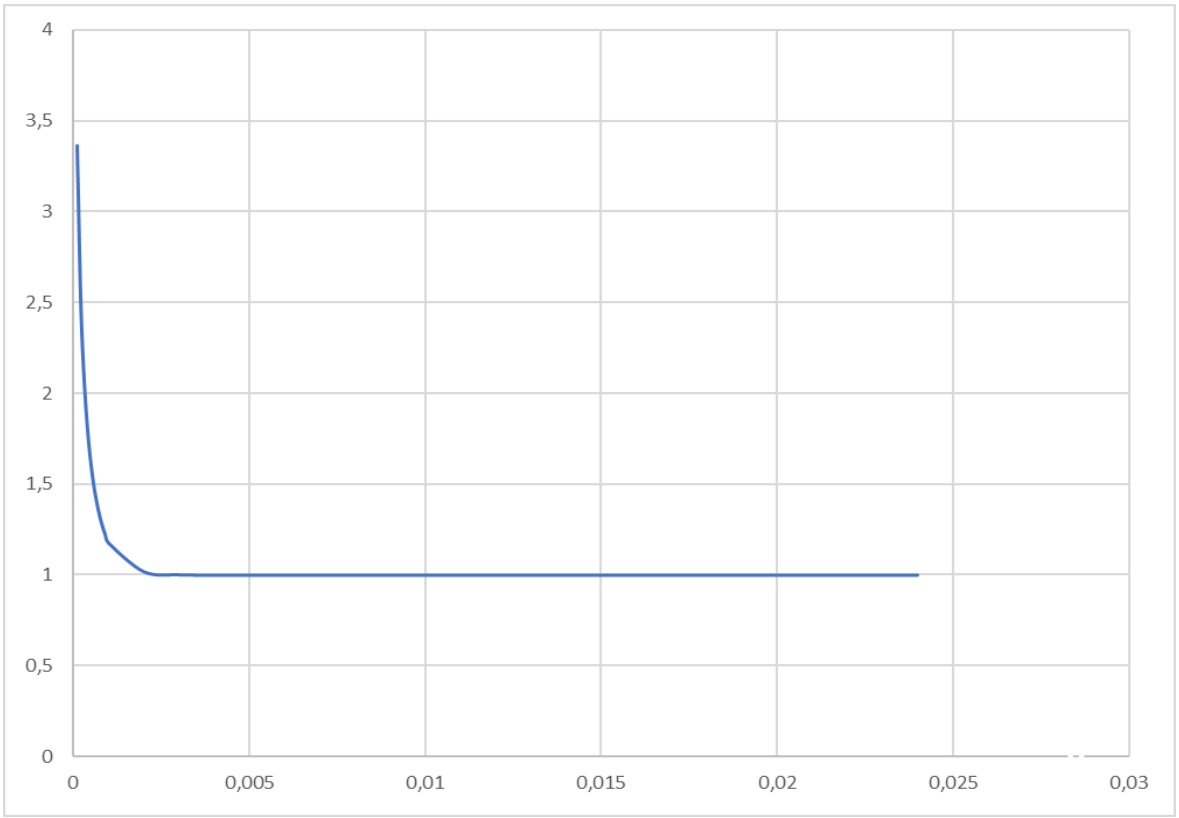

Рис. 1. Зависимость (взятого со знаком минус) двоичного логарифма

вероятности (17) от параметра θ при $n = 541$

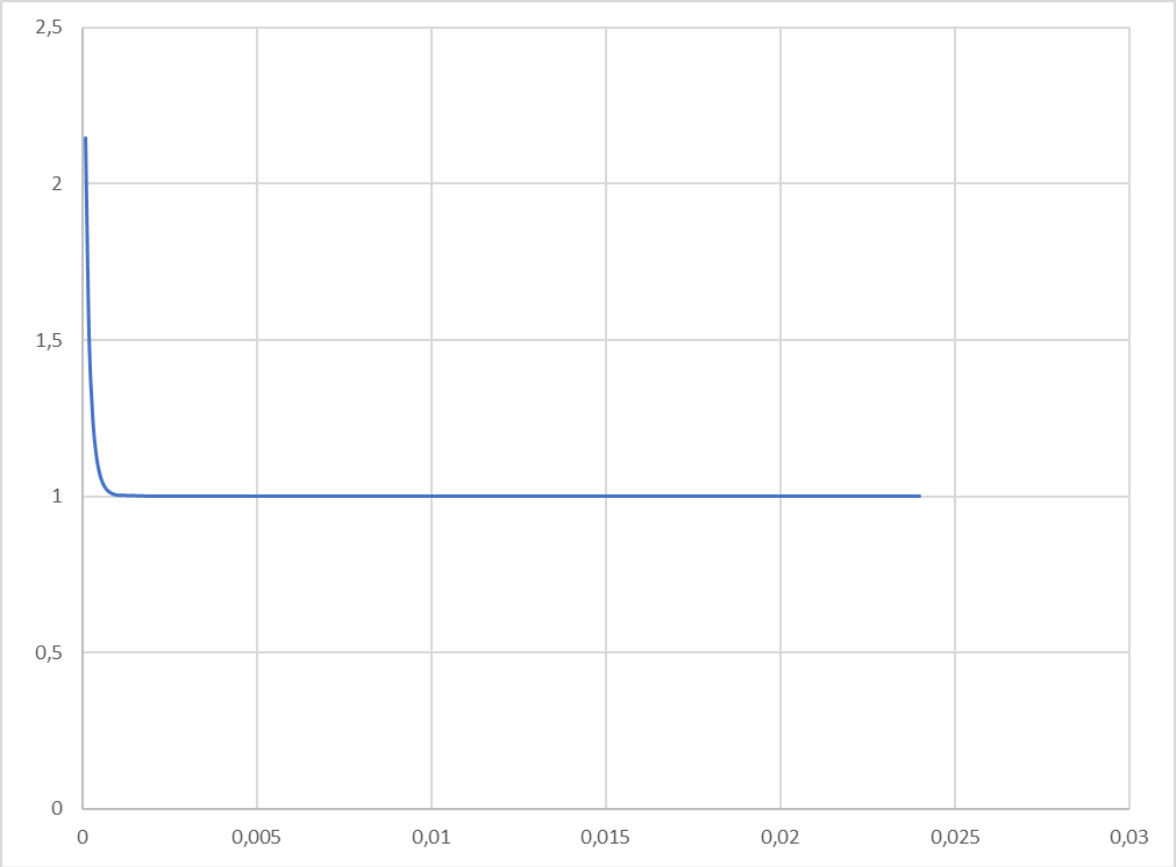

Рис. 2. Зависимость (взятого со знаком минус) двоичного логарифма вероятности (17) от параметра θ при $n = 1499$

В случае (б) вероятность $\pi_{n,q}$ быстро уменьшается с ростом q при фиксированных n и θ, обращаясь тождественно в нуль при $q > 3n+1$. Аналогичное поведение вероятности наблюдается с уменьшением параметра θ при фиксированных n и q, см. табл. 1, 2. При этом вероятность необратимости случайного многочлена в кольце $R_{n.q}$ не превосходит $1{,}5 \cdot 10^{-2}$, что существенно меньше $0{,}5$.

Таблица 1

Численные значения вероятности (16) при $n = 541$, $p = 3$

q θ	0,0001	0,001	0,01	0,1	0,2	0,3	0,4
59	$1{,}2 \cdot 10^{-44}$	$4{,}7 \cdot 10^{-25}$	$1{,}3 \cdot 10^{-8}$	$6{,}1 \cdot 10^{-3}$	$1{,}2 \cdot 10^{-2}$	$1{,}4 \cdot 10^{-2}$	$1{,}5 \cdot 10^{-2}$
73	$3{,}4 \cdot 10^{-55}$	$1{,}4 \cdot 10^{-31}$	$3{,}3 \cdot 10^{-11}$	$2{,}7 \cdot 10^{-3}$	$7{,}3 \cdot 10^{-3}$	$9{,}7 \cdot 10^{-3}$	$1{,}1 \cdot 10^{-2}$
257	$3{,}4 \cdot 10^{-243}$	$1{,}5 \cdot 10^{-157}$	$4{,}8 \cdot 10^{-75}$	$9{,}9 \cdot 10^{-17}$	$9{,}9 \cdot 10^{-10}$	$3{,}6 \cdot 10^{-6}$	$8{,}9 \cdot 10^{-6}$
331	$1{,}0 \cdot 10^{-323}$	$8{,}0 \cdot 10^{-214}$	$3{,}7 \cdot 10^{-107}$	$9{,}3 \cdot 10^{-26}$	$1{,}8 \cdot 10^{-14}$	$1{,}5 \cdot 10^{-8}$	$6{,}8 \cdot 10^{-8}$
383	0	$6{,}3 \cdot 10^{-258}$	$3{,}9 \cdot 10^{-133}$	$7{,}6 \cdot 10^{-34}$	$8{,}0 \cdot 10^{-19}$	$9{,}8 \cdot 10^{-11}$	$7{,}8 \cdot 10^{-10}$
487	0	0	$5{,}0 \cdot 10^{-186}$	$4{,}6 \cdot 10^{-52}$	$7{,}1 \cdot 10^{-29}$	$8{,}2 \cdot 10^{-16}$	$2{,}4 \cdot 10^{-14}$

Таблица 2

Численные значения вероятности (16) при $n=1499$, $p=3$

q θ	0,0001	0,001	0,01	0,1	0,2	0,3	0,4
463	0	$7{,}6\cdot10^{-250}$	$5{,}9\cdot10^{-106}$	$2{,}1\cdot10^{-19}$	$4{,}1\cdot10^{-11}$	$2{,}5\cdot10^{-8}$	$5{,}8\cdot10^{-7}$
659	0	0	$1{,}2\cdot10^{-181}$	$7{,}2\cdot10^{-37}$	$4{,}4\cdot10^{-20}$	$2{,}5\cdot10^{-14}$	$1{,}9\cdot10^{-11}$
787	0	0	$3{,}3\cdot10^{-235}$	$5{,}3\cdot10^{-51}$	$1{,}9\cdot10^{-27}$	$2{,}9\cdot10^{-19}$	$3{,}7\cdot10^{-15}$
827	0	0	$7{,}1\cdot10^{-254}$	$3{,}2\cdot10^{-56}$	$3{,}4\cdot10^{-30}$	$4{,}2\cdot10^{-21}$	$1{,}6\cdot10^{-16}$
1151	0	0	0	$9{,}9\cdot10^{-105}$	$2{,}8\cdot10^{-56}$	$1{,}2\cdot10^{-38}$	$1{,}1\cdot10^{-29}$
1289	0	0	0	$1{,}2\cdot10^{-129}$	$4{,}6\cdot10^{-70}$	$6{,}3\cdot10^{-48}$	$1{,}2\cdot10^{-36}$

Выводы

Полученные аналитические соотношения позволяют оценивать (а в ряде практически важных случаев – вычислять) значения вероятности обратимости случайных многочленов, используемых в качестве секретных ключей рассмотренной модификации криптосистемы NTRU. Эти соотношения могут быть использованы также для выбора параметров n, q и θ указанной криптосистемы.

Выбор в качестве q большого простого числа предпочтительнее (по критерию высокой вероятности обратимости многочлена) по сравнению с распространенным вариантом, в котором $q=2^l$ (см. рис. 1, 2 и табл. 1, 2). Отметим, что это условие относительно параметра q не вступает в конфликт с другими известными требованиями к криптосистеме, связанными со стойкостью и практичностью.

Список литературы: 1. *Hoffstein, J., Pipher, J., Silverman, J.H.* NTRU: a new high speed public key cryptosystem // Preprint, presented at the rump session of Crypto'96. – 1996. 2. *Steinfeld, R.* NTRU cryptosystem: resent developments and emerging mathematical problems in finite polynomial rings // http://users.monach.edu.au/~rste /NTRU_survey.pdf. – 2014. 3. *Bernstein, D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch.* NTRU Prime // http://eprint.iacr.org/2016/461. 4. *American* National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. – 2010. 5. *Hirschhorn, P., Hoffstein, J., Howgrave-Graham, N., Whyte, W.* Choosing NTRU parameters in light of combined lattice reduction and MITM aproaches // Applied Cryptography and Network Security, LNCS. – Vol. 5536. – 2009. – P. 437 – 455. 6. *Stehle´D., Steinfeld R.* Making NTRU as secure as worst-case problems over ideal lattices // Advances in Cryptology – EUROCRYPT 2011. – Proceedings. – Springer-Verlag. – 2011. – P.27–47. 7. *Hoffstein, J., Pipher, J., Schanck, J.M., Silverman, J.H., Whyte, W., Zhang, Z.* Choosing parameters for NTRUEncrypt // http://eprint.iacr.org/2015/708. 8. *Елизаров В.П.* Конечные кольца. – Москва : Гелиос АРВ, 2006. – 304 с. 9. *Ленг, С.* Алгебра ; пер. с англ. – Москва : Мир, 1968. – 564 с. 10. *Лидл, Р., Нидеррайтер, Г.* Конечные поля : в 2 т. ; пер. с англ. – Москва : Мир, 1988. – 818 с. 11. *Babai, L.* The Fourier transform and equations over finite abelian groups // http://people.cs.uchicago.edu/~laci /ren/fourier.pdf. – 2002.

Институт специальной связи и защиты информации
НТУ «КПИ» имени И. Сикорского

Поступила в редколлегию 12.04.2017