УДК 519.7

А.Н. АЛЕКСЕЙЧУК, А.А. МАТИЙКО

ДОСТИЖИМАЯ ВЕРХНЯЯ ГРАНИЦА SUP-НОРМЫ ПРОИЗВЕДЕНИЯ ЭЛЕМЕНТОВ КОЛЬЦА УСЕЧЕННЫХ МНОГОЧЛЕНОВ И ЕЕ ПРИМЕНЕНИЕ К АНАЛИЗУ NTRU-ПОДОБНЫХ КРИПТОСИСТЕМ

Аннотация. Получен ответ на вопрос, поставленный в 2008 г. В. Любашевским, об эффективном алгоритме вычисления параметра $\theta(f)$, характеризующего величину sup-нормы произведения элементов кольца усеченных многочленов по модулю заданного унитарного многочлена $f(x)$ с вещественными коэффициентами. Рассмотрено применение полученных результатов к оцениванию вероятности ошибочного расшифрования сообщений в NTRU-подобных криптосистемах.

Ключевые слова: решеточная криптография, кольцо усеченных многочленов, sup-норма произведения многочленов, NTRU-подобная криптосистема, вероятность ошибочного расшифрования.

ПОСТАНОВКА ЗАДАЧИ И ОБЗОР ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

Пусть $f(x)=x^n - c_{n-1}x^{n-1} - \cdots - c_0$ — унитарный многочлен степени $n>1$ над полем $\mathbf{R}$ вещественных чисел. Обозначим $R_f = \mathbf{R}[x]/(f(x))$ кольцо усеченных многочленов (truncated polynomials), состоящее из всех вещественных многочленов степени не выше $n-1$ с операциями сложения и умножения по модулю $f(x)$. Отождествим произвольный многочлен $a(x)=a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in R_f$ с вектором его коэффициентов $a=(a_0, a_1, \ldots, a_{n-1})$. Многочлен, равный произведению элементов $a(x), b(x) \in R_f$ в кольце R_f, обозначим символом $a(x) \cdot^f b(x)$, а вектор коэффициентов этого многочлена — символом $a \cdot^f b$. Далее определим sup-норму и l_1-норму многочлена $a(x) \in R_f$ (вектора a), полагая $||a||_\infty = \max\limits_{0 \le i \le n-1} |a_i|$ и $||a||_1 = |a_0| + \cdots + |a_{n-1}|$ соответственно.

Кольца вида R_f широко используются при построении решеточных (lattice based) и, в частности, NTRU-подобных криптосистем (см., например, статью [1] и ссылки к ней). При этом вопрос о корректности работы таких криптосистем (а именно малости вероятности ошибочного расшифрования сообщений законным получателем) приводит к задаче нахождения верхних оценок sup-нормы многочлена $a(x) \cdot^f b(x)$ в терминах норм многочленов-сомножителей. Решению этой задачи посвящена работа [2], где введен параметр, равный наименьшему числу $\theta(f)$ со свойством

$$\forall a(x) \in R_f : \max_{0 \le i \le n-1} \| a(x) \cdot^f x^i \|_\infty \le \theta(f) \| a \|_\infty , \tag{1}$$

и показано, что

$$\| a(x) \cdot^f b(x) \|_\infty \le n\theta(f) \| a \|_\infty \| b \|_\infty , \; a(x), b(x) \in R_f . \tag{2}$$

В [2] получена также верхняя граница $\theta(f) \le \max\limits_{0 \le i,j \le n-1} \| x^i \cdot^f x^j \|_\infty$ и найдены точные значения параметра $\theta(f)$ для многочленов $f(x)=x^n - 1$, $f(x)=x^n + 1$ и $f(x)=x^n + x^{n-1} + \cdots + 1$. При этом остается открытым вопрос о существовании алгоритма, позволяющего вычислять значение $\theta(f)$ для любого унитарного многочлена $f(x)$.

В настоящей статье показано, что значение $\theta(f)$ совпадает с нормой билинейного отображения $(a, b) \mapsto a \cdot^f b$, заданного на произведении нормированных векторных пространств $(\mathbf{R}^n, \|\cdot\|_\infty) \times (\mathbf{R}^n, \|\cdot\|_1)$ и принимающего значения в нормированном векторном пространстве $(\mathbf{R}^n, \|\cdot\|_\infty)$. Это позволяет предложить алгоритм вычисления значения $\theta(f)$ для любого напередзаданного унитарного многочлена $f(x)$ степени n за $O(n^2)$ операций над n-мерными векторами, а также получить более точную по сравнению с (2) (достижимую) верхнюю границу $||a(x) \cdot^f b(x)||_\infty \le \theta(f)||a||_\infty ||b||_1$, $a(x), b(x) \in R_f$. Кроме того, получено усиление леммы 2.11 из работы [2], утверждающей, что если $b(x)$ — случайный многочлен из R_f с независимыми коэффициентами, распределенными в интервале $[-B, B]$ по произвольному закону с математическим ожиданием 0, то для любого $a(x) \in R_f$ справедливо неравенство

$$\mathbf{P}(\|a \cdot^f b\|_\infty \ge \theta(f) B \|a\|_\infty \sqrt{n} \log n) \le 4ne^{-\frac{\log^2 n}{8}}. \tag{3}$$

Новая оценка, полученная в настоящей статье, утверждает, что вероятность в левой части неравенства (3) ограничена сверху значением $2ne^{-\frac{\log^2 n}{2}}$. Наконец, рассмотрено применение полученных результатов к оцениванию вероятности ошибочного расшифрования сообщений в NTRU-подобных криптосистемах.

ТОЧНОЕ ЗНАЧЕНИЕ И АЛГОРИТМ ВЫЧИСЛЕНИЯ ПАРАМЕТРА $\theta(f)$

Пусть E_1, E_2 и E_3 — нормированные векторные пространства с нормами $\|\cdot\|'$, $\|\cdot\|''$ и $\|\cdot\|'''$ соответственно, $B: E_1 \times E_2 \to E_3$ — билинейное отображение. Согласно известному определению (см., например, [3, п. 1.8]) нормой отображения B называется наименьшее число $||B||$ такое, что $\|B(a, b)\|''' \le \|B\| \, \|a\|' ||b||''$ для любых $a \in E_1$, $b \in E_2$.

Рассмотрим в качестве B билинейное отображение $B_f(a, b) = a \cdot^f b$, полагая $(E_1, \|\cdot\|') = (E_3, \|\cdot\|''') = (\mathbf{R}^n, \|\cdot\|_\infty)$, $(E_2, \|\cdot\|'') = (\mathbf{R}^n, \|\cdot\|_1)$.

Лемма 1. Справедливо равенство $\theta(f) = \|B_f\|$.

Доказательство. Из определения нормы следует, что

$$\|a(x) \cdot^f x^i\|_\infty \le \|B_f\| \, \|a(x)\|_\infty \, \|x^i\|_1 = \|B_f\| \, \|a(x)\|_\infty, \; a(x) \in R_f, \; 0 \le i \le n-1.$$

Следовательно, согласно определению параметра $\theta(f)$ выполняется неравенство $\theta(f) \le \|B_f\|$.

Далее, для любых $a(x), b(x) \in R_f$ имеем

$$\|a(x) \cdot^f b(x)\|_\infty = \left\| \sum_{i=0}^{n-1} b_i (a(x) \cdot^f x^i) \right\|_\infty \le \sum_{i=0}^{n-1} |b_i| \, \|a(x) \cdot^f x^i\|_\infty \le$$

$$\le \sum_{i=0}^{n-1} |b_i| \theta(f) \|a(x)\|_\infty = \theta(f) \, \|a(x)\|_\infty \, \|b(x)\|_1,$$

откуда вытекает, что $\|B_f\| \le \theta(f)$. Лемма доказана.

Обозначим $S = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ c_0 & c_1 & & \dots & c_{n-1} \end{pmatrix}$ сопровождающую матрицу многочлена $f(x) = x^n - c_{n-1}x^{n-1} - \ldots - c_0$.

Лемма 2. Для любых $a(x), b(x) \in R_f$ справедливо равенство $a \cdot^f b = ab(S)$. Другими словами, вектор коэффициентов произведения многочленов $a(x)$ и $b(x)$ в кольце R_f равен произведению вектор-строки a на матрицу $b(S)$.

Доказательство. Обозначим e_i вектор коэффициентов многочлена x^i, $0 \le i \le n-1$.

Вначале убедимся в справедливости равенства

$$e_0 a(S) = a. \tag{4}$$

Действительно, используя индукцию по i, нетрудно проверить, что $e_0 S^i = e_i$, $0 \le i \le n-1$. Следовательно, $e_0 a(S) = \sum_{i=0}^{n-1} a_i e_0 S^i = \sum_{i=0}^{n-1} a_i e_i = a$, что и требовалось доказать.

Заметим, что поскольку $f(x)$ является минимальным многочленом матрицы S, то отображение $a(x) \mapsto a(S)$ является изоморфизмом кольца R_f на кольцо, состоящее из всех квадратных матриц вида $b(S)$, где $b(x) \in R_f$. При этом изоморфизме многочлену $a(x) \cdot^f b(x)$ соответствует матрица $a(S)b(S)$ и на основании формулы (4), последовательно применяемой к многочленам $a(x) \cdot^f b(x)$ и $a(x)$, справедливы равенства $a \cdot^f b = e_0 a(S)\, b(S) = ab(S)$. Лемма доказана.

Зададим sup-норму вещественной $n \times n$-матрицы A, полагая $\| A \|_\infty = \max\{ \| Ax^{\mathrm{T}} \|_\infty : \| x \|_\infty = 1\}$, где максимум берется по всем векторам $x = (x_1, \ldots, x_n) \in \mathbf{R}^n$ таким, что $\| x \|_\infty = 1$. Нетрудно увидеть, что

$$\| A \|_\infty = \max\{ \| A_1 \|_1, \| A_2 \|_1, \ldots, \| A_n \|_1 \}, \tag{5}$$

где $A_1, A_2, \ldots, A_n$ — строки матрицы A.

Для любых $i, j, k \in \{0, 1, \ldots, n-1\}$ обозначим $(x^i \cdot^f x^j)_k$ k-й коэффициент многочлена $x^i \cdot^f x^j$. Рассмотрим $n \times n$-матрицу B_k с элементами $B_k(i, j) = (x^i \cdot^f x^j)_k$.

Лемма 3. Справедливо равенство $\theta(f) = \max\limits_{0 \le k \le n-1} \| B_k \|_\infty$.

Доказательство. Из определения матрицы B_k следует, что для любых многочленов $a(x), b(x) \in R_f$ k-й коэффициент многочлена $a(x) \cdot^f b(x)$ равен $(a(x) \cdot^f b(x))_k = bB_k a^{\mathrm{T}}$. Следовательно, $| (a(x) \cdot^f b(x))_k | \le \| b \|_1 \, \| B_k a^{\mathrm{T}} \|_\infty \le$ $\le \| b \|_1 \, \| B_k \|_\infty \, \| a \|_\infty$, $0 \le k \le n-1$ и

$$\| a \cdot^f b \|_\infty \le (\max_{0 \le k \le n-1} \| B_k \|_\infty) \| a \|_\infty \, \| b \|_1. \tag{6}$$

Отсюда на основании леммы 1 вытекает, что $\theta(f) \le \max\limits_{0 \le k \le n-1} \| B_k \|_\infty$.

Для доказательства равенства $\theta(f) = \max\limits_{0 \le k \le n-1} \| B_k \|_\infty$ достаточно убедиться, что существует пара многочленов $a(x), b(x) \in R_f$, для которых неравенство (6) обращается в равенство.

Действительно, выберем число $l \in \{0, 1, \ldots, n-1\}$ и вектор $a \in \mathbf{R}^n$ такие, что $\| B_l \|_\infty = \max_{0 \le k \le n-1} \| B_k \|_\infty$, $\| B_l a^{\mathrm{T}} \|_\infty = \| B_l \|_\infty \; \| a \|_\infty$. Положим $b = e_i$, где i — номер наибольшей по модулю координаты вектора $B_l a^{\mathrm{T}}$. Для указанных a и b выполняются равенства $|(a(x) \cdot^f b(x))_l| = | b B_l a^{\mathrm{T}} | = \| B_l a^{\mathrm{T}} \|_\infty = \| B_l \|_\infty \; \| a \|_\infty = \| B_l \|_\infty \; \| a \|_\infty \; \| b \|_1$. При этом по доказанному для любого $0 \le k \le n-1$ имеют место неравенства

$$| (a(x) \cdot^f b(x))_k | \le \| B_k \|_\infty \; \| a \|_\infty \; \| b \|_1 \le \| B_l \|_\infty \; \| a \|_\infty \; \| b \|_1 .$$

Следовательно, $\| a \cdot^f b \|_\infty = \max_{0 \le k \le n-1} | (a(x) \cdot^f b(x))_k | = \| B_l \|_\infty \; \| a \|_\infty \; \| b \|_1$ и неравенство (6) обращается в равенство.

Лемма доказана.

На основании леммы 3 и формулы (5) можно предложить следующий алгоритм вычисления параметра $\theta(f)$ по многочлену $f(x) = x^n - c_{n-1} x^{n-1} - \cdots - c_0$.

Для каждого $k = 0, 1, \ldots, n-1$:

1) положить $(x(0), x(1), \ldots, x(n-1)) = e_k$;
2) вычислить $x(i+n) = c_0 x(i) + \cdots + c_{n-1} x(i+n-1))$ для $i = 0, 1, \ldots, n-1$;
3) положить $B_k(i, j) = x(i+j)$, $i, j = 0, 1, \ldots, n-1$;
4) положить $\theta_k = \max_{0 \le i \le n-1} \{ | B_k(i, 0) | + | B_k(i, 1) | + \cdots + | B_k(i, n-1) | \}$.

Результатом выполнения алгоритма является $\theta_k(f) = \max_{0 \le k \le n-1} \theta_k$.

Теорема 1. Приведенный алгоритм корректно вычисляет значение $\theta(f)$ за $O(n^2)$ операций над n-мерными векторами. При этом $\theta(f)$ равно наибольшему элементу матрицы $U = \sum_{j=0}^{n-1} \mathrm{abs}(S^j)$, где $\mathrm{abs}(S^j)$ — матрица, составленная из модулей элементов матрицы S^j, $0 \le j \le n-1$.

Доказательство. Первое утверждение теоремы следует непосредственно из леммы 3 и формулы (5), применяемой к матрице $A = B_k$ при $k = 0, 1, \ldots, n-1$.

Для доказательства второго утверждения заметим, что на основании леммы 2 (i, j)-й элемент матрицы B_k равен $(x^i \cdot^f x^j)_k = e_i S^j e_k^{\mathrm{T}}$, $i, j, k \in \{0, 1, \ldots, n-1\}$. Поэтому l_1-норма i-й строки матрицы B_k равна значению $\sum_{j=0}^{n-1} | e_i S^j e_k^{\mathrm{T}} | = \sum_{j=0}^{n-1} e_i \mathrm{abs}(S^j) e_k^{\mathrm{T}}$, которое совпадает с (i, k)-м элементом матрицы U. Доказательство завершается применением леммы 3 формулы (5).

Теорема доказана.

ВЕРОЯТНОСТНЫЕ РЕЗУЛЬТАТЫ

Докажем следующую теорему, усиливающую оценку, приведенную в [2, лемма 2.11].

Теорема 2. Пусть $b(x)$ — случайный многочлен из R_f с независимыми коэффициентами, распределенными в интервале $[-B, B]$ по произвольному закону с математическим ожиданием 0. Тогда для любого $a(x) \in R_f$ справедливо неравенство

$$\mathbf{P}(\| a \cdot^f b \|_\infty \ge \theta(f) B \| a \|_\infty \sqrt{n} \log n) \le 2n e^{-\frac{\log^2 n}{2}} . \qquad (7)$$

Доказательство. Обозначим $c(n) = \theta(f) B \| a \|_\infty \sqrt{n} \log n$. Оценим сверху вероятность $p_k = \mathbf{P}(| (a(x) \cdot^f b(x))_k | \ge c(n))$, $0 \le k \le n-1$.

На основании леммы 2 справедливо равенство $(a(x)\cdot^f b(x))_k = ba(S)e_k^{\mathrm{T}} = \sum_{i=0}^{n-1} b_i m_i$, где $b=(b_0,\ldots,b_{n-1})$, $m_i = e_i a(S) e_k^{\mathrm{T}}$, $0 \le i \le n-1$. Заметим, что

$$|m_i| = \left| \sum_{j=0}^{n-1} a_j (e_i S^j e_k^{\mathrm{T}}) \right| \le \sum_{j=0}^{n-1} |a_j| |e_i S^j e_k^{\mathrm{T}}| \le \|a\|_\infty \sum_{j=0}^{n-1} |e_i S^j e_k^{\mathrm{T}}| \le \|a\|_\infty\, \theta(f),$$

где последнее неравенство вытекает из теоремы 1.

Таким образом, случайная величина $(a(x)\cdot^f b(x))_k$ является суммой независимых случайных величин $b_i m_i$, распределенных в интервале $[-B\|a\|_\infty\, \theta(f), B\|a\|_\infty\, \theta(f)]$ и имеющих математическое ожидание 0. Отсюда на основании неравенства Гефдинга [4] следует, что $p_k \le 2\exp\left\{-\frac{2c(n)^2}{n(2B\|a\|_\infty\, \theta(f))^2}\right\} = 2\exp\left\{-\frac{\log^2 n}{2}\right\}$. Наконец, формула (7) вытекает из оценки $\mathbf{P}(\|a\cdot^f b\|_\infty \ge c(n)) \le n \max_{0\le k\le n-1} p_k$.

Теорема доказана.

Применим полученные результаты к нахождению верхней границы вероятности ошибочного расшифрования сообщений в NTRU-подобной криптосистеме над кольцом $R_{f,q} = \mathbf{Z}_q[x]/(f(x))$, где $\mathbf{Z}_q$ — кольцо классов вычетов по модулю q, а $f(x)$ — унитарный многочлен степени n с целыми коэффициентами. Предположим, что q не делится на 3, а элементы кольца $\mathbf{Z}_q$ отождествляются с целыми числами в интервале $[-(q-1)/2, (q-1)/2]$ для нечетного q и в интервале $[-q/2, q/2-1]$ для четного q. Для любого $u = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1} \in \mathbf{Z}[x]$ обозначим $u \bmod q$ многочлен $(u_0 \bmod q) + (u_1 \bmod q)x + \cdots + (u_{n-1} \bmod q)x^{n-1} \in R_{f,q}$. Аналогично понимается обозначение и для $u \bmod 3$.

Секретным ключом рассматриваемой NTRU-подобной криптосистемы является пара многочленов (F, g) таких, что $F, g \in R_{f,q}$, $\|F\|_\infty = \|g\|_\infty = 1$ и многочлен $\varphi = 1+3F$ обратим в кольце $R_{f,q}$, а соответствующим открытым ключом (public key) является элемент кольца $R_{f,q}$, равный $h = 3g\varphi^{-1}$.

Множество открытых текстов шифрсистемы состоит из всех многочленов $m \in R_{f,q}$ таких, что $\|m\|_\infty = 1$. Для зашифрования открытого текста m на открытом ключе h генерируется случайный многочлен $r \in R_{f,q}$ такой, что $\|r\|_\infty = 1$, и вычисляется шифрованный текст $E_h(m, r) = (m + rh) \bmod q$. Расшифрование произвольного текста $c \in R_{f,q}$ на секретном ключе (F, g) выполняется по формуле $D_\varphi(c) = c\varphi (\bmod q) \bmod 3$. Если при этом $D_\varphi(E_h(m, r)) \ne m$, то происходит ошибка расшифрования.

Поведение вероятности ошибочного расшифрования сообщений в NTRU-подобных криптосистемах (при различных предположениях относительно распределений независимых случайных элементов F, g, m, r) исследовалось в [5–7] для случая $f(x) = x^n - 1$ и в работе [8] — для случая $f(x) = x^n - x^{n/2} + 1$ (при четном n). В работе [9] получены неасимптотические оценки вероятности ошибочного расшифрования сообщений в алгоритме NTRUEncrypt ($f(x) = x^n - 1$) при фиксированном секретном ключе.

Следующая теорема обобщает один из результатов работы [9] на случай кольца $R_{f,q}$.

Теорема 3. Пусть $F, g \in R_{f,q}$, $\|F\|_\infty = \|g\|_\infty = 1$, многочлен $\varphi = 1+3F$ обратим в кольце $R_{f,q}$ и $h = 3g\varphi^{-1}$. Пусть также m и r — случайные многочлены из

$R_{f,q}$ с независимыми в совокупности коэффициентами, распределенными на множестве $\{-1, 0, 1\}$ по произвольному закону с математическим ожиданием 0. Тогда справедливо неравенство

$$\mathbf{P}(D_\varphi(E_h(m, r)) \neq m) \leq 2n\exp\left\{-\frac{(q-2)^2}{144\, n\, \theta(f)^2}\right\}. \tag{8}$$

Доказательство. Из данных выше определений следует, что в случае ошибки расшифрования модуль, по крайней мере одного из коэффициентов многочлена $m\varphi + 3rg \in \mathbf{Z}[x]$, больше либо равен $q/2$. Следовательно, справедливы соотношения

$$D_\varphi(E_h(m, r)) \neq m \Rightarrow \|m(1+3F)+3rg\|_\infty \geq q/2 \Rightarrow \|mF + rg\|_\infty \geq (q-2)/6.$$

Для любого $k \in \overline{0, n-1}$ обозначим $p_k(F, g)$ вероятность того, что модуль k-го коэффициента случайного многочлена $mF + rg$ больше либо равен $q/2$. Повторяя рассуждения, приведенные в доказательстве теоремы 2, с учетом равенств $\|F\|_\infty = \|g\|_\infty = 1$, $\|m\|_\infty = \|r\|_\infty = 1$ получаем, что k-й коэффициент каждого из многочленов mF и rg является суммой не более n независимых случайных величин, распределенных в интервале $[-\theta(f), \theta(f)]$ и имеющих математическое ожидание 0. Отсюда на основании неравенства Гефдинга следует, что $p_k(F, g) \leq 2\exp\left\{-\frac{(q-2)^2}{144\, n\, \theta(f)^2}\right\}$. Наконец, формула (8) вытекает из оценки $\mathbf{P}(D_\varphi(E_h(m, r)) \neq m) \leq n \max\limits_{0 \leq k \leq n-1} p_k(F, g)$.

Теорема доказана.

В табл. 1 приведены результаты расчетов, полученные с помощью предложенного алгоритма и формулы (8), для ряда значений параметров, используемых в современных NTRU-подобных криптосистемах [1, 8]. Отметим, что эти результаты справедливы при очень слабых (указанных в теореме 3) ограничениях относительно многочленов F, g, m и r. При этом во многих случаях они позволяют получить содержательную информацию о величине вероятности ошибочного расшифрования сообщений при любом фиксированном значении секретного ключа.

Таким образом, предложенный алгоритм вычисления значений параметра $\theta(f)$ базируется на его естественной интерпретации как нормы некоторого билинейного отображения на произведении определенных нормированных векторных пространств. Это позволяет получить более точную по сравнению с известной работой [2] верхнюю границу sup-нормы произведения элементов кольца R_f, усилить лемму 2.11 из работы [2], а также установить оценки вероятности ошибочного расшифрования сообщений в NTRU-подобных криптосистемах над кольцом R_f при фиксированном ключе.

Таблица 1. Верхние оценки вероятности ошибочного расшифрования сообщений в NTRU-подобных криптосистемах

Криптосистема	Исходные данные для расчетов			Полученные результаты	
	n	q	$f(x)$	$\theta(f)$	Верхняя оценка (8)
NTRUEncrypt	443	2048	$x^n - 1$	1	$2^{-84,88}$
Falcon	512	12289	$x^n + 1$	1	$2^{-2944,16}$
Falcon	768	18433	$x^n - x^{n/2} + 1$	2	$2^{-1097,28}$
NNTRU	768	7681	$x^n - x^{n/2} + 1$	2	$2^{-181,72}$
SNTRUPrime	761	4591	$x^n - x - 1$	2	$2^{-58,74}$

СПИСОК ЛИТЕРАТУРЫ

1. Albrecht M.R., Curtis B.R., Deo A., Davidson A., Player R., Postlethwaite E.W., Virdia F., Wunderer T. Estimate all the {LWE, NTRU} schemes! *Cryptology ePrint Archive,* Report 2018/331. URL: http://eprint.iacr.org/2018/331.
2. Lyubashevsky V. Towards practical lattice-based cryptography, Ph.D, 2008. URL: https://escholarship/org/uc/item/0141w93p.
3. Картан А. Дифференциальное исчисление. Дифференциальные формы / Пер. с франц. Москва: Мир, 1971. 392 с.
4. Hoeffding W. Probability inequalities for sums of bounded random variables. *J. Amer. Statist. Assoc.* 1963. Vol. 58, N 301. P. 13–30.
5. Hirschhorn P., Hoffstein J., Howgrave-Graham N., Whyte W. Choosing NTRU parameters in light of combined lattice reduction and MITM approaches. *Applied Cryptography and Network Security*, LNCS. 2009. Vol. 5536. P. 437–455.
6. Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Z. Choosing parameters for NTRUEncrypt. *Cryptology ePrint Archive*. Report 2015/708. URL: http://eprint.iacr.org/2015/708.
7. Chen C., Hoffstein J., Whyte W., Zhang Z. NIST PQ Submission: NTRUEncrypt. A lattice based algorithm. URL: https://cscr.nist.gov/Projects/Post-Quantum-Cryptography, 2017.
8. Lyubashevsky V., Seiler G. NTTRU: Truly fast NTRU using NTT. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2019. Vol. 3. P. 180–201.
9. Матійко О.А., Олексійчук А.М. Оцінки помилкового розшифрування повідомлень у шифросистемі NTRUEncrypt при фіксованому ключі. *Захист інформації.* 2018. Т. 20, № 2. С. 89–94.

Надійшла до редакції 09.09.2020

А.М. Олексійчук, О.А. Матійко

ДОСЯЖНА ВЕРХНЯ МЕЖА SUP-НОРМИ ДОБУТКУ ЕЛЕМЕНТІВ КІЛЬЦЯ ЗРІЗАНИХ ПОЛІНОМІВ ТА ЇЇ ЗАСТОСУВАННЯ ДО АНАЛІЗУ NTRU-ПОДІБНИХ КРИПТОСИСТЕМ

Анотація. Отримано відповідь на питання, поставлене в 2008 р. В. Любашевським, про ефективний алгоритм обчислення параметра $\theta(f)$, що характеризує величину sup-норми добутку елементів кільця зрізаних поліномів за модулем заданого унітарного полінома $f(x)$ з дійсними коефіцієнтами. Розглянуто застосування отриманих результатів до оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних криптосистемах.

Ключові слова: решіткова криптографія, кільце зрізаних поліномів, sup-норма добутку поліномів, NTRU-подібна криптосистема, ймовірність помилкового розшифрування.

A.N. Alekseychuk, A.A. Matiyko

ACHIEVABLE UPPER BOUND FOR THE SUP-NORM OF THE ELEMENTS' PRODUCT IN THE RING OF TRUNCATED POLYNOMIALS AND ITS APPLICATION TO THE ANALYSIS OF NTRU-LIKE CRYPTOSYSTEMS

Abstract. The answer to the question posed in 2008 by V. Lyubashevsky about an efficient algorithm for calculating the parameter $\theta(f)$ that characterizes the value of the sup-norm of the elements' product in the ring of truncated polynomials modulo a given mimic polynomial $f(x)$ with real coefficients is obtained. The application of the obtained results to the estimation of decryption failure probability of messages in NTRU-like cryptosystems is considered.

Keywords: lattice-based cryptography, truncated polynomial ring, sup-norm of polynomials' product, NTRU-like cryptosystem, decryption failure probability.

Алексейчук Антон Николаевич,
доктор техн. наук, доцент, профессор кафедры Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: alex-dtn@ukr.net.

Матийко Александра Андреевна,
преподаватель Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского», e-mail: alexm1710@ukr.net.