УДК 511.48:519.61

Е. А. Киршанова

АНАЛИЗ СТРУКТУРЫ И СТОЙКОСТИ КРИПТОСИСТЕМЫ NTRU

Делается обзор структуры криптосистемы NTRU. Рассмотрены возможные пути атаки на криптосистему, в частности атака, основанная на применении числовых решеток.

The structure of NTRU cryptosystem is described. Variants of attacks on NTRU cryptosystem, particularly an attack based on lattices are considered.

Ключевые слова: NTRU-криптосистема, кольцо усеченных многочленов, числовые решетки, атака «встретимся на середине».

Key words: NTRU-cryptosystem, polynomial truncated ring, lattices, meet-in-the-middle attack.

Криптосистема NTRU (*N-th degree truncated polynomial ring*) основана на алгебраической структуре полиномиального кольца (см.[1; 6]). Поиск кратчайшего вектора в заданной числовой решетке — трудноразрешимая задача. NTRU относят к *быстрым криптосистемам* — ее можно использовать в устройствах с ограниченными ресурсами, поэтому она эффективна и возможно ее дальнейшее применение и развитие.

Основы криптосистемы. Пусть R — полиномиальное кольцо с неприводимым многочленом $R = \frac{Z[x]}{(x^N - 1)}$. В таком кольце произведение (обозначается $*$) задается не как обычное произведение многочленов, а как «произведение свертки», то есть X^N заменяется на 1, X^{N+1} — на X и так далее (см. [6]). Такое кольцо R называют *кольцом усеченных многочленов*. Необходимые параметры криптосистемы — это N (размерность кольца R), p и q — два взаимно простых в R числа (обычно q — большое). Многочлены $f \in R$ и $g \in R$ выбираются пользователем Бобом так, чтобы многочлен f был обратим в R. Боб вычисляет f_q^{-1} и f_p^{-1} в кольцах $R = \frac{Z[x]}{(q, x^N - 1)}$ и $R = \frac{Z[x]}{(p, x^N - 1)}$ соответственно. Для генерации открытого ключа Боб вычисляет многочлен h: $h = f_q^{-1} * g (\mathrm{mod} q)$.

Зашифровка. Для зашифровки текста $m \in R$ Алиса (сторона, желающая отослать сообщение) использует открытый ключ Боба (сторона, принимающая сообщение) h, выбирает случайным образом многочлен $r \in R$ и вычисляет e (шифр-текст): $e \equiv r * h + m (\mathrm{mod} q)$.

Расшифровка. Используя свой секретный ключ, Боб вычисляет: $a \equiv f * e (\mathrm{mod} q)$. Коэффициенты для a Боб выбирает так, чтобы они лежали в интервале $(-0,5q, 0,5q)$. Затем он приводит многочлен a по модулю p и вычисляет $f_q^{-1} * a (\mathrm{mod}\, p)$. Полученное значение есть m.

Как это работает? Опишем основную цепочку сравнений (см. [1]).

Когда Боб вычисляет сравнение $a \equiv f * e (\mathrm{mod} q)$, в действительности:

$a \equiv f * e (\mathrm{mod} q) = f * (r * h + m) (\mathrm{mod} q) =$ [так как $e \equiv r * h + m (\mathrm{mod} q)$]

$= f * (r * p \cdot f_q * g + m) (\mathrm{mod} q) =$ [так как $h = p \cdot f_q^{-1} * g (\mathrm{mod} q)$]

$= p \cdot r * g + f * m (\mathrm{mod} q)$ [так как $f * f_q = 1 (\mathrm{mod} q)$].

$$b = f * m (\mathrm{mod}\, p); \quad f_p * b = f_p * f + m = m (\mathrm{mod}\, p).$$

Разберем некоторые методы оптимизации параметров NTRU.

1. Большую часть времени занимают вычисления произведений в кольце и нахождения обратных. Поэтому для уменьшения времени выполнения представим секретный ключ f в виде: $f = 1 + p \cdot f_1 \cdot f_1 \in R$. Тогда $f_p^{-1} = 1$, и необходимость вычислять обратный по $(\mathrm{mod}\, p)$, и второе произведение при дешифровании исчезает (см. [2]).

2. Необязательно p быть целым, p может быть и многочленом, главное, чтобы p и q были взаимно просты в кольце R. При выборе $p = X + 2$ имеем все требования криптосистемы (взаимная простота эквивалентна тому, что элементы p, q и $X^N - 1$ образуют единичный идеал в $Z[X]$) и отображение {бинарный многочлен $m(x)$} $\to R/pR$ инъективно [2].

Вестник Российского государственного университета им. И. Канта. 2010. Вып. 10. С. 112 – 115.

Открытый и секретный ключи криптосистемы — многочлены, их можно представить в виде векторов, а вектора, в свою очередь, — в виде векторов *n*-мерных числовых решеток. Такое представление ключей криптосистемы дано в [3]. Рассмотрим основные шаги. Секретные ключи Боба (*f, g*) представим в виде короткого вектора $(f, g) \in Z^{2n}$. Решетка этих секретных параметров будет *q*-ичной решеткой $\Delta_q((T \cdot f,\ T \cdot g)^T)$ (ее определение и характеристики см. в [3]). При таких условиях открытый ключ будет выглядеть $H = \begin{bmatrix} I & 0 \\ T \cdot h & q \cdot I \end{bmatrix}$, где $h = [T \cdot f]^{-1} \cdot g (\mathrm{mod}\, q)$. Зашифровка текста $m\{1,0,-1\}^n$ с $d_f + 1$ положительных единиц и с d_f отрицательных производится с помощью наугад выбранного вектора $r \in \{1,0,-1\}^n$ по схеме: $\begin{bmatrix} -r \\ m \end{bmatrix} \mathrm{mod} \begin{bmatrix} I & 0 \\ T \cdot h & q \cdot I \end{bmatrix} = \begin{bmatrix} 0 \\ (m + [T \cdot h] \cdot r) \mathrm{mod}\, q \end{bmatrix}$ (редукция вектора ошибок (-*r, m*) по базису *H*). Первые *n* координат всегда нулевые, а *n*-размерное векторное пространство $(m + [T \cdot h] \cdot r) \mathrm{mod}\, q = c$ и будет зашифрованным сообщением. Расшифровывается сообщение умножением шифр-текста *c* на матрицу $[T \cdot f] \mathrm{mod}\, q$.

Кроме этого в статье [3] представлены основанные также на числовых решетках GHH/HNF и Adjtai-Dwork криптосистемы.

В любом описании криптосистемы не обходится без рассмотрения конкретных числовых значений параметров, а вместе со значением и длины ключей. В [3] представлена таблица, отражающая зависимость длины ключа и оценки безопасности от параметров *n, q* и d_f.

Теоретическая сложность алгоритма NTRU дана в [4]. Зашифровка текста длиной $(n-k) \cdot \log_2 p$ бит займет $O(n^2)$ арифметических операций, столько же расшифровка сообщения (длина шифр-текста $n \cdot \log_2 q$ бит). Тогда длины секретного и открытого ключей равны $2n \cdot \log_2 p$ бит и $n \cdot \log_2 q$ бит. Также в [4] приведена сравнительная таблица криптосистем NTRU, RSA, McEliece и GHH. По ней видно, что криптосистема NTRU выигрывает у последних двух за счет длины открытого и секретного ключей (длины ключей в McEliece и GHH равны N^2), а у RSA — за счет высокой скорости зашифровки/расшифровки и создания ключей.

Таблица

Сравнительная таблица криптосистем (*N* — параметр безопасности)

Параметры шифрования	NTRU	RSA	GGH
Скорость зашифровки	N^2	N^2	N^2
Скорость расшифровки	N^2	N^2	N^2
Длина открытого ключа	N	N	N^2
Длина секретного ключа	N	N	N^2

Анализ безопасности криптосистемы описан в [4]. Наиболее очевидный способ — атака перебором. Злоумышленник может искать:

1) секретный ключ *f*, подбирая его так, чтобы $f * h (\mathrm{mod}\, q)$ было небольшим;

2) многочлен *g*, подбирая его так, чтобы $g * h^{-1} (\mathrm{mod}\, q)$ было небольшим;

3) вектор ошибок *r*, проверяя $e - r * h (\mathrm{mod}\, q)$.

Пытаясь отыскать секретный ключ f (*f* представлен как $f = 1 + p \cdot F$), мы точно знаем, что первая координата этого многочлена равна 1. Тогда при полном переборе векторов (а именно так удобнее представлять многочлен) останется проверить $\binom{2}{N-1}$ всевозможных вариантов для *f* (поворотов оставшихся $d_f - 1$ единиц), при этом проверяя произведение $f * h$ (это произведение есть многочлен g и оно состоит из 0 и 1). Такой многочлен появится d_f раз среди $\binom{2}{N-1}$, поскольку существует d_f поворотов многочлена *f* с единицей на первом месте. Злоумышленнику останется отыскать подходящий ключ из этих d_f многочленов.

Существуют и другие способы, которыми злоумышленник может «взломать» криптосистему. Один из них — атака «встретимся на середине» (см. [5]). Главный ее момент — представление $f:(f_1+f_2)*h=g$. Для коэффициентов это уравнение перепишем так: $(f_1*h)[i]=-(f_2*h)[i]+0$ или 1. Поэтому злоумышленник будет перебирать всевозможные значения f_1 и f_2, замечая, что полученные коэффициенты вектора f_2 должны отличаться от коэффициентов f_1 не более чем на 1 (все вычисления проводятся по модулю q). Таких совпадений получится $d_f!$ (для «лидирующей» единицы существует $(d_f-1)!$ положений (d_f-1) единиц). Злоумышленнику останется проверить их. Оценка времени выполнения алгоритма и необходимое количество памяти описаны в [5].

Также интересна атака, основанная на алгоритмах с применением числовых решеток. Основные определения и теоремы, связанные с числовыми решетками, описаны в [6]. Так, *алгоритм Бабая* (алгоритм возвращает решение задачи *CVP* — нахождение ближайшей точки, принадлежащей решетке, к данной, не принадлежащей ей) достаточно подробно описан в [7]. Обширный материал о числовых решетках с обоснованием основных задач, решаемых с их помощью, представлен в [8]. Кроме того, там предложены несколько схем шифровки NTRU и схемы цифровой подписи NTRU. Алгоритм зашифровки, описанный выше, в статье [8] называется «сырым», и там предложены другие схемы (обе схемы применяют к исходному тексту хэш-функции).

Почти всю используемую литературу и статьи можно найти в [9]. Там же описаны примеры ко всем важным алгоритмам.

Список литературы

1. *The NTRU public key cryptosystem* // A tutorial. The NTRU Cryptosystems, Inc. URL: http://securityinnovation. com/cryptolab/tutorials. shtml.
2. *Hoffstein J., Silverman J.* Optimization for NTRU // Public-key cryptography and computational number theory. Berlin-N.-Y.: Walter de Gruyter, 2001.
3. *Micciiancio D., Regev O.* Lattice-based cryptography. July 22, 2008.
4. *Hoffstein J., Lieman D., Pipjer J., Silverman J.* NTRU: A public key cryptosystem. URL: http://grouper. ieee. org/groups/1363/lattPK/submissions/ntru. pdf.
5. *Howgrave-Graha N., Silverman J., Whyte W.* Meet-in-the-middle attack on an NTRU private key // NTRU Cryptosystems Technical Report #004. Version 2.
6. *Hoffstein J., Pipher J., Silverman J.* An introduction to mathematical cryptography. Springer. 2008.
7. *Galbraith S.* Mathematic of public key cryptography.
8. *Hoffstein J., Howgrave-Graham N., Pipher J., Silverman J.* Practical lattice-based cryptography: NTRUEncrypt and NTRUSign.
9. Application security, secure software development, and software secure training. URL: http://securityinnovation. com.

Об авторе

Елена Алексеевна Киршанова — студ., РГУ им. И. Канта, e-mail: kirshanoff@gmail.com.

Author

Elena Kirshanova — student, IKSUR, e-mail: kirshanoff@gmail.com.