УДК 519.719.2

РАЗДЕЛЕНИЕ СЕКРЕТА В ПОСТКВАНТОВЫЙ ПЕРИОД

Г.В. Матвеев

Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь, matveev@bsu.by

Криптография на основе решеток в настоящее время является одной из самых популярных областей математической криптографии. Криптографические конструкции на основе решеток являются ведущими кандидатами для постквантовой криптографии с открытым ключом. Это еще больше мотивирует изучение криптографических конструкций на основе решеток. В этой статье мы предлагаем метод разделения секрета основанный на теории решеток.

В разделе 1 содержатся необходимые сведения из постквантовой криптографии, краткий обзор двух работ по разделению секрета, а также постановка задачи и формулировка цели и задач исследования.

В разделе 2 приведены основные факты по теории модулярного разделения секрета и указаны ссылки на работы по теории решеток, на которых основано наше исследование.

В разделе 3 содержаться полученные результаты, их обсуждение и сравнение с уже известными результатами.

Ключевые слова: постквантовая криптография; криптография на основе решеток; китайская теорема об остатках; модулярное разделение секрета.

SECRET SHARING IN THE POST-QUANTUM PERIOD

G.V. Matveev

Belarusian State University, 4 Niezalieznasci Avenue, Minsk 220030, Belarus,
e-mail: matveev@bsu.by

Lattice-based cryptography is one of the most popular areas in mathematical cryptography nowadays. Lattice-based cryptographic constructions are the leading candidates for public-key post-quantum cryptography. This further motivates the study of lattice-based cryptographic constructions . In this paper, we introduce a method of lattice-based secret sharing scheme.

The organization of the paper is as follows:

Section 1 contains the necessary information from post-quantum cryptography, a brief overview of two works on the secret sharing, as well as the formulation of the task and the formulation of the purpose and objectives of the study. Section 2 provides basic facts on the theory of modular secret sharing and references on the theory of lattices on which our study is based. Section 3 contains the results obtained, their discussion and comparison with the known results.

Keywords: post-quantum cryptography; lattice-based cryptography; Chinese Remainder Theore; modular secret sharing.

Введение

Идея квантовых вычислений была независимо предложена Юрием Ивановичем Маниным и Ричардом Фейнманом в начале 1980-х. С тех пор была проделана большая работа по созданию действующего квантового компьютера.

Известно, что квантовый компьютер может значительно ускорить решение ряда задач, таких как факторизация чисел и дискретное логарифмирование в группе точек эллиптической кривой. Это становиться существенной проблемой для криптографии, так как безопасность распространенных стандартизированных систем зависит от сложности решения этих задач.

Тем не менее, квантовые вычисления довольно длительное время оставались лишь потенциальной возможностью, которую нельзя было технически реализовать. Однако в последнее время перспектива создания квантовых компьютеров улучшилась [1] и это стимулировало NIST объявить открытый конкурс по созданию новых постквантовых стандартов. Основное требование для алгоритмов шифрования постквантовой криптографии состоит в том, что они должны быть основаны на NP- сложных задачах. Отметим такие знаковые события события:

2003 год: Д.Бернштейн предлагает термин “постквантовая криптография”,

2006 год: первая конференция PQCrypto,

2017 год: объявлен конкурс NIST.

Уже проведены три этапа конкурса NIST, определены перспективные направления и произведен конкурсный отбор участников.

В настоящее время разработка алгоритмов постквантовой криптографии ведется по четырем направлениям, использующих:

1. Теорию решеток (Lattice based cryptography),
2. Коды, исправляющие ошибки (Code based cryptography),
3. Многочлены в конечных полях (Multivariate, quadratic equations cryptography),
4. Теорию хэш-функций для больших данных (Hash-based cryptography).

На третьем этапе конкурса NIST победителями признаны:

1. По направлению, использующему теорию решеток: три криптосистемы с открытым ключом CRYSTALS-Kyber, NTRU, SABER и две системы цифровой подписи CRYSTALS-Dilithium, FALCON.

2. По направлению, использующему коды, исправляющие ошибки – криптосистема Мак-Элиса.

3. По направлению, использующему многочлены в конечных полях – система цифровой подписи Rainbow.

По итогам конкурса напрашивается очевидный вывод о том, что теория решеток становится вычислительной базой основных постквантовых стандартов. Это, безусловно, повлечет разработку новых и оптимизацию известных решеточных алгоритмов, что делает привлекательным и естественным более широкое криптографическое применение этих алгоритмов.

В настоящей работе теория решеток применяется и для изучения модулярного разделения секрета. Первые результаты в этой области получил Н. Шенец в работе [2], в которой рассматривается задача построения модулярных схем разделения секрета на основе целочисленных решеток.

Особенностью подхода, предложенного Н. Шенцом, является использование мономиального упорядочения на полугруппе $Z^n > 0$, которое применяется для определения частичного секрета участника. В рамках предложенного подхода была построена однородная асимптотически идеальная многомерная пороговая схема разделения секрета.

Решеточный подход применяется и для решения еще одной важной задачи в теории разделения секрета. А именно, в работе [3] предложен способ увеличения порога для любой схемы Шамира даже в случае если такое увеличение и не предполагалось заранее. Найденное решение поставленной задачи не требует дополнительного обмена информацией между дилером и участниками протокола. Надо сказать, что эта проблема решалась и ранее, но лишь путем дополнительного обмена информацией между дилером и участниками протокола либо для этой цели разрабатывались специальные схемы разделения секрета. Основе предложенного способа лежит решеточное декодирование кода Рида-Соломона.

В настоящей работе предлагается более простой способ разделения секрета не использующий мономиальное упорядочение для определения частичного секрета участника. Получен ряд структурных результатов и, в частности, построена однородная асимптотически идеальная многомерная пороговая схема разделения секрета.

1. Методология исследования

Для решения поставленной задачи используется классическая теория сравнений (модулярная арифметика) и CRT-алгоритм, в частности, а также теория решеток [4]. Полученные результаты можно рассматривать как многомерное обобщение модулярного целочисленного разделения секрета [5].

Напомним основные понятия и задачи теории разделения секрета.

Под *схемой разделения секрета* (СРС) понимают распределение секрета c на части $c_1, c_2, ..., c_t$ между t участниками и такой алгоритм вычисления секрета c, при котором его могут вычислить лишь заранее определенные (разрешенные) подмножества участников.

Дадим теперь строгие определение структуры доступа и пороговой структуры доступа в частности.

Определение 1. *Под структурой доступа Г будем понимать любое семейство подмножеств множества всех участников со свойством монотонности, т.е.*

$$A \in \Gamma, A \subset B \subset I \Rightarrow B \in \Gamma.$$

Среди СРС важное место занимают пороговые схемы. СРС называется *(k,t)*-пороговой схемой, если разрешенными являются все подмножества мощности не меньше k, где k - некоторое фиксированное число $1 \le k \le t$.

Под реализацией структуры доступа Г будем понимать такой алгоритм, который позволяет восстанавливать секрет лишь для подмножеств участников, содержащихся в семействе Γ.

При разработке схем разделения секрета стараются удовлетворить нескольким естественным требованиям. К их числу в первую очередь относится требование *идеальности* схемы разделения секрета, т.е. чтобы размер частичного секрета c_i не превышал размера основного секрета c. С другой стороны, желательно, чтобы неразрешенные множества участников не получали никакой дополнительной информации к имеющейся априорной о возможном значении секрета c – это требование *совершенности*. Иногда требование *идеальности* включает в себя требование *совершенности.*

В криптографии традиционно широко используется вычисление в кольцах вычетов Z_m. Видимо, этим объясняется популярность следующей пороговой *(k,t)*-схемы. Рассмотрим систему $m_1 < m_2 < ... < m_t$ попарно взаимно простых модулей, для которых выполнено условие

$$M_1 = m_1 m_2 ... m_k > m_{t-k+2} m_{t-k+3} ... m_t = M_2.$$

Одновременно требуется, чтобы разность $M_1 - M_2$ была по возможности большой. Секрет c выбирается случайным образом из промежутка (M_2, M_1), а частичный секрет c_i i-го участника, $i = 1, 2, ..., t$, есть наименьший неотрицательный вычет c по модулю m_i. Предполагается, что каждый участник знает не только свой частичный секрет c_i, но и модуль m_i.

В основе модулярной схемы лежит утверждение о том, что любая система сравнений

$$\begin{cases} x \equiv c_{i_1} (\mathrm{mod}\, m_{i_1}), \\ x \equiv c_{i_2} (\mathrm{mod}\, m_{i_2}), \\ \quad \vdots \\ x \equiv c_{i_s} (\mathrm{mod}\, m_{i_s}) \end{cases}$$

имеет единственное решение в промежутке (M_2, M_1), если $s \geq k$, и имеет достаточно много решений в противном случае.

Основная трудность в построении этих схем заключается в подборе модулей $m_1, m_2, ..., m_t$, удовлетворяющих условию $M_1 = m_1 m_2 ... m_k > m_{t-k+2} m_{t-k+3} ... m_t = M_2$. По этой причине в кольце целых чисел условия идеальности и совершенности можно реализовать лишь с некоторым приближением. Как показано в работах [6], [7] этот недостаток схемы устраняется путем перехода от кольца целых чисел к кольцу многочленов от одной переменной над полем Галуа. На этом пути впервые были построены идеальные модулярные схемы разделения секрета.

2. Результаты и их обсуждение

Рассмотрим конечнопорожденный Z-модуль Z^n. Пусть $a_1, a_2, \ldots, a_n$ линейно независимые над полем R векторы из Z^n.

Определение 2. *Решеткой Λ в Z^n называется множество всех векторов (точек) $x = \sum_{i=1}^{n} u_i a_i$, где $u_i \in Z$, а векторы $a_1, a_2, \ldots, a_n$ называют базисом решетки Λ.*

Если каждая точка решетки Λ является также точкой решетки M, то Λ называется подрешеткой решетки M.

Для построения схемы разделения секрета необходимо определить:

1. как выбирать модули участников (здесь в качестве модулей выступают подрешетки),
2. как строить вектор-вычет (частичный секрет) участника,
3. как выбирать вектор-секрет для заданной структуры доступа,
4. как восстанавливать вектор-секрет по частичным секретам.

В работе [2] предложен способ построения частичного секрета использующий мономиальные упорядочения. Сначала на $Z^n > 0$ задается

порядок. Каждому участнику i дается в качестве открытого ключа некоторая подрешетка Λ_i, заданная ее базисной матрицей A^i. Секретом является некоторая точка $c \in Z^n > 0$.

Как и в одномерном случае, каждый участник в качестве частичного должен получить минимальный в некотором смысле представитель своего класса $\{A^i x + c,\ x \in Z^n\}$. А именно, среди всех представителей класса $\{A^i x + c,\ x \in Z^n\}$ участнику i дается минимальный относительно заданного порядка на $Z^n > 0$ вектор c_i. Так определяется процедура приведения секрета по модулю подрешетки [2].

Для восстановления секрета с необходимо найти пересечение классов, а именно решить следующую задачу:

$$\{A^i x + s^i\} \cap \{A^j y + s^j\} = \{A^{ij} z + s^{ij}\},\ x, y, z \in Z^n,$$

где A^{ij} – базисная матрица пересечения подрешеток Λ_i и Λ_j, а s^{ij} минимальный представитель пересечения классов. Ясно, что в общем случае пересечение классов может быть пусто. В данном случае пересечение не пусто, поскольку каждому классу принадлежит точка с.

Отметим, что выбор (генерация) модулей и секрета в предложенной схеме напрямую зависит от рассматриваемой структуры доступа и заданного порядка.

Наш подход основан на следующем важнейшем параметре решетки и не зависит от мономиальных упорядочений решеток.

Определение 3. Фундаментальным параллелепипедом решетки называется множество точек

$$P = \{\sum_{i=1}^{n} x_i\ a_i, 0 \le x_i\ < 1\}.$$

1. В качестве открытых ключей участников выбираются подрешетки $\{\Lambda_i\}$, $i=1,2,\ldots,n$.

2. Частичный секрет участника определяется как вычет вспомогательного секрета $S = \sum_{j=1}^{j=n} \alpha_j a_j$, $\alpha_j \in R$ по модулю подрешетки $s_i = S \bmod \Lambda_i$. Под вычетом в данном случае понимается представитель смежного класса $S + \Lambda_i$ в фундаментальном параллелепипеде решетки Λ_i

$$s_i = \sum_{j=1}^{j=n} \{\alpha_j^i\} a_j,\ 0 \le \{\alpha_j^i\} < 1,$$

где $\{\alpha_j^i\}$ – дробная часть α_j^i.

В рамках предложенного подхода получены следующие результаты.

Теорема 1. *Существует решеточно-модулярная реализация произвольной структуры доступа.*

Теорема 2. *Существует однородная асимптотически совершенная и асимптотически идеальная пороговая схема разделения секрета в* Z^n.

Качество схемы можно улучшить путем перехода от целочисленной решетки Z^n к решетке над кольцом многочленов от одной переменной над полем Галуа.

Теорема 3. *Существует идеальная и совершенная решеточно-модулярная реализация пороговой структуры доступа в решетке над кольцом многочленов.*

Замечание. *Предложенный алгоритм для вычисления вычета по модулю решетки имеет полиномиальную сложность* $O(n^3)$.

Таким образом, к настоящему времени в статьях [2], [3] и в данной работе решены следующие задачи:

1. Предложены алгоритмы приведения секрета по модулю подрешетки.

2. Доказана возможность многомерной модулярной реализации произ-вольной структуры доступа.

3. Построена однородная асимптотически совершенная и асимптотически идеальная пороговая схема разделения секрета в Z^n.

4. Решена задача по увеличению порога схемы разделения секрета после распределения частичных секретов

Библиографические ссылки

1. Bernstein D., Lange T. Post-quantum cryptography // Nature, № 549. 2017. P. 188–194. URL: https://doi.org/10.1038/nature23461.
2. Шенец Н.Н. Многомерное модулярное разделение информации // Информатика. 2007. № 4(16). С. 125–132.
3. Steinfeld R., Pieprzyk J. and Wang H.. Lattice-Based Threshold Changeability for Standard Shamir Secret-Sharing Schemes // IEEE Transactions on Information Theory, vol. 53, no. 7, p. 2542-2559, July 2007, doi: 10.1109/TIT.2007.899541.
4. Касселс Дж.В.С. Введение в геометрию чисел. М.: Мир, 1965. 421 с.
5. Asmuth C.A., Bloom J. A modular approach to key safeguarding // IEEE Trans. on inf. theory. 1983. Vol.29. P. 156–169.
6. Galibus T, Matveev G. Generalized Mignotte's Sequences Over Polynomial Rings Electronic Notes // Theoretical Computer Science. 2007. Vol. 186. P. 43–48. DOI: 10.1016/j.entcs.2006.12.044.
7. Galibus T, Matveev G, Shenets N. Some structural and security properties of the modular secret sharing. In: Symbolic and Numeric Algorithms for Scientific Computing, 2008. SYNASC 2008. // Los Alamitos: IEEE Computer Society Press. 2009. P. 197–200. DOI: 10.1109/SYNASC.2008.14.