ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 4
2016

А. В. Трепачева (Ростов-на-Дону, ЮФУ). **Криптоанализ полностью гомоморфных криптосистем, основанных на алгебре октонионов.**

Проблеме построения полностью гомоморфного криптосистем (ПГК) посвящено большое количество статей [1], в связи с их большой практической и теоретической актуальностью. Недавно появилось направление исследований [2-3], посвященное ПГК на основе октонионов. В данной работе проводится анализ криптостойкости ПГК [2] против атаки по известным открытым текстам (АИОТ) и атаки по шифртекстам (АШ).

Октонион — это вектор $\mathbf{a} = [a_0, \dots, a_7] \in \mathbb{Z}_n^8$ (в данном случае над кольцом вычетов по модулю n). Для $\mathbf{a} \in \mathbb{Z}_n^8$ определяется ассоциированная матрица $\mathbf{A_a} \in \mathbb{Z}_n^{8\times 8}$, элементы которой равны различным a_i, иногда взятым с обратным знаком [4]. Для октонионов $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_n^8$ их сумма — $[a_0+b_0, \dots, a_7+b_7]$, а произведение — $\mathbf{b}\cdot\mathbf{A_a}$. Норма $\mathbf{a}$ — $||a|| = \sqrt{a_0^2 + \dots + a_7^2}$. Существуют такие $\mathbf{a}$, что можно определить обратный по умножению элемент $\mathbf{a}^{-1}$, нейтральный элемент при этом — $\mathbf{1} = [1, 0, \dots, 0] \in \mathbb{Z}_n^8$. Октонионы образуют нормированную неассоциативную и некоммутативную алгебру деления [5].

Кратко опишем ПГК [2]. Задан RSA-модуль $n = pq \in \mathbb{N}$, $\log(p), \log(q) \geqslant 512$. Открытый текст $m \in \mathbb{Z}_p$ отображается в $\mathbf{m} = m\mathbf{1} + r\mathbf{z} \in \mathbb{Z}_n^8$, $r \in \mathbb{Z}_n$, $\mathbf{z} \in \mathbb{Z}_n^8$ — случайные, $||\mathbf{z}|| = 0$, $z_0 \neq 0$. Шифртекст m — это $\mathbf{c}_m(\mathbf{x}) \in (\mathbb{Z}_n[\mathbf{x}])^8$, $\mathbf{x} = (x_0, \dots, x_7) \in \mathbb{Z}_n^8$ — переменная. Выполняется

$$\mathbf{c}_m(\mathbf{x}) = \mathbf{k}_0(\cdots(\mathbf{k}_{t-1}(\mathbf{m}(\mathbf{k}_{t-1}^{-1}(\cdots(\mathbf{k}_0^{-1}\mathbf{x})\cdots))))\cdots), \tag{1}$$

где $\mathbf{k}_0, \dots, \mathbf{k}_{t-1}\mathbb{Z}_n^8$ — обратимые октонионы, образующие секретный ключ. Пусть $g_0(x) = \mathbf{k}_{t-1}^{-1}(\cdots(\mathbf{k}_0^{-1}\cdot\mathbf{x})\cdots)$, $g_1(x) = \mathbf{k}_0\cdots(\mathbf{k}_{t-1}\cdot\mathbf{x})\cdots)$. Тогда при расшифровании сначала вычисляется $\mathbf{m} = g_0(c_m(g_1(\mathbf{1})))$, а затем извлекается m. В [2] вводятся операции $+, \cdot$ на шифртекстах — $\mathbf{c}_{m_0+m_1}(\mathbf{x}) = \mathbf{c}_{m_0}(\mathbf{x}) + \mathbf{c}_{m_1}(\mathbf{x})$, $\mathbf{c}_{m_0\cdot m_1}(\mathbf{x}) = \mathbf{c}_{m_0}(\mathbf{c}_{m_1}(\mathbf{x}))$, которые соответствуют $+, \cdot$ открытых текстов. В силу этого криптосистема становится ПГК. В [2] приводится некоторое обоснование криптостойкости данной ПГК, однако оно не является достаточно полным и строгим.

В работе [4] было предложено преобразование ПГК [2], которое сводит работу с октонионами к работе с матрицами. А именно, секретный ключ ПГК [2] однозначно отображается в 8×8 матрицу $\mathbf{K} \in \mathsf{M}_8(\mathbb{Z}_n)$. Шифровка $m \in \mathbb{Z}_p$ отображается в шифртекст вида $\mathbf{C_m} = \mathbf{K}^{-1}\cdot\mathbf{A_m}\cdot\mathbf{K} \in \mathsf{M}_8(\mathbb{Z}_n)$, где $\mathbf{A_m}$ — ассоциированная матрица для октониона $\mathbf{m} = m\mathbf{1} + r\mathbf{z}$. Расшифрование теперь вычисляется по формуле $\mathbf{A_m} = \mathbf{K}\cdot\mathbf{C_m}\cdot\mathbf{K}^{-1}$ и далее извлекается m. Сложение и умножение шифртекстов — теперь обычное сложение и умножение матриц.

Соответствие между шифртекстами-октонионами и шифртекстами-матрицами следующее: элемент $c_{i,j}$ матрицы $\mathbf{C_m}$ соответствует коэффициенту при переменной x_i в j-м элементе октониона $\mathbf{c}_m(\mathbf{x})$.

Основной результат данной работы — АИОТ и АШ на ПГК [2], использующие преобразование из [4], описанное выше.

Теорема 1. *ПГК* [2] *являются нестойкой к АИОТ.*

Д о к а з а т е л ь с т в о. Пусть известный открытый текст m соответствует шифртексту $\mathbf{C_m}$. Положим $\mathbf{C_0} = \mathbf{C_m} - \mathbf{I} \cdot m$ ($\mathbf{I}$ — единичная матрица).

Для дешифрования шифртекста $\mathbf{C} \in \mathsf{M}_8(\mathbb{Z}_n)$ домножаем матрицу $\mathbf{C_0}$ на такое число, чтобы все элементы, кроме диагонального, были идентичны матрице $\mathbf{C}$, а затем вычитаем получившуюся матрицу из матрицы $\mathbf{C}$. В полученной диагональной матрице на диагонали будет стоять искомый открытый текст. ■

Также при наличии достаточно большого числа шифртекстов возможна эффективная АШ. Возможны две стратегии такой атаки:

- Легко заметить, что в ПГК [2] при открытом тексте $m = 0$ шифртекст $\mathbf{c}_0(x) = \mathbf{c}_{r\mathbf{z}}(x)$ таков, что $||\mathbf{c}_{r\mathbf{z}}(\mathbf{1})|| = 0$. Это наводит на мысль о следующей стратегии атаки: вычитаем друг из друга матрицы шифртекстов и проверяем норму матрицы-разности. Если она равна нулю, то считаем найденным шифртекст нуля и сводим к задаче криптоанализа с известным открытым текстом.
- Имеющиеся шифртексты вычитаем попарно один из другого. Получаем набор матриц, среди которых ищем подобные (т. е. получающиеся одна из другой умножением на константу). Найдя такие матрицы, считаем что они являются шифртекстами нуля и снова используем далее атаку с известным открытым текстом.

Теорема 2. *При наличии последовательности из w шифртекстов ПГК* [2] *можно взломать с вероятностью* $1 - (1 - p_{m'})^w - w \cdot (1 - p_{m'})^{w-1}$, *где* $p_{m'}$ — *вероятность появления наиболее часто встречающегося открытого текста* (*в соответствии с вероятностным распределением на множестве открытых текстов*).

Доказательство этой теоремы опирается на лемму 1 из [6]. В [6] так же показано, что при Гауссовом распределении вероятностей с небольшой дисперсией на множестве открытых текстов вероятность успеха данной АШ достаточно велика.

Работа выполнена при финансовой поддержке гранта РФФИ № 15-07-00597 а.

СПИСОК ЛИТЕРАТУРЫ

1. *Бабенко Л. К., Буртыка Ф. Б., Макаревич О. Б., Трепачева А. В.,* Полностью гомоморфное шифрование (обзор). — Вопросы защиты информации, 2015, № 3, с. 3–26.
2. *Yagisawa M.* Improved fully homomorphic encryption with composite number modulus.
3. *Wang Y.* Octonion algebra and noise-free fully homomorphic encryption (fhe) schemes. arXiv preprint arXiv:1601.06744, 2016.
4. *Wang Y.* Notes on two fully homomorphic encryption schemes without bootstrapping. Technical report.
5. *Baez J.* The octonions. Bulletin of the American Mathematical Society, 2002, 39(2), с. 145–205.
6. *Трепачева А. В.* Атака по шифртекстам на одну линейную полностью гомоморфную криптосистему. — Прикладная дискретная математика. Приложение. 2015, № 8, с. 75–78.