Секция «Дискретная математика и математическая кибернетика»

Криптоанализ полностью гомоморфного шифра, основанного на алгебре октонионов

Викторовна Алина Трепачева

Аспирант

Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Кафедра безопасности информационных технологий, Ростов-на-Дону, Россия

E-mail: alina1989malina@ya.ru

Полностью гомоморфные криптосистемы (ПГК) могут позволить решить много проблем компьютерной безопасности. Однако, большинство известных на данный момент ПГК (см. [1,2]) неэффективны, и исследователи предлагают все новые варианты.

В частности, в [3] была предложена ПГК, конструкция которой основана на неассоциативной алгебре октонионов.

В данной работе проведен анализ стойкости ПГК [3] к атаке по известным открытым текстам (АИОТ). Пусть даны пары (открытый текст, шифртекст) – $(m_l, \mathbf{c}_{m_l}(\mathbf{x})), l = \overline{1,t}$, сделанные на одном ключе. Тогда относительно ключа можно составить полиномиальную систему уравнений от многих переменных над $\mathbb{Z}_n$.

$$\left\{F_{i,j,l}(\mathbf{a}_1, ..., \mathbf{a}_k, \mathbf{z}_1, ..., \mathbf{z}_k, \mathbf{r}_1, ..., \mathbf{r}_s) = e_{i,j,l}, i = \overline{0,7}, j = \overline{0,7}, l = \overline{1,t} \right. \quad (1)$$

В данной работе проведено исследование возможности решить (2) с помощью вычисления базиса Гребнера [4] и методов линеаризации и XL. Дана оценка общего числа мономов в (2) и классифицированы виды этих мономов. Также даны общие асимптотические оценки сложности операции умножения шифртекстов (в [3] это сделано только для конкретных численных значений k, s). Асимптотика сложности умножения сравнивается со сложностью решения (2) и на основании этого будут сделаны выводы о том пригодна ли ПГК [3] для практики, и если да, то при каких значениях k, s.

Источники и литература

1) Guellier, A. Can Homomorphic Cryptography ensure Privacy? // PhD thesis, Inria. IRISA. Supelec Rennes, equipe Cidre. Universite de Rennes 1, 2014.

2) Gentry, C. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.

3) Kapur, D., Cai,Y. An algorithm for computing a Gröbner basis of a polynomial ideal over a ring with zero divisors // Mathematics in Computer Science. – 2009. – Т. 2. – №. 4. – С. 601-634.

Слова благодарности

Работа поддержана грантом РФФИ 15-07-00597 А