The computer simulation of attacks on the ring-homomorphic encryption

A. V. Trepacheva[1] (Rostov-on-Don, Southern Federal University)
alina1989malina@yandex.ru

The ring-homomorphic encryption allows computing on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The plaintexts are from some algebraic ring.

Thus, for ring-homomorphic encryption the following system of equation must holds:

$$\begin{aligned} D(E(m_1) \oplus E(m_2)) &= m_1 + m_2 \qquad (1) \\ D(E(m_1) \odot E(m_2)) &= m_1 \cdot m_2 \end{aligned}$$

where $m_1, m_2 \in \mathcal{M}$ are some plaintexts (from plaintexts ring $\mathcal{M}$), D and E are decryption and encryption functions, respectively.

The system of equations imposes strict security requirements on encryption. In particular, such classical attacks as the known-plaintext attack, the ciphertext-only attack, and the chosen-plaintext attack must be reviewed in ring-homomorphic context.

This work proposes the mathematical model, allowing to analyze the ability to construct secure ring-homomorphic encryption. The model consists of algebraic structures, connected by relations deduced from (1). And finally, simulation attacks on toy-sizes encryptions allow evaluating the number of operations for secret key recovery in comparison with number of operations for encryption, decryption and homomorphic computations.

[1]The work is supported by Russian Ministry of Education and Science according to the project No. 2.6264.2017/8.9