INVESTIGATION AND COMPARATIVE ANALYSIS OF FULEECA AND BISCUIT POST-QUANTUM DIGITAL SIGNATURE ALGORITHMS

Telnova A.A., Hrinenko T.O.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
Nariezhnii O.P.
V. N. Karazin Kharkiv National University, Kharkiv, Ukraine

The first quantum processors began to appear in the early 2000s, and their development has not stopped since then. The development of quantum processors raises the issue of developing cryptographic algorithms whose stability will remain satisfactory even after the creation of quantum computers whose power will be sufficient to pose a threat to all modern cryptography.

Among others, this issue is being studied by the NIST organization – the National Institute of Standards and Technology. Thus, in response to the significant development and progress of quantum computing, in December 2016, NIST published a public call for applications for participation in the Post-quantum cryptography standardization process to select quantum-resistant cryptographic algorithms [1].

The purpose of the work is to study and analysis the FuLeeca and Biscuit algorithms that participate in the NIST competition to determine their ability to ensure the security of electronic signatures in the post-quantum period, to assess their effectiveness and practicality of implementation in various systems, and to identify possible areas for improving these algorithms.

The paper discusses the basics of FuLeeca and Biscuit algorithms, including quasi-cyclic Lie codes and multidimensional computation; analyses the speed of key generation, signature, and signature verification for both algorithms; estimates the computing resource requirements and implementation efficiency; assesses the resistance of the algorithms to classical and quantum attacks; and identifies the advantages and disadvantages of each algorithm in the context of modern threats. As a result of the study, the FuLeeca and Biscuit algorithms were compared by various criteria.

The data show that FuLeeca demonstrates high speed and efficiency and ease of implementation. Biscuit provides high resistance to quantum attacks due to its utilization, but requires more computing resources. Therefore, FuLeeca is suitable for applications that require high performance and speed of key and signature generation, but can reduce security requirements. Biscuit is recommended for critical applications with high security requirements where the main factor is resistance to quantum attacks, such as in government and military systems.

References

1. Additional PQC Digital Signature Candidates Announced | Computer Security Resource Center. URL: https://csrc.nist.gov/news/2023/additional-pqc-digital-signature-candidates (date of access: 25.05.2024).