COMPARATIVE CHARACTERISTICS OF WAVE AND RYDE IN THE TERMS OF SECURITY AND PERFORMANCE

Telnova A.A., Hrinenko T.O.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The development of quantum computers threatens modern cryptographic algorithms. Post-quantum digital signature (PQDS) algorithms have been developed to provide cryptographic security in the face of quantum computers that can break traditional cryptographic algorithms. In 2022, the National Institute of Standards and Technology launched an additional selection stage for PQDS standardization, choosing 40 candidates. This paper discusses algorithms based on common classes of PQDS problems, including code-based cryptosystems and multi-party computing (MPC) protocols.

The purpose of this paper is to study and compare code-based and MPC signatures on the example of WAVE and RYDE digital signatures, which will serve as a basis for further analysis of these digital signature mechanisms.

The paper presents the results of a comparative analysis of the WAVE and RYDE algorithms in terms of their foundations, performance and data size, and algorithmic resistance to attacks. In particular, it was found that the WAVE algorithm is based on lattice theory and uses a noise coding method to protect against attacks [1], while the RYDE algorithm is based on error-corrected codes [2] and offers a compromise between security and performance. The performance of both algorithms was also investigated in the context of key generation and signature creation and verification, where RYDE had smaller key and signature sizes and faster key generation compared to WAVE, but WAVE provided a higher level of security. Both algorithms demonstrated high resistance to classical and quantum attacks. However, WAVE is better protected against denial-of-service (DoS) attacks, while RYDE is optimized for running on devices with limited resources.

The results of the study show that WAVE is a promising solution for highly secure systems such as government and military applications. RYDE, in turn, is more optimal for commercial applications that require speed and efficient use of resources.

References

1. Gustavo Banegas, Kévin Carrier, André Chailloux, Alain Couvreur, Thomas Debris-Alazard, Philippe Gaborit, Pierre Karpman, Johanna Loyer, Ruben Niederhagen, Nicolas Sendrier, Benjamin Smith, Jean-Pierre Tillich. WAVE Specification Document. 2023. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/wave-spec-web.pdf.

2. Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Matthieu Rivain, Jean-Pierre Tillich, Adrien Vinçotte. RYDE Specification Document. 2023. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ryde-spec-web.pdf