Contribution ID: **34** Type: **not specified**

Quantum Enhancement of Cryptography

Quantum computers promise to revolutionize several fields, including cryptography. In recent years, researchers have made significant progress in developing quantum algorithms that can solve computational problems much faster than classical computers. These advances have led to concerns about the security of traditional cryptography algorithms, as they may be vulnerable to quantum attacks. In this article, we provide a comprehensive overview of the quantum enhancement of cryptography algorithms and examine the impact of quantum computing on various encryption and decryption schemes, including RSA, AES and Elliptic Curve Cryptography (ECC). We also discuss efforts to develop post-quantum cryptography and provide an outlook on the future of the field. The article concludes with an insight into the importance of preparing for the advent of quantum computing in cryptography and the need for continued research and development in this area.

Primary author: WYROSTKIEWICZ, Michał (Warsaw University of Technology)

Co-author: GAŁCZYŃSKA, Barbara

Presenters: GAŁCZYŃSKA, Barbara; WYROSTKIEWICZ, Michał (Warsaw University of Technology)

Session Classification: Session B (Poster)