Секція 1

MODERN APPROACHES TO SOLVING THE PROBLEMS OF POST-QUANTUM CRYPTOGRAPHY

Serhii Butenko
National Aerospace University «Kharkiv Aviation Institute»
Research adviser: Vladimir Pevnev
Language adviser: Iryna Shulga

Actuality. Today, a large number of corporations and governments consider quantum computers and related quantum computing to be one of the most promising areas for fundamental research. The development of these technologies may pose a threat of compromising all widely used cryptographic algorithms. For this reason, the study of the impact of quantum computing on modern and promising crypto algorithms is a priority task [1].

The purpose is to study the impact of quantum computing on modern crypto algorithms. Identify opportunities to improve crypto algorithms to minimize and/or eliminate the likelihood of their possible compromise. Investigate promising crypto algorithms created to solve the problems of post-quantum cryptography.

Main points. When researching the impact of advanced quantum computers on modern cryptographic systems the primary task is to determine their potential computing capabilities. Today cryptography researchers most often assume that large-scale quantum computers will allow compromising all modern crypto algorithms in a relatively short period of time. In this case, symmetric encryption algorithms with a key length of 256 bits and asymmetric algorithms with a key length of 2048 bits (for the RSA algorithm) and 256 bits (for the ECC algorithm) are considered as modern. Also, modern crypto algorithms include hashing algorithms with length of output sequence equal to 256-bit [2].

In the process of improving existing encryption and hashing algorithms the main approach is to increase the key length for encryption algorithms and the length of the output sequence for hashing algorithms respectively. According to the conclusions of most researchers the minimum permissible key length should be 512 bits. This will ensure the crypto resistance of these algorithms in the near future [3].

In the case of the asymmetric encryption algorithms researchers' opinions differ. In the analyzed scientific papers the researchers propose increasing the key length similarly to symmetric algorithms. But some researchers believe that increasing the key length will lead to a significant decrease in performance making them irrelevant [3].

The most authoritative report in this area is the NIST report. According to this report increasing the key length for symmetric encryption algorithms is

proposed. A similar approach for hashing algorithms is used (increasing the length of the output sequence). In the case of modern asymmetric algorithms their using is considered inappropriate [4].

Another approach is to create new algorithms. The main goal in this case is to increase the complexity of the brute-force search problem. The complexity of solving these problems allows to ensure the required level of crypto resistance [5].

Conclusions. Most researchers today identify large-scale quantum computers as a significant threat to the compromise of modern crypto algorithms. According to the study modern versions of crypto algorithms should be considered potentially vulnerable if a large-scale quantum computer with a significant number of qubits is created. Based on these modern symmetric crypto algorithms require increasing key length which will ensure an appropriate level of cryptographic resistance. In the case of asymmetric encryption algorithms a replacement according to the requirements for post-quantum cryptography will need to be created.

List of references

1. A Survey about Post Quantum Cryptography Methods / J. R. J. EAI Endorsed Transactions on Internet of Things. 2024. Volume 10. DOI: 4108/eetiot.5099.
2. Pinto J. Post-Quantum Cryptography. ARIS2 - Advanced Research on Information Systems Security. 2022. Volume 2(2). Page 4–16. DOI: 10.56394/aris2.v2i2.17.
3. Post-Quantum Cryptography trends and perspectives. European Scientific e-Journal. 2021. DOI: 10.47451/inn2024-03-01.
4. Chen L., Stephen J. Report on Post-Quantum Cryptography. 15 p. DOI: 10.6028/NIST.IR.8105.
5. Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations / R. Bavdekar. 2023 International Conference on Information Networking (ICOIN). Thailand. 2023. DOI: 10.1109/icoin56518.2023.10048976.

Author Information

Serhii Butenko, a PhD student from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», s.butenko@student.csn.khai.edu
Vladimir Pevnev, Dr. Sc., professor from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», v.pevnev@csn.khai.edu
Iryna Shulga, PhD of Pedagogic Sciences, associate professor, Head of the Department of Foreign Languages, National Aerospace University «Kharkiv Aviation Institute», i.shulga@khai.edu