Post Quantum Cryptography
Impact to the public key cryptography

Juha Luukkanen
juha.luukkanen@insta.fi

The questions that concern the researcher are:

1. How does a quantum computer break public key cryptography?
2. Who will develop the first quantum computer powerful enough to break public key cryptography, and what is the motivation for development?
3. When will the first quantum computer that threatens public key cryptography become a reality?
4. What are the methods to protect public key cryptography against the threat posed by quantum computers?

The nature of the study is thus descriptive, and a qualitative research approach was chosen as the research approach.

The interviews used in this qualitative study were conducted as a semi-structured interview in which the researcher formulates thematic questions based on research questions and research themes.

CONCLUSIONS

The first conclusion of this study is that it is very likely that breaking public key cryptography in the future will be done using Shor's algorithm with either an ion trap or a superconducting quantum computer. Shor's algorithm requires 4099 logical qubits to crack the most commonly used 2048-bit RSA key. Error correction may require hundreds of qubits to implement a single logical qubit, which could result in a large total number of physical qubits required to break the RSA key. It is estimated that it would take around 20 million qubits to decrypt 2048-bit encryption.

The second conclusion of the study is that the first quantum computers that threaten the security of a public key are likely to be developed by a well-known player with sufficient resources and already involved in the development process. However, the primary motivation for developing a quantum computer is not to break the encryption of the public key, but other use cases. The first efficient general-purpose quantum machine is more likely to be developed by a company, a university, or a joint project between them than by a governmental actor. It is possible that the principle of a scalable quantum computer will be developed by a university and a larger player with sufficient resources will develop a more powerful quantum computer capable of challenging even public key cryptography.

Quantum computing is expected to continue to develop rapidly in the future. The third conclusion of the study is that a quantum computer capable of cracking the 2048-bit RSA key will be implemented in about 15 years. Implementation may be faster than estimated due to the exponential acceleration of quantum computing. The quantum computer that threatens public key cryptography is expected to become a reality in the 2030s or early 2040s.

The fourth conclusion of the study is that the best way to protect public key cryptography against the threat of a quantum computer is through developing quantum secure protocols. The most vulnerable to the threat posed by a quantum computer is high-security communication over a medium where someone can intercept and record the communication. Information that is wanted to be kept encrypted for long periods of time is also at risk. Preparing for the threat of quantum computing to public key cryptography solutions should be started well in advance. The threat to public key cryptography posed by quantum computers is real, but it can be protected against.

DISCUSSION

The first research question is how a quantum computer breaks public key cryptography. It is very likely that breaking public key cryptography with a quantum computer will succeed in the future. This conclusion is supported by the fact that all informants interviewed for the study believe that an efficient error-corrected general-purpose quantum computer is feasible. A number of different players already have functional quantum computers. Today's universal quantum computers are small, about 15-130 qubits, and do not yet pose a threat to the security of the RSA key. Annealing Quantum processor-based computers have already been presented with implementations of 5760 qubits, but they are not general-purpose and are most effective in optimisation problems and thus do not threaten public key cryptography. Breaking a 2048-bit RSA key using Shor's algorithm requires a general-purpose quantum computer with about 4000 error-corrected logical qubits.

The answer to the second research question, who will develop the first quantum computer powerful enough to break public key cryptography, and what is the motivation for development, is a little more complex. The question may seem irrelevant, what does it matter who develops the quantum computer? When the question is put in the context of the research, the threat posed by the quantum computer to public key cryptography, it is understood that it affects the visibility of progress in development. The progress of public research projects can be monitored, and it is possible to know in advance when they will start to threaten the encryption of the public key. There is no visibility of the progress of secret projects, and there is no way of knowing for sure whether an actor is already in possession of an advanced quantum computer today.

Informants did not see breaking public key cryptography as the primary motivation for developing a quantum computer but were thought to be motivated by general interest, such as quantum chemistry, pharmaceutical research, artificial intelligence and machine learning. However, it is true that the ability of a quantum computer to break public key cryptography will be of interest to many actors who will use a generic quantum computer when its capability reaches a sufficient level.

It is difficult to predict the exact timing of the implementation of a quantum computer that breaks the encryption of the public key. The answer to the third research question, when a quantum computer breaks the public key cryptography, is that a quantum computer capable of cracking a 2048-bit RSA key will be implemented in about 15 years. The informants interviewed for the study expect the quantum computer to become a reality within 10-20 years. In previous studies, such as the quantum threat timeline report 2020, the majority of respondents predict that a quantum computer will be capable to factor 2048 bits of the RSA key in about 20 years.

Quantum machine manufacturers have presented schedules in which the number of qubits in quantum computers will increase rapidly in the future. The rapid development of quantum computing is justified by doubly exponential rate of development due to its quantum nature. The study identified noise reduction and error correction as the main challenges in quantum computing development. It is possible that the development of a quantum computer will slow down due to some fundamental problem.

The answer to the last research question, what are the methods to protect public key cryptography against the threat posed by quantum computers, is that the best way to protect public key cryptography against the threat of a quantum computer is through developing quantum-safe protocols. But developing protocols alone is not enough: it is needed to start preparing for quantum threats early enough. The threat posed by a quantum computer against public key cryptography should be assessed using a threat assessment method and the best protection chosen on a case-by-case basis. Based on research interviews, the threat posed by a quantum computer is not considered intolerable because the development of quantum-safe algorithms is well under way. The NIST PQC competition standard draft release is expected to take place between 2022 and 2024. It has been suggested that one should wait for the announcement of the winner of the competition before starting to implement the algorithms. Two of the interviewees see no obstacle to starting to implement the algorithms proposed in the competition if the implementer has sufficient understanding and know-how. The operating principles of PQC algorithms differ from the traditional algorithms currently in use. The requirements of the new algorithms shall be carefully implemented. The informant interviewed for the study raised the risk that at least at the beginning there may be errors in the implementation of algorithms that compromise data security. Experts suggest that hybrid algorithms, which use both the traditional and PQC algorithms together, are a viable option for the transition period.

BUSINESS FINLAND
INSTA
jamk | University of Applied Sciences