Slovak University of Technology in Bratislava
Faculty of Electrical Engineering and Information Technology

Ing. Peter Špaček

Post-Quantum key establishment

Dissertation Thesis Abstract

to obtain the Academic Title of **"philosophiae doctor"**
abbreviated as **"PhD."**

in the doctorate degree study programme:	**9.2.9 Applied Informatics**
in the field of study:	**Applied Informatics**
Form of Study:	**full-time study**

Place and Date: **Bratislava, 6. 7. 2022**

Dissertation Thesis has been prepared at:

Institute of Computer Science and Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava

Submitter: **Ing. Peter Špaček**

Faculty of Electrical Engineering and Information Technology
Slovak University of Technology in Bratislava
Ilkovičova 3, 812 19 Bratislava

Supervisor: **prof. Ing. Pavol Zajac, PhD.**

Faculty of Electrical Engineering and Information Technology
Slovak University of Technology in Bratislava

Readers: **Mgr. Marek Sýs, PhD.**

Katedra počítačových systémů a komunikací
Masarykova univerzita, Brno

Prof. Maria Isabel González Vasco

Área de Matemática Aplicada – MACIMTE
Uviersidad Rey Juan Carlos, Madrid

Dissertation Thesis Abstract was sent: ....
Dissertation Thesis Defence will be held on: .... at .... at

Faculty of Electrical Engineering and Information Technology,
Slovak University of Technology in Bratislava,
Ilkovičova 3, 812 19 Bratislava,
in room C502

prof. Dr. Ing. Miloš Oravec
Dean of the Faculty of Electrical Engineering and Information Technology,
Slovak University of Technology in Bratislava

Contents

1 Introduction

The motivation for this research is a significant progress in the research in the quantum technologies field in the last years [1], [2], [3], [4]. Quantum computer poses a threat for security of communication, as the security mechanisms rely on the fact that an effective way of solving mathematical problems used in public-key encryption is not known. There are two algorithms designed for quantum computers that are relevant in this context:

1. **Shor's algorithm**, published in 1994 by Peter Shor [5], is a quantum computer algorithm for prime factorization and discrete logarithms in polynomial time.
2. Lov Grover published a database search algorithm in 1996 [6]. One interesting consequence is that **Grover's algorithm** is able to find the n-bit key with complexity $\sqrt{2^n}$ iterations [7]. Note, that a conventional computer would need 2^{n-1} iteration to find the same key.

Most used public-key algorithms for key exchange or digital signatures are vulnerable to quantum machines [8], [9]. Based on the integer factorization problem, the RSA cipher is the apparent victim of Shor's algorithm. Other commonly used public ciphers, Diffie-Hellman or its variant based on the elliptic curves over finite fields (ECDH). As mentioned in [10], Shor's algorithm can also be used for computing discrete logarithms. And because solving Diffie-Hellman problem can be achieved by solving discrete logarithms [11], Diffie-Hellman is also not suitable for post-quantum usage. Proos and Zalka [12] have shown that breaking cryptography based on elliptic curves is more straightforward than breaking RSA.

Symmetric ciphers are not entirely broken with Grover's algorithm. But the square root speed up of brute-force attacks requires changing what is considered "secure". The Advanced Encryption Standard *(AES)* [**aes**] is widely used for providing data confidentiality. With Grover's algorithm in mind, the security level of *AES-128* is lowered to 64-bit ($\sqrt{2^{128}} = 2^{64}$). That means that AES settings with 128 bits or lower key length will no longer be secure, and AES needs to be used with 192 or 256 bits for key sizes [13].

Applying Grover's algorithm on DES, however, brings its 56-bit security to only 185 iterations. 3DES is also not secure enough for the quantum world. Its 112-bit key is lowered to 56-bit security, and that is not considered secure [14].

Hash functions suffers from the same consequences from a quantum computer as symmetric cryptography. Grover's algorithm can be used to find a collision using square root speedup. Brassard et al.[15] showed that by creating a table of size $\sqrt[3]{2^n}$ together with using Grover's algorithm, he can reduce the security level of hash functions three times. That means that for hash functions we need at least 224-bit variants.

The aim of our research project in the field of secure post-quantum cryptography is to research the ways to design a protocol, which could replace the currently used TLS protocol, but would be resistant to quantum computer attacks. At the same time, the increasing use of IoT devices must be considered. In the thesis, we look for suitable algorithms for such devices, and modify the TLS Handshake protocol to be more efficient for limited devices. A crucial part of system security is operational security. Therefore, we need to focus on different mechanisms to secure the operational security, using the Trusted Execution Environment (TEE), and with methods for protection against side-channel attacks. If TEE is used for critical operations in post-quantum TLS protocol, the key management and the other consequences must also be taken into account.

2 Research objectives

We can identify several objectives connected to the aim of our work. These are subgoals we will follow when elaborating this research work:

- We need to review the details of the TLS protocol, its mechanisms, and the structure of its messages. We will identify aspects that can be reused and aspects that need to be replaced.
- We will search for possible replacement mechanisms for key exchange that should resist quantum computers.
- We will collect suitable TLS implementations for our experiments and choose the best one for the practical aspect of our research.
- We will design and implement a post-quantum key exchange mechanism in the TLS context.
- In designing a new TLS-like protocol, we will consider the growing world of IoT devices. This should be projected into key exchange choices, as well as the architecture of the new protocol.
- We will find available methods for ensuring operational security and implement the chosen solution.
- We will test our solution with a set of experiments to find whether our solution is suitable for use in practice.

As we see from the objectives, a few important questions have emerged. First is the question of operational security. We need to consider not only the cryptoanalysts breaking ciphers, but also the "line of least resistance" attackers. This includes malware obtaining secret keys, monitoring cryptographic operations to leak some side-channel information, etc.

Quantum-secure algorithms themselves require more memory space, more computational power, or/and more time. Symmetric cryptography needs longer keys and blocks, public-key cryptography needs to be changed completely, and may have different challenges, e.g. enc/dec time ratio. Also, changes are required on the protocol level to achieve our goal. This may result in a delays in communication establishment, a need for memory space for the keys, and overall delays in communication. So, another important aspect is the trade-off or the "cost" of post-quantum secure TLS protocol.

3 Overview of the thesis

The first chapter presents the preliminaries. We describe post-quantum security, we review the details of the TLS protocol, its mechanisms, and the structure of its messages. We present operational security and similar research. We describe TLS implementations. We found possible replacement mechanisms for key exchange that should resist quantum computers in the NIST post-quantum standardization process and explained related concepts.

The post-quantum level of security in TLS requires design changes. We present those changes in the second chapter, together with possible candidates for key exchange algorithms. We identify parts of TLS that can be reused and parts that need to be replaced. We also consider limited devices and the growing world of IoT. We introduce SEcube and our concept of post-quantum HSM to provide a higher level of operational security. Also, we add an option to use of protected implementation of Kyber.

We chose the s2n implementation of TLS and modify it to support our experiments. In the third chapter, we mention some of the implementation challenges that we encountered to explain the artifact of our design research. We also describe the building blocks and sources for the implementation of our study.

In the chapter four, we test and evaluate all components and steps of the post-quantum TLS key agreement process. We show the successful post-quantum decryption and key agreement on the host and HSM use. We also show successful symmetric cryptography use in TLS Record protocol after post-quantum key exchange.

4 Results and contribution of our research

Our hypotheses, which we defined in the first chapter, were successfully confirmed, and we created the proof of concept of post-quantum TLS. We used SEcube and implemented Hardware Security Module for post-quantum public key algorithms and used it in our post quantum TLS. We found that the use of such setting is possible, and we consider delays caused still in acceptable range.

We can conclude that we were able to finish our research with positive results. We showed that the use of post-quantum cryptography in the TLS setting is possible and practical in real-world use. We were able to speed up the handshake for limited devices with the possibility of client and server swapping roles in the key exchange. We designed, implemented, and tested the first post-quantum hardware security module with auspicious results. There are still many steps that need to be taken to bring post-quantum cryptography into practical use, and this work is one of the steps to get closer to the goal.

The main contribution of the work can be perceived from several points of view: The first point of view is a contribution for Transport Layer Security (TLS) protocol research. Our work brought a post-quantum mechanisms for exchanging keys into the environment of one of the most used communication protocols today. From this point of view, the work pushes the boundaries of the TLS protocol to meet the requirements of security in the post-quantum world.

Another point of view is the view from the development of Hardware Security Modules (HSMs). We designed and implemented an HSM module for post-quantum key exchange for TLS Handshake purposes. The module offers not only asymmetric cryptographic algorithms for key exchange, but also key management and their use in symmetric ciphers in a secure environment.

Last but not least, we can look at the contribution of the work from the perspective of IoT devices. We evaluated the possibilities of public key post-quantum algorithms for limited devices, we found out which algorithms can be used in such an environment and which cannot. We also proposed a way to modify the TLS protocol so that when using post-quantum asymmetric algorithms, the lightweight client does as little computation as possible.

Our research in this field has opened even more questions. There are several possible directions of the future research following this work:

- Authentication of both server and client can be added to our design. This can be done using post-quantum signatures or post-quantum KEM. The comparison of these two approaches under the same conditions would be interesting.

- More research in the protection of post-quantum algorithms from side-channel attacks is required. This is crucial for the integration of post-quantum algorithms into IoT devices.
- Some platforms (as SEcube) provide FPGA. It would be interesting to see hardware implementation of post-quantum algorithms PQcube system.
- Specification of several standards would need to be changed to allow post-quantum public-key cryptography. This includes recognizing post-quantum algorithms in Internet Assigned Numbers Authority (IANA), adapting protocols to allow key encapsulation mechanism API, etc.

Bibliography

1. 40 years of quantum computing. *Nature Reviews Physics*. 2022, vol. 4, no. 1, pp. 1–1. Available from DOI: `10.1038/s42254-021-00410-6`.
2. BALL, Philip. First quantum computer to pack 100 qubits enters crowded race. *Nature*. 2021, vol. 599, no. 7886, pp. 542–542. Available from DOI: `10.1038/d41586-021-03476-5`.
3. MORZHIN, O. V. and PECHEN', A. N. Maximization of the Uhlmann–Jozsa Fidelity for an Open Two-Level Quantum System with Coherent and Incoherent Controls. *Physics of Particles and Nuclei*. 2020, vol. 51, no. 4, pp. 464–469. Available from DOI: `10.1134/s1063779620040516`.
4. ARUTE, Frank et al. Quantum supremacy using a programmable superconducting processor. *Nature*. 2019, vol. 574, no. 7779, pp. 505–510. ISSN 1476-4687. Available from DOI: `10.1038/s41586-019-1666-5`.
5. SHOR, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*. 1995, no. 5, p. 1484.
6. GROVER, L.K. A fast quantum mechanical algorithm for database search, Proceedings. *28th Annual ACM Symposium on the Theory of Computing*. 1996, p. 212.
7. ARUNACHALAM, Srinivasan and WOLF, Ronald de. *Optimizing the Number of Gates in Quantum Search*. arXiv, 2015. Available from DOI: `10.48550/ARXIV.1512.07550`.
8. BUCHANAN, William and WOODWARD, Alan. Will quantum computers be the end of public key encryption? *Journal of Cyber Security Technology*. 2017, vol. 1, no. 1, pp. 1–22. Available from DOI: `10.1080/23742917.2016.1226650`.
9. MAVROEIDIS, Vasileios, VISHI, Kamer, ZYCH, Mateusz D and JØSANG, Audun. The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*. 2018.
10. EKERÅ, Martin and HÅSTAD, Johan. Quantum Algorithms for Computing Short Discrete Logarithms and Factoring RSA Integers. In: LANGE, Tanja and TAKAGI, Tsuyoshi (eds.). *Post-Quantum Cryptography*. Cham: Springer International Publishing, 2017, pp. 347–363. ISBN 978-3-319-59879-6.

11. MAURER, Ueli M. and WOLF, Stefan. The Relationship Between Breaking the Diffie–Hellman Protocol and Computing Discrete Logarithms. *SIAM Journal on Computing*. 1999, vol. 28, no. 5, pp. 1689–1721. Available from DOI: 10.1137/S0097539796302749.

12. PROOS, John and ZALKA, Christof. Shor's Discrete Logarithm Quantum Algorithmfor Elliptic Curves. 2003, vol. vol. 3, pp. 317–344.

13. GRASSL, Markus, LANGENBERG, Brandon, ROETTELER, Martin and STEINWANDT, Rainer. Applying Grover's algorithm to AES: quantum resource estimates. In: *Post-Quantum Cryptography*. 2016, pp. 29–43.

14. HIDARY, Jack D. A Brief History of Quantum Computing. In: *Quantum Computing: An Applied Approach*. Cham: Springer International Publishing, 2019, pp. 11–16. ISBN 978-3-030-23922-0. Available from DOI: 10.1007/978-3-030-23922-0_2.

15. BRASSARD, Gilles, HØYER, Peter and TAPP, Alain. Quantum cryptanalysis of hash and claw-free functions. In: LUCCHESI, Cláudio L. and MOURA, Arnaldo V. (eds.). *LATIN'98: Theoretical Informatics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 163–169. ISBN 978-3-540-69715-2.