Quantum-resistant digital signatures schemes for low-power IoT

1st Hannes Hattenbach
Computational Science
Freie Universität
Berlin, DE
hannes.hattenbach@fu-berlin.de

***Abstract*—**

***Index Terms*—Internet of Things, Quantum Resistance, Secure Signatures, Power Constraint Devices**

I. Introduction

The quantum revolution is coming. With quantum computers[1] on the way to get more and more functional, people are fearing a loss of their security and privacy. Or as [1] puts it, "principles of data integrity, message authentication, and nonrepudiation, are going to have profound aftermath on sensory data in terms of security and privacy." That is because there are algorithms based on Shors algorithm that can forge signatures and decrypt encrypted messages whos security is based on discrete logarithms, including elliptic curves or prime factoriztion, like our most common schemes ECDSA and RSA respectively are. The quantum computer only needs access to the public keys of these asymetric schemes. The expenditure to forge a signature[2] with classic[3] computers rises exponentially with increased key length, therefor beeing essentially unbreakable by classic computers. A sufficient quantum computer on the other hand can derive a private key from a public key in polynomial time, therefor rendering these schemes broken.

That is why there are currently schemes under standarization [2] that are based on other hard problems (not number theory) like so called lattice problems that cannot be that easily forged by quantum computers to save our privacy and security.

One of the use cases not directly comming to mind for the end user, but beeing as important non the less is signing sensitive sensor data in the Internet of Things (IoT). Another problem coming up in the IoT compared to end-user-devices like Laptops and Smartphones though is the severe ressource contraintness. The IoT consist of low power devices with wery few storage and computing power.

In this paper i am going to evaluate existing signature schemes and their usage possibilities for the IoT regarding their performance metrics.

Therefor i am going to give a small introduction and background to quantum computing, beeing a little more detailed about their ability to break current encryption and signature standards. In the next section i will give an overview over current candidates for Quantum Resistant (QR) Algorithms and giving performance metrics for those. The following chapter will then focus on signature schemes in the IoT, starting with additional performance metrics relevant in the IoT. With a little more details about two failed signature schmemes to highlight potetial pitfalls. And finally focussing on the best signature contender for the IoT so far: FALCON.

[1]compare section III-A

[2]that is considered secure under normal circumstances

[3]we refer to classic if something is not directly leveraging entanglement or superposition

II. Background

A. Cryptography

Loosely speaking the main topic of cryptography can be devided into three groups. The first of these groups is about one way functions, that shall not, as the name implies, be effeciently reverseable. If we create a smaller value of constant length from a bigger set of possibly variable length, we commonly refer to that as hashing. Cryptographic hashing is important for a variety of different applications like storing and matching passwords without the ability to infer any knowledge about that password. Hashing itself can be used for the next pillar of cryptography: signatures. Signature shemes are used to proof integrety or authenticity of any data. A signature scheme conisists of two parts, signing and verifying. The last group is encryption, which ensures privacy/confidentiality of any data, s.t. only the right entities can decrypt this data. These shemes consist of the two parts encryption and decryption. Additionally to those parts for signatures as well as encryption there needs to be process of key-generation. We also differentiate between symetric and asymetric schemes. The first one has a different private and public key while the latter uses the same for de- and encryption. More details about which of those schemes will be more or less endangered by quantum computing are in section III-A and III-B.

B. Internet of Things

The IoT consists of devices of all sorts, having in common, that they communicate with each other and the enviroment rather than directly with humans. Those devices range from automatic lights and smart home devices to tiny interconnected sensors in automatic fabrication. A common characteristic though is, that most of these devices have limited processing power, flash storage and random access memory (RAM). A

TABLE I
IETF IoT CLASSES

Class	RAM	Flash
C0	<< 10 KiB	<< 100 KiB
C1	10 KiB	100 KiB
C2	50 KiB	250 KiB

popular example for hobbiest IoT devices is the ESP32 from Espressif Microsystems. They offer multiple Modules with up to 240Mhz Clock on the 32 IC, up to 16MiB Flash Storage and 320KiB RAM. Which is more than other compareable devices but way less then a lower spec modern smartphone, with 10 times the frequency, 4GB of RAM and 64GB of storage.

Since the IoT consists of very different types of constrained nodes the IETF introduced different classes on which to classify IoT nodes, those can be seen in table II-B

III. QUANTUM RESISTANT SECURITY

A. Quantum Computing

In contrast to classical computers, where information is processed in discete states, a quantum computer leverages quantum mechanics to operate on so-called qubits - quantum objects that can be in superposition or entangled with each other. Opening a new kind of computing. One of the implications of that is, that it is now possible to factor large numbers in polynomial time using an algorithm deverloped by Shor [3]. This algorithm uses a so-called Quantum-Fourier-Transform (QFT) to (probablisticly) get the frequencys of which a given function output occurs. That can be used together with euclids algorithm of finding the greatest common devisor to derive the prime factors. Prior to to quantum computers this was considered a hard problem that could only be computed in exponential time and was therefor considered practically impossible and was used as the basis-problem for RSA encryption. Similar to that other common schemes like ECDSA can also be broken be slightly modidied versions of Shors Algorithm.

B. QR Algorithms

The two main algorithms with practical use cases that have a great speed-up compared to classical solutions, are the already introduced algorithm by Shor and an algorithm by Grover that can essentially reverses one-way functions by creating a superposition over all possible inputs, flipping all inputs with the wanted output (without knowing the inputs) and then flipping this state about its mean and repeating this process a lot of times [4]. While Shors algorithm provides exponential speed-up, Grovers algorithm only provides quadratic speed-up. It was also shown, that something similar to grovers algorithm but with exponential speedup is impossible [5]. Which implies that Hashing as well as symetric cryptography stays relatively secure. The quadratic speedup provided by quantum computers can easily be mitigated by doubling the key length. On the other hand though, classical asymetric cryptography is endangered by shors algorithm and quantum computers.

TABLE II
QR SECURITY CLASSES AND THEIR TRADITIONAL COUNTERPARTS AS CLASSIFIED BY THE NIST

Class	security compareable to
1	AES-128
2	SHA256
3	AES-192
4	SHA384
5	AES-256

But not all asymetric cryptography schemes are equally affected. There are different proposals, both for QR encryption and for QR signature schemes. They all do have in common though, that their security is not absolutely mathematically prooven, but based upon assumptions. We therefor need to consider a few measures that make schmemes more or less secure.

1) Performance Metrics: Some performance metrics exist in QR schemes as well as in classic schemes.

Keylength and key exchange message length [6] are the more obvious ones. The computing time also comes to mind as a performance metric. Here you need to differentiate between key generation, which is less important, since it should only occur rarely, and signing as well as signature verification [4].

Primarely in signatures another metric arises: how often can a private key be used before it needs to be switched out for another one, because the signature leaked information of the key. This is not particularly relevant in most cases, as methods can be used to create long term procedures from short term procedures (those where a key can rarely, if ever, be recycled). But it is relevant in the case of the IoT, since those methods require extra memory which is sparse in IoT-devices. Additionally they tend to make the signatures themself longer, which also is not preferrable in the IoT. [6]

Additionally to more tradidional performance metrics we somehow need to measure the security of given schmemes against an attack by a quantum computer. Sadly there is currently no standard benchmark to measure quantum resistance [7], nevertheless the NIST created a standard that describes how secure a scheme is against a quantum computer by classifiing it within 5 classes that can be determined with grovers algorithm [8], [9]. Those classes can be seen in table III-B1

2) Encryption:

3) Signatures:

IV. QR SIGNATURES IN IOT

1) Performance Metrics in IoT:

A. qTESLA

B. FALCON

V. CONCLUSION

REFERENCES

[1] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, “On the role of hash-based signatures in quantum-safe internet of things: Current solutions

[4] as well as its counterparts de- and encryption

and future directions," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 1–17, 2021.
[2] https://github.com/PQClean/PQClean.
[3] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999. [Online]. Available: https://doi.org/10.1137/S0036144598347011
[4] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, pp. 325–328, Jul 1997. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.79.325
[5] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997. [Online]. Available: https://doi.org/10.1137/S0097539796300933
[6] R. A. Perlner and D. A. Cooper, "Quantum resistant public key cryptography: A survey," in *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, ser. IDtrust '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 85–93. [Online]. Available: https://doi.org/10.1145/1527017.1527028
[7] T. M. Fernández-Caramés, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2020.
[8] A. Khalid, S. McCarthy, M. O'Neill, and W. Liu, "Lattice-based cryptography for iot in a quantum world: Are we ready?" in *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, 2019, pp. 194–199.
[9] M. J. O. Saarinen, "Mobile energy requirements of the upcoming nist post-quantum cryptography standards," in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2020, pp. 23–30.