Post Quantum Security

TENG LIANG YU BENJAMIN, GU BOYUAN, WAN FENG YAO, KOH HONG KAI, T GURU

Information Security, Singapore Institute of Technology
10 Dover Dr, Singapore 138683

2103201@sit.singaporetech.edu.sg, 2103210@sit.singaporetech.edu.sg, 2103199@sit.singaporetech.edu.sg, 2103209@sit.singaporetech.edu.sg, 2103202@sit.singaporetech.edu.sg

Abstract - **Security is essential in our devices today, for they contain much valuable data that we wish to keep private. This has become especially important in the age of quantum computing, where traditional protections may not hold. Post-Quantum Cryptography is one of the main defences against the hacking power of quantum computers, yet Quantum Cryptography devices are still vulnerable to physical attacks like Side-Channel Analysis. Specifically, this review looks at lattice-based cryptography and the hash-based system for Post-Quantum Cryptography, and power consumption, differential photonic emission, and acoustic side-channel attacks for Side-Channel Analysis.**

I. Introduction

Data has been used increasingly in every aspect of our lives, making us more comfortable and boosting our productivity. With the idea of making everything more suited to our personal needs, we have been using data about our behaviours in every aspect. These data, collected from our online surfing habits, purchase history, and other areas could be extremely personal. Businesses and us store this data in devices secured with complex cryptographical methods that we have our full trust in. Yet, in a world where quantum technology is developing increasingly rapidly, new quantum computers would be able to run Grover's and Shor's algorithms, compromising the security of traditional symmetric and public-key cryptography [1] as demonstrated by the proposed processor, "Sycamore" [2]. Thus, we must pay close attention to the field of post-quantum security to secure our data.

In general, ensuring post-quantum security comes in two main aspects, Post-Quantum Cryptography (PQC) and defending against Side-Channel Attacks (SCA). PQC is the antithesis to Quantum Hacking. It aims to create encryptions that are much less vulnerable to Quantum Hacking by using different cryptographic algorithms to secure the security of private and public-key cryptography [3]. Many PQC schemes have already been implemented and used in defending our devices. An example would be the NewHope key exchange scheme which has been tested in the Google Chrome Canary web Browser. Furthermore, a quantum-resistant cryptographic library called liboqs has been integrated into the openssl library [4]. Despite such schemes, we must not forget about the physical side of things. Most devices where our data is stored, like our phones, are easily accessible with little physical protection, making them vulnerable to SCAs, which take advantage of how an algorithm is performed in the device rather than overcoming the underlying mathematics. Despite being more specific, such attacks are much more powerful than others and are considered very seriously by the implementers of many cryptographic devices. In this review, we provide an outlook on the current state of post-quantum security, with the main focus on Post-Quantum Cryptography and whether common attacks like Side-Channel Attacks could still be used against it.

II. Post-Quantum Cryptography

One such Quantum Cryptography method is the lattice-based system. The basis of this system is the Shortest Vector Problem [5], where from the basis of a lattice (Fig 1), one has to find the shortest non-zero vector in a lattice. For example, we choose a coordinate point (4,2) and multiply the points by themselves (4 x 2 and 2 x 2) to get a new point (8,4). With this methodology, we can build a whole grid of evenly spaced points using a set of coordinates like (2,0) and (0,2) [6]. In other words, the lattice points with even coordinates are generated by the basis consisting of vectors (2,0) and (0,2). The concept is that by selecting a basis, we are selecting a full lattice, specifically the one whose points are formed by the basis's vectors. A basis is a basic finite object that could be represented in the computer's memory. With this system, we will have the ability to replace current algorithms and even make way for completely new classes of incredibly powerful cryptographic tools that quantum computers would not be able to breach.

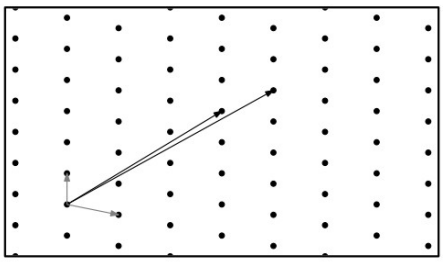

Fig. 1. Example of a 2D Lattice

The main advantage of the lattice-based system is that there is currently no known algorithm, quantum or otherwise, that can solve this lattice-based problem in less than exponential time. This means that each coordinate added will increase the time taken exponentially, unlike current RSA encryption. Adding on, this system is extremely adaptable when it comes to creating cryptographic systems. Adaptability is crucial for it to work long term and not just be a quick fix. With studies on lattices dating back to the 80s, there is already a lot of understanding and knowledge about lattices which will be key to giving proper insight when working with lattices to develop cryptographic systems. However, there are also downsides to this crypto type. Lattice-based

crypto generally requires much more bandwidth with the usage of around 1.5-2.5kB for a key exchange at 128 bit security level. This is considerably greater than the bandwidth used by current cryptos like the elliptic curve which takes up just 64 bytes. Moreover, it has also been proven to be difficult to deduce how effective and reliable the lattice crypto could be when dealing with attacks [7].

Another such Quantum Cryptography method is the hash-based system. The general idea of hash-based cryptography is a hash-based signature that can only be used once. Some of the most common and efficient Hash-Based examples include the stateful algorithms Multi-Tree eXtended Merkle Signature Scheme ($XMSS^{MT}$) (Fig 2), the Hierarchical Signature System (HSS), and the stateless algorithm SPHINCS+. It is considered to be very powerful cryptography due to using the well-known and accepted Secure Hash Algorithm 2 (SHA-2), which is believed to be able to withstand quantum hacking by supercomputers. Additionally, if the system is incapacitated, it can be reverted to normal just by changing to a secure hash function, which is cost-effective and referred to as 'crypto-agile' [8].

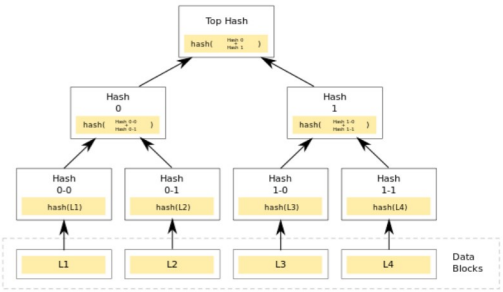

Fig. 2. Merkle Tree to visualise XMSS

However, there are many challenges that come with the idea of implementing Post-Quantum Cryptography. One of these challenges is that the current public and private key encryptions between IoT devices cannot be directly replaced with those resistant to quantum hacking. PQC algorithms have very large signature sizes, demand a lot of processing power, and use very large public and private keys that are not compatible with current devices due to a lack of proper technological infrastructure [9]. Current keys are only about a hundred or thousand bits long, which does not require much processing power to enable encryption and decryption, but PQC keys are estimated to be about tens of kilobytes to a megabyte, so these keys must be stored efficiently. Also, as these PQC algorithms would be very new when implemented, people might not have been familiar with the mathematical understanding behind these algorithms, which may lead to security lapses in the event of quantum hacking [10].

III. Side-Channel Analysis

Side-Channel Attack/Analysis (SCA) is the observation and collection of valuable secret data, such as execution time or power consumption, of a cryptosystem under attack [11]. SCAs are hard to pick up and are often undiscovered as they leave little to no trace of their activities. They are also effective against systems that are physically disconnected from the actual computer system mainframe as well as Virtual Machines (VMs) and cloud computing environments where the attacker and target have similar computing hardware [12].

An example of a SCA would include analysing the power consumption during cryptographic key generation (Simple Power Analysis), in which information regarding the secret key can be obtained. Since different math and processing operations will require and use different unique power profiles, Simple Power Analysis can reveal the order in which microprocessor instructions are being executed, which can unravel certain cryptographic algorithms.

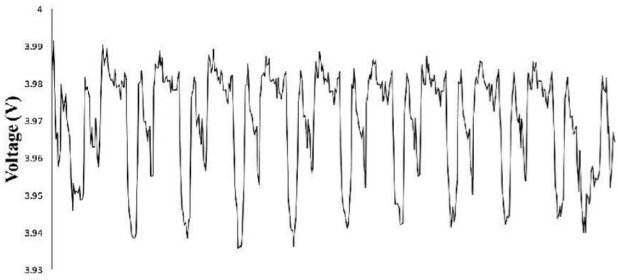

Fig. 3. Simple Power Analysis on AES-128

Another example of SCAs includes Differential Photonic Emission Analysis [13], which can reveal the secret key of a cryptographic device while the device is decrypting or encrypting data. SCAs rely on information leakage, and with the onset of IoT devices in the not-so-far future, SCAs pose a serious threat to our data.

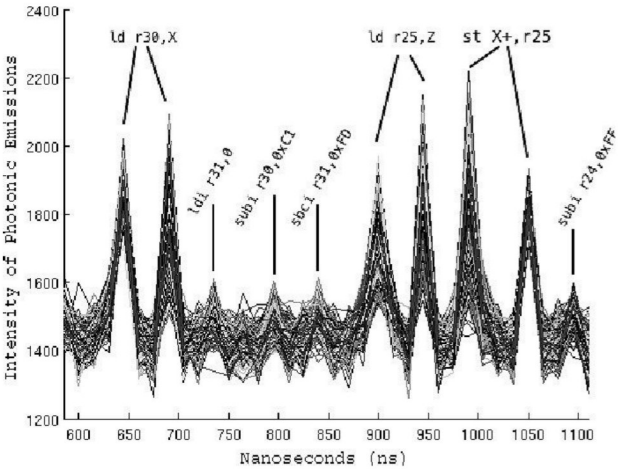

Fig. 4. Recording that shows registers' information through Differential Photonic Emission Analysis

A third example of SCAs is Acoustic Side-Channel Attacks. Every key on the keyboard will produce a different sound during typing, and attackers can use programs known as 'keyloggers' to record the sounds of keyboard typing, and afterwards reverse engineer the data from the keylogger into the original unencrypted message. This also affects touchscreen typing, as the sound waves of fingers typing

against the touch screen keyboard are also distinguishable, much like an actual keyboard [14]. Tracking these sounds can provide malicious parties with sufficient information to plan their attack on these cryptographic systems.

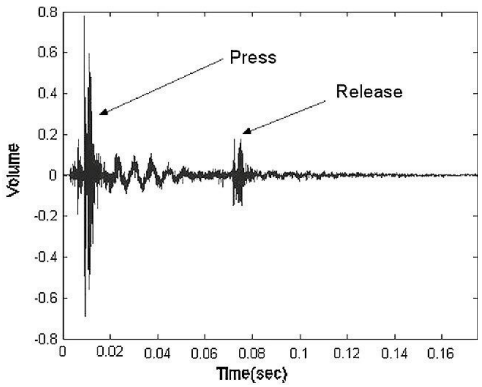

Fig. 5. Recording of a key being pressed then released

Even with secure algorithms such as AES-256, which uses 256 bits long keys, and is very tough to brute-force even for quantum computers, the possibility of these algorithms being brute-forced successfully is much higher when the consequences of Side-Channel Attacks are not taken into consideration [15]. Hence, SCAs are seen as a major danger in cryptography algorithms.

Clearly, SCAs are a threat to cryptography algorithms due to the fact that it can extract the secret key without reverse-engineering these algorithms in question. While Post-Quantum Cryptography are supposedly foolproof techniques that are secure against any quantum computer's abilities, it is exactly this characteristic that makes SCA more enticing. Ideally, SCAs can extract all parts of a secret key, regardless of length. Thus it is no surprise that SCAs pose a legitimate risk of overcoming Post-Quantum Cryptography.

IV. Discussion

Post-Quantum Cryptography is currently being researched by the US National Institute of Standards and Technology (NIST). NIST has hosted a competition to discover and understand the available types of PQC standards that will eventually replace RSA as the main form of cryptography everywhere in the world by the years 2022 to 2024 [16].

Additionally, as these new cryptography methods are being developed, it is important to take into account the risk of Side Channel Analysis, such that these unbreakable algorithms do not get compromised due to information leakage from physical sources.

A counter view to post-quantum cryptography is that although it seems promising, it rests on the fact that currently there is no way to solve these algorithms in less than exponential time. However, just like RSA technology was once considered unbreakable, future mathematicians and programmers may come up with groundbreaking technologies that can help to disrupt these currently unbreakable systems.

V. Conclusion

With the birth of quantum computers, devices secured with traditional cryptographic algorithms will become vulnerable. While Post-Quantum Cryptography (PQC) algorithms could protect us from this, it is still important to take into account Side-Channel Attacks (SCA) for such algorithms could still be cracked through SCAs if there is a lack of proper security when implemented. Despite their limitations, PQCs have proven to be promising in securing our devices and data in this post-quantum world.

VI. References

[1] Chowdhury, S., Covic, A., Acharya, R.Y. *et al.* Physical security in the post-quantum era. *J Cryptogr Eng* (2021). https://doi.org/10.1007/s13389-021-00255-w

[2] Arute, F., Arya, K., Babbush, R. *et al.* Quantum supremacy using a programmable superconducting processor. *Nature* **574,** 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5

[3] CB Insights. (2021, September 8). *Post-Quantum Cryptography: A Look At How To Withstand Quantum Computer Cyber Attacks*. CB Insights Research. https://www.cbinsights.com/research/post-quantum-cryptography/

[4] Lukas Malina, Lucie Popelova, Petr Dzurenda, Jan Hajny, Zdenek Martinasek, On Feasibility of Post-Quantum Cryptography on Small Devices, IFAC-PapersOnLine, Volume 51, Issue 6, 2018, Pages 462-467, ISSN 2405-8963, https://doi.org/10.1016/j.ifacol.2018.07.104. (https://www.sciencedirect.com/science/article/pii/S2405896318308474)

[5] Y. Chuang, C. Fan and Y. Tseng, "An Efficient Algorithm for the Shortest Vector Problem," in IEEE Access, vol. 6, pp. 61478-61487, 2018, doi: 10.1109/ACCESS.2018.2876401.

[6] Wickr, J. A. (2020, August 15). *What is lattice-based Cryptography & why you should care*. Medium. Retrieved October 16, 2021, from https://medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717

[7] *3 weaknesses of post-quantum cryptography*. Quantropi. (2021, August 4). Retrieved October 16, 2021, from https://www.quantropi.com/3-weaknesses-of-post-quantum-cryptography/

[8] Corporation, I. (2020). *Math Paths to Quantum-safe Security: Hash-based Cryptography*. ISARA Corporation. https://www.isara.com/blog-posts/hash-based-cryptography.html

[9] *NIST previews post-quantum cryptography challenges* -. (2021, May 3).GCN. https://gcn.com/articles/2021/05/03/nist-post-quantum-encryption.aspx

[10] Freeman, J. B. (2021, July 26). *What Is Post-Quantum Cryptography?* Freeman Law. https://freemanlaw.com/what-is-post-quantum-cryptography/

[11] Joye, M. (2009). *Basics of Side-Channel Analysis*. SpringerLink. https://link.springer.com/chapter/10.1007/978-0-387-71817-0_13?error=cookies_not_supported&code=37e523c0-2c24-4e83-a8d5-ab2953fc9001

[12] Wright, G., & Gillis, A. S. (2021, April 6). *side-channel attack*. SearchSecurity. https://searchsecurity.techtarget.com/definition/side-channel-attack

[13] Prouff, E. (ed.): Constructive Side-Channel Analysis and Secure Design - 4th International Workshop, COSADE 2013, Paris, France,

6–8 March 2013. LNCS, vol. 7864. Springer, Heidelberg (2013) doi: 10.1007/978-3-642-40026-1

[14] Mulloy, E. (2020, December 3). *Side-Channel Attacks and Hardware Vulnerabilities*. SD Solutions, LLC. https://www.sdsolutionsllc.com/side-channel-attacks-and-hardware-vulnerabilities/

[15] Lake, J. (2021, April 16). *What is a side-channel attack and how do they work?* Comparitech. https://www.comparitech.com/blog/information-security/side-channel-attack/

[16] Comandar, L., Bobier, J., Coden, M., & Deutscher, S. (2021, July 1). *Ensuring Online Security in a Quantum Future*. BCG Global. https://www.bcg.com/publications/2021/quantum-computing-encryption-security