Article

Roadmap of Post-Quantum Cryptography Standardization: Side-Channel Attacks and Countermeasures

Ari Shaller, Linir Zamir and Mehrdad Nojoumian*

Florida Atlantic University
Department of Electrical Engineering and Computer Science
777 Glades Road, Boca Raton, FL 33431; {ashaller2017,lzamir2016,mnojoumian}@fau.edu
* Correspondence: mnojoumian@fau.edu

Abstract: Quantum computing utilizes properties of quantum physics to build a fast-computing machine that can perform quantum computations. This will eventually lead to faster and more efficient calculations especially when we deal with complex problems. However, there is a downside related to this hardware revolution since the security of widely used cryptographic schemes, e.g., RSA encryption scheme, relies on the hardness of certain mathematical problems that are known to be solved efficiently by quantum computers, i.e., making these protocols insecure. As such, while quantum computers most likely will not be available any time in the near future, it's necessary to create alternative solutions before quantum computers become a reality. This paper therefore provides a comprehensive review of attacks and countermeasures in Post-Quantum Cryptography (PQC) to portray a roadmap of PQC standardization, currently led by National Institute of Standards and Technology (NIST). More specifically, there has been a rise in the side-channel attacks against PQC schemes while the NIST standardization process is moving forward. We therefore focus on the side-channel attacks and countermeasures in major post-quantum cryptographic schemes, i.e., the final NIST candidates.

Keywords: Post-Quantum Cryptography; Side-Channel Attacks; Attacks on PQC.

Citation: Shaller, A.; Zamir, L.; Nojoumian, M. Roadmap of Post-Quantum Cryptography Standardization: Side-Channel Attacks and Countermeasures. *Journal Not Specified* **2022**, *1*, 0. https://doi.org/

Received:
Accepted:
Published:

1. Introduction

It is known that quantum computing is an incoming threat towards many of the current major Public-Key Cryptosystems (PKC), such as Rivest–Shamir–Adleman (RSA), Diffie-Hellman (DH), and Elliptic Curve (EC) cryptosystems. These cryptographic schemes rely on the hardness of Integer Factoring (IF) problem or Discrete Logarithm (DL) problem, which can be broken in polynomial time using Shor's algorithm [1,2]. There are many predictions towards the realization of large-scale quantum computers, ranging from as early as 2026 [3,4] to somewhere between thirty to forty years to come [5]. Despite that, the issue of quantum computing is deemed concerning enough that the National Institute of Standards and Technology (NIST) announced their plan on standardizing and transitioning from conventional cryptography to Post-Quantum Cryptography (PQC), followed by a similar announcement from the National Security Agency (NSA).

Post-quantum cryptography refers to cryptographic algorithms that are based on hard mathematical problems, which can withstand the attacks of both conventional and quantum computers. There are major families of the PQC cryptosystems that are as follows: *Code-based*, *hash-based*, *isogeny-based*, *lattice-based*, and *multivariate-based*. There are many cryptosystems being studied throughout the years, including some of the earlier ones, McEliece [6] and Niederreiter [7]. Although these cryptosystems are quantum-resistant, they are still vulnerable to side-channel attacks. This type of attack, first demonstrated in the research by Paul Kocher et al. [8,9], is able to recover secret information by exploitation of physical leakages. More specifically, the authors studied the exploitation of timing variation on DH, RSA, and other cryptosystems and continued on the topic of side-channel attacks with simple and differential power analysis.

Although extensive research has been conducted regarding other kinds of information leakage., the literature is still lacking compared to the number of algorithms available to be tested, the kind of side-channels and attacks to be observed, and the hardware or software to be employed. Besides, there are an overwhelming number of open problems to be scrutinized in this landscape. We therefore assess attacks and countermeasures in PQC by focusing on latest advancements in this field.

1.1. Our Motivation and Contribution

Side-Channel Attack (SCA) is comparatively inexpensive and easy to perform since comprehensive understanding of the system is sometimes not needed. This type of attack does not affect only particular algorithms, but all implementation-specific algorithms. With the threat of quantum computers, and therefore, the increase in effort to create quantum-resistant algorithms, there are emerging algorithms that are required to be assessed and evaluated from various security perspectives.

Security against SCA is unknown in many of these algorithms. This can become a source of leakage in a wide range of information systems. Indeed, even without considering new post-quantum hardware and software technologies, if security against side-channel attacks is ignored, the new algorithms will still be insecure in their real-world implementations despite being resilient against quantum attacks. That is why, in addition to quantum-safe algorithms, it is imperative that researchers also pay as much attention to the study of PQC algorithms with side-channel resistance.

As stated earlier, the literature on post-quantum cryptography, especially on side-channel attacks and its countermeasures, is still lacking. In other words, with the number of newly-developed algorithms, attacks, software, or hardware, there is a significant gap in the literature that needs to be filled. This paper therefore provides a roadmap for researchers in academia and industries who are conducting research on quantum-safe software and hardware platforms.

1.2. Organization of the Paper

Section 2 provides preliminary materials regarding PQC. Section 3 reviews side-channel attacks and countermeasures regarding post-quantum cryptography in the order of code-based, hash-based, isogeny-based, lattice-based, and multivariate-based families. Finally, Section 4 provides concluding remarks.

2. Preliminary Materials

This section provides a basic introduction to post-quantum cryptography and its major families, including the mathematical methods used for each cryptography family. Additionally, it will introduce the methods for evaluating side-channel leakage.

2.1. Post-Quantum Cryptography

PQC is a cryptographic paradigm that is secured by definition against attacks of both conventional and quantum computers. Quantum computers provide adversaries with the ability to solve computationally expensive mathematical problems faster than any classical computer. This can then break some of the most commonly used cryptographic encryption systems, which rely on the hardness of some mathematical problem. Note that there is no PQC setting such that the underlying mathematical problem can not be solved. In the worst case scenario, it can be solved by exhaustive search. All of these mathematical problems are based on computationally hard problems, which have appropriate algorithms to solve them, but are computationally too expensive even for quantum computers. Many PQC solutions have been made to meet the requirements and criteria of post-quantum cryptography, and depending on its mathematical foundation, each of those proposed algorithms belongs to one of the families of post-quantum cryptography. These major families are code-based, hash-based, isogeny-based, lattice-based, and multivariate.

1. *Code-Based*: Cryptosystems from this family utilizes error-correcting codes that operate on bits. These codes receive its name for its ability to detect and correct a limited number of errors in a sequence of bits. The first cryptosystem of this family was proposed in 1978 by Robert J. McEliece [6].The McEliece cryptosystem utilizes a generator matrix for its public-key and a Goppa code for its private-key. In 1986, Niederreiter [7] developed a cryptosystem with a parity check matrix. Later, there were some modifications and improvements on the McEliece cryptosystem, for example using systematic generator matrix and quasi-cyclic moderate parity check.
2. *Hash-Based*: The idea of hash-based cryptography is that multiple instances of One-Time Signature Scheme (OTS) are combined with a secure hash function so that they can be used more than once. Merkle [10] proposed this and created Merkle Signature Scheme (MSS) that now has many variants including the eXtended Merkle Signature Scheme (XMSS) and the multi-tree version XMSS^{MT}. There are two kinds of hash-based signature algorithms: Stateful and stateless. Stateful hash-based signatures are more difficult to manage because each signature key has a state that must be changed after the key has been used. On the other hand, stateless signatures do not need to change the state of the signature key, resulting in an easier implementation.
3. *Isogeny-Based*: This cryptography is based on the hard problem of finding an isogeny between two supersingular elliptic curves. This idea was first introduced by Rostovtsev and Stolbunov in 2006 [11] as isogenies between ordinary elliptic curves. In 2012, the algorithm was broken using a 'subexponential-time quantum algorithm' attack by Childs, Jao and Soukharev in [12]. That same original idea was then further developed by Jao and De Feo as a key exchange mechanism over supersingular elliptic curves. The new algorithm, named Supersingular Isogeny Diffie-Hellman (SIDH) [13], utilizes the idea of walking through a sequence of supersingular elliptic curves. Compared to the code-based and lattice-based cryptography, the isogeny-based cryptosystem has a much smaller key size.
4. *Lattice-Based*: First introduced by Ajtai in 1996 [14], lattice-based cryptography is based on the hardness of solving lattice problems. One of these problems is called the Short Vector Problem (SVP). In 1997, Ajtai and Dwork [15] presented a public-key cryptosystem using the modification of this problem called u-SVP, which tries to find a unique nonzero shortest vector v in an n dimensional lattice L. The first scheme of this family is NTRU, proposed in 1998 by Hoffstein et al. [16].
5. *Multivariate*: This family of cryptography is constructed based on multivariate polynomials over a finite field. Matsumoto and Imai created an asymmetric cryptosystem based on multivariate polynomials, called C* in 1988 [17]. A decade later, in 1999, Kipnis et al. [18] proposed a new scheme, named Unbalanced Oil-and-Vinegar (UOV), that is a modification of the previously Oil and Vinegar scheme by Patarin [19].

Table 1 illustrates the cryptographic schemes from the six PQC families based on the National Institute of Standards and Technology (NIST) third-round standardization results. NIST recognized the potential threats quantum computing can bring to current security algorithms such as RSA, so they initiated a standardization process with a competition to find the best overall post-quantum cryptography algorithms. There are four finalists for public-key cryptosystems, i.e., *Classical McEliece, Crystal-Kyber, NTRU*, and *SABER*. Moreover, there are three finalists for digital signatures, i.e., *Crystal-Dilithium, Falcon*, and *Rainbow*.

2.2. Side-Channel Attacks

In a side-channel attack, an adversary gains information from power output traces, electromagnetic radiations, execution times or any other leaked residual data by relating this information with operations made by the attacked unit. This relationship can create a