Security and Quantum Computing: A Perspective

Prasanna Ravi[†,*], Anupam Chattopadhyay[*], and Shivam Bhasin[†]

[†]Temasek Labs, Nanyang Technological University, Singapore
[*]SCSE, Nanyang Technological University, Singapore

***Abstract*—The promise of scalable quantum computing is causing major upheaval in the domain of cryptography and security. In this perspective paper, we review the progress towards the realization of large-scale quantum computing. We further summarize the imminent threats towards existing cryptographic primitives. To address this challenges, there is a consolidated effort towards the standardization of new cryptographic primitives, namely post-quantum cryptography (PQC). We discuss the underlying mathematical problems that define different classes of PQC candidates, and their resistance to an adversary having access to large Quantum computer. In parallel to this thread of research, several classical cryptographic primitives have been ported to the Quantum world as well. We discuss, in that context - Quantum Key Distribution (QKD), Physically Unclonable Function (PUF) and True Random Number Generator (TRNG). For those implementations, we take a sneak preview in the resulting implementation-related vulnerabilities.**

I. Introduction

In general, quantum computers can be broadly classified into universal gate quantum computers and quantum annealers [1]. The universal gate quantum computer/processor can be seen as a quantum counterpart to a classical general purpose microprocessor, where IBM (127 qubit) [2], [3], Google (72 qubit) [4] are in rapid pursuit of building faster and larger universal gate based quantum computers. On the other hand, the quantum annealers are akin to Application-Specific IC (ASIC), which can be used for solving a specific set of combinatorial optimization problems over discrete search space. However, the problems of interest in the domain of security primarily eyes the growth of universal quantum computers, which is not polynomially equivalent to quantum annealer.

The evolution of large-scale quantum computers are not only fuelled by their threats to security though. There are potentially massive performance gain to be obtained by quantum computers in the domains of molecular chemistry, financial derivative pricing, supply-chain optimization and machine learning, to name a few. There is also a concerted effort to demonstrate so-called *quantum advantage* even with small-scale and noisy quantum computers [5]. To test these algorithmic advances, there are increasingly powerful quantum computers that are made available by the manufacturers and system designers through cloud-based services. To aid the design efforts, software development kits are released as well from vendors, such as, IBM, Google, Xanadu, Microsoft and Rigetti.

A. Error Correction for Scalable Quantum Computing

There are several obstacles towards scalable quantum computer implementation, such as, achieving entanglement over many qubits, qubit fidelity, environmental noise. Quantum error correction codes paved the way for robust quantum computing, which, however needs to be implemented in a fault-tolerant manner so that, the error correction circuit itself is immune to issues like gate control error. Among various quantum error correction codes, surface code is considered a fore-runner now, due to its low-cost implementation in current quantum technologies.

The growth of a quantum computer is marked through its capabilities of achieving entanglement over larger number of qubits (as in IBM 127-qubit) and ability to perform large number of quantum gate operations in a noise-resilient manner. Due to the necessity of associated error correction codes, to achieve the operation of a single *logical* qubit, several *physical* qubits are needed. This ratio is dependent on the underlying quantum technology, error correction codes, and could therefore require up to 1000 physical qubit to realize 1 logical qubit [6]. These details are important to account for when we proceed with the estimation of *quantum attack complexity* since, for all the existing cryptosystems, currently available Quantum computers are inadequate for mounting a practical attack. Therefore, researchers resort to analytical estimations, as we will discuss in the following.

II. Threats on Cryptographic Primitives from Scalable Quantum Computers

In the following, we briefly review the quantum-empowered threats on classical cryptography.

A. Public-Key Cryptography

The security public key cryptography in use today rely on fundamental hard problems in number theory like the integer factorisation and the discrete logarithm problem which are intractable by classical computers. Both of these are now within the reach of a large-scale quantum computer.

The best known algorithm for factorisation for example, is the general number field sieve method which scales exponentially with the number of operations with respect to the size of the prime. However, Shor's algorithm [7], the most well known quantum algorithm can solve the same problem in polynomial time ($\mathcal{O}(n^3)$), thus providing an exponential speed up. In recent times, there has been a steady growth of studies of accurate cost estimation for breaking cryptographic primitives using quantum computers. Proos et al. [8] reported that about $6n$ qubits would be required to break Elliptic curve cryptography where n is the bit length of the order of the group. Thus, it would take about $6*255 = 1530$ logical qubits to break ECC for a 255-bit curve (e.g. Curve25519, Ed25519). Further optimizations on the quantum circuit design is being done to reduce the attack complexity[9].

In a recent study by Gidney et al [10], the logical qubit required for factoring an n-bit number is shown to be $3n + 0.002nlgn$. Under reasonable assumptions about the gate error rate, cycle time, and other parameters, it is hypothesized that a 2048-bit RSA integer can be factored within 8 hours, if 20 million physical qubits are available.

B. Private-Key Cryptography

Compared to public-key cryptography, private-key cryptographic algorithms remained more resilient to a quantum adversary. The standard approach has been to first, apply Grover's search algorithm for brute-forcing the secret key, which gives a quadratic speed-up. This was improved in [11].

Meet-in-the-middle attacks, taken from classical setting to quantum, are studied for AES [12], [13]. A core ingredient of quantum attacks on symmetric-key ciphers is an efficient quantum circuit for the cipher itself, since the encryption operation is called multiple times during the attack. Consequently, there is a recent growth of studies on efficient quantum circuit for symmetric-key ciphers [14]. Despite these advances, the quantum attack complexity remained in the exponential order for private-key ciphers.

III. Post-Quantum Cryptography

Sustained progess towards realizing large scale quantum computers has long prompted the cryptographic community towards devloping public-key cryptographic primitives that are resistant to attack from quantum computers. This led to a new area of cryptographic research called *post-quantum cryptography* (PQC). The core idea of PQC is to build cryptographic primitives based on hard problems that are considered to be intractable for quantum computers.

A. NIST PQC Standardization Process

As a first significant step towards wide scale adoption of PQC, NIST called for proposals for standardization of post-quantum cryptographic schemes and in particular three primitives which are considered to be the *workhorses* of public-key cryptography: Public-Key Encryption (PKE), Digital Signature (DS) and Key-Encapsulation Mechanisms (KEM)[15]. Based on the underlying hard problem, PQC can be broadly classified into five main categories: (1) Lattice-based (2) Code-based (3) Hash-based (4) Multivariate Quadratic-based and (5) Supersingular Isogeny-based cryptography. The first round of NIST PQC process which started in December 2017 with 69 submissions (49 PKE/KEMs and 40 DS schemes), is in its third and final round with seven finalist candidates and eight alternate candidates [16] for PKEs, KEMs and DSs [16] (Refer Tab.I). While NIST considers immediate standardization of a subset of the main finalists (after the third round), alternate candidates could be considered for standardization in the future, probably after an additional fourth round.

Table I
Tabulation of the post-quantum cryptographic schemes that are currently competing in the NIST standardization process. Main Finalists are higlighted in *Italics font*.

Type of Cryptography	Type of Scheme	Scheme
Lattice-based	Key-Exchange	*Kyber* *SABER* *NTRU* FrodoKEM NTRU Prime
	Digital Signatures	*Dilithium* *FALCON*
Code-based	Key-Exchange	*Classic McEliece* BIKE HQC
MQ-based	Digital Signatures	*RainBow* GeMSS
Hash-based	Digital Signatures	Picnic SPHINCS+
Isogeny-based	Key-Exchange	SIKE

NIST identified the following three criteria for evaluating the PQC schemes - (1) Security (2) Cost and Performance and (3) Algorithm and Implementation Characteristics.

1) Security: Theoretical post-quantum security as well as classical security guarantee serves as the most important evaluation criterion for standardization. NIST is likely to choose a suite of cryptographic algorithms based on different families of cryptosystems rather than a single winner [16], so as to reduce the risk of potential cryptanalysis of that single selected candidate, and rather have readily available fallback options.

2) Cost and Performance: This criterion covers three aspects - (a) speed (runtime) (b) resource efficiency (RAM/gate-count) and (c) communication bandwidth (size of public-keys, ciphertexts and signatures). While runtime is critical for high-performance applications (general purpose CPUs/GPUs), resource efficiency comes to the fore for applications involving embedded devices, and communication bandwidth is an important factor in use-cases that require frequent transmission of public-keys or signatures [17]. So, it is likely that NIST might select a portfolio of schemes catering to different types of use-cases and constraints.

3) Algorithm and Implementation Characteristics: Resistance of PQC schemes against implementation-level attacks such as Side-Channel Attacks (SCA) and Fault-Injection Attacks (FIA) also emerged as an important criterion in the standardization process. NIST is especially interested in evaluating the cost of incorporating countermeasures to counter SCA/FIA. Moreover, candidates that can serve as drop-in replacements within protocols such as TLS and IPSec are more preferable, compared to those which require significant re-engineering effort for integration [16].

In the following, we provide a brief overview of different categories of PQC schemes, with special focus on schemes in the final round of the NIST process. Please refer the NIST website for specification of all the finalist candidates [18].

B. Lattice-based Cryptography

This category offers both KEMs and signature schemes, with a majority of finalists (7 out of 15) based on hard problems over lattices. They base their security predominantly based on two well-known problems - (1) Learning With Error (LWE) or Rounding (LWR) problem and (2) NTRU problem. In general, lattice-based schemes are characterized by excellent implementation performance. Thus, they are seen by NIST as the most promising candidates for standardization, as they are immediately suitable for general-purpose applications [16].

Given their portability to different platforms and particularly embedded devices, lattice-based schemes has received the most attention with respect to SCA and FIA [19], [20]. In parallel to identifying attacks, there have been notable advances towards developing secure and efficient countermeasures for lattice-based schemes against SCA/FIA [21], [22]. Thus, extensive research on lattice-based cryptography, right from theory until practice makes it a readily available alternative for PKC in the post-quantum era.

C. Code-based Cryptography

This category offers KEMs, built upon hard problems in the well-established field of error correcting codes. Classic Mceliece (finalist) is built upon the 1979 McEliece cryptosystem based on linear goppa codes [23], that has resisted classical/quantum cryptanalysis for more than 40 years now. However, very large public keys (hundreds of KBs) and very slow runtimes do not make them suitable for general-purpose applications. On the other hand, BIKE and HQC are two other more recent code-based KEMs (alternate finalists) built upon the more efficient QC-MDPC codes. While they offer more balanced performance, they provide lower speeds and larger public keys compared to lattice-based KEMs. However, a mature cryptanalysis of code-based KEMs, make them a conservative option for KEMs, especially in use-cases where speed/bandwidth is not critical. There have been a few side-channel attacks targeting the decryption procedure of code-based schemes [24], [25], while not much attention has been given towards designing SCA/FIA protected implementations.

D. Hash-based Cryptography

This category offer signature schemes, primarily built using symmetric key primitives such as hash functions [26]. Thus, their security guarantees are backed by well-established notions from private key cryptography. SPHINCS+ (alternate finalist) is a prominent hash-based signature scheme, but suffers from very large signatures and slow signing times. Picnic is an alternate finalist for signatures, whose security also relies on hash functions and block-ciphers. While the size of public keys and signatures are comparable with structured lattice-based schemes, slower signing and verification times serve as an important drawback. Given their strong security assurances, hash based signatures can serve as conservative choices for high-security use-cases. The signing procedure of hash based signatures has been targeted by fault injection attacks [27], [28] and side-channel attacks [29] on embedded devices. However, there has not been much attention devoted towards protected implementations of hash-based signature schemes.

E. Multivariate Quadratic-based Cryptography

Rainbow (main finalist) and GeMSS (alternate finalist) are two signature schemes belonging to this category, which base their security on hardness of solving multivariate quadratic (MQ) equations over a finite field. While MQ-based schemes offer very small signatures, they suffer from very large public keys (two orders of magnitude higher than lattice-based schemes) accompanied with slow signing times. However, the main disadvantage of MQ-based schemes is the relatively poor track record of cryptanalysis, with the latest attack mounted on the Rainbow signature scheme [30] this year. While the specification of Rainbow has been updated to mitigate the attack, cryptanalysis of MQ-based schemes in an active research topic, that will be closely monitored by the PQC community.

F. Supersingular Isogeny-based Cryptography

This category offers KEMs whose security is based on hardness of computing supersingular isogenies over elliptic curves. SIKE is the only KEM (alternative finalist) from this category, and has the main advantage of offering the smallest public key and ciphertext sizes of all PQC based KEMs, which makes it very attractive for limited bandwidth applications. However, very slow runtimes (two orders of magnitude slower than lattice-based KEMs) serves as a main drawback. Given its similarity to traditional ECC based cryptography, SIKE has been subjected to a number of different side-channel attacks and there have been proposals for appropriate countermeasures [31], [32], along the same lines of practical implementations of ECC. However, more study towards side-channel and fault-injection analysis is desirable.

IV. Quantum-Enabled Security: Quantum Key Distribution

Quantum key distribution (QKD) is an alternative approach for key-exchange, which works by harnessing the fundamental properties of quantum mechanics [33]. QKD offers Information Theoretic Security (ITS), and therefore unconditionally secure against an attacker with unlimited computational power. This is in stark contrast to traditional cryptographic schemes, which are only conditionally secure against an attacker with well-defined and finite computational capabilities. Thus, QKD also serves as a natural alternative for key exchange against a quantum adversary. An important point to note is that one does not need a quantum computer to implement a QKD system.

A. Basic operation of QKD

The security of QKD is based on the notion that it is impossible to obtain information about a quantum state, without perturbing it. This makes it possible to detect the amount of eavesdropping that occurs on the communication channel, and simply discard those bits that have been perturbed. In this way, two parties can exchange data in plaintext over a quantum channel. A basic and concrete instantiation of a QKD system is a simple QKD link (Fig.1).

It consists of two channels - quantum and classical channel between the communicating parties (Alice and Bob). Alice encodes a secret key into non-orthogonal states of light, which is sent over the quantum channel to Bob. Bob measures the received quantum states and sends a correlated bitstream on the classical channel back to Alice. If the correlation computed by Alice is large enough beyond a certain threshold, it implies that no significant eavesdropping has occured, with a very high probability. Thus, a secret key can be generated from the correlated bit strings. Otherwise, this process has to be repeated until a key is shared. A unique feature of this mechanism is the ability of the communicating parties to verify the presence of an eavesdropper (Eve) or a man-in-the-middle using the correlation computed over the transferred data. Thus, a QKD-based key exchange consists of two phases - (1) Quantum phase where the message is tranferred over classical channel and (2) Classical phase where key reconciliation happens over the classical channel.

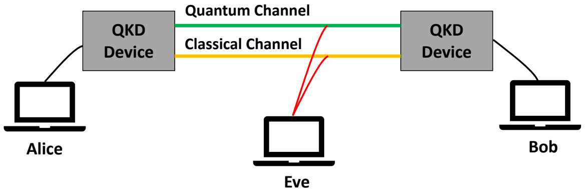

Figure 1. Pictorial Illustration of a QKD link

Since QKD relies on the presence of a classical channel, an authenticated classical channel is mandatory, as use of unauthenticated channels can lead to easy man-in-the-middle attacks. Thus, QKD cannot be implemented as a standalone protocol, but has to be combined with either classical private-key or public-key cryptographic schemes for authentication.

B. Implementation Aspects of QKD

QKD systems can be classified into different categories based on the (1) Encoding mechanism and (2) Quantum communication medium.

1) Based on Encoding/Decoding: Based on the encoding/decoding mechanism, it is majorly split into two categories - Discrete Variable QKD (DVQKD) and Continuous Variable QKD (CVQKD). While DVQKD relies on discetely encoding information on polarization of single photons [33], it is hindered by technological limitations for implementation. CVQKD, however is a more popular approach which works by encoding information over continuous variables in photon states [34], and can be implemented using off-the-shelf telecom components.

Most approaches based on DVQKD/CVQKD have a common disadvantage of being limited by the distance-rate trade-off, with a definite upper bound on the key rate achievable at a given distance [35]. While this fundamental limit can be overcome by using quantum repeaters, these devices are currently not technologically feasible to be implemented. Very recently, a new approach known as Twin-Field (TF) QKD protocol was proposed [36], which overcomes the upper bound on the key rate. While TFQKD has been shown to be feasible at a distance of 500km, it is also plagued by other physical effects such as dark counts and photon losses, which practically influence the key rate at long distances. However, continuous research towards increasing the distance limit of TFQKD [37], offers a positive outlook towards deployment of QKD over long distances.

2) Based on Communication Mediums: QKD can be implemented over different types of communication mediums - (1) Optical Fiber and (2) Free-Space. While optical fiber-based channels offer several advantages of providing physically robust channels as well as guiding properties, they lack flexibility and portability, and are plagued by the distance-rate limitation due to propagation losses. The other type of communication medium used is the free-space link. While QKD in terrestrial free-space (air) is also plagued by propagation losses, satellite-based QKD in empty outer space is seen as an attractive approach for realizing QKD at a global scale. A recent work has demonstrated free-space sattelite-based QKD at a distance of over 1200 km with a key-rate of 1Kbps [38], while longer distances seem very much possible with advancing research. Current fiber-based QKD technologies can provide the same rate only at a distance of 100-150 km.

C. Usage of QKD for Secure Communication

There are two possible approaches towards using QKD to secure communciation in today's digital networks.

1) QKD With Unconditionally Secure One-Time-Pad: One can simply utilize the QKD keys to encrypt messages using the One-Time-Pad (OTP) scheme. Given that both QKD and OTP are both unconditionally secure, the resulting protocol is also unconditionally secure. The obvious drawbacks of this scheme include (1) key management issues (2) communication rate limited by key rate of QKD. Though this cannot be used for general-purpose applications, this is a very attractive alternative for highly sensitive information such as security of industrial secrets and government classified information.

2) QKD With Computationally Secure Symmetric Ciphers: The other more practical alternative is to use QKD keys within symmetric encryption and authentication schemes such as AES and HMAC. While this approach is only as secure as the computational security of the symmetric cryptographic scheme, it can be readily used within existing security protocols as well as traditional classical internet. Dedicated QKD links can be used as a source for unconditionally secure keys, and QKD can be instantiated readily to refresh keys. This approach guarantees forward secrecy, wherein recovery of a single key does not compromise secrecy of previously shared keys or future keys.

D. Side Channel Attacks on Quantum Key Distribution

Since QKD is implemented only using classical hardware, it has also been targeted by a number of implementation-level side-channel attacks. They can be divided into two categories: (1) Quantum specific and (2) Non-Quantum specific. Quantum specific attacks attempt to exploit leakage from the transmitter or receiver acting on the quantum channel. Prior works have shown that intense pulses of light can be injected in the quantum channel to (1) exploit information about phase modulators used by Alice and Bob and therefore about the shared key [39] and (2) mount a detector-blinding attack that allows Eve (eavesdropper) to mimic correct behaviour by changing detector response characteristics [40]. Moreover, random temporal delays to pulses can be added to perform time-shift attacks to recover the key [41].

The Non-Quantum specific attacks can target leakage from operations that classically manipulate the secret such as (1) TRNG/PRNG used to generate the secret key and (2) key reconciliation during the classical phase of the QKD etc. In this respect, Park *et al.* [42] showed that a single EM side-channel trace is sufficient to recover the entire key from the key-reconciliation operation. Protection against non-quantum specific attacks on QKD, can be done by borrowing well-established techniques from SCA to protect classical private-key and public-key cryptopgraphic implementations.

Thus, it is imperative to consider attacks on both the quantum and non-quantum phases of the QKD, while building secure hardware for QKD. Another very exciting direction towards resisting implementation level attacks, is the concept of Measurement-device independent quantum key distribution (MDI-QKD) [43], where security can be proven independent of the devices implementing the QKD. This presents a very powerful defence against side channel attacks on QKD and might probably inspire research works on also designing inherently side-channel resistant cryptographic algorithms. Though it has still not been demonstrated in practice, recent results close the gap between theory and practice, with respect to practical demonstration of MDI-QKD [44].

V. Quantum-enabled Security: Further Primitives

Quantum mechanical properties have been leveraged by researchers to also design two classes of primitives, following their classical counterparts - namely random number generator and Physical Unclonable Function (PUF). We discuss a few design propositions here.

A. Quantum Random Number Generator

Random number generators rely on a source of entropy. Extending the principles of classical entropy sources, quantum random number generator (QRNG) is derived from a quantum source of entropy. It was shown in [45] that the quantum noise in photon sources can be leveraged to generate QRNG using consumer grade hardware, e.g., a mobile phone. A common issue with QRNG is that it is tainted by classical noise as well. Given a particular quantum-to-classical noise ratio, QRNG extraction is presented in [46]. An important component of QRNG-based protocols is to test the quality of randomness. A third-party, device-independent and privacy-preserving randomness testing of QRNG is proposed here [47]. A comprehensive discussions about QRNG is presented in [48].

B. Quantum Physical Unclonable Function

Physical Unclonable Function (PUF) circuits provide a unique device identifier, thereby bypassing the necessity of key distribution. PUF-based protocols for device authentication, key generation and digital signatures are deployed in classical hardware. While both TRNG and PUF do rely on a source of entropy, PUFs require repeatability of the so-called challenge-response pairs. There are several propositions in literature, where PUFs are implemented leveraging quantum properties.

Quantum PUFs, or QPUFs have been realized using quantum confinement [49], superposition and decoherence [50]. For both QTRNG, and QPUF, the readout model has to be established. In that setting, the security protocol plays an important role. For example, it was shown that for a classical readout of QPUF, an adversary with statistical queries can model the QPUF [51]. To address this gap, models for quantitative characterization of QPUF with both classical and quantum readout is developed [52]. The resilience of QPUFs against quantum game-based attacks is studied in [53].

VI. Conclusion

The rapid evolution of large-scale quantum computers have created a major upheaval in the domain of security. In this paper, we studied these effects. First, we presented the current state of quantum computing followed by the estimates of their size - necessary to completely break current cryptosystems. Second, we present an overview of two dominant research trends namely, post-quantum cryptography and quantum key-distribution to combat the threat of quantum-enabled adversary. We closed the study with a brief review of further quantum primitives such as quantum PUF and quantum random number generators.

References

[1] Mark W Johnson, Mohammad HS Amin, Suzanne Gildert, Trevor Lanting, Firas Hamze, Neil Dickson, R Harris, Andrew J Berkley, Jan Johansson, Paul Bunyk, et al. Quantum annealing with manufactured spins. *Nature*, 473(7346):194, 2011.

[2] IBM. Ibm announces advances to ibm quantum systems and ecosystem. *https://www-03.ibm.com/press/us/en/pressrelease/53374.wss*.

[3] IBM. Ibm quantum breaks the 100-qubit processor barrier. *https://research.ibm.com/blog/127-qubit-quantum-processor-eagle*.

[4] Google. A preview of bristlecone, google's new quantum processor. *https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html*.

[5] Frank et al Arute. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[6] Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A*, 86:032324, Sep 2012.

[7] Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[8] John Proos and Christof Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *arXiv preprint quant-ph/0301141*, 2003.

[9] Thomas Häner, Samuel Jaques, Michael Naehrig, Martin Roetteler, and Mathias Soeken. Improved quantum circuits for elliptic curve discrete logarithms. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 425–444, Cham, 2020. Springer International Publishing.

[10] Craig Gidney and Martin Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, April 2021.

[11] Andre Chailloux, Maria Naya-Plasencia, and Andre Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. Cryptology ePrint Archive, Paper 2017/847, 2017. https://eprint.iacr.org/2017/847.

[12] Kyungbae Jang, Anubhab Baksi, Gyeongju Song, Hyunji Kim, Hwajeong Seo, and Anupam Chattopadhyay. Quantum analysis of AES. *IACR Cryptol. ePrint Arch.*, page 683, 2022.

[13] Zhenyu Huang and Siwei Sun. Synthesizing quantum circuits of AES with lower t-depth and less qubits. *IACR Cryptol. ePrint Arch.*, page 620, 2022.

[14] Kyungbae Jang, Anubhab Baksi, Jakub Breier, Hwajeong Seo, and Anupam Chattopadhyay. Quantum implementation and analysis of default. Cryptology ePrint Archive, Paper 2022/647, 2022. https://eprint.iacr.org/2022/647.

[15] NIST. Post-quantum crypto project. http://csrc.nist.gov/groups/ST/post-quantum-crypto/, 2016.

[16] Dustin Moody, Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Jacob Alperin-Sheriff. Status report on the second round of the nist post-quantum cryptography standardization process, 2020-07-22 2020.

[17] The transport layer security (tls) protocol version 1.3 (may 2016). https://tools.ietf.org/html/draft-ietf-tls-tls13-13, 2016.

[18] NIST. Post-Quantum Crypto Project - Round 3 Submissions. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions/, 2021.

[19] Prasanna Ravi, Anupam Chattopadhyay, and Anubhab Baksi. Side-channel and fault-injection attacks over lattice-based post-quantum schemes (kyber, dilithium): Survey and new results. *Cryptology ePrint Archive*, 2022.

[20] Prasanna Ravi, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. Generic side-channel attacks on cca-secure lattice-based pke and kems. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 307–335, 2020.

[21] Prasanna Ravi, Romain Poussier, Shivam Bhasin, and Anupam Chattopadhyay. On configurable sca countermeasures against single trace attacks for the ntt. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*, pages 123–146. Springer, 2020.

[22] Joppe W Bos, Marc Gourjon, Joost Renes, Tobias Schneider, and Christine van Vredendaal. Masking kyber: First-and higher-order implementations. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 173–214, 2021.

[23] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.

[24] Brice Colombier, Vlad-Florin Dragoi, Pierre-Louis Cayrel, and Vincent Grosso. Message-recovery profiled side-channel attack on the classic mceliece cryptosystem. Cryptology ePrint Archive, Paper 2022/125, 2022. https://eprint.iacr.org/2022/125.

[25] Qian Guo, Andreas Johansson, and Thomas Johansson. A key-recovery side-channel attack on classic mceliece. Cryptology ePrint Archive, Paper 2022/514, 2022. https://eprint.iacr.org/2022/514.

[26] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[27] Dorian Amiet, Lukas Leuenberger, Andreas Curiger, and Paul Zbinden. Fpga-based sphincs+ implementations: Mind the glitch. In *2020 23rd Euromicro Conference on Digital System Design (DSD)*, pages 229–237. IEEE, 2020.

[28] Laurent Castelnovi, Ange Martinelli, and Thomas Prest. Grafting trees: a fault attack against the sphincs framework. In *International Conference on Post-Quantum Cryptography*, pages 165–184. Springer, 2018.

[29] Matthias J Kannwischer, Aymeric Genêt, Denis Butin, Juliane Krämer, and Johannes Buchmann. Differential power analysis of xmss and sphincs. In *International Workshop on Constructive Side-Channel Analysis and Secure Design*, pages 168–188. Springer, 2018.

[30] Ward Beullens. Breaking rainbow takes a weekend on a laptop. Cryptology ePrint Archive, Paper 2022/214, 2022. https://eprint.iacr.org/2022/214.

[31] Brian Koziel, Reza Azarderakhsh, and David Jao. Side-channel attacks on quantum-resistant supersingular isogeny diffie-hellman. In *International Conference on Selected Areas in Cryptography*, pages 64–81. Springer, 2017.

[32] Aymeric Genêt, Natacha Linard de Guertechin, and Novak Kaluđerović. Full key recovery side-channel attack against ephemeral sike on the cortex-m4. In *International Workshop on Constructive Side-Channel Analysis and Secure Design*, pages 228–254. Springer, 2021.

[33] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[34] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.

[35] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):1–15, 2017.

[36] Marco Lucamarini, Zhiliang L Yuan, James F Dynes, and Andrew J Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, 2018.

[37] Jiu-Peng Chen, Chi Zhang, Yang Liu, Cong Jiang, Weijun Zhang, Xiao-Long Hu, Jian-Yu Guan, Zong-Wen Yu, Hai Xu, Jin Lin, et al. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Physical review letters*, 124(7):070501, 2020.

[38] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017.

[39] Vadim Makarov. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics*, 11(6):065003, 2009.

[40] Artem Vakhitov, Vadim Makarov, and Dag R Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of modern optics*, 48(13):2023–2038, 2001.

[41] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006.

[42] Dongjun Park, GyuSang Kim, Donghoe Heo, Suhri Kim, HeeSeok Kim, and Seokhie Hong. Single trace side-channel attack on key reconciliation in quantum key distribution system and its efficient countermeasures. *ICT Express*, 7(1):36–40, 2021.

[43] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[44] René Schwonnek, Koon Tong Goh, Ignatius W Primaatmaja, Ernest Y-Z Tan, Ramona Wolf, Valerio Scarani, and Charles C-W Lim. Device-independent quantum key distribution with random key basis. *Nature communications*, 12(1):1–8, 2021.

[45] Bruno Sanguinetti, Anthony Martin, Hugo Zbinden, and Nicolas Gisin. Quantum random number generation on a mobile phone. *Phys. Rev. X*, 4:031056, Sep 2014.

[46] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul. Maximization of extractable randomness in a quantum random-number generator. *Phys. Rev. Applied*, 3:054004, May 2015.

[47] Janusz E. Jacak, Witold A. Jacak, Wojciech A. Donderowicz, and Lucjan Jacak. Quantum random number generators with entanglement for public randomness testing. *Scientific Reports*, 10(1):164, 2020.

[48] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Rev. Mod. Phys.*, 89:015004, Feb 2017.

[49] J. Roberts, I. E. Bagci, M. A. M. Zawawi, J. Sexton, N. Hulbert, Y. J. Noori, M. P. Young, C. S. Woodhead, M. Missous, M. A. Migliorato, U. Roedig, and R. J. Young. Using quantum confinement to uniquely identify devices. *Nature Scientific Reports*, 5(16456), 2015.

[50] Koustubh Phalak, Abdullah Ash Saki, Mahabubul Alam, Rasit Onur Topaloglu, and Swaroop Ghosh. Quantum puf for security and trust in quantum computing. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 11(2):333–342, 2021.

[51] Niklas Pirnay, Anna Pappa, and Jean-Pierre Seifert. Learning classical readout quantum pufs based on single-qubit gates. *Quantum Machine Intelligence*, 4(2):14, 2022.

[52] Giulio Gianfelici, Hermann Kampermann, and Dagmar Bruß. Theoretical framework for physical unclonable functions, including quantum readout. *Phys. Rev. A*, 101:042337, Apr 2020.

[53] Myrto Arapinis, Mahshid Delavar, Mina Doosti, and Elham Kashefi. Quantum Physical Unclonable Functions: Possibilities and Impossibilities. *Quantum*, 5:475, June 2021.