The Impact of Quantum Computing on IT Security

A KVANUTMSZÁMÍTÁSTECHNIKA HATÁSA AZ INFORMATIKAI BIZTONSÁGRA

NYÁRI Norbert[1]

Abstract

Cryptography, that is the science of encryption is one of the important sub-areas of IT security, that of logical security in particular. Achieving quantum supremacy, quantum computing becoming mainstream, poses a growing threat overtime to the security of currently prevalent cryptographic algorithms.

This paper discussing quantum computing also examines what quantum dominance means and why this new technology is dangerous to the security of today's electronic information systems.

It then introduces the quantum cryptographic and quantum communication solutions currently available, and presents post-quantum cryptographic efforts around the world, including the latest studies of the US National Institution of Standards and Technology (NIST), the EU-European Union Agency for Cybersecurity (ENISA), and the NATO as well.

Keywords

IT security, cryptography, quantum computing, post quantum cryptography

Absztrakt

Az informatikai biztonság, azon belül is a logikai védelem egyik fontos részterülete a kriptográfia, vagyis a rejtjelezés tudománya. A kvantumfölény elérése, a kvantumszámítástechnika mainstream-mé válása egy olyan veszélyt jelent az aktuálisan elterjedt rejtjelező algoritmusok biztonságára, melynek bekövetkezési valószínűsége az idő előrehaladtával egyre nagyobb.

Jelen cikk a kvantumszámítástechnika tárgyalása során kitér arra is, hogy mit jelent a kvantumfölény, és miért veszélyes ez az új technológia a mai elektronikus információs rendszerek biztonságára.

Ezt követően sorra veszi a jelenleg elérhető kvantumkriptográfiai és kvantum kommunikációs megoldásokat, majd bemutatja a posztkvantum kriptográfiai törekvéseket szerte a világból kitérve az USA National Institution of Standards and Technology (NIST), az EU European Union Agency for Cybersecurity (ENISA), továbbá a NATO legfrissebb tanulmányaira is.

Kulcsszavak

informatikai biztonság, kriptográfia, kvantum számítástechnika, posztkvantum kriptográfia

[1] nyari.norbert@uni-obuda.hu | ORCID: 0000-0003-0229-7584 | doctoral candidate, Óbuda University Doctoral School on Safety and Security Sciences | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

Cybersecurity is a key factor in modern life, because either the bodies of public administration or private firms are highly bound to the electronic information systems. Such systems are considerably exposed to cyberspace threats. Information being a high-valued asset nowadays needs to be adequately protected. The goal of IT security can be summarized in the CIA principle, that is a secure electronic information system guarantees the Confidentiality, Integrity and Accessibility of the managed information. This is done through several layers of security, one of them is logical security.

Cybersecurity often relies on cryptography besides other subfields. Fundamentally cryptography aims to ensure the confidentiality, the integrity of data, the authentication of either entities or data origin, and finally the non-repudiation. So, practically speaking cryptography helps implementing the C and I from the well-known CIA principle. [1]

The term *cryptography* stems from the ancient Greek word kryptós, which means secret or hidden, and graphein meaning “to write”. [2] It is the science of information concealing methods, used in secure communication allowing the sender and the original recipient to exchange messages while outsiders being unable to get know of the contents of the messages. The contents of these messages, the information to be communicated is called *plaintext*, the encrypted message is referred with the term *ciphertext*, and we call *cipher* any method of transforming a message to conceal its meaning. The *key* is a parameter of the cipher, it must be kept secret, in some cases it is shared between the parties involved in the communication. There are usually other parameters than the key e.g., initialization vector, salt etc. that are not required to understand the article and are therefore not discussed in detail. [2]

Kerckhoff formulated basic expectations for cryptographic systems in the 19th century, some of which are still valid today. *Kerckhoffs's principles* which state that even fully disclosing everything (except the key of course) about a cryptosystem to the public should not compromise its security. Such systems are considered sufficiently safe even if it is not possible to break them by practical methods, theoretical unbreakability is not a prerequisite according to Kerckhoffs’s principles. [2] [1]

Built from well-defined *cryptographic primitives* as basic building blocks a cryptographic system (or *cryptosystem*) is providing information security services. The designer of such systems not necessarily has to be competent in the mathematical and practical considerations involved in cryptographic primitives. [1] Hereinafter I shall examine the algorithms with this level of detail.

Commonly used cryptographic primitives are following Kerckhoffs’s principles regarding unbreakability, since they are based on mathematical problems with such computational difficulties that solving them is not feasible with regular computers. Practically speaking breaking them is hard enough not to worth the effort for most of the attackers (they are lacking money, computational capacity etc.). [2] Note Kerckhoffs’s principles mentioned above.

There are several primitives, I shall cover the following types in the current article: *symmetric-key cryptography* (SKC), *Public-key cryptography* (PKC), *Cryptographic Hash Functions* (CHF), *Digital Signature* and Cryptographically Secure Pseudorandom Number

Generator (CSPRNG). Other primitives such as Mix Networks, Private Information Retrieval, Commitment Scheme are related to hard-to-trace communications and ensuring anonymity, which goes beyond the scope of this publication. [1]

Regarding to Alfred Menezes cryptosystems can be classified into five main categories regarding security: "Unconditionally security, Complexity-theoretic security, Provable security, Computational security and Ad hoc security". *Unconditionally secure* systems withstand attacks from adversaries even with unlimited computational resources, this is often called Perfect security. [1]

Complexity-theoretic security is based on a gap between efficient algorithms guaranteed for the rightful users and the computational infeasibility of breaking the cryptosystem for an attacker. [3] In this scheme attackers are modeled as having the same, feasible computational resources as rightful users. [1]

A cryptosystem is said to be *computational secure* when breaking it needs a level of computation power which exceeds the resources of an assumed attacker. *Provable security* is a subclass of Computational security, breaking such system is "as difficult as solving a well-known mathematical problem". [1] Provable security systems include the commonly used PKC algorithm RSA (Rivest, Shamir, Adleman), which I shall discuss later on.

Finally, *Ad hoc security* means the cryptosystem is safe against the attack of a known adversary with fixed resources. [1]

One more topic needs to be highlighted before I get into the details: *Quantum technology*, which is a still emerging discipline including essentially everything based on quantum mechanics. Stemming from physics and engineering quantum technology relies on the principles of quantum physics, including quantum entanglement and quantum superposition. It has many subareas including, but not limited to *quantum computing*, *quantum communications* and *quantum cryptography*. [4]

In the following I shall introduce the basic concepts of quantum computing. I then discuss cryptographic primitives considering their quantum computing threats. Finally, I review the recent NIST, ENISA and NATO studies in the topic.

QUANTUM COMPUTING

The basic unit of information in *quantum computing* is called *qubit* (or quantum bit) Qubits are defined as two-level quantum systems. The basic difference to classical computing however is that qubits can also be at any of the infinitely many intermediate levels or states between 0 and 1, unlike classical bits. [4] Theoretical *quantum computers* make it possible to use the quantum properties of qubits in order to perform quantum computations, and run quantum algorithms, allowing to perform certain operations in a completely different, and importantly, much more efficient way. [4]

Quantum supremacy or (*quantum advantage*) is an important concept. Harrow and Montanaro defines it as "when a universal quantum computer performs a computational task that is beyond the capability of any classical computer, an event known as quantum supremacy". [5] Chris Bernhardt states that the existence of a universal quantum computer with at least 72 qubits would mean quantum supremacy. [6]

There is a keyword in both above definitions that can be easily overlooked when it comes to publication of quantum computation related results: "*universal*". Articles about quantum supremacy so far are demonstrations that a concrete, programmable quantum device is capable of solving a problem with quantum algorithm, a problem which cannot be solved in feasible time with regular computers. However, this says nothing about the usefulness of the problem solved with quantum computers, yet it is important because it generates competition among IT companies that promotes technical development. I shall present examples later.

In my humble opinion a new term should be introduced cases where quantum supremacy is specific for a computational task, or it is achieved on an experimental, computation specific, that is not universal hardware. I would suggest that *quantum supremacy* should stay the way Harrow and Montaro defined it (see above), but *quantum advantage* should not be the synonym for quantum supremacy and should mean cases where the "universal" restriction would not hold.

According to ETSI White Paper No. 8 'Quantum Safe Cryptography and Security' some cryptographic algorithms are "*known to be vulnerable"* to quantum attacks and some others are "*thought to be safe"* from such attacks, that is quantum safe. Should a cryptographic primitive be well examined and proves to be resistant against known types of quantum attacks, it is regarded as quantum safe. [7]

In my understanding quantum computing poses no direct threat to cryptography at the moment because real-life quantum computers lacking the processing power for breaking cryptographic systems. Notwithstanding, cryptographers are working on finding quantum safe ways of cryptography in order to prepare for the so-called quantum apocalypse, the time of the real quantum supremacy. In my humble opinion this preparation is vital, for this new technology will fundamentally change the field of cryptography eventually breaking most of current cryptography techniques used.

SYMMETRIC-KEY CRYPTOGRAPHY

Firstly, *symmetric-key cryptography* (SKC) consists of algorithms that use the *same key* for encrypting and decrypting messages. Using the same key on both ends (encryption and decryption) is a downside, because in some *cases key distribution can be challenging*. there are two large families of algorithms in SKC: stream ciphers and block ciphers. Stream ciphers encrypt handling the message as a stream of bytes or letters (typically bytes), encrypting one byte at a time. Block ciphers take several bits and encrypt them as a single block, the length of the plain text must be a multiple of the block size, so it is padded if necessary. Commonly used SKC algorithms are AES, Twofish, Blowfish, RC4, IDEA etc. [2]

It is vital for optimal security that the used *symmetric key* has been generated using a *statistically good quality random numbers* utilizing real random generator or at least cryptographically safe pseudo random number generator (CSPRNG). [1]

However, it is worth highlighting the *OTP symmetric key algorithm* because it provides *unconditional security*. It has downsides unfortunately. In this case the length of the key must be at least equal to the length of the message. This makes key distribution even harder. [2] Let us consider a message which is 4 GB, in this case the key must be 4 GB as well, and it must be available to both ends while kept secret. There are a few restrictions though, which must be met in order to ensure the security OTP encryption, one that *it is forbidden to reuse the key*. [2]

In my understanding, OTP cannot be attacked any more efficient with quantum computers given that it is utilized properly (no repeating of keys), because *the only way to attack it is through brute force*, that is trying all the possible keys for a ciphertext. Even if the brute forcing process speeded up, the attacker would not be able to choose the original message, because brute forcing an OTP encrypted message of length n will result in the list of all the n-length possible cleartexts.

SKC algorithms can be attacked in many ways including but not limited to known-plaintext attack. The known-plaintext attack (KPA) is a cryptanalytic attack model based on the assumption that the attacker has managed to get hold of a few pairs of plaintext and its associated ciphertext. [1]

I highlight this type of attack, because in 1996 Grover presented a *quantum searching algorithm which gives a quadratic speed up to KPA attacks* against SKC algorithms, notwithstanding AES-256 is still considered quantum-safe. [8] [9]. The SKC is considered quantum secure provided that the key size is large enough, as a rule of thumb the keysize should be doubled. [8]

CRYPTOGRAPHIC HASH FUNCTIONS

Cryptographic Hash Functions are mathematical algorithms maps a *fixed length message digest* or hash to data or message of arbitrary size. There are a few restrictions though. The computation of the message *digest must be relatively quickly done*. The function must be deterministic that is, the same input must result in the same hash value. Generating a message that results in a certain hash value must be infeasible. Finding two different messages with the same message digest (*collision*) should also be *infeasible*. Even a one-bit change in the original message changes the output hash value to such an extent that the new hash value conspicuously does not correlate with the old hash value. [2] [1]

Collision is inevitable though because of the arbitrary length and number of the input and the fixed number of the output values, stemming from the fixed message digest length. [1]

Hash functions can be keyed or unkeyed. Unkeyed functions are mainly used for modification detection (MDCs), see digital signature below and keyed ones are primarily for message authentication (MACs). [1]

In the 2020 article 'Quantum Collision Attacks on AES-like Hashing with Low Quantum Random Access Memories' authors state that "The first dedicated quantum attack on hash functions was presented at EUROCRYPT 2020 by Hosoyamada and Sasaki" This attack can be performed against a specific hash algorithm AES-MMO. [10] Hosoyamada and Sasaki showed that *classically secure hash functions are potential subjects to attacks from quantum computers*. [11]

In my understanding these proposed *quantum attacks shorten the time needed* to find collisions, so increasing the *length of the message digest will strengthen hash algorithms* against quantum attacks.

PUBLIC-KEY CRYPTOGRAPHY

The third category is *Public-Key Cryptography* (PKC), which is based on the usage of keypairs. A keypair consist of *a private key and a public key*. While the public key can be securely disclosed to anyone, the private key must be kept secret. [2] Public-key cryptography is there basically many aspects in modern life such as communication between computers on networks, securing payments with credit cards etc. [2]

The PKC can be used for message encryption. In this case, the public key is used to encrypt a message for the holder of the private key. Such message can be decrypted only with the private key. In this scheme, communicating parties exchange their public keys and use them respectively. Unfortunately, *public-key encryption is much slower than symmetric-key encryption*. [2] According to Alfred Menezes "The security of many public-key cryptosystems *relies on* the apparent intractability of *computational problems"*. [1] Invented in 1978, the *RSA* algorithm is a prominent example of PKC relying heavily on either *prime factorization* or the algebraic structure of *elliptic curves*. [1]

Digital signature, the other application of PKC is much more common utilizing the *DSA* algorithm rooted in the *discrete logarithm* problem. [1]. In this scenario the holder of the private key encrypts a hash of a document and attaches the message digest to the document. Anyone who has the public key can verify if the document was signed by the holder of the private key. [2]

PKC algorithms are *computationally secure*, their security is based on the difficulty of mathematical computations like computing the factors of large integer numbers. There is no known algorithm for solving such calculation in feasible time running on regular computers. The calculation grows much more difficult (for regular computers) increasing the size of the prime factors, practically speaking increasing the key size. [2]

Mathematical problems like the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem *cannot be handled with regular computers in feasible time*, but all of them can be *easily solved with Shor's algorithm* running on a large-scale quantum computer. [12] [13]

Shor's algorithm *has been implemented* since its discovery in 1994, with the number 15 being successfully factorized in 2001 by a group at IBM with an experimental 7-qubit quantum computer. [14] In 2012 the number 21 was factorized. [15] [6]

This also shows that quantum computing is *not a direct threat* at the moment but quantum computers *breaking RSA* seems to be *a question of time*. [6]

KEY EXCHANGE AND KEY DISTRIBUTION

Key exchange or Key Establishment methods are designed to solve the previously mentioned key-distribution problem. To establish a secure communication between two parties a few things must be done in advance. They must be *agreed on a cryptographic algorithm* SKC or PKC. Using SKC both parties must have the symmetric key. In case of PKC, they must exchange their public keys. This process is known as the key exchange.

In case of PKC, the key distribution is rather simple, because as it was stated before, public keys can be safely disclosed to anyone, without the risk of compromising the secure communication. The identification of the holder of the keypair is a remaining problem though. [2]

The so-called *Public Key Infrastructure* (PKI) is aimed to solve the problem of the identification of the users utilizing *Certificate Authorities* (CA) and *Regional Authorities* (RA). A certificate is created in "chain of trust" or a "certification path". The chain of trust means that every issued certificate is signed by the level above. The chain basically consists of the root certificate, the one or more RA certificates below that, and the CA certificates on the lowest level. The root certificate is the exception regarding the signature, because it has no level above it, so it must be a self-signed certificate. [2] Practically speaking the certificate holder's identity is certified by an authority through a digital signature.

A *digital certificate* (or PKI certificate) has many usages, firstly, it is used to identify users, servers or other entities when communicating over public or untrusted networks, furthermore, to sign electronic documents or computer programs and eventually to encrypt data or communication. [2] Practically speaking the certificate proves the ownership of the public key, by storing it together in a PKI with information about the owner. The *certificate is signed digitally by the issuing CA* and the signature is attached in the certificate. [2] The X.509 standard defines the most common format for public key certificates. [2]

Currently PKI is heavily relying on PKC so it will be a main subject to large-scale quantum computer attacks in the future.

Published in 1976 the *Diffie-Hellman Key Exchange* cryptographic protocol enables communicating parties to securely *exchange secret keys* on a *public channel* even if an attacker is monitoring it. The solution of Whitfield Diffie and Martin E. Hellman is one of the first public key systems known. [2] [16] It uses prime numbers raised to determined powers to establish keys. Computing the key for an attacker from the captured network data is mathematically overwhelming, even if everything on the public channel is monitored, that is the algorithm is computationally secure. [2] [17]

Both the Diffie-Hellman Key Exchange and PKC are based on *compute-intensive* mathematical problems *significantly exceeding* the computing power of *today's computers* from an attacker perspective, including the difficulty of factoring large numbers, exponentiation, and modular arithmetic. [2] [17] As stated above these problems are easily solvable with a sufficiently powerful quantum computer. So Diffie-Hellman key exchange is neither quantum safe.

There is however a post-quantum cryptographic algorithm called *Supersingular isogeny Diffie–Hellman key exchange (SIDH)* which can be a replacement for Diffie-Hellman key exchange in the future. [18]

CRYPTOSYSTEMS

As stated, in the Introduction, *cryptosystems* are designed and *constructed using cryptographic primitives*. The overall security depends on the primitives used and the proper usage of them. [1] Needless to say, such systems are exposed to quantum attacks to the extent that their individual components.

A prominent and widely used example of cryptosystems is *Transport Layer Security (TLS)*, formerly Secure Sockets Layer (SSL), it is commonly used on TCP/IP networks to ensure privacy and data integrity in client-server communication. The latest version is TLS 1.3 effective since August 2018, it is described in detail in the RFC8446 standard. [19] The best-known form is HTTPS protocol for access websites on the Internet. [2]

Before the *creating the secure* communication *channel*, the client and server must *agree on using TLS* for the session, they establish a stateful connection by using the so-called handshake procedure utilizing *a public-key algorithm to set up various parameters* for the later used symmetric-key cipher and a *shared secret key* specific for the current session. After that *all additional network traffic* is encrypted using a *symmetric key algorithm*. Basically RSA, digital certificates and Diffie-Hellman key exchange is used for this handshake, but the standard allows other algorithms as well. [19]

Previously stated that RSA, and Diffie-Hellman are not quantum safe, so should quantum computers with high computational performance appear, there will be a serious issue around the world given that the phenomenon hits the industry unprepared.

POST-QUANTUM CRYPTOGRAPHY AND QUANTUM CRYPTOGRAPHY

The *still emerging* quantum technology holds many opportunities regarding *communication* and *cryptography*. *Post-quantum cryptography* (or quantum-safe) refers to cryptographic algorithms that are "*thought to be secure"* (that is not proven to be vulnerable) against a cryptanalytic attack by a *quantum computer*. [7] I would like to stress that the goal is not necessarily to implement cryptographic algorithms using quantum technology, but to find new ways of concealing information, whether using quantum computing or not, that can withstand even quantum attacks in the future. [6]

As previously stated, post-quantum cryptography means cryptographic primitives which can withstand attacks from large-scale quantum computers. Quantum-safe is often used as a synonym for post-quantum cryptography. Quantum cryptography means cryptographic primitives based on quantum technology. I think that the following nomenclature would describe the situation more precisely: *Post-Quantum Cryptography* should be a generic term, including all solutions that can withstand quantum attacks (quantum based or not), *quantum-safe* (or quantum-proof, quantum-resistant) should not be a synonym for quantum cryptography but mean the regular computing algorithms which can withstand quantum attacks and finally quantum cryptography meaning cryptographic primitives based on quantum technology.

Quantum Key Distribution (QKD) is currently the best known and most widely used application of quantum cryptography. According to Alfred Menezes, *Unconditional security* (provable) can be achieved against attackers based on the laws of quantum physics "provided the parties have access to (aside from the quantum channel) a conventional channel subject to only passive adversaries" [1] [20]

QKD is the process of *a key establishment* using quantum communication, that is creating a *random key* on a quantum communications channel. The channel could be fiber optics or free space. After the key establishment done with quantum communication, the key can be used for SKC algorithms e.g., OTP. There are two QKD protocols BB84 (1984) and E91 (1991). On practical level has a few setbacks though, the range of communication is limited. So far the best result on fiber optics was 12 km in December 2020 by the Indian Defence Research and Development Organization and 300 meters in free space, in March 2021, by the Indian Space Research Organization. [6] [20] [21]

QKD has *commercial implementations* as well, six companies offer QKD systems worldwide, including the Swiss company, *ID Quantique*. In 2004 the first bank transfer was carried out with QKD in Vienna, Austria, in 2007 Swiss ballot results were transmitted to the capital with QKD. [20] [21]

Regarding to the article 'The European Quantum Communication Infrastructure (EuroQCI) Initiative' "Since June 2019 all 27 EU member states signed the European Quantum Communication Infrastructure (*EuroQCI*) Declaration, signalling their commitment to the EuroQCI initiative”. The EuroQCI project aims to create a quantum communication infrastructure based on QKD *across Europe* and to facilitate quantum technology development. In parallel, member states are working on designing and implementing national quantum communication networks. [22] As for Hungary, the Quantum Information National Laboratory Hungary aims to build the Hungarian regional quantum network in order to connect to the European quantum internet. [23]

According to the current state of science, the so-called quantum apocalypse does not seriously affect symmetric cryptographic primitives. Increasing the key sizes (at least double them) however will certainly be necessary in time. [8] [13]

Today's dynamically evolving quantum computers, which still exist as *special-purpose hardware*, do not have the computational capacity yet to break real-life cryptographic algorithms. There are however several *efforts worldwide* that aim to deal with the problem of PKC not being quantum safe.

NIST (US National Institution of Standards and Technology) has a program named *Post-Quantum Cryptography Standardization* aiming to find *replacements* for current public-key algorithms, since they shall be potential subjects to quantum attacks in the not-too-distant future. As a first step, NIST, with the involvement of the cryptographic community, has begun to develop a minimum set of acceptance and evaluation criteria for the potential candidates. The submission period for post-quantum candidate algorithms ended in November 2017. The process has been through two rounds already. [24]

Round 3 candidates for standardization were announced on 22nd July 2020 with 7 finalists and 8 alternatives. According to Dustin Moody, a member of NIST PQC team, *finalists* are the “most promising algorithms we expect to be ready for standardization at the end of the 3rd round” and *alternates* are “candidates for potential standardization, most likely after another (4th) round”. [25] The candidates include 4 algorithms for PKC and Key-establishment Algorithms (with 5 alternatives) and 3 algorithms for Digital Signature Algorithms (with 3 alternatives). [26] A *virtual conference* was held June 7th-9th, 2021 where each submission team had the opportunity to give updates on their submitted algorithm. [27] The release of *draft standards* and call for public comments is *expected in 2022-2023*. [25]

ETSI (European Telecommunications Standards Institute) has a working group called “*ETSI Quantum-Safe Cryptography (QSC) working group”* aiming to “assess and make recommendations for quantum-safe cryptographic primitives, protocols, and implementation considerations”. In August 2020 ETSI released *TR 103 619* defining *migration strategies and recommendations “*for Quantum-Safe schemes and enhancing cryptography awareness”. [28]

In September 2021 ETSI supported the NIST Post-Quantum Cryptography Standardization program with *two technical reports* regarding *quantum-safe PKC,* and *quantum-safe digital signature* (ETSI TR 103 616 V1.1.1 (2021-09) "Quantum-Safe Signatures" and ETSI TR 103 823 V1.1.1 (2021-09) "Quantum-Safe Public Key Encryption and Key Encapsulation"). [29]

ISO/IEC also has a *working group* on quantum computing so as to get demands or requirements for quantum computing and establish a unified understanding of the *terminology and vocabulary* for this emerging technology. [30] [31]

In May 2021 *ENISA* (European Union Agency for Cybersecurity) published a freely available *study on the current situation* on the Post-Quantum Cryptography standardization process. [32] In the Chapter six, *Quantum Mitigation* the study offers *two proposals* that can be implemented against quantum capable adversaries. The first one is a *hybrid approach* of pre- and post-quantum cryptographic schemes, the other one suggests the *use of pre-shared keys* into all key establishment via PKC. [32]

NATO is working on two post-quantum projects under the "Science for Peace and Security (SPS) Programme" in the field of *secure communication*. "NATO partner country Malta aims to establish and implement post-quantum cryptographic solutions and protocols", with experts from the University of Malta and universities of many other partner countries including the USA, Slovakia and Spain. [33]

The aim of the other NATO project is to create an underwater *quantum communication channel* between Italy and Malta utilizing already existing optical fibers, creating the basic infrastructure for *quantum communication* between the two countries with a portable quantum station in both countries. The project also contributes to the protection of *critical infrastructures* in Malta. [33]

As for *quantum supremacy*, in 2019, a group of researchers at Google published a paper stating that they created a quantum processor that carried out a *specific calculation* in 200 seconds. The same calculation would take 10,000 years with even the best regular supercomputer. Also stating "This dramatic increase in speed compared to all known classical algorithms is an experimental realization of *quantum supremacy for this specific computational task*" [34] This is great news, it surely facilitates further research, but it is unfortunately not the quantum supremacy we wait for. In the previously suggested nomenclature, I would call this *quantum advantage*.

In 2020, a Chinese group of researchers *at University of Science and Technology of China (USTC)* also claimed to reach *quantum supremacy*. Their paper states that their quantum computer generated the certain number of samples in 20 seconds, that would take 600 million years for a classical supercomputer. [35] This is *quantum advantage* as well.

Led by the Chinese quantum physicist Pan Jianwei, *USTC* research team designed quantum computing system, called "Zuchongzhi 2.1" in October 2021, the first time for China to reach quantum supremacy in superconducting quantum computing. The *66-qubit* programmable quantum computer is stated to have a "calculation complexity more than 1 million times higher than Google's Sycamore processor". The other quantum computer prototype, "Jiuzhang 2.0", is light-based and it "can implement large-scale Gaussian boson sampling (GBS) 1 septillion times faster than the world's fastest existing supercomputer". [36] This is a great progress as well, but it proves *quantum advantage* (instead of quantum supremacy), because "Jiuzhang 2.0" is a special-purpose hardware.

In October 2021, Amazon Web Services (AWS) opened a new quantum computing facility ("AWS Center for Quantum Computing") in California. The facility, with the aim of developing and building the company's own large-scale superconducting quantum computer, has been built in cooperation with the California Institute of Technology (Caltech). The new center's team shall consist of experts from academic institutions and from Amazon supplemented by Caltech researchers. [37]

SUMMARY

As I wrote earlier, I think *some concepts need to be refined* on the subject, and these clarified terms should be used consequently, like quantum supremacy, post-quantum cryptography etc. The *ISO/IEC AWI 4879* standard on Quantum Computing Terminology and Vocabulary may make this change. [31]

Although quantum computing means *no direct threat to cryptography yet*, I think it is vital to *find post-quantum alternatives* for quantum-endangered cryptographic primitives. All efforts from standardization institutes, research groups are highly welcomed. Unfortunately, it is *not possible to estimate* when we can expect a *breakthrough* in quantum computing, but the world *must be prepared* to replace current PKC solutions when this breakthrough occurs, considering that many systems worldwide depend on digital signatures and public-key cryptography.

RESOURCES USED

[1] A. J. Menezes, Handbook of applied cryptography, CRC Press, 1996.

[2] A. S. Tannenbaum, Computer Networks, New Jersey: Pearson Education, 2003.

[3] S. Neukamm, "Complexity Theoretic Cryptography," 2005.

[4] M. A. López, Quantum Technologies - Digital transformation, social impact, and cross-sector disruption, Inter-American Development Bank (IDB), 2019.

[5] Harrow, Aram W.; Montanaro, Ashley, "Quantum computational supremacy," Nature, vol. 549, no. 7671, pp. 203-209, 2017.

[6] C. Bernhardt, Quantum Computing for Everyone, Cambridge, Massachusetts U.S.A.: MIT Press, 2019.

[7] ETSI, Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges, ETSI, 2015.

[8] D. J. Bernstein, "Grover vs. McEliece," Sendrier N. (eds) Post-Quantum Cryptography. PQCrypto 2010. Lecture Notes in Computer Science, vol. 6061, 2010.

[9] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proceedings of the twenty-eighth annual ACM symposium on the, Philadelphia, Association for Computer Machinery, 1996, pp. 212-219.

[10] Xiaoyang Dong et al., "Quantum Collision Attacks on AES-like Hashing with Low Quantum Random Access Memories," Cryptology ePrint Archive, Report 2020/1030, 2020.

[11] Akinori Hosoyamada and Yu Sasaki, "Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound," Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniquess, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II, pp. 249-279, 2020.

[12] W. P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, 1997.

[13] D. J. Bernstein, "Introduction to post-quantum cryptography," in Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography, Berlin, Springer, 2009.

[14] Vandersypen, Lieven M. K.; Steffen, Matthias; Breyta, Gregory; Yannoni, Costantino S.; Sherwood, Mark H. & Chuang, Isaac L., "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," NATURE, vol. 414, no. 20, pp. 883-887, 2001.

[15] Martín-López, Enrique; Martín-López, Enrique; Laing, Anthony; Lawson, Thomas; Alvarez, Roberto; Zhou, Xiao-Qi; O'Brien, Jeremy L., "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," Nature Photonics, vol. 6, no. 11, pp. 773-776, 2012.

[16] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, p. 644–654., 1976.

[17] A. Anastasios, "How is Diffie-Hellman Key Exchange Different than RSA?," 14 07 2020. [Online]. Available: https://www.venafi.com/blog/how-diffie-hellman-key-exchange-different-rsa. [Accessed 17 10 2021].

[18] Wikipedia, "Supersingular isogeny key exchange," 08 04 2021. [Online]. Available: https://en.wikipedia.org/wiki/Supersingular_isogeny_key_exchange. [Accessed 24 10 2021].

[19] RFC, "The Transport Layer Security (TLS) Protocol Version 1.3," 08 2018. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8446. [Accessed 20 10 2021].

[20] Wikipedia, "Quantum cryptography," 01 10 2021. [Online]. Available: https://en.wikipedia.org/wiki/Quantum_cryptography#Quantum_cryptography_beyond_key_distribution. [Accessed 24 10 2021].

[21] Wikipedia, "Quantum key distribution," 13 10 2021. [Online]. Available: https://en.wikipedia.org/wiki/Quantum_key_distribution. [Accessed 24 10 2021].

[22] European Comission, "The European Quantum Communication Infrastructure (EuroQCI) Initiative," 21 10 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci. [Accessed 31 10 2021].

[23] Quantum Information National Laboratory Hungary, "Realization of a Quantum Communication Network," [Online]. Available: https://qi.nemzetilabor.hu/research-fields/realization-quantum-communication-network. [Accessed 31 10 2021].

[24] NIST, "Post-Quantum Cryptography Standardization," 03 01 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization. [Accessed 20 10 2021].

[25] D. Moody, "NIST Status Update on the 3rd Round," [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf. [Accessed 24 10 2021].

[26] NIST, "Post-Quantum Cryptography - Round 3 Submissions," 03 01 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions. [Accessed 20 10 2021].

[27] NIST, "Third PQC Standardization Conference," 10 02 2021. [Online]. Available: https://csrc.nist.gov/events/2021/third-pqc-standardization-conference. [Accessed 24 10 2021].

[28] ETSI, "Quantum-Safe Cryptography (QSC)," [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography. [Accessed 24 10 2021].

[29] ETSI, "ETSI RELEASES TWO TECHNICAL REPORTS TO SUPPORT US NIST STANDARDS FOR POST-QUANTUM CRYPTOGRAPHY," 06 10 2021. [Online]. Available: https://www.etsi.org/newsroom/news/1981-2021-10-etsi-releases-two-technical-reports-to-support-us-nist-standards-for-post-quantum-cryptography. [Accessed 24 10 2021].

[30] IEC, "Quantum computing: the latest frontier for international standards," 03 08 2020. [Online]. Available: https://www.iec.ch/blog/quantum-computing-latest-frontier-international-standards. [Accessed 24 10 2021].

[31] ISO/IEC AWI, "ISO/IEC AWI 4879 - Information technology — Quantum computing — Terminology and vocabulary," [Online]. Available: https://www.iso.org/standard/80432.html. [Accessed 24 10 2021].

[32] ENISA, "Post-Quantum Cryptography: Current state and quantum mitigation," 03 05 2021. [Online]. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation. [Accessed 24 10 2021].

[33] NATO, "NATO works on quantum cryptography with Malta," 16 04 2019. [Online]. Available: https://www.nato.int/cps/en/natohq/news_165733.htm. [Accessed 20 10 2021].

[34] Frank Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, p. 505–510, 2019.

[35] Zhong, Han-Sen; Wang, Hui; Deng, Yu-Hao; Chen, Ming-Cheng; Peng, Li-Chao; Luo, Yi-Han; Qin, Jian; Wu, Dian; Ding, Xing; Hu, Yi; Hu, Peng , "Quantum computational advantage using photons," Science, vol. 370, no. 6523, pp. 1460-1463, 2020.

[36] Global Times, "Chinese researchers achieve quantum advantage in two mainstream routes," 26 10 2021. [Online]. Available: https://www.globaltimes.cn/page/202110/1237312.shtml. [Accessed 31 10 2021].

[37] D. Leprince-Ringuet, "AWS's new quantum computing center aims to build a large-scale superconducting quantum computer," 29 10 2021. [Online]. Available: https://www.zdnet.com/article/awss-new-quantum-computing-center-is-dedicated-to-building-a-large-scale-superconducting-quantum-computer/. [Accessed 31 10 2021].

[38] L. Buttyán and I. Vajda, Kriptográfia és alkalmazásai, Budapest: Typotex, 2005.

[39] Roetteler, Martin; Naehrig, Michael; Svore, Krysta M.; Lauter, Kristin, "Quantum resource estimates for computing elliptic curve discrete logarithms," 2017.