WP/21/71

IMF Working Paper

Quantum Computing and the Financial System: Spooky Action at a Distance?

by Jose Deodoro, Michael Gorbanyov, Majid Malaika, and Tahsin Saadi Sedik

INTERNATIONAL MONETARY FUND

 WP/21/71

IMF Working Paper

Asia and Pacific Department

Quantum Computing and the Financial System: Spooky Action at a Distance?[1]

Prepared by Jose Deodoro, Michael Gorbanyov, Majid Malaika, and Tahsin Saadi Sedik

Authorized for distribution by Shanaka J. Peiris

March 2021

Abstract

The era of quantum computing is about to begin, with profound implications for the global economy and the financial system. Rapid development of quantum computing brings both benefits and risks. Quantum computers can revolutionize industries and fields that require significant computing power, including modeling financial markets, designing new effective medicines and vaccines, and empowering artificial intelligence, as well as creating a new and secure way of communication (quantum Internet). But they would also crack many of the current encryption algorithms and threaten financial stability by compromising the security of mobile banking, e-commerce, fintech, digital currencies, and Internet information exchange. While the work on quantum-safe encryption is still in progress, financial institutions should take steps now to prepare for the cryptographic transition, by assessing future and retroactive risks from quantum computers, taking an inventory of their cryptographic algorithms (especially public keys), and building cryptographic agility to improve the overall cybersecurity resilience.

JEL Classification Numbers: O30, O33

Keywords: quantum computing, quantum-safe encryption, cybersecurity, fintech.

Author's E-Mail Address: JDeodoro@imf.org; MGorbanyov@imf.org; MMalaika@imf.org; TSaadisedik@imf.org

[1] We would like to thank, without implications, Andreas Bauer, Sonja Davidovic, Davide Furceri, Dong He, and Herve Tourpe for their helpful comments and suggestions on earlier versions of the paper; and Mariam Souleyman for excellent administrative and editorial assistance.

Table of Contents

"I cannot seriously believe in it [...]
physics should represent a reality in time and space,
free from spooky action at a distance."

Albert Einstein[2]

I. INTRODUCTION

The quantum revolution is underway, with the pace of innovations accelerating in recent years. The most notable and much discussed example of quantum technology is quantum computing—the use of quantum physics to perform calculations that are intractable for even the most powerful current and future classical supercomputers.[3] Leading technological companies have already developed working prototypes of quantum computers and provided access to them for researchers through their cloud services. Around the world, dozens of known projects are underway, from major corporations to startups and universities, to build quantum systems using different core technologies. If one of them overcomes current technological obstacles and creates a fully functional quantum computer or finds a way to use the existing models to solve practical computational tasks that are beyond the limits of conventional computers, it would have profound implications.

Quantum computing has the potential to transform the global economy and the financial sector, by accelerating scientific discovery and innovation. Fully functional quantum computers—when they appear—should revolutionize industries and fields that require significant computing power for simulations and optimizations that are too complex for conventional computers. For the financial system, quantum machines can greatly reduce the time to analyze complex risk positions or run Monte Carlo simulations, as well as increase their accuracy. Quantum computing can also speed up machine learning and artificial intelligence.

Beyond computing, quantum technologies give rise to novel ways of fast and secure data transmission (i.e., quantum Internet), which has been successfully tested, and, at least in theory, will be unbreakable. Yet another long-term prospect is quantum cryptography, which could enhance cybersecurity.

However, quantum computers would also crack many cryptographic algorithms underpinning today's cybersecurity. Algorithms enabling security of the financial system, including Internet communications, mobile banking transactions, and digital currencies and distributed ledger technologies, could become obsolete or would require a significant upgrade. For some applications it may be already too late because of retroactive risks presented by quantum computers, as any information assumed secure today can be captured and stored, and then

---

[2] Macmillan (1971, p. 158).

[3] In the literature on quantum computing, computers that process information according to classical laws of physics are referred to as classical computers, as opposed to quantum computers. In this paper, we use the terms *classical*, *conventional*, *digital*, and *traditional* computers interchangeably.

deciphered once efficient quantum computers are created.[4] In fact, almost any encrypted personal or financial message sent and recorded today may be deciphered by a powerful quantum computer in the future. Most financial institutions and regulators have not internalized these novel risks yet.

While waiting for quantum-safe encryption standards, financial system regulators can play an important role by raising awareness of potential risks. Financial institutions should take steps now to prepare for a cryptographic transition. They should assess future and retroactive risks from quantum computers, including from information that has already been captured or that may be captured now, stored and exploited years later. Financial institutions should develop plans to migrate current cryptography to quantum-resistant algorithms. As a first step, they should take an inventory of public-key cryptography used within the institution, as well as by partners and third-party suppliers. These will eventually need to be transitioned to post-quantum cryptography once standards are available. And finally, they should build *cryptographic agility* to improve the overall cybersecurity resilience going forward. Past experiences of algorithm replacements, even though much simpler than the transition to post-quantum standards, show that they can be extremely disruptive and often take years or decades to accomplish. Therefore, the time for action is now.

The rest of the paper is organized as follows. Section II describes key concepts of quantum computing, sections III and IV discuss potential benefits and risks of quantum computers, and section V summarizes the main messages and presents the way forward. To complete the picture, paper's annexes provide a glossary of technical terms (Annex I), a brief history of encryption, cryptoanalysis and digital computers (Annex II), and a description of the main cryptographic algorithms currently in use and their vulnerabilities (Annexes III and IV).

II. WHAT IS QUANTUM COMPUTING?

Quantum computing is the use of quantum phenomena such as *superposition* and *entanglement* to perform computations. The basic unit of a quantum computer is *qubit (*short for *quantum bit)*, typically realized by quantum properties of subatomic particles, like the spin of electrons or the polarization of a photon. While each bit, its counterpart in digital computers, represents a value of either zero or one, qubits represent both zero and one (or some combination of both) at the same time, a phenomenon called superposition. Quantum entanglement is a special connection between pairs or groups of quantum elements, whereas changing the state of one element affects other entangled elements instantly, regardless of the distance between them. This is a so counterintuitive phenomenon that Albert Einstein famously derided entanglement as "spooky action at a distance" (Macmillan, 1971). By entangling qubits, the number of represented states rises exponentially, making it possible to explore a huge number of possibilities instantly and conduct parallel calculations on a scale that is beyond the reach of traditional computers. Thanks to superposition and entanglement, adding just a few extra fully functioning qubits can lead to exponential leaps in processing power.

[4] These risks are known as "harvest now, decrypt later" attacks.

Theoretically, quantum computers can outpace current (and future) traditional computers, the so-called *quantum "supremacy"* or *quantum advantage*. It is possible to model quantum computers' states with traditional computers, but the resources required for it rise exponentially. One qubit can have values of zero and one at the same time and can be modeled with two traditional logical bits each holding values of zero or one. For two qubits, four traditional bits are needed; for three qubits, eight bits, and so on. To model a quantum computer with 54 qubits, one would need $2^{54} = 18{,}014{,}398{,}509{,}481{,}984$, which is about 18 quadrillion bits of traditional logical memory. As of end-2019, there was only one supercomputer in the world that had such a large memory—*Summit* (OLCF-4) supercomputer developed by IBM for Oak Ridge National Laboratory. To model a quantum computer with 72 qubits, one would need 2^{72}, about 5 Sextillion bits. This can be achieved, for example, by stacking together 262 thousand Summit-type supercomputers. A 100-qubit quantum computer would require more bits than all atoms of planet earth, and a 280-qubits would require more bits than all atoms in the known universe. These numerical examples illustrate the exponential power of quantum computers.

Quantum computers are not only more powerful, they are also fundamentally different from today's digital computers. They require different algorithms and infrastructure to solve existing and new mathematical problems. For illustration purposes, some complex computational tasks could be compared to a maze (e.g., finding the fastest route between two cities or the most efficient supply chain). This maze has multitude of ways leading nowhere and only one leading to the exit. Traditional computer tries to solve this problem the same way we might try to escape a maze—by trying every possible corridor and turning back at dead ends until we eventually find the way out. This can take very long time. But superposition allows a quantum computer to try all the possible paths at once (i.e., *quantum parallelism*). This drastically reduces the time needed to find the solution, the so-called *quantum speedup.*

The quantum speedup depends, among other things, on the computational problems and the algorithms used. Grover's and Shor's algorithms are the two best known quantum algorithms. They yield a polynomial speedup and an exponential speedup, respectively, over their classical counterparts (Kothari, 2020). A *polynomial speedup* is when a quantum computer solves a problem in time T, but a classical computer needs time T^2. For example, Grover's algorithm can solve a problem on a quantum computer with 1,000 steps that would take 1,000,000 steps on a classical computer. This type of algorithms can be used for the so-called NP-complete problems, described as looking for a needle in an exponentially large haystack (e.g., finding symmetric keys and hash functions). An *exponential speedup* is where a quantum computer takes time T but a classical computer takes time 2^T. If T is 100, there is huge difference between 100 and 2^{100}—more than all atoms of planet earth. This type of algorithms includes Shor's algorithm, which can break *asymmetric (public) keys.* Such impressive speedups are one of the most promising and compelling aspects of quantum computers.

Motivated by their potential power, researchers from leading technological companies are developing working prototypes of quantum computers. In 2019, Google engineers used their quantum machine powered by 54-qubit *Sycamore* processor—which had 53 qubits working

at that moment—to perform a specific computation task in just 200 seconds, while they estimated that the most powerful digital supercomputer available at that time would take 10,000 years to execute that task. Google engineers presented it as proof of *quantum "supremacy"*, which is the confirmation that quantum computers may perform tasks virtually impossible for traditional computers (Arute et al., 2019). A competing research team from IBM disputed Google's claims, while promoting their own quantum computers. IBM claims that Google's estimates are inaccurate, and that the world's fastest computer, *Summit*—built by IBM—could be modified to obtain the same results in about 3 days (Pednault et al., 2019), though they have not shown that in practice. Cementing claims for quantum advantage, in December 2020 a team of researchers from the University of Science and Technology of China in Hefei announced that their photon quantum computer, named *Jiuzhang*, performed in 200 seconds a calculation that on one of the most powerful supercomputers in the world would take 2.5 billion years to complete (Zhong et al., 2020). Importantly, they carried out the task on a photonic quantum computer working at room temperature.

Alongside, many other technological companies—from industry leaders to start-ups and universities—are working on quantum computers, increasing the probability of a break-through. As of January 2021, IBM has deployed 28 quantum computers for public and commercial use through its cloud services. In September 2020, IBM released a roadmap to produce a 1,000-plus qubit device called *Quantum Condor* by the end of 2023. Effectively, it means doubling or tripling the number of cubits in the quantum computer each year. Microsoft and Amazon also have launched beta versions of quantum computing cloud services—Microsoft *Azure* and AWS *Bracket*—powered by suppliers such as 1Qbit, Rigetti, IonQ, and D-Wave. Around the world, there are at least 87 known projects underway to build quantum systems using different core technologies.[5]

To reap the benefits of quantum computing, researchers need to build quantum machines that compute with lower error rates. Superposition and entanglement are fragile states. The interaction of qubits with the environment produces computation errors. Any external disturbances or noise, such as heat, light or vibrations, inevitably yanks qubits out of their quantum state and turns them into regular bits. Classical computers are also prone to random computational errors, albeit in much lower rates. By employing redundancy, error correction processes enable classical computers to produce practical, error-free computations. However, such techniques are not applicable to quantum physics because of the *no-cloning principle*: it is physically impossible to copy the running state of a qubit.

In 1994, Peter Shor proposed a theoretical quantum error correcting code, achieved by storing the information of one qubit onto a highly entangled state of several qubits. This scheme uses many ordinary qubits to create a single error-free entity: the formers are denominated as *physical qubits*, whereas the latter as *logical qubits*. But just adding more qubits might not boost a machine's performance. The frequency of errors in delicate qubits and their operations, caused by noises, tends to increase as more qubits are connected. IBM has developed the concept of *quantum volume* to measure progress in quantum computing,

[5] "Uncertainty principals: Commercialising quantum computers."—The Economist, September 26, 2020.

which adjusts the number of qubits, among other things, for error rate and the quality of connectivity between qubits.[6] IBM expects that quantum volume will be more than doubling every year. Today's quantum devices have error rates that are too high, which are one of the most pressing issues for quantum computers.

The race to build better quantum computers is intensifying, with companies using different technologies. It is possible to classify early quantum computing hardware community into two general categories or types. First, quantum computers based on the *quantum gates* and *quantum circuits* are the most similar to our current classical computers based on *logical gates*.[7] The other great family of quantum computers are *analog* quantum computers. These quantum computers directly manipulate the interactions between qubits without breaking these actions into gate operations. The best-known analog machines are *quantum annealers*. Some experimental quantum annealers are already commercially available, the most prominent example is the D-Wave processor, with over 5,000 qubits. This machine has been heavily tested in laboratories and companies worldwide, including Google, LANL, Texas A&M, USC. Companies are also using several strategies to implement physical qubits. For example, Alibaba, IBM, Google, D-Wave, and Rigetti use *superconducting qubits*, IonQ uses *trapped ion qubits*, while Xanadu and the University of Science and Technology of China are developing *photonic* quantum computers.

For the foreseeable future, quantum computers are expected to complement, not replace, classical computers. While desk quantum computers are far away, public can already have access to quantum computing through cloud services provided by companies such as IBM and D-Wave. People can use their classical computers to perform calculations on quantum computers and receive the results back on their classical computers. In the near future, quantum applications would probably be hybrid, since quantum and classical computing technologies have complementary strengths (National Academies of Sciences, 2019).

III. Potential Benefits of Quantum Computing

Quantum computers can transform the financial system, as they can solve many problems considerably faster and more accurately than the most powerful classical computers. Simulation, optimization, and machine learning (ML) are three areas where quantum computers can have an advantage over classical computers (Bouland et al. 2020; Egger et al., 2020; and Orus et al. 2019):

- Simulations: Monte Carlo-based methods. The use of simulations by the financial sector is ubiquitous. For example, Monte Carlo methods are used to price financial instruments and to manage risks. However, Monte Carlo simulations are computationally intensive, often leading to tradeoffs between accuracy and efficiency. Quantum computing could

[6] "Cramming More Power Into a Quantum Device."— IBM research blog, March 4, 2019.

[7] While the final objective is to build fully error-corrected quantum computers, an intermediate objective is to build practical commercial applications of *noisy intermediate-scale quantum* (NISQ) computers. Currently noise is present in both *quantum annealers* and NISQ types of machine, limiting the complexity of the problems that they can solve.

perform simulations such as pricing and risk management almost in real time, without the need to take unrealistic assumptions to simplify the models.

- Optimization models. Financial institutions make myriad of optimization calculations every day. For example, to determine the best investment strategy for a portfolio of assets, allocate capital, manage cash in ATM networks, or increase productivity. Some of these optimization problems are hard, if not impossible, for traditional computers to tackle. Approximations are used to solve the problems within a reasonable time frame. Quantum computers could perform much more accurate optimizations in a fraction of the time without the necessity to use approximations.
- Machine learning (ML) methods, including neural networks and deep learning. Financial institutions are increasingly using ML. Examples include estimating the risk level of loans by credit scoring and detecting frauds by finding patterns that deviate from normal behavior. However, such ML tasks face the curse of *dimensionality*. The time needed to train an ML algorithm on classical computers increases exponentially with the number of dimensions considered. Even if the classical computer can handle these tasks, it would take too much time. Quantum computers have the potential to outperform classical algorithms by accelerating ML tasks (quantum speedup), enabling them to tackle more complex analyses while increasing accuracy.

Beyond finance, quantum computing has the potential to be a catalyst for scientific discovery and innovation. An important application of quantum computing is for models of particle physics, which are often extraordinarily complex and require vast amounts of computing time for numerical simulation. Quantum computers would enable precision modeling of molecular interactions and finding optimal configurations for chemical reactions. They can transform areas such as energy storage, chemical engineering, material science, drug discovery and vaccines, simulation, optimization, and machine learning. Specifically, this would allow the design of new materials such as lightweight batteries for cars and airplanes, or new catalysts that can produce fertilizers more efficiently—a process which today accounts for over 2 percent of the world's carbon emissions (Martinis and Boixo, 2019). Quantum computers could also improve weather forecasts, optimize traffic routes and supply chains, and help us better understand climate change.

Beyond computing, quantum technologies give rise to novel ways of data transmission, storing and manipulating. Quantum networks can transmit information in the form of entangled qubits between remote quantum processors almost instantaneously (*quantum teleportation*) and securely using *quantum key distribution* (QKD). Until recently, such networks could function only in laboratory conditions, but experiments confirmed their viability for long-distance secure communications (Boaron et al., 2018). Moreover, data could be transmitted wirelessly through quantum satellite in space. Scientists in China were able to transmit data using quantum satellite launched in 2016 between mobile ground station in Jinan (in north-east China) and a fixed station in Shanghai. ICBC bank and the People's Bank of China are using satellite-based QKD for information exchanges between distant

cities, such as Beijing and Urumqi in the far north-west.[8] [9] In the Netherlands, a team from Delft University of Technology is building a network connecting four cities with quantum technology. They have demonstrated that it can send entangled quantum particles over long distances.[10] In the U.S., a consortium of major institutions led by Caltech have demonstrated sustained, high-fidelity quantum teleportation over long distances. They achieved the successful teleportation of qubits across 44 kilometers of fiber in two testbeds: the Caltech Quantum Network and the Fermilab Quantum Network.[11]

Another promising venue is quantum sensing devices. Advances have been reported in quantum radar, imaging, metrology, and navigation, which would enable greater precision and sensitivity. For example, medicine has started to reap the benefits of quantum sensors, by revolutionizing the detection and treatment of diseases. In the U.S., the Defense Advanced Research Projects Agency (DARPA) is running the Quantum-Assisted Sensing and Readout (QuASAR) program. Building on established control and readout techniques from atomic physics, it aims to develop a suite of measurement devices that could find application in the areas of biological imaging, inertial navigation and robust global positioning systems.[12]

IV. POTENTIAL RISKS OF QUANTUM COMPUTING

While quantum computing has tremendous potential to benefit the society, it brings new risks and challenges. The massive computing power of quantum machines threatens modern cryptography, with far-reaching implications for the financial stability and privacy. Quantum computers can solve what is known in complexity theory as *hard* mathematical problems exponentially faster than the most powerful classical supercomputers, potentially making today's main cryptographic standards obsolete. In particular, quantum computing has the potential to make *asymmetric cryptography* (*public-key cryptography*) obsolete, while reducing the strength of other cryptographic keys and *hashes*.

Today's cryptography is based on three main types of algorithms: *symmetric keys*, *asymmetric (public) keys*, and *algorithmic hash functions*, or *hashing* (see Annex III and IV for further descriptions). These cryptographic algorithms, for the most part, have had the upper hand in maintaining the necessary security to protect data, provide integrity checks and digital signatures. They are generally deemed secure and unbreakable with today's most advanced hardware and cryptanalysis techniques using conventional computers.

---

[8] China Reaches New Milestone in Space-Based Quantum Communications,—Scientific American, June 25, 2020.

[9] China has developed the world's first mobile quantum satellite station, NewScientist, January 10, 2020.

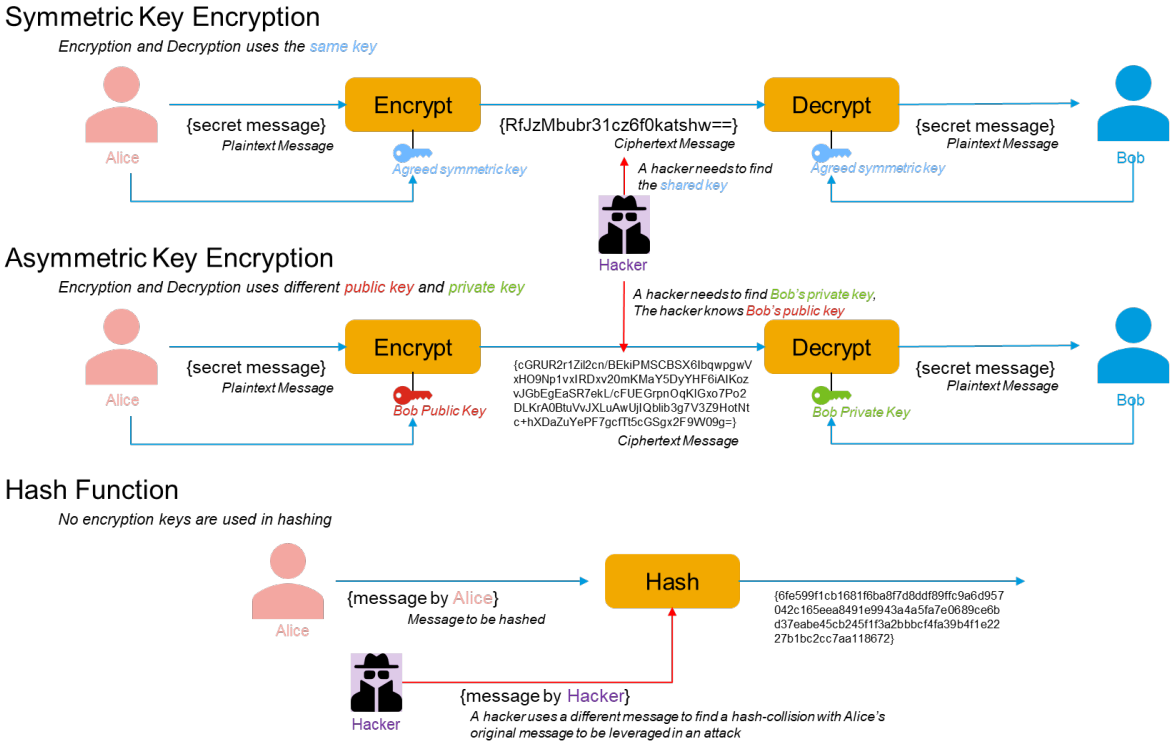
[10] Unhackable internet, MIT Technology Review, April 2, 2020.

[11] Researchers achieve sustained, high-fidelity quantum teleportation, Phys.org, December 29, 2020.

[12] https://www.darpa.mil/program/quantum-assisted-sensing-and-readout.

With symmetric-key encryption, an attacker needs to find the secret key shared between the sender and receiver to decrypt the cipher message as shown in Figure 1 (top panel).[13] Conversely, with public-key encryption, the attacker needs to find the receivers' private key, knowing their public key, to decrypt the message (middle panel). Asymmetric encryption algorithms are widely used to secure communications over the Internet. Successful attacks against these standard cryptographic algorithms would compromise secure connections, endangering the security of banking, e-commerce, and other services. With hash functions (bottom panel), an attacker would attempt to find a *hash-collision* to match the output digest with a crafted and different input, allowing to produce counterfeit authentication digests for transactions or documents.

Figure 1: Types of Cryptographic Algorithms



Source: Authors

Risks from quantum computing vary depending on the types of cryptographic algorithms:

- Symmetric cryptography, under certain conditions, is believed to be quantum resistant. Current security standards recommend the usage of AES algorithm with 256 bits keys for symmetric encryption. Known as AES 256, this algorithm is widely used for multiple purposes, such as securing Internet websites or wireless networks. An attacker would have to try 2^{256} combinations to break a 256-bit AES key using brute force, an effort that

[13] *Cryptanalysis*, the analysis of the encrypted secret message (*ciphertext*) to gain as much information as possible about the original message, studies the algorithms, mathematics and techniques to uncover the secret messages. By exploiting weaknesses in the underlying encryption methods, much can be learned about the original message without knowing the secret key (see Annex III).

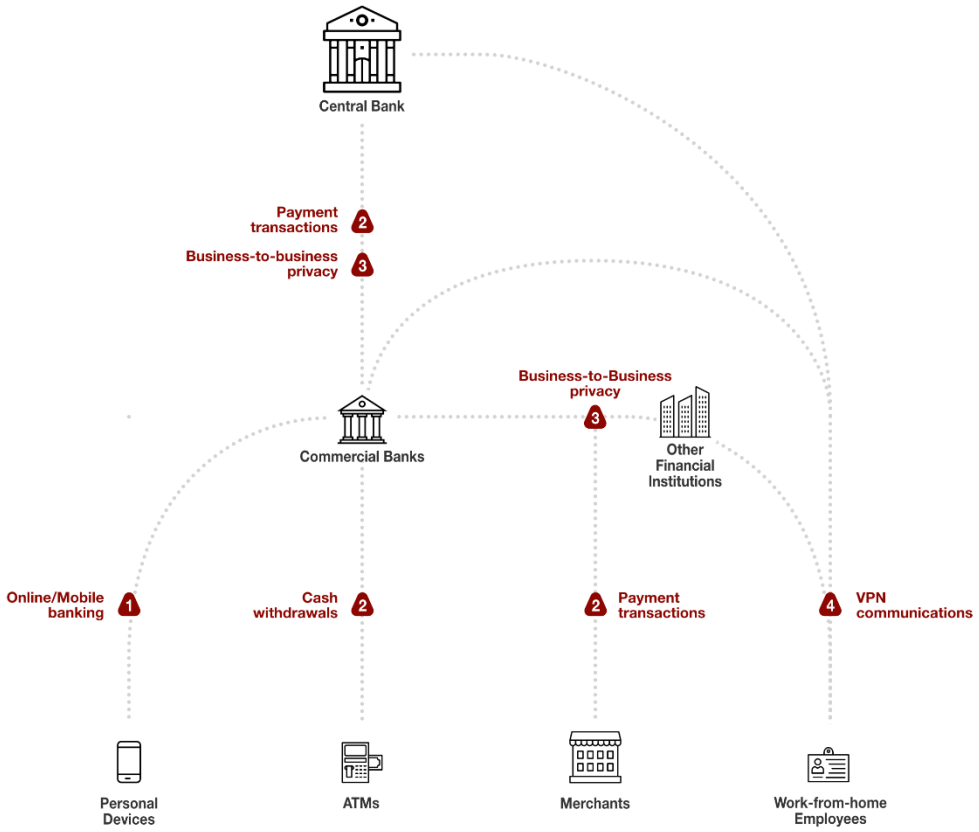
would require a timespan of over 7 billion years to be executed by a classical supercomputer, half the current age of the universe (CISA, 2019). A quantum computer may reduce the complexity of breaking symmetric encryption key by half, for example, by using Grover's algorithm (Grassl et al., 2015). However, it would still have to run for millions of years to break a single AES key using known methods. This leads most experts to believe that that algorithm is quantum resistant for now, and so are other symmetric encryption methods of the similar nature.

- Hashing functions are also believed to be quantum resistant under determined conditions. Hashing generates unique fixed-size codes according to arbitrary inputs. They are used to validate information and are leveraged in several cryptographic methods for diverse purposes, such as validating information or generating authentication codes. Their novelty stems from the quasi impossibility to reverse them. Given a determined hash code, it would take thousands of years to produce inputs that generate the same code (this is called a *collision attack*). As with symmetric cryptography, using Grover's algorithm, a quantum computer could reduce the time to reverse a hash function from 2^n to $2^{n/2}$, n being the number of bits used for the hash output. Therefore, longer hash functions like the SHA-3 family, which typically generate 256-bits outputs, are considered quantum safe and expected to remain as approved standards for now.

- Public (or asymmetric) keys, however, can become obsolete with quantum computing. Theoretically, a fully functioning quantum computer can break an asymmetric key in a few hours by using Shor's algorithm and related optimizations (Gidney et al., 2019). Furthermore, researchers believe that advancements in quantum computing will reach a level of optimization that would allow quantum computers to break today's public keys in less time than it takes to generate them using digital computers (Monz et al, 2016 and Anschuetz et al, 2018).

Critical protocols behind digital data and communication security of the financial sector rely heavily on public-key cryptography. In the age of the Internet, public keys aim to achieve critical security services underpinning the financial sector. These include (Burr and Lyons-Burke, 1999): (i) *authentication/authorization* (the ability to corroborate the identity of a party that originated particular data, transaction, or participates in a protocol); (ii) *privacy/confidentiality* (the ability to ensure that unauthorized individuals are not able to access protected data); and (iii) *integrity* (the ability to know that data has not been altered). For example, today's digital certificates and digital signatures are based on asymmetric keys. These critical security services supporting the financial sector would be compromised by a sufficiently powerful quantum computer, threatening sensitive information managed and communicated by financial institutions and central banks. Putting it simply, an attacker who can forge signatures can effectively spend other people's funds or masquerade as any entity.

Figure 2: Quantum Computing: Selected Risks to the Financial Sector



Source: Authors

Figure 2 shows some potential impacts of quantum computers on the different communication protocols used by the financial system:

1. Online/Mobile Banking. Using a quantum computer, an attacker may compromise public keys for standard Internet protocols and eavesdrop on any communications between users and financial institutions. Furthermore, an attacker may compromise the authentication and authorization schemes, whether it's *session-token* or public-key

based financial system to produce counterfeit transactions. Moreover, in the case of central bank digital currencies (CBDC) and blockchain networks, attackers may extract valid wallet keys from publicly available records, granting them the ability to appropriate of users' credits and tokens.

2. Payment Transactions and Cash Withdrawals. ATMs are connected through private networks. This makes it easy for attackers to tap into connections relying on public-key encryption and use the same venues applicable to online or mobile banking to forge transactions.
3. Business to Business Privacy. Corporate point-to-point networks also use public-key encryption to build secure channels, authenticate and authorize data exchanges between businesses. By compromising such channels, attackers would have full access to information that, once captured, would allow them easy points of entry to invade corporate internal networks, by impersonating users or servers through *man-in-the-middle* attacks. By forging certificates, for instance, attackers would be able to add their own resources to the enterprise network. Another form of attacks may be to record available encrypted data now, and decrypt it once a quantum computer is available, allowing them to reveal current trade secrets in the future, for instance.
4. VPN Communications. VPN connections are used by staff of financial institutions to work from home and to access organizational internal and sensitive resources. Such connections typically use public-key encryption to authenticate business and workstations which would be vulnerable to the same issues as the business-to-business connections.

Other applications relying on public-key cryptography include popular blockchain-based digital assets such as Bitcoin or Ethereum and password-protected web applications. The best known of these protocols is HTTPS, used by 96 percent of Internet websites (Google Report, 2020). Therefore, quantum computing is an existential threat to many business sectors that rely on asymmetric cryptography for their day-to-day operations (ETSI, 2020).

While the ability to use longer keys renders symmetric encryption and hashing quantum-safe today, they are not immune to further advances in quantum computing. As the quantum computing field becomes widely researched and understood, new schemes and algorithms emerge continuously. Shor's algorithm, for instance, has been improved several times since its inception, mainly to reduce its processing requirements. New algorithms and analysis are created that significantly lessen the quantum hardware capability needed to solve problems that go beyond the realm of classical supercomputers (Cade, 2020). It is, therefore, reasonable to assume that, as research progresses, new algorithms would be discovered to target today's advanced symmetric cryptography and cryptographic hashing functions and turning them obsolete, as in the case of public-key cryptography.

Achieving a quantum-safe environment will require a different mindset by governments, firms, and individuals. More than 50 percent of organizations, including government

agencies, admit running outdated software.[14] Past experiences with replacing the data encryption standard (DES) and various hash functions (SHA-1, MD5) suggest that it takes at least a decade to replace a widely deployed cryptographic algorithm (National Academies of Sciences, 2019). Migration to quantum-resistant algorithms is likely to be much more complex than previous experiences, given the ubiquitous use of public keys. Therefore, even if all product providers made their software quantum-resistant, public and private organizations alike would need a different approach to obsolescence management. This would be even more complicated and expensive for legacy systems that no longer have software updates issued by their manufacturers.

V. THE WAY FORWARD

We are on the threshold of the quantum computing age. Quantum computers can speed up the process of scientific discovery, from designing new materials for more efficient batteries to creating better drugs and vaccines. Quantum computers could also transform the financial system as they would solve many problems considerably faster and more accurately than the most powerful classical supercomputers. Leveraging on quantum computers' potential will also require new approaches and algorithms. This includes developing new error-correction schemes, creating new programming languages, forming communities of potential users, and developing common standards to ensure the interoperability between different quantum computing approaches and communications.

Quantum computers may also cause substantial disruptions, including undermining the financial stability. An important risk of quantum computing relates to the existing encryption algorithms that could become obsolete, especially the widely used public-key algorithms. Cryptoanalysis history is full of cautionary tales about perceived unbreakable cryptography made obsolete by new technologies (Annex II). The race has already started to develop new quantum-safe encryption standards and algorithms. For example, in the U.S., the National Institute of Standards and Technology (NIST) is running a competition for a quantum-safe encryption algorithm, targeting to announce a winner by 2024 (NIST, 2020). If fully functional quantum computers become a reality before or shortly after that, organizations (firms and governments) would have a narrow window to mitigate this risk. In Europe, the European Telecommunication Standards Institute (ETSI) is spearheading deployment of quantum-safe standards (ETSI, 2015, 2017, 2020). These works feed into activities of other standard-setting bodies such as the International Telecommunications Union (ITU) and the Internet Engineering Task Force (IETF).

While waiting for quantum resistant standards, financial system's regulators can play an important role by raising awareness of the financial community to the current and forthcoming risks and challenges. First, financial institutions should develop plans to migrate current cryptography to quantum-resistant algorithms. ETSI (2020) has outlined a framework of actions that an organization should take to enable migration to a quantum-safe

[14] "Thousands of Organizations Run the Majority of their Computers on Outdated Operating Systems, Nearly Tripling Chances of a Data Breach."—BitSight.

cryptographic state. The framework comprises three stages: (i) inventory compilation, (ii) preparation of the migration plan, and (iii) migration execution:

- Inventory compilation. An organization cannot plan migration without prior knowledge of its assets that quantum computing would affect. Thus, the first stage of migration is to identify the set of cryptographic assets (both hardware and software) and processes in the system. The framework would require managing the business process, allocating a budget and ensuring accountability. The costs could be significant, including financial, temporal, organizational and for technical provisions.

- Preparation of the migration plan. The migration plan would determine whether an asset identified in stage 1 will be migrated or retired, as some assets may become obsolete through redesign. Sequencing the migration is important given the interdependency of assets. If backwards compatibility is required during the migration, then the application will have to support both classical and quantum-safe algorithms. This may be achieved by using individual classical and quantum-safe algorithms, or by using hybrid algorithms depending on the existing cryptographic agility. For example, in November 2020, IBM announced plans to add quantum-safe cryptography to its cloud services, on top of the current standards.[15] Provisions for cryptographic agility should be considered for any new or updated cryptography. If a vulnerability is found in the quantum-safe algorithm, it may be necessary to switch to a different one, although sometimes the vulnerability may be addressed by patches and updates. Ensuring cryptographic agility will make these upgrades easier.

- Migration execution. The role of this stage is to implement the migration plan from stage 2 against the inventory from stage 1. This stage also includes mitigation management. A key element of mitigation management is conducting exercises to simulate and test the migration plan to determine its viability. These exercises are important, as they can uncover missing inventory elements (it is probable that the inventory will be incomplete).

This framework assumes an orderly, planned migration. However, immediate availability of a viable quantum computer that is used to attack public keys could require immediate transition to a quantum-safe cryptography. In this case, an emergency migration could require quick simultaneous execution of key measures outlined above.

Given the pace of innovations and uncertainty about when quantum-safe standards become available, financial institutions should build cryptographic agility. This is a property that permits smooth changing or upgrading cryptographic algorithms or parameters to improve the overall cybersecurity resilience in the future. Over the longer term, there may be a need to implement quantum cryptographic methods to reduce cybersecurity risks.

Beyond the financial stability, quantum computing raises important privacy risks, and regulators should work with industry experts to understand these risks. Regulations such as the United States Gramm-Leach-Bliley Act (Gramm-Leach, 1999), or the European's

[15] https://newsroom.ibm.com/2020-11-30-IBM-Cloud-Delivers-Quantum-Safe-Cryptography-and-Hyper-Protect-Crypto-Services-to-Help-Protect-Data-in-the-Hybrid-Era.

General Data Protection Regulation (GDPR, 2018) already guide the protection of information, but may require further scrutiny to ensure quantum-resistant encryption of data exchange and storage. Importantly, given that quantum computers represent retroactive risks, the time for action is now.

The IMF has an important role to play in raising the awareness of its members about financial stability risks from quantum computers and promoting quantum-safe standards and practices. At the multilateral level, IMF should encourage member countries to collaborate closely in developing common standards and protocols to ensure interoperability. At the bilateral level, it should encourage country authorities to develop encryption migration plans in the financial sector surveillance, for example, as part of the dialogue on ensuring operational resilience of financial institutions, markets, and infrastructure.

ANNEX I. GLOSSARY OF TECHNICAL TERMS USED IN THE PAPER

Cryptanalysis studies the encrypted secret message (**ciphertext**) to gain as much information as possible about the original message.

Cryptography is the science of transmitting secret information using public channels. A cryptologic system performs transformations on a message, the **plaintext**, and uses a key to render it unintelligible, producing a new version of the message, the **ciphertext**. To reverse the process, the system performs inverse transformations to recover the plaintext, decrypting the ciphertext (Dooley, 2018).

Cryptographic agility (or **crypto agility**) is the property that permits changing or upgrading cryptographic algorithms or parameters. While not specific to quantum computing, crypto agility would make defense against quantum computers easier by allowing substitution of today's quantum-vulnerable public-key algorithms with quantum-resistant algorithms.

HTTPS (Hypertext Transfer Protocol Secure) is a Web communication protocol used between network devices for secure communication. It encrypts both the information a user sends to a website, and the information that the website sends back—for example, credit card information, bank statements, and e-mail.

Quantum annealing is a process for finding the global minimum of a given objective function over a given set of candidate solutions (candidate states), by a process using quantum fluctuations. It finds an absolute minimum size/length/cost/distance from within a possibly very large, but nonetheless finite set of possible solutions using quantum fluctuation-based computation instead of classical computation.

Quantum computing is the use of a non-classical model of computation. Whereas traditional models of computing such as the Turing machine or Lambda calculus rely on classical representations of computational memory, a quantum computation could transform the memory into a quantum superposition of possible classical states. A **quantum computer** is a device that could perform such computation.

Quantum entanglement is a label for the observed physical phenomenon that occurs when a pair or group of particles is generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the pair or group cannot be described independently of the state of the others, even when the particles are separated by a large distance.

Quantum gate is a basic quantum circuit operating on a small number of qubits. They are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits.

Quantum key distribution (QKD) is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.

Quantum mechanics (also known as **quantum physics**, quantum theory, the wave mechanical model, or matrix mechanics) is a fundamental theory in physics which describes nature at the smallest scales, including atomic and subatomic.

Quantum superposition is a fundamental principle of quantum mechanics, where a system is in more than one state at a time. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct states.

Quantum "supremacy" is demonstrating that a programmable quantum device can solve a problem that classical computers practically cannot (irrespective of the usefulness of the problem). By comparison, the weaker **quantum advantage** is demonstrating that a quantum device can solve a problem faster than classical computers. Using the term "supremacy" has been controversial, and quantum advantage is now often used for both descriptions.[16]

Qubit or quantum bit is the basic unit of quantum information. It is the quantum version of the classical binary bit. A qubit is a two-state (or two-level) quantum-mechanical system, one of the simplest quantum systems displaying the peculiarity of quantum mechanics. It allows the qubit to be in a coherent superposition of both states/levels simultaneously, a property which is fundamental to quantum mechanics and quantum computing.

Symmetric key is an approach in **cryptography** when the same key must be used to either decrypt or encrypt a message. **Asymmetric cryptography** uses a pair of related keys, when one is used to encrypt a payload and the other to decrypt it. In **public-key cryptography**, users publish one of the keys, the **public key**, and keep the other secret, the **private key**. Then public key is used to encrypt the message and the private key is needed to decrypt it.

[16] Instead of 'supremacy' use 'quantum advantage': Nature, December 10, 2019.

ANNEX II. A BRIEF HISTORY OF ENCRYPTION, CRYPTOANALYSIS AND DIGITAL COMPUTERS

Encryption and Cryptoanalysis

Since ancient times, cryptography has been a race between those trying to keep secrets and adversaries trying to uncover them. The earliest examples of *transposition ciphers* go back to at least 485 B.C., when the Greek soldiers would wrap a strip of papyrus around a staff, a *scytale*, write a message down its length, and send off the papyrus. The receivers could unscramble messages by wrapping them around another scytale of the same thickness. In this case, the staff's shape represented the encryption *key*. The first known historical record of *substitution cipher* is from Roman Empire: Emperor *Julius Caesar* is believed to send encrypted messages to the orator Cicero replacing each letter by its third next down the alphabet. The *Caesar cipher* was broken as early as the 7th century by Arab cryptographers, who documented the techniques of cryptoanalysis, the science of undoing ciphers (Singh, 1999). In "A Manuscript on Deciphering Cryptographic Messages", the philosopher al-Kindī observed that every language has a characteristic frequency of letters and sequences and that by capturing them using sample texts of that language, the cryptanalyst might decipher any message.

Simple substitutions became obsolete in the 1700s because of the proliferation of *Black Chambers*—offices kept by European nations for breaking ciphers and gathering intelligence. As Black Chambers industrialized cryptoanalysis, cryptographers were forced to adopt more elaborated substitutions by turning to polyalphabetic methods. Instead of referring to a single alphabet for encryption, cryptographers would switch between two alphabets for choosing replacement symbols. The *Vigenère cipher,* believed to be the first polyalphabetic method and also called *Le Chiffre Indéchiffrable*, was first described in 1553 and remained popular until it was broken in the 19th century.

World War I intensified the need for secrecy. The radio had brought new capabilities to the field, such as the coordination of troops at a long distance. However, open waves also allowed enemies to listen to communications. Each nation used its own encryption methods. Some, like the *Playfair cipher* used by the British, remained unbroken during the war; others, like the German ADFGVX, were broken. In the period following the World War I, machines became the logical solution for the increase in the volume of material to decrypt. Several mechanical cryptographic devices were invented in the period preceding World War II, such as the M-94 cipher device used by the US military; the C-36 by the French Army; and the Enigma by the German Army (Dooley, 2018). Also, several devices were invented to break their encryption. To break Enigma, Alan Turing—one of the inventors of the digital computer—created *Bombes* for the British secret operation center. *Colossus*, the first programmable computer based on Turing's design, enabled the British to break the *Lorenz* cipher, which protected communications from the German high command. The US navy built fully automatic analog machines to break the cipher from Japan's Purple device.

After World War II, digital computers dominated cryptography. Whereas mechanical devices are subject to physical limitations, computers operate at a much higher speed and scramble numbers, not letters, giving access to a large set of new operations. At the beginning of the

1960s, the transistor replaced the vacuum tube in digital circuits for computers and, at the end of that decade, the Internet was invented, kick-starting the current digital age. By the early 1970s, computers became available for business customers, which demanded secrecy capabilities from vendors. As regular citizens became computer users, cryptography became necessary, for instance, to enable credit card transactions or transmission of personal information through public networks. A plethora of new cryptographic schemes appeared, leading the *American National Bureau of Standards* to intervene in 1973 and open a public competition to choose a cryptographic standard for the United States. IBM's *Lucifer* cipher, renamed *Data Encryption Standard* (DES), was elected as America's official standard in 1977. After DES was broken in a public competition in 1997, it was replaced as standard by Triple-DES in 1999, and retired when NIST adopted Advanced Encryption Standard (AES) in the early 2000s.

Until mid-1970s, all cryptographic methods used *symmetric keys*: the same key must be used to either decrypt or encrypt a message. Thus, to use cryptography, senders and receivers had to share keys in advance, a complicated matter of logistics. Whitfield Diffie, Martin Hellman, and Ralph Merkle solved the problem in 1976. The *Diffie-Hellman* key exchange allowed two parties to agree on a secret key using a public channel. The trio effectively created *asymmetric cryptography*, whereby operations are associated with a pair of related keys: when one is used to encrypt a payload, the other decrypts it and vice versa. Two years later, Rivest, Shamir and Adleman extended the concept with *public-key cryptography*, whereby users publish one of the keys, the *public key*, and keep the other secret, the *private key*. Asymmetric methods enabled new applications. For instance, people may claim their identity by showing a plaintext message and the cipher produced by their private key, which could be verified by decrypting the cipher using their public key. Asymmetric cryptography (including RSA), also known as public-key cryptography, is widely used over the Internet, including by the financial system, for key exchanges, digital signatures, non-repudiation and authentication. Public and private keys also underpin digital currencies and blockchain technologies.

Asymmetric or public-key cryptography is the most vulnerable to quantum computing. Potential advantages of quantum computers became apparent in the early 1980s, when Richard Feynman pointed out essential difficulties in simulating quantum mechanical systems on classical computers, and suggested that building computers based on the principles of quantum mechanics would allow us to avoid those difficulties (Nielsen, 2010). The idea was refined throughout the 1980s. In 1994, Peter Shor published an algorithm that would allow one to perform prime factorization much faster when using quantum properties. As prime numbers are used at the core of most asymmetrical cryptography methods, Shor's algorithm used on quantum computers might render most Internet security invalid.

While quantum computing poses a threat to Internet security, quantum mechanics can also provide unbreakable cryptography. In the 1980s, researchers from IBM proposed a novel way to leverage photon polarization to perform key distribution. By using the laws of physics, *Quantum Key Distribution* (QKD) can become impenetrable because eavesdroppers cannot intercept communications without interfering with them. Such experimental systems have been implemented since the 1990s, but they are very far from commercial use.

Digital Computers

The origin of classical computers may be traced to 17th century France. In the small town of Clermont-Ferrand, Blaise Pascal built the first machine that enabled humanity to manipulate numbers by mechanically performing the four basic arithmetic operations. Human ability to do math was enhanced again in 1822 by the English polymath Charles Babbage's *Difference Engine*. It could tabulate polynomial functions, which enabled the mechanical approximation of complex calculations such as logarithmic or trigonometric functions. Babbage also designed a general-purpose computer, the *Analytical Engine*. However, the project was terminated due to engineering and funding issues, and a working engine was never built in Babbage's lifetime. The next notable machines in history were *differential analyzers*, analog computers that use wheel-and-disc mechanisms to perform integration of differential equations. The first differential analyzer built at MIT by Vannevar Bush in 1931 played a particularly important role in history for inspiring one of Bush's graduate students, Claude Shannon. In 1938, he invented digital circuits for his master thesis (Shannon, 1938), proving that complex mathematical operations may be performed by running electricity through specific configurations of electronic components.

Shannon's work was complemented by Alan Turing's doctoral thesis. It came as an answer to the challenge produced by David Hilbert and Sir Bertrand Russel in the previous decade, the *Entscheidungsproblem*, or the halting problem: mathematicians should search for an algorithm to prove whether any statement is true in a system. The *Turing Machine* was an imaginary device composed of a mechanism that moves an infinite tape back and forth, writes symbols to it, and reads recorded symbols. The *Church-Turing thesis* then states that this device can compute any function on natural numbers as long as there is an effective method of obtaining its value. And, conversely, that such a method exists only if the device can compute that function.

Thus, engineering met mathematics: by the time Claude Shannon invented digital circuits, Turing had just designed the mathematical blueprint of a general-purpose computer. The resulting circuitry, *Turing-complete* digital computers, were capable of computing every function the imaginary machine can compute. While the *Colossus*, a war secret built by British intelligence to break Hitler's communications, was the first in history, modern computers are based on the architecture designed within a team lead by John Von Neumann, first used in 1949's EDVAC (Electronic Discrete Variable Automatic Computer). Contemporary digital devices are *Turing-complete* devices generally composed of processing units (e.g., CPU), storage devices (e.g., RAM/ROM and disk drives), and input and output mechanisms (e.g., keyboard and video). Desktop computers and smartphones follow this same design.

Once the design was invented, engineering advanced enormously in speeding up each of its components. For instance, vacuum tubes were prominent components of CPUs in early machines, needed for their singular capacity to control the direction of the flow of electrons through its terminals. However, tubes presented several challenges related to durability and reliability. They were replaced by transistors invented in the 1940s, which in turn were replaced by integrated circuits throughout the 1960s. Since then, performance and size of

digital computers have been dictated by the technology of fabrication of integrated circuits. Since the 1960s such technologies have allowed us to double the number of components in each single integrated circuit every 18 months, as foreseen by Intel's Gordon Moore in 1965—the so-called Moore's law. Such advance, for instance, is the reason we were able to cram all computing power used in the Apollo 11 lunar landing capsule in 1969 into a single device by early 2010s. Similar leaps occurred for other components, spawning things like paper-thin foldable displays, or pinhead-sized devices that can store entire encyclopedias.

However, since such machines are Turing machines at its core, they are also bound by Turing machine's limitations. One of such is their inability to tackle certain mathematical problems, the so-called NP-Hard problems. The most infamous of them is the *Traveling Sales agent problem*—calculating the shortest route through a series of cities and visiting each exactly once. Digital computers can calculate solutions for small setups, roughly by comparing all possible paths to each other. As problem size grows, mathematicians invented heuristic algorithms for finding reasonable solutions without going through all possibilities, but there is no certainty that the optimal path will be found.

As every NP-Hard problem is equivalent to the traveling sales agent, unlocking its solution would set in motion a whole new universe of possibilities, for many optimizations. This is the key held by quantum computers.

ANNEX III. MODERN CRYPTOGRAPHIC ALGORITHMS AND THEIR VULNERABILITIES TO CURRENT TECHNOLOGIES

Today's cryptography is based on three main types of algorithms: symmetric keys, asymmetric (public) keys and algorithmic hash functions, or hashing. Appendix IV lists the current and past main algorithms.

AES algorithm is currently the accepted standard for symmetric-key encryption. NIST selected it in 2001 to replace the former standard (Triple-DES). Although multiple publications introduced new cryptanalysis schemes attempting to undermine AES, the cryptographic community proved them ineffective. For example, Biryukov and others (2010) outlined an effective attack against specific variations of AES, which reduces the encryption strength. However, such attacks were deemed impractical and dismissed as a non-threat to AES encryption algorithms.

The RSA algorithm, a popular standard for asymmetric (public-key) encryption, is widely used to protect confidentiality and digital signature. The RSA algorithm has been resilient to cryptanalysis techniques since its publication in 1977, despite several attempts to challenge its strength. Earlier it was suggested that some knowledge of the plaintext message, under specific conditions, could weaken the encryption (Durfee, 2002). However, RSA algorithms continue to be resilient. Although some schemes may be used to reduce time and memory required to break public-key encryption, so far it has been proven that adequate key sizes and best practices make public-key cryptography resilient to classical computer attacks. It would take billions of years for a digital computer to break the current standard RSA 2,048-bit key (CISA, 2019).

Algorithmic hash functions were temporarily impacted by cryptanalysis, but recent progress restored their effectiveness. In 2005, the mathematician Lenstra demonstrated a hash-collision attack[17] against one of the most used hashing functions named MD5 (Lenstra et. al, 2005). Other researchers later demonstrated that a decent desktop computer equipped with a cheap graphics processor (GPU) could find a hash-collision in less than a minute. MD5 algorithm was officially retired by NIST in 2011. However, it is still widely used despite its known weaknesses, demonstrating the long-lasting issue with replacing legacy systems. NIST ran a competition to create the next standard for the algorithmic hash function named SHA-3 to overcome the cryptanalysis advancement undermining MD5 and the earlier versions of the SHA algorithms. While there are some possible weaknesses,[18] SHA-3 was selected in 2015 and became the approved standard (Morawiecki et. al, 2014). Furthermore, almost any cryptographic algorithm can be strengthened by increasing its key sizes, but that would require more processing power and thus increase the costs of running the algorithm, often making it prohibitively expensive.

---

[17] In a hash collision attack, an attacker attempts to find two inputs to the hash algorithm that would produce the same hash value. When such a collision is found, the algorithmic hash functions is deemed insecure.

[18] They described a preimage attack based on rotational cryptanalysis that reduces the algorithm rounds against SHA-3 512 bit variation. As a result, less time and memory would be required to find a hash-collision.

Beyond the encryption algorithm itself, a different class of attacks studies the exogenous systems. Side-channel attacks target the software, firmware, and hardware used to implement the encryption algorithm. Software and hardware vulnerabilities are usually easier to find and exploit compared to breaking the underlying mathematical techniques of the encryption algorithm. Vulnerabilities, or bugs, are the result of implementation mistakes during the development phases. However, some vulnerabilities may be the result of misuse or misconfiguration of the cryptographic libraries. The Heartbleed vulnerability (CMU, 2014) was a devastating example of a vulnerability discovered in OpenSSL, a widely used cryptographic library to secure network communication. (Lazar et. al., 2014) reported that 17 percent of the vulnerabilities in cryptographic libraries published by CVE[19] between 2011 and 2014 were mistakes made during the development phases while the remaining 83 percent were related to misuse or misconfiguration by the hosting applications.

[19] The Common Vulnerabilities and Exposures (CVE) is an international cybersecurity community effort to maintain a list of common identifiers for publicly known cybersecurity vulnerabilities.

ANNEX IV. MAIN CRYPTOGRAPHIC ALGORITHMS

	Symmetric Algorithms	Description	Cryptanalysis State
1	**Enigma**	The Enigma was an encryption machine built by the Nazi Germany to encrypt/decrypt messages during World War II.	The Enigma's encryption was broken in 1932 by the Polish Cipher Bureau with the assistance of the French and British allies. The Enigma had several poorly designed procedures that made reverse-engineering possible. The British used the Bombe machine to assist with breaking the encrypted messages by crunching the permutations (Tang et. al, 2018).
2	**DES**	Data Encryption Standard was developed in 1970s by IBM. A version of it was officially published as U.S. federal standard in 1977. DES key size was 56 bits.	DES was cracked in 1998 by the Electronic Frontier Foundation by building a machine named the EFF DES cracker and brute-forcing the DES key where it took the machine 3 days to find the encryption key (EFF, 1999).
3	**Triple-DES**	Triple Data Encryption Standard (Triple DES) or TDEA (Triple Data Encryption Algorithm) was introduced in 1995 due to the growing concern of DES's strength to withstand brute-force attacks. Triple-DES is still approved by the US government to protect sensitive unclassified data but under certain conditions (using three distinctive keys with certain key length).	New cryptanalysis schemes such as meet-in-the-middle attack proved effective in reducing Triple-DES key strength, deeming some variation of the algorithm insecure. NIST is deprecating Triple-DES by the end of 2023 (NIST , 2019).
4	**AES**	Advanced Encryption Standard was selected in the 1997 NIST program to develop a DES replacement. AES was introduced in 2001 by NIST and had key sizes of 128, 192, and 256 bits with 10, 12, and 14 rounds respectively.	In the early 2000s, some cryptanalysts proposed ways to break the standard, but the cryptography community proved them ineffective. In 2009 a new side-channel attack was introduced reducing the AES key strength slightly. Biryukov et al. (2010) presented an effective attack to AES 192 and 256 bit keys reducing their strengths to 176 and 22.9 bit keys respectively.
5	**Twofish**	One of the five AES finalists in the 1997 NIST program to develop a replacement to DES. While having a similar structure as DES, Twofish has been demonstrated to be efficient with memory usage and speed of encrypting/decrypting messages compared with other symmetric algorithms.	Moriai, et al. (1999) presented a truncated differential cryptanalysis of the block cipher in Twofish reducing the number of rounds to 5 from a random permutation requiring a known plaintext. The same year Ferguson (1999) presented an impossible differentials attack breaking 6 rounds of the 256 bit key version using 2^{256} steps which is faster than an exhaustive search.

	Asymmetric Algorithms	Description	Cryptanalysis State
1	**Diffie-Hellman**	Diffie-Hellman is one of the first public-key exchange methods. Named after Whitfield Diffie and Martin Hellman who published it, this algorithm was considered a breakthrough in cryptography as it enabled parties to exchange secure messages over an untrusted communication channel (Diffie et. al, 1976).	Diffie-Hellman key exchange is known to be susceptible to man-in-the-middle attacks. Newer variations of Diffie-Hellman have addressed this issue. However, Heninger (2015) discusses a method to perform precomputations for a prime number that can weaken the standard and make it less secure than widely believed.
2	**ElGamal**	ElGamal is an asymmetric key encryption based on Discrete Logarithm (El Gamal, 1985) an the Diffie-Hellman key exchange. ElGamal is widely used in the Pretty Good Privacy (PGP) email encryption system and GNU Privacy Guard (GPG), among others.	Cryptanalysis approaches against ElGamal were introduced in Allen (2008). However, the authors admit that these attacks are effective against the algorithm in certain length and key selection conditions and can be avoided by configuring the cryptosystems.
3	**Rivest–Shamir–Adleman (RSA)**	Developed and published by Rivest–Shamir–Adleman in 1977, this algorithm stems from the difficulty of factoring large integers that are the product of two large prime numbers. RSA is widely used for key establishment as well as generating and verifying digital signatures.	Initially, proposed attacks were for scenarios where the same plaintext is used with different public keys (different recipient) with access to the ciphertext. Johan Håstad found an improvement of the attack where the plaintext doesn't have to be the same, but with linear relationship among the plaintext messages. Don Coppersmith later improved this attack to gain some efficiencies (Durfee, 2002). However, proper length selection and following best practices confirms RSA's strong security.
4	**Elliptic Curve Digital Signature Algorithm (ECDSA)**	ECDSA requires smaller encryption keys compared to other asymmetric encryption algorithms. In addition, the execution time of ECDSA to encrypt/decrypt messages is faster than other asymmetric keys, and this algorithm requires less storage space and transmission bandwidth.	Proposed schemes to reduce the strength of ECDSA include Pohlig-Hellman algorithm, Pollard's Rho and the most effective Parallelized Pollard's Rho algorithm. However, best practices in randomization and key selection would deem these algorithms ineffective (Johnson et. al, 2001).
5	**Super-singular Isogeny Key Exchange (SIDH)**	In efforts to develop a quantum-safe asymmetric (public-key) cryptographic algorithm, SIDH was developed based on the conjectured difficulty of finding isogenies between supersingular elliptic curves. It is motivated by the development of a subexponential-time quantum algorithm for constructing isogenies between elliptic curves (De Feo et. al., 2011).	Galbraith et al. (2016) state that certain attacks against SIDH—such as side-channel and fault attacks—may reduce the key strength. The authors believe that the industry will see more literature and research in the cryptanalyses of SIDH in the near future as it becomes more popular and widely adopted.

	Hash Functions	Description	Cryptanalysis State
1	**MD5**	This cryptographic hash function was developed by cryptographer Ronald Rivest from MIT Laboratory for Computer Science. MD5 function produces a 128-bit long hash digest. It became an RFC#1321 standard in 1991 and was widely used for integrity checks as well as password hashing, among other sensitive functions.	Lenstra et al. (2005) demonstrated a hash-collision attack by generating two public keys with the same MF5 hash digest. Therefore, MD5 is considered a weak hash function and is no longer used for critical security functions.
2	**SHA-1**	A cryptographic hash function developed and designed in 1995 by the NSA. SHA-1 function produces a 160 bit hash digest with more rounds than MD5. SHA-1 was widely used among the major web browsers with SSL certificates.	In 2017 a group of researchers demonstrated a full collision attack against SHA-1 (Stevens et al., 2017). SHA-1 was deprecated by NIST in 2011.
3	**SHA-2**	A cryptographic hash function developed and designed in 2001 by the NSA. SHA-2 hash function can produce different digest sizes 224, 256, 384, or 512 bits with 64 or 80 rounds. SHA-2 replaced SHA-1 with SSL certificates among other secure protocols like SSH, PGP and IPSec.	Over the years, cryptographers have proposed attacks against SHA-2 reducing specific variations of the algorithm, which weakened SHA-2's strength. Dobraunig et al. (2016) used differential cryptanalysis, in addition to sophisticated search tools to maximize effectiveness with SHA-512/224 and SHA-512/256. SHA-2 is still a valid standard and is widely used.
4	**SHA-3 (Keccak)**	The latest member of the Secure Hash Algorithm selected through the NIST 2007 competition that was completed by 2015. SHA-3 (originally named KECCAK) is not a variation of its predecessor (Sha-2, SHA-1 or MD5). SHA-3's algorithm is structurally different and is based on a cryptographic sponge function (Bertoni et al., 2007). SHA-3 hash function can produce different digest sizes 224, 256, 384, and 512.	Morawiecki et al. (2014) describe a preimage attack based on rotational cryptanalysis to reduce the algorithm rounds against SHA-3 512 bit variation, which can slightly reduce the time and memory needed to break this algorithm.

REFERENCES

Allen, Bryce D. 2008. "Implementing several attacks on plain ElGamal encryption."— Graduate Theses and Dissertations, 11535. Mimeo available at https://lib.dr.iastate.edu/etd/11535.

Anschuetz, E., Olson, J., Aspuru-Guzik, A. and Cao, Y. 2019. "Variational quantum factoring". In *International Workshop on Quantum Technology and Optimization Problems* (pp. 74-85). Springer, Cham.

Arute, F., Arya, K., Babbush, R. et al., 2019. "Quantum supremacy using a programmable superconducting processor."— Nature 574, 505–510. https://www.nature.com/articles/s41586-019-1666-5#citeas.

Bertoni Guido, Joan Daemen, Michaël Peeters and Gilles Van Assche. 2007. "Sponge Functions."— ECRYPT Hash Workshop 2007, https://www.researchgate.net/publication/242285874_Sponge_Functions.

Biryukov Alex, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, Adi Shamir. 2010. "Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds."—Advances in Cryptology – EUROCRYPT 2010, pp 299-319. https://link.springer.com/chapter/10.1007/978-3-642-13190-5_15.

Boaron Alberto, Gianluca Boso,Davide Rusca, C´edric Vulliez,Claire Autebert, Misael Caloz, Matthieu Perrenoud, Ga¨etan Gras, F´elix Bussi`eres, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. 2018. "Secure quantum key distribution over 421 km of optical fiber."—July 9, 2018. Mimeo available at https://arxiv.org/pdf/1807.03222.pdf.

Bouland, Adam, Wim van Dam, Hamed Joorati, Iordanis Kerenidis, Anupam Prakash. 2020. "Prospects and Challenges of Quantum Finance": https://arxiv.org/pdf/2011.06492.pdf

Burr William and Kathy Lyons-Burke. 1999. "Public Key Infrastructures for the Financial Services Industry. Mimeo. National Institute of Standards and Technology.

Cade, Chris, Lana Mineh, Ashley Montanaro, and Stasja Stanisic. 2020. Strategies for solving the Fermi-Hubbard model on near-term quantum computers. Physical Review B.

CISA. 2019. "Understanding Encryption."—CISA, August 2019. Mimeo available at https://www.nd.gov/itd/sites/itd/files/legacy/alliances/siec/CISA%20Encryption%2028AUG19.pdf

CMU. 2014: "OpenSSL TLS heartbeat extension read overflow discloses sensitive information."—by CERT Coordination Center. Mimeo available at https://www.kb.cert.org/vuls/id/720951/.

Diffie Whitfield and Martin Hellman. 1976. “New Directions in Cryptography.”—IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976. https://ee.stanford.edu/~hellman/publications/24.pdf.

De Feo Luca, David Jao, and Jerome Plut. 2011. “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies.”—Mimeo available at https://eprint.iacr.org/2011/506.pdf.

Dobraunig Christoph, Maria Eichlseder, and Florian Mendel. 2016. “Analysis of SHA-512/224 and SHA-512/256.”—Advances in Cryptology—ASIACRYPT 2015, pp 612-630, https://link.springer.com/chapter/10.1007%2F978-3-662-48800-3_25.

Dooley, J.F. 2018. “History of Cryptography and Cryptanalysis. Codes, Ciphers, and Their Algorithms,”—Springer.

Glenn Durfee. 2002. “Cryptanalysis of RSA Using Algebraic and Lattice Methods.”—Stanford University. Mimeo available at http://theory.stanford.edu/~gdurf/durfee-thesis-phd.pdf.

EFF. 1998. “Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design.”—The Electronic Frontier Foundation (EFF), distributed by O’Reilly & Associates, inc. https://archive.org/details/crackingdes00elec.

Egger D. J. et al. 2020. “Quantum Computing for Finance: State-of-the-Art and Future Prospects,” in IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-24, 2020, Art no. 3101724, doi: 10.1109/TQE.2020.3030314.

Macmillan. 1971. “The Born-Einstein Letters: Correspondence between Albert Einstein and Max and Hedwig Born from 1916–1955, with commentaries by Max Born.” —Macmillan, 1971.

El Gamal Taher.1985. “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.”— IEEE Transactions on Information Theory, Volume: 31, Issue: 4 , Jul 1985, https://ieeexplore.ieee.org/document/1057074.

ETSI. 2015: “Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges.”—European Telecommunications Standards Institute, ETSI White Paper No. 8, June 2015. Mimeo available at https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

ETSI. 2017. “Quantum-Safe Cryptography; Quantum-Safe threat assessment.”—European Telecommunications Standards Institute, group report, March 2017. Mimeo available at https://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf.

ETSI. 2020. “CYBER; Migration strategies and recommendations to Quantum Safe schemes”. Available at: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

Ferguson, Niels. 1999. “Impossible differentials in Twofish.”—Twofish Technical Report #5, October 19, 1999. Mimeo available at https://www.schneier.com/academic/paperfiles/paper-twofish-impossible.pdf.

Galbraith et. al. 2016. Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti, “On the Security of Supersingular Isogeny Cryptosystems.”—Advances in Cryptology – ASIACRYPT 2016, pp 63-91, https://link.springer.com/chapter/10.1007%2F978-3-662-53887-6_3.

Google Report. 2020. “HTTPS encryption on the web.”—Google Transparency Report. Mimeo available at https://transparencyreport.google.com/https/overview?hl=en.

Gramm-Leach-Bliley Act. 1999. Financial Services Modernization Act of 1999, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

GDPR. General Data Protection Regulation, 2018. https://gdpr-info.eu/.

Gidney Craig and Martin Eker. 2019. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.”—December 6, 2019. Mimeo available at https://arxiv.org/pdf/1905.09749.pdf.

Grassl Markus, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. 2015. “Applying Grover’s algorithm to AES: quantum resource estimates.” Mimeo available at https://arxiv.org/pdf/1512.04965.pdf.

Heninger, Nadia. 2015. “How Diffie-Hellman Fails in Practice.”—Presentation available at https://simons.berkeley.edu/talks/nadia-heninger-2015-07-07.

Kothari, Robin. 2020. “Quantum speedups for unstructured problems: Solving two twenty-year-old problems”. Microsoft Research Blog: https://www.microsoft.com/en-us/research/blog/quantum-speedups-for-unstructured-problems-solving-two-twenty-year-old-problems/

Johnson Don, Alfred Menezes and Scott Vansto. 2001. “The Elliptic Curve Digital Signature Algorithm (ECDSA).”—Mimeo available at https://www.cs.miami.edu/home/burt/learning/Csc609.142/ecdsa-cert.pdf.

Lazar David, Haogang Chen, Xi Wang, and Nickolai Zeldovich. 2014. “Why does cryptographic software fail? A case study and open problems.”—MIT CSAIL. Mimeo available at https://people.csail.mit.edu/nickolai/papers/lazar-cryptobugs.pdf.

Lenstra Arjen, Xiaoyun Wang and Benne de Weger. 2005. "Cryptology ePrint Archive: Report 2005/067."—Mimeo available at https://eprint.iacr.org/2005/067.

Martinis John, and Sergio Boixo. 2019. "Quantum Supremacy Using a Programmable Superconducting Processor." Google AI Blog: https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html.

Morawiecki Pawe, Josef Pieprzyk, and Marian Srebrny. 2014. "Rotational Cryptanalysis of Round-reduced Keccak."—Conference Paper, July 2914. Mimeo available at https://www.researchgate.net/publication/267247045_Rotational_Cryptanalysis_of_Round-Reduced_Keccak.

Moriai Shiho, and Yiqun Lisa Yin, "Cryptanalysis of Twofish (II). 1999."—Mimeo available at https://www.schneier.com/twofish-analysis-shiho.pdf.

Monz, T., Nigg, D., Martinez, E.A., Brandl, M.F., Schindler, P., Rines, R., Wang, S.X., Chuang, I.L. and Blatt, R. 2016: "Realization of a scalable Shor algorithm". *Science*, *351*(6277), pp.1068-1070.

National Academies of Sciences. 2019. "Engineering, and Medicine: Quantum Computing: Progress and Prospects." The National Academies Press, Washington, DC.

Nielsen, M.A. and Chuang, I.L. 2010. "Quantum Computation and Quantum Information."—Cambridge University Press.

NIST. 2019. "Transitioning the Use of Cryptographic Algorithms and Key Lengths."—NIST, March 21, 2019. Mimeo available at https://csrc.nist.gov/News/2019/NIST-Publishes-SP-800-131A-Rev-2

NIST. 2020. "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process."—National Institute of Standards and Technology Internal Report 8240, July 2020. Mimeo available at https://csrc.nist.gov/publications/detail/nistir/8309/final

Orus Roman, Samuel Mugel, and Enrique Lizaso. 2019. "Quantum computing for finance: overview and prospects."—Reviews in Physics, Volume 4, November 2019. Mimeo available at https://doi.org/10.1016/j.revip.2019.100028.

Pednault, Edwin, John A. Gunnels, Giacomo Nannicini, Lior Horesh, and Robert Wisnieff. 2019. "Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits." Mimeo available at https://arxiv.org/abs/1910.09534.

Shannon, C.E.. 1938. "A symbolic analysis of relay and switching circuits." *Electrical Engineering*, *57*(12), pp.713-723.

Singh, S. 1999. “The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography,”—Doubleday Books.

Stevens Marc, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov. 2017 . “The first collision for full SHA-1.”—Cryptology ePrint Archive: Report 2017/190. Mimeo available at https://eprint.iacr.org/2017/190.

Tang Lynda, Nayoung Lee, Sophie Russo. 2018. “Breaking Enigma.”. Mimeo available at https://www.semanticscholar.org/paper/Breaking-Enigma-Tang-Lee/692ea1d3eee5f423639d36f495bc6c7f7614806c.

Zhong, Han-Sen, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen et al. 2020. “Quantum computational advantage using photons.”—Science, December 3, 2020.