Next Steps Towards the Adoption of Post-Quantum Algorithms

—

James Richard

Cleveland State University

December 5, 2022

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Quantum computing poses a unique threat to cybersecurity. Using the quirks of quantum mechanics, scientists have been able to develop algorithms that may jeopardize our national security and the security of the internet in the not-so-distant future. In particular, a quantum algorithm called Shor's algorithm has the ability to crack many of the methods currently used for public key cryptography: RSA and elliptic curve cryptography. The technology required to run Shor's algorithm at any meaningful scale does not exist yet, but the industry is rapidly progressing and we need to prepare.

Post-quantum algorithms—algorithms that are resistant to quantum attacks—are the most likely solutions to this issue. In 2016 the National Institute of Standards and Technology (NIST) began a search for these algorithms [1], and in July 2022 they announced four algorithms that they would like to include in future standardization: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+ [2]. However, the work isn't over. This report will explore the wider context behind these issues and what next steps may need to be taken in order to preserve our future cybersecurity.

1.0 INTRODUCTION

"Quantum computing" has been a buzz-phrase in popular science for a long time. Since Peter Shor published the first significant cryptographic algorithm for quantum computers in 1994 (an algorithm with the ability to break RSA keys in polynomial time[1]) [3], many academics and journalists have warned about the potential for a global collapse of cybersecurity caused by quantum computing.

Some are skeptical. In 2019, Dyakonov [4] argued that the technical hurdles scientists and engineers would need to overcome to create useful quantum processors (processors with at least $1,000$ to $100,000$ qubits[2]; experts differ on the exact threshold) are insurmountable. At that time, the largest general purpose quantum computer—Google's Bristlecone—had 72 qubits (pronounced the same as "cubits") [5]. However, we have made a lot of progress since then. On November 9th, 2022 IBM unveiled the current largest quantum computer [6], the 433-qubit IBM Osprey (shown in fig. 1) [7]. We are almost halfway to that $1,000$-qubit lower bound[3].

In addition, the quantum computing industry shows no signs of slowing down. The International Data Corporation (IDC) projects that quantum computing market will grow from $412 million in 2020 to $8.6 billion in 2027 [9]. And, in 2021, the running total of investments spent on quantum research and technology worldwide exceeded $25 billion [10]. This may not seem like much compared to other industries, but, as argued in [11], it is significant for a narrow technology that is still in development. Based on our current technological progress and market conditions, it appears that quantum computers are here to stay. For a more detailed analysis of the quantum computing market, see [12].

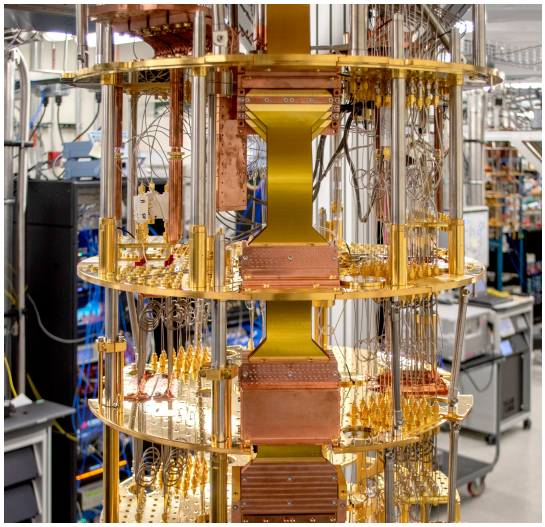

Figure 1: The IBM Osprey, a 433-qubit quantum computer [7]

National security is also a concern. Although IBM, a US-based company, appears to be leading the so called "quantum race" at the moment, we are not alone in our endeavours. Over the past four years, scientists in Germany, France, and Poland have been working on quantum computers and related research [11]. Our largest competitor, however, is China. As of 2021, our Chinese counterparts have invested the equivalent of $10 billion into quantum initiatives. That is over eight times the amount US investors

[1] In Computer Science, *polynomial time* is term that essentially means "fast." More technically, it means that as the input space of a polynomial time algorithm increases linearly, the execution time of that algorithm increases with proportion to some polynomial (as apposed to an exponential function).

[2] The quantum equivalent of a bit. We will talk more about this in section 2.2.

[3] Some may disagree with this statement, arguing that the complexity of quantum computers should increase exponentially with size (and therefore halfway is not really halfway). However, over a four year period the size of our quantum processors have increased by a factor of six; such improvements point to fast, and even exponential, growth. See Neven's Law [8].

have spent—around $1.2 billion [10]. And the Chinese have shown significant progress. Two studies published by Chinese researchers in 2021 describe their progress with a 56-qubit quantum computer called the Zuchongzi and a photonic quantum computer called the Jiuzhang 2.0 [13]. China has been long understood by the U.S. Intelligence Community as one of the greatest threats to our national security [14–16], so from a national cybersecurity perspective this is particularly concerning.

In light of these issues, how should we respond? How should we prepare our systems for the advent of powerful quantum computing? In short, the answer lies in post-quantum algorithms—classical algorithms (algorithms that run on classical computers) that are resistant to quantum attacks—and there are a variety of algorithms that may fit the bill. In 2016, the National Institute of Standards and Technology (NIST), a branch of the U.S. Department of Commerce, published a "Call for Proposals for Post Quantum Standardization" [1], and by the proposal deadline in 2017 a total of 69 algorithms had been accepted as submissions for the first round [17]. NIST evaluated these algorithms during a five-year, multi-round process, and, at then end of that process (in June 2022), they announced four winners: a general encryption algorithm called CRYSTALS-Kyber and three digital signature algorithms: CRYSTALS-Dilithium, FALCON, and SPHINCS+ [2].

Identifying these algorithms is the first but certainly not the last step to securing our systems against future quantum attacks. This report, which is intended for a general but somewhat informed audience, will provide a wider context for our current state of quantum-preparedness and examine what steps may need to be taken next in order to preserve future public safety.

2.0 A BACKGROUND ON QUANTUM COMPUTING

2.1 The Early Years

Figure 2: Attendees of the 1981 Physics of Computation conference [18]

As described in [19], quantum computing theory began to emerge in the 1980s as physicists found connections between physical (especially thermodynamic) systems, the theory of information, and computing. Yuri Manin and Paul Benioff were among the first to describe machines similar to quantum computers, but other physicists including Richard Feynman, Tommaso Toffoli,

and John Archibald Wheeler quickly followed up on their ideas, narrowing them down and solidifying what we now think of today as a quantum computer. Many of those physicists' publications (which followed the 1981 Physics of Computation conference) can be found in the 1982 issues of the *International Journal of Theoretical Physics*.

2.2 The Theory

Quantum computing is a complicated and often confusing field; I will attempt to summarize the relevant points here, but for a deeper understanding I would recommend taking a class, reading Dr. Ryan O'Donnell's lecture notes for his class on quantum computation and information (which was taught at Carnegie Mellon University) [20], or using some other resource.

2.2.1 Superposition and entanglement

Quantum computing relies on the existence of two fundamental properties: superposition and entanglement. Superposition describes the ability of an object (or more generally a system) to be in multiple states at the same time. For example, a qubit may be in two states (represented by the numbers 0 and 1) at once. Mathematically, the superposition of this qubit is described as a linear combination of states:

$$z_0|0\rangle + z_1|1\rangle \tag{1}$$

In this expression, the states 0 and 1 are represented by $|0\rangle$ and $|1\rangle$, respectively, and the weights, or *amplitudes*, of the linear combination are represented by z_0 and z_1. We use the letter z because these amplitudes are complex[4]. Before we continue, some more terminology: the notation used for this kind of expression is called bra-ket notation, and the $|...\rangle$ symbols are called kets.

When a qubit is measured, only a single state can be read. The probability that any given state will be measured is the absolute square of that state's amplitude, and, by extension, the squares of the amplitudes of a superposition must add up to one. For example, the superposition of a qubit with a 50% chance of collapsing to 0 and a 50% chance of collapsing to 1 could be represented by the equation below. Because amplitudes can be complex, however, this is not the only solution.

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

In some cases two or more objects may share a single superposition. For example, a superposition shared by two qubits (let's call them qubit A and qubit B) could be represented by the expression

$$z_{00}|00\rangle + z_{01}|01\rangle + z_{10}|10\rangle + z_{11}|11\rangle$$

where $|00\rangle$ represents the state $A = 0$, $B = 0$, $|01\rangle$ represents the state $A = 0$, $B = 1$, etc. If this expression is irreducible (i.e. it cannot be broken into smaller expressions following the form of eq. (1)), the amplitudes and probabilities associated with each qubit are dependant on each other. In other words, they are entangled.

[4]Complex numbers are numbers that follow the form $a + bi$ where $i = \sqrt{-1}$. They are a superset of the real numbers.

Superposition and entanglement are fundamental to the theory of quantum mechanics, and, although they are strange concepts, they have strong experimental evidence. Superposition is supported by the double-slit experiment and Dirac's three polariser experiment [21], and entanglement is supported by the experimental violations of Bell's inequality [22, 23]. However, it is important to note that physicists vary widely on how these experiments should be interpreted.

2.2.2 Computing with qubits

Quantum computing is generally achieved by sequentially applying logic gates to a group of entangled[5] qubits (which can be done without actually measuring the values of those qubits). Each logic gate modifies the superposition of those qubits, and at the end of the process we are left with a superposition that can be statistically measured and interpreted.

There are many types of gates involved in quantum computation; some operate pretty much like normal AND, OR, and XOR logic gates. Others change qubit properties like phase and basis. However, they must all be reversible. If they are not, information must be lost, and because of the laws of thermodynamics that lost information will get converted into heat. This is not an issue for normal computers because they are used to working at room temperature. Quantum computers, however, operate at near absolute zero temperatures, and any excess heat in the quantum processor will add noise to the output.

2.3 Applications

One of the main motivations for the development of quantum computing, as described by Richard Feynman during the keynote speech of the Physics of Computation conference in 1981 [25], was and still is the ability that quantum computers have to simulate quantum systems. The probabilistic nature of quantum systems make it time consuming and often impractical for classical computers to simulate with accuracy. However, using quantum computers, we can simulate physics with physics. This is beneficial for physicists, but also for researchers in fields including chemistry, biology, and drug discovery. For information on our current progress within this field, see [26].

More than a decade after Feynman's talk, in 1994, Peter Shor invented the first cryptographic quantum algorithm. Shor's algorithm is significant because of its ability to break certain types of encryption, but breaking encryption is not the only application for quantum computing in cryptography. Many are researching ways to encrypt data using quantum computers and distribute private keys using quantum entanglement [27].

Quantum computing also has applications in finance [28] and artificial intelligence [29].

2.4 Hardware Advances

The first quantum computer, which operated using nuclear magnetic resonance (NMR), was built in 1998. It had 2 qubits and was used to solve Deutsch's problem [30] and run Grover's algorithm (see section 3.2) on a trivially small four-state system [31]. Several other quantum computers using NMR were built over the next few years, including a 5-qubit computer at the Technical University of Munich [32] and a 7-qubit computer at the Los Alamos National Labratory [33].

[5] Entanglement is not always required. See [24]

Since then, a lot of other methods for building quantum computers have been invented. In 1999, Nakamura, Pashkin, and Tsai showed that a superconducting circuit could be used as a qubit [34]. Knill, Laflamme, and Milburn showed in 2000 that single photons could be used to do quantum computations [35]. In 2003, another group of scientists implemented the Deutsch-Jozsa algorithm (which solves Deutsch's problem) on an ion trap processor, which uses charged particles suspended in an electromagnetic field [36].

Most of today's large quantum computers use qubits made from superconducting loops [37]. Trapped ions also show promise, but are difficult to scale with our current technology. See [38] for more detail on our current progress and challenges with trapped ion technology.

3.0 QUANTUM THREATS AGAINST CRYPTOGRAPHIC SYSTEMS

3.1 Shor's Algorithm

Even though it was invented in the 1990s, Shor's algorithm is still the most significant cryptographic quantum algorithm to date. Through the use of some qubits and a lot of clever mathematics, Shor's algorithm can be used to break RSA encryption (a public key algorithm that has been widely used in the past but is now falling out of favor [39]) and elliptic curve cryptography (a method that many are using to replace RSA) [40]. If actualized, this would be devastating for internet security.

3.2 Grover's Algorithm

Grover's algorithm is another quantum algorithm that could potentially cause some security issues. It provides a quadratic speed up over classical algorithms that brute force[6] "black-box" or "one-way" functions (functions whose inverse is difficult to calculate). This includes hash functions and symmetric keys[7]. For example, it would normally take 2^{128} iterations to brute force a 128-bit symmetric key, but Grover's algorithm can do it in $\sqrt{2^{128}} = 2^{64}$ iterations. A quadratic speed up is not enough to transform exponential algorithms into polynomial ones, however, and because of this Grover's algorithm is not really a game changer. Security can be maintained by simply doubling key length (i.e. 128-bit keys should replaced by 256-bit keys when 128 bits of security is required) [41].

4.0 NIST'S POST-QUANTUM ALGORITHMS

As was mentioned in the introduction, post-quantum algorithms may be the solution that fixes these security vulnerabilities. So far the NIST has identified four post-quantum algorithms that it would like to include in a future update of its cryptography standards: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+. Three out of these four algorithms (CRYSTALS-Kyber,

[6] A word which here means "try every possibility until an answer is found."

[7] Symmetric keys are encryption keys that can be used to both encrypt and decrypt messages. In order to preserve security, these keys must kept secret (unlike the public keys in RSA).

CRYSTALS-Dilithium, and FALCON) are based on mathematical structures called lattices. SPHINCS+ is based on hashing [2].

CRYSTALS-Kyber, described as a general purpose encryption algorithm in [2], is a key encapsulation mechanism (KEM)—an algorithm used to share symmetric keys between parties using public key cryptography. The other algorithms focus on digital signatures (cryptographic tools that are used to verify the origin of data).

5.0 THE DIFFICULTY OF IMPLEMENTATION

5.1 Key Sizes and Computation Time

One of the main practical differences between post-quantum algorithms and the algorithms commonly used today is that the post-quantum algorithms tend to use larger key sizes and take more time or processing power to run. For example, table 1 compares the secret key sizes of CRYSTALS-Kyber with RSA. Table 2, as presented in [42], compares the duration of TLS handshakes[8] that use CRYSTALS-Kyber and SPHINCS+ and the duration of TLS handshakes that use ECDHE-ECDSA, a widely used algorithm based on elliptic curves. These results were benchmarked on a Raspberry Pi 3 Model B+ (RPi3), an ESP32-PICO-KIT V4 (ESP32), and a Fieldbus Option Card (FOC).

Equivalent Symmetric Key Size (in bits)[9]	CRYSTALS-Kyber		RSA	
	Variation	Secret Key Size (in bits)	Variation	Secret Key Size (in bits)
128	Kyber-512	13056	RSA-3072	3072
192	Kyber-768	19200	RSA-7680	7680
256	Kyber-1024	25344	RSA-15360	15360

Table 1: The secret key sizes of equivalently secure CRYSTALS-Kyber and RSA variations

Cipher Suite	RPi3	ESP32	FOC
Server			
KYBER-SPHINCS+-SHA-256	840 ms	23,000 ms	52,000 ms
KYBER-SPHINCS+-SHAKE-256	5,100 ms	64,000 ms	200,000 ms
ECDHE-ECDSA	43 ms	890 ms	4,400 ms
Client			
KYBER-SPHINCS+-SHA-256	67 ms	970 ms	2,300 ms
KYBER-SPHINCS+-SHAKE-256	240 ms	2,800 ms	9,000 ms
ECDHE-ECDSA	49 ms	1,100 ms	5,700 ms

Table 2: Comparison of handshake runtime for different cipher suites (rounded to two significant figures), as presented in [42]

[8] A part of the HTTPS protocol; it is used by all modern web traffic.

[9] This metric is often used to compare the security of various keys and algorithms.

If these tables are to be believed, switching from our current algorithms to post-quantum algorithms could prove to be an issue for programs that require small keys and fast processing times, including the programs that run on Internet of Things (IoT) devices. This is not to say that it cannot be done. However, more thought will have to be put into the selection and implementation of post-quantum algorithms for environments with limited resources.

5.2 Algorithm Complexity

The mathematical complexity of these algorithms may also be problematic for those implementing them. Hekkala et al. [43] implemented and tested the performance of two general purpose KEM algorithms, CRYSTALS-Kyber and SABER, along with the digital signature algorithm CRYSTALS-Dilithium. SABER, which is another lattice-based algorithm, was also submitted to the NIST but did not win. They found that these algorithms were incredibly hard to understand and implement—a lot more so than RSA. In fact, they had to use reference implementations created by the inventors of these algorithms. In addition, the non-deterministic nature of some of these algorithms made their implementations quite hard to debug.

6.0 CONCLUSIONS

Transitioning to post-quantum algorithms will not be easy, but it is possible. When asked by Davide Castelvecchi during an interview in 2020, Peter Shor said that he "thinks the only obstruction to replacing RSA with a secure post-quantum cryptosystem will be will-power and programming time" [44]. However, he also said that there is a risk for complacency because the amount of will-power and programming time that will be required for this transition is enormous—comparable even to the effort spent on fixing the Y2K bug.

6.1 Learning from the Past

The millennium, of Y2K, bug (Y2K stands for the year 2000) was caused by an issue fundamental to the way dates were stored on computers back in the 20th century. Only the last two digits of the year were stored; 1980 would be stored as "80" and 1995 would be stored as "95." Many worried that, when the year 2000 came around, computer systems would crash on a global scale because of interpreting the digits "00" as the year 1900 instead of the year 2000.

An enormous amount of effort was put into fixing this bug. The Garner Group estimated that between $300 and $600 billion was spent world wide on this issue [45]. In 1998, the 105th Congress passed a bill that promoted the sharing of information so that Y2K bugs in various computer systems could be fixed more efficiently [46].

When the year 2000 finally came, a computer billed a customer for century's worth of late fees [47] and the medical tests for 150 women were calculated incorrectly [48]. However, nothing happened at a global scale. Because of this, some doubt that the Y2K bug was ever a significant issue.

Others vehemently disagree, arguing that the Y2K bug was largely averted because of the work of so many programmers [49]. In 1999, programmers attempted to remove the Y2K bug from the computer systems at a nuclear power plant in Pennsylvania. They missed something, however,

and when they tested in the plant's entire digital monitoring system crashed (there was an analog backup, thankfully) [50]. We will never know what would have truly happened if the international community hadn't rallied together to fix this issue, but I am glad that they did.

6.2 Moving Forward

A lot more work is needed—more research, more testing, and more programming. I would argue that the best way to do this is to follow the example that we set two decades ago: by encouraging the cooperation of companies, non-profit organizations, universities, governments, and the wider open source community. It will require the contribution of many skilled researchers, mathematicians, and programmers to transition our computer systems to use algorithms that can resist the attacks of the quantum computers that will some day be built.

7.0 FURTHER READING

For more information on the current state of quantum computing, I would recommend reading Laszlo Gyongyosi and Sandor Imre's "A Survey on quantum computing technology" [51] or Gill, et al.'s "Quantum computing: A taxonomy, systematic review and future directions" [52].

"Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" [53] explores many of the same issues presented in this paper. In addition to post-quantum cryptography, it considers quantum-key distribution (QKD)[10] as a potential solution to the cybersecurity risks posed by quantum computers.

[10] QKD uses entanglement to distribute symmetric keys.

REFERENCES

[1] "NIST Asks Public to Help Future-Proof Electronic Informatiom". In: *National Institute of Standards and Technology* (Dec. 20, 2016). URL: https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information (visited on 11/25/2022).

[2] "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms". In: *National Institute of Standards and Technology* (July 5, 2022). URL: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (visited on 11/25/2022).

[3] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[4] Mikhail Dyakonov. "When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing". In: *Ieee Spectrum* 56.3 (2019), pp. 24–29.

[5] David Shaw. "Quantum Outlook 2019". In: *Fact Based Insight* (Dec. 17, 2018). URL: https://www.factbasedinsight.com/quantum-outlook-2019/ (visited on 11/23/2022).

[6] Karmela Padavic-Callaghan. "IBM unveils world's largest quantum computer at 433 qubits". In: *New Scientist* (Nov. 9, 2022). URL: https://www.newscientist.com/article/2346074-ibm-unveils-worlds-largest-quantum-computer-at-433-qubits/ (visited on 11/22/2022).

[7] *IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two*. IBM. Nov. 2022. URL: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two (visited on 11/23/2022).

[8] Kevin Hartnett. "A New Law to Describe Quantum Computing's Rise?" In: *Quanta Magazine* (June 18, 2019). URL: https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/ (visited on 11/23/2022).

[9] "IDC Forecasts Worldwide Quantum Computing Market to Grow to $8.6 Billion in 2027". In: *International Data Corporation* (Nov. 29, 2021). URL: https://www.idc.com/getdoc.jsp?containerId=prUS48414121 (visited on 11/23/2022).

[10] "Overview on quantum initiatives worldwide – update mid 2021". In: *Qureca* (July 19, 2021). URL: https://www.qureca.com/overview-on-quantum-initiatives-worldwide-update-mid-2021/ (visited on 11/23/2022).

[11] Wiktor Sędkowski. "Quantum Race". In: *Warsaw Institute* (Nov. 22, 2021). URL: https://warsawinstitute.org/quantum-race/ (visited on 11/22/2022).

[12] Evan R. MacQuarrie et al. "The emerging commercial landscape of quantum computing". In: *Nature Reviews Physics* 2.11 (Oct. 2020), pp. 596–598. DOI: 10.1038/s42254-020-00247-5. URL: https://doi.org/10.1038%2Fs42254-020-00247-5.

[13] Charles Choi. "Two of World's Biggest Quantum Computers Made in China". In: *IEEE Spectrum* (Nov. 6, 2021). URL: https://spectrum.ieee.org/quantum-computing-china (visited on 11/23/2022).

[14] *Annual Threat Assessment of the U.S. Intelligence Community*. Office of the Director of National Intelligence. URL: https://www.intelligence.gov/annual-threat-assessment (visited on 11/23/2022).

[15] Brooke Singman. "China poses 'biggest long-term threat to economic and national security,' FBI Director Wray warns". In: *Fox News* (July 6, 2022). URL: https://www.foxnews.com/politics/china-poses-biggest-long-term-threat-economic-national-security-fb-director-wray-warns (visited on 11/23/2022).

[16] Cassie Buchman. "What are the biggest threats to US national security?" In: *News Nation* (Aug. 2, 2022). URL: https://www.newsnationnow.com/world/biggest-threats-to-u-s-national-security/ (visited on 11/23/2022).

[17] *Post Quantum Algorithms: Round 1 Submissions*. National Institute of Standards and Technology. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions (visited on 11/25/2022).

[18] "Celebrating the 40-year anniversary of the Physics of Computation Conference". In: *IBM Research* (Mar. 15, 2021). URL: https://research.ibm.com/blog/qc40-physics-computation (visited on 12/03/2022).

[19] "40 years of quantum computing". In: *Nature Reviews Physics* 4.1 (Jan. 2022), pp. 1–1. ISSN: 2522-5820. DOI: 10.1038/s42254-021-00410-6. URL: https://doi.org/10.1038/s42254-021-00410-6.

[20] Ryan O'Donnell. *Lecture Notes for 15-859BB: Quantum Computation and Information*. Carnegie Mellon University. 2015. URL: https://www.cs.cmu.edu/~odonnell/quantum15/ (visited on 11/26/2022).

[21] Paul Adrien Maurice Dirac. *The principles of quantum mechanics*. 27. Oxford university press, 1981.

[22] S. Goldstein et al. "Bell's theorem". In: *Scholarpedia* 6.10 (2011). revision #91049, p. 8378. DOI: 10.4249/scholarpedia.8378.

[23] Johannes Handsteiner et al. "Cosmic Bell Test: Measurement Settings from Milky Way Stars". In: *Phys. Rev. Lett.* 118 (6 Feb. 2017), p. 060401. DOI: 10.1103/PhysRevLett.118.060401. URL: https://link.aps.org/doi/10.1103/PhysRevLett.118.060401.

[24] Ben P Lanyon et al. "Experimental quantum computing without entanglement". In: *Physical review letters* 101.20 (2008), p. 200501.

[25] Richard P. Feynman. "Simulating physics with computers". In: *International Journal of Theoretical Physics* 21.6 (June 1982), pp. 467–488. ISSN: 1572-9575. DOI: 10.1007/BF02650179. URL: https://doi.org/10.1007/BF02650179.

[26] Andrew J. Daley et al. "Practical quantum advantage in quantum simulation". In: *Nature* 607.7920 (July 2022), pp. 667–676. ISSN: 1476-4687. DOI: 10.1038/s41586-022-04940-6. URL: https://doi.org/10.1038/s41586-022-04940-6.

[27] Li Xi-Han et al. “Quantum secure direct communication with quantum encryption based on pure entangled states”. In: *Chinese Physics* 16.8 (2007), p. 2149.

[28] Román Orús, Samuel Mugel, and Enrique Lizaso. “Quantum computing for finance: Overview and prospects”. In: *Reviews in Physics* 4 (2019), p. 100028. ISSN: 2405-4283. DOI: https://doi.org/10.1016/j.revip.2019.100028. URL: https://www.sciencedirect.com/science/article/pii/S2405428318300571.

[29] Charles Q. Choi. “AI Fuses With Quantum Computing in Promising New Memristor”. In: *IEEE Spectrum* (Apr. 13, 2022). URL: https://spectrum.ieee.org/quantum-memristor (visited on 12/01/2022).

[30] Jonathan A Jones and Michele Mosca. “Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer”. In: *The Journal of chemical physics* 109.5 (1998), pp. 1648–1653.

[31] Isaac L. Chuang, Neil A. Gershenfeld, and Mark Kubinec. “Experimental Implementation of Fast Quantum Searching”. In: *Physical Review Letters* 80 (1998), pp. 3408–3411.

[32] R. Marx et al. “Approaching five-bit NMR quantum computing”. In: *Phys. Rev. A* 62 (1 June 2000), p. 012310. DOI: 10.1103/PhysRevA.62.012310. URL: https://link.aps.org/doi/10.1103/PhysRevA.62.012310.

[33] “Scientists make seven-bit quantum leap in computer research”. In: *MIT News* (Mar. 29, 2000). URL: https://news.mit.edu/2000/quantum-0329 (visited on 12/03/2022).

[34] Y. Nakamura, Yu. A. Pashkin, and J. S. Tsai. “Coherent control of macroscopic quantum states in a single-Cooper-pair box”. In: *Nature* 398.6730 (Apr. 1999), pp. 786–788. ISSN: 1476-4687. DOI: 10.1038/19718. URL: https://doi.org/10.1038/19718.

[35] E. Knill, R. Laflamme, and G. Milburn. *Efficient Linear Optics Quantum Computation*. 2000. DOI: 10.48550/ARXIV.QUANT-PH/0006088. URL: https://arxiv.org/abs/quant-ph/0006088.

[36] Stephan Gulde et al. “Implementation of the Deutsch–Jozsa algorithm on an ion-trap quantum computer”. In: *Nature* 421.6918 (Jan. 2003), pp. 48–50. ISSN: 1476-4687. DOI: 10.1038/nature01336. URL: https://doi.org/10.1038/nature01336.

[37] Paul Smith-Goodson. “Quantum Computer Battle Royale: Upstart Ions Versus Old Guard Superconductors”. In: *Forbes* (Sept. 16, 2019). URL: https://www.forbes.com/sites/moorinsights/2019/09/16/quantum-computer-battle-royale-upstart-ions-versus-old-guard-superconductors/ (visited on 12/03/2022).

[38] Colin D Bruzewicz et al. “Trapped-ion quantum computing: Progress and challenges”. In: *Applied Physics Reviews* 6.2 (2019), p. 021314.

[39] Lila Kee. “RSA Is Dead — We Just Haven’t Accepted It Yet”. In: *Forbes* (May 6, 2021). URL: https://www.forbes.com/sites/forbestechcouncil/2021/05/06/rsa-is-dead---we-just-haventaccepted-ityet/ (visited on 12/03/2022).

[40] Donny Cheung et al. “On the Design and Optimization of a Quantum Polynomial-Time Attack on Elliptic Curve Cryptography”. In: (2007). DOI: 10.48550/ARXIV.0710.1093. URL: https://arxiv.org/abs/0710.1093.

[41] Daniel J Bernstein. "Grover vs. mceliece". In: *International Workshop on Post-Quantum Cryptography*. Springer. 2010, pp. 73–80.

[42] Kevin Bürstinghaus-Steinbach et al. "Post-quantum tls on embedded systems: Integrating and evaluating kyber and sphincs+ with mbed tls". In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. 2020, pp. 841–852.

[43] Julius Hekkala, Kimmo Halunen, and Visa Antero Vallivaara. "Implementing Post-quantum Cryptography for Developers." In: *ICISSP*. 2022, pp. 73–83.

[44] Davide Castelvecchi. "Quantum-computing pioneer warns of complacency over Internet security". In: *Nature* 587.7833 (2020), pp. 189–190.

[45] *The Year 2000 Problem: Fourth Report by the Committee on Government Reform and Oversight*. U.S. House of Representatives, Oct. 26, 1998. URL: https://www.congress.gov/105/crpt/hrpt827/CRPT-105hrpt827.pdf (visited on 12/05/2022).

[46] *Year 2000 Information and Readiness Disclosure Act*. Public Law 105-271, 1998. URL: https://www.congress.gov/bill/105th-congress/senate-bill/2392.

[47] *Y2K Bug*. Nostalgia Central. URL: https://nostalgiacentral.com/pop-culture/fads/y2k-bug/ (visited on 12/05/2022).

[48] John Leyden. "Down's Syndrome screening failures linked to Y2K bug". In: *The Register* (Sept. 14, 2001). URL: https://www.theregister.com/2001/09/14/downs_syndrome_screening_failures_linked/ (visited on 12/05/2022).

[49] Francine Uenuma. "20 Years Later, the Y2K Bug Seems Like a Joke—Because Those Behind the Scenes Took It Seriously". In: *Time* (Dec. 30, 2019). (Visited on 12/05/2022).

[50] Rajiv Ch and rasekaran. "Big Glitch at Nuclear Plant Shows Perils of Y2K Tests". In: *The Washington Post* (Mar. 7, 1999). URL: https://www.washingtonpost.com/archive/politics/1999/03/07/big-glitch-at-nuclear-plant-shows-perils-of-y2k-tests/a148232f-5760-403c-bc14-b00382b6852d/ (visited on 12/05/2022).

[51] Laszlo Gyongyosi and Sandor Imre. "A Survey on quantum computing technology". In: *Computer Science Review* 31 (2019), pp. 51–71. ISSN: 1574-0137. DOI: https://doi.org/10.1016/j.cosrev.2018.11.002. URL: https://www.sciencedirect.com/science/article/pii/S1574013718301709.

[52] Sukhpal Singh Gill et al. "Quantum computing: A taxonomy, systematic review and future directions". In: *Software: Practice and Experience* 52.1 (2022), pp. 66–114.

[53] Michele Mosca. "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" In: *IEEE Security & Privacy* 16.5 (2018), pp. 38–41. DOI: 10.1109/MSP.2018.3761723.