The Downtown Review

Volume 9 | Issue 2 Article 4

May 2023

Making the Transition to Post-Quantum Cryptography

J. Simon Richard
Cleveland State University

Introduction

"Quantum computing," which uses particles under the influence of quantum mechanics to run computations, 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], 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 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 (Shaw 2018). However, we have made a lot of progress since then. On November 9th, 2022, IBM unveiled the current largest quantum computer, the 433-qubit IBM Osprey (Padavic-Callaghan 2022). We are almost halfway to that $1,000$-qubit lower bound.[3]

If we sit on our hands, quantum computers could threaten the security of a large portion of our internet in the not-so-distant future.

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 ("IDC Forecasts Worldwide Quantum Computing Market to Grow to $8.6 Billion in 2027" 2021). And, in 2021, the running total of investments spent on quantum research and technology worldwide exceeded $25 billion ("Overview on quantum initiatives worldwide – update mid 2021" 2021). This may not seem like much compared to other industries, but, as argued by Sędkowski (2021), 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 MacQuarrie et al. (2020).

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

[1] In Computer Science, *polynomial time* is a 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 opposed to an exponential function).

[2] The quantum equivalent of a bit; it's pronounced the same as "cubit."

[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 sizes of our quantum processors have increased by a factor of six; such improvements point to fast, and even exponential, growth. See Neven's Law (Hartnett 2019).

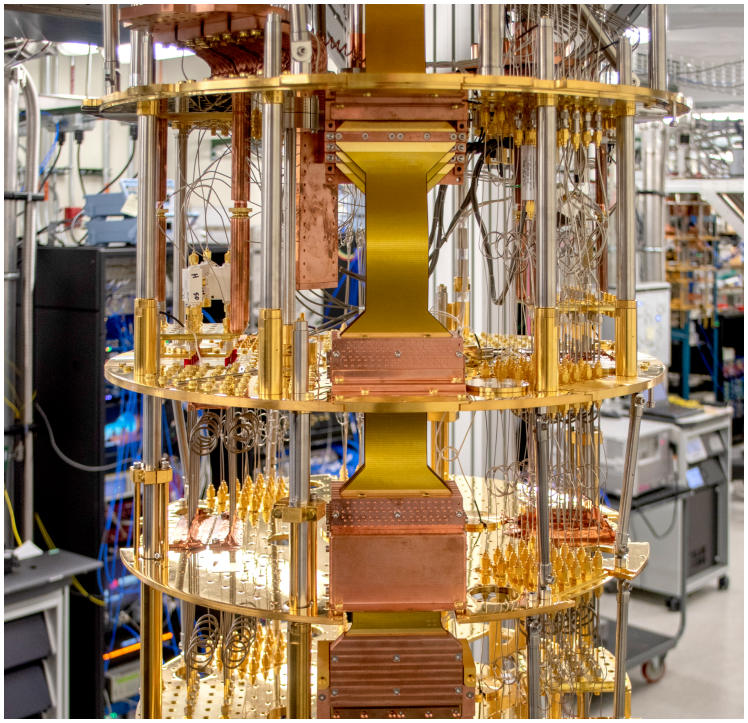

Figure 1: A component of the IBM Osprey, a 433-qubit quantum computer (*IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two* 2022)

have been working on quantum computers and related research (Sędkowski 2021). 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 have spent—around $1.2 billion ("Overview on quantum initiatives worldwide – update mid 2021" 2021). 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 (Choi 2021). China has been long understood by the U.S. Intelligence Community as one of the greatest threats to our national security (*Annual Threat Assessment of the U.S. Intelligence Community* 2022; Singman 2022; Buchman 2022), 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 algo-

rithms 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" ("NIST Asks Public to Help Future-Proof Electronic Informatiom" 2016), and by the proposal deadline in 2017 a total of 69 algorithms had been accepted as submissions for the first round (*Post Quantum Algorithms: Round 1 Submissions* 2022). 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+ ("NIST Announces First Four Quantum-Resistant Cryptographic Algorithms" 2022).

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 submit a possible way forward as inspired by the efforts taken to prevent the millennium bug (a.k.a. the Y2K bug). In the end, we conclude that more research, testing, and programming enabled by the cooperation of a wide array of institutions will be required.

A Background on Quantum Computing

Figure 2: Attendees of the 1981 Physics of Computation conference "Celebrating the 40-year anniversary of the Physics of Computation Conference" 2021

As described in "40 years of quantum computing" (2022), quantum computing theory began to emerge in the 1980s as physicists found connections among 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 as the 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*.

Quantum Mechanics and the Qubit

Quantum computing relies on the existence of two fundamental properties described by quantum mechanics: 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, consider the qubit. A qubit is a quantum system (it could be a particle, a superconducting circuit, a photon, or something else; it doesn't matter) in the superposition of two states, which we will call 0 and 1. Mathematically, this superposition 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. They are mathematically equivalent to vectors.

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.

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

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

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 dependent on each other. In other words, they are entangled.

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 classic double-slit experiment, which demonstrates that superpositions can interfere with each other without collapsing, and Dirac's three polarizer experiment, which makes observations that are best explained by the collapsing of superpositions (Dirac 1981). Entanglement is supported by experimental violations of Bell's inequality, an inequality that describes how a particular type of system should behave if it is not entangled (Goldstein et al. 2011; Handsteiner et al. 2017). However, please note that physicists vary widely on the interpretation of these experiments and the broader implications of these concepts.

Computing with Qubits

Quantum computing is generally achieved by applying operations to a group of entangled[5] qubits using quantum logic gates—physical components that can change qubit superpositions without forcing them to collapse. After a number of quantum logic gates have been applied, the qubits 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. Otherwise, information is lost, which produces heat.[6] And since heat is essentially molecular motion, it has the potential to add noise to the output signal. It is also for this reason that many (but not all) quantum computers operate at near absolute zero temperatures.

In order to actually build a quantum computer, you need to implement the qubits themselves. There are a variety of technologies that make this possible, but

[5] Entanglement is not always required. See Lanyon et al. (2008)

[6] Just like energy, information is a conserved quantity; it cannot just disappear.

a discussion on these technologies is outside the scope of this paper.

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 (Feynman 1982), was and still is the ability that quantum computers have to simulate quantum systems. The probabilistic nature of quantum systems makes them time-consuming and often impractical to simulate using classical computers. 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 Daley et al. (2022).

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 (Xi-Han et al. 2007). If they are successful, it would be possible to entirely circumvent the security threats posed by Shor's algorithm. This paper's discussion is still germane, however, because most internet users will not have access to local quantum computing in the foreseeable future.

Quantum computing can also be used in machine learning. As described by Schuld et al. (2014), many classical machine learning algorithms have quantum counterparts. This includes quantum neural networks (QNNs), which have been widely studied (Avramouli et al. 2022). These algorithms, along with Grover's Algorithm (discussed below), have applications in a wide variety of fields including the financial sector (Orús et al. 2019).

Quantum Threats Against Cryptographic Systems

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, as described in Kee 2021) and elliptic curve cryptography, a method that many are using to replace RSA (Cheung et al. 2007). If actualized, this would be devastating for internet security. According to one survey, over 50% of the top 1 million websites are still using RSA (*EV certificate usage declining: Is the internet*

becoming more secure? 2021). Even if a fraction of these websites were breached, millions of the 5.16 billion people who currently use the internet (DataReportal 2023) could be impacted.

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[7] "black-box" or "one-way" functions (functions whose inverse is difficult to calculate). This includes hash functions, which are vital to securing passwords and signing digital documents, and symmetric encryption keys.[8] 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; for example, 128-bit keys should be replaced by 256-bit keys when 128 bits of security is required (Bernstein 2010).

NIST's Post-Quantum Algorithms

As was mentioned in the introduction, the NIST identified four post-quantum algorithms that may be able to fix these security vulnerabilities. Three out of these four algorithms (CRYSTALS-Kyber, CRYSTALS-Dilithium, and FALCON) are based on mathematical structures called lattices. SPHINCS+ is based on hashing ("NIST Announces First Four Quantum-Resistant Cryptographic Algorithms" 2022). CRYSTALS-Kyber, described as a general purpose encryption algorithm in "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms" (2022), 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).

The NIST's work is not done. At least one other call for proposal requesting the submition of post-quantum digital signature schemes has been announced; its submission deadline in on June 1st, 2023 (*Post-Quantum Cryptography: Digital Signature Schemes* 2023).

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

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

The Difficulty of Implementation

One of the main practical differences between post-quantum algorithms and the algorithms commonly used today is that post-quantum algorithms tend to use larger key sizes. For example, as displayed in table 1, the secret keys used by CRYSTALS-Kyber are significantly larger than the secret keys used by equivalently secure variations of RSA.

In some cases, post-quantum algorithms also take more time or processing power to run. For example, table 2 (Bürstinghaus-Steinbach et al. 2020) compares the durations of TLS handshakes[9] that use post-quantum algorithms with the durations of TLS handshakes that use ECDHE-ECDSA, a widely used algorithm based on elliptic curves. Each algorithm was tested on three devices: the Raspberry Pi 3 Model B+ (RPi3), the ESP32-PICO-KIT V4 (ESP32), and a Fieldbus Option Card (FOC). In this table, we find that the post-quantum TLS algorithms tend to take longer than ECDHE-ECDSA-based TLS (although this is not true 100% of the time).

Equivalent AES Key Size (in bits)	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

These issues may complicate the transition to post-quantum algorithms because our current infrastructure has not been built with these computational costs in mind. As concluded by Bürstinghaus-Steinbach et al. (2020), some embedded environments will be able to handle post-quantum algorithms without modification, but embedded devices acting as TLS servers may need additional hardware acceleration. In general, we will not be able to use post-quantum algorithms as drop-in replacements for our current algorithms; more consideration will be required.

The mathematical complexity of these algorithms may also be problematic for those implementing them. Hekkala et al. (2022) 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.

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

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 TLS handshake runtimes for different cipher suites (rounded to two significant figures), as presented in Bürstinghaus-Steinbach et al. (2020)

They found that these algorithms were incredibly hard to understand and implement. 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.

Conclusion

Transitioning to a post-quantum world 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." However, he also acknowledged that there is a risk of complacency. The amount of willpower and programming time that will be required for this transition is enormous, comparable even to the effort spent on fixing the Y2K bug (Castelvecchi 2020).

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. Each year was represented only by its last two digits; 1980 would be represented by "80" and 1995 would be represented by "95." Many worried that, when the year 2000 came around, critical computer systems around the world would crash after 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 worldwide on this issue (*The Year 2000 Problem: Fourth Report by the Committee on Government Reform and Oversight* 1998). 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 (*Year 2000 Information and Readiness Disclosure Act* 1998).

When the year 2000 finally came, a computer billed a customer for a century's worth of late fees (*Y2K Bug* 2022) and the medical tests for 150 women were calculated incorrectly (Leyden 2001). However, nothing happened on 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 (Uenuma 2019). In 1999, programmers attempted to remove the Y2K bug from the computer systems at a nuclear power plant in Pennsylvania. They missed something, however; when they tested in the plant's entire digital monitoring system crashed[10] (Ch and rasekaran 1999). 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.

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 in order to protect our computer systems from the attacks of the quantum computers that will someday be built.

Further Reading

For a deeper understanding of the theory behind quantum computing, consider reading Dr. Ryan O'Donnell's lecture notes for his class on quantum computation and information, which was taught at Carnegie Mellon University (O'Donnell 2015).

For more information on the current state of quantum computing, see Laszlo Gyongyosi and Sandor Imre's "A Survey on quantum computing technology" (2019) and Gill et al.'s "Quantum computing: A taxonomy, systematic review and future directions" (2022).

Michele Mosca's "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" explores many of the same issues presented in this paper. In addition to post-quantum cryptography, it considers quantum key distribution[11] as a potential solution to the cybersecurity risks posed by quantum computers.

[10] There was an analog backup, thankfully.

[11] Quantum key distribution (QKD) uses entanglement to distribute symmetric encryption keys.

References

"40 years of quantum computing". *Nature Reviews Physics*, vol. 4, no. 1, Jan. 2022, pp. 1–1. https://doi.org/10.1038/s42254-021-00410-6.

"Annual Threat Assessment of the U.S. Intelligence Community", www.intelligence.gov/annual-threat-assessment. Accessed 23/11/2022.

Avramouli, Maria, et al. "Quantum Machine Learning: Current State and Challenges". *Proceedings of the 25th Pan-Hellenic Conference on Informatics*. PCI '21, Association for Computing Machinery, 2022, pp. 397–402, https://doi.org/10.1145/3503823.3503896.

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

Buchman, Cassie. "What are the biggest threats to US national security?" *News Nation*, 2 Aug. 2022. www.newsnationnow.com/world/biggest-threats-to-u-s-national-security/. Accessed 23/11/2022.

Bürstinghaus-Steinbach, Kevin, et al. "Post-quantum tls on embedded systems: Integrating and evaluating kyber and sphincs+ with mbed tls". *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. 2020, pp. 841–52.

Castelvecchi, Davide. "Quantum-computing pioneer warns of complacency over Internet security". *Nature*, vol. 587, no. 7833, 2020, pp. 189–90.

"Celebrating the 40-year anniversary of the Physics of Computation Conference". *IBM Research*, 15 Mar. 2021. research.ibm.com/blog/qc40-physics-computation. Accessed 3/12/2022.

Ch, Rajiv, and rasekaran. "Big Glitch at Nuclear Plant Shows Perils of Y2K Tests". *The Washington Post*, 7 Mar. 1999. www.washingtonpost.com/archive/politics/1999/03/07/big-glitch-at-nuclear-plant-shows-perils-of-y2k-tests/a148232f-5760-403c-bc14-b00382b6852d/. Accessed 5/12/2022.

Cheung, Donny, et al. "On the Design and Optimization of a Quantum Polynomial-Time Attack on Elliptic Curve Cryptography". 2007. https://doi.org/10.48550/ARXIV.0710.1093.

Choi, Charles. "Two of World's Biggest Quantum Computers Made in China". *IEEE Spectrum*, 6 Nov. 2021. spectrum.ieee.org/quantum-computing-china. Accessed 23/11/2022.

Daley, Andrew J., et al. "Practical quantum advantage in quantum simulation". *Nature*, vol. 607, no. 7920, July 2022, pp. 667–76. https://doi.org/10.1038/s41586-022-04940-6.

DataReportal. Digital 2023: Global Overview Report. 2023. datareportal.com/reports/digital-2023-global-overview-report. Accessed 2/5/2023.

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

Dyakonov, Mikhail. "When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing". *Ieee Spectrum*, vol. 56, no. 3, 2019, pp. 24–29.

"EV certificate usage declining: Is the internet becoming more secure?", 13 Dec. 2021, www.helpnetsecurity.com/2021/12/13/newer-tls-protocols/. Accessed 2/5/2023.

Feynman, Richard P. "Simulating physics with computers". *International Journal of Theoretical Physics*, vol. 21, no. 6, June 1982, pp. 467–88. https://doi.org/10.1007/BF02650179.

Gill, Sukhpal Singh, et al. "Quantum computing: A taxonomy, systematic review and future directions". *Software: Practice and Experience*, vol. 52, no. 1, 2022, pp. 66–114.

Goldstein, S., et al. "Bell's theorem". *Scholarpedia*, vol. 6, no. 10, 2011, revision #91049, p. 8378. https://doi.org/10.4249/scholarpedia.8378.

Gyongyosi, Laszlo, and Sandor Imre. "A Survey on quantum computing technology". *Computer Science Review*, vol. 31, 2019, pp. 51–71. https://doi.org/https://doi.org/10.1016/j.cosrev.2018.11.002.

Xi-Han, Li, et al. "Quantum secure direct communication with quantum encryption based on pure entangled states". *Chinese Physics*, vol. 16, no. 8, 2007, p. 2149.

Handsteiner, Johannes, et al. "Cosmic Bell Test: Measurement Settings from Milky Way Stars". *Phys. Rev. Lett.*, vol. 118, 6 Feb. 2017, p. 060401. https://doi.org/10.1103/PhysRevLett.118.060401.

Hartnett, Kevin. "A New Law to Describe Quantum Computing's Rise?" *Quanta Magazine*, 18 June 2019. www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/. Accessed 23/11/2022.

Hekkala, Julius, et al. "Implementing Post-quantum Cryptography for Developers." *ICISSP*. 2022, pp. 73–83.

"IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two", Nov. 2022, newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two. Accessed 23/11/2022.

"IDC Forecasts Worldwide Quantum Computing Market to Grow to $8.6 Billion in 2027". *International Data Corporation*, 29 Nov. 2021. www.idc.com/getdoc.jsp?containerId=prUS48414121. Accessed 23/11/2022.

Kee, Lila. "RSA Is Dead — We Just Haven't Accepted It Yet". *Forbes*, 6 May 2021. www.forbes.com/sites/forbestechcouncil/2021/05/06/rsa-is-dead---we-just-haventaccepted-ityet/. Accessed 3/12/2022.

Lanyon, Ben P, et al. "Experimental quantum computing without entanglement". *Physical review letters*, vol. 101, no. 20, 2008, p. 200501.

Leyden, John. "Down's Syndrome screening failures linked to Y2K bug". *The Register*, 14 Sept. 2001. www.theregister.com/2001/09/14/downs_syndrome_screening_failures_linked/. Accessed 5/12/2022.

MacQuarrie, Evan R., et al. "The emerging commercial landscape of quantum computing". *Nature Reviews Physics*, vol. 2, no. 11, Oct. 2020, pp. 596–98. https://doi.org/10.1038/s42254-020-00247-5.

"NIST Announces First Four Quantum-Resistant Cryptographic Algorithms". *National Institute of Standards and Technology*, 5 July 2022. www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. Accessed 25/11/2022.

"NIST Asks Public to Help Future-Proof Electronic Informatiom". *National Institute of Standards and Technology*, 20 Dec. 2016. www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information. Accessed 25/11/2022.

O'Donnell, Ryan. "Lecture Notes for 15-859BB: Quantum Computation and Information", 2015, www.cs.cmu.edu/~odonnell/quantum15/. Accessed 26/11/2022.

Orús, Román, et al. "Quantum computing for finance: Overview and prospects". *Reviews in Physics*, vol. 4, 2019, p. 100028. https://doi.org/https://doi.org/10.1016/j.revip.2019.100028.

"Overview on quantum initiatives worldwide – update mid 2021". *Qureca*, 19 July 2021. www.qureca.com/overview-on-quantum-initiatives-worldwide-update-mid-2021/. Accessed 23/11/2022.

Padavic-Callaghan, Karmela. "IBM unveils world's largest quantum computer at 433 qubits". *New Scientist*, 9 Nov. 2022. www.newscientist.com/article/2346074-ibm-unveils-worlds-largest-quantum-computer-at-433-qubits/. Accessed 22/11/2022.

"Post Quantum Algorithms: Round 1 Submissions", csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions. Accessed 25/11/2022.

"Post-Quantum Cryptography: Digital Signature Schemes", csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals. Accessed 5/5/2023.

Schuld, Maria, et al. "An introduction to quantum machine learning". *Contemporary Physics*, vol. 56, no. 2, Oct. 2014, pp. 172–85. https://doi.org/10.1080/00107514.2014.964942.

Sędkowski, Wiktor. "Quantum Race". *Warsaw Institute*, 22 Nov. 2021. warsawinstitute.org/quantum-race/. Accessed 22/11/2022.

Shaw, David. "Quantum Outlook 2019". *Fact Based Insight*, 17 Dec. 2018. www.factbasedinsight.com/quantum-outlook-2019/. Accessed 23/11/2022.

Shor, P.W. "Algorithms for quantum computation: discrete logarithms and factoring". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–34, https://doi.org/10.1109/SFCS.1994.365700.

Singman, Brooke. "China poses 'biggest long-term threat to economic and national security,' FBI Director Wray warns". *Fox News*, 6 July 2022. www.foxnews.com/politics/china-poses-biggest-long-term-threat-economic-national-security-fb-director-wray-warns. Accessed 23/11/2022.

The Year 2000 Problem: Fourth Report by the Committee on Government Reform and Oversight. 26 Oct. 1998. www.congress.gov/105/crpt/hrpt827/CRPT-105hrpt827.pdf. Accessed 5/12/2022.

Uenuma, Francine. "20 Years Later, the Y2K Bug Seems Like a Joke—Because Those Behind the Scenes Took It Seriously". *Time*, 30 Dec. 2019. Accessed 5/12/2022.

"Y2K Bug", nostalgiacentral.com/pop-culture/fads/y2k-bug/. Accessed 5/12/2022.

Year 2000 Information and Readiness Disclosure Act. 1998. www.congress.gov/bill/105th-congress/senate-bill/2392.