ZHFE$^-$ Over Other Public-Key Cryptosystems in the Quantum Era

Reece Pena

Department of Computer Science, Binghamton University

CS301: Ethical, Social, and Global Issues in Computing

Dr. George Weinschenk

March 28, 2020

Abstract

As we approach the quantum era of computing, the looming threat that quantum computers will destroy all classical encryption schemes has become prevalent in research groups. Organizations, companies, and individuals rely on said encryption schemes to ensure our information and data stays out of the hands of the nefarious and others unauthorized to access it. If a quantum computer were used for malicious purposes it could wreak havoc on national security, economies, or other systems in several unprecedented ways. To combat this looming threat, cryptographers have been working tirelessly to produce cryptosystems immune to quantum computing attacks, and thus labeled as quantum-resistant. Cryptosystems are defined as a collection of algorithms used to secure information. The responsibility of these algorithms lies in generating a unique key to encrypt and decrypt information. One quantum-resistant cryptosystem known as $ZHFE^-$ has come to fruition and shows promise. $ZHFE^-$ offers a stronger encryption method than other quantum-resistant cryptosystems by reducing the key size and maintaining integrity after securing an indefinite amount of data. However, the long and arduous process of putting such quantum-resistant systems into motion implies insufficient time to secure our current information if a quantum computer were created within the next 25 years.

ZHFE$^-$ Over Other Public-Key Cryptosystems in the Quantum Era

Entering the quantum computing era threatens the sanctity of online privacy, data, and information. Modern cryptosystems involved in the protection and safekeeping of our information may render themselves virtually useless. Quantum computers, when constructed on a large enough scale, can attack and decrypt these once-thought-to-be impenetrable encryption schemes. This proposed quantum-attack was proven possible when Peter Shor created a quantum computing device that could efficiently solve some of the world's hardest mathematical problems on which contemporary cryptosystems derive strength; however, there exist cryptosystems seemingly immune to attacks by quantum computers and offer a future for digital privacy. In contrast to other quantum-resistant public-key algorithms, the ZHFE- encryption algorithm provides a stronger method of protecting our privacy against the looming threat of quantum computing attacks.

In the present-day, most technology relies heavily upon asymmetric public-key cryptosystems to safeguard data. As proven in Shor's algorithm, quantum computers expose a fatal vulnerability with these asymmetric cryptosystems; despite the attacks, extensive research has shown that symmetric algorithms, among other public-key schemes, remain just as difficult to crack with the use of a quantum computer. Observe Lamport's signature, NTRU, and McEliece cryptosystems when it comes to quantum-resistant public-key algorithms, as they offer effective schemes to secure and encrypt our information in the quantum era. Alongside these algorithms, an unconventional cryptosystem utilizing chaos theory has been proposed, but it has been met with much skepticism. ZHFE-, on the other hand, offers a stronger method of

encryption in the quantum age. ZHFE- utilizes hidden field equations (HFE) in tandem with a notably small key size in comparison to other quantum-resistant algorithms.

Background

When public-key algorithms first came into fruition in 1976, cryptographers had come across a breakthrough in the field (Chen, 2020, sect. 1). Public-key algorithms work by distributing a key pair with a unique public-key to encrypt a message, and a unique private key to decrypt it. To generate these keys public-key schemes took advantage of the difficulty to solve integer factorization problems in polynomial time. According to Craig Costello (2019, tstp. 3:09), a renowned cryptographer and TED Talk host, integer factorization with large enough numbers would take the lifespan of the universe to solve with a supercomputer.

Quantum computers operate based on qubits rather than normal bits. Qubits are essentially the quantum version of bits. A qubit can take on the property 0 or 1 similar to a normal bit as well as any value between 0 and 1 (Costello, 2019, tstp. 9:34). Chen (2020, sect. 1) then describes how utilizing qubits on quantum computers, Shor's algorithm can solve difficult integer factorization problems in polynomial time, ultimately shaking the very core of public-key cryptography. Due to this vulnerability The National Institute of Standards and Technology (NIST), who originally made public-key cryptography the standard, works feverishly to develop quantum-resistant algorithms to combat this change (Chen, 2020, sect. 2).

The privacy and safety of our world now rely on the development of quantum-resistant cryptosystems. Lacking quantum-resistant encryption, anyone with access to a quantum computer could and malicious intent could wreak havoc. Not only would hackers have access to our personal information, but also data pertinent to critical infrastructures such as power grids,

hospitals, or even nuclear missiles (Costello, 2019, tstp. 7:55); however, quantum computers can do much more than possibly hack, as they have many ethical applications. Quantum computers may play an essential role in the future of the human race, pushing boundaries we had never thought possible. They can simulate biological and chemical functions, impossible with classical computers, and assist in solving some of the world's biggest problems (Costello, 2019, tstp. 6:19).

Precedent and Related Technology

We will discuss the various quantum-resistant public-key cryptosystems alternatives to the proposed ZHFE$^-$ cryptosystem. Perlner et al. (2009), employees of NIST, detail the aforementioned quantum-resistant cryptosystems in "Quantum Resistant Public-Key Cryptography: A Survey."

Lamport's Function

Perlner et al. (2009, sect. 3) begin to describe how the security of Lamport's function derives itself from the axiom of the irreversibility of a one-way function *f*. He then states that in most cases, the function *f* represents a cryptographic hash function. Perlner also provides the general logic behind the secrets, Lamport's function works by assigning two random secrets to each bit *k* in the plaintext message, $S_{0,k}$ and $S_{1,k}$ respectively, therefore requiring 2*n* secrets for a message of *n* size. The secrets, when concatenated, form the private key. The public-key consists of a formula as follows: if bit *k* is 0 then reveal $S_{0,k}$, otherwise reveal $S_{1,k}$ (Perlner, 2009, sect. 3). The formula for the public-key effectively reveals half of the secrets and thus information about the private key. Due to the public-key containing information about the private key, the security

of Lamport's signature sharply declines for more than one signature and a user must generate a new signature for each encrypted message (Perlner, 2009, sect. 3).

NTRU Cryptosystem

The NTRU cryptosystem provides an alternative to Lamport's signature, which unlike Lamport's and akin to other public-key cryptosystems relies on the difficulty of solving certain mathematical problems in polynomial time. These difficult problems are known as NP-Hard. NTRU specifically draws its difficulty from lattice problems, as an infinite number of lattice bases can generate the same lattice (Perlner, 2009, sect. 5). Furthermore, Perlner (2009, sect. 5) details how NTRU utilizes lattices that have an additional layer of symmetry within them, effectively reducing the basis from a normal $n \times n$ matrix to an $n/2$-dimensional polynomial, to select the coefficients of the polynomial we choose from a field in which n equals the number of elements. He then explains that the private key consists of a polynomial of a lattice basis consisting of short vectors, while the public-key consists of a polynomial of a lattice basis consisting of long vectors. Perlner also analyzes with Table 1 that due to the nature of NTRU, key lengths are in kilobits rather than megabits and it performs about 10-100 times faster than classical public-key cryptosystems.

McEliece Scheme

One of the oldest cryptographic public-key systems known as McEliece will still hold up as quantum-resistant. Founded upon the axiom that distinguishing an easy code from a hard code (i.e a code unsolvable in polynomial time) remains difficult, the security of McEliece cryptosystems persist (Perlner, 2009, sect. 6). Moreover, Perlner (2009, sect. 6) specifies McEliece's scheme refers to decoding problems in which a solver must correct the errors of an

arbitrary linearly-transformed binary vector. He then describes how McEliece plugs a *k*-bit message and an *n*-bit codeword into a Goppa Code, the easy code, and constructs the code such that reconstruction into the original message is possible by using a different code of length *t*-bits or less, $t = (n - k)/\log_2(n)$. The easy code in *n x k* matrix form then left-multiplies itself by an *n*-bit permutation of the matrix and right multiplies by an arbitrary invertible binary matrix to construct the public-key (Perlner, 2009, sect. 6). Perlner (2009, sec.6) equates the three matrices that construct the public-key to the private key and the cryptosystem can then use it to deconstruct the public-key and reconstruct the message. According to Perlner's statistics, provided by Table 1, the impressive speed of the cryptosystems directly contrasts the negative, the scheme suffers from abnormally large key sizes of approximately a million bits due to the magnitude of *n* and *k* requiring at least 1000 bits as shown in Table 1.

Table 1

Comparison of Public-Key Cryptographic Algorithms

	Estimated Time (PC)						
	Setup (ms)	Public Key Operation (ms)	Private Key Operation (ms)	Limited Lifetime?	Public Key Size (kbits)	Private Key Size (kbits)	Message Size (kbits)
Lamport Signature	1	1	1	1 signature	~10	~10	~10
Lamport w/Merkle	1	1	1	2^{40} signatures	0.08	~250	~50
McEliece Encryption	0.1	0.01	0.1	no	500	1000	1
McEliece Signature	0.1	0.01	20,000	no	4000	4000	0.16
NTRUEncrypt	0.1	0.1	0.1	no	2	2	2
NTRUSign	0.1	0.1	0.1	2^{30} signatures	2	2	4
RSA	2000	0.1	5	no	1	1	1
DSA	2	2	2	no	2	0.16	0.32
Diffie-Hellman	2	2	2	no	2	0.16	1
ECC	2	2	2	no	0.32	0.16	0.32

Note. Data from Perlner et al. (2009).

A Chaos Theory Alternative

Some more far-fetched methods of encryption have also been introduced into the cryptographic community as of late. One especially interesting scheme utilizes the fundamentals of chaos theory: essentially if minor changes occur in initial conditions, drastic changes occur in the results. According to Jeremy Hsu (2020, para. 7), a journalist for IEEE Spectrum Magazine, Andrea Fratcholli et Al., researchers in *Nature Communications* journal, have claimed that using chaotic light states can protect our digital keys. Hsu then explains that the researchers constructed a tiny patterned silicon chip, akin to human fingerprints, that act as mazes for light to refract randomly. The cryptosystem then analyzes the specific pattern of refractions to generate the keys (Hsu, 2020, para. 8) Any irreversible alteration to the conditions of the chip, such as slightly different lighting conditions or a droplet of water, will change the pattern of refraction, thus securing the keys (Hsu, 2020, para. 9). This scheme has been met with much skepticism by the scientific community, with one source stating that the authors of the paper barely understand the fundamentals of cryptography (Hsu, 2020, para. 19). We will avoid further discussion on this subject matter, due to the uncertainty and skepticism surrounding it, as the analysis of the ZHFE$^-$ cryptosystem proceeds.

Support

The ZHFE$^-$ Cryptosystem

The ZHFE$^-$ cryptosystem was created and proposed by Pelrner et. al (2016), employees of the NIST, as a modification of its predecessor ZHFE. ZHFE was originally proposed by Porras, et. al. (2014), researchers from various universities around the globe, in “ZHFE, a New Multivariate public-key Encryption Scheme”. Porras (2014, sect. 1) reports that the ZHFE encryption scheme belongs to a class of cryptographic schemes known as Multivariate

Public-Key Cryptography (MPKC) which rely on the difficulty of finding solutions to a system of quadratic equations over a finite field. Perlner also states that quantum computers are unable to significantly reduce the difficulty of said systems of equations, thus enabling MPKC as a viable choice for the foundation of quantum-resistant cryptosystems. Moreover, ZHFE specifically derives from a very important MPKC scheme known as hidden field equations (Porras, 2014, sect. 1.1).

Hidden Field Equations

Porras et al. (2014, sect. 1.1) then illustrate how hidden field equations belong to a type of cryptographic function known as trapdoors, easily evaluated functions that require secret information to invert. HFE works by taking a finite field k of order q and then selecting a degree $n \in Z^+$ irreducible polynomial with a codomain parameter y, $g(y) \in k[y]$. He then explains that following the selection of the polynomial, the algorithm creates a field extension $K = k[y]/(g(y))$, an isomorphism $\varphi = K \rightarrow k^n$ defined alongside an invertible quadratic map $F : K \rightarrow K$, and a degree bound $D \in Z^+$ is declared. Porras also declares that the invertible quadratic map F as shown in Figure 1, now referred to as the core map, creates a univariate polynomial with the coefficients $a_{i,j}, b_i, c \in K$ being chosen at random and $degree(F) \leq D$. Porras continues to define the public-key P as an isomorphic transformation of a random core map F, and two invertible affine transformations over k^n S, T, so that $P = T \circ \varphi \circ F \circ \varphi^{-1} \circ S$. The paper then describes the private key as F alongside S and T. Furthermore, Porras et al. suggest a low degree bound D to allow decryption in a reasonable timeframe.

Figure 1

Equation Forming the Invertible Quadratic Map

$$F(x) = \sum_{0 \leq j \leq i}^{n-1} a_{i,j} x^{q^i + q^j} + \sum_{i=0}^{n-1} b_i x^{q^i} + c$$

Note. This equation creates a univariate polynomial utilized in ZHFE. From Porras et al. (2014)

ZHFE's improvements upon HFE

ZHFE, being a derivative of hidden field equations, takes the general aspect of the core map one step further. Rather than producing a single-core map with the aforementioned equation *F*, Porras et al. (2014, sect. 1.2) chose to generate two separate core maps with varying coefficients and high degrees labeled as *F'* and *F''*. Normally, using a high degree polynomial makes the decryption process nearly impossible; however, the possibility to construct high-degree polynomials in such a way that the decryption process remains fast exists. Porras et al. (2014, sect. 1.2) then detail To do this the algorithm constructs a new low-degree univariate polynomial Ψ, as shown in Figure 2, utilizing *F'* and *F'',* with α_i and β_i being defined as random scalars, and F'_0 - F'_{n-1} being the powers of *F'* and F''_0 - F''_{n-1} being the powers of *F''*. Then Porras explains how low-degree univariate polynomial Ψ allows the decryption process to invert the new core map *G*, defined as *G* = (*F'*,*F''*). With the new low-degree univariate polynomial, high degree polynomials are hidden and utilized by ZHFE, thus increasing the security of the function without making the decryption process too much longer. Similar to HFE, the process for creating the public-key varies slightly with the use of a new core map, $P = T \circ (\varphi \times \varphi) \circ G \circ \varphi^{-1} \circ S$ (Porras, 2014, sect. 2.1). Now *S* and *T*, the scalars α_i and β_i, and Ψ compose the private key to allow deriving of the new core map.

Figure 2

Equation Forming Low-Degree Univariate Polynomial

$$\Psi(x) = x(\alpha_1 F'_0 + \ldots + \alpha_n F'_{n-1} + \beta_1 F''_0 + \ldots + \beta_n F''_{n-1}) +$$

$$x^q(\alpha_{n+1} F'_0 + \ldots + \alpha_{2n} F'_{n-1} + \beta_{n+1} F''_0 + \ldots + \beta_{2n} F''_{n-1})$$

Note. This equation utilizes two high-degree polynomials, *F'* and *F''*. From Porras et al. (2014)

Modifying ZHFE

Expanding upon ZHFE, Perlner et al. (2016) performed various analyses of the cryptosystem at hand, deducing the possibility of removing two public equations from ZHFE. To maintain the symmetry of univariate polynomials *F'* and *F''*, Perlner (2016, sect. 6.1) removed one equation from each, effectively mapping both of them from $K_q{}^n \rightarrow K_q{}^{n-1}$. Thus, ZHFE$^-$ was created, as it reduced key size by 2% and boosted the speed of the encryption process by 2% due to there being two fewer public equations (Pelner, 2016, sect. 6.3).

ZHFE$^-$ Comparisons

In comparison to the aforementioned quantum-resistant algorithms, ZHFE$^-$ provides a stronger method of encryption. For the protection of our future, we require a cryptosystem with indefinite duration, so any limited lifetime algorithms will not suffice. Therefore, according to the statistics in Table 1 provided by Perlner (2009), all Lamport signature schemes alongside NTRUSign are regarded as insufficient for safeguarding our information for an extended period. This insufficiency leaves ZHFE$^-$, NTRUEncrypt, and both McEliece encryption schemes as potential candidates; however, McEliece schemes suffer from massively bloated key sizes with a message of size 0.16KB requiring 8000KB to store private and public-keys in some cases

(Perlner,2009). ZHFE$^-$ with a message of size 0.16KB requires merely ~97 KB (2% less than the 99KB required by ZHFE)(Perlner, 2016, sect. 6.3; Porras,2014, sect. 2.3). Thus ZHFE- 's efficiency surpasses that of McElice's scheme due to the latter's bloated key sizes. Moreover, Perlner (2009, sect. 5) explains that NTRUEncrypt has suffered from 10+ relatively minor attacks since its creation, and was found vulnerable to ciphertext attacks as well. On the other hand, ZHFE$^-$ was analyzed as resistant to its notable attacks with parameter restriction (Perlner, 2016, sect. 5). Thus, in comparison to the history of attacks on NTRUEncrypt, ZHFE$^-$ stands as the current strongest method of quantum-resistant cryptography among the algorithms compared.

Social Impact

Per today's societal agreements and funding agencies, approaches towards new technologies should utilize innovative and responsible methods. These methods assume that all stakeholders are present in the discussions of the direction technologies (Vermaas, 2017, para. 1). The enigmatic nature of quantum theory limits the population of people who can truly understand and debate about topics within the field (Vermaas, 2017, para. 3). Due to this lack of understanding, often only experts and professionals participate in current discussions of quantum technologies and their significant impacts. According to Pieter Vermaas (2017, para. 1), a researcher in the philosophy of technology at the Delft University of Technology in the Netherlands, these discussions should involve every governmental body, social scientist, ethicists, and every stakeholder. The quantum era will affect every being on our planet. We must discuss the benefits and ramifications of quantum technologies at the same level as we converse about nanotechnology and artificial intelligence (Vermaas, 2017, para. 3). The future of mankind

may depend on us expanding the groups of people who understand the fundamentals of quantum technologies and bridging the gap caused by the enigmatic state of quantum theory.

Quantum Cryptography Implications

More specifically, quantum cryptography brings up the question of whether or not the future of our data will remain secure. According to Vermaas (2017, sect. 12), when Shor's attack was first created it became clear that quantum computers will compromise our digital privacy, communications between governmental organizations, financial institutions, and commercial companies. Vermaas also hypothesized that although it may seem as if we are safe for the time being since a quantum computer capable of decrypting public-key cryptosystems has yet to exist on a large enough scale, some may reason that anyone wishing to seek harm will store and cache while they wait for the means of decryption to become available. The National Academies of Science, Engineering, and Medicine (NASEM, 2019, sect. 4.4), authors of *Quantum Computing: Progress and Prospects*, conclude a large commercial interest in deploying quantum-resistant cryptosystems before the construction of a quantum computer large enough in scale. Therefore, we must begin planning our transition into the quantum era with the utilization of cryptosystems, such as ZHFE^{-}, immediately.

Migration to the Quantum Era

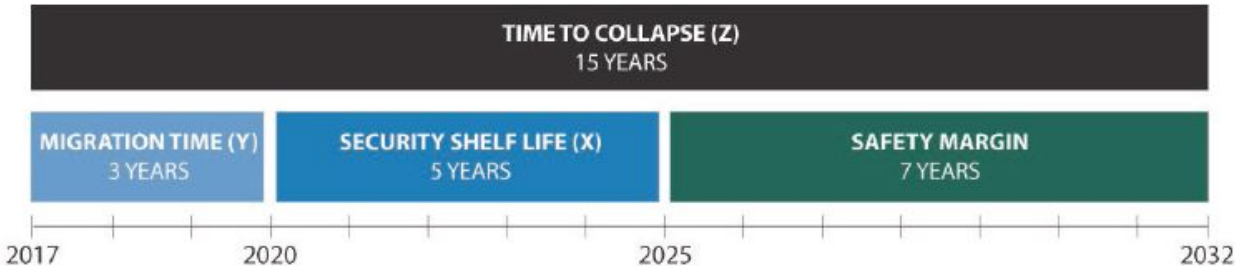
The arduous task of transition from quantum-vulnerable to quantum-resistant cryptosystems will realistically take many years (NASEM, 2019, sect. 4.1.1). According to NASEM (2019, sect. 4.4), such an example of a transition of similar magnitude was the process of switching from SHA-1, a vulnerable cryptographic hash function that secured passwords, to its successor SHA-256. NASEM also stated that this process began as early as 2004 and as late

as 2018 it was still yet deprecated across the whole web. When it comes to encryption as a whole, this transition holds a much higher precedent. The vast majority of the internet must be updated with new quantum-resistant cryptosystems before the deprecation and removal of quantum-vulnerable cryptosystems can occur (NASEM, 2019, sect. 4.4). The responsibility of setting the standards thus falls unto NIST, the organization responsible for setting standards in cases such as SHA-1 to SHA-256 and now quantum-vulnerable to quantum-resistant. The NIST has estimated the release of standards for quantum-resistant cryptosystems to sometime between 2022-2023 (Chen, 2020, sect. 5). Following the release of the aforementioned standards, governmental bodies must take steps to phase-out old cryptosystems. These steps include the implementation of standards into programming languages, review and revision of current protocols, updating of all software and hardware with standards, destruction of vulnerable sensitive information, and resigning along with the redistribution of any other pertinent information. Totaling the time required for each step, and with comparison to the switch between SHA-1 to SHA-256, this process could take as long as 20 years to complete (NASEM, 2019, sect. 4.4). If a quantum computer with at least 2,500 logical qubits comes to completion within the next 15 years, a sizable amount of data will remain compromised, but we can limit the impact if we act fast and effectively (NASEM, 2019, sect. 4.4). NASEM (2019, sect. 4.4) provides a means to model this timeline, we create three variables: The security shelf-life X (the interval of protection for data we care about), the migration time Y (time required to create and put standards in place), and the collapse time Z (time required to create an operational quantum computer of sufficient scale). NASEM provides Figure 3, which models a time-line with a

generously low time-frame for the migration time, while Figure 4 models a more realistic time-line. In both situations, time is of the essence for maximum protection.

Figure 3

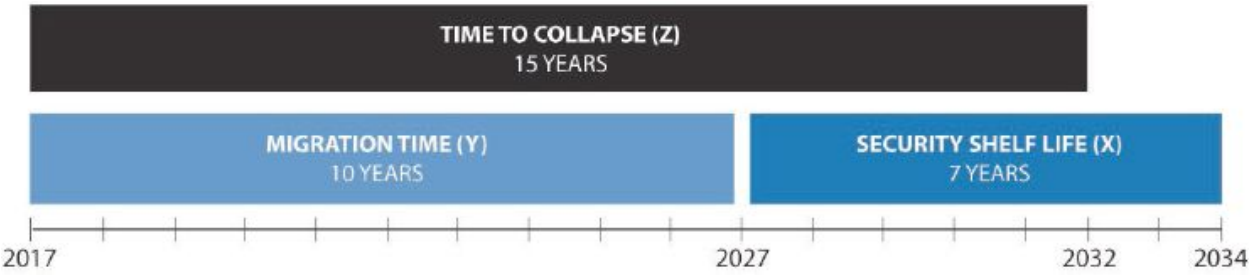
Mosca's Model for a Safe Transition to Post-Quantum Cryptography



Note. Time-frames are hypothetical. From NASM (2019)

Figure 4

Mosca's Model for a Transition That Is Too Long



Note. Time-frames are hypothetical. From NASM (2019)

Ethical Analysis

Although the ethics of quantum computing is up for debate, many ethicists and codes of ethics are obliged to agree with the decision of transitioning from quantum-vulnerable cryptosystems to quantum-resistant cryptosystems. Thomas Hobbes, for example, would argue that when we created the social contract with our government we sacrificed some of our liberties

for various protections. In terms of the transition to quantum-resistance, governmental bodies such as the NIST will most likely request that individual vendors, companies, and persons update their software and protocols accordingly, regardless of personal feelings toward the matter; thus, the government maintains their end of the contract by ensuring the Populous has effective cryptosystems in place to protect our privacy. Expanding upon this, John Locke would state that privacy is morally necessary and needs to be protected. Furthermore, Locke would acknowledge the benefits of the aforementioned social contract, as it protects the masses from the immoral few and secures peace. Thus, a transition to quantum-resistance would be ethical in the eyes of Hobbes and Locke. Additionally, Immanuel Kant's deontological view, and applications of universality to the categorical imperative, would also fall in-line with the decision to update cryptosystems. Kant would debate that since the application of quantum-resistant cryptosystems universally would have no problems arise, as it only has a net positive outcome for the privacy of all people, it is morally permissible. Moreover, ACM's code of ethics (ACM, 2018, cd. 1.6) 1.6 would further support the verdict to transition. The ACM code states that computing professionals should take measures to prevent the re-identification of anonymized data or unauthorized access and collection of data. Thus, every computing professional who respects the ACM code of ethics would also align with the agreement to transition to quantum-resistant cryptosystems, to better protect individual and group privacy. Conclusively, taking into consideration the agreements of the aforementioned ethicists and codes as well as the lack of any viable disagreements from notable ethicists, the transition from quantum-vulnerable to quantum-resistant cryptosystems remains favored by most.

Conclusion

Although the task of migrating to new cryptosystems may seem daunting, it remains possible. If used nefariously, quantum computers will break classical encryption schemes when built on a large enough scale (approximately 2,500 logical qubits). Members of the scientific community have continued working diligently to remedy the situation by proposing quantum-resistant cryptosystems and schemes. ZHFE$^-$ has proven itself one of the strongest quantum-resistant cryptosystems available among Lamport's function, NTRU-based cryptosystems, and McEliece schemes. ZHFE$^-$'s ability to maintain its encryption ability over an indefinite amount of time in tandem with its small key size set it apart from the aforementioned schemes. Thus, by utilizing ZHFE$^-$ agencies can secure the digital privacy and information of the people; however, the looming crisis doesn't stop with ZHFE$^-$. Scientists should continue research in the rapidly evolving field of post-quantum cryptography. Any day someone could make a ground-breaking discovery of a cryptosystem that will fully protect against quantum computing attacks; perhaps simply finding the ideal parameters for ZHFE$^-$. On the other hand, quantum computers have unrealized potential and the likelihood that there could never exist a foolproof way of securing our information exists.

References

Association for Computing Machinery (2018). ACM Code of Ethics and Professional Conduct. *ACM*. https://www.acm.org/code-of-ethics

Chen, L., & Moody, D. (2020). New mission and opportunity for mathematics researchers: Cryptography in the quantum era. *Advances in Mathematics of Communications*, *14*(1), 161–169. 10.3934/amc.2020013

Costello, C. (2019, May). *In the war for information, will quantum computers defeat cryptographers?* [Video] TED Talks. https://www.ted.com/talks/craig_costello_in_the_war_for_information_will_quantum_computers_defeat_cryptographers

Hsu, J. (2020, February 17). New cryptography method promising perfect secrecy is met with skepticism. *IEEE Spectrum Magazine*, Tech-Talk. https://spectrum.ieee.org/tech-talk/telecom/security/new-cryptography-method-promises-perfect-secrecy-amidst-skepticism

National Academies of Sciences, Engineering, and Medicine (2019). Quantum Computing: Progress and Prospects. *The National Academies Press*, 108-112. 10.17226/25196

Perlner, R. A., & Cooper, D. A. (2009). Quantum resistant public-key cryptography: A survey. *Proceedings of the 8th Symposium on Identity and Trust on the Internet - IDtrust 09*, 85–93. 10.1145/1527017.1527028

Perlner, R., & Smith-Tone, D. (2016). Security analysis and key modification for ZHFE. *Post-Quantum Cryptography 2016 Lecture Notes in Computer Science*, 197–212. 10.1007/978-3-319-29360-8_13

Porras, J., & Baena, J., & Ding, J. (2014). ZHFE, a New Multivariate public-key Encryption Scheme. *Post-Quantum Cryptography 2014 Lecture Notes in Computer Science*, 229-245. 10.1007/978-3-319-11659-4_14.

Vermaas, P.E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics Inf Technol* 19, 241–246. 10.1007/s10676-017-9429-1