POST-QUANTUM CRYPTOGRAPHY BASED ON CODES: A GAME CHANGER FOR SECRECY IN AERONAUTICAL MOBILE TELEMETRY

Morteza Shoushtari, Farah Arabian, Willie K. Harrison
Department of Electrical and Computer Engineering
Brigham Young University
Provo, UT, 84602
morteza.shoushtari@byu.edu, farah.arabian@byu.edu, willie.harrison@byu.edu

ABSTRACT

The future development of quantum computing threatens a host of modern cryptographic security efforts, and thus presents a new security threat to wireless communications systems. Encryption algorithms for aeronautical mobile telemetry (AMT) may likewise be vulnerable to quantum attacks based on Grover and Simons' algorithms. Post-quantum cryptography focuses on developing appropriate cryptographic algorithms that are impervious to both quantum and classical attacks and can therefore provide data confidentiality in a post-quantum computing world. This paper proposes the application of post-quantum cryptography as a future security solution in AMT systems with a focus on code-based techniques and provides a road map for studying the next generation of cryptosystem in AMT. We further suggest and analyzed (in terms of secrecy) the use of the McEliece cipher as a special case of a code-based post-quantum cryptographic solution for the integrated Network Enhanced Telemetry (iNET) communications system and show how it may be deployed.

INTRODUCTION

If and when quantum computers achieve their potential, they will be capable of solving quantum algorithms using quantum computations. In some cases, this capability can offer profound improvements in computational speed over classical algorithms executed on classical systems. In terms of modern cryptanalysis, this new capability would be a game changer, leaving many of our current cryptosystems vulnerable to attack. Quantum computers have the ability to rapidly find logical patterns and relationships in large amounts of data, and tackle some problems that were previously thought to be impossible to be solved in a realistic amount of time due to their complexity. Aeronautical mobile telemetry (AMT) systems, like many other systems that transport and store data of a sensitive nature, need to be prepared to adjust/adapt by incorporating post-quantum cryptographic techniques before quantum computing becomes practically feasible.

The works of [1, 2, 3] provide quantum attack algorithms that may be utilized by quantum computers to break and/or weaken encryption algorithms that are in use today. As a result, there has been a surge of interest in post-quantum cryptography [4, 5], which is focused on cryptosystems

that are resilient to quantum and classical attacks. In other words, post-quantum cryptosystems are designed to be immune to any secrecy penetration, even if the attacker is equipped with a quantum computer.

This paper explores potential candidates of post-quantum cryptography for aeronautical mobile telemetry systems. We specifically investigate the possibility of using one of the candidates, known as the McEliece cipher, which we will show is a suitable post-quantum cryptographic algorithm for the iNET system management standard. The iNET is a telemetry standard that is designed to enhance both the reliability and secrecy of the transmission link between test article and ground station compared to old-fashioned point-to-point links [6]. Traditional telemetry systems consist of only one transmission link between test article and ground station; however, iNET considers a secondary bidirectional link between test article and ground station with the purpose of efficiency improvement in the sense of transmission reliability [7, 8]. We consider a wiretap scenario that makes use of the McEliece encryption algorithm on the iNET standard. We also perform a secrecy analysis of such a system, wherein we show that the McEliece cipher can be used in telemetry links to bring about post-quantum cryptography, and that the iNET structure can be used to alleviate some of the drawbacks of McEliece cryptosystems.

The organization of the remainder of the paper is as follows. We first explore existing cryptosystems in aeronautical mobile telemetry, and then provide a list of candidates for post-quantum cryptography that can be applied to telemetry links with short descriptions of each. We evaluate the use of code-based cryptosystems by focusing on McEliece's algorithm applied to the iNET system structure, and then conclude the paper.

PRE-QUANTUM CRYPTOGRAPHY

A. *Symmetric vs. Asymmetric Cryptography*

There are several different approaches to ensure confidentiality, integrity, and authenticity in wireless communications systems, such as computational and information-theoretic approaches [9]. The cryptographic algorithms categorized in the computational approach, are mathematical operations that transform the data into an encrypted version that makes it unreadable to attackers. Cryptosystems can generally be categorized into two main groups: *symmetric* and *asymmetric* algorithms.

- **Symmetric Encryption Algorithms**: In this method, the same secure key is used for both the encryption and decryption processes, hence handling and exchanging keys in a secure way are two main challenges in symmetric cryptography. The key must be shared among legitimate parties before initiating any information transmission. Advanced Encryption Standard (AES), Rivest Cipher (RC), and Data Encryption Standard (DES) are examples of symmetric encryption algorithms.

- **Asymmetric Encryption Algorithms**: In this approach, which is also known as public key cryptography, encryption and decryption processes are executed using different keys. All

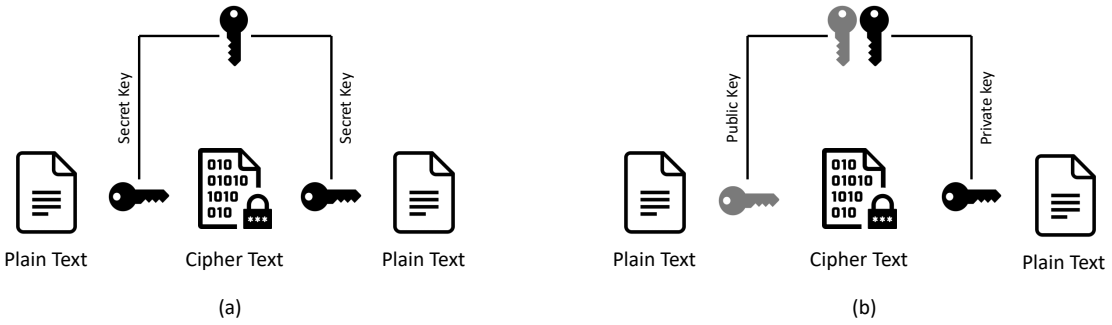

Figure 1: (a) Symmetric cryptosystem. (b) Asymmetric cryptosystem for confidentiality.

users wishing to establish secure communications under this paradigm generate two keys: a public key that can be shared with the world, and a private key that is kept secret and shared with no one. Either key can be used for encryption, depending on whether users are aiming for confidentiality or authentication. The other key in the pair can then decrypt the message. In the case of confidentiality, entities wishing to communicate securely with a user perform encryption with the user's public key. Only the user can decrypt the message since only the user has access to the private key. In the case of authentication, a user encrypts a message with their private key, which allows anyone else to decrypt the message with the user's public key and, hence, verify that the message came from the user. Encryption/decryption with combinations of keys can also be used to bring about confidential and authenticated communication as long as all users have generated key pairs. Resource utilization, such as power and memory consumption, tends to be higher for asymmetric algorithms compared to symmetric ones. The most popular asymmetric encryption algorithms are Rivest–Shamir–Adleman (RSA) and Digital Signature Algorithm (DSA).

The concepts of symmetric and asymmetric encryption for confidentiality are shown in Figure 1. Symmetric encryption tends to be faster and more suitable for applications with large payloads, such as telemetry systems, although asymmetric systems may provide security for future AMT if computational complexity can be adequately addressed.

B. Encryption in Aeronautical Mobile Telemetry - AES

The most widely used symmetric cryptographic algorithm in AMT systems is AES. AES is a data encryption algorithm developed by the National Institute of Standards and Technology (NIST) in 2001 [10]. AES is a symmetric block encryption algorithm that exploits a 128-bit block size of data, designed with three different key lengths of 128-bits, 192-bits, and 256-bits. The processes of encryption and decryption are executed in several rounds as shown in Figure 2 [11]. The key length dictates the number of rounds as indicated in Table 1. A larger key length corresponds to a higher number of rounds, which provides a stronger level of security. Generally speaking, a key length of 256 bits is deemed secure for modern applications; however, Grover's algorithm [2] and Simon's algorithm [3] reduce the validity of this statement for quantum computers. These algorithms significantly weaken AES, and further advances in quantum algorithms may exacerbate the problem. Shor's algorithm [1] completely breaks some forms of asymmetric cryptography

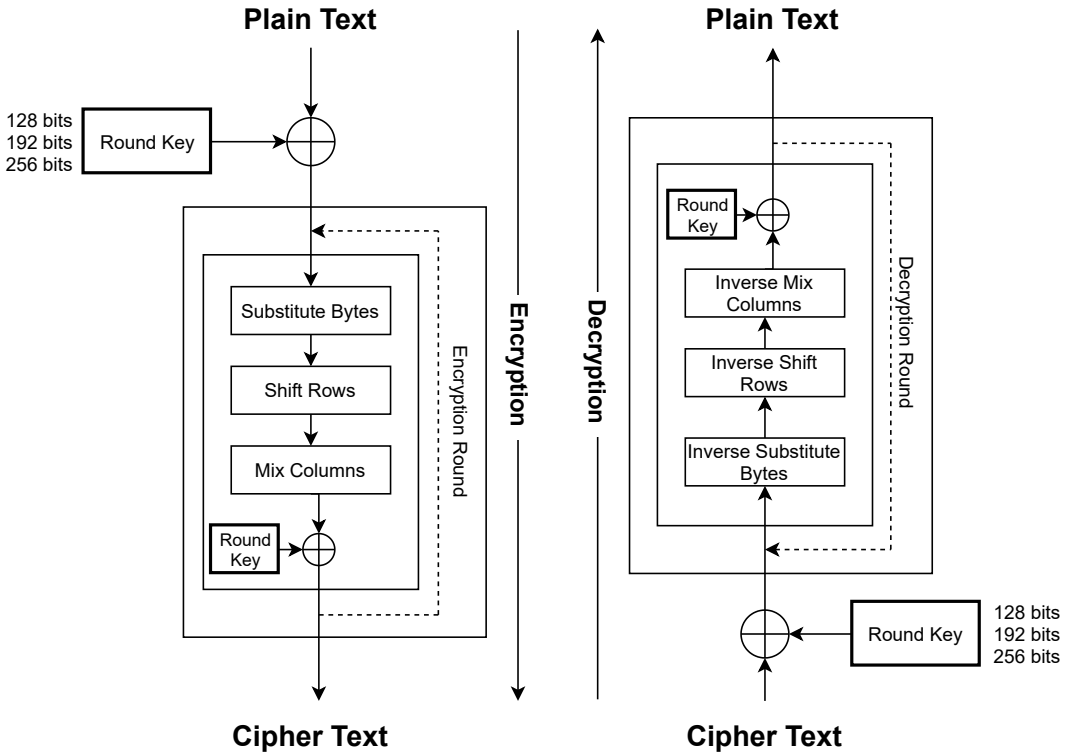

Figure 2: The AES mathematical encryption and decryption procedure.

Key length	Number of rounds
128-bit	10
192-bit	12
256-bit	14

Table 1: Number of encryption/decryption rounds based on the key length.

using quantum computing, resulting in a need for careful consideration in potential replacements to any current cryptosystems.

POST-QUANTUM PUBLIC-KEY CRYPTOGRAPHY

Computational security, i.e., modern cryptography, relies on the assumed hardness of various mathematical tasks. Shor, in [1], provided algorithms that invalidate the hardness of some well-known problems, especially in asymmetric cryptosystems, such as the difficulty of factoring large integers and the computation of discrete logarithms over finite fields. He presented a quantum algorithm that calculates the prime factors of a large number in polynomial time, rather than exponential time using classical algorithms. The best known classical algorithm require 2^n operations, where n is defined as the input size. As the size of the input increases, the number of operations grows exponentially, but operation growth for Shor's algorithms is in polynomial time [12]. More-

over, Grover, in [2], presented a searching algorithm for the symmetric cryptosystem that reduces the security of the key to half against a brute-force attack. In another word, a 256-bit AES cryptosystem in a post-quantum world would have the same security that is currently provided by a 128-bit AES cryptosystem. One possible solution to prevent the reduction in security is to simply expand the size of the key, but this requires extra rounds in both the encoder and decoder, and therefore is not desirable for real-time applications such as aeronautical mobile telemetry systems. Furthermore, Simon's algorithm is another quantum algorithm that has been used by quantum computers to attack multiple symmetric cryptosystems [3]. Finally, there exist active research topics focused on attacking symmetric cryptosystems which may speed up search algorithms to achieve super-polynomial time [13]. Accordingly, quantum computing threatens both symmetric and asymmetric encryption algorithms.

The goal of post-quantum cryptography is to create cryptosystems that are secure against quantum and traditional computers while also being able to work with existing communications protocols and network infrastructure. There are five primary candidates for post-quantum cryptographic algorithms including code-based cryptography, lattice-based cryptography, isogeny-based cryptography, multivariate-quadratic cryptography, and hybrid schemes.

A. Code-based cryptosystems

Code-based cryptosystems are mainly based on the idea of error-correcting linear codes. The first code-based cryptosystem was introduced by McEliece in 1978 [14]. The original McEliece algorithm is based on the generator matrix of a binary Goppa code, and its security relies on the problem of syndrome decoding, which has been classified as a nondeterministic polynomial time (NP)-complete problem. Owing to the fact that attacking McEliece is provably NP-complete, we need not fear that quantum computing will render the cipher obsolete. McEliece's cryptosystem has fast encryption and decryption procedures, and therefore represents a great candidate for AMT post-quantum cryptography, possibly allowing for real-time processing. However, the McEliece algorithm has two main disadvantages: low encryption rate and large key size, which can both be addressed by replacing binary Goppa codes with other families of codes such as Reed-Solomon codes and low-density parity-check (LDPC) codes, although each of these potential alterations present slightly different problems for an attacker. Additional research is still being done in this area to ensure that such changes do not compromise the security of the system.

B. Lattice-based cryptosystems

Lattice-based cryptosystems are based on the difficulty of lattice problems, such as the Shortest Vector Problem (SVP). In [15], it is shown that polynomial factors in lattice problems can be classified as a *hard problem*. The goal of lattice-based computational problems is to find the shortest nonzero vector in a lattice or finding a lattice vector that is close to a target vector not in the lattice. Lattice-based cryptosystems have strong secrecy and easy implementation, but they need large key sizes and overhead, which may present challenges for real time applications such as in AMT. Finding an optimal way to compress the keys (preserving the secrecy level) can be a good mathematical solution for this problem.

C. *Isogeny-based cryptosystems*

One of the latest and most challenging (implementation-wise) post-quantum cryptographic ideas is found in isogeny-based cryptosystems. Security is based on the difficulty of finding a path in the isogeny graph of supersingular elliptic curves [16]. To prevent quantum attacks, the singular curves need to be noncommutative, which makes it more difficult to find the path. This method requires a very small key compared to other post-quantum cryptosystem candidates, making it a suitable candidate for real-time applications such as AMT.

D. *Multivariate-quadratic cryptosystems*

Multivariate cryptography makes use of a set of quadratic polynomials over a finite field. Security derives from the difficulty of solving a system of polynomial equations. Many proposed systems use quadratic equations for efficiency [17]. Attacking these systems is proven to be NP-hard or NP-complete [18]. The public key for multivariate encryption is a function of multivariate polynomials, usually quadratic, over a finite field, and its idea is based on the fact that solving a multivariate polynomial system over a finite field is an NP-complete problem [19]. For use in AMT, evaluation of compression and optimization techniques on the keys are required since this method also uses large key sizes.

E. *Hybrid cryptosystems*

Hybrid cryptosystems merge pre-quantum and post-quantum ciphers to provide a double protection in the communication system. This kind of cryptosystem seems to be the next step after post-quantum cryptography.

These five candidates for post-quantum cryptosystems, along with some of their most well-known algorithms are shown in Figure 3. Note that many of these are only candidate algorithms, and still require vetting prior to broad use. Even when mathematical algorithms are provably hard, this is not enough to guarantee that implementations of the algorithms are secure. For example, Rainbow was recently cracked, and is no longer being considered as a viable algorithm for post-quantum cryptography[20]. Others may follow as the vetting process for new cryptosystems continues.

A CODE-BASED CRYPTOSYSTEM FOR INET

The wiretap channel model for the iNET standard is shown in Figure 4. A downlink radio channel is assumed, where the test article is the transmitter and the ground station is the receiver. The secret message is assumed to be a length-k binary vector with bits chosen independently, uniformly at random. There are two telemetry links between legitimate parties (test article and ground station); one is used for key exchange and the other is used for data transmission. Note that the key can be updated as often as desired using this approach, and the initial key can be shared prior to launch/take off of the test article if desired. The goal is to transmit a secret message m

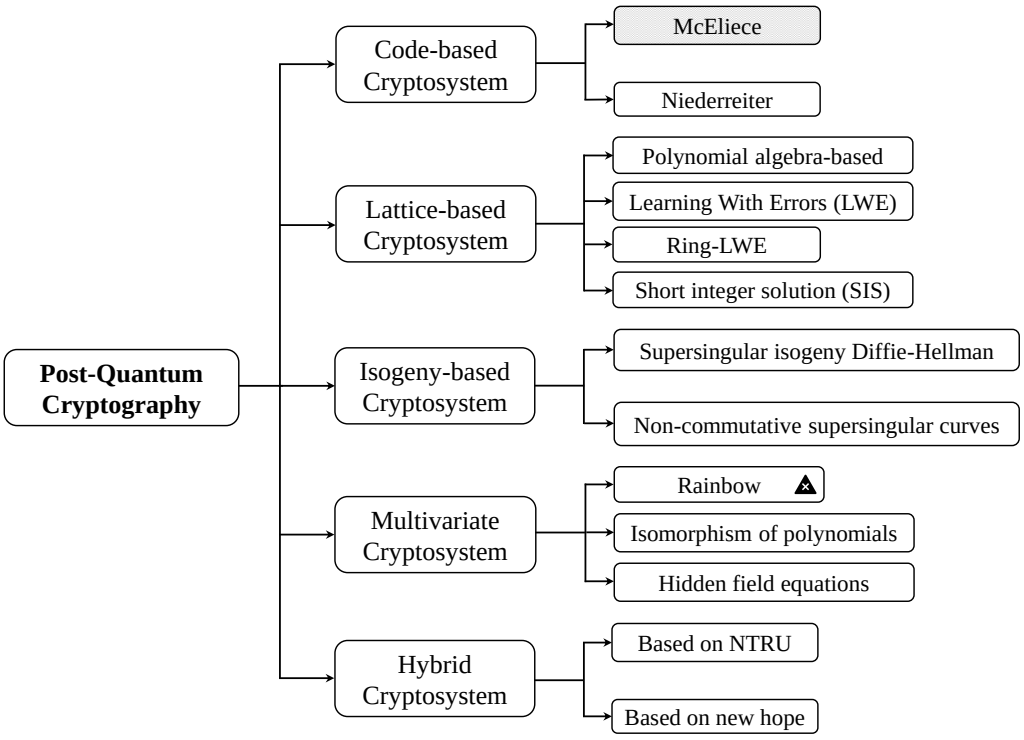

Figure 3: Post-quantum cryptosystem candidates and their well-known algorithms.

from test article to ground station in the presence of an eavesdropper who has error-free access to both telemetry links. Symmetric key encryption would not work here since the eavesdropper sees the transmitted key, but asymmetric encryption is a perfect fit. Note that the 'tag' applied to each codeword in the figure solves the authentication problem for the test article, and is discussed in more detail later.

We adopt the McEliece cryptosystem [14], which is one of the code-based post-quantum cryptographic algorithms, that uses coding randomization in the encryption process. The security of the algorithm is based on the hardness of decoding a general linear code in the way shown below, which cannot be solved in polynomial time; hence, it is known to be non-deterministic polynomial-time hardness, or NP-hard in short. The original algorithm uses binary Goppa codes, that has an easy decoding process, but any error-correction linear code with a fast decoding algorithm can be used. The McEliece cryptosystem consists of three main steps: 1) a key generation algorithm which produces a public and private key pair, 2) an encryption algorithm, and 3) a decryption algorithm. These steps are explained in the following.

A. Key Generation

The key generator is implemented in the ground station to produce the following three main components:

- A binary (n, k)-linear code $\mathcal{C}$, where n is the length of the codeword and k is the length of the message, with the code rate of k/n. This linear code can correct t or less errors efficiently,

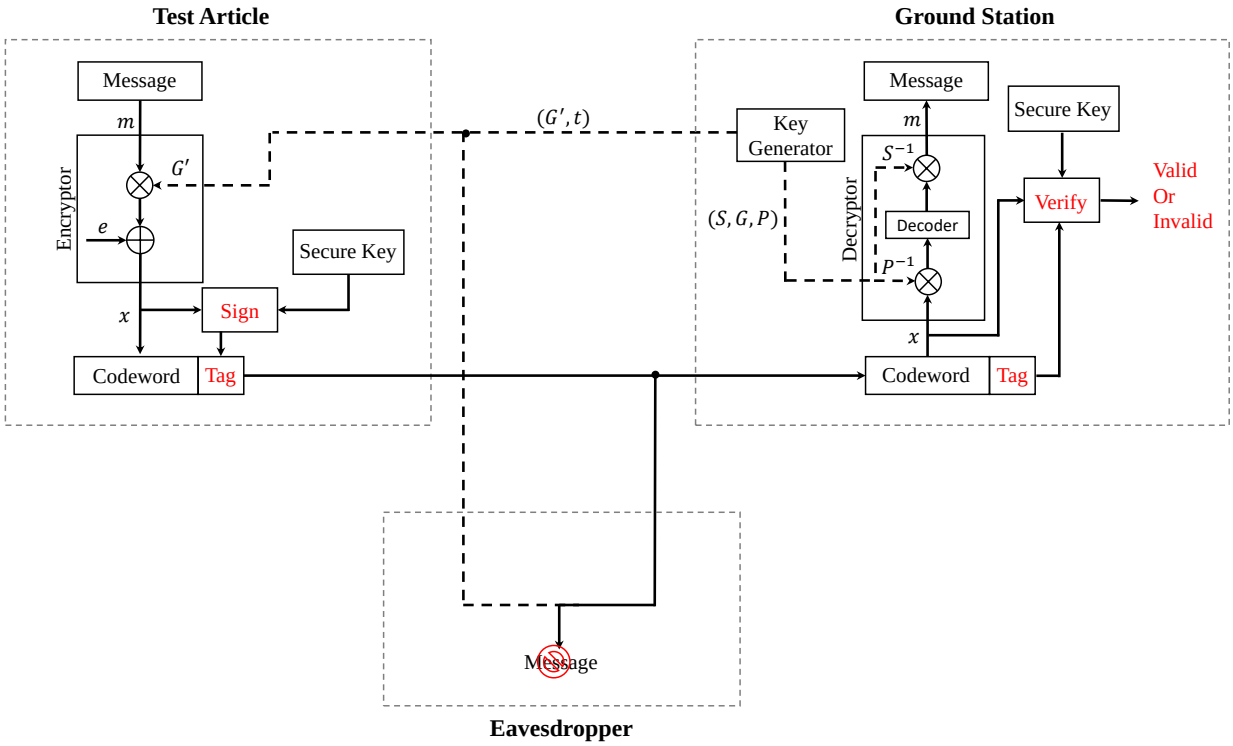

Figure 4: McEliece cryptosystem for the iNET standard in a wiretap scenario.

and is fully defined by a $k \times n$ generator matrix G.

- A random $k \times k$ binary non-singular scrambling matrix S.
- A random $n \times n$ permutation matrix P.

Having (S, G, P) form the key generator then the ground station computes the $k \times n$ matrix G' as:

$$G' = SGP. \tag{1}$$

Before data transmission phase begins, meaning during the signaling initialization, the ground station transmits (G', t), known as the public key to the test article, and keeps (S, G, P), known as the private key to itself, to be used for the decryption procedure.

B. Encryption

As the second step of the cryptographic algorithm, encryption needs to be performed after key generation. The encryption process mathematically converts the message stream to ciphertext. Suppose that the test article is intended to transmit the k-bit secret message m to the ground station, that has public key (G', t), as shown in Figure 4. The test article performs the following three steps to complete the encryption process:

1. Encode m by using the public key provided by the ground station to calculate $x' = mG'$.

2. Generate a random binary n-bit error vector e with Hamming weight t (containing exactly t ones in the otherwise zero vector of length n).

3. Compute the ciphertext/codeword as follows

$$x = mG' + e = x' + e. \tag{2}$$

The test article then transmits x to the ground station. Note that the eavesdropper possesses the public key, and has full knowledge of x; however, there are $\binom{n}{t}$ different patterns of the error vector e. With appropriate values of n and t, recovering the message m is NP-hard.

C. *Decryption*

Decryption is the last process of the cryptosystem, and is performed at the ground station. Decryption transforms encrypted information x into its original format m using knowledge of the private key.

1. First, the ground station calculates the inverses of the permutation and scrambling matrices, P^{-1} and S^{-1}, respectively.

2. Then it computes $\hat{x} = xP^{-1}$. Substituting x from (2) gives

$$\hat{x} = (mG' + e)P^{-1}. \tag{3}$$

   Substituting G' as shown in (1), then

$$\hat{x} = (mSGP + e)P^{-1} = mSG + eP^{-1}. \tag{4}$$

3. The ground station then applies the efficient decoder to $\hat{x}$. Since the code can correct t errors, the permuted error vector is removed. The message recovered through this decoder will be the scrambled message, $m' = mS$.

4. Finally, the message is recovered by applying S^{-1} as

$$m = (mS)S^{-1} = m. \tag{5}$$

D. *Numerical Example*

The original McEliece algorithm is based on Goppa codes with $n = 1024$, $k = 512$, and $t = 50$. We use a toy example here to illustrate the concept. Let $\mathcal{C}$ be the $(n, k) = (7, 4)$ Hamming code. All Hamming codes have minimum distance three, and can correct any single bit error, i.e., $t = 1$. One possible generator matrix is

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{6}$$

The ground station chooses a 7×7 permutation matrix P and a 4×4 scrambling matrix S. For our example, let

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{7}$$

Note that every row and every column of P has exactly one '1', which makes it a permutation matrix. Now, given the G, S, and P matrices from above, the public key (G') per (1) is

$$G' = SGP = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}, \tag{8}$$

where G' is computed in $\mathbb{F}_2$. The public key (G', t) is shared with the test article prior to data transmission.

Now, suppose the test article wants to communicate message $m = [0\ 1\ 1\ 0]$ to the ground station. First the test article needs to select an n-bit random error vector e with weight 1, for example $e = [0\ 1\ 0\ 0\ 0\ 0\ 0]$. Then the test article computes the codeword x per (2) as

$$x = mG' + e = [1\ 0\ 0\ 1\ 1\ 0\ 1] + [0\ 1\ 0\ 0\ 0\ 0\ 0] = [1\ 1\ 0\ 1\ 1\ 0\ 1], \tag{9}$$

which the test article then sends to the ground station.

Upon receiving x, the ground station applies the inverse of the permutation matrix

$$P^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}, \tag{10}$$

to calculate $\hat{x}$ per (3), which is

$$\hat{x} = [1\ 1\ 1\ 1\ 1\ 0\ 0]. \tag{11}$$

In the next step, the ground station decodes $\hat{x}$ using the Hamming decoding algorithm. The decoder computes the syndrome of $\hat{x}$ as $[0\ 1\ 1]$, which is corresponds to the error pattern $[0\ 0\ 1\ 0\ 0\ 0\ 0]$ (based on syndrome decoding). Then the ground station uses the output of the Hamming decoder to correct the detected error of $\hat{x}$, which leads to the correct codeword

$$x = [1\ 1\ 0\ 1\ 1\ 0\ 0]. \tag{12}$$

Since the generator matrix G is in the systematic form ($[I_k|\Gamma]$), for $k = 4$, it is obvious that

$$mS = [1\ 1\ 0\ 1]. \tag{13}$$

The last step of the decryption uses (5) to compute

$$m = mSS^{-1} = [1\ 1\ 0\ 1] \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = [0\ 1\ 1\ 0], \tag{14}$$

which is equal to the original transmitted message from the test article.

Performance Analysis

There are two potential attacks on the McEliece cryptosystem. The first is to attempt to recover the components of the public key, G', including G, S, and P matrices. The second is the brute force approach of constructing the original vector m from the transmitted codeword x. Both attacks have been proved to be computationally intractable, especially when n and t are large.

The first attack can be prevented because there are too many possibilities for the scrambling matrix S and the permutation matrix P to recover the generator matrix, so G is sufficiently obscure because P permutes the rows of G, and S scrambles the columns.

The secrecy of the second attack, which involves breaking down x into its original message m, depends on the code type and its corresponding parameters, such as dimensions and error-correction capability. As mentioned earlier, the original version of the McEliece algorithm has been designed with $n = 1024$, $k = 524$, and $t = 50$, hence there are $\binom{1024}{50} = 3.1901e + 85$ different patterns for e [14].

Finally, we should note that although the McEliece cryptosystem is based on the syndrome-decoding problem which has been shown to be an NP-complete problem [21], however, NP-completeness only implies that the worst case of syndrome-decoding is hard to solve. There may exist instances when the hardness of the decoding algorithm will be lessened, and these should be avoided in practice [22].

One drawback of the McEliece cryptosystem is the authentication problem of the transmitter. Due to the fact that the encryption method is not a one-to-one process and the overall encryption technique is clear to everyone, the McEliece algorithm cannot be utilized for authentication or signature schemes. For instance, in the case where the eavesdropper is an active attacker, it might send fake messages that have been encrypted with the ground station's public key.

To protect the system from such attacks, we suggest implementing a Hash-based signature using a different secure key which is placed in the test article ahead of time. This extra piece helps the ground station to authenticate the legitimate transmitter. The idea is to add an authentication tag, which uses a hashing algorithm on the codeword x along with the secure key, to the codeword on the transmitter side. The receiver can then verify the identity of the transmitter by checking the tag during the decoding process as shown in Fig 4. Note that many variants of this idea could be implemented. We showcase only one possibility here.

CONCLUSION

In this paper we have discussed well-known security vulnerabilities that may occur in communication systems upon the advent of full-scale quantum computing. We briefly reviewed both pre-quantum and post-quantum cryptosystems. Post-quantum solutions are an active branch of research amongst security engineers and computer scientists, and specific algorithms discussed herein are still being researched and vetted for possible vulnerabilities. We further showed how the McEliece algorithm may be used in the iNET standard to bring about secure communication over telemetry links, even in cases where keys need to be refreshed during test. This paper provides useful examples and guidelines for the next generation of cryptographic algorithms in AMT, but does not provide a complete security solution for post-quantum cryptography. Additional research is required to ensure that implementations are secure, and that new cryptosystems can support the required throughput and computational limitations imposed by telemetry links.

ACKNOWLEDGEMENTS

The authors wish to thank Daniel Harman for an early proofreading of the paper.

REFERENCES

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, (New York, NY, USA), p. 212–219, Association for Computing Machinery, 1996.

[3] D. Simon, "On the power of quantum computation," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 116–123, 1994.

[4] D. J. Bernstein and T. Lange, "Post-quantum cryptography—dealing with the fallout of physics success." Cryptology ePrint Archive, Paper 2017/314, 2017. `https://eprint.iacr.org/2017/314`.

[5] M. Raavi, P. Chandramouli, S. Wuthier, X. Zhou, and S.-Y. Chang, "Performance characterization of post-quantum digital certificates," in *2021 International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–9, 2021.

[6] P. J. Noonan, T. A. Newton, G. C. Willden, T. B. Grace, and W. A. Malatesta, "iNET system manager," in *Proc. Int. Telemetering Conf. (ITC)*, Oct. 2014.

[7] D. S. Skelley, "Integrated network-enhanced telemetry," in *Proc. Int. Telemetering Conf. (ITC)*, 2003.

[8] M. Rice, K. Temple, T. Chalfant, D. Ernst, and C. Kahn, "Spectrum allocations: The aeronautical telemetry story in the USA," *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 12, pp. 50–58, 2018.

[9] W. K. Harrison, K. Nelson, and S. Dye, "Physical-layer security for aeronautical telemetry," in *Proc. Int. Telemetering Conf. (ITC)*, Nov. 2018.

[10] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, "Advanced encryption standard (aes)," 2001-11-26 2001.

[11] M. Shoushtari and W. Harrison, "Secrecy coding in the integrated Network Enhanced Telemetry (iNET)," 9 2021.

[12] M. Hayward, "Quantum computing and shor's algorithm," 2015.

[13] M. Krelina, "Quantum technology for military applications," *EPJ Quantum Technology*, vol. 8, pp. 1–18, 2021.

[14] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *DSN Report*, vol. 42-44, pp. 114–116, 1978.

[15] J. C. Lagarias, H. W. Lenstra, and C.-P. Schnorr, "Korkin-zolotarev bases and successive minima of a lattice and its reciprocal lattice," *Combinatorica*, vol. 10, pp. 333–348, 1990.

[16] A. Rostovtsev and A. Stolbunov, "Public-key cryptosystem based on isogenies," 2006. stolbunov@list.ru 13297 received 13 Apr 2006, last revised 29 May 2006.

[17] T. Yasuda, X. Dahan, Y.-J. Huang, T. Takagi, and K. Sakurai, "A multivariate quadratic challenge toward post-quantum generation cryptography," *ACM Commun. Comput. Algebra*, vol. 49, p. 105–107, nov 2015.

[18] D. J. Bernstein, *Introduction to post-quantum cryptography*, pp. 1–14. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[19] S. Gao and R. Heindl, "Multivariate public key cryptosystems from diophantine equations," *Designs, Codes and Cryptography*, vol. 67, no. 1, pp. 1–18, 2013.

[20] W. Beullens, "Breaking rainbow takes a weekend on a laptop." Cryptology ePrint Archive, Paper 2022/214, 2022. `https://eprint.iacr.org/2022/214`.

[21] E. Berlekamp, R. McEliece, and H. van Tilborg, "On the inherent intractability of certain coding problems (corresp.)," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[22] C. Monyk, "Quantum cryptography," in *Handbook of Information and Communication Security* (P. P. Stavroulakis and M. Stamp, eds.), pp. 159–174, Springer, 2010.