 doi:10.20944/preprints202104.0734.v1

Article

Code-based Post-Quantum Cryptography

Chithralekha Balamurugan[1,†], Kalpana Singh[2,‡]*, Ganeshvani Ganesan[3,†], and Muttukrishnan Rajarajan[4,§]

[1] Pondicherry University; tchithralekha.csc@pondiuni.edu.in
[2] IRT SystemX; kalpana.singh@irt-systemx.fr
[3] Pondicherry University; vaniganesh0306@gmail.com
[4] City, University of London; r.muttukrishnan@city.ac.uk
* Correspondence: kalpana.singh@irt-systemx.fr; Tel.: +33 755962727
† Pondicherry University, Chinna Kalapet, Kalapet, Puducherry 605014, India: Pondicherry University
‡ 2 Boulevard Thomas Gobert, 91120 Palaiseau, France: IRT SystemX
§ Northampton Square, Clerkenwell, London EC1V 0HB, United Kingdom: City, University of London

Abstract: Cryptography has been used from time immemorial for preserving the confidentiality of data/information in storage or in transit. Thus, cryptography research has also been evolving from the classical Caesar cipher to the modern cryptosystems based on modular arithmetic to the contemporary cryptosystems based on quantum computing. The emergence of quantum computing imposes a major threat on the modern cryptosystems based on modular arithmetic whereby, even the computationally hard problems which constitute for the strength of the modular arithmetic ciphers could be solved in deterministic time. This threat triggered post-quantum cryptography research in order to design and develop post-quantum algorithms that can withstand quantum computing attacks. This paper provides a review of the various post-quantum cryptography and, in specific, code-based cryptography research dimensions. The research directions that are yet to be explored in code-based cryptography research is another key contribution of this paper.

Keywords: Quantum computing; Post-quantum cryptography; Code-based cryptography; cryptosystem; cryptography; Privacy

1. Introduction

Cryptographic systems are built upon complex mathematical problems such as integer factorization and computing discrete logarithms [1] [2], which can only be solved if knowledge of some secret data is available; typically a very large number. Without these numbers, it is impossible to reverse-engineer encrypted data or create a fraudulent digital signature. These numbers are what we know as cryptographic keys. For instance, the RSA algorithm [3] works by using pairs of very large prime numbers to generate public and private keys. The public key can be used to create a mathematical challenge that can only be solved by someone who holds the private key. Attempting to guess the answer, by way of a brute-force search, would take thousands of years using contemporary computers. Unlike their classical counterparts, quantum computers will be able to solve these mathematical problems incredibly quickly. The asymmetric algorithms we use today for digital signatures and key exchange will no longer be strong enough to keep data secret once a sufficiently powerful quantum computer can be built.

This means that core cryptographic technologies that we have to rely on, RSA and elliptic curve cryptography, will become insecure. By contrast, symmetric algorithms and hash functions are only partially affected by quantum computers – the best quantum algorithms are about twice as fast as their classical counterparts, so key lengths and hash sizes will need to double. But we can still continue to use the same families of symmetric algorithms (such as AES) without concern.

This context alludes to the fact that asymmetric algorithms which are in widespread use today can succumb to quantum attacks and hence, quantum attack resistant or in other words post-quantum cryptographic algorithms need to be evolved.

Certain candidate families of post-quantum schemes have been realized including code-based [4], hash-based [5], multivariate [6], lattice-based [7,8] and isogeny-based [9] solutions. The maturity in post-quantum research has led to the formulation of various post-quantum cryptosystems, standardization of post-quantum algorithms by various standardization bodies world-wide, industry adoption of post-quantum technology and the development of open source post-quantum libraries.

In this paper, a literature review of post-quantum research in the above said dimensions have been carried out and presented here. Further, a deep dive into code-based cryptography (CBC) has been carried out with respect to the linear codes and their operations and relationships, CBC cryptosystems, attacks on CBC, etc. This deep dive has been instrumental in identifying the prospective research directions that could be explored in CBC research.

Section 2 briefs about quantum computing and alludes to the motivation for post-quantum cryptographic research. Section 3 reviews post-quantum research dimensions with due summaries and comparisons. Section 4 explains the CBC research dimensions. Section 5 describes the white spaces that are yet to be addressed in CBC research. Section 6 concludes the paper.

2. Quantum Computing

A quantum computer is a machine which employs quantum-physical phenomena to perform computations in a way that's fundamentally different from a "normal", classical, computer [10]. Whereas a classical computer is, at any point in time, in a fixed state-such as a bit string representing its memory contents-the state of a quantum computer can be a "mixture", a so-called superposition, of several states. Classical computers carry out logical operations using the definite position of a physical state. These are usually binary, meaning its operations are based on one of two positions. A single state - such as on or off, up or down, 1 or 0 - is called a bit. Note that the internal state is hidden: the only way to get information about the state is to perform a measurement, which will return a single non-superimposed classical output, such as a bit string, that is randomly distributed according to the internal state, and the internal state gets replaced by the measurement outcome.

The work was initiated by several mathematicians and physicists such as Paul Benioff (1980) [11], Yuri Manin (1980) [12], Richard Feynman (1982) [13], and David Deutsch (1985) [14]. With decades of research, the development of quantum computing has been challenging yet groundbreaking.

Thus, Quantum computing constitutes for a new computing paradigm which is expected to solve complex problems that require far more computational power than what is possible with current generation of computer technologies. Advance research in materials science, molecular modelling, and deep learning are a few examples of complex problems that quantum computing can solve. Quantum computing, in essence, is the ultimate in parallel computing, and hence has the potential to tackle problems conventional computers can't handle.

Shor's 1994 and Grover's 1996 Algorithms

On the quantum algorithmic development, there are two groundbreaking algorithms which have laid out a strong foundation towards breaking today's number theoretic based public key cryptosystems. In 1994, Shor proposed a polynomial-time (efficient) algorithm [15] for solving integer factorization and discrete logarithm problems. The algorithm relies on the existence of quantum computers, and hence this type of algorithms is called quantum algorithms in this article. Shor's quantum algorithm and its variants can be used for breaking most of the currently used public-key cryptosystems. %including those based on ECC, which is generally used in Blockchain systems and cryptocurrencies.

 doi:10.20944/preprints202104.0734.v1

In 1996, Grover proposed an $O(\sqrt{N})$-time quantum algorithm for functions with N-bit domains [16]. This quantum algorithm once realized on quantum computers can be used for breaking symmetric key cryptosystems, and to defend against attacks based on Grover's algorithm, we need to double the key sizes in order to achieve the similar level of security against conventional computers.

For example, for 128-bit symmetric key security, we need to use symmetric key cryptosystems which are originally designed for achieving 256-bit security against attacks based on Grover's quantum algorithm. It is also predicted that quantum computers will be able to break several of today's cryptographic algorithms that are used to secure communications over the internet, provide root of trust for secure transactions in the digital economy and encrypt data. To protect against attacks from quantum computers, vendors of security products and service providers must constantly assess the risk associated with the choice of crypto algorithms. The choice of algorithms will have to evolve from those that are quantum resistant to entirely new algorithms for the post-Quantum world.

3. Post-Quantum Cryptography

Post-quantum cryptography (PQC) is about devising cryptographic algorithms that are secure in the quantum era with security against both classical/conventional and quantum computers. There are several candidate approaches for building post-quantum cryptographic schemes as described below in Subsection 3.1 [17], [18], [19].

3.1. Post-quantum cryptography candidates

This subsection delineates the candidates of the PQC schemes. These are hash-based cryptography, code-based cryptography, multivariate cryptography, lattice-based cryptography and isogeny-based cryptography schemes.

Hash-based cryptography

Hash-based cryptography focuses on designing digital signature schemes based on the security of cryptographic hash functions, e.g. SHA-3. These schemes are based on the security of hash functions (as one-way function) and require less security assumptions than number-theoretic signature schemes (e.g. RSA, DSA). Ralph Merkle in 1989 introduced Merkle Signature Scheme (MSS) [20] that is based on a one-time signatures (e.g. the Lamport signature scheme) and uses a binary hash tree (Merkle tree). The MSS is resistant against quantum computer algorithms. More details can be found in this survey on hash-based schemes Butin (2017) [21]. Sphincs+ hash-based signature [22] is chosen as an alternate solution in the outcome of third round of NIST standardisation process.

Code-based cryptography

Code-based cryptography [23] has its security relying on the hardness of problems from coding theory, for example, Syndrome Decoding (SD) and Learning Parity with Noise (LPN). These cryptosystems are based on error correcting codes to construct a one-way function. The security is based on the hardness of decoding a message which contains random errors and recovering the code structure. Classic McEliece code-based encryption scheme [4] is chosen as a finalist scheme in the outcome of third round of NIST standardisation process.

Multivariate cryptography

Multivariate-based cryptography has its security relying on the hardness of solving multivariate systems of equations.These schemes are based on systems of multivariate polynomial equations over a finite field F. There are several variants of multivariate cryptography schemes based on Hidden Field Equations (HFE) trapdoor functions such as The Unbalanced Oil and Vinegar Cryptosystems (UOV). UOV are used for signatures.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

Other examples of multivariate cryptography are Rainbow, TTS or MPKC schemes. More about current state of the multivariate cryptography schemes can be found in the paper of Ding and Petzoldt (2017) [24]. Two multivariate-based signature schemes are chosen in the outcome of third round of NIST. Rainbow [25] is one of the finalist. GeMSS [26] is one of the alternate finalist scheme.

Lattice-based cryptography

Lattice-based cryptography seems to be one of the most active directions in recent years due to several key reasons. First, it has strong security guarantees from some well-known lattice problems, for example, Shortest Vector Problem (SVP) and the Ring Learning With Errors (RLWE) problem [27]. Second, it enables powerful cryptographic primitives, for example, fully homomorphic encryption (FHE) and functional encryption [28]. Third, some new lattice-based cryptographic schemes have become quite practical recently, for example, the key exchange protocol NewHope [29], and a signature scheme BLISS [30].

Lattice-based cryptography is one of the successful scheme in the third round result of the NIST standardisation process. Kyber [31], NTRU [32], SABER [33] lattice-based encryption schemes are chosen as the finalists schemes. NTRUprime [34] is in the alternate finalist lattice-based encryption scheme. Dilithium [35], Falcon [36] lattice-based signature schemes are also finalist schemes.

Isogeny-based Cryptography

Isogeny-based cryptography is a specific type of post-quantum cryptography that uses certain well behaved maps between abelian varieties over finite fields (typically elliptic curves) as its core building block. Its main advantages are relatively small keys and its rich mathematical structure, which poses some extremely interesting questions to cryptographers and computer allegorists. These schemes are based on supersingular elliptic curve isogenies [9] that are secure against quantum adversaries. These schemes are secured under the problem of constructing an isogeny between two supersingular curves with the same number of points. Isogeny-based schemes may serve as digital signatures or key exchange such as Supersingular Isogeny Diffie-Hellman (SIDH) scheme [37]. SIKE [38] is only isogeny-based encryption scheme in the alternate list of NIST third round result. There is no isogeny-based signature scheme identified in the NIST third round outcome.

Comparison of Post-Quantum Cryptography Algorithms

A comparison of the various post-quantum cryptographic algorithms categories along with the most prevalent algorithm in each category is provided in Table. 1. An earlier comparison of Post-Quantum Cryptographic algorithms has also been attempted in [39].

3.2. Industry adoption of PQC

The industry adoption of post-quantum cryptography is happening very aggressively. In this front, the following lines of works are found to be available

- Industry survey of post-quantum cryptography
- Revenue Assessment of post-quantum cryptography
- Industry initiatives in PQC – PQC R&D, PQC based products, PQC products, PQC consulting

3.2.1. Industry survey

The industry survey has been carried out by Digicert involving IT Directors, IT Generalists, IT security professionals and other professionals belonging to USA, Germany and Japan. The survey focused on identifying the following:

- The awareness or the understanding about PQC with industry professionals

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

Table 1. Comparison of PQC algorithms

S. No.	Post-Quantum Algorithm Category	Post-Quantum Algorithms available in this Category	Name of Most Prevalent Algorithm	Type of Algorithm - Encryption/ Signature/ Key Excha- nge	Public Key	Private Key	Signa- ture	Strengths	Weaknesses	Li bo qs	Attacks	Other Detailed Comparisons
1	Lattice Based Crypto- gaphy	1. Encr- yption/ Decry- ption 2. Signa- ture 3. Key Exch- ange (RLWE)	NTRU Encrypt	E	6130 B	6743 B	–	1. More efficient encryption and decryption, in both hardware and software implementations 2. Much faster key generation allowing the use of disposable keys . 3. low memory use allows it to use in applications such as mobile devices and Smart-cards.	1. Com- plexity is high in NTRU 2. There is the possi- bility of the occur- rence of a decryption failure from a validly created ciphertext	✓	Brute Force attack, meet-in- middle attack, lattice reduction attack, chosen cipher text attack	Gaithru et al 2014
			BLISS II (Bimodal Lattice Signature Scheme)	S	7 KB	2 KB	5 KB			✗	Side Channel Attack, Branch tracing attack, Rejection Sam- pling, Scalar Product Leakage	Espitau et al 2017
2	Multi- Variate	Signature only	Rainbow	S	124 KB	95 KB	424 KB	It is based on the difficulty of solv- ing systems of mul- tivariate equations	Only Sig- nature Scheme is available and not a complete cryptosys- tem	✓	Direct Attack, Min Rank At- tack, High Rank Attack, UOV Attack, UOV Reconciliation attack, Attacks against hash function	[Petzoldt]
3	Hash Based Signature	Signature Only	SPHINCS	S	1 KB	1 KB	41 KB	1. Best alternative to number theore- tic signature 2. Small and medi- um size signatures 3. Small Key size	1. Only Signature Scheme is available and not a complete crypto- system	✗	Subset Re- silience, One- wayness, Second Pre-image re- sistance, PRG, PRF and unde- tectability, Fault Injection Attacks	Bernstein et al [2015]
			SPHINCS+	S	32 B	64 B	8 KB		2. Speed	✓	Distinct- function multi- target second- preimage re- sistance, Pseu- dorandomness (of function families), and in- terleaved target subset resilience, Timing Attack, Differential and Fault Attacks	[Bernstein 2019]
4	Super singular elliptic curve isogeny cryptog- raphy	Key Ex- change Only	Supersing- ular Isogeny Diffie Helman (SIDH)	K	751 B 564 (com- pressed SIDH)	48 B 48 (com- pressed SIDH)	–	Difficulty of com- puting isogenies between super- singular elliptic curves which is im- mune to quantum attacks	Cannot be used for non- interactive key ex- change, can only be safely used with CCA2 protection	✓	Side channel at- tacks, Auxiliary points active at- tack, adaptive at- tack	Costello et al 2016
5	Code- Based Cryp- togra- phy	1. En- cryp- tion / Decryp- tion 2. Signa- ture	Classic Mc Eliece Cryp- tosystem	E	1 MB	11.5 KB	–	One of the cryp- tosystem which is successful till the third round of NIST Post-Quantum al- gorithm standard- ization process	Very Large Key size	✓	Structural Attack, Key recovery attack, Squaring Attack, Power Analysis Attack, Side Channel attack, Reaction attack, Distinguishing attack, message recovery attack	Tillich 2018, Repka et al, 2014

 doi:10.20944/preprints202104.0734.v1

- The industry professionals' prediction of timelines by which Quantum Computers would break the existing modular arithmetic cryptographic algorithms
- The understanding among the industry professionals about the significance of threat imposed by quantum computing on existing cryptographic algorithms
- The study of industry readiness to adopt PQC

The results obtained indicate that the awareness of PQC among industry professionals is reasonably good and they have a clear understanding of an appropriate timeline by which quantum computers would break the existing cryptographic algorithms. The impact of the threat imposed by PQC is also well perceived by the industry professionals. The survey also reveals the industry readiness in the adoption of PQC to be beyond 50%. These aspects indicate that the industry survey has helped to comprehend the line of thought and the industry awareness and preparedness for PQC among industry professionals which is very important to start being precautious and working out plans for adoption of PQC given the discernment of the threat due to quantum computing technology.

3.2.2. Revenue assessment of post-quantum cryptography

As per the ten year Market and Technology Forecast Report in [40], a comprehensive study about the prospective markets for PQC products and services has been carried out. The IT industry, cyber security industry, telecommunications industry, financial services industry, healthcare industry, manufacturing industry, PQC in IoT and public sector applications of PQC have been identified as prospective markets for PQC in the report. An elaborate study of how PQC could augment or enhance the functioning of the above industries has been detailed in the report. A ten year forecast of revenue assessment of PQC in each of the above industries is detailed in the said report, which is indicative of the prospective industry market and trend for PQC .

3.2.3. Industry initiatives in PQC–PQC R& D, PQC-based products, PQC products, PQC consulting

The IT industry has been closely following up with post-quantum cryptographic research and the standardization process. The industry initiatives could be observed in terms of the following.

- Research and development in post-quantum cryptography - organizations like IBM [41], Microsoft [42], etc. conduct research and development in post-quantum cryptography.
- Development of post-quantum based products - For example, Avaya has tied up with Post-Quantum (a leading organization developing post-quantum solutions), to incorporate post-quantum security into its products
- PQC products - Organizations like Infineon, Qualcomm (OnBoard Security), Thales, Envieta, etc. have developed post-quantum security hardware/software products [40].
- Post-quantum consulting - Ultimaco is one of the leading players which provides for post-quantum cryptography consulting.

The Table. 2 provides a comparison of the various industry initiatives of PQC with respect to PQC R&D, PQC based security products development, PQC product development and PQC consulting.

3.3. Standardization Efforts in PQC

The standardization of Post-Quantum algorithms has been taken up by different standardization bodies across the globe. The following section provides an overview of the standardization activities taken up by the following standardization bodies viz. NIST, ITU, ISO, ETSI, CRYPTREC.

Table 2: Summary of Industry Initiatives in Post-Quantum Cryptography

S. No.	Name of the Organization	Country	Type of PQC work involved	Algorithms used	Collaborator	PQC product developed
1.	Avaya [43]	USA	PQC based products		Post-Quantum	Quantum-safe messaging, voice calls and document sharing
2.	Envieta Systems [44]	USA	PQC products, PQC Consulting		–	Developed Hardware and Software Post-Quantum Implementation Cores including those for embedded systems as well
3.	Google [45]	USA	PQC products	HRSS-SXY (variant of NTRU encryption) and SIKE (supersingular isogeny)	Cloudfare	Post-quantum cryptography˙encryption and signature methods for chrome browser
4.	IBM [41]	Switzerland	R&D	Lattice-based Cryptography	–	Quantum safe Cloud and Systems
5.	Infineon [46]	Germany	PQC products	Variant of New Hope Algorithm	–	implemented a post-quantum key exchange scheme on a commercially available contactless smart card chip Post-Quantum security for Government Identity Documents,ICT technology, Automotive Security,Communication Protocols
6.	Isara [47]	Canada	PQC products	Hierarchical Signature Scheme (HSS) and eXtended Merkle Signature Scheme (XMSS)	Futurex, Post-Quantum	ISARA Radiate? Quantum-safe Toolkit is a high-performance, lightweight, standards-based quantum-safe software development kit, built for developers who want to test and integrate next-generation post-quantum cryptography into their commercial products
7.	Microsoft Research [42]	USA	PQC products	FrodoKEM , SIKE, Picnic, QTesla	–	Post-Quantum SSH, TLS, VPN
8.	Qualcomm / OnBoard Security [48]	USA	PQC based products	pqNTRUsign	OnBoard Security	OnBoard Security has developed a digital signature algorithm that can resist all known quantum computing attacks. pqNTRUsign will replace RSA and ECDSA, the most commonly used quantum-vulnerable signature schemes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

3.3.1. NIST

NIST is one of the primary bodies involved in the standardization of post-quantum algorithms [49]. The standardization process began in 2016 and it is currently in the third round after two previous rounds of Post-quantum algorithms evaluations. The third round finalists comprise of 4 public-key encryption algorithms and 3 digital signature algorithms along with 5 and 4 alternate candidates for public key encryption and digital signature algorithms respectively. These are listed in the table below. For the purpose of standardization, the algorithm submissions were first ensured to fulfill certain minimum acceptability requirements prior to evaluation and evicted otherwise. In each round, the evaluations were carried out using a set of criteria under security, cost and efficiency with respect to algorithm implementation aspects respectively. From Table. 3, it is obvious that lattice-based post-quantum technology has the majority contribution among the list of standardized post-quantum algorithms.

Table 3: NIST Standardization Efforts [50]

Post-Quantum Algorithm Type	Third Round Finalist	Technology	Alternate Candidates	Technology
Public Key Encryption / Key Encapsulation Mechanisms	Classic McEliece	Code	BIKE	Code
	CRYSTALS KYBER	Lattice	FrodoKEM	Lattice
	NTRU	Lattice	HQC	Code
	SABER	Lattice	SIKE	Supersingular Isogeny
Digital Signature Algorithms	CRYSTALS - DILITHIUM	Lattice	GeMSS	Multivariate Polynomial
	FALCON	Lattice	PICNIC	Other
	RAINBOW	Multivariate Polynomial	SPHIMCS+	Hash

3.3.2. International Telecommunication Union (ITU)

International Telecommunication Union (ITU) has two study groups SG13 and SG17 for PQC and a focus group FG QIT4N [51] which works on pre-standardization activities. SG13 has provided a plethora of standards under the categories of i)Architecture, Framework, Function of Quantum Key Distribution Network and ii) Quality of Service of Quantum Key Distribution Network. Some of these standards are published and many are work-in-progress. SG17 has provided a set of standards related to the security aspects of Quantum Key Distribution Network. FG QIT4N group focuses on the pre-standardization activities related to Quantum Information Technology for Networks. It has two working groups WG1 and WG2 working on this and relevant technical reports have been published by these working groups. A detailed listing of the standards and pre-standardization reports of ITU could be found in [51].

3.3.3. European Telecommunications Standards Institute (ETSI)

European Telecommunications Standards Institute (ETSI) ETSI develops ETSI group specifications and group reports describing quantum cryptography for ICT networks. The ETSI has been involved in Standardization activities of QKD since 2008. The standards developed by ETSI pertain to Quantum Safe Cryptography, CYBER and Quantum Key Distribution. Various standards under the said three categories have been developed by ETSI. The listing and details of the standards under the said categories could be found in [52].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

3.3.4. ISO

ISO/IEC JTC 1/SC 27 IT Security techniques include 5 working groups [51], [53]. SC27 has developed many cryptography standards in the past 28 years. In ISO/IEC JTC 1/SC27, WG2 is for standardization of Cryptography and security mechanisms. The standards cover a large scope, from relatively advanced topics such as homomorphic encryption, group signatures to some essential functions such as block ciphers and hash functions. A six month study period on Quantum Resistant Cryptography was initiated at SC 27/WG 2 meeting held in Jaipur, India October 2015. After the first six months, the study period has extended three times and determined to close at SC 27/WG 2 meeting held in Berlin, Germany November 2017. As a result of the study period, it was determined to generate a WG2 standing document (SD). An outcome of this post-quantum cryptography study is SD8. SD8 provides a survey on different categories/families of post-quantum cryptography and is intended to prepare WG2 experts for standardization. SD8 is created in multiple parts, where each part corresponds to each of the post-quantum cryptographic technique vis. Hash, Lattice, Code, etc. ISO/IEC JTC1 SC27 WG3 (ISO/IEC 23837) focusses on Security requirements, test and evaluation methods for quantum key distribution. This addresses QKD implementation security issues. A High-level framework for the security evaluation of QKD module under the Common Criteria (CC) (ISO/IEC 15408) framework has been evolved.

3.3.5. CRYPTREC

CRYPTREC is the Cryptography Research and Evaluation Committees set up by the Japanese Government to evaluate and recommend cryptographic techniques for government and industrial use. The following activities have been carried out as part of CRYPTREC.The CRYPTREC cipher list was published in 2013 followed by the CRYPTREC Report 2014 on lattice problems. The Cryptanalysis Evaluation Working Group was formed in 2015. This group has published a Report on PQC in 2018. CRYPTREC plans to revise the CRYPTREC Cipher List to include post-quantum algorithms by 2022-2024. The details of the above activities are detailed in [54]

Table. 4 provides a summary of all the standardisation efforts described.

In addition to the above efforts, the following works are being carried out by other organizations for PQC:

- IETF has formulated a Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2), [55], [56]
- libpqcrypto [57] is a new cryptographic software library produced by the PQCRYPTO project. libpqcrypto collects this software into an integrated library, with i) a unified compilation framework ii) an automatic test framework iii) automatic selection of the fastest implementation of each system iv) a unified C interface following the NaCl/TweetNaCl/SUPERCOP/libsodium API, v) a unified Python interface vi)command-line signature/verification/encryption/decryption tools, and vii) command-line benchmarking tools.
- The Cloud Security Alliance Quantum Safe Security Working Group's [58] goal is to address key generation and transmission methods that will aid the industry in understanding quantum-safe methods for protecting data through quantum key distribution (QKD) and post-quantum cryptography (PQC). The goal of the working group is to support the quantum-safe cryptography community in development and deployment of a framework to protect data whether in movement or at rest. Has published several reports and whitepapers on Quantum safe cryptography
- NSA is publicly sharing guidance on quantum key distribution (QKD) and quantum cryptography (QC) as it relates to securing National Security Systems (NSS). NSA is responsible for the cybersecurity of NSS, i.e., systems that transmit classified and/or otherwise sensitive data. Due to the nature of these systems, NSS owners require especially robust assurance in their cryptographic solutions; some amount of uncertainty may be acceptable for other system owners, but not for NSS. While it

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

Table 4: Summary of standardisation efforts in Post-Quantum Cryptography

Parameter	Country	Focus area of standardization in PQC	Function Standards / QOS Standards	Status
NIST	USA	Quantum resistant Algorithm Standardization for Cryptography, Key encapsulation mechanism, digital signature	Function Standards	Round 1 and Round 2 of standardization process is completed. Round 3 in progress
ETSI	Europe	Quantum Safe Cryptography, Quantum Key Distribution	Function Standards	Published standards
ISO	NA (A Non-Governmental Organization)	Quantum Key Distribution	Function Standards	Work in progress – Standards yet to be published
ITU	A specialized agency of United Nations	Quantum Key Distribution	Function and QOS Standards	Only two standards published. Others are work in progress
CRYPTREC	Japan	Quantum resistant Algorithm Standardization for Cryptography, Key encapsulation mechanism, digital signature	Function Standards	List of standardized algorithmsis expected to be published between2022-2024

has great theoretical interest and has been the subject of many widely publicized demonstrations, it suffers from limitations and implementation challenges that make it impractical for use in NSS operational networks.

4. Code-based Cryptography

Linear Codes [18] are originally used for Digital Communication and based on Coding Theory. Coding theory is an important study which attempts to minimize data loss due to errors introduced in transmission from noise, interference or other forces. Data to be transmitted is encoded by the sender as linear codes which is decoded by the receiver. Data encoding is accomplished by adding additional information to each transmitted message to enable the message to be decoded even if errors occur.

Different codes are being studied to provide solutions for various problems occurring in applications. The most prominent type of error-correcting codes are called linear codes. The linear codes can be represented by k x n matrices where k is the length of the original messages, n is the length of the encoded message. It is computationally difficult to decode messages without knowing the underlying linear code. This hardness underpins the security of the code-based cryptosystem which includes all cryptosystems, symmetric or asymmetric, whose security relies, partially or totally, on the hardness of decoding in a linear error correcting code, possibly chosen with some particular structure or in a specific family of linear codes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

[59], [60]Linear codes are linear block codes over an alphabet $A = F_q$, where F_q denotes the finite field with $q = p^l$ elements $l \in N^x$, p prime. The alphabet is often assumed to be binary that is $p = 2, l = 1, q = 2$, F2= $\{0, 1\}$. The encoding of the source bits is done in blocks of predefined length k, giving rise to the name "block code". In code-based Cryptography, only binary codes are considered i.e. codes over F2.

The following are the matrices used in code-based cryptography.

- A Generator matrix G of an $[n, k]$ code C is a kn matrix G such that $C = \{xG : x \in F_2^k\}$. Generator matrix is of the form $(I_k \mid Q)$, where I_k is the $(k \times k)$ identity matrix and Q is a $k \times (n\text{-}k)$ matrix (redundant part).
- A Parity- Check matrix H of an $[n, k]$ code C is an $(n\text{-}k) \times n$ matrix H such that $C = \{c :\in F_2^n : Hc^T = 0\}$.
- Parity-check matrix H is generated from the generator matrix as $H = (Q^T \mid I_{n-k})$.

Encoding process applies an injective F_2 -linear function $f_c : F_2^k \to F_2^n$ on an input block of length k. i.e Every codeword can be generated by multiplying a source vector $x \in F_2^k$ with $GC = x \cdot G \mid x \in F_2^k \leq F_2^n$. Hence, the matrix G corresponds to a map $F_2^k \to F_2^n$ mapping a message of length k to an n-bit string. This encoding process corresponds to encryption in code-based cryptography.

The decoding process is about finding the closest codeword $x \in C$ to a given $y \in F_2^n$ assuming that there is a unique closest codeword. Decoding a generic binary code of length n and without knowing anything about its structure requires about $2^{\frac{(0.5+o(1))\times n}{log_2(n)}}$ binary operations assuming a rate $\approx 1/2$. The following are the common decoding techniques [60]:

- List Decoding – given C and x, outputs the list $L_c(x, t) := \{c \in C \mid d(x, c) \leq t\}$, of all codewords at distance at most t to the vector x with decoding radius t.
- Minimum Distance Decoding - Minimum distance decoding (MDD) is also known as nearest neighbour decoding and tries to minimize the Hamming distance $d(x; y)$ for all codewords $y \in C$ given a received F_2^n.
- Maximum Likelihood Decoding - Given a received codeword $x \in F_2^n$ maximum likelihood decoding (MLD) tries to find the codeword $y \in C$ to maximize the probability that x was received given that y was sent.
- Syndrome Decoding - For an $[n; k; d]$ code C we can assume that the parity check matrix H is given. Syndrome $S = [Y][H^T]$, Y is received code and $x = e + Y$ where e is the error bit.

The decoding process corresponds to the decryption in code-based cryptography.

4.1. Different Types of Error Correcting Codes

Error Correcting Codes could be broadly classified into Block Codes and Convolutional Codes [60].

In Block Codes, the input is divided into blocks of k digits. The coder then produces a block of n digits for transmission and the code is described as an (n, k) code as depicted in Fig. 1. Linear block Codes and Non-Linear Block Codes are types of Block Codes.

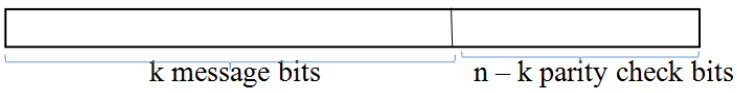

Figure 1. Sample Code Word of length n.

In convolutions coding, the coder input and output are continuous streams of digits. The coder outputs n output digits for every k digits input, and the code is described as a rate k/n code. The different types of linear codes used are as follows [61], [62] [59] : Hamming Code, Simplex Code, Reed Muller Code, Reed Solomon Code, BCH

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

(Bose, Chaudhuri, Hocquenghem) Code, Generalized Reed Solomon Code, Wozencraft Ensemble, Alternant Code, Justesen Code, Golay Code, Quadratic Residue Code. Here, the Alternant Code is a family of codes by itself and consists of the following codes in its family – Goppa Codes, Generalized Shrivastava Codes, Shrivastava Code, Chien-Choy Generalized BCH code, Narrow sense primitive BCH Code and t-error correcting BCH code. The more recent types of codes include Low Density Parity Check Code (LDPC), Medium Density Parity Check Code (MDPC), Quasi-Cyclic Alternant Code, Quasi-Dyadic Goppa Code [63], Rank Metric (Gabidulin) Code, etc..

The different types of non-linear codes are as follows [61]: Conference matrix code, Delsarte-Geothals Generalized kerdock code, Hadamard matrix code, Geothals non linear code, Preparata code, Nordstorn robinson code, Kerdock code, etc..

4.2. Operations on Codes

In many applications, the allowed length of the error control code is determined by system constraints unrelated to error control. When the length of the code one wish to use is unsuitable, the code's length can be modified by the following operations on codes viz. i) puncturing, ii) extending, iii) shortening, iv) lengthening, v) expurgating, or vi) augmenting which can be carried out in the following ways:

- An (n, k) code is punctured by deleting any of its parity bits to become a $(n-1, k)$ code.
- An (n, k) code is extended by adding an additional parity bit to become a $(n+1, k)$ code.
- An (n, k) code is shortened by deleting any of its information bits to become a $(n-1, k-1)$ code.
- An (n, k) code is lengthened by adding an additional information bit to become a $(n+1, k+1)$ code.
- An (n, k) code is expurgated by deleting some of its codewords. If half of the codewords are deleted such that the remainder form a linear subcode, then the code becomes a $(n, k-1)$ code.
- An (n, k) code is augmented by adding new codewords. If the number of codewords added is 2k such that the resulting code is linear, then the code becomes a $(n, k+1)$ code.

4.3. Properties to be fulfilled by Linear Codes

Researchers have specified certain bounds to be fulfilled in order to constitute for linear codes. These bounds are specified in terms of the hamming distance of the linear code. Towards this, we have the following definitions [61]:

- The Hamming Distance between two linear codes in F_2^n is the number of coordinates where they differ.
- The Hamming Weight of a linear code is the number of non-zero coordinates.
- The Minimum Distance d_{min} of a linear code C is the smallest Hamming weight of a nonzero codeword in C.
- A code is called maximum distance separable (MDS) code when its d_{min} is equal to $n-k+1$. A family of well-known MDS non-binary codes is Reed-Solomon codes.

There exists many bounds for linear codes,which are mentioned below. Plotkin bound and the Hamming bound are upper bounds on d_{min} for a given fixed value of n and k. The Hamming bound is a tighter bound for high rate codes but the Plotkin bound is for low rate codes.

- Singleton Bound [61], [59]: The minimum distance d_{min} for an (n, k) Binary Linear Block Code is bounded by $d_{min} \leq (n-k+1)$.
- Plotkin bound [61]: For any (n, k) binary linear block code, $d_{min} \leq \frac{n \times 2^{k-1}}{(2^{k}-1)}$,the minimum distance of a code cannot exceed the average weight of all nonzero codewords.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

- Gilbert Varshamov Bound [61]: For a fixed value of n and k, Gilbert-Varshamov Bound gives a lower bound on d_{min}. According to this bound, if $\sum_{j=0}^{(d_{min}-2)} \binom{n-1}{j} \leq 2^{n-k}$ then there exists an (n,k) binary linear block code whose minimum distance is outlast d_{min}.
- A Hamming sphere of radius t contains all possible received vectors that are at a Hamming distance less than t from a code word. The size of a Hamming sphere for an (n,k) Binary Linear Block Code is, $V(n,t)$, where $V(n,t) = \sum_{j=0}^{t} \binom{n}{j}$.
- The Hamming bound: A t-error correcting (n,k) Binary Linear Block Code must have redundancy n − k such that $(n\text{-}k) \geq \log_2 V(n,t)$. An (n,k) Binary Linear Block Code which satisfies the Hamming bound is called a perfect code.

4.4. Relationship Between Codes

Based on the study of the various linear codes, the following relationship between codes have been identified as part of this research work, which are depicted in Fig. 2. The relationship between the special codes are depicted in Fig. 3.

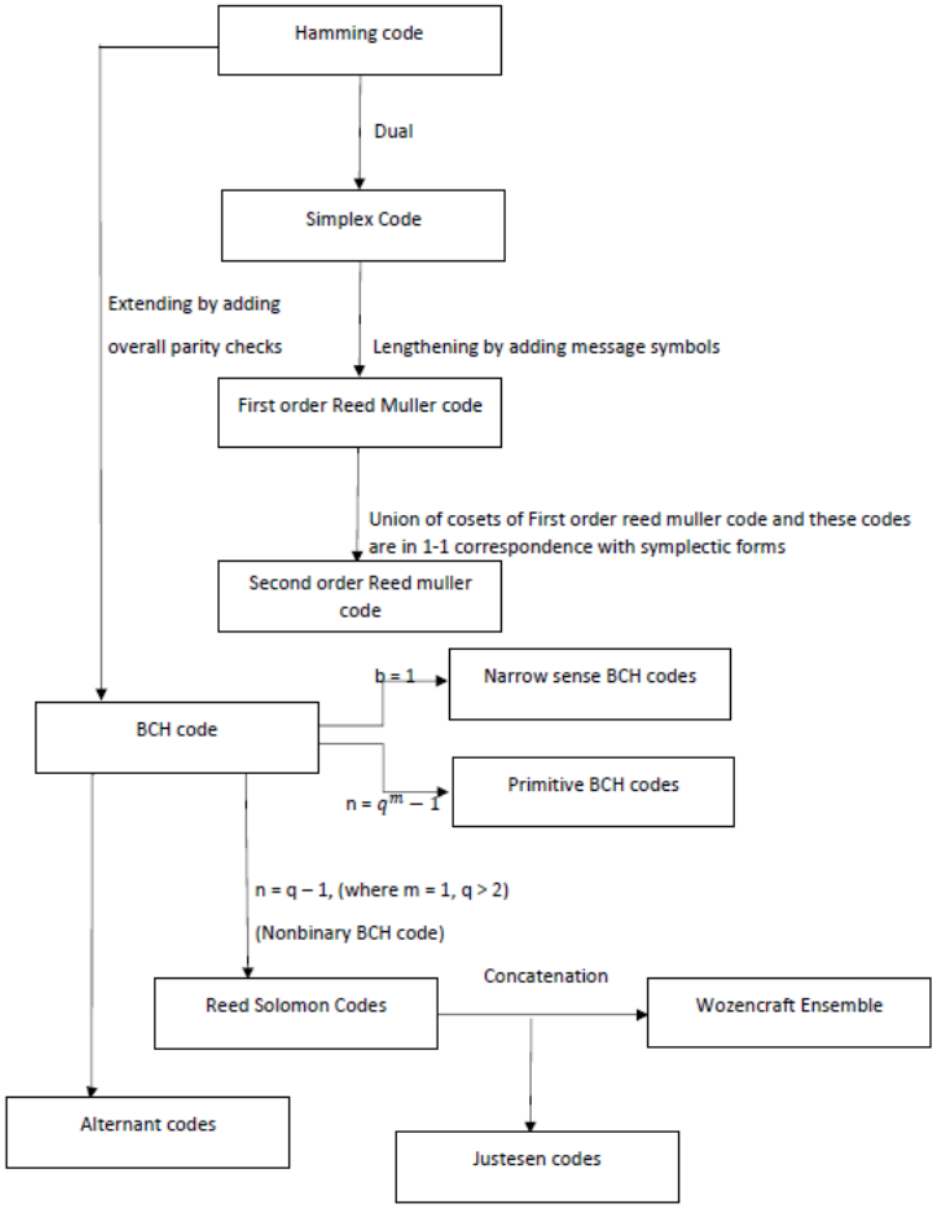

Figure 2. Relationship Between Codes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

4.5. Common Code-based Cryptosystems

Code-based Cryptosystems provide for code-based cryptography and code-based signature schemes.

4.5.1. Code-based Cryptography

McEliece and Niedereitter are the two of the earliest cryptographic algorithms developed in code-based cryptography. The McEliece was initially built in 1978 using the binary goppa code with [n,k] = [1024, 524] [64]. Subsequently, several variants of McEliece were built using different linear codes [65]. But, those variants were proven to be susceptible to attacks [18], [66] and only the McEliece built using the Binary Goppa Code is found to be quantum attack resistant till date. Thus, it has also been chosen for the third round of standardization by NIST. The McEliece has quadratic complexity in block length and no polynomial time quantum algorithm is found to decode the general linear block code [23]. Also, the Cryptosystem incorporates an element of randomness in every encryption by the use of e which is a randomly generated error vector [67]. These are the advantages of McEliece [67]. The large key size is the limitation of McEliece [67], [23].

The Niedereitter cryptographic algorithm was developed in 1986 and is very similar to McEliece and encrypts messages using parity check matrices unlike generator matrices used in McEliece and uses the Generalized Reed Solomon Codes. Table. 5 shows an indicative comparison of the two cryptosystems.

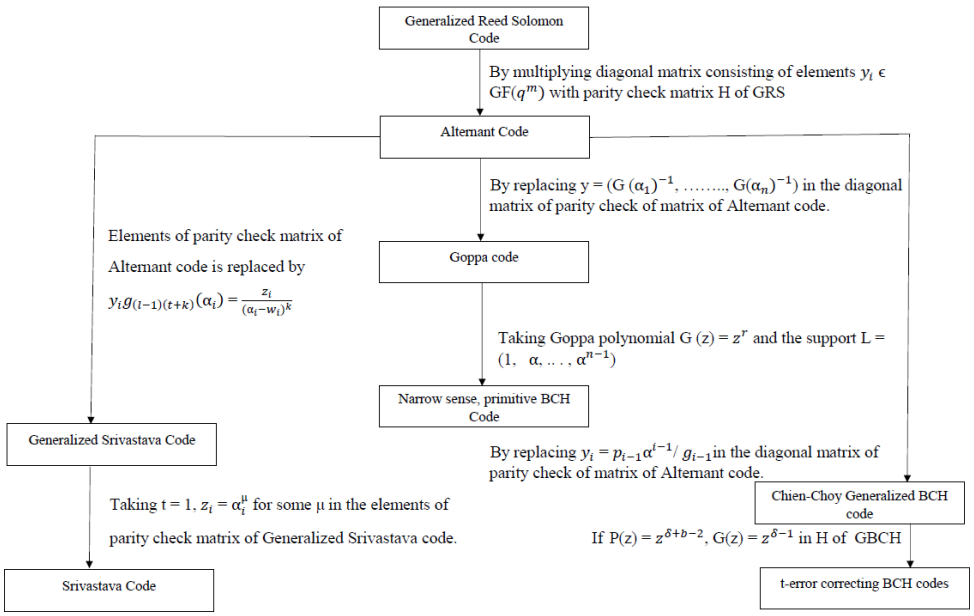

Figure 3. Special codes.

4.5.2. Code-based signature schemes

Signature schemes based on linear codes have been developed based on FDH-like (Full Domain Hash) approach by Courtois–Finiasz–Sendrier (called CFS) and uses Goppa Codes. The modified CFS signature – mCFS was developed by Dallot. Signature schemes based on Fiat-Shamir Transformation on zero knowledge identification schemes have been developed by Stern et al [], Jain et al [], Cayrel et al []. But none of the code-based signature schemes have been shortlisted by NIST for the third round of standardization. A comparison of the latter three signature schemes is provided in Table. 6 [71].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

Table 5: Common Code-based Cryptosystems, Codes used and thier Application.

S.No	Code-based Cryptography	Technique & Codes used	Applied to
1	Mc Eliece	Binary Goppa Codes, GRS, Concatenated Codes, Product codes, Quasi- Cyclic, Reed muller codes, Rank matric (Gadidulin) codes, LDPC, MDPC, Genaralized Shri vastava codes	Computing Systems, Embedded Devices [68], FPGA systems [69]
2	Niederreiter	GRS Codes	Computing Systems, FPGA Systems [70]

Table 6: Comparison of Code-based signature schemes

	Stern		**Jain et al**		**Cayrel et al**	
Keygen	0.0170	ms	0.0201	ms	0.339	ms
Sign	31.5	ms	16.5	ms	24.3	ms
Verify	2.27	ms	135	ms	9.81	ms
sk	1.24	bits	1536	bits	1840	bits
pk	512	bits	1024	bits	920	bits
System	65.5	kB	65.5	kB	229	kB
prams	245	kB	263	kB	229	kB
Signature						

4.6. Attacks in Code-based Cryptography

The following are the different types of attacks which the code-based cryptographic algorithms have been subject to [2].

- **Broadcast attack** - This attack aims to recover a single message sent to a number of recipients. Here the cryptanalyst knows only several ciphertexts of the same message. Since the same message is encrypted with several public-keys, it was found that it is possible to recover the message.
- **Known partial plaintext attack** - A known partial plaintext attack is an attack for which only a part of the plaintext is known.
- **Generalised known partial plaintext attack** - this attack allows to recover the plaintext by knowing some bit's positions of the original message.
- **Message-resend attack** - A message-resend condition is given if the same message is encrypted and sent twice (or several times) with two different random error vectors to the same recipient.
- **Related-message** - In a related-message attack against a cryptosystem, the attacker obtains several ciphertexts such that there exists a known relation between the corresponding plaintexts.
- **Chosen plaintext (CPA) and chosen-ciphertext attacks (CCA)** –
  - A chosen-plaintext attack is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key. For some chosen-plaintext attacks, only a small part of the plaintext needs to be chosen by the attacker: such attacks are known as plaintext injection attacks. Two forms of chosen-plaintext attack can be distinguished:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

    - Batch chosen-plaintext attack, where the cryptanalyst chooses all plaintexts before any of them are encrypted.
    - Adaptive chosen-plaintext attack, where the cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.
  - In a chosen-ciphertext attack, an attacker has access to a decryption oracle that allows to decrypt any chosen-ciphertext (except the one the attacker attempts to reveal). In the general setting, the attacker has to choose all ciphertexts in advance before querying the oracle
    - In the adaptive chosen-ciphertext attack, formalised by Rackoff and Simon (1991), he is able to adapt this selection depending on the interaction with the oracle. A specially noted variant of the chosen ciphertext attack is the lunchtime, midnight, or indifferent attack, in which an attacker may make adaptive chosen-ciphertext queries but only up until a certain point, after which the attacker must demonstrate some improved ability to attack the system
- Reaction - This attack can be considered as a weaker version of chosen-ciphertext attack. Here, instead of receiving the decrypted cipher texts from the oracle, the attacker only observes the reaction of this one. Usually, this means whether the oracle was able to decrypt the ciphertext.
- Malleability - Malleability is a property of some cryptographic algorithms. An encryption algorithm is malleable if it is possible for an adversary to transform a ciphertext into another ciphertext which is decrypted to a related plaintext.

4.7. Related work

This section provides the state-of-the-arts in the direction of code-based cryptography. We reviewed the surveys from 2008 till now. In 2008, Overbeck and Sendrier [72] published a comprehensive state-of-the-art of code-based cryptography. In this work, authors illustrate the theory and the practice of code-based cryptographic systems.

In 2011, Cayrel et al. [73] presented a survey paper which includes state-of-the-art of publications since 2008 in the code-based cryptography, including encryption and identification schemes, digital signatures, secret-key cryptography, and cryptanalysis. This work provides a comprehensive study and an extension of the chapter "Code-based cryptography" of the book [74].

In the same year 2014, Repka and Cayrel [75] proposed a survey paper on Cryptography Based on Error Correcting Codes. This paper surveys the code-based cryptography existing schemes as well as implementations and side channel attacks. This work also recalls briefly the basic ideas, and provides a roadmap to readers.

In 2015, PQCRYPTO project Horizon 2020 ICT-645622 [76] published a report on post-quantum cryptography for long-term security which provides the PQCRYPTO project's intermediate report on optimized software. This report also provides the preliminary software implementation results of selected post-quantum schemes and the corresponding parameters for embedded systems. This report surveys modern post-quantum schemes in regard to their implementation on such small embedded microcontrollers. This report reviews the most popular schemes in post-quantum cryptography such as encryption and digital signatures schemes.

 doi:10.20944/preprints202104.0734.v1

In 2017, Sendrier [65] published a survey paper which focuses on the McEliece public-key encryption scheme and its variants which are the candidates of post-quantum public-key encryption standard. This paper also focuses on other cryptographic primitives using codes such as zero-knowledge authentication and digital signature.

In parallel to this work in 2017, Bucerzan et al, [77] analyzed the evolution of the main encryption variants coming from code-based cryptography field. Authors focus on the security issues and Rank based cryptography. This paper provides the details and survey on the McEliece encryption scheme. In addition to this, these papers detail the main security threats for the scheme and for each of the mentioned variants.

The most recent survey in the code-based cryptography was published in 2018 [78]. In this paper, authors survey on code-based cryptography, essentially for encryption and signature schemes. Authors also provide the main ideas for theoretical and physical cryptanalysis.

According to the best of our knowledge, these are the surveys available in the direction of code-based cryptography.

In our survey work, we brief our understanding of post-quantum computing by explaining the algorithmic techniques in PQC. We summarize the recent candidates of post-quantum cryptography available in each of the PQC techniques. Table 1 presents a detailed comparison of all recent post-quantum cryptographic solutions which are novel. Such a detailed comparison could not be found in the recent works in PQC. We also focus on industry adoption of PQC schemes. Inside this industry adoption section, we detail the industry surveys of PQC. Table 2 delineates the summary of industry initiatives in PQC direction which is another of our novel contribution. In addition to this, we consolidate the standardization efforts in PQC by studying the standardization works pertaining to the standardization bodies viz. NIST, ITU, ISO, ETSI, CRYPTREC.

For the code-based cryptography, we present the relations between the linear codes and explain how this relationship could be leveraged towards bettering code-based cryptography. This is explained as part of the future research directions section. In addition to this, the other future research directions possible in code-based cryptography are also delineated.

5. Research Directions Identified in Code-based Cryptography

In this section, we lay out some of the research directions which have been least explored and still remain as white spaces in the code-based cryptographic research. Though this paper elaborates on both PQC and code-based cryptography, the future research directions confines only to code-based cryptography for two reasons i) future research direction in PQC ultimately boils down to any one of the PQC schemes viz. code-based, lattice-based, etc and ii) our current research directions centres around code-based cryptography.

5.1. Dynamic Code-based Cryptographic Algorithms

The linear codes are many in number and various code-based cryptographic algorithms using these code variants have been proposed. However, these cryptosystems

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

except the McEleice cryptosystem which uses binary Goppa codes have been reported to be broken, discouraging the use of other linear codes. Even The variants of the McEliece algorithm using the other different types of linear codes apart from binary Goppa codes have been found to be susceptible to attacks. This is because the static code used in the algorithm is known earlier and also it results in a known structure of the linear code which could be cryptanalyzed easily. However, the study of linear codes and the relationships between them, as described above explicate that it is possible to transform one code to another by means of some operations on codes viz. augmenting, puncturing, extending, ...etc. The existing variants of code-based cryptographic algorithms, for example, the McEliece uses a single code (binary goppa) as the basis for the encryption algorithm. Since, it is possible to transform one linear code to another using the possible code transformation operations, the same could be exploited in the encryption. Thereby, the cryptographic algorithm can dynamically choose to use any type of linear code to perform the encryption operation. This dynamic code transformation may produce any other existing linear codes or a new code which fulfils the properties for linear codes viz. Gilbert Varshmov bound, Singleton bound, etc. – for example, from the alternant code one can transform to the Generalized Shrivastava code or to a new code fulfilling the linear code bounds. This dynamic approach provides two fold advantages viz. i) the cryptographic algorithm can dynamically choose to use a particular type of linear code randomly with every session or even in between sessions so that it becomes very difficult to break the cipher since the structure of the linear code keeps varying ii)renders the otherwise unsafe linear codes to provide for quantum attack resistance thereby augmenting the utility of the various types of linear codes available in code-based cryptographic algorithms.

5.2. Use of other Types of Codes in Code-based Cryptography

Codes have been existing for long in the computing domain and there are a variety of codes available which have been used for a variety of encoding purposes. The following is a representative list of encoding purposes commonly encountered in the computing domain [79]. i) To encode data for digital data communication ii) To encode data for digital data communication with error correction capabilities iii) To encode data in a compressed format for faster message communication iv) To represent data in a digital system v) To store and manipulate data in a digital system vi) Programmatic representation of Character set vii) To communicate digital data confidentially viii) To represent data or data set features to be used in machine learning ix)To represent data in a format comprehensible for visually challenged persons.
In each of the above said seven purposes, the encoding achieves either one of the following encoding i) Alphabets / character set encoded to another alphabet ii) Alphabets / character set encoded to a sequence of alphabets iii) character set encoded to a number iv) Alphabets / character set encoded to binary / BCD / Hexadecimal / Octal through ordinal encoding, v) Alphabets / character set encoded to image(s) / symbol(s) / pattern(s) vi) Alphabets / character set encoded to a compressed code vii) Binary data encoded to linear codes viii) Data encoded to a vector ix) Data encoded to a non-numerical label.

As is evident from above, the said encoding types work at multiple levels of abstractions viz. The encoding may work to encode alphabets or a complete character set or it may encode binary data or it may encode a data unit.

Since, we consider encoding from a cryptographic perspective, the following requirements are to be fulfilled by the code / encoding technique in order to constitute for a complete and secure code / encoding technique. These requirements have already been identified in our earlier work in [80].

Support for encoding of complete character set – Some coding techniques provide code for encoding only the alphabets like the Caesar cipher, A1Z26, Atbash codes, etc. How-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

ever, since a plain text message may be alphanumeric comprising of alphabets, numbers and special characters, it is important that the coding technique helps to encode the complete character set.

Possible for representation, manipulation and storage in digital systems –Some encoding techniques result in the production of codes which are in the form of image(s) or symbol(s) or pattern(s) for the alphabet or character set that is encoded. However, these image(s) or symbol(s) or pattern(s) cannot be directly represented, manipulated and stored in digital systems. Dorabella cipher, Morse codes, Dice Cipher, Rosicrucian Cipher are some examples of such coding techniques which produce symbols or patterns as codes which are not suitable for direct representation, manipulation and storage in digital systems.

Enables Data Hiding – Since the codes are approached from the perspective of cryptography, enabling data hiding as a result of encoding is one of the important properties expected to be fulfilled by the code and hence the encoding technique.

Support for multiple data type – Since, the plain text may not only be plain text and also be of any data type viz., audio, video, etc. it is essential that the encoding technique is able to encode any data type.

Dynamicity of encoding – Usually, the encoding techniques provide for static encoding whereby a particular element of a character set or data is always encoded to the same code any time encoding happens. This may enable ease of encoding – but approached from a cryptographic perspective, a dynamic encoding scheme which produces a different code for an element of the character set or data for different data communications sessions should help augment the strength and effectiveness of the encoding.

Variable Encoding – Even in a single session of communication, the plain text to be encoded should be subject to the production of varied codes unlike the Caesar cipher codes, Atbash Cipher codes which produce the same code for the same character in all of the plain text which leaves lot of ques for easy decoding.

Hard Decoding -The encoding technique should be able to produce codes which are hard to decode. In other words, the decoding should be a computationally hard problem to solve.

Randomness of Encoding – Usually, an encoding technique comprises of steps constituting for the generation of code in some particular static order. If the steps of encoding itself is randomized, then it constitutes for a higher strength of the generated code making the decoding a computationally hard problem to solve.
Possibility for Decoding – Though the decoding is required to be a computationally hard problem, it should be possible to decode the code given the key – unlike the hash codes which cannot be decoded since the process of hashing is a one way function.

Random Character Set and Collating Sequence - In encoding, the character set considered and its collating sequence are usually adopted. To provide for a high degree of randomness and hence to render strength to the code,it should be possible to use alphabets across character sets and specify a user defined collating sequence of those alphabets chosen.

Table 7 shows the various requirements for data encoding listed above and the types of codes available in each of them and the properties fulfilled by each of them.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

From the comparison in table 7, it is observed that more than the linear codes which are presently used in code-based cryptography, the DNA codes provide promising scope to be used for cryptography. This has been described in detail in [80]. Though, research in DNA cryptography is active and the domain has been explored in interesting dimensions, the DNA cryptography has not been proven to be quantum attack resistant. If DNA cryptography is proved to be quantum attack resistant, then it provides for a bio-inspired, best value addition to the field of code-based cryptography. This dimension needs to be explored in further detail.

Table 7: Requirements fulfillment of various codes

S. No.	Purpose of Encoding	Code	Type of Code	Properties to be Fulfilled for Encoding									Support
				Complete Character Set Encoding	Representation, manipulation and Storage in Digital Systems	Data Hiding	Support Multiple Data Types	Dynamic Encoding	Variable Encoding	Hard Decoding	Randomness of Encoding	Possible for Decoding	
1	To encode data for digital data communication	All codes generated using Line coding techniques [81]	Binary data encoded to digital signals	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗
2	To encode data for digital data communication with error correction capabilities [81]	All codes generated using Block Codes and Convolutional Coding Techniques [61]	Binary data encoded to linear or non-linear codes with error detection and correction capabilities	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗
3	To encode data in a compressed format for faster message communication	Huffman Codes [82],	Alphabets / character set encoded to a compressed code	✓	✓	✓	NA	✗	✗	✓	✗	✓	✗
		Morse Code [?]	a)Alphabets/ Character set encoded to a compressed code	✓	✓	✓	NA	✗	✗	✓		✓	✗
			b)Alphabets/ Character set encoded to image(s)/ symbols(s)/ patterns(s)										
4	To represent data in a digital system	Ascii, Unicode,..[83], [84]	Alphabets / character set encoded to a number	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗
5	To store and manipulate data in a digital system	Binary, BCD, Hexadecimal, Octal [85]	Alphabets / character set encoded to binary / BCD / Hexadecimal / Octal through ordinal encoding	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗
6	Programmatic Representation of Character Set	HTML Code [86]	Alphabets / character set encoded to a Hexadecimal number	✓	✗	✓	✗	✗	✗	✗	✗	✓	✗
7	To communicate digital data confidentially	Atbash, Caesar Cipher, Columnar Cipher, Combination cipher, Grid Transposition cipher, Keyboard Code, Phone code, Rot Cipher, Rout Cipher [79]	Alphabets encoded to another alphabet	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗
		A1Z26	Alphabets encoded to a number	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗
		QR Code, Bar Code, Dice Cipher, Digraph cipher, Dorabella Cipher, Rosicrucian Cipher, Pigpen cipher[79], [87], [88]	Alphabets / Character Set encoded to image(s) / symbol(s) / pattern(s)	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗
		Francis Bacon Code [79]	Alphabets / character set encoded to a sequence of alphabets	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗
		DNA Code [80]	Alphabets / character set encoded to a sequence of alphabets	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	To represent data or data set features to be used in machine learning	Ordinal Code or label code	Data encoded to a non-numerical label	NA	✓	✓	NA	NA	NA	NA	NA	✓	✗
		One Hot Encoding, Dummy Encoding, Effect Encoding, Binary Encoding, Base N Encoding, Multi-Label Binarizer, DictVectorizer [89]	Data is converted to a vector	NA	✓	✓	NA	NA	NA	NA	NA	✓	✗
		Hash Encoding [89]	Data is converted to its hash value	NA	✓	✓	NA	NA	NA	NA	NA	✗	✗
		Bayesian Encoding [90]	Data is encoded to its average value	NA		✓	NA	NA	NA	NA	NA	NA	✗
9	To represent data in a format comprehensible for visually challenged persons	Braille Code [91]	Alphabets / character set encoded to image(s) / symbol(s) / pattern(s)	✓	✓	✓	NA	✗	✗	✗	✗	✓	✗

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 28 April 2021 doi:10.20944/preprints202104.0734.v1

5.3. Privacy Preserving Code-based Cryptography

Privacy preserving encryption algorithms are the need of the hour owing to the growing privacy issues and concerns globally. Privacy preserving encryption can be achieved using the following ways:

- Attribute Based Encryption - Key Policy based encryption and Cipher Policy based encryption [92]
- Homomorphic encryption [93]

Whereas, the attribute based encryption provides for selective decryption of cipher text based on the fulfillment of attributes by the receiver, the homomorphic encryption enables to perform computations on the encrypted data itself eliminating the requirement for decryption.
In code-based cryptography, only the McEliece cryptosystem has been proven to be somewhat homomorphic [94]. But, attribute based encryption in code-based cryptography is yet to be explored. Hence, there is a need for lot of research to enable the maturity of this dimension of code-based Cryptography and its practical use in privacy demanding domains such as healthcare, financial sector, etc. This constitutes for another prospective line of research in code-based cryptography.

5.4. Prospective Applicability of codes with lattice-based Cryptography

Codes and Lattices are having similar mathematical properties. A linear code C of length n and dimension k is a k-dimensional subspace of finite field F_q^n typically endowed with hamming metric.

Given n-linearly independent vectors $b_1, \ldots, b_n$ in R^n, the lattice generated by them is the set of vectors

$L(b1, ..., bn) = \sum_{i=1}^{n} xibi : xi \in Zfor1 \leq i \leq n$

The vectors $b_1, \ldots, b_n$ are known as a basis of the lattice.

Both of them are vector spaces over some finite fields.

1. code-based cryptography employs only Binary linear codes F_q^n for developing cryptographic primitives. Typical lattice-based cryptographic schemes have used q-ary lattices to solve SIS and LWE problems [95]. Linear code of length n and dimension k is a linear subspace F_q^n which is called a q - ary code. The possibility of using q-ary lattices [96] to implement ternary codes i.e q - ary codes in code-based cryptographic schemes is an unexplored area. It may be noted here that the DNA cryptography is a Quaternary code which has received due exploration from the authors but only needs to be ascertained for its quantum attack resistance.
2. There is a major lattice algorithmic technique that has no clear counterpart for codes, namely, basis reduction. There seems to be no analogue notions of reduction for codes, or at least they are not explicit nor associated with reduction algorithms. We are also unaware of any study of how such reduced bases would help with decoding tasks. This observation leads to two questions.

- Is there an algorithmic reduction theory for codes, analogue to the one of lattices ?
- If so, can it be useful for decoding tasks ?

These questions are potential leads towards prospective research directions in code-based cryptography.

6. conclusion

Post-quantum cryptography research has branched out in many dimensions and considerable research outcome has been emerging in each of these dimensions. While this evinces the maturity of post-quantum cryptography research, each of these outcome are available in discrete sources hindering the broad spectrum view and comprehension of these outcome. This paper addresses this limitation, whereby, it provides a one stop reference of the entire spectrum of post-quantum cryptography research and provides a review of the same.

Also, from the NIST standardization, it has been observed that though code-based cryptography provides scope to be recognized as a complete cryptosystem with the availability of encryption, key exchange and digital signature schemes, unlike its post-quantum counterparts which provide for a subset of these. Hence, code-based cryptography has been explored in detail and the promising research directions that can augment the prospects of code-based cryptography have been identified and described. Thereby, this paper provides for two solid contributions in the roadmap of post-quantum computing research.

Author Contributions: "Conceptualization, T.C. and K.S.; methodology, T.C. and K.S; formal analysis, T.C.; investigation, T.C. and K.S.; resources, T.C. and K.S.; writing—original draft preparation, T.C. and K.S.; writing—review and editing, T.C., K.S., G. G.; supervision, T.C., K.S., M.R.; project administration, K.S.; funding acquisition, K.S. All authors have read and agreed to the published version of the manuscript."

Funding: "This research received a funding of IRT SystemX"

Acknowledgments: This research work has been carried out under the leadership of the Institute for Technological Research SystemX, and therefore granted within the scope of the program "Recherche Exploratoire"

Conflicts of Interest: "The authors declare no conflict of interest."

References

1. Song, Y.Y. Integer factorization and discrete logarithmsh. Primality testing and integer factorization in public-Key cryptography. Springer, 2004, pp. 139–191.
2. Cayrel, P.L.; Gueye, C.T.; Ndiaye, O.; Niebuhr, R. Critical attacks in code-based cryptography. *International Journal of Information and Coding Theory* **2015**, *3*, 158.
3. Rivest, R.; A., S.; L., A. A method for obtaining digital for signatures and public-Key cryptosystems. *Communications of the ACM* **1978**, *21*, 120–126.
4. McEliece, R.J. A public-key cryptosystem based on algebraic. *Coding Thv* **1978**, *4244*, 114–116.
5. Merkle, R. *Secrecy, Authentication, and Public Key Systems*; Computer Science Series, UMI Research Press, 1982.
6. Patarin, J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. International Conference on the Theory and Applications of Cryptographic Techniques, 1996, pp. 33–48.
7. Hoffstein, J.; Pipher, J.; Silverman, J.H. NTRU: A ring-based public key cryptosystem. International Algorithmic Number Theory Symposium. Springer, 1998, pp. 267–288.
8. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)* **2009**, *56*, 34.
9. Jao, D.; De Feo, L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. *PQCrypto* **2011**, *7071*, 19–34.
10. Nielsen, M.A.; Chuang, I. Quantum computation and quantum information, 2002.
11. Benioff, P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of statistical physics* **1980**, *22*, 563–591.
12. Manin, Y. *Mathematics and physics*; 1981.
13. Feynman, R.P. Simulating physics with computers. *International journal of theoretical physics* **1982**, *21*, 467–488.
14. Deutsch, D. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, 1985.
15. Shor, P.W. Algorithms for quantum computation: Discrete Logarithms and Factoring. 35th Annual Symposium on Foundations of Computer Science. IEEE Computer Society, 1994, pp. 124–134.
16. Grover, L.K. A fast quantum mechanical algorithm for database search. 28th annual ACM symposium on Theory of Computing, 1996, pp. 212–219.
17. Buchmann, J.; Lauter, K.; Mosca, M. Postquantum Cryptography-State of the Art. *IEEE Security & Privacy* **2017**, *15*, 12–13.
18. Gauthier Umana, V. Post Quantum Cryptography. PhD thesis, Technical University of Denmark, 2011.
19. Wikipedia. Post-quantum cryptography. https://en.wikipedia.org/w/index.php?title=Post-quantum-cryptography&oldid=999863701.
20. Merkle, R. A certified digital signature. Advances in Cryptology – CRYPTO'89. Springer, 1989, pp. 218–238.
21. Butin, D. Hash-based signatures: State of play. *IEEE Security & Privacy* **2007**, *15*, 37–43.
22. Bernstein, D.J.; Hülsing, A.; Kölbl, S.; Niederhagen, R.; Rijneveld, J.; Schwabe, P. The SPHINCS+ Signature Framework. Cryptology ePrint Archive: Report 2019/1086, 2019.
23. Joachim, R. An Overview to Code Based Cryptography. hkumath.hku.hk/~ghan/WAM/Joachim.pdf, 2016.
24. Ding, J.; Petzoldt, A. Current state of multivariate cryptography. *IEEE Security & Privacy* **2017**, *15*, 28–36.

25. shing Chen, M.; Ding, J.; Kannwischer, M.; Patarin, J.; Petzoldt, A.; Schmidt, D.; Yang, B.Y. Rainbow signature. https://www.pqcrainbow.org/.
26. Casanova, A.; Faueère, J.C.; Macario-Rat, G.; Patarin, J.; Perret, L.; Ryckeghem, J. GeMSS: A great multivariate short signature. https://www-polsys.lip6.fr/Links/NIST/GeMSS.html.
27. Chi, D.P.; Choi, J.W.; Kim, J.S.; Kim, T. Lattice based cryptography for beginners. Cryptology ePrint Archive: Report 2015/938, 2015.
28. Lepoint, T. Design and implementation of lattice-based cryptography. PhD thesis, Ecole Normale euérieure de Paris - ENS Paris, 2014.
29. Alkim, D.; Ducas, L.; Pöppelmann, T.; Schwabe, P. Post-quantum key exchange - a new hope. Cryptology ePrint Archive: Report 2015/1092, 2015.
30. Ducas, L.; Durmus, A.; Lepoint, T.; Lyubashevsky, V. Lattice signatures and bimodal gaussians. Cryptology ePrint Archive: Report 2013/383, 2013.
31. Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM. Cryptology ePrint Archive: Report 2017/634, 2017.
32. Chen, C.; Danba, O.; Hoffstein, J.; Hülsing, A.; Rijneveld, J.; Saito, T.; Schanck, J.M.; Schwabe, P.; Whyte, W.; Xagawa, K.; Yamakawa, T.; and, Z.Z. NTRU:A submission to the NIST post-quantum standardization effort. https://ntru.org/.
33. D'Anvers, J.P.; Karmakar, A.; Roy, S.S.; Vercauteren, F. Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. Cryptology ePrint Archive: Report 2018/230, 2018.
34. Bernstein, D.J.; Chuengsatiansup, C.; Lange, T.; van Vredendaal, C. NTRU Prime: reducing attack surface at low cost. Cryptology ePrint Archive: Report 2016/461, 2016.
35. Ducas, L.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehle, D. CRYSTALS – Dilithium: Digital Signatures from Module Lattices. Cryptology ePrint Archive: Report 2017/633, 2017.
36. Fouque, P.A.; Hoffstein, J.; Kirchner, P.; Lyubashevsky, V.; Pornin, T.; Prest, T.; Ricosset, T.; Seiler, G.; Whyte, W.; Zhang, Z. Falcon: Fast-Fourier Lattice-based compact signatures over NTRU. https://www.di.ens.fr/~prest/Publications/falcon.pdf.
37. Supersingular isogeny Diffie–Hellman key exchange (SIDH). https://en.wikipedia.org/wiki/Supersingular_isogeny_key_exchange.
38. CraigCostello, PatrickLonga, and MichaelNaehrig. Efficient algorithms for supersingular isogenyDiffie-Hellman. *Annual International Cryptology Conference* **2016**.
39. Valyukh, V. Performance and compari-son of post-quantum crypto-graphic algorithms. http://www.liu.se, 2017.
40. Post-Quantum Cryptography: A Ten-Year Market and Technology Forecast. https://www.researchandmarkets.com/reports/4700915/post-quantum-cryptography-a-ten-year-market-and#relb0-5118342, May 2020.
41. IBM - Post-quantum cryptography. https://researcher.watson.ibm.com/researcher/view_group.php?id=8231.
42. Microsoft - Post Quantum Cryptography. https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/.
43. Avaya and Post-Quantum to Team on Identity-as-a-Service. https://www.avaya.com/en/about-avaya/newsroom/pr-us-1803012c/.
44. Post Quantum Consulting | Envieta. https://envieta.com/post-quantum-consulting.
45. Google and Cloudflare are testing post-quantum cryptography. https://www.revyuh.com/news/hardware-and-gadgets/google-cloudflare-testing-post-quantum-cryptography/.
46. Post-quantum cryptography: cybersecurity in post-quantum computer world - Infineon Technologies. https://www.infineon.com/cms/en/product/promopages/post-quantum-cryptography/.
47. Post-quantum cryptography: cybersecurity in post-quantum computer world - Infineon Technologies. https://www.infineon.com/cms/en/product/promopages/post-quantum-cryptography/.
48. Security Innovation Announces Intent to Create OnBoard Security Inc. https://www.globenewswire.com/news-release/2017/02/14/917023/0/en/Security-Innovation-Announces-Intent-to-Create-OnBoard-Security-Inc.html.
49. Post-Quantum Cryptography | CSRC. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
50. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process.
51. Qin, H. Standardization of quantum cryptography in ITU-T and ISO/IEC, Qcrypt 2020 Industry Session, August 12, 2020. https://2020.qcrypt.net/slides/Qcrypt2020_ITU_ISO.pdf.
52. ETSI ICT Standards. https://www.etsi.org/standards.
53. Chen, L. Preparation of Standardization of Quantum-Resistant Cryptography in ISO/IEC JTC1 SC27. https://docbox.etsi.org/Workshop/2018/201811_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/01worldtour/NICT_Moriai.pdf, 2018.
54. Shinohara, N.; Moriai, S. Trends in Post-Quantum Cryptography : Cryptosystems for the Quantum Computing Era. https://www.ituaj.jp/wp-content/uploads/2019/01/nb31-1_web-05-Special-TrendsPostQuantum.pdf, 2019.
55. Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2). https://tools.ietf.org/id/draft-tjhai-ipsecme-hybrid-qske-ikev2-03.html.
56. Paterson, K. Post-quantum Crypto Standardisation in IETF/IRTF. www.isg.rhul.ac.uk/{~}kp.
57. libpqcrypto: Intro. https://libpqcrypto.org/.

58. Quantum-safe Security | Cloud Security Alliance. https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/.
59. Minihold, M. Linear Codes and Applications in Cryptography. Master's thesis, Vienna University of Technology, 2013.
60. Londahl, C. Some Notes on Code-Based Cryptography. PhD thesis, Lund University, 2015.
61. F.J. Mac Williams, N.S. *The Theory of Error-Correcting Codes*; North Holland Publishing Company, 1977.
62. Minder, L. Cryptography Based on Error Correcting Codes. PhD thesis, Ecole Polytechnique Federale De Lausanne, 2007.
63. Sendrier, N. On the Use of Structured Codes in Code Based Cryptography **2009**. pp. 59–68.
64. Valentijn, A. Goppa Codes and Their Use in the McEliece Cryptosystems. Honors thesis, Syracuse University, 2015.
65. Sendrier, N. Code-Based Cryptography: State of the Art and Perspectives. *IEEE Security Privacy* **2017**, *15*, 44–50.
66. Sadkhan Al Maliky, S.B.; Abbas, N.A. Multidisciplinary perspectives in cryptology and information security. *Multidisciplinary Perspectives in Cryptology and Information Security* **2014**, *i*, 1–443.
67. Roering, C. Coding Theory-Based Cryptopraphy : McEliece Cryptosystems in Sage Coding Theory-Based Cryptography : McEliece Cryptosystems in Sage. Honors theis, College of Saint Benedict / St. John's University, 2015.
68. Heyse S., von Maurich I., G.T. Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices. In *Cryptographic Hardware and Embedded Systems - CHES 2013. CHES 2013. Lecture Notes in Computer Science, vol 8086*; Bertoni G., C.J.e., Ed.; Springer, Berlin, Heidelberg, 2013; pp. 273–292.
69. von Maurich, I.; Güneysu, T. Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices. 2014 Design, Automation Test in Europe Conference Exhibition (DATE), 2014, pp. 1–6.
70. Heyse, S.; Güneysu, T. Code-based cryptography on reconfigurable hardware : tweaking Niederreiter encryption for performance. *Journal of Cryptographic Engineering* **2013**, pp. 29–43.
71. Roy, P.S.; Morozov, K.; Fukushima, K. Evaluation of Code-based Signature Schemes. https://eprint.iacr.org/2019/544, 2019.
72. Overbeck, R.; Sendrier, N. Code-Based Cryptography. Springer, 2008, pp. 95–146.
73. Cayrel, P.L.; ElYousfi, M.; Hoffmann, G.; Meziani, M.; Niebuhr, R. Recent Progress in Code-Based Cryptography. International Conference on Information Security and Assurance. Springer, 2011, pp. 21–32.
74. Bernstein, D.J.; Buchmann, J.; Dahmen, E. *Post-Quantum Cryptography*; Springer, 2008.
75. Repka, M.; Cayrel, P.L. *Cryptography Based on Error Correcting Codes: A Survey*; IGI Global, 2014.
76. PQCRYPTO. Post-Quantum Cryptography for Long-Term Security. Technical report, Project number: Horizon 2020 ICT-645622, Coordinator: Technische Universiteit Eindhoven, 2015.
77. Bucerzan, D.; Dragoi, V.; Kalachi, H. Evolution of the McEliece Public Key Encryption Scheme. International Conference for Information Technology and Communications SecITC 2017. Springer, 2017, pp. 129–149.
78. Drăgoi, V.; Richmond, T.; Bucerzan, D.; Legay, A. Survey on Cryptanalysis of Code-Based Cryptography: from Theoretical to Physical Attacks. 7th International Conference on Computers Communications and Control (ICCCC). IEEE, 2018.
79. Best Codes : 27 Steps - Instructables. https://www.instructables.com/Best-Codes/.
80. Hussain, U.N. A Novel String Matrix Modeling Based DNA Computing Inspired Cryptosystem . PhD thesis, Pondicherry University, 2016.
81. Line Coding Techniques. https://technologyuk.net/telecommunications/telecom-principles/line-coding-techniques.shtml.
82. Huffman, D.A. A Method for the Construction of Minimum-Redundancy Codes. *Proceedings of the IRE* **1952**, *40*, 1098–1101.
83. ASCII - Wikipedia. https://en.wikipedia.org/wiki/ASCII.
84. Unicode - Wikipedia. https://en.wikipedia.org/wiki/Unicode.
85. Number systems (binary, octal, decimal, hexadecimal). https://www.mathemania.com/lesson/number-systems/.
86. HTML Codes. https://www.html.am/html-codes/.
87. QR code - Wikipedia. https://en.wikipedia.org/wiki/QR{_}code.
88. Barcode - Wikipedia. https://en.wikipedia.org/wiki/Barcode.
89. Categorical Data Encoding Techniques to Boost your Model in Python! https://www.analyticsvidhya.com/blog/2020/08/types-of-categorical-data-encoding/.
90. Categorical Feature Encoding in SAS (Bayesian Encoders) - Selerity. https://seleritysas.com/blog/2021/02/19/categorical-feature-encoding-in-sas-bayesian-encoders/.
91. Braille - Wikipedia. https://en.wikipedia.org/wiki/Braille.
92. Vipul Kumar RajaniKanth Aluvalu, P.J. International Journal of Innovative and Emerging Research in Engineering **2015**. *2*.
93. Homomorphic encryption - Wikipedia. https://en.wikipedia.org/wiki/Homomorphic{_}encryption.
94. Zhao, C.c.; Ya-Tao, Y.; Zi-chen, L. The Homomorphic Properties of McEliece Public-Key Cryptosystem. 2012, pp. 39–42.
95. Cayrel, P.L.; Alaoui, S.; Hoffmann, G.; Véron, P. An Improved Threshold Ring Signature Scheme Based on Error Correcting Codes. Proceedings of the 4th international conference on Arithmetic of Finite Fields, 2012, pp. 45–63.
96. Campello, A.; Jorge, G.; Costa, S. Decoding q-ary lattices in the Lee metric. *Computing Research Repository - CORR* **2011**. doi:10.1109/ITW.2011.6089382.