

A Lightweight McEliece Cryptosystem Co-processor Design

Lake Bu, Rashmi Agrawal, Hai Cheng, and Michel A. Kinsy
 Adaptive and Secure Computing Systems Laboratory
 Department of Electrical and Computer Engineering, Boston University
 (bulake, rashmi23, chenghai, mkinsy)@bu.edu

ABSTRACT

Due to the rapid advances in the development of quantum computers and their susceptibility to errors, there is a renewed interest in error correction algorithms. In particular, error correcting code-based cryptosystems have reemerged as a highly desirable coding technique. This is due to the fact that most classical asymmetric cryptosystems will fail in the quantum computing era. Quantum computers can solve many of the integer factorization and discrete logarithm problems efficiently. However, code-based cryptosystems are still secure against quantum computers, since the decoding of linear codes remains as NP-hard even on these computing systems. One such cryptosystem is the McEliece code-based cryptosystem. The original McEliece code-based cryptosystem uses binary Goppa code, which is known for its good code rate and error correction capability. However, its key generation and decoding procedures have a high computation complexity. In this work we propose a design and hardware implementation of a public-key encryption and decryption co-processor based on a new variant of McEliece system. This co-processor takes the advantage of the non-binary Orthogonal Latin Square Codes to achieve much smaller computation complexity, hardware cost, and the key size.

KEYWORDS

Code-based post-quantum cryptosystem, McEliece public-key encryption, Non-binary Orthogonal Latin Square Codes.

1 INTRODUCTION

Since the possibility of using quantum effects in computation was brought up by Feynman in 1959, numerous efforts have been dedicated to realize and even commercialize the quantum computers. In the past three years, a number of significant milestones have been reached in this area. From late 2017 to early 2018, technology companies such as IBM, Intel, and Google, announced their construction and testing of 50-, 49-, and 72-qubit computers, respectively. In July 2018, for the first time, researchers at the University of Sydney successfully realized a multi-qubit computation on a system of trapped ions, which is believed to be the leading platform in building general quantum computers [3]. In December 2018, IonQ claimed to have built a quantum computer with 160 qubits. Besides these advances in physical implementation of quantum computers, key breakthroughs in the verification of quantum computation were also achieved [1], and more efficient error correction schemes were recently proposed as well. These efforts are rooted in the fact that quantum computers promise greater computational power. But these developments also bring with them burning security concerns. For example, Shor's algorithm [6], leveraging quantum Fourier transform, is able to solve the integer factorization problem efficiently. Therefore, current popular cryptographic algorithms such as RSA, ElGamal, Diffie-Hellman, and ECC, which rely on the

hardness of integer factorization and discrete logarithm (the two are also closely related), are vulnerable to quantum computer-based algorithms.

In response to the aforementioned security challenges associated with quantum computers, a number of new cryptosystems has been proposed for the post-quantum era. In early 2017, NIST launched a campaign for a post-quantum cryptography standardization. Up to February 2019, totally 27 out of 69 candidates of this new standard made to the second round of competition [5]. Among the 27, the two most likely contenders are the lattice-based cryptosystems (12 candidates), and the code-based cryptosystems (8 candidates). Both of them are able to construct public-key cryptosystems and key exchange mechanisms.

Compared to the popular lattice-based ring-learning with error (Ring-LWE) cryptosystem, error-correcting code (ECC)-based schemes have a much larger key size, which is considered a drawback. However, they do bear the advantage of withstanding the test of time. For example, since its formulation by Robert McEliece in 1978 [4], the McEliece code-based technique has so far proven to be cryptanalysis resistant (although sometimes increasing the key size is necessary). The conventional McEliece cryptosystem uses the binary Goppa code, which has good code rate and error correction capability. However, comparing with other binary codes, the generating and decoding (error-correction) of binary Goppa codes have relatively high complexity since they involve intensive computations over finite fields, including modulo polynomial operations. In addition, the key size of McEliece systems is usually large. For a binary Goppa code with an $k \times n$ generating matrix, the key size is kn with k, n in thousands of bits.

Therefore, to address these issues, we propose a new variant of McEliece cryptosystem and its encryption-decryption co-processor. The proposed system is based on the generalized non-binary Orthogonal Latin Square Code (OLSC), which is known for its simple encoding and decoding algorithms, leading to potential efficient hardware implementation. In addition, the non-binary OLSC is able to work with non-binary messages through binary matrices. In other words, a long message is able to be processed by relatively small matrices, which reduces the key size.

2 THE OLSC-BASED CRYPTOSYSTEM

2.1 The McEliece Algorithm

The detailed protocol of the public-key cryptosystem (PKC) can be found in [4]. Here we provide a brief introduction to aid the presentation of the co-processor.

Key generation: Alice picks a binary (n, k, t) ECC code C with k information (plaintext) bits, n total codeword length, and the capability of correcting up to t random errors. The $k \times n$ generating matrix of C is denoted by G . Alice also picks a $k \times k$ binary non-singular matrix S and a $n \times n$ permutation matrix P . Then Alice

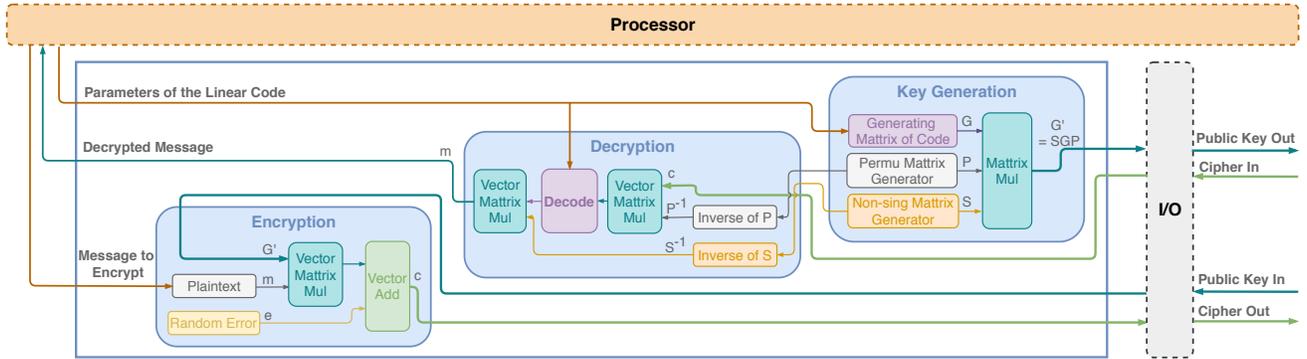


Figure 1: McEliece Cryptosystem Co-Processor Architecture.

computes the public key G' as:

$$G' = SGP. \quad (1)$$

Alice keeps S, G, P as the private key.

Encryption: Bob converts his message (plaintext) into a k -bit binary vector m , and generates the n -bit cipher $\{c\}$ as:

$$c = mG' + e, \quad (2)$$

where e is a binary vector weight t .

Decryption: Alice decrypts the cipher by performing:

$$m = (\text{Decode}(cP^{-1}))S^{-1} \quad (3)$$

where $\text{Decode}()$ stands for the error correction function of C , and P^{-1}, S^{-1} are the inverse matrices of P, S respectively.

2.2 Cryptosystem Co-Processor Architecture

The McEliece based public key encryption cryptosystem co-processor has three modules: the *Key Generation*, *encryption* and *decryption*, shown in Fig 1. Of the three modules, the decryption unit has the highest complexity and consumes the most hardware resources, especially, its *Decode* stage. Therefore, our efficient implementation primarily targets the *Decode* sub-module.

The Orthogonal Latin Square Code (OLSC): The OLSC technique is a t -error-correcting binary code with its decoding matrix $H = [M|I]$, where M consists of $2tq$ orthogonal Latin squares sized $q \times q$, and I an identity matrix. Its generating matrix is $G = [I|M^T]$, where T stands for transpose. Once constructed, the columns of generating matrices can be permuted to create different OLSCs with the same parameters.

Algorithm 1 is the decoding procedure of OLSC codes, which consists mostly of binary linear operations. Thus, it can be carried out fast and efficient in hardware. In [2], authors generated the binary OLSC to non-binary codes while still maintaining low decoding complexity. By replacing the binary Goppa code with the non-binary OLSC, the decoding stage only requires (1) binary vector-matrix multiplication and (2) k parallel majority votings among q non-binary vectors each. This feature enables much faster decryption time than the Goppa-code based scheme, as shown in Table 1.

Due to this simpler decoding mechanism, in the OLSC-based McEliece cryptosystem co-processor, we are able to design a single-cycle (one-step) decoding unit. This design is much faster than an equivalent binary Goppa code-based system. The non-binary OLSC is able to encode a kb -bit plaintext with a $k \times n$ generating matrix G (b being the size of each non-binary symbol), while binary

Goppa code can only deal with k -bit plaintexts with such a matrix. In other words, given the same size of plaintext, the key size of the non-binary OLSC-based McEliece cryptosystem is $1/b$ that of the Goppa code-based. Given a proper verification on the security level of the OLSC-based scheme with various decoding techniques, it could serve as an efficient and high speed variant of the McEliece cryptosystem.

Algorithm 1: OLSC-based McEliece Cryptosystem

```

1  Let  $G' = SGP$  and  $t$  be the public key, and  $\{G, S, P\}$ 
   the private key, where  $G$  is a  $k \times n$  OLSC
   encoding matrix with random permutation of
   columns, and  $H$  as its corresponding decoding
   matrix. Let each Latin square be of size  $q \times q$ ,
    $m$  be the plaintext, and  $c$  the encrypted cipher.
2
3  Precompute:  $S^{-1}, P^{-1}$  as the inverse to  $S, P$ .
4
5   $c' \leftarrow cP^{-1}$ 
6   $u \leftarrow Hc' \times H$ 
7  for  $i=0$  to  $n$ 
8      $m'_i \leftarrow (u_i > q/2)? \sim c'_i : c'_i$ 
9   $m \leftarrow m'S^{-1}$ 
10 return  $m$ 

```

Table 1: Complexity Analysis

	Finite Field Ops	Latency (cycles)
Binary Goppa Code-based	$O(n^2)$	$O(n)$
OLSC-based	0	$O(1)$

REFERENCES

- [1] Dorit Aharonov, Michael Ben-Or, Elad Eban, and Urmila Mahadev. 2017. Interactive proofs for quantum computations. *arXiv preprint arXiv:1704.04487* (2017).
- [2] Lake Bu and Mark Karpovsky. 2016. A hybrid self-diagnosis mechanism with defective nodes locating and attack detection for parallel computing systems. In *On-Line Testing and Robust System Design (IOLTS), 22nd International Symposium on*. IEEE, 245–250.
- [3] Science Daily. 2018. World-first quantum computer simulation of chemical bonds using trapped ions. (2018). sciencedaily.com/releases/2018/07/180724110028.htm
- [4] Robert J McEliece. 1978. A public-key cryptosystem based on algebraic. *Coding Thv* 4244 (1978), 114–116.
- [5] NIST. 2019. PQC Standardization Process. (2019). csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates
- [6] Peter W Shor. 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review* 41, 2 (1999), 303–332.