An Improved McEliece Variant Scheme Based on Parity-Check Codes (Postprint)

Authors: Li Mengdong, Sun Yuqing, Wei Yier, Sipei Cheng

Date: 2018-09-12T00:00:00+00:00

Abstract

The McEliece public-key encryption scheme is a public-key cryptosystem based on coding theory, whose security can be reduced to the general linear code decoding problem and is capable of resisting quantum attacks. This paper proposes an improved McEliece variant scheme based on quasi-cyclic moderate-density parity-check (QC-MDPC) codes and quasi-cyclic low-density parity-check (QC-LDPC) codes. The primary improvement involves combining the parity-check matrices of QC-LDPC codes and QC-MDPC codes as the private key, generating concatenated codewords of both for application in the McEliece variant scheme, and presenting an improved decoding algorithm. Analysis demonstrates that under 80-bit security, this cryptosystem features a small key size and low implementation complexity, and can resist recently proposed key recovery attacks specifically targeting QC-MDPC and QC-LDPC schemes.

Full Text

Preamble

Title: An Improved McEliece Variant Scheme Based on Parity-Check Codes

Authors: Li Mengdong[1],[2], Sun Yuqing[2], Wei Yier[2], Cheng Sipei[1]

Affiliations: 1. Beijing Electronic Science & Technology Institute, Beijing 100070, China 2. Institute of Communication Engineering, Xidian University, Xi' an 710071, China

Abstract: The McEliece public-key cryptosystem is a coding-theory-based public-key cryptosystem whose security can be reduced to the general linear code decoding problem, enabling resistance against quantum attacks. This paper proposes an improved McEliece variant scheme based on quasi-cyclic moderate-density parity-check (QC-MDPC) codes and quasi-cyclic low-density

parity-check (QC-LDPC) codes. The main improvement combines the parity-check matrices of QC-LDPC and QC-MDPC codes as the private key, applies the concatenated codewords of both codes to the McEliece variant scheme, and presents an improved decoding algorithm. Analysis demonstrates that under 80-bit security, the system achieves small key sizes and low implementation complexity while resisting recently proposed key recovery attacks targeting QC-MDPC and QC-LDPC schemes individually.

Keywords: QC-LDPC; QC-MDPC; McEliece PKC; bit-flipping decoding algorithm

0 Introduction

With the rapid development of quantum computers in recent years, selecting post-quantum secure encryption schemes has become crucial to avoid quantum attacks. Public-key cryptosystems based on error-correcting codes represent one of the primary candidates capable of resisting quantum computer attacks, as their security can be reduced to the general linear code decoding problem, offering excellent security properties. The classic McEliece and Niederreiter schemes based on binary Goppa codes, while fast in implementation, suffer from large key sizes. Many attempts to improve this drawback by using alternative codes to achieve more compact key representations have been broken [1,2].

Currently, the most promising McEliece variants that maintain both security and short key lengths employ QC-MDPC codes. Baldi et al. [3] first applied QC-LDPC codes to the McEliece cryptosystem. These codes, lacking excessive algebraic structure while possessing fast decoding algorithms, enabled the cryptosystem to achieve both smaller public keys and corresponding security levels. However, this approach was soon broken by Otmani et al. [4] using structural attacks that exploited vulnerabilities in low-dimensional dual codes. Subsequently, Baldi et al. [5] improved their previous QC-LDPC scheme to resist Otmani' s attacks.

In 2013, Misoczki et al. [6] proposed a McEliece public-key cryptosystem using QC-MDPC codes, proving its resistance to known attacks on LDPC codes while maintaining the short-key advantage of QC-LDPC codes. Nevertheless, in 2016, Guo et al. [7] presented a key recovery attack on Misoczki' s QC-MDPC scheme. This attack exploited correlations between decoding error probabilities and the key' s distance spectrum through extensive experiments to recover the secret key. In the same year, Shooshtari et al. [8] demonstrated that when the circulant blocks in Baldi' s improved QC-LDPC McEliece scheme had even sizes, the system became vulnerable to information set decoding attacks. Later in 2017, Fabšič et al. [9] applied Guo et al.'s attack methodology to this scheme, similarly using extensive experiments to find dependencies between permutation matrices and decoding error probabilities to recover keys.

To maintain the advantages of short keys and high transmission rates in McEliece variants while resisting attacks targeting both QC-LDPC and QC-MDPC variants, this paper designs a McEliece cryptosystem that combines

two parity-check codes. The analysis shows that with appropriate parameters, this scheme can resist Guo et al.' s key recovery attack while avoiding attacks targeting QC-LDPC codes.

1 Preliminaries

1.1 Related Definitions

Definition 1 (LDPC Code). A codeword $\mathbf{c}$ is a low-density parity-check code whose parity-check matrix $\mathbf{H}$ has low density, making it a sparse matrix that can be represented by a Tanner graph (see Figure 1 [Figure 1: see original paper]).

Definition 2 (MDPC Code). An MDPC code is a code with slightly higher density than LDPC codes. An (n, r, w)-MDPC code is a linear code of length n and codimension r whose parity-check matrix has constant row weight w. The row and column density of MDPC parity-check matrices is higher than that of LDPC codes. In practice, LDPC parity-check matrices typically have row weights less than or equal to 10, while MDPC parity-check matrix row weights range around $O(\sqrt{n})$. For security parameters between 80 and 256 bits, MDPC code parity-check matrices typically select row weights between 90 and 644.

Definition 3 (Quasi-Cyclic Code). For a linear code, if there exists a small integer p (such as 2, 3, 4, etc.) such that every codeword in the set, when cyclically shifted by p positions, generates another codeword in the set, then the code is called a quasi-cyclic code.

Definition 4 (QC-LDPC/QC-MDPC Code). When an (n, r, w)-LDPC/MDPC code is also quasi-cyclic, or when defined by a circulant block parity-check matrix where $\mathbf{H} = [\mathbf{H}_0, \mathbf{H}_1, \ldots, \mathbf{H}_{n_0-1}]$, it is called a quasi-cyclic low/medium density parity-check code, i.e., QC-LDPC/QC-MDPC code.

Definition 5 (Circulant Matrix). A matrix is called circulant if each row is a successive cyclic shift of the first row.

Definition 6 (Matrix Density). The density of matrix $\mathbf{H}$ refers to the average number of 1s per row in $\mathbf{H}$, i.e., $d_r = \frac{\text{number of 1s in } \mathbf{H}}{r}$.

Definition 7 (λ-bit Security). Any attacker must expend computational cost (number of elementary operations) $T \geq 2^{\lambda}$ to successfully attack the system; or any effective attack has success probability $\varepsilon \leq 2^{-\lambda}$; or a combination of both scenarios.

1.2 Traditional McEliece Cryptosystem

The McEliece cryptosystem [10], proposed in 1978, is a public-key cryptosystem based on coding theory. The encryption and decryption processes use three matrices: $\mathbf{G}$, $\mathbf{S}$, and $\mathbf{P}$, where $\mathbf{G}$ is a $k \times n$ generator matrix of an $[n, k]$ linear code that can correct t errors (McEliece proposed using binary Goppa codes); $\mathbf{S}$ is a $k \times k$ random non-singular (invertible) matrix; and $\mathbf{P}$ is an $n \times n$ random

permutation matrix. The public key is computed as $\mathbf{G}' = \mathbf{SGP}$ together with the error-correcting capability t, while the private key consists of $(\mathbf{G}, \mathbf{S}, \mathbf{P})$.

Encryption: For a plaintext $\mathbf{m}$, randomly generate an error pattern $\mathbf{e}$ with weight less than or equal to t. The ciphertext is $\mathbf{c} = \mathbf{mG}' + \mathbf{e}$.

Decryption: Multiply both sides of the equation by $\mathbf{P}^{-1}$ to obtain $\mathbf{cP}^{-1} = \mathbf{mSG} + \mathbf{eP}^{-1}$. Use the fast decoding algorithm for Goppa codes to correct the error pattern $\mathbf{eP}^{-1}$ and compute $\mathbf{mS}$, then recover $\mathbf{m}$.

1.3 Tanner Graph Representation of LDPC/MDPC Codes

Both LDPC and MDPC codes can be represented by Tanner graphs for their parity-check matrices. For example, the parity-check matrix of a $(20, 15, 4)$-LDPC code is as follows:

$$\mathbf{H}_{(20,15,4)} = \begin{pmatrix} 1\&0 & 0\&0 & 0\&1 & 0\&0 & 0\&1 & 0\&0 & 0\&0 & 1 \\ 0\&1 & 0\&0 & 0\&1 & 0\&0 & 0\&0 & 1\&0 & 0\&0 & 1 \\ 0\&0 & 1\&0 & 0\&0 & 1\&0 & 0\&1 & 0\&1 & 0\&0 & 0 \\ 0\&0 & 0\&1 & 0\&0 & 1\&0 & 0\&0 & 0\&0 & 1\&0 & 1 \\ 0\&0 & 0\&0 & 1\&0 & 0\&1 & 0\&0 & 0\&1 & 0\&1 & 0 \\ 1\&1 & 1\&1 & 1\&0 & 0\&0 & 0\&0 & 0\&0 & 0\&0 & 0 \\ 0\&0 & 0\&0 & 0\&1 & 1\&1 & 1\&1 & 0\&0 & 0\&0 & 0 \\ 0\&0 & 0\&0 & 0\&0 & 0\&0 & 0\&0 & 1\&1 & 1\&1 & 1 \end{pmatrix}$$

In the Tanner graph representation, v_i (where $i = 0, 1, \ldots, 19$) are variable nodes (corresponding to row elements of the parity-check matrix), and c_j (where $j = 0, 1, \ldots, 14$) are check nodes (corresponding to columns of the parity-check matrix). Each check node corresponds to a parity-check equation, as shown on the right side of Figure 1 [Figure 1: see original paper]. Tanner graphs are primarily used in iterative decoding algorithms.

The general decoding process of the bit-flipping (BF) iterative algorithm can be summarized as follows:

a) Initialize decoding iteration count $I = 0$ and receive codeword $\mathbf{r}$.
b) Compute the syndrome $\mathbf{s} = \mathbf{rH}^T$. If $\mathbf{s}$ is all zeros, stop iteration and output the codeword; if $\mathbf{s} \neq 0$, proceed to the next step.
c) For each variable node, check the number of unsatisfied parity-check equations connected to it.
d) If a variable node' s count exceeds a specified threshold b, flip that bit.
e) Update the syndrome. Traverse and check the number of flipped variable nodes connected to the j-th $(j = 0, 1, \ldots, r-1)$ check node, and update $\mathbf{s}$. If the number of flips is zero, update $I = I + 1$; otherwise, set $I = 0$.
f) Otherwise, determine if the iteration count $I = I_{\max}$. If so, terminate iteration and output decoding failure; otherwise, return to step b).

2 Improved Scheme Description

We first establish the main notation used in the scheme, with additional symbols defined as needed during the description. Let n denote the length of the concatenated code, n_1 and n_2 represent the lengths of QC-MDPC and QC-LDPC codes respectively, and k, r, and w denote the information length, parity length, and row weight of the parity-check matrix of the concatenated code, with R representing the code rate.

The proposed scheme consists of three algorithms: key generation, encryption, and decryption. The main improvement combines the parity-check matrices of QC-LDPC and QC-MDPC codes as the private key, applies the concatenated codewords of both codes to the McEliece variant scheme, and provides an improved decoding algorithm. The parity-check matrix $\mathbf{H}$ is composed of $\mathbf{H}_1$ and $\mathbf{H}_2$, which can be transformed into systematic form. From this, we can determine two QC-MDPC and QC-LDPC codes with lengths n_1 and n_2 respectively, which are concatenated into a new quasi-cyclic linear code of length $n = n_1 + n_2$.

2.1 Key Generation

a) Randomly generate two vectors $\mathbf{h}_0$ and $\mathbf{h}_1$ with weights w_0 and w_1 respectively, where $w_0 + w_1 = w$.
b) Use vector $\mathbf{h}_0$ as the first row of parity-check matrix $\mathbf{H}_1$.
c) The remaining $r - 1$ rows of $\mathbf{H}_1$ are obtained by cyclically shifting each block of the first row. Similarly, use $\mathbf{h}_1$ as the first row of $\mathbf{H}_2$, with its remaining $r - 1$ rows obtained by cyclic shifts, where $\mathbf{H} = [\mathbf{H}_1|\mathbf{H}_2]$.

From the obtained parity-check matrix $\mathbf{H}$, left-multiplying by $\mathbf{Q}^{-1}$ yields its systematic form $\mathbf{H}_{\text{sys}} = [\mathbf{I}_r|\mathbf{P}]$, from which we can derive the corresponding $k \times n$ generator matrix $\mathbf{G}$. This can also be expressed as $\mathbf{G} = [\mathbf{G}_1|\mathbf{G}_2]$, where $\mathbf{G}_1$ and $\mathbf{G}_2$ are generator matrices capable of correcting t_1 and t_2 errors for the two component codes respectively. Due to the random components in QC-MDPC codes, there is no need to add scrambling and permutation matrices.

2.2 Encryption

a) Randomly generate an error pattern $\mathbf{e} \in \mathbb{F}_2^n$ where the first n_1 portion has weight at most t_1 and the second n_2 portion has weight at most t_2.
b) Compute the ciphertext: $\mathbf{c} = \mathbf{mG} + \mathbf{e}$.

2.3 Decryption

This paper proposes an improved BF algorithm (new-BF) with the following parameters: variable node count n, check node count r, counter value T_j for $j = 0, 1, \ldots, r - 1$, threshold b, and flip count f_j.

Input: Received vector $\mathbf{r} \in \mathbb{F}_2^n$, maximum iteration count $I_{\max}$, parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{r \times n}$.

Output: Codeword $\mathbf{c} \in \mathbb{F}_2^n$ such that $\mathbf{cH}^T = \mathbf{0}$; or decoding failure.

The algorithm proceeds as follows:

a) Initialize iteration counter $I = 0$ and compute syndrome $\mathbf{s} = \mathbf{rH}^T$.
b) For each check node j ($j = 0, 1, \ldots, r-1$), if $s_j \neq 0$, increment the counters T_i for all variable nodes i connected to check node j.
c) Check counters: if $T_i \geq b$ for variable node i, flip the i-th bit.
d) Update the syndrome. Traverse and check the number of flipped variable nodes connected to the j-th ($j = 0, 1, \ldots, r-1$) check node, and update $\mathbf{s}$. If the number of flips is zero, increment I; otherwise, set $I = 0$.
e) Compute and check if all parity-check equations are satisfied. If not, return to step b); if yes, end decoding.

Decryption: Using the improved BF algorithm to obtain $\mathbf{c}$, after error correction, select the first k bits to recover the plaintext $\mathbf{m}$.

Solutions to several issues in the decoding process:

a) **Threshold calculation/selection.** The threshold directly impacts the number of iterations. If too high, few errors are corrected per iteration; if too low, more correct bits than error bits may be flipped. In Gallager' s original bit-flipping algorithm, the threshold b is precomputed before each decoding iteration, with formulas ensuring certain decoding failure probabilities. Based on Maurich et al.' s [17] test results for several decoding schemes, this threshold calculation method is viable and is adopted in this paper.

b) **Iteration limit.** Research [17] shows that bit-flipping decoding algorithms stop after very few iterations, typically 3-5 on average, with further iterations having minimal impact on success rates. Literature [6] also recommends keeping iterations under 10, as excessive iterations may increase decoding failure probability. Therefore, the iteration count is set to a small integer within 10.

c) **Syndrome update.** Instead of recalculating the syndrome by multiplying the updated codeword with the transpose of the parity-check matrix, this paper updates syndrome values by checking the number of flips of variable nodes connected to each check node. The original scheme requires $(n-w)r$ operations per iteration for syndrome update, while the improved approach requires only wr operations, representing a significant reduction.

3 Security Performance Analysis

3.1 Hard Problems

The security of the proposed McEliece variant relies on the coset weight problem in general linear code decoding, which has been proven to be NP-complete [11] and can resist quantum attacks.

Coset Weight Problem: Given a matrix $\mathbf{H} \in \mathbb{F}_2^{r \times n}$, an n-dimensional vector $\mathbf{s} \in \mathbb{F}_2^r$, and a positive integer t, find a vector $\mathbf{e} \in \mathbb{F}_2^n$ with Hamming weight $wt(\mathbf{e}) \leq t$ such that $\mathbf{eH}^T = \mathbf{s}$, where $\mathbf{H}$ can be transformed into systematic form.

Additionally, the cryptosystem remains secure as long as the following two problems hold: (a) correcting t errors in a quasi-cyclic linear code is hard; (b) determining whether a codeword generated by an $r \times n$ matrix has minimum distance w is hard. These problems have been proven NP-hard in the non-cyclic case [12], with their exact status in the cyclic case unknown. However, consensus suggests that the cyclic property itself does not simplify these problems, similar to lattice-based cryptography.

3.2 Related Attacks

Attacks on coding-theory-based public-key cryptosystems primarily fall into two categories: structural attacks and decoding attacks. Structural attacks aim for key recovery, directly recovering the private key from the public key, while decoding attacks target message recovery, attempting to recover plaintext directly from ciphertext. Decoding attacks mainly involve information set decoding, while structural attacks primarily consist of recently proposed key recovery attacks on QC-MDPC and QC-LDPC schemes [7,9].

3.2.1 Information Set Decoding Attack

Information set decoding attacks aim to find k non-error positions in the error vector using the public key and intercepted ciphertext, such that the $k \times k$ matrix formed by selecting the corresponding columns from the generator matrix is invertible. Given the encryption process $\mathbf{c} = \mathbf{mG}' + \mathbf{e}$, selecting k non-error positions and corresponding columns yields an invertible $\mathbf{G}'_{k\times k}$, allowing recovery of plaintext $\mathbf{m}$ by multiplying both sides by $\mathbf{G}'^{-1}$.

The current best MMT algorithm [13] requires a work factor of $\tilde{O}(2^{0.054n})$, with complexity being an exponential function. Therefore, if code length n and information length k are sufficiently large (e.g., selecting $n = 12005$), the attack becomes infeasible.

3.2.2 Key Recovery Attack

Key recovery attacks select special error patterns $\mathbf{e}$ (see Figure 2 [Figure 2: see original paper]) for encryption and decoding tests. For QC-MDPC codes, Guo et al. showed that recovering only the first half $\mathbf{h}_0$ of the first row vector $\mathbf{h}$ of parity-check matrix $\mathbf{H}$ suffices.

Direct application of this attack to the proposed scheme is infeasible for three reasons:

a) The private key structure in this paper is shown in Figure 3 [Figure 3: see original paper]. For syndrome calculation, only half of $\mathbf{h}$ participates—specifically, the first row vector $\mathbf{h}_0$ and a small portion of $\mathbf{h}_1$ row vectors. The adversary cannot determine the distribution and respective proportions of the two parity-check matrices in the system to recover the key.

b) The inclusion of the QC-LDPC parity-check matrix in our scheme increases the probability that $s_j = 0$ due to its lower density compared

to QC-MDPC, reducing the number of unsatisfied parity-check equations and consequently decreasing decoding failure probability. Additionally, literature [14] confirms that our decoding algorithm remains applicable with relatively low complexity, reducing decoding error probability and increasing attack complexity even in the worst-case QC-MDPC decoding scenario.

c) Guo et al.' s attack has inherent limitations: it lacks explicit numerical relationships, relies heavily on sample experiments for computing the key's distance spectrum, and has unclear boundaries for distinguishing whether $\mathbf{h}_0$ exists in the distance spectrum.

For Fabšič et al.' s [9] reaction attack on QC-LDPC McEliece, the attack is infeasible for two reasons: first, it exploits correlations between sparse permutation matrices $\mathbf{P}$ and soft-decision decoding error probabilities, but our scheme no longer multiplies the generator matrix by scrambling and permutation matrices; second, our codewords consist of QC-LDPC and QC-MDPC concatenation, and the introduction of MDPC codes inherently increases attack complexity.

3.2.3 Other Attacks

For weak key attacks, Bardet et al. [15] proposed a method to find weak keys in QC-MDPC-based public-key encryption schemes, but this attack cannot be applied to our scheme because the QC-LDPC portion of the public key does not satisfy their weak key conditions. For OTD attacks, which target $\mathbf{S}$ and $\mathbf{P}$ in QC-LDPC schemes, our scheme is immune as it eliminates these matrices.

4 Parameter Selection and Implementation Efficiency Analysis

4.1 Parameter Selection

Parameter selection involves certain tradeoffs. For instance, increasing n enlarges the public key and reduces computational efficiency, while decreasing n increases decoding failure probability. The choice of r is typically a prime number, as this makes $x^r + 1$ an irreducible polynomial, allowing efficient selection of invertible elements in $\mathbb{F}_2[x]/(x^r + 1)$ with any odd-weight polynomial.

The selection of code length n and parity-check matrix row weight w affects the error-correcting capability of iterative decoding algorithms. This capability increases with larger n and decreases with larger w, resulting in QC-MDPC schemes having lower error-correcting capability than QC-LDPC schemes. However, appropriate parameter selection [6] ensures QC-MDPC security. The concatenation of both code types enhances error-correcting capability relative to QC-MDPC alone while resisting attacks targeting single-code-type schemes, achieving higher security.

Recommended parameters for QC-MDPC and QC-LDPC schemes are also the most commonly used:

a) **QC-MDPC codes:** Literature [6] recommends parameters providing 80-bit security with code length $n = 9602$ and information length $k = 4801$

bits, which also yields the smallest public key size among alternatives.

b) **QC-LDPC codes:** Baldi et al. [5] improved and optimized parameters from [3], achieving code rate $R = 2/3$ with code length $n = 24576$ and information length $k = 16384$ bits.

Our parameter selection (see Table 1) constrains the concatenated code length to maintain small public key sizes while preserving random distributions. We select $n_1 = 9604$ and $r = 4802$ for QC-MDPC codes, maintaining security, and $n_2 = 12005$ for QC-LDPC codes, ensuring 80-bit security. The concatenated code achieves code rate $R = 4/5$ and $w = 55$, with increased code rate improving spectral efficiency and performance.

Table 1: Parameter Selection

Parameter	QC-MDPC	QC-LDPC
n	9604	12005
r	4802	2401
w	90	55
t	84	95

4.2 Key Size and Complexity Analysis

4.2.1 Key Size Analysis

The public key in our scheme is $\mathbf{P} \in \mathbb{F}_2^{r\times(n-r)}$. Since both components have cyclic structure and can be transformed into systematic form, the public key size is $r \times (n-r)$ bits. As shown in Table 2 , the public key size is significantly reduced compared to Goppa-code and QC-LDPC-based McEliece schemes, and slightly larger than QC-MDPC-based schemes while resisting key recovery attacks on QC-MDPC.

Table 2: Comparison with Several Schemes

Scheme	Public Key (Bytes)	Information Bits	Encryption Operations	Decryption Operations
McEliece (original)				
QC-LDPC				
QC-MDPC				
This work				

4.2.2 Complexity Analysis

1) Key Generation: a) Unlike LDPC and original McEliece schemes, our scheme eliminates encryption of the generator matrix, reducing at least $k \times n$ operations. b) The generated parity-check matrices are circulant, requiring consideration of only the first row vector followed by $r-1$ cyclic shifts, resulting in low complexity. c) Computing $\mathbf{P}$ from $\mathbf{H}$ requires matrix inversion. Since $\mathbf{H}$ is circulant, we can employ an efficient matrix inversion algorithm [16] to reduce computational operations.

2) Encryption: Includes multiplication of the plaintext vector with the generator matrix and addition of the error pattern, with operation counts shown in Table 2.

3) Decryption: Using the improved BF algorithm to obtain $\mathbf{c}$, after error correction, selecting the first k bits yields the plaintext. Decryption complexity primarily involves the improved BF decoding algorithm, with operation counts shown in Table 2.

5 Conclusion

This paper proposes an improved McEliece variant based on concatenated codes defined by two parity-check matrices with different densities. Analysis shows that the cyclic structure enables compact keys, the improved decoding algorithm reduces computational complexity compared to the original, and the scheme resists both information set decoding and key recovery attacks. Parity-check-code-based cryptosystems are important post-quantum cryptography schemes, and this variant proves feasible. Future work will focus on the efficiency and security of bit-flipping decoding algorithms.

References

[1] Couvreur A, Marquez-Corbella I, Pellikaan R. Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes [J]. IEEE Trans on Information Theory, 2016, PP (99): 1.

[2] Bardet M, Chaulet J, Dragoi V, et al. Cryptanalysis of the McEliece public key cryptosystem based on polar codes [M]. Post-Quantum Cryptography. Berlin: Springer International Publishing, 2016: 118-143.

[3] Baldi M, Chiaraluce F. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes [C]// Proc of IEEE International Symposium on Information Theory. 2007: 2591-2595.

[4] Otmani A, Tillich J P, Dallot L. Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes [J]. Mathematics in Computer Science, 2010, 3 (2): 129-140.

[5] Baldi M, Bodrato M, Chiaraluce F. A new analysis of the McEliece cryptosystem based on QC-LDPC codes [C]// Proc of International Conference on

Security and Cryptography for Networks. Berlin: Springer-Verlag, 2008: 246-262.

[6] Misoczki R, Tillich J P, Sendrier N, et al. MDPC-McEliece: new McEliece variants from Moderate Density Parity-Check codes [C]// Proc of IEEE International Symposium on Information Theory Proceedings. 2013: 2069-2073.

[7] Guo Q, Johansson T, Stankovski P. A key recovery attack on MDPC with CCA security using decoding errors [M]// Advances in Cryptology. Berlin: Springer, 2016: 789-815.

[8] Shooshtari M K, Ahmadian-Attari M, Johansson T, et al. Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes [J]. IET Information Security, 2016, 10 (4): 194-202.

[9] Fabšič T, Hromada V, Stankovski P, et al. A Reaction Attack on the QC-LDPC McEliece Cryptosystem [C]// Proc of International Workshop on Post-Quantum Cryptography. Cham: Springer, 2017: 51-68.

[10] Mceliece R J. A public-key cryptosystem based on algebraic coding theory [J]. Deep Space Network Progress Report, 1978, 44: 114-116.

[11] Berlekamp E R, Mceliece R J, Van Tilborg H C A. On the inherent intractability of certain coding problems (Corresp.) [J]. IEEE Trans on Inf Theory, 1978, 24 (3): 384-386.

[12] Vardy A. The intractability of computing the minimum distance of a code [J]. IEEE Trans on Information Theory, 2002, 43 (6): 1757-1766.

[13] May A, Meurer A, Thomae E. Decoding Random Linear Codes in Õ (20.054n) [C]// Proc of the 17th International Conference on Theory and Application of Cryptology and Information Security. Berlin: Springer, 2011: 107-124.

[14] Chaulet J, Sendrier N. Worst case QC-MDPC decoder for McEliece cryptosystem [C]// Proc of IEEE International Symposium on Information Theory. 2016: 1366-1370.

[15] Bardet M, Dragoi V, Luque J G, et al. Weak keys for the quasi-cyclic MDPC public key encryption scheme [M]// Progress in Cryptology. Berlin: Springer International Publishing, 2016: 346-367.

[16] Baldi M, Bambozzi F, Chiaraluce F. On a family of circulant matrices for quasi-cyclic low-density generator matrix codes [J]. IEEE Trans on Information Theory, 2011, 57 (9): 6052-6067.

[17] Maurich I V, Oder T. Implementing QC-MDPC McEliece encryption [J]. ACM Trans on Embedded Computing Systems, 2015, 14 (3): 1-27.

Note: Figure translations are in progress. See original paper for figures.