Higher-Order Masking Scheme against DPA Attack in Practice: McEliece Cryptosystem Based on QD-MDPC Code

Mu Han[1], Yunwen Wang[1], Shidian Ma[2*], Ailan Wan[1], Shuai Liu[1]
[1] School of Computer Science and Communication Engineering, Jiangsu University
Zhenjiang, 212013, China
[e-mail: hanmu@ujs.edu.cn, 2221508018@stmail.ujs.edu.cn, sweetlan@ujs.edu.cn]
[2] School of Automotive Engineering Research Institute, Jiangsu University
Zhenjiang, 212013, China
[e-mail: masd@ujs.edu.cn]
*Corresponding author: Shidian Ma

Received December 3, 2017; revised May 30, 2018; revised July 13, 2018; accepted August 19, 2018; published February 28, 2019

Abstract

A code-based cryptosystem can resist quantum-computing attacks. However, an original system based on the Goppa code has a large key size, which makes it unpractical in embedded devices with limited sources. Many special error-correcting codes have recently been developed to reduce the key size, and yet these systems are easily broken through side channel attacks, particularly differential power analysis (DPA) attacks, when they are applied to hardware devices. To address this problem, a higher-order masking scheme for a McEliece cryptosystem based on the quasi-dyadic moderate density parity check (QD-MDPC) code has been proposed. The proposed scheme has a small key size and is able to resist DPA attacks. In this paper, a novel McEliece cryptosystem based on the QD-MDPC code is demonstrated. The key size of this novel cryptosystem is reduced by 78 times, which meets the requirements of embedded devices. Further, based on the novel cryptosystem, a higher-order masking scheme was developed by constructing an extension Ishai-Sahai-Wagne (ISW) masking scheme. The authenticity and integrity analysis verify that the proposed scheme has higher security than conventional approaches. Finally, a side channel attack experiment was also conducted to verify that the novel masking system is able to defend against high-order DPA attacks on hardware devices. Based on the experimental validation, it can be concluded that the proposed higher-order masking scheme can be applied as an advanced protection solution for devices with limited resources.

Keywords: QD-MDPC code, McEliece cryptosystem, DPA attack, Masking scheme

This research was supported by Natural science fund for colleges and universities in Jiangsu Province (12KJD580002), Jiangsu Graduate Innovation Fund (KYLX_1057) and Key research and development plan of Jiangsu province in 2017 (industry foresight and generic key technology) (BE2017035)

http://doi.org/10.3837/tiis.2019.02.033 **ISSN : 1976-7277**

1. Introduction

With the rapid development of quantum-computing theory and technology, traditional public key cryptosystems face high security risks [1]. According to the principle of Shor's algorithm, many researchers believe that cryptosystems based on the number theory problem will no longer be safe in the age of quantum computers. However, public key cryptosystems based on coding theory will be able to resist quantum-computing attacks [2]. In 1978, the original code-based cryptosystem, the McEliece public cryptosystem based on the Goppa code, was proposed [3]. Compared with a traditional public key cryptosystem, code-based cryptography is of higher efficiency during the encryption and decryption process. However, the large key size of the original McEliece makes it difficult to be applied in practice on embedded devices with limited resources [4]. Recently, to reduce the key size, some improved McEliece cryptosystems have been developed based on various types of error correcting codes such as the LDPC, MDPC, QC-MDPC, and QD-Goppa codes [5-8]. Although these improved cryptosystems satisfy the application requirements of embedded devices, they cannot defend against side channel attacks [9].

The most widely used technique for implementing a side channel attack is a power analysis method. Among all power analysis methods, the differential power analysis (DPA) attack is most threatening to cryptographic algorithms [10, 11] because of the low implementation cost, large attack intensity, and small key search space. Therefore, many studies have been conducted on defending against DPA attacks [12-14]. As of now, there are two developed defense technologies against DPA attacks, namely, masking technology [13] and hiding technology [14]. Among them, masking technology is more popularly applied owing to its relatively low cost.

On the other hand, code-based cryptography against DPA attacks has also been proposed [15, 16]. In 2014, Maurich et al. proposed the use of a masking scheme for code-based cryptosystems by adding redundancy calculations [15]. However, this scheme can only resist a simple power analysis (SPA), but not a DPA attack. In 2016, Chen et al. proposed a masking scheme that uses the principle of secret sharing to protect the key and syndrome matrix of a code-based cryptosystem [16]. The scheme is able to defend against low-order DPA attacks, although its high-order DPA defense capability is very limited [17].

In this paper, a masking scheme for McEliece cryptosystems based on the QD-MDPC code is presented. The proposed scheme is able to defend against higher-order DPA attacks. The design of the scheme is divided into two parts. (1) First, a novel QD-MDPC McEliece cryptosystem and a QD-MDPC code are constructed. Compared with the original scheme, the key size of the novel scheme has been reduced by 78 times, and a lower complexity is achieved. At the same time, structural and decoding attack tests were conducted and successfully defended, which verifies the security of the new scheme. (2) Based on the new cryptosystems, a higher-order masking scheme is proposed by extending the ISW security-masking scheme over F_{2^n}. A side-channel attack experiment for the masking scheme on the FPGA platform has been conducted. The experimental results verify that the proposed scheme is able defend against high-order DPA attacks.

The rest of the paper is organized as follows: In Section 2, the related basic knowledge and information are reviewed. In Section 3, a novel McEliece cryptosystem designed through the construction of the QD-MDPC code is described, and the complexity and security of the novel scheme are analyzed. In Section 4, a higher-order masking scheme for the QD-MDPC McEliece cryptosystem is proposed. In Section 5, a side-channel attack experiment conducted

on the masking scheme is discussed. Finally, Section 6 presents some concluding remarks regarding this research.

2. Preliminaries

2.1 Code-Based Cryptosystem

- Coding Theory [18]

Definition 1 (linear codes). A binary (n, r) linear code C with length n, dimension n-r, and co-dimension r is a $(n-r)$-dimensional vector subspace of F_{2^n}. It is spanned by the rows of a matrix $G \in \mathrm{F}_2^{k\times n}$, called a generator matrix of C. Equivalently, it is the kernel of a matrix $H \in \mathrm{F}_2^{r\times n}$, called a parity-check matrix of C. The codeword $c \in C$ of a vector $m \in \mathrm{F}_2^{(n-r)\times n}$ is $c = mG$. The syndrome $s \in \mathrm{F}_2^r$ of a vector $e \in \mathrm{F}_2^n$ is $s = He^T$.

Definition 2 (Hamming weight). The Hamming weight of a vector $x_1, x_2, \ldots, x_n \in F_2^n$ is the number $wt(x)$ of its non-zero components.

Definition 3 (dyadic matrix). Here, R is a ring, and vector $h = (h_0, \cdots, h_{n-1}) \in R^n$. The dyadic matrix $\Delta\,(h) \in R^{n\times n}$ is a symmetric matrix with components $\Delta_{i,j} = h_{i\oplus j}$, where $\oplus$ denotes a bitwise exclusive-or. Sequence h is the seed of the dyadic matrix. The form of $\Delta\,(h)$ follows formula (1).

$$\Delta\,(h) = \begin{bmatrix} h_{0\oplus 0} & \cdots & h_{0\oplus n} \\ \vdots & \ddots & \vdots \\ h_{n\oplus 0} & \cdots & h_{n\oplus n} \end{bmatrix} \tag{1}$$

A quasi-dyadic matrix contains several dyadic matrices. If n is a power of 2, then a $2^k \times 2^k$ dyadic matrix M can be recursively characterized as $M = \begin{bmatrix} A & B \\ B & A \end{bmatrix}$, where A and B are $2^{k-1} \times 2^{k-1}$ dyadic submatrices. It is clear that the seed $h = (h_0, \cdots, h_{n-1})$ of a dyadic matrix coincides with its first row, and each row is a permutation of h.

Definition 4 (MDPC code). A (n, r, w) MDPC code is easily generated by picking a random $r \times n$ matrix with rows of weight w:

(1) Generate r vectors $(h_i \in \mathrm{F}_{2^n})_{0\le i\le r}$ of weight w uniformly at random.

(2) The MDPC code is defined by a parity-check matrix $H \in \mathrm{F}_{2^n}$ of the i-th row h_i.

With overwhelming probability, this matrix is of full rank, and the rightmost $r \times r$ block is always invertible after possibly swapping a few columns.

The BF Decoding Algorithm - Gallager proposed a BF decoding algorithm for the LDPC code [19]. According to the parity-check matrix H of the QD-MDPC code, which has a larger density, the decision threshold T is set as $Max_{upc} - \delta$, where δ is a small integer [20]. The number of iterations is reduced through an increase in the number of flipping bits per iteration, and thus the decoding complexity is reduced. The BF decoding algorithm is shown in Algorithm 1.

Algorithm 1 BF decoding algorithm	
Input: $Max_i \in N^*$, $\delta \in N$, $y \in \mathrm{F}_{2^n}$, $H \in \mathrm{F}_{2^{r\times n}}$	
Output: $c \in \mathrm{F}_{2^n}$, such as $Hc^T = 0$ or fall	
1: while ($\delta > 0$) do	
2: $c = y$; $D = 0$	// D denotes the number of iterations.
3: while ($D < Max_i$) do	

```
4:        Max_upc = 0; counter_i = 0 (1 ≤ i ≤ n)
5:        s = Hc^T                    // counter stores the upc number of each message bit.
6:        for i = 1 to r do
7:            if s[i] = 1 do
8:                for j = 1 to n do
9:                    counter_H[i][j] = counter_H[i][j] + 1
10:               end for
16:           end if
17:       end for
18:       for i = 1 to n do
19:           if counter_i ≥ (Max_upc − δ) do
20:               flips the bit c_i
21:           end if
22:       end for
23:       if Hc^T = 0 then
24:           return c
25:       end if
26:   end while
27:   δ = δ − 1
28: end while
29: return fall
```

- The original McEliece cryptosystem

The first code-based cryptosystem was based on the Goppa code, proposed by McEliece [3] in 1978. A binary Goppa code is defined by a (irreducible) polynomial of degree t over F_{2^m}. Corresponding to each such polynomial, there exists a binary Goppa code of length $n = 2^m$, dimension $k > n - mt$, and minimum distance $d = 2t + 1$, where t is the number of errors correctable using an efficient decoding algorithm.

Key Generation. The public-key is $G' = SGP$, where G is a $k \times n$ generator matrix for the Goppa code, S is a $k \times k$ non-singular matrix, and P is an $n \times n$ permutation matrix. In addition, the private keys are S, G, and P.

Encryption. First set a plaintext m, and then generate an error vector e, whose Hamming weight is at most t. Finally, compute $c = mG' \oplus e$.

Decryption. First compute $cP^{-1} = mSG \oplus eP^{-1}$, and then compute $mS = \varphi_D(cP^{-1})$, where φ_D is the decoding algorithm of the Goppa code. Finally, compute the plaintext $mSS^{-1} = m$.

2.2 DPA Attack [10]

A DPA attack is one of the most popular side channel attacks. The total energy consumption of a common CMOS circuit is mainly caused by a dynamic energy consumption, which is mainly related to the processing, which is the physical circuit basis of an energy attack.

The DPA attack includes two steps: waveform acquisition and data analysis. A waveform acquisition occurs on the hardware part; however, this article mainly uses the simulation software, and thus is mainly related to a data analysis, the detailed steps of which are as follows:

(1) Decrypt different ciphertext N groups and measure the energy trace during the McEliece operation process $\{P_i \mid 1 \le i \le N\}$.

(2) Select a bit of the output value of the attack point as a function D, with b indicating the bit value, called an intermediate value. It is easy to see that the value of b depends on key

K and plaintext M, which can be indicated as $D\ (K, M)$. The related value during an attack is then estimated to obtain the corresponding intermediate value. According to the intermediate value, the energy trace of N groups can be divided into two categories, $S_1 = \{P_1|D = 1, 1 \leq i \leq N\}$ and $S_0 = \{P_1|D = 0, 1 \leq i \leq N\}$.

(3) The average power consumptions of sets S_1 and S_0 are calculated separately. The results are $A_1 = \frac{1}{S_1}\sum S_1\ (i)$ and $A_0 = \frac{1}{S_0}\sum S_0\ (i)$. Here, S_1 and S_0 indicate the number of energy traces corresponding to the collection $|S_1| + |S_0| = N$.

(4) The difference between them is $T = A_1 - A_0$. If the key is correctly estimated, and the classification of the energy traces is correct, that is, all traces of b = 1 point to S_1, and the remaining traces of b = 0 are assigned to S_0, an obvious peak occurs in the energy traces. If the key is not correct, the peak of T will be very small or no peak will occur.

- TVLA Test

A leakage assessment is the only method of detection, whose purpose is to find a potential side channel information leak of the cryptosystem. When a DPA attack model attacks a cryptosystem, it is mainly based on the side channel information. A leakage assessment mainly detects the existence of side channel information. This methodology is called a test vector leakage assessment (TVLA) [22].

A TVLA test is applied to verify the security of our McEliece cryptographic algorithm, and is successfully used in a first-order side-channel analysis [22]. For a high-order DPA attack, we also need to update the TVLA metric computation formula. A detailed description of how to modify the TVLA metric method for a high-order DPA attack has been provided [25].

The first byte of ciphertext c and the inverse matrix P^{-1} perform multiplications over F_{2^8}, and the result of such a multiplication operation is used as an attack target. First, 100,000 energy traces are collected for the TVLA test, and each energy trace has 2,000 leakage points. These energy traces are then partitioned into two sets. Next, we compute the mean and standard deviation of each set [26]. The mean is marked as u_1 and u_0, and the standard deviation is marked as σ_1 and σ_0. Finally, the TVLA value is computed.

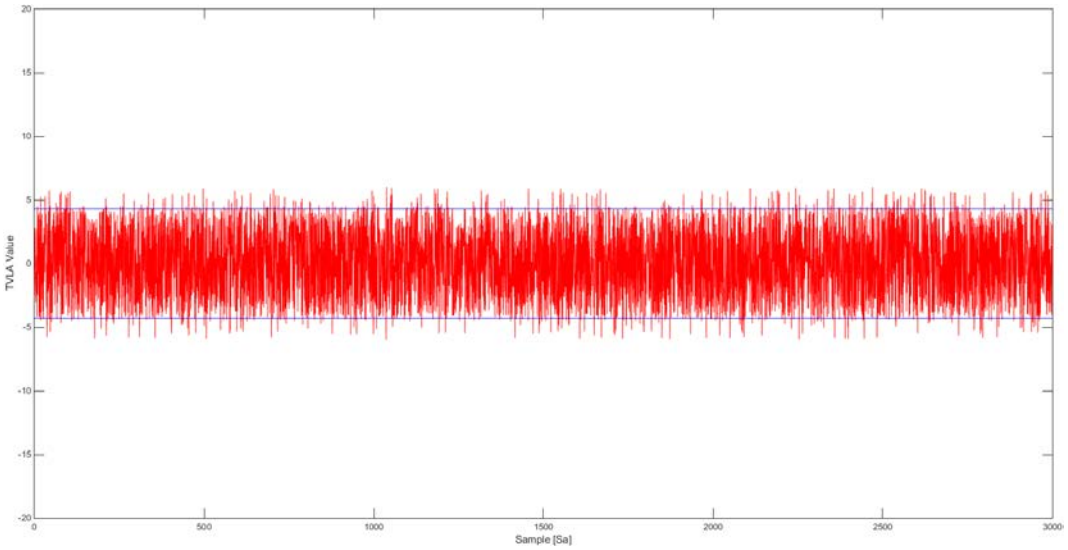

Fig. 1. TVLA test results

As shown in **Fig. 1**, the TVLA value exceeds the safe value (such as ± 4.5 [26]). If any TVLA value in **Fig. 1** does not exceed the security value, it means that the McEliece algorithm does not participate in the leakage associated with the key information.

3. McEliece Cryptosystem Based on QD-MDPC Code

In this section, we first construct the QD-MDPC code by compacting the public-key matrix of the MDPC code using a quasi-dyadic matrix. A McEliece cryptosystem based on the QD-MDPC code is then constructed.

3.1 Constructing QD-MDPC Code

We select a linear code with length $n = 2^m$, dimension $k = 2^{m-1}$, and co-dimension $r = 2^{m-1}$, where m denotes a positive integer. The parity-check matrix H over F_{2^n} is shown in formula (2).

$$H = [H_0|H_1|\dots|H_{n_0-1}] \tag{2}$$

where H_n is a dyadic matrix. We set $h_n = (e_0, \dots, e_{r-1}) \in \mathrm{F}_{2^n}$, $n = 0, 1, \dots, n_0 - 1$, and then dyadic matrix H_n is as shown in formula (3).

$$H_n = \begin{pmatrix} e_0 & \cdots & e_{r-1} \\ \vdots & \ddots & \vdots \\ e_{r-1} & \cdots & e_{(r-1)\oplus(r-1)} \end{pmatrix} \tag{3}$$

We assume that H_{n_0-1} is a non-singular matrix. The generator matrix G can be denoted as $G = [I|Q]$, where

$$\mathrm{Q} = \begin{bmatrix} (H_{n_0-1}^{-1} \cdot H_0)^T \\ (H_{n_0-1}^{-1} \cdot H_1)^T \\ \vdots \\ (H_{n_0-1}^{-1} \cdot H_{n_0-2})^T \end{bmatrix} \tag{4}$$

and I denotes the identity matrix. Finally, a QD-MDPC code is constructed using the parity-check matrix H and the generator matrix G.

3.2 McEliece Cryptosystem Based on QD-MDPC Code

The novel McEliece cryptosystem is constructed as follows:

- Key Generation.

(1) Generate a parity-check matrix $H \in \mathrm{F}_{2^{r\times n}}$ of the QD-MDPC code, as described above.

(2) Generate its corresponding generator matrix $G \in \mathrm{F}_{2^{k\times n}}$, as described above.

(3) Compute the public-key matrix $G' = SGP$, where we randomly select a k-order non-singular matrix S and an n-order permutation matrix P, which are used to generate a complete public-key G', and only the first line elements of G' need to be stored.

The n-order permutation matrix P, k-order non-singular matrix S, and generator matrix G are private keys, and the matrix G' is a public key.

- Encryption. To encrypt a plaintext $m \in \mathrm{F}_{2^k}$ into $c \in \mathrm{F}_{2^n}$, the following are applied:

(1) Generate $e \in \mathrm{F}_{2^n}$ of $w(e) \le t$ at random.

(2) Compute ciphertext $c = mG' \oplus e$.

- Decryption. To decrypt a ciphertext $c \in \mathrm{F}_{2^n}$ into $m \in \mathrm{F}_{2^k}$, the following are applied:

(1) Compute $cP^{-1} = mSG \oplus eP^{-1}$.

(2) Compute $mS = \varphi_H(cP^{-1})$ using the BF decoding algorithm.

(3) Compute plaintext $mSS^{-1} = m$.

3.3 Performance Analysis

(1) Security Analysis

Recently, the LDPC code was successfully cracked using the dual code attack (DCA) and information set decoding attack (ISDA) [6, 28]. Aiming at the problem of structural defects of the error-correcting code, both of the above attacks are the main methods of attack of a McEliece cryptosystem by searching for low-weight codewords [29]. The DCA attack method attempts to obtain a private key according to the public key, and then recover the plaintext. Meanwhile, the ISDA attack method attempts to decrypt the ciphertext directly. The following analysis will show that our McEliece can resist DCA and ISDA attacks.

- DCA Attack Analysis

The DCA attack method obtains a private-key according to the public key by searching for a low-weight codeword in the dual code of the QD-MDPC code. We give a parity-check matrix H'. Attackers can easily find the line weight of H' according to the sparseness of its structure, and then decrypt the ciphertext. If the work factor (WF), namely, the time complexity of successfully attacking a cryptosystem, is greater, the public key cryptosystem based on the error-correcting code has more security. For the LDPC code, the WF of the DCA is heavily correlated with the line weight of H', and does not have a significant correlation with code length n [20]. To allow the QD code to resist a DCA, we use the MDPC code to improve the QD code, and the QD-MDPC code then generates a parity-check matrix H that has a larger density. Thus, our code generates a more compact matrix G, and does not need to resist a DCA by increasing the length of the code, as with the LDPC code. It can be seen from the above that McEliece based on the QD-MDPC code can resist a DCA.

- ISDA Attack Analysis

Among the currently known attack methods, ISDA has the smallest WF. According to the encryption process $c = mG' \oplus e$, and if public key G' is known, attackers can restore k-bit plaintext m by intercepting n-bit ciphertext c. ISDA first obtains the following three parameters: the selection of (1) k-bits c_k from ciphertext c, (2) the corresponding k-bits e_k from error vector e, and (3) the corresponding k-order matrix G'_k from public key G'. It then computes $c_k = mG'_k \oplus e_k$. If G'_k is a non-singular matrix, we set its inverse matrix as G'^{-1}_k, and the attackers then compute $m = (x_k \oplus e_k)G'^{-1}_k$. If $e_k = 0$, attackers can easy obtain the plaintext $m = x_k G'^{-1}_k$. Therefore, the WF of ISDA is associated with the error correcting vector e, and increases when the density of the error correcting vector e is added [20]. The MDPC code is compared with the LDPC code, and has a higher error correction capability. McEliece based on the QD-MDPC code can increase the WF by increasing the density of error correcting vector e, which allows our algorithm to obtain a high level of security.

(2) Efficiency Analysis

This section demonstrates that our algorithm improves the efficiency of a McEliece cryptosystem based on the Goppa code in terms of the key size, bit rate, and encryption and decryption complexity.

- Key Size and Bit Rate

According to the characteristics of a dyadic matrix, the first row of each dyadic sub-matrix can generate an entire quasi-dyadic matrix. In this paper, we take the finite field F_{2^8} as an example to analyze the efficiency of the novel McEliece cryptosystem. The size of a public key is $8 * p$, where p is taken from $[2^{11}, 2^{14}]$. When p is changed, the change in key size is as shown in **Fig. 2**.

The key size of the original McEliece cryptosystem based on Goppa is 32,730 Bytes. If parameter p takes the maximum value in **Fig. 2**, the key size of our scheme is reduced by about 78 times when compared with the conventional schemes.

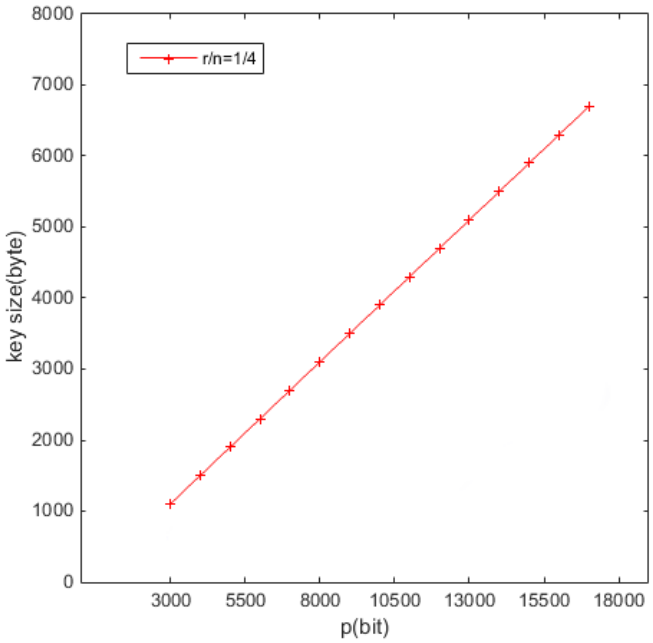

Fig. 2. Key size of the novel McEliece with the change in p

- Encryption Complexity

The complexity of the McEliece encryption includes the complexity of the key generation and encryption. In the process of key generation, we need to compute the inverse matrix $H_{n_0-1}^{-1}$, and then obtain the public key G'. According to the dyadic characteristics of a block matrix, we use a fast algorithm to obtain the inverse matrix $H_{n_0-1}^{-1}$, which reduces the computational complexity. The encryption operations include a matrix multiplication and matrix addition.

As shown in **Fig. 3**, with the increase in the p value, the bit encryption requires binary operands, and an operand does not exceed 2,550 bytes in the novel McEliece encryption. Thus, our algorithm has less computational complexity compared with the conventional algorithms.

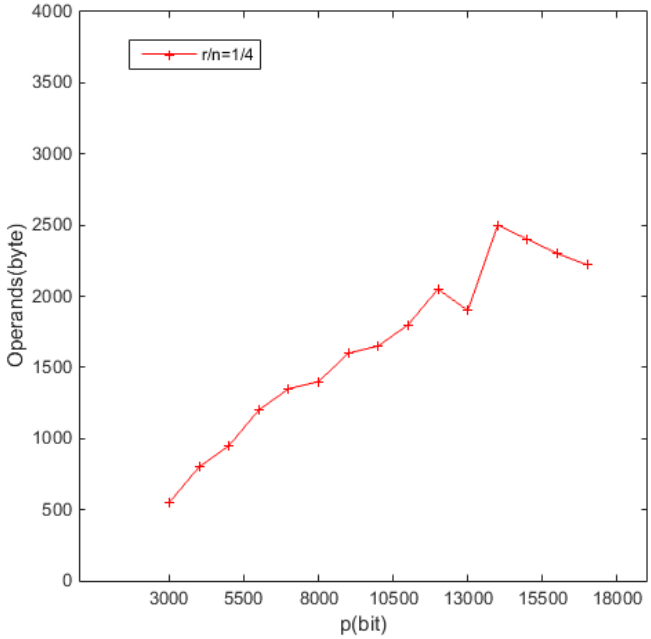

Fig. 3. Encryption complexity of novel McEliece

- Decryption Complexity

A decoding algorithm is the key to determining the decryption complexity. Currently, many decoding algorithms of error-correcting codes can be generally divided into two classes: 1) an algorithm with a strong error-correcting capability and high computational complexity, such as the sum product algorithm (SPA) [23], and 2) an algorithm with low computation complexity, such as the BF decoding algorithm. A comparative analysis between the BF and SPA decoding algorithms when used to decode our novel McEliece cryptosystem is shown in **Fig. 4**.

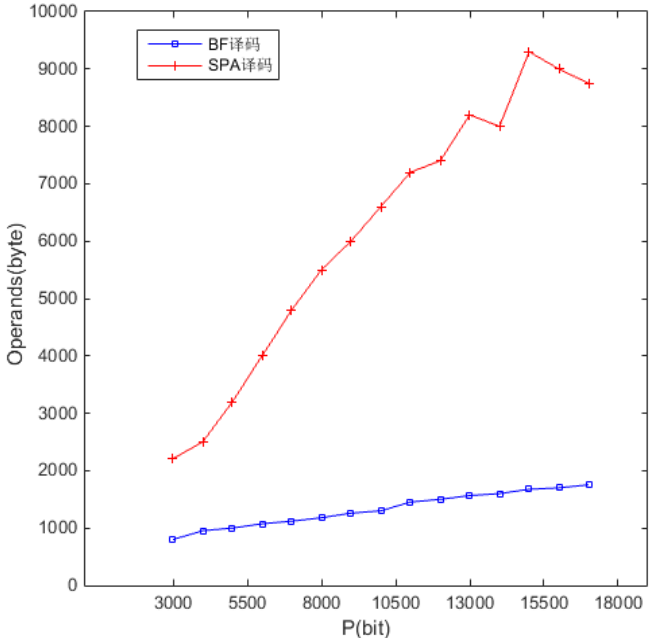

Fig. 4. Decryption complexity of novel McEliece

As shown in **Fig. 4**, the computational complexity of the SPA decoding algorithm is 5 to 6 times the computational complexity of the BF decoding algorithm. Thus, we use the BF decoding algorithm to decode the McEliece cryptosystem based on the QD-MDPC code.

4. Higher-Order Masking for McEliece Based on QD-MDPC Code

4.1 DPA Attack Analysis

An implementation of the McEliece cryptographic algorithm based on the QD-MDPC code includes a linear operation (XOR) and non-linear operation (multiplication over F_{2^n}). When the McEliece cryptographic algorithm based on the QD-MDPC code is applied to hardware devices, a linear operation cannot cause a leakage of information, but more energy will be consumed when carrying out a non-linear operation, and such energy consumption causes a leakage of key information. Thus, if an adversary implements a DPA attack, a non-linear operation faces high risks. A DPA attack analysis of McEliece based on the QD-MDPC algorithm is shown in **Fig. 5**.

In **Fig. 5**, the positions of AP1, AP2, and AP3 are non-linear operation parts of the algorithm, and thus these positions can easily reveal a private key if they suffer from a DPA attack.

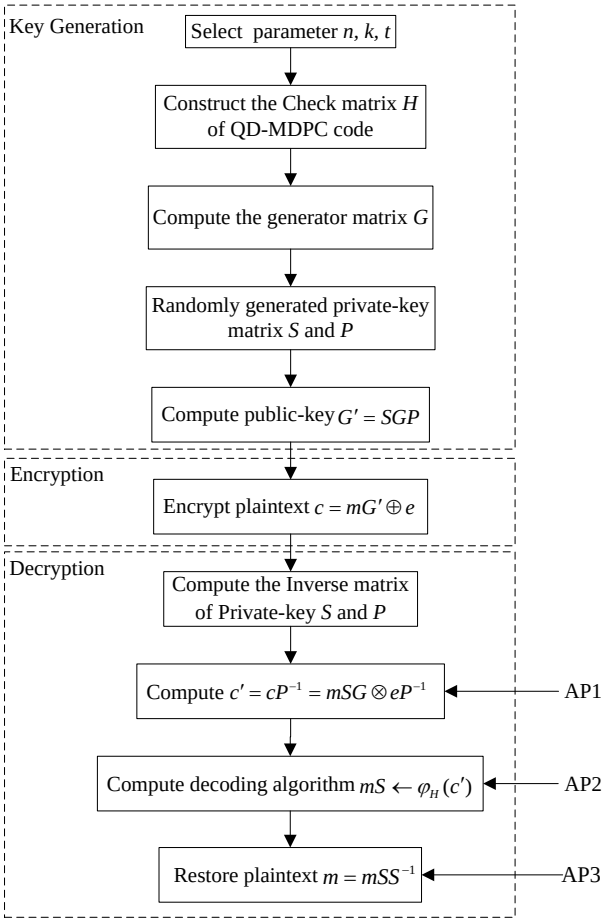

Fig. 5. DPA attack positions for McEliece based on QD-MDPC code

4.2 Higher-Order Masking Scheme for McEliece based on QD-MDPC code

As described in Section 4.1, multiplication over $F_{2^n}$of McEliece based on the QD-MDPC code algorithm is vulnerable to a DPA attack. To securely carry out a multiplication operation over F_{2^n}, we propose a higher-order masking scheme according to the ISW security masking scheme.

Because the original ISW masking scheme [3] can only ensure the security of an XOR operation over finite field F_2, we first need to extend the original ISW masking scheme from finite fields F_2 to F_{2^n} to guarantee the operational security of multiplication over finite field F_{2^n}

- Extension of ISW Masking Scheme as Follows:

Step 1: A higher-order masking scheme for multiplication over F_{2^n} (non-linear functions) is initialized as follows:

(1) We suppose that a and b are sensitive variables, such that $a = g(k)$ and $b = h(k)$ for two F_2-linear functions g and h, where k is a random number over F_{2^n}.

(2) Data k is randomly split into $(k_i)_i$, $0 \le i \le d$, which satisfies $\oplus_{i=0}^{d} g(k_i) = \oplus_{i=0}^{d} a_i$ and $\oplus_{i=0}^{d} h(k_i) = \oplus_{i=0}^{d} b_i$, where d denotes the security level, that is, the order of the DPA attack.

Step 2: Function f is defined from $F_{2^n} \oplus F_{2^n} \to F_{2^n}$, following formula (5).

$$f(x, y) = h(x) \odot g(y) \oplus g(x) \odot h(y) \tag{5}$$

where x denotes the share k_i, y denotes the share k_j, and $\odot$ denotes the multiplication over F_{2^n}. According to formula (5), formula (6) is derived by introducing a random number k:

$$v_{j,i} = a_i b_j \oplus a_j b_i \oplus v_{i,j} = v_{i,j} \oplus f(k_i, k_j) \tag{6}$$

where $v_{i,j}$ denotes a random number.

Step 3: $f(k_i, k_j)$ cannot be directly computed because it will leak into two different shares of a and b at the same time. To avoid such a leakage, we use an additional fresh random value, denoted as $v'_{i,j}$, to split in the computation of $f(k_i, k_j)$.

It can be determined whether the F_2 linearity of g and h implies the F_2 bilinearity of f. That is, for every $x, y, r \in F_{2^n}$, f satisfies formula (7).

$$f(x, y) = f(x, y \oplus r) \oplus f(x, r) \tag{7}$$

To protect shares a_j and b_j, formula (8) is derived through formula (7).

$$v_{j,i} = (v_{i,j} \oplus f(k_i, k_j \oplus v'_{i,j})) \oplus f(k_i, v'_{i,j}) \tag{8}$$

Step 4: To protect the shares a_i and b_j, and not increase the number of computations, we derive from formula (8) the expression for generating a random number in our scheme (formula (11)) based on formulas (9) and (10). The function w maps F_{2^n} to F_{2^n}.

$$w(x) = h(x) \odot g(x) \tag{9}$$

where x denotes the share k_i, and $\odot$ denotes the multiplication over F_{2^n}. The F_2 linearity of g and h then implies the following relation between f and w. For every $x, y \in F_{2^n}$, f satisfies formula (10).

$$f(x, y) = w(x \oplus y) \oplus w(x) \oplus w(y) \tag{10}$$

We then obtain formula (11).

$$v_{j,i} = ((v_{i,j} \oplus w(k_i \oplus v'_{i,j} \oplus k_j)) \oplus w(k_i \oplus v'_{i,j}) \oplus w(k_j \oplus v'_{i,j})) \oplus w(v'_{i,j}) \tag{11}$$

where the brackets indicate the order in which the operations are processed.

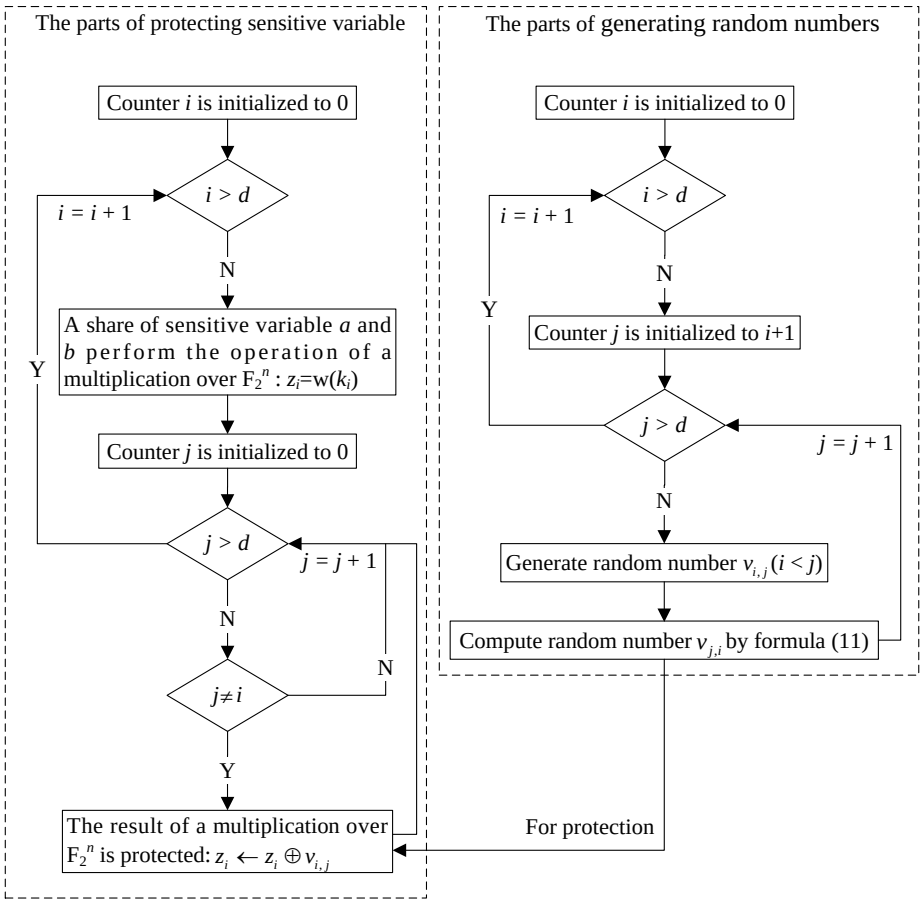

Fig. 6. Extension ISW masking scheme

Step 5: According to **Fig. 6**, each loop generates d random numbers to respectively ensure that the shares of a and b perform the multiplication over F_{2^n}, that is, $z_i = z_i \oplus v_{i,0} \oplus \ldots \oplus v_{i,i-1} \oplus v_{i,i+1} \oplus \ldots \oplus v_{i,d}$.

The extension the ISW masking scheme is as shown in **Fig. 6**. We set the random array as $v = \{v_{i,j} | \, 0 \le i \le d, 0 \le j \le d, i \ne j\}$, where $v_{i,j}$ $(i < j)$ is generated by a random number generator, and $v_{i,j}$ $(i > j)$ is produced through the expression used to generate random numbers that we described earlier in this section. Next, we conduct a multiplication over F_{2^n} for the shares of a and b, and then obtain the result $z_i = a_i \odot b_i$. Finally, the result is used to XOR d random numbers in the inner loop. Note that d random numbers are independent of each other and are uniformly distributed. We compute $\oplus_{i=0}^{d} z_i = z$ to remove the mask, and obtain the real value z.

A specific comparison between the extension of the ISW masking scheme and the original ISW masking scheme is shown in **Table 1**.

Table 1. Comparison and analysis of the schemes

Scheme	Protect position	Whether it is suitable to protect McEliece based on QD-MDPC code algorithm
The original ISW [3]	Masking logic AND gate over F_2	No
Our scheme	Masking multiplication over F_{2^n}	Yes

In **Table 1**, we can see that the original ISW masking scheme mainly protects the logic AND gate, that is, the XOR operation over F_2, and thus this scheme is unsuitable for protecting the OQ-MDPC McEliece algorithm over F_{2^n}. However, our extension of ISW masking scheme as shown above is constructed through defining the sensitive variables in the form of polynomial over F_{2^n}, so it can protect the multiplication over F_{2^n}, and allow the QD-MDPC McEliece algorithm to resist against a high-order DPA attack.

- Higher-Order Masking Scheme for McEliece based on QD-MDPC Code

According to the extension ISW masking scheme that we designed, a high-order masking scheme for McEliece based on the QD-MDPC code is proposed. We also need to consider the logic problem involved in the decryption process. The specific flow of McEliece based on the masking encryption algorithm of the QD-MDPC code is given in Algorithm 2.

Algorithm 2 A higher-order masking encryption algorithm for McEliece based on QD-MDPC code

Input: plaintext *m*

Output: ciphertext *c*

1: Construct the check matrix *H* of QD-MDPC code

2: Select the random non-singular matrix *S* and the permutation matrix *P*

3: Compute the generator matrix *G*

4: Compute public-key matrix $G' = SGP$

5: Encrypt plaintext $c = mG' \oplus e$

6: Compute syndrome $cP^{-1} = \text{matMult}(c, P^{-1}, \text{true})$

7: Compute BF decoding algorithm $c' = mS = \varphi_H(cP^{-1})$

8: Restore plaintext $\text{matMult}(c', S^{-1}, \text{true}) = m$

The specific flow of McEliece based on the masking decryption algorithm of the QD-MDPC code is given in Algorithm 3.

Algorithm 3 A higher-order masking decryption algorithm for McEliece based on QD-MDPC code

Input: private-key Matrix P^{-1}, ciphertext *c*, boolean variable *bv*, or private-key matrix S^{-1}, the output *mS* of BF decoding algorithm, boolean variable *bv*

Output: $rl = (rl_1, rl_2, \ldots rl_{ct})$

1: if (*bv*) do /*judge output data*/

2: $ct = n$

3: $cr = n$

4: $mv_{row}^{1\times ct} = c$

5: $mk_{row,col}^{ct\times cr} = P^{-1}$

6: else

7: $ct = r$

8: $cr = r$

9: $mv_{row}^{1\times ct} = mS$

10: $mk_{row,col}^{ct\times cr} = S^{-1}$

11: end if

12: for *col*=1 to *cr* do

13: for *row*=1 to *ct* do

14: $(z_0, z_1, \ldots, z_d)$ is the result in which the higher-order makes a multiplication over F_{2^n}, and the input is mv_{row} and $mk_{row,col}$

15: $Z = z_0 \oplus z_1 \oplus \ldots \oplus z_d$ /*remove mask operation*/

16: $rl_{col} = rl_{col} \oplus Z$

17: end for

18: end for

4.3 Security Analysis

A typical higher-order masking scheme (that is, a d-order masking scheme) must satisfy both of the following characteristics to ensure its integrity and security [21]:

(1) Authenticity: Every tuple of d or less intermediate variables must be independent of any sensitive variables.

(2) Integrity: At the end of the computation, the sum of the d shares must yield the expected ciphertext (and more generally, each masked transformation must result in a set of shares whose sum equals the correct intermediate result).

4.3.1 Authenticity Analysis for Masking Scheme

The security analysis of the masking scheme is based primarily on the following assumption: If the masked intermediate variables do not have a dependency on the real intermediate variables, the energy consumption of the masked intermediate variables do not have a dependency on the real intermediate variables. Therefore, when the assumption does not hold, our masking scheme is vulnerable to a DPA attack. We use the lemma of the security proof on the intermediate variables proposed by Blomer and Canright to analyze the security of our masking scheme [24, 27]. The masking scheme theoretically has high-order security if all masked intermediate variables generated from our masking scheme satisfy the following lemmas.

Lemma 1 [24]. For any $u \in \mathrm{F}_{2^n}$, if $r \in \mathrm{F}_{2^n}$ in the collection $\{0, 1, \ldots, 2^n - 1\}$ obeys a uniform distribution and is independent of u, $z = u \oplus r$ also satisfies a uniform distribution.

Lemma 2 [24]. For any $u, u' \in \mathrm{F}_{2^n}$, if $r, r' \in \mathrm{F}_{2^n}$ in the collection $\{0,1, \ldots, 2^n - 1\}$ obey a uniform distribution and are independent of u and u', $Z = (u \oplus r)(u' \oplus r')$ also satisfies formula (12).

$$\Pr(Z = i) = \begin{cases} \frac{2^{n+1}-1}{2^{2n}} & if\ i = 0 \\ \frac{2^n - 1}{2^{2n}} & if\ i \neq 0 \end{cases} \tag{12}$$

This is called a random multiplication distribution.

Lemma 3 [27]. For any $u \in \mathrm{F}_{2^n}$ that obeys a uniform distribution, if F_{2^n} has a bijective function f from $\mathrm{F}_{2^n} \to \mathrm{F}_{2^n}$, $y = f(u)$ also obeys a uniform distribution.

Now, we use Lemmas 1, 2, and 3 to prove that our masking scheme is secure.

Theorem 1 [27]. If $u = \{u_1, u_2, \ldots, u_{2n}\} \in \mathrm{F}_{2^n}$ obeys a uniform distribution, the two half subsets of u, $y_1 = [u_1, u_2, \ldots, u_n]$ and $y_2 = [u_{n+1}, u_{n+2}, \ldots, u_{2n}]$ are independent of each other and are uniformly distributed.

(1) We suppose that, in our designed masking scheme, the random masks $v_{i,j} \overset{\$}{\leftarrow} \mathrm{F}_{2^n}$ and $v'_{i,j} \overset{\$}{\leftarrow} \mathrm{F}_{2^n}$ all obey a uniform distribution, and are independent of sensitive variables a and b and shares k_i $(0 \le i \le d)$. According to Lemma 1, we obtain $(k_i \oplus v'_{i,j}) \oplus k_j$, where $k_i \oplus v'_{i,j}$ and $k_j \oplus v'_{i,j}$ both obey a uniform distribution in formula (11). Because $\mathrm{g}(*)$ and $\mathrm{h}(*)$ are linear functions, that is, a bijective function, according to Lemma 3, formula (9) is substituted into formula (11) to obtain $\mathrm{h}(k_i \oplus v'_{i,j} \oplus k_j)$, $\mathrm{g}(k_i \oplus v'_{i,j} \oplus k_j)$, $\mathrm{h}(k_i \oplus v'_{i,j})$, $\mathrm{g}(k_i \oplus v'_{i,j})$, $\mathrm{h}(k_j \oplus v'_{i,j})$, $\mathrm{g}(k_j \oplus v'_{i,j})$, $h(v'_{i,j})$, and $\mathrm{g}(v'_{i,j})$, which also obey a uniform distribution. Therefore, according to Lemma 2, we obtain $\mathrm{w}(k_i \oplus v'_{i,j} \oplus k_j)$, $\mathrm{w}(k_i \oplus v'_{i,j})$, and $\mathrm{w}(k_j \oplus v'_{i,j})$, which all obey a uniformly distribution in formula (11). Finally, according to Lemma 1, $v_{i,j}$ $(0 \le j < i \le d)$ generated through formula (11) is also uniformly distributed.

(2) It can be seen from the above discussion that all random numbers $v_{i,j}$ obey a uniform distribution over F_{2^n}, and are independent of the result of $z_i = a_i \odot b_i$. Then, d $v_{i,j}$ are used to respectively protect the result z_i, that is, $z_i = z_i \oplus v_{i,0} \oplus \ldots \oplus v_{i,i-1} \oplus v_{i,i+1} \oplus \ldots \oplus v_{i,d}$. Thus, according to Lemma 1, the outputs $(z_0, z_1, \ldots, z_{d-1}, z_d)$ of the higher-order masking scheme obey a uniform distribution, and are independent of each other.

Therefore, attackers can apply a statistical analysis on any d masked intermediate values and cannot obtain the relevant information of the private key. It can be theoretically proven that the higher-order masking scheme described in Section 4.2 has high-order security.

4.3.2 Integrity Analysis of Masking Scheme

This section verifies the completeness of our masking scheme using a counter-evidence method. The specific analysis process is as follows:

We assume that the mask removal operation is incorrect, that is, $z \neq z_0 \oplus z_1 \oplus \ldots \oplus z_d$. Because the results of formula (11) and formula (6) are the same, a hypothetical condition is derived for formula (13).

$$\begin{aligned} \mathrm{z} &\neq (a_0 b_0 \oplus v_{0,1} \oplus v_{0,2} \oplus \ldots \oplus v_{0,d}) \oplus \ldots \oplus (a_d b_d \oplus v_{d,0} \oplus v_{d,1} \oplus \ldots \oplus v_{d,d-1}) \\ &\neq \big(a_0 b_0 \oplus v_{0,1} \oplus v_{0,2} \oplus \ldots \oplus v_{0,d}\big) \oplus \ldots \oplus (a_d b_d \oplus v_{0,d} \oplus f(k_0, k_d) \oplus v_{1.d} \oplus \\ &\quad f(k_1, k_d) \oplus \ldots \oplus v_{d-1,d} \oplus f(k_{d-1}, k_d)) \end{aligned} \tag{13}$$

Formula (13) is then used to derive formula (14) through formula (5).

$$\begin{aligned} z &\neq (a_0b_0 \oplus v_{0,1} \oplus v_{0,2} \oplus \ldots \oplus v_{0,d}) \oplus \ldots \oplus (a_db_d \oplus v_{0,d} \oplus a_0b_d \oplus a_db_0 \oplus v_{1,d} \oplus \\ &\quad a_1b_d \oplus a_db_1 \oplus \ldots \oplus v_{d-1,d} \oplus a_{d-1}b_d \oplus a_db_{d-1}) \\ &\neq (a_0 \oplus a_1 \oplus \ldots \oplus a_d)(b_0 \oplus b_1 \oplus \ldots \oplus b_d) \end{aligned} \quad (14)$$

Because $a = a_0 \oplus a_1 \oplus \ldots \oplus a_d$ and $b = b_0 \oplus b_1 \oplus \ldots \oplus b_d$ both hold, $(a_0 \oplus a_1 \oplus \ldots \oplus a_d)(b_0 \oplus b_1 \oplus \ldots \oplus b_d) = ab = z$ also holds. Finally, in this section it can be concluded that the hypothetical condition is incorrect. That is, the higher-order masking scheme has completeness.

5. Side Channel Attack Experiment

5.1 Experiment Environment

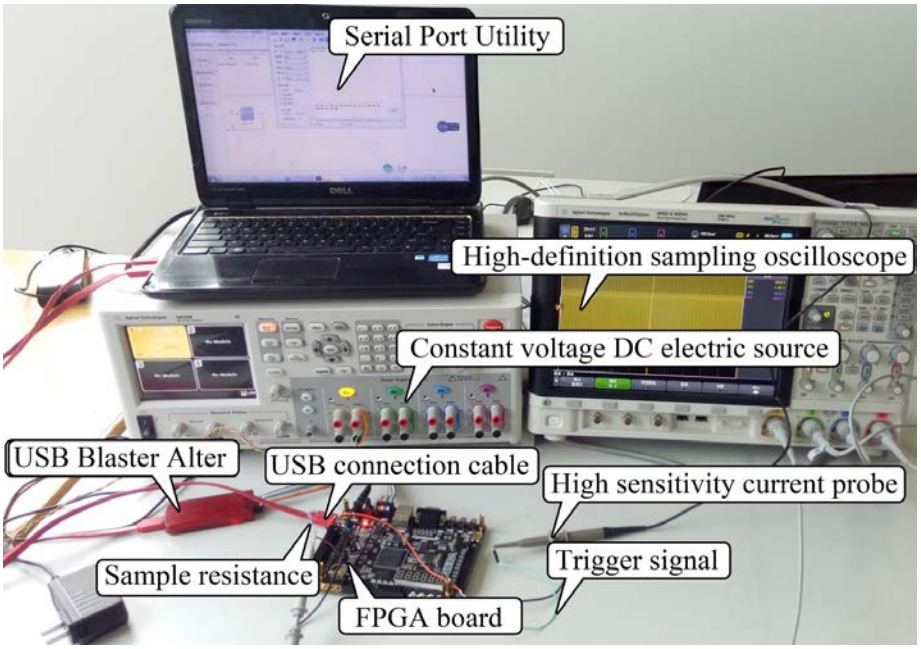

Fig. 7. Simulation experiment environment

In the experiment, the following devices were used: an FPGA board, high-definition sampling oscilloscope, USB Blaster Altera tool, 1 Ω resistance, constant voltage DC electric source, USB connection cable, high-sensitivity current probe, and a PC. The PC configuration was as follows: an Intel Core i5-7300HQ@2.50 GHz CPU, with a 64-bit Windows 7 operating system. We used Verilog in Quartus II 13.0 software to edit the McEliece based on the QD-MDPC code, the MATLAB power analysis program, the Serial Port Utility software, and BenchVue.

Our target is the output of the multiplication over F_{2^n} in the matrix multiplication, because this section involves all bytes of a private key in the McEliece encryption algorithm. We conducted comparative single-group experiments, as described in this section. McEliece based on the encryption algorithm of the QD-MDPC code without masking protection is compared with our scheme. The above verifies the effectiveness of McEliece resisting against a DPA

attack based on the masking algorithm of the QD-MDPC code. The experiment environment is as shown in **Fig. 7**.

5.2 Setup of DPA Attack for McEliece based on QD-MDPC code

The experimental environment described in this section contains two parts: a combinational logic module (McEliece algorithm) and a control module. Overall, the control module controls the start to the end of the encryption/decryption process and the data storage. Here, the parameters of the QD-MDPC code are set to n = 128, k = 64, and t = 49.

(1) To supply electricity to the FPGA board, the voltage of the constant voltage DC electric source is adjusted to 5 V. The positive electrode of the electric source in the FPGA chip is in-series with a 1 Ω resistor. A high-definition sampling oscilloscope probe is used to collect the changes in voltage on the 1 Ω resistor.

(2) The PC is connected to the high-definition sampling oscilloscope to obtain the collected energy traces through the configuration of the Ethernet interface.

(3) The PC is connected to the FPGA board through the USB Blaster Altera tool, and at the same time its USB interface is connected to the serial port of the board. We use the Serial Port Utility software to transmit the ciphertext and decryption signal. In the McEliece encryption algorithm, we set a set trigger signal. When the McEliece encryption algorithm runs the computation process of the matrix multiplication, it is pulled high to drive that the oscilloscope measures the energy consumption of the section. Mainly using the probe, the oscilloscope measures the voltage of the sample resistor. In this experiment, all multiplications over F_{2^8} are selected as attack points in the process of computing $cP^{-1} = mSG \oplus eP^{-1}$.

(4) After the McEliece algorithm has been executed, the PC receives plaintext m from the board, and obtains the collected energy traces from the oscilloscope, which is stored in a local file.

(5) The PC uses the MATLAB power analysis program to conduct the correlation analysis of the leak points of all energy traces. According to the results of the correlation analysis, we found that some points more easily leak the key information. Finally, we obtain the results of the DPA attack.

5.3 Attack Results

For McEliece based on the QD-MDPC McEliece encryption algorithm with our masking scheme protection, we first use the real inverse matrix P^{-1} (It is 0xDD123456789⋯⋯), which is fed into the decryption engine. The oscilloscope then collects the actual energy traces for the attack point. A total of 1,000,000 energy traces are collected, and each energy trace only has 2,000 leakage points.

According to the steps described in Section 5.2 and the principles of the DPA attack described in Section 2.2, we run the MATLAB power analysis program to conduct a correlation analysis for the leak points of all energy traces. The purpose is to find the leak points that easily leak the key information. This type of leak point is expressed as an obvious peak in **Fig. 8**.

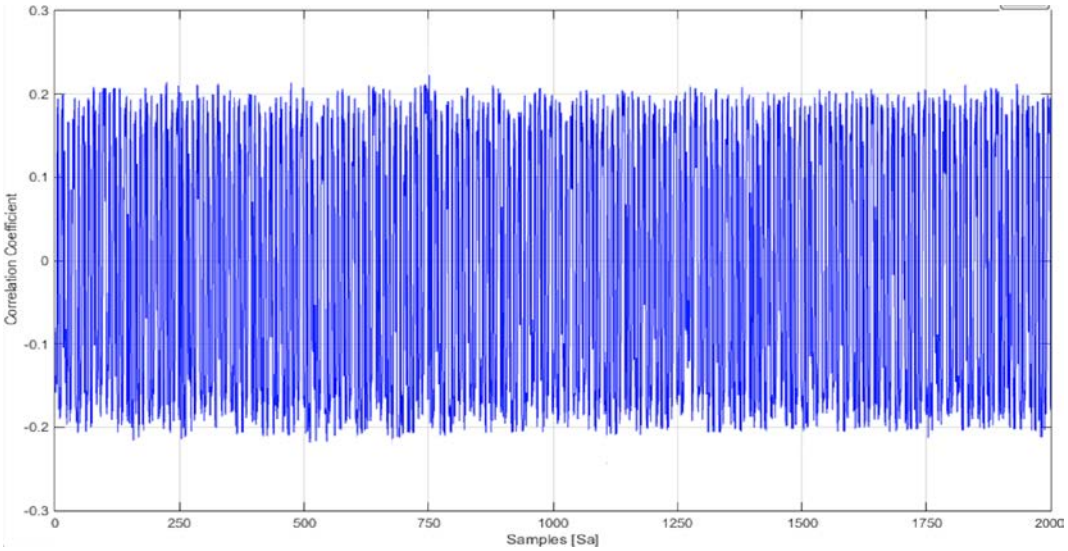

Fig. 8. Results of correlation analysis on first key byte

Fig. 9. Results of second-order DPA attack for first key byte

As shown in **Fig. 8**, leak points that are more vulnerable to a DPA attack do not exist. That is, there are no obvious peaks in **Fig. 8**. Then, a second-order DPA attack model (d = 2) analyzes the leak points of all energy traces. Finally, the result of the DPA attack is shown in **Fig. 9**. If a second-order DPA attack is successful, there will be an obvious peak at 0xDD of the abscissa. Therefore, the second-order DPA attack model does not successfully attack McEliece based on the QD-MDPC code masking scheme, that is, the red part (key = 0x34) of the waveform is not the correct key value.

Next, we use the third-order DPA attack model to attack McEliece based on the McEliece masking cryptographic algorithm of the QD-MDPC code. Because the required energy traces from the first-order DPA attack model to the third-order DPA attack model will continuously increase, in this experiment, 100,000,000 energy traces are collected. We run the MATLAB power analysis program to conduct the correlation analysis for the leak points of all energy

traces. The results of the correlation analysis are shown in **Fig. 10**.

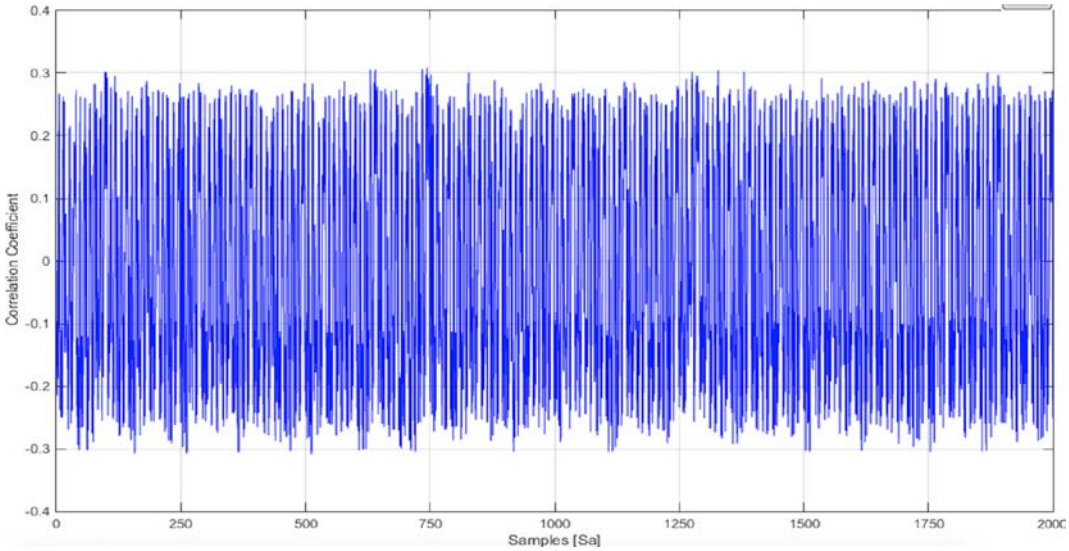

Fig. 10. Results of correlation analysis on first key byte

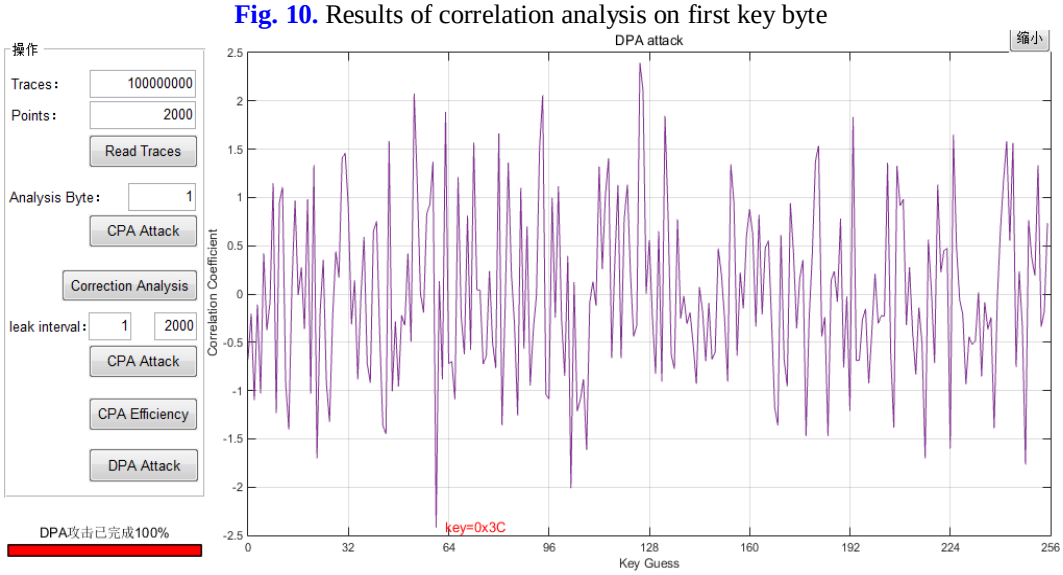

Fig. 11. Results of third-order DPA attack for first key byte

Fig. 10 does not show an obvious peak. Then, McEliece based on the masking cryptographic algorithm of the QD-MDPC code, which is realized in hardware, is attacked using a third-order DPA attack model (d = 3). The results of the DPA attack are shown in **Fig. 11**. At 0xDD of the abscissa, the absolute value of the corresponding difference coefficient is not the largest. Thus, the third-order DPA attack is not successful.

5.4 Comparative Results of the Experiment

For McEliece based on the QD-MDPC code encryption algorithm without a masking scheme protection, we use the real inverse matrix P^{-1} (It is 0xDD123456789⋯⋯) to collect 60,000 actual energy traces. The remaining parameters are set exactly the same as those described in Section 5.3. The results of the correlation analysis are shown in **Fig. 12**.

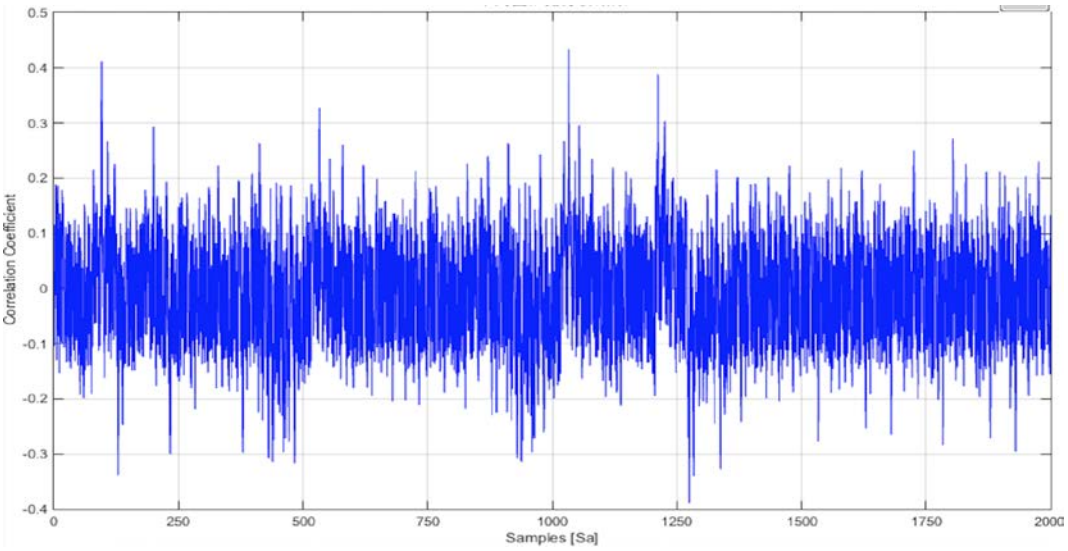

Fig. 12. Results of correlation analysis on first key byte

There are many obvious peaks in **Fig. 12**, and these leak points are more vulnerable to a leak of the key information. Finally, a first-order DPA (d = 1) model attacks the interval [1, 125]. The results of the DPA attack are shown in **Fig. 13**. At 0xDD of the abscissa, the absolute value of the corresponding difference coefficient is the largest. Thus, the first-order DPA model is effective for the McEliece algorithm, and is realized in hardware.

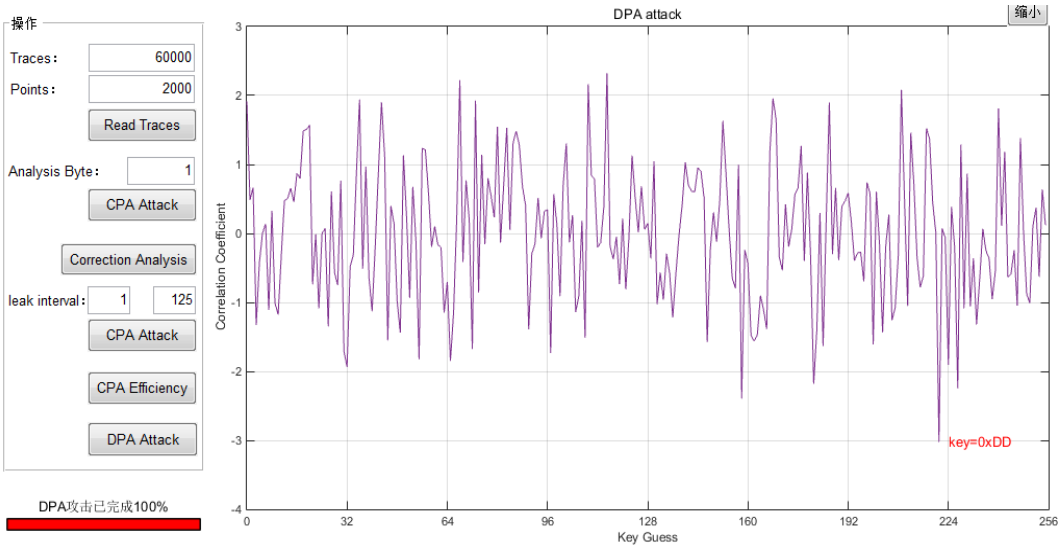

Fig. 13. Results of first-order DPA attack for first key byte

5.5 Comparison and Analysis of Attack Results

The DPA attack model described in Sections 5.4 and 5.5 was used to analyze the security of the McEliece algorithm. The attack results are shown in **Table 2**.

Table 2. Comparison and analysis of attack results

Algorithms	Attack method	Number of energy traces	Time (s)
Without masked protection	First-order DPA model	60,000	1,500
With our masking scheme	Second-order DPA model	1,000,000	40,000 (Unsuccessful)
With our masking scheme	Third-order DPA model	100,000,000	6,000,000 (Unsuccessful)

According to **Table 2**, we found that McEliece based on the QD-MDPC code, which is realized in hardware, cannot defend against a first-order DPA attack. Attackers can easily obtain the first byte 0xDD of the private-key inverse matrix P-1 in 1,500 s. However, for McEliece based on the QD-MDPC code with our masking scheme protection, we analyze 1,000,000 energy traces without obtaining the correct key value. Even when 100,000,000 energy traces are analyzed, our proposed scheme can still defend against a high-order DPA attack.

We conduct a logic synthesis and apply a circuit design for the McEliece encryption algorithm with and without our masking scheme protection under the FPGA platform.

Table 3. Comparison of algorithmic circuit design

Indicators	Without masked protection	With our masking scheme
Frequency (MHz)	50	50
Area (LE)	11k	13k
Performance (Mbps)	300	255
Decryption Memory (bit)	80k	82k

According to **Table 3**, under the same frequency, the complexity of McEliece based on the cryptographic scheme of the QD-MDPC code, which is based on higher-order masking, increases by about 20.8% in the area of hardware implementation. Two reasons can explain this problem: our scheme needs to update the mask and apply higher-order protection on the multiplication over F_{2^n} . In addition, because our scheme has these logical units, it will inevitably lead to a decrease in throughput.

However, it can be concluded that the higher-order masking scheme designed in this study can allow McEliece based on the QD-MDPC code to defend against high-order DPA attacks. Moreover, the performance of the algorithm has not been significantly reduced, and can still meet the performance requirements of its field of application.

6. Conclusion

In this paper, we presented a McEliece algorithm based on the cryptographic scheme of the QD-MDPC code, which is based on higher-order masking. The design of our scheme can be divided into two parts. First, we construct a QD-MDPC code to solve the problem in which Goppa McEliece has a huge key size. We then design a higher-order masking scheme by constructing an extension of the ISW masking scheme. The scheme allows McEliece based on the encryption algorithm of the QD-MDPC code, which is realized in hardware, to defend against high-order DPA attacks. An analysis shows that McEliece based on the QD-MDPC code is about 78 times higher than Goppa McEliece in terms of the key size, and has a lower encryption and decryption complexity. Meanwhile, a security analysis shows that McEliece

based on the QD-MDPC code can resist structural and decoding attacks, and that a higher-order masking scheme has higher security. Finally, side-channel attack experiment shows that the McEliece masking cryptographic algorithm, which is realized in hardware, can defend against a high-order DPA attack. Our scheme consumes fewer resources, and is suitable for devices with little memory and weak communication capacity.

Recently, many statistical analysis methods have been gradually applied to a DPA attack model, such as a correlation power analysis. In particular, a power analysis technique can also be combined with other attack techniques. This new type of attack technology [30] achieves a higher success rate for attacking the McEliece cryptographic algorithm. Thus, how to resist against such attacks will become a significant challenge.

References

[1] Dragoi V, Kalachi H T., "Cryptanalysis of a public key encryption scheme based on QC-LDPC and QC-MDPC codes," *IEEE Communications Letters*, vol. 22, no. 2, pp. 264-267, December, 2017. Article (CrossRef Link).

[2] Shor P W., "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. of Computer Vision, 2009 IEEE 12th International Conference on. America*, pp. 1484-1509, November, 1994. Article (CrossRef Link).

[3] Samokhina M, Trushina O., "Code-Based Cryptosystems Evolution," in *Proc. of Ivth International Conference on Engineering and Telecommunication. IEEE*, pp. 15-17, December, 2017. Article (CrossRef Link).

[4] Baldi M, Santini P, Chiaraluce F., "Soft McEliece: MDPC code-based McEliece cryptosystems with very compact keys through real-valued intentional errors," in *Proc. of Information Theory (ISIT), 2016 IEEE International Symposium on. IEEE*, pp. 795-799, July, 2016. Article (CrossRef Link).

[5] Bolkema J, Gluesing-Luerssen H, Kelley C A, et al., "Variations of the McEliece Cryptosystem," *Algebraic Geometry for Coding Theory and Cryptography*, Springer, Cham, vol. 9, pp. 129-150, November, 2017. Article (CrossRef Link).

[6] Misoczki R, Tillich J P, Sendrier N, et al., "MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes," in *Proc. of IEEE International Symposium on Information Theory Proceedings. IEEE*, pp. 2069-2073, July, 2013. Article (CrossRef Link).

[7] Heyse S., "Implementation of McEliece Based on Quasi-dyadic Goppa Codes for Embedded Devices," in *Proc. of Post-Quantum Cryptography -, International Workshop, Pqcrypto 2011*, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings. DBLP, vol. 7071, pp. 143-162, 2011. Article (CrossRef Link) .

[8] Löndahl C, Johansson T, Shooshtari M K, et al., "Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension," *Designs, Codes and Cryptography*, vol. 80, no. 2, pp. 359-377, August, 2016. Article (CrossRef Link).

[9] Avanzi R, Hoerder S, Dan P, et al., "Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems," *Journal of Cryptographic Engineering*, vol. 1, no. 4, pp. 271-281, December, 2011. Article (CrossRef Link).

[10] Kocher P, Jaffe J, Jun B., "Differential Power Analysis," in *Proc. of Annual International Cryptology Conference*, Springer, Berlin, Heidelberg, vol. 1666, pp. 388-397, December, 1999. Article (CrossRef Link).

[11] Chen C, Eisenbarth T, Maurich I V, et al., "Differential Power Analysis of a McEliece Cryptosystem," in *Proc. of International Conference on Applied Cryptography and Network Security*, Springer International Publishing, vol. 9092, pp. 538-556, June, 2015. Article (CrossRef Link).

[12] Cui J, Chen L, Zhang Y, et al., "A secret sharing scheme based on AES," *International Journal of Security & Its Applications*, vol. 8, no. 6, pp. 295-302, 2014. Article (CrossRef Link).

[13] Yoshikawa M, Kojima Y., "Efficient Random Number for the Masking Method against DPA Attacks," in *Proc. of International Conference on Systems Engineering. IEEE Computer Society*, pp. 321-324, August, 2011. Article (CrossRef Link).
[14] Chen J, Wang Q, Guo Z, et al., "A Circuit Design of SMS4 against Chosen Plaintext Attack," in *Proc. of International Conference on Computational Intelligence and Security. IEEE*, PP. 371-374, February, 2016. Article (CrossRef Link).
[15] Maurich I V, Güneysu T., "Towards Side-Channel Resistant Implementations of QC-MDPC McEliece Encryption on Constrained Devices," in *Proc. of International Workshop on Post-Quantum Cryptography*, Springer International Publishing, vol. 8772, pp. 266-282, 2014. Article (CrossRef Link).
[16] Chen C, Eisenbarth T, von Maurich I, et al., "Masking large keys in hardware: A masked implementation of mceliece," in *Proc. of International Conference on Selected Areas in Cryptography*, Springer, Cham, vol. 9566, pp. 293-309, August, 2015. Article (CrossRef Link).
[17] Yuan M, Bai G., "Improving Second-Order DPA Attacks with New Modeled Power Leakages," in *Proc. of International Conference on Computational Intelligence and Security*, IEEE, PP. 394-397, February, 2016. Article (CrossRef Link).
[18] Cancellieri G., "Polynomial theory of error correcting codes," Springer, 2015. Article (CrossRef Link).
[19] Hailes P, Xu L, Maunder R G, et al., "A survey of FPGA-based LDPC decoders," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1098-1122, December, 2016. Article (CrossRef Link).
[20] Ze-Hui Li, Ya-Tao Yang, Zi-Cheng Li., "New public key cryptography based on QC-MDPC code," *Application Research of Computers*, vol. 32, no. 3, pp: 881-884, March, 2015. Article (CrossRef Link).
[21] Rivain M, Prouff E., "Provably secure higher-order masking of AES," in *Proc. of International Conference on Cryptographic Hardware and Embedded Systems*, Springer-Verlag, vol. 6225, pp. 413-427, 2010. Article (CrossRef Link).
[22] Roy D B, Bhasin S, Patranabis S, et al, "Testing of Side-Channel Leakage of Cryptographic Intellectual Properties: Metrics and Evaluations," Springer, Cham, pp. 99-131, January, 2017. Article (CrossRef Link).
[23] Gupta A, Rajan B S., "Decoding network codes using the sum-product algorithm," in *Proc. of IEEE International Conference on Communications. IEEE*, pp. 423-427, July, 2016. Article (CrossRef Link).
[24] Blömer J, Guajardo J, Krummel V., "Provably Secure Masking of AES," *Selected Areas in Cryptography*, Springer Berlin Heidelberg, vol. 3357, pp. 69-83, January, 2004. Article (CrossRef Link).
[25] Schneider T, Moradi A., "Leakage Assessment Methodology," in *Proc. of International Workshop on Cryptographic Hardware and Embedded Systems*, Springer Berlin Heidelberg, vol. 9293, pp: 495-513, September, 2015. Article (CrossRef Link).
[26] Cooper J, Goodwill G, Jaffe J, Kenworthy G, et al., "Test vector leakage assessment (TVLA) methodology in practice," in *Proc. of International Cryptographic Module Conference*, Holiday Inn Gaithersburg, pp. 24–26, February, 2013. Article (CrossRef Link).
[27] Canright, D., "Avoid mask re-use in masked Galois multipliers," *Faculty Publications Including Published Articles*, pp. 1-7, January, 2009. Article (CrossRef Link).
[28] Heyse S, Zimmermann R, Paar C., "Attacking code-based cryptosystems with information set decoding using special-purpose hardware," in *Proc. of International Workshop on Post-Quantum Cryptography*, Springer, Cham, vol. 8772, pp. 126-141. 2014. Article (CrossRef Link).
[29] Shooshtari M K, Ahmadian-Attari M, Johansson T, et al., "Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes," *IET Information Security*, vol. 10, no. 4, pp. 194-202, June, 2016. Article (CrossRef Link).
[30] Ren Y, Wu L, Wang A., "Double Sieve Collision Attack Based on Bitwise Detection," *KSII Transactions on Internet & Information Systems*, vol. 9, no. 1, pp. 296-308, 2015. Article (CrossRef Link).

[31] Han M, Hua L, Ma S., "A Self-Authentication and Deniable Efficient Group Key Agreement Protocol for VANET," *KSII Transactions on Internet & Information Systems*, vol.11, no. 7, July, 2016. Article (CrossRef Link).

Mu Han is an Associate Professor with the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China. She received her Ph.D. degree in Computer science and application technology from Nanjing University of Science and Technology, Nanjing, China. Her research interests include security and communication in side channel attack, cryptography, etc.
E-mail: hanmu@ujs.edu.cn

Yunwen Wang is pursuing a master's degree candidate. at the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China. His research direction is lightweight cryptography and side channel attack.
E-mail: 2221508018@stmail.ujs.edu.cn

Shidian Ma is an Associate Professor with the Automotive Engineering Research Institute, Jiangsu University, Zhenjiang, China. He received his Ph.D. degree in vehicle engineering from Jiangsu University, China. His research interests include automotive electronic control technology, road traffic active safety prevention and control, and security and communication in VANET, etc.
E-mail: masd@ujs.edu.cn

Ailan Wan is pursuing a master's degree candidate. at the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China. Her research direction is information security of intelligent network vehicles, cryptography, and security of electronic control units in vehicular networks.
E-mail: sweetlan@ujs.edu.cn

Shuai Liu is pursuing a master's degree candidate. at the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China. His research direction is lightweight cryptography and side channel attack.
E-mail: 2211608026@stmail.ujs.edu.cn