McEliece cryptosystem based identification and signature scheme using chained BCH codes

Le Van Thai
Faculty of Electronics Engineering
Ha Noi University of Industry
Ha Noi, Viet Nam
Email:thailv@haui.edu.vn

Pham Khac Hoan
Faculty of Radio Electronics
Le Quy Don University
Ha Noi, Viet Nam
Email: hoanpk2012@gmail.com

***Abstract* – Identity-based Public Key Cryptography ID-PKC allows to manage authentication of pubic key efficiently. Identification and signature scheme allow managing public key without digital authentication. This paper proposed McEliece cryptosystem based identification and the signature scheme using chained BCH codes and permuted decoding based on the norm of syndrome. The proposed signature scheme allows to use codes with short length and distance yet increasing the numbers of correctable errors and coding speed, to reduce the complexity of making signature procedures and verification as well as to construct a secured identification and signature scheme.**

Keywords* – *Code based cryptosystem, digital signature scheme, Stern identification scheme, BCH codes.

I. INTRODUCTION

Digital Signature is used in reality to authenticate and do non-repudiation of messages [1,2]. In fact, digital signature schemes were widely used in many fields but most of the schemes based on difficult problems such as prime factor analysis, finite discrete logarithm or elliptic curve. In 1997, Shor [3] published the integer factorization algorithm and calculation of discrete logarithm running in polynomial time on the quantum computer. Therefore, Union of Scientist related to codes researched mathematical problems that can defeat quantum algorithm. A Code-based cryptosystem is one of potential research trends for post-quantum cryptography due to its computational complexity of syndrome decoding solution for NP-complete error-correction codes that reported by Berlekamp, McEliece and Van Tilborg [4].

McEliece proposed the first algebraic coding-based public key cryptography in 1978 [5]. Variant of McEliece cryptosystem is Niederreiter cryptosystem [6] was introduced in 1986. However, McEliece or Niederreiter cryptosystem or any other ones based on error-correction code is impossible to sign the arbitrary document because a random syndrome has error vector that has larger weight than code's error correcting capacity. In 2001, Courtois, Finiasz and Sendrier firstly proposed the digital signature scheme using Niederreiter cryptosystem (CFS-scheme). However, signing procedure requires a large number of repeat steps with an average of $t!$ times [7].

Another approach to solving the above problem is to construct a structure of the code and decoding algorithm to achieve a reasonable ratio between the number of decodable syndromes and the total number of available syndromes. Fundamental solution to solve this requirements is using chained BCH code (and its variants) in which each code has code distance not large with the increasing of error correctable capability owing to permuted decoding based norm of syndrome, that is a new parameter based on structure of BCH codes [8].

Identity-based Public Key Cryptography ID-PKC allows to efficiently manage authentication of the public key. Each user has his own *id* (Identity) and from that receive a public key, so it is not necessary to authenticate the public key certificate. However, it is more complicated to create private key and needs a trusted third party to create a private key for each user from his *id*.

Recently, there is some digital identification and signature scheme based on error-correcting codes. Stern identification scheme based on syndrome decoding problem while Veron identification scheme based on finding smallest weight codewords. By using efficiently Fiat-Shamir paradigm, it can transfer these schemes to the digital signature scheme. And by using identification and signature scheme that allow simplifying key management procedure through a key generating center (KGC) instead of a digital authentication procedure. Recently, Cayrel et.al, build an identification and signature scheme based on CFS digital signature and Stern protocol [9,10,11]. These schemes determined the security against attacks of an information set decoding (ISD) and structural attacks. However, these schemes yet have the fundamental disadvantage of CFS signature scheme that is signing procedure repeated about $t!$ times and need large key size. In this paper, we construct a secured identification scheme that does not requires repeated signing that based on the provided key from the *id* of the user, using chained BCH code, reduce the key size, complexity of signing and identifying progress and to increase processing speed.

The remaining of the paper are organized as follows: Section 2 reports McEliece cryptosystem and CFS signature scheme. In Section 3 a norm of syndrome-based permutation decoding method for BCH code is proposed. Section 4 proposes a method to construct the identification and signature scheme using chained BCH code is proposed. In Section 5, an analysis and evaluation of quality and security of proposed identification and signature scheme is presented.

978-1-4673-6547-5/15/$31.00 ©2015 IEEE

II. THE MCELIECE CRYPTOSYSTEM AND CFS SIGNATURE SCHEME

A. The McEliece cryptosystem

McEliece cryptosystem includes three algorithms: generating a public and secret key; coding and decoding algorithm. Diagram of McEliece cryptosystem is depicted in Fig.1 [5].

Key generation:

- Choose a Goppa code C that can correct t errors with generator matrix G', the size of $k \times n$.
- Choose a random invertible binary-matrix S, the size of $k \times k$.
- Choose a random permutation matrix P, the size of $n \times n$.
- Calculate matrix $G = S.G'.P$, the size of $k \times n$.
- Public key is (G, t) and the secret key is (S, G', P).

Message encryption:

- Send a message m with the public key (G, t) to the receiver, encode message m as a binary chain with the length of k.
- Generate a random vector e with the length of n and its weight is not larger than t (The number of bit with value "1" $\leq t$).
- Calculate codeword $c = mG + e$ and send it to the receiver.

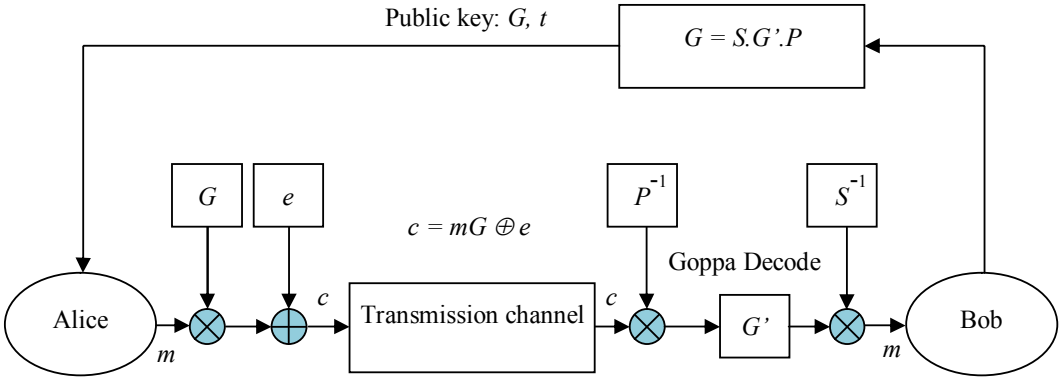

Fig. 1. The McEliece cryptosystem

Message decryption:

Upon receipt of the codeword c, the receiver decodes message:

- Calculate P^{-1} that is invertible matrix of P.
- Calculate $cP^{-1} = (mS)G + eP^{-1}$.
- Decode cP^{-1} to mSG'.
- Calculate $m=(mS)S^{-1}$.

Because $cP^{-1} = mGP^{-1} + eP^{-1} = mSG' + ezP^{-1}$ and P are the permutation matrixes so eP^{-1} has the largest weight t. Goppa code C can correct t errors and codeword mSG' can also correct t errors owing to Peterson algorithm or other algorithms. Thus, message $m' = mS$ can be calculated. In order to recover to the original message from the transmitter, multiplying m' with the invertible matrix of S then we have $m = m'S^{-1} = mSS^{-1}$, that is the original message.

B. Digital signature scheme CFS

Niederreiter cryptography is a variant of McEliece cryptosystem. Niederreiter cryptography uses the check matrix H instead of generator matrix G used in the original McEliece cryptosystem. CFS signature scheme based on Niederreiter cryptosystem using the complete decoding method to decode out of code distance limit by finding the most closed codeword from the code pool. To decode a syndrome that corresponds to an error having weight of $t + \delta$, it can add random δ colums of the check matrix with syndrome and decode the newly created syndrome. If all of δ columns correspond to several error positions that mean the new syndrome can be mapped to a codeword having weight of t and it is decodable. If decoding is impossible, it should re-try with other δ columns until the syndrome is decoded. δ is chosen to satisfy that number of error types is larger than total numbers of available syndromes. If δ is large enough then it is possible to decode any syndrome corresponds to an error having the weight that is smaller or equal to $t + \delta$. Signing algorithm must repeat the decoding process until decoding is done, this means it is a slow signing algorithm. Another solution is to take a random syndrome (by using a hash function) and try to decode it, if decoding is impossible then mixing the message and hash it again. Repeat this process until it is decodable [7].

III. NORM OF SYNDROME-BASED PERMUTED DECODING TO ENHANCE ERROR CORRECTABLE CAPACITY OF BCH CODES

A check matrix of BCH-code with structural distance $\delta = 2t + 1$ defined by:

$$H = \left[\beta^{bi}, \quad \beta^{(b+1)i}, \quad .... \quad \beta^{(b+2t-1)i}\right]^T, \quad 0 \leq i \leq n-1. \qquad (1)$$

Thus, syndrome of arbitrary error vector consists of δ-1 elements of fields $GF(2^m)$ formed by $s(e) = (s_1, s_2, ..., s_{\delta-1})$.

Symbol σ is cyclic-shift permutation and under its impact error vector $e = (e_1, e_2, ..., e_n)$ is one-position right-shift to $\sigma(e) = (e_n, e_1, e_2, e_3, ..., e_{n-1})$. Set of all different biunique

vectors $\sigma^{\lambda}(e)$ with $0 \le \lambda \le n-1$ of arbitrary error vector e is called σ-orbit. Elements of *σ-orbit* are replaced by each other through cyclic-shift permutation. Each *σ-orbit* has a generator vector and the first coordinate of this vector is non-zero.

Let e be an arbitrary error vector, and binary BCH-code having check matrix (1), we have:

$$s(\sigma(e)) = (\beta^{b} s_1, \beta^{b+1} s_2, ..., \beta^{b+\delta-2} s_{\delta-1}). \quad (2)$$

Let norm of syndrome be vector $N(S)$ having $C_{\delta-1}^{2}$ at coordinates N_{ij}, $1 \le i < j \le \delta-1$ expressed by:

$$\begin{aligned} N_{ij} &= s_j^{(b+i-1)/h_{ij}} / s_i^{(b+j-1)/h_{ij}} \\ &\quad khi \quad s_i \neq 0, h_{ij} = GCD(b+i-1, b+j-1); \\ N_{ij} &= \infty \quad khi \quad s_j \neq 0; s_i = 0; \\ N_{ij} &= - \quad khi \quad s_i = s_j = 0. \end{aligned} \quad (3)$$

For example, for binary BCH-code with $d = 5$ (C_5), norm of syndrome is given by:

$$N = s_2 / s_1^3. \quad (4)$$

The basic property of norm of syndrome is invariance to cyclic-shift permutation. From Eq.(2), for all error vector e satisfy the following equation:

$$N(s(\sigma(e))) = N(s(e)) \quad (5)$$

The nature of norm-syndrome-based decoding method is: Elements of σ-orbit are replaced by each other through cyclic-shift permutation. Norm indicates σ-orbit in which the error vector exists, determines the corresponding generator vector e_0 and then comparing the received syndrome S and $S(e_0)$ to determine the number of cyclic-shifts to transform e_0 to e, therefore it will find the exact error vector [8].

A special point of the norm-syndrome method is when partitioning error vectors into non-overlap classes having distinct norm-syndrome that can enhance the capability of BCH-code error correction [12]. Note that BCH code with $d = 5$ (C_5) norm of syndrome has $n + 2$ distinct values that corresponds with $n(n+2)$ non-zero error vector meanwhile the primitive BCH code C_5 has $2^{2m} = (n+1)^2$ different syndrome values.

The primitive BCH-code C_5 over the field $GF(2^5)$ with generator polynomial $x^5 + x^2 + 1$ beside 16 classes of error with a weight of 1,2 (16 *σ-orbit)* can correct error classes with a weight of 3 with generator vector formed $e_{1,2,3}$, $e_{1,2,8}$, $e_{1,2,10}$, $e_{1,3,5}$, $e_{1,3,6}$, $e_{1,3,7}$, $e_{1,3,10}$, $e_{1,4,6}$, $e_{1,4,7}$, $e_{1,4,8}$, $e_{1,4,9}$, $e_{1,4,10}$, $e_{1,5,6}$, $e_{1,5,14}$, $e_{1,8,10}$, $e_{1,11,12}$ (16 σ-orbit) because their norms are biunique different. This means with all non-zero syndromes, it can find only one error vector with smallest weight that is also burst error with shortest length.

Given the reciprocal code C_5 has check matrix $H = \left[H_1 | H_2\right] = \left[\alpha^{z}, \alpha^{-z}\right]^{T}$, syndrome $S = (s_1, s_2) = (\alpha^{i}, \alpha^{j})$, norm of syndrome is formed by:

$$N = s_1.s_2. \quad (6)$$

If consider *σ-orbit* partition, norm corresponds to random errors with a weight of 1, 2 and some types of error with a weight of 3 not same. For example, reciprocal code has a length of 31, d=5, with primitive elements α is root of polynomial $x^5 + x^2 + 1$, corrects not only error classes with a weight of 1,2 (16 *σ-orbit*) but also error class with a weight of 3 with error positions that satisfy $i_2 - i_1 = i_3 - i_2 = 1, 2, 4, 8$ (with generator vector $e_{1,2,3}$, $e_{1,3,5}$, $e_{1,5,9}$, $e_{1,9,17}$) and other error classes with generator vector formed with $e_{1,2,6}$, $e_{1,2,9}$, $e_{1,2,11}$, $e_{1,2,14}$, $e_{1,3,6}$, $e_{1,3,9}$, $e_{1,3,11}$, $e_{1,4,5}$, $e_{1,4,6}$, $e_{1,4,12}$, $e_{1,6,11}$, $e_{1,6,13}$, $e_{1,5,16}$ (15 σ-orbit). Note that two error classes with generator vector $e_{1,3,6}$, $e_{1,4,6}$ has $N=0$ but $s_1 = 0$, $s_2 = 0$. Thus all non-zero-value syndromes have appropriate error vectors. Other notice is that with dual generator polynomials, BCH-codes will have the same characteristics.

In [12] investigates the capability of error correction of the extended reciprocal code. Assuming that sort columns of H_1 in the other order and replace the corresponding columns of H_2 with them. The i^{th} column of H_1 shows m bit of the integer number $i-1$, $1 \le i \le n = 2^m$ and with the odd-m it will get the code $\tilde{C}$ having check matrix $\tilde{H} = (\tilde{H}_1, \tilde{H}_2, I)^{T}$, with code distance $d = 6$. The reciprocal code $\tilde{C}$ allows to correct simultaneously random error with a weight of 1 and 2, error modules with length of 4 in degree of 3, and even error modules with length of 4 in degree of 4 if selecting the appropriate generator polynomial.

In a general case, it can enhance error correction capacity of codes if code structure is constructed properly. BCH code C_5 and enhanced BCH code, reciprocal code and its enhance with the appropriate generator polynomial allows correcting both errors of degree 1,2 and all burst error of degree 4 and majority error with degree of 3. For BCH code C_7 and its enhance, they can correct not only errors with degree smaller than 3 but also most of burst errors with the length of 4, 5, and more than 90% of the burst error with length of 6, 7 and more than 80% of burst error with length of 8, 9, 10 [12]. Thus owing to norm-syndrome method, it can implement the digital signature scheme that overcomes basic disadvantages of McEliece and Neidereiter cryptography-based digital signature.

IV. CONSTRUCTION OF DIGITAL SIGNATURE SCHEME AND IDENTIFICATION USING CHAINED BCH CODE BASED ON NORM-SYNDROME DECODING METHOD

A. Digital signature scheme using chained BCH code (BCHS)

In order to construct chained error-correction code-based digital signature system, it needs to use a family of linear code with given parameters that have good decoding characteristics. Each code of this family must have decoding algorithm at the complexity degree of polynomial. Let Γ be the family of linear codes. A code $C_i \in \Gamma$ is defined by length of n_i, number of information bits k_i and correction capacity t_i. This code family must be sufficient large in order to against overall attacks and each code C_i of a family is computed from check matrix H_i. The system constructed from chained code is called chained check matrix that has the following forms (assumption with l codes):

$$\begin{bmatrix} H_1 & ... & ... \\ ... & H_i & ... \\ ... & ... & H_l \end{bmatrix}$$

Assume use the binary BCH code and variants of BCH code (reciprocal codes, extended BCH code) to be element

codes. The norm of syndrome value and generator vector are put in tables. In order to decode one codeword, calculate its syndrome and norm, from the norm we can find generator vector, and from the degree of syndrome element s_i number of cyclic shifts will be found [12].

1) Parameters of digital signature

a) Secret key:

- Each family l of BCH code C_5 and reciprocal codes C_5 , BCH code C_7 (d = 5,7) and enhanced BCH codes (d = *6,8*), the check matrix of each code is sorted in principal diagonal to create check matrix H of chained code:

$$H\left[(N-K)\times N\right]=\begin{bmatrix} H_1 & L & L \\ L & H_i & L \\ L & L & H_l \end{bmatrix} \quad (6)$$

- A permutation matrix $P[N\times N]$ in the field of $GF(2)$

- An invertible matrix $S[(N-K)\times(N-K)]$ in the field of $GF(2)$.

b) Public key:

- Public key using to check the signature is public matrix H' that is calculated from private (secret) elements $\{S,H,P\}$. This is check matrix of code appropriated with chained BCH code.

- The output of hash function has length of N-K bits.

2) Signing and verification algorithm

a) Signing a document:

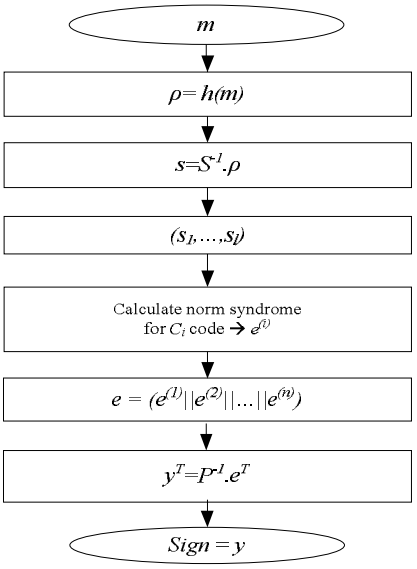

Fig. 2. Signature generation algorithm

- Signed document m is given in the form of binary;

- Calculate hash value: $\rho = h(m)$;

- Calculate syndrome and divide into syndrome of each code: $s = s^{(1)}...s^{(i)}...s^{(l)} = S^{-1}.\rho$;

- Calculate norm of syndrome for each element code, decode element codes by permuted method based-on norm of syndrome;

- Unify decoded error vectors $e = e^{(1)}...e^{(i)}...e^{(l)}$;

- Calculate $y^T = P^{-1}.e^T$;

- Signature has form of y.

The above algorithm is despited in Fig 2.

b) Signature verification:

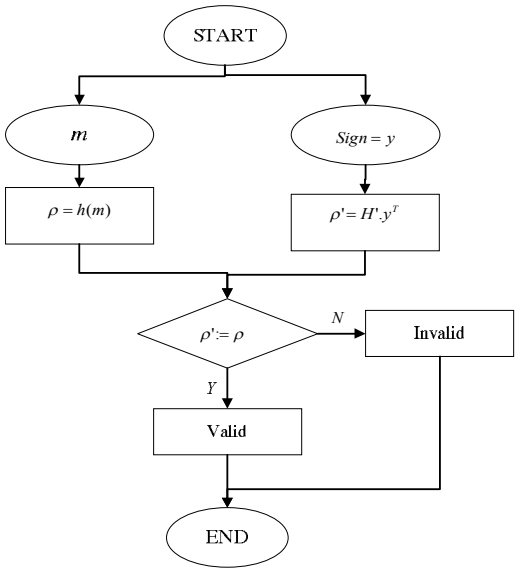

Fig. 3. Signature veryfication algorithm

In verifying procedures, we have document m, signature y:

- Calculate: $\rho = h(m)$;

- Calculate: $\rho' = H'.y^T = S.H.P.P^{-1}.e^T = S.H.e^T = S.s.$

- Signature verification: the signature is valid if $\rho = \rho'$.

Diagram of signature verifying í shown in Fig 3.

B. Identification scheme based on chained BCH code.

Stern identification scheme:

Given the check matrix H with size of n - k × n in the field $GF(2)$ and hash function h. Each user has a private key x with the length of n bit and the weight of w. The public key s is calculated from syndrome of x: $s = H.x^T$. This value is calculated one time during the survival time of H. Assume that Pr (prover) want to prove to V (verifier) that he is matched with the s public key. Stern protocol is described as follows [9,11]:

1) Pr choose randomly a word y with the length of n and a permutation π in {1, 2, …, n}. Then Pr send to V commitments c_1, c_2, c_3 that satisfy the following: $c_1 = h(\pi \| Hy^T)$; $c_2 = h(\pi(y))$; $c_3 = h(\pi(y+x))$.

2) V send back to Pr a message b in {0, 1, 2}.

3) Pr receives b with three situations happened:

- If $b = 0$: Pr corresponds to y and π;
- If b =1: Pr corresponds to $y+x$ and π;
- If b = 2: Pr corresponds to $\pi(y)$ and $\pi(x)$.

4) Verifying happens on three situations:

- If b = 0: V verifies that c_1, c_2 was right calculation;

- If $b = 1$: V verifies that c_1, c_3 was right calculation, but note that: $Hy^T = H(y+x)^T + s$;

- If $b = 2$: V verifies that c_2, c_3 was rigth calculation and the weight of $\pi(x)$ equals to w.

5) Repeat the above steps until security levels guaranteed.

The above protocol has two main disadvantages that are large size of the public key and need large repetition cycles. For example: to guarantee the authentication probabilities to be 2^{-16}, 2^{-32} it needs 28, 56 repetition cycles, respectively.

Identification scheme based on chained BCH code.

Assume that the identification number of *Pr* is *id*, find *y* so that $h(id) = s = H'.y^T$. This means it needs decode *h(id)* by using the above mentioned norm of syndrome method. Identification-based scheme *IBS = (MKg, UKg, Pr, V)* include 4 following algorithms:

- Master key generating algorithm *MKg*: using key creation algorithm like BCHS'signature as mentioned above to creat key-couple to sign and verify, setup the Master public key *mpk = H'* and Master secret key *msk = {S, H, P}*.

- User private key generating algorithm *UKg*: Input of master secret key *msk* and identification *id* to find out secret key *SK[ID]* ← *UKg(msk, id)*. Here, using signature algorithm BCHS to create signature *y* satisfies $h(id) = s = H'.y^T$. Setup secret key of user *SK(id) = y*.

- Interactive algorithms *Pr*, *V*: using Stern identification scheme with the algorithm *Pr* initiated by *SK(id) = y*, using the same check matrix of chained BCH code and algorithm *V* initiated by *mpk, id*.

V. EVALUATION OF COMPLEXITY AND SECURITY

The proposed scheme consists of two parts: the first part using syndrome decoding method to determine the private key of user (prover) and the second one based on Stern identification scheme with the same check matrix. Steps of implementing Stern identification protocol includes 4 main procedures: Multiply of vectors-random matrix; hash function; permutation (create and perform random permutation); vector creation and random permutation. Parameters of identification scheme guarantee the security is same as the security of BCHS signature scheme because security of Stern scheme with the same parameter is pooled digital signature scheme.

A. Complexity of signature and verification

1) Complexity of signature:

Complexity of signature mainly depends on decoding algorithm for chained BCH-code. Decoding operation is implemented in each element code. In order to simply the evaluation, assume that element codes have the same parameter *(n, k)*. Assume each couple of original BCH and reciprocal code use the similar generator polynomial of field $GF(2^m)$. In order to build a mapping table between norm of syndrome and generator vector (maximum diameter is $D=(n+1/2)$, it requires $0(n^2)$ calculations of norm of syndrome. Calculation of norm of syndrome equals to use the memory of $m.2^m$ size. Thus, decoding l element codes need degree of complexity of $0(N^2(\log_2 N)^2$. The remained calculations are multiplication of binary matrix with degree of complexity of $N^2/2$ and $(N-K)^2/2$ of binary operations. Therefore, the degree of complexity is: $0(N^2(\log_2 N)^2) + N^2/2 + (N-K)^2/2$.

2) Complexity of signature verification:

It is defined by complexity of syndrome decision from error vector. Its implementation is matrix multiplication $N \times (N - K)$ with N length of vector, and it requires $N.(N - K)/2$ binary calculations.

Especially, linear mathematics (scalar multiplication or bit permutation) easily perform the operations on the hardware, and can protect against the Differential Power Analysis - DPA attacks very efficiently.

B. Security:

There are two types of attack digital signature scheme based on McEliece cryptosystem, they are:

1) Decoding attack.

Assume H is a binary matrix with degree of $(N-K)\times N$, s is binary vector with size of $N - K$ and an integer p. Question: does exist an vector x, size of N and its weight is not over p that satisfy: $H.x^T = s$.

Efficient algorithm for this case is to use Information Set Decoding (ISD) based on the algorithm of Canteaut and Chabaud. Work factor (*WF*) of ISD attack based on finding codewords that have smallest weight about $W \approx 2^{ncH(R+R_0)+d}$, with $c = 0{,}12$; $d = 10$, $R_0 = 3{,}125.10^{-2}$ and $H(R)$ is entropy of discrete binary sources having appearence probability of bit 1 equals to code rate R [13]. In fact, decoding attack in the case of using decoding out of code distance has more complicated process.

2) Structural attack.

Complexity of structure attacks to public keys in the proposed digital signature can estimate by finding all possible sets of permutation matrix $P(N!)$, secret code and invertible matrix $S\left(0.29\times 2^{(N-K)}\right)$.

Assume that attacks can detect H and S, so matrix P will be found. After that with each secret key it has to check until to find a valid key. For the proposed scheme, complexity of structure attacks increases due to the safety of code series that determined by BCH codes, extended BCH code, reciprocal codes with different lengths and various generator polynomials. It also applies permutation with element BCH-codes to increase their amounts.

In order to illustrate, system parameters is chosen as follow: Hash function uses SHA, length of hash value is 160 bits, element codes include: one BCH code C_5 (31, 21), one code C_6(32,21) and extended reciprocal code $\tilde{C}$(32, 21); three codes C_7 (31, 16); two codes C_7 (63, 45) in the field of $GF(2^6)$; two codes C_7 (127, 106); each of the above codes allows extend the capability to correct one bit more. Thus, total number of check bits are 160, the entire coding length is $N = 56$. Coding rate $R = 0.72$. Number of errors can be corrected is $t_\Sigma = 38$ at maximum. The length of signature is $N = 568$ bits, syndrome length is 160 bits. With ISD attack using Canteaut and Chabaud method, numbers of main calculations are $2^{65,3}$

[13]. However, in order to implement this attack, it is more complecated because decoding work is out of correction ability, meanwhile attack methods are assumed the decoding works is in the code distance. When implementing ISD attack with Gaussian elimination such as Canteaut and Chabbane [14], with the code *(N, K, t)*, choose a random set with *K* columns, error probalility is determined as follows:

$$P_{dec} = \frac{C_{N-K}^{t}}{C_{N}^{t}}. \quad (7)$$

Work factor (*WF*) to find out codeword with a weight *t* equals to:

$$WF = \frac{P(K)}{P_{dec}} \quad (8)$$

Where: *P(K)* is complexity degree of Gaussian elimination, and it is about K^3.

With the chosen parameters, the security level of digital signature scheme achieves $2^{96,7}$.

In order to implement structural attack in the most convenient situation is when determine the parameters n_i, k_i of each element code, from that determine the use of these element codes. Assume to change parameter *b* to hide matrix of element BCH code (with structural distance d = 5, 7), to public generator polynomials in the field of $GF(2^m)$, m = 5, 6, 7. Furthermore, it also uses variants such as extended BCH code, reciprocal codes and its extensions so the number of selectable codes increases suddenly. On the otherhand, there are corresponding 6; 6; 14 premitive polynomials with degree of 5, 6, 7. Codes are sorted in the random orders. Therfore, number of different element codes are 10668 codes, complexity degree that determines structure of 10 element codes is about $(6.2^5)^6.(6.2^6)^6.(14.2^7)^6.6.6.14 \approx 2^{170}$.

BCHS signature compares to Niederreiter cryptosystem-based signature that has the following characteristics:

+ Signing algorithm faster than 32,000 times.
+ Size of public key smaller than 90 times.
+ Length of signature longer than 4.3 times.
+ Security sudden increase due to difficult attack with the regular algorithm.

TABLE I. COMPARISION BETWEEN BCHS AND NIEDERREITER CRYPTOGRAPHY-BASED SIGNATURE - CFS

Signature	Niederreiter	BCHS
Singnature length	132	568
Key size	2^{23}	$2^{16,5}$
Complexity of signature	2^{33*}	2^{18**}
Decoding attack ISD	2^{80}	$2^{96,7}$
Structural attack	2^{119}	2^{170}

*: Document hashed 38! times.
**: Document hashed only 1 times.

VI. CONCLUSION

Norm of syndrome-based permuted decoding method allows enhancing error correction capacity of code and increasing the ratio of decodable syndromes to approximate 1. Digital signature scheme using chained BCH code is proposed that permits reducing size of key 90 times, shortening signing time 32,000 times compared with CFS signature scheme and allow increasing security much more times because of difficulty of decoding and structural attacks with the above schemes when using chained BCH code with decoding method that is out of error correction ability. Signing and verifying algorithm has reduced complexity through reducing the length and distance of element codes and using norm-syndrome-based decoding method. However, this scheme requires should have fairly large memory capacity to store the set of norm values of different generator polynomials. This task is performed on large servers at the center key generator so there is not too difficult problems and can be performed. Combination of signature scheme and identification allows simplifying the authentication of the public key. With the above advantages, it allows implementing signature scheme easily and identifying on devices having constrained resources as smartcard.

References

[1] D.R Stinson. Cryptography, Theory and Practice, CRC Press 1995.

[2] WENBO MAO. "Modern Cryptography: Theory and Practice", Prentice Hall PTR, 2003, p. 648.

[3] P.W.Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26:1484–1509, 1997.

[4] E. Berlekamp, R. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory, 24(3):384–386, 1978.

[5] McEliece, R.J (1978). A Public-Key Cryptosystem Based on Algebraic Coding Theory, The Deep Space Network Progress Report, DSN PR 42–44, pp. 114-116.

[6] H. Niederreiter (1986). Knapsack-type Cryptosystems and Algebraic Coding Theory, Problems of Control and Information Theory, 15(2):159-166.

[7] N. Courtois, M. Finiasz, N. Sendrier. How to acheive a McEliece based digital signature scheme. Rapport de recherche INRIA N° 4118, ISSN 0249-6399, Fevirier 2001.

[8] В.А. Липницкий, В.К. Конопелько (2007). Норменное декодирование помехоустойчивых кодов и алгебраические уравнения, Минск, Изд. центр БГУ, 2007.

[9] P.L.Cayrel, S. M. Alaoui. Dual construction of Stern-based signature scheme, World Academy of science, egineering and technology, Vol. 4, No. 3, 2010.

[10] P.L.Cayrel, P.Gaborit and M. Giraul. Identity-based identification and signature schemes using correcting codes, International Workshop on Coding and Cryptography, WCC 2007, pp 69-78.

[11] Sidi Mohamed El Yousfi Alaoui, Pierre-Louis Cayrel, and Meziani Mohammed. Improved identity-based identification and signature schemes using Quasi-Dyadic Goppa codes. International Journal of Advanced Science and Technology, Vol.35,October, 2011.

[12] P.K. Hoan, L.V Thai, V.S Ha. Simultaneous correction of random and burst errors using norm of syndrome for BCH codes, National Conference on Electronics and Communications, REV2013-KC01, pp 154-158, 2013.

[13] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. IEEE Transactions on Information Theory, vol.44(1), pp 367-378, 1998.

[14] Canteaut and H. Chabbane. A further improvement of the workfactor in an attempt at breaking Mceliece's cryptosystem, Proceeding of Eurocode'94, Inria, pp. 163-167.