International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 7 Issue: 3 25 - 28

A Novel Digital Signature based on Error Correcting Codes

Younes Bayane, Fatima Amounas and Lahcen El Bermi
Computer Sciences Department,
Moulay Ismaïl University, Faculty of Sciences and Technics,
Errachidia, Morocco
Bayane.younes@gmail.com, f_amounas@yahoo.fr, elbermi.lahcen@gmail.com

Abstract— A digital signature is a cryptographic primitive for ensuring the authenticity of digital documents. A valid digital signature allows checking that a message was created by a known sender (authentication), that the sender cannot deny having sent the message (nonrepudiation), and that the message was not altered in transit (integrity).The idea of constructing practical signatures based on error correcting codes was introduced by Courtois et al in [1]. The main goal is to make digital signature for which the security is based on decoding syndrome problem.
In this paper, a new construction of digital signature is considered which is an extension of the error correcting code construction. The proposed method consists of reordering the message bits to get a decodable word. Then apply an efficient decoding algorithm to get signature.

Keywords- *Cryptography , Error correcting code, McEliece Cryptosystem, Niederreiter Cryptosystem, syndrome decoding problem, Digital signature,CFS signature.*

*****

I. INTRODUCTION

Arguably today's asymmetric cryptographic algorithms are all based on the hardness of the integer factorization problem and the discrete logarithm problem. Up to now, no efficient algorithms for solving these problems are known using today's computers. However, this picture changes drastically if quantum computers are considered. In 1994, Shor proposed in [2] a quantum algorithm that can solve both the integer factorization problem and the discrete logarithm problem in polynomial time on a quantum computer. In order to find an alternative to the threatened schemes, the Post Quantum Cryptography emerged recently and has received increased attention in the last years, especially after 2016 when the NIST began to standardize it. Nowadays, there are many categories of problems that are studied for post quantum cryptography. One of those problems that are considered well-understood is the cryptography based on error correcting codes. Since devise of the first cryptosystem based on error correcting codes in 1978 by McEliece and its dual variant in 1986 by Niederreiter, many cryptographic primitives have been implemented based on the same ideas, especially after both cryptosystems have shown a high level of security in [3]. Thus, in 1990, Xinmei Wang proposed the first code-based signature scheme based on error correcting codes in [4]. The signature is generated in the same way as the plaintext is encrypted in the Rao-Nam scheme in [5]. Unfortunately, it was proved unsecure shortly after in [6]. Several signature constructions based on Goppa Code Distinguishing problem were subsequently designed, this is outlined below.

II. BACKGROUND

In 2001, Courtois, Finiasz and Sendrier published the first practical digital signature based on error correcting codes theory. They adopted the idea of the Niederreiter cryptosystem for this purpose. This means that having a linear code with an efficient decoding algorithm whose parity check matrix H is a m*n matrix, there is a way to find for any binary vector s of length r called a syndrome, a word of smallest Hamming weight x of length n such that $Hx^T = s^T$. To sign a message, one has to use a hash function h to produce a binary string of length r. The decoding algorithm of the parity check matrix H is then applied to get a word x of smallest Hamming weight such that $Hx^T = h(m)^T$. The signature of the message m is then the word x. According to the authors, the signature can be made using Goppa codes of a high rate. They also proved the security of their scheme relying on two problems assumed to be hard, namely: the syndrome decoding problem and the distinguishability of a binary Goppa code from a random code. In 2009, it was realized that the original parameters can be attacked by considered attack of Daniel Bleichenbacher never published. Subsequently, another variation called Parallel-CFS was presented in [7], which avoids the attack of Bleichenbacher. The new scheme has the same advantages as the original CFS, but it suffers from two drawbacks, namely: (i) it has no consistent proof from point of view of distinguishability, taking in consideration the distinguisher of high Goppa codes presented in [8] and (ii) need of large keys to get a good security parameters with a reasonable signature cost.Other schemes were proposed. So Kabatianskii, Krouk, and Smeets presented in [9] and [10] the KKS signature scheme based on arbitrary linear error-correcting codes. Actually, they proposed three versions which share the same principle: The signature is a code word of a linear code; but use different linear codes. There are also some attempts to change the original strategy by using other code families. So in [11] Low Density Generator Matrix codes (LDGM) were adopted. Low Rank Parity Check codes (LRPC) were used in [12]. Convolutional codes in [13] and more recently quasi-cyclic codes in [14]. Due to attack described in [15] on the McEliece Cryptosystem based on convolutional codes, there are some doubts about the consistency of the scheme described in [13], but up to now, there is no consistent proof.

The remainder of this paper is organized as follows. Section II makes a survey of the Niederreiter cryptosystem, an overview of the CFS signature is presented in section III, which is followed by the introduction of our solution in section IV. We describe it, and then demonstrate its correctness and its unforgeability.

III. NIEDERREITER CRYPTOSYSTEM

In 1978, McEliece proposed the first public key cryptosystem based on coding theory in [16], called McEliece cryptosystem. It is based on Goppa codes and uses a generator matrix for encryption.In 1986, Niederreiter proposed a dual variant of McEliece cryptosystem in [17] that uses parity check matrix for encryption, known as the Niederreiter cryptosystem. Furthermore, he suggests using Reed-Solomon codes proved later to be insecure in [18]. However, it has been shown in [19] that by using Goppa codes with appropriate parameters, the Niederreiter cryptosystem is equivalent to McEliece in term of security.

The following algorithm describes the steps of the scheme applied over a Galois field:

A. *Key Generation:*

Choose an (n, k)-code C over a Galois field Fq having an (n — k) × n parity check matrix H and an efficient decoding algorithm γ.

- Choose randomly an (n — k) × (n — k) nonsingular matrix Q over F_q.
- Choose randomly an n × n permutation matrix P over F_q.
- The private key is: (H, P, Q, γ).
- The public key is: $\hat{H} = QHP$.

B. *Encryption:*

To encrypt a message m ∈ F_{nq} of weight t:

- Compute the syndrome $c = \hat{H}m^T$.
- The cipher is: c.

C. *Decryption:*

To decrypt a cipher c ∈ F_{n-k}

- Compute $Q^{-1}c$ to get HPmT witch correspond to a syndrome.
- Apply the algorithm γ to get Pm^T.
- Apply P^{-1} to Pm^T to get m.

IV. CFS SIGNATURE

In 2001, Courtois, finiasz and Sendrier published in [1-1] the first practical digital signature based on error correcting codes known as CFS signature. To produce a signature, the signer has to hash the document to sign into a cipher, then decrypt it using a secret key. To check the signature, the receiver has to compare the hash of the document with the encryption of the signature using the public key associated to the signer private key.

The following algorithm describes the signature scheme, in more details:

A. *Key Generation:*

- Choose an (n, k)-binary code C over a Galois field F_q having an (n — k) × n parity check matrix H and an efficient decoding algorithm γ.
- Choose randomly an (n — k) × (n — k) nonsingular matrix Q over F_q.
- Choose randomly an n × n permutation matrix P over F_q.

B. *Signature*

To sign a message m:

Do

$i \leftarrow i + 1$

$X \leftarrow \gamma(Q^{-1}h(h(m)||i))$

While no X found;

The signature is: (i, XP).

C. *Checking signature validity*

- Compute $s_1 = HXT$ and $s_2 = h(h(m)||i)$.
- The signature is valid if $s_1 = s_2$.

V. PROPOSED SCHEME

A. *Phases of the scheme*

Our scheme is a variant of the CFS signature. It implements the operations performed in Niederreiter cryptosystem in reverse: the decoding operation in order to get a signature, then the encoding operation to check the validity of the signature.

It contains roughly the following phases:

- Key generation
- Message signing
- Signature checking

The following table presents notifications used in the rest of the document to describe the scheme:

Table I. Notifications

m	Binary string
h()	Hash function
C	Goppa code
Q	Nonsingular matrix
H	Parity check matrix of the code C
P	Secret permutation matrix
$\hat{H}$	Public key matrix
σ	Signature
W(x)	Hamming weight of the word x

P'	Permutation matrix
γ	Efficient decoding algorithm for the code C

The proposed scheme can be described as follows:

1) Key generation phase

Alice randomly chooses a triple (Q, H, P) as her secret key. Q is a (n — k) × (n — k) nonsingular matrix, P an n × n permutation matrix and H an (n— k) × n parity check matrix having an efficient decoding algorithm γ. She then computes the public key:

$$\hat{H} = QHP. \quad (1)$$

2) Signing phase

To sign a message m, Alice follows theses steps:

a) Hash the massage m:

$$s = h(m). \quad (2)$$

b) Select a random word y such that y is decodable and

$$W(y) = W(Q^{-1}s). \quad (3)$$

c) Generate the permutation matrix P', such that

$$y = Q^{-1}s\,P'. \quad (4)$$

d) Compute

$$x = \gamma(y), \quad (5)$$

and Put

$$X = xP. \quad (6)$$

e) Send (m, σ), such that

$$\sigma = (X, P'). \quad (7)$$

3) Checking Phase

To check if signature is valid, Bob follows these steps:

a) Compute

$$s_1 = \hat{H}X^{T}P'^{,T}. \quad (8)$$

b) Compute

$$s_2 = h(m). \quad (9)$$

c) The signature is valid if

$$s_1 = s_2. \quad (10)$$

B. *Demonstration of correctness*

The correctness of the signature is justified by the following equations:

Having

$$x = \gamma(y),$$

that means that:

$$y = Hx^{T} = HP(xP)^{T} = HPX^{T}.$$

We have also

$$y = Q^{-1}h(m)P',$$

Then

$$Q^{-1}h(m)P' = HPX^{T},$$

This is equivalent to saying that

$$h(m) = QHPX^{T}P'^{,T} = \hat{H}X^{T}P'^{,T}.$$

C. *Demonstration of unforgeability*

To sign a message, the attacker needs to decode the hash of the message .But to execute this task, he must know the structure of the code whose parity matrix is the unknown matrix H. That means that he has to solve a problem of decoding by syndrome.

VI. CONCLUSION

In this paper we have proposed a new digital signature scheme based on error correcting codes using bit position exchanging. This method has the same advantages as the CFS scheme. In fact, it produces short signatures with high level of security. Moreover, it allows to facilitate the decoding task by randomly choosing a decodable word in respect of Hamming metric.

We discussed the mathematical aspect to prove the correctness and the unforgeability, based on the difficulty of syndrome decoding problem.

In the future, we will extend this approach to produce blind signature and signcryption schemes.

REFERENCES

[1]N.Courtois, M.Finiasz, and N.Sendrier. How to achieve a McEliece-based digital signature scheme. In Advances in Cryptology - ASIACRYPT 2001, volume 2248 of Lecture Notes in Comp. Sc., pages 157 – 174, 2001.

[2]P.W.Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Sci. Stat. Comp. 26, 1484, 1997.

[3]N.Sendrier: Code-Based Cryptography: State of the Art and Perspectives. IEEE Security & Privacy, Vol.15, Issue 4, pages 44 – 50, 2017.

[4]X.M. Wang: Digital signature scheme based on error–correcting codes. Electronics Letters, Vol.26, No.13, pages 898–899, 1990.

[5]T.R.N. Rao and K.H. Nam: Private–key algebraic–code encryptions. IEEE Transactions on Information Theory, Vol.35, No.4, pages 445–457, 1989.

[6]L. Harn, D.C. Wang: Cryptoanalysis and modification of digital signature scheme based on error–correcting codes. Electronics Letters 28(2), pages 157–159, 1992.

[7]M.Finiasz. Parallel-CFS - strengthening the CFS McEliece-based signature scheme. In Selected Areas in Cryptography 17th International Workshop, 2010.

[8]JC.Faugère, V.Gauthier, A.Otmani, L.Perret, and JP.Tillich. A distinguisher for high rate McEliece cryptosystems. In Proc. IEEE Inf. Theory Workshop- ITW 2011, pages 282 – 286, 2011.

[9]G.Kabatianskii, E.Krouk, and B. J. M.Smeets. A digital signature scheme based on random error-correcting codes. In IMA Int. Conf., volume 1355 of Lecture Notes in Comp.Sc., pages 161 - 167. Springer, 1997.

[10]G.Kabatianskii, E.Krouk, and B.J.M.Smeets. Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept. John Wiley & Sons, 2005.

[11]M.Baldi, M.Bianchi, F.Chiaraluce, J.Rosenthal, and D.Schipani. Using LDGM codes and sparse syndromes to achieve digital signatures. In Post-Quantum Cryptography 2013, volume 7932 of Lecture Notes in Comp. Sc., pages 1 - 15. Springer, 2013.

[12]P.Gaborit, O.Ruatta, J.Schrek, and G.Zémor. Ranksign: An efficient signature algorithm based on the rank metric. In Post-Quantum Cryptography 2014, volume 8772 of Lecture Notes in Comp. Sc., pages 88 - 107. Springer, 2014.

[13]D.Gligoroski, S.Samardjiska, H.Jacobsen, and S.Bezzateev. McEliece in the world of Escher. IACR Cryptology ePrint Archive, Report2014/360, 2014.

[14]E.Persichett: Efficient One-Time Signatures from QuasiCyclic Codes. ACM-New York, NY, USA, 2018.

[15]G.Landais and JP.Tillich. An efficient attack of a McEliece cryptosystem variant based on convolutional codes. In Post-Quantum Cryptography 13, volume 7932 of Lecture Notes in Comp. Sc., pages 102 - 117. Springer, June 2013.

[16]R.J.McEliece: A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42 - 44, 114|116, 1978

[17]H.Niederreiter. Knapsack-type Cryptosystems and Algebraic Coding Theory. Problems of Control and Information Theory 15, vol. 1, n° 6, 1986, pages 159 – 166, 1986.

[18]V.M.Sidelnikov, S.O.Shestakov: On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl. 2(4), 439 – 444, 1992.

[19]Y.X.Li, R.H.Deng, X.M.Wang: On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Transactions on Information Theory 40(1), 271 – 273, 1994.