International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

A Novel Blind Signature based on Error Correcting Codes

Younes Bayane[1,2], Fatima Amounas[1], Hassain Sadki[1], Lahcen El Bermi[2]
[1]R.O.I Group, Computer Sciences Department, Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco
[2]GL-ISI, Computer Sciences Department, Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco

***Abstract*—** *Cryptography based on the theory of error correcting Codes have recently received significant attention by researchers due to high performance as compared to the other existing schemes. It is one of the most promising of designing the cryptographic schemes with strong security guarantees. In this paper we attempt to develop a novel blind signature scheme based McEliece cryptosystem. From security analysis, we prove that the proposed scheme based on coding theory meets the requirements like correctness, blindness, unforgeability and untraceability. The steps of the implementation of our algorithm are also investigated.*

***Keywords*—** *Cryptography, Error correcting codes, Blind signature, Non-repudiation.*

I. Introduction

Code-based cryptosystems were established as promising alternatives for asymmetric cryptography [1]. The idea to use error-correcting codes in order to construct public key cryptosystems was published in 1978 by McEliece [2]. McEliece used Goppa codes, which has a crucial impact on the security of the cryptosystem. Compared to other public key cryptosystem such RSA, McEliece has the advantage to resist quantum attacks so far, this property makes this scheme an interesting candidate for post-quantum cryptography [3]. In the field of cryptography, A blind signature scheme is a variant of digital signature scheme. Blind Signature is a form of digital signature in which the message is blinded before it is signed, in order to allow the requester to get a signature without giving the signer any information about the actual message or the resulting signature. The blind signature schemes must meet the following requirements, namely, correctness, blindness, unforgeability and untraceability [4]. Several blind signature schemes are proposed in the literature. In [5] the authors proposed a blind signature scheme based on RSA. A blind signature based on elliptic curve is proposed by Preeti Singh in [6]. Recently, code based public key cryptography has received a wide attention by many researchers. In [7] the author presented a conversion from signature schemes connected to coding theory into blind signature schemes. In [8], Junyo and al. proposed an efficient blind signature scheme based on Neiderreiter cryptosystem. In [9] Siyuan Chen et al. proposed a secure blind signature based on coding theory which can produce a valid signature without many loops unlike existing code-based signature schemes. In this paper, we attempt to develop a novel blind signature scheme based McEliece cryptosystem. The rest of the paper is organized as follows: Basic concept of McEliece cryptosystem and Blind Signature scheme is discussed in section 2. Our blind signature scheme is presented in section 3. Section 4 is devoted to the experimental results. The performance of this scheme is examined in section 5. Finally, conclusions are made in section 6.

II. Background Information

A. McEliece Cryptosystem

The McEliece cryptosystem is the most successful cryptosystem based on error-correcting linear codes. The main components of this system are:

- F: any family of linear codes with an efficient decoding algorithm.
- D: an efficient decoding algorithm.
- t: number of errors.
- G: a private linear block code generator matrix.
- S: a secret scrambling matrix.
- P: a secret permutation matrix
- m: plaintext message
- c: cipher text.

The McEliece scheme includes three algorithms [10]:

Key generation:

1. Pick a random [n, k, 2t + 1]-linear code *C* over F_2 that has an efficient decoding algorithm D that can correct up to t errors.
2. Compute a k×n generator matrix G for *C*.
3. Generate a random k×k binary non-singular matrix S.
4. Generate a random n×n permutation matrix P.
5. Compute the k×n matrix G'= SGP.

   The public key is (G', t)

   The private key is (S, G, P, D).

Encryption: To encrypt a plaintext $m \in \{0, 1\}^k$, choose a random vector $e \in \{0, 1\}^n$ of weight t and compute the cipher text as

$$c = mG' + e$$

Decryption. To decrypt a cipher text $c \in \{0, 1\}^n$, first calculate

$$cP^{-1} = (mS)G + eP^{-1}$$

Since (mS)G is a valid codeword for the chosen linear code and eP^{-1} has weight t, the decoding algorithm D can be applied to cP^{-1} to obtain c'=mS.

Then compute m with

$$m = c'S^{-1}$$

Younes Bayane, Fatima Amounas, Hassain Sadki, and Lahcen El Bermi, "A novel blind signature based on error correcting codes", *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 2, pp. 386-389, 2017.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

B. Blind Signature Scheme

The concept of a blind signature scheme was first proposed by chaum in [11]. In the blind signature scheme, there are three participants, namely, the requester, the signer and the verifier. First, the requester blinds the message and sends the blind message to the signer. After receiving the blind message, the signer can use a private key to sign it and send the blind signature back to the requester. Once the requester receives it, he unblinds" the blind signature to obtain the signature and sends it to the verifier. After the verifier receives the signature, he can use a public key to verify the legitimacy of the signature. Figure 1 illustrates the flow of the blind signature.

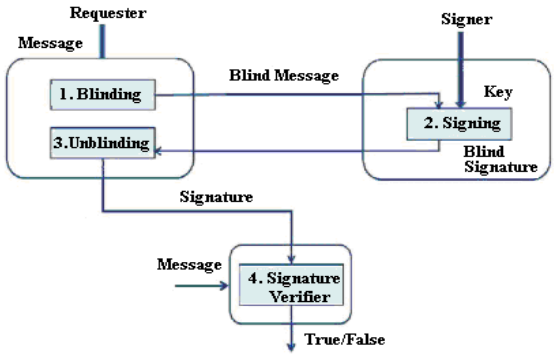

Fig. 1. Flow of blind signature.

III. Proposed Method

In this section, the underlying principles of the new blind signature scheme are explained using two kinds of participants: a signer and a requester. The request who wants the signature of a message and the signer who sign the message into signature. Before signing the message, the request has to hash the message in order to hide the information. The proposed blind signature scheme contains four phases. They are

- Blinding
- Signing
- Unblinding
- Verifying

The main notifications used throughout the paper are elaborated in table I. Table II illustrates the flow of the proposed blind signature.

TABLE I. Notifications.

m	Secret message
H	Hash function
G	A private linear block code generator matrix
M	A secret scrambling matrix
P	A secret permutation matrix
PK	A public key matrix
A^{-1}	The inverse of matrix A
σ	Signature

The proposed scheme can be summarized as follows:

A. Blinding Phase

To blind the secret message m, the requester does the following steps:

Step 1. Generates a secret message m and computes H(m) where H is the Hash function.
Step 2. Chooses an irreducible polynomial P_1 ($\deg P_1 \leq k$), as blinding factor. Then computes: $H(X) = K(X)P_1(X) + R(X)$.
Step 3. Computes H(X) mod $P_1(X)$ and sends it back to the signer for signing operation.

B. Signing Phase

The signer receives the blinded message from the requester; he generates the blind signature σ' *as follows:*

$$\sigma' = P^T G^T M^T R$$

Then, he sends the message-signature σ' back to the requester.

C. Unblinding Phase

When the requester receives the blind signature σ' from the signer, the unblinding operation is given as follows:

$$Q(X) = (K(X)P(X)/R(X)+1)$$
$$\sigma = \sigma' Q$$

The requester needed to verify the blind signature and message are intended to him.

D. Verifying Phase

Digital signature can verify by examining the correctness of the equation:

$$H(X) \stackrel{?}{=} H'(X) = PK \times \sigma$$

If H'(X) =H(X) then σ is the valid signature of the message m, otherwise reject.

TABLE II. Flow of the proposed blind signature scheme.

Request	**Blinding Phase** Compute H(m) where H is the Hash function. Polynomial P_1 ($\deg(P_1) \leq k$) (blinding factor) $H(X) = K(X)\ P_1(X) + R(X)$ Send (R)
Signer	**Signing Phase** Private Key: (P, G, M) Public Key: $PK = (M^t)^{-1}(G^t)^{-1}(P^t)^{-1}$ Compute $\sigma' = P^t G^t M^t R$ Send σ'
Request	**Unblinding Phase** Compute $Q(X) = ((K(X)P(X)/R(X) + 1)$ $\sigma = \sigma' Q$
Verifying Phase Any party who has the public key of the signer can verify the signature. $H'(X) = PK \times \sigma$ $H'(X) \stackrel{?}{=} H(X)$	

IV. Implementation and Results

In this section, we implement the proposed blind signature scheme using visual studio C#. The following set of figures shows the various steps involved in our proposed scheme. A plaintext "cryptography based on error correcting codes" is taken as the input to the algorithm.

Younes Bayane, Fatima Amounas, Hassain Sadki, and Lahcen El Bermi, "A novel blind signature based on error correcting codes", *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 2, pp. 386-389, 2017.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

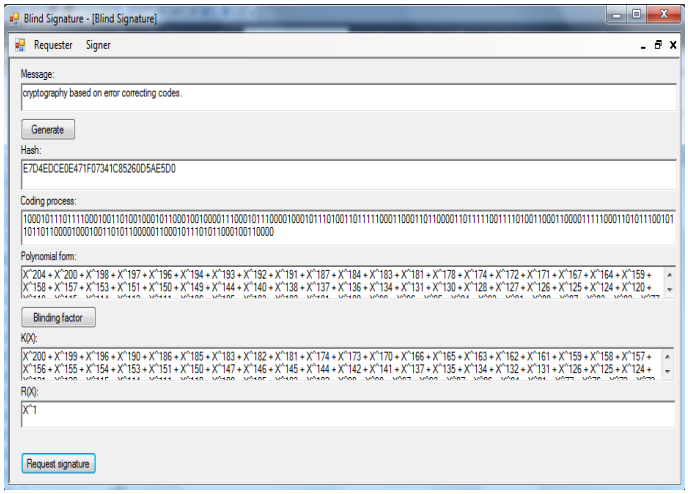

Fig. 2. Snapshot of Blinding phase.

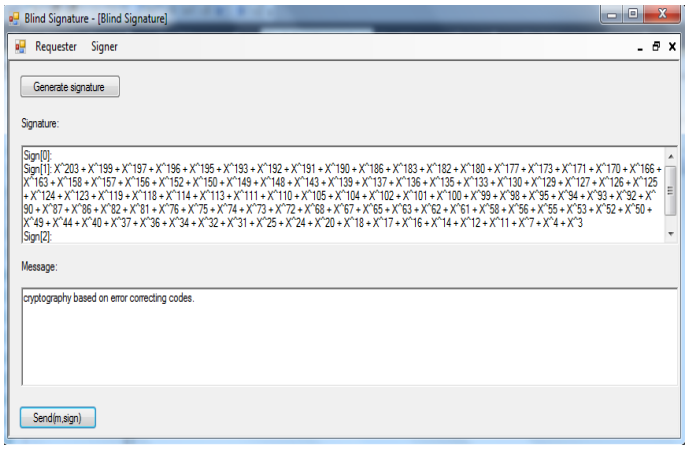

Fig. 3. Snapshot of Signing phase.

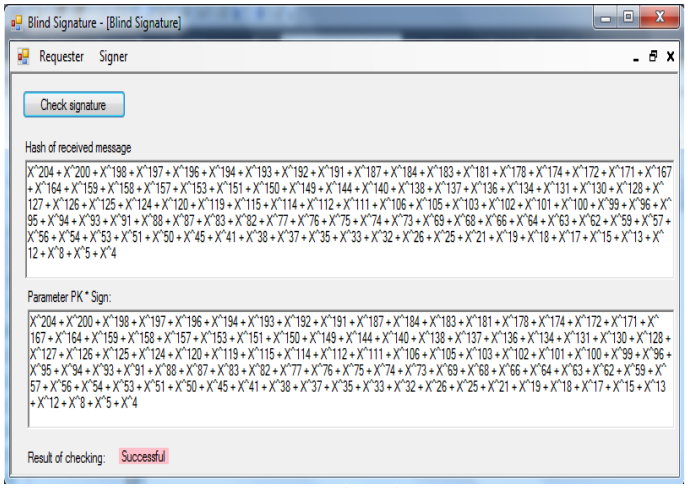

Fig. 4. Snapshot of Verifying phase.

V. Security Analysis

In this section, we examine the correctness, blindness, unforgeability and untraceability of the proposed scheme.

- *Correctness*

In our proposed scheme, we prove the verification equation $H'(X) = {}^{?} H(X)$.

The correctness of our scheme can be easily verified as follows:

$$H'(X) = PK \times \sigma$$
$$= (M^t)^{-1}(G^t)^{-1}(P^t)^{-1}\ ((K(X)P(X)/R(X)+1)\ \sigma')$$
$$= (K(X)P(X)/R(X)+1)\ R(X)P^tG^tM^t)(M^t)^{-1}(G^t)^{-1}(P^t)^{-1}$$
$$= (K(X)P(X)+R(X))\ P^tG^tM^t\ (M^t)^{-1}(G^t)^{-1}(P^t)^{-1}$$
$$= H(X)$$

Here σ is the signature of message m signed by the signer and anyone can generate H(m) and verify the correctness of the equation. Then, σ is the valid signature of the message m.

- *Blindness*

Blindness is the most important property in a blind signature. In this experiment, blindness means that the signer does not know the content of the message when he signs the message. The requester calculates H(m) and generates H(X) defined in polynomial form. The blind factor P_1 is chosen randomly by the request. Hence, the signer can not know the message m.

- *Unforgeability*

No one can forge the signature σ. If someone wants to forge the signer signature, he must get the blinding factor from the request and the private key of the signer. If attacker tried to fake σ' he cannot obtain R because they don't know (P, G, M). So, it is impossible to forge a message to satisfy the equation $H(X) = PK \times \sigma$.

- *Untraceability*

The signer cannot link the signature to the message as signer only has the information (R, σ') for each blind signature requested. Therefore, without the knowledge of the secret information of the requester H(m) and P_1, can not trace the blind signature.

VI. Conclusion

This paper suggests a novel blind signature scheme based on the error-correcting codes. The implementation with graphical user interface using visual studio C# has been presented. The security of the proposed scheme is the same as the security of McEliece scheme. Through security analysis, the proposed scheme has the basic features such as blindness, unforgeability, untracability. Therefore, it can be efficiently applied to electronic cash payment systems or anonymous voting systems.

References

[1] P.-L. Cayrel, S. Mohamed El Yousfi Alaoui, G. Hoffmann, M. Meziani, and R. Niebuhr, "Recent progress in code-based cryptography," *International Journal of Security and Its Applications*, vol. 5, no. 4, pp. 133-144, 2011.

[2] R. McEliece. "A public-key cryptosystem based on algebraic coding theory," The Deep Space Network Progress Report, DSN PR 42–44, 1978.

[3] F. Strenzke, "Efficiency and implementation security of code-based cryptosystems," PhD dissertation, Universität Darmstadt, Germany, 2013.

[4] M. S. Hwang, C. C. Lee, and Y. C. Lai, "An untraceable blind signature scheme," *IEICE Trans. Fundam Electron Commun. Comput. Sci. (Inst. Electron Inf. Commun. Eng.)*, vol. E86-A, no. 7, pp. 1902-1906, 2003.

[5] Chien H Y, Jan J K , and Tseng Y M . , "RSA-Based partially blind signature with low computation," *Proc. of the 8th IEEE International Conference on Parallel and Distributed Systems*, pp. 385-389, 2001.

[6] P. Singh, "Blind signature scheme based on elliptical curve cryptography (ECC)," *IOSR Journal of Computer Engineering*, vol. 17, issue 2, pp. 28-36, 2015.
[7] R. Overbeck, "A step towards QC blind signatures," IACR Cryptology ePrint Archive 2009: 102, 2009.
[8] J. Ye, F. Ren, D. Zheng, and K. Chen, "An efficient blind signature scheme based on error correcting codes," *Advances in Computer Science: an International Journal*, vol. 4, issue 4, no.16, pp. 21-26, 2015.
[9] S. Chen, P. Zeng, and K.-K. Raymond Choo, "A provably secure blind signature based on coding theory," *IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS)*, 2016.
[10] N. N. Abdulrazaq and T. M. Qaradaghi, "Cryptosystem based on error correcting codes," *ZANCO Journal of Pure and Applied Sciences*, vol. 28, issue 2, pp. 99-109, 2016.
[11] D. Chaum, Blind Signature System. Advances in cryptology: proceedings of crypto 1982, Heidelberg: Springer-Verlag, pp. 199-252, 1982.