ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 4, No.16 , July 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

an Efficient Blind Signature Scheme based on Error Correcting Codes

Junyao Ye[1, 2], Fang Ren[3] , Dong Zheng[3] and Kefei Chen[4]

[1] Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China
sdyejunyao@sjtu.edu.cn

[2] School of Information Engineering, Jingdezhen Ceramic Institute, Jingdezhen 333403,China
sdyejunyao@sjtu.edu.cn

[3] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications Xi'an 710121, China
dzheng@sjtu.edu.cn

[4] School of Science, Hangzhou Normal University, Hangzhou 310000, China
kfchen@sjtu.edu.cn

Abstract

Cryptography based on the theory of error correcting codes and lattices has received a wide attention in the last years. Shor's algorithm showed that in a world where quantum computers are assumed to exist, number theoretic cryptosystems are insecure. Therefore, it is important to design suitable, provably secure post-quantum signature schemes. Code-based public key cryptography has the characteristic of resisting the attack from post-quantum computers. We propose a blind signature scheme based on Niederreiter PKC, the signature is blind to the signer. Our scheme has the same security as the Neiderreiter PKC.Through performance analysis, the blind signature scheme is correct; also it has the characteristic of blindness, unforgeability and non-repudiation. In addition, its efficiency is higher than the signature scheme based on RSA scheme. In the near future, we will focus our research on the group signature and threshold ring signature based on error correcting codes.

Keywords: *Code-based PKC, Blind Signature, Unforgeability, Non-repudiation, Error Correcting Codes.*

1. Introduction

Digital signature algorithms are among the most useful and recurring cryptographic schemes. Cryptography based on the theory of error correcting codes and lattices has received a wide attention in the last years. This is not only because of the interesting mathematical background but as well because of Shor's algorithm[1], which showed that in a world where quantum computers are assumed to exist, number theoretic cryptosystems are insecure. Therefore, it is of utmost importance to ensure that suitable, provably secure post-quantum signature schemes are available for deployment, should quantum computers become a technological reality.

The concept of blind signature was first proposed by Chaum et al.[2] in CRYPTO'82. In a blind signature mechanism, the user can get a valid signature without revealing the message or relevant information to the signer. What's more, the signer won't be able to connect the signature with the corresponding signature process in the future. In 1992, Okamoto proposed a blind signature scheme[3] based on schnorr signature[4]. In 2001, Chien et al.[5] proposed a partial blind signature scheme based on RSA public key cryptosystem. In 2007, Zheng Cheng et al.[6] proposed a blind signature scheme based on elliptic curve. There are a variety of mature blind signature scheme used in electronic cash scheme[7]. Hash function[8] can compress the message of arbitray length to fixed length. A secure hash function has the characteristic of onewayness and collision-resistance, which is widly used in digtal signature.

There are many blind signature schemes at present, but the development of post-quantum computers has posed a huge threat to them. Code-based public key cryptography can resist the attack from post-quantum algorithm. Until now, just a literature[9] related to blind signature based on error correcting codes. In this paper[9], the authors proposed a conversion from signature schemes connected to coding theory into blind signature schemes, then give formal security reductions to combinatorial problems not connected to number theory. This is the first blind signature scheme which can not be broken by quantum computers via cryptanalyzing the underlying signature scheme employing Shor's algorithms[1]. In our paper, we propose a blind signature scheme based on Niederreiter [10] public key cryptosystem. Our scheme realizes the blindness, unforgeability, non-repudiation of the bind signature scheme, lastly we analyze the security of our scheme.

The remainder of this paper is organized as follows. Section 2 discusses theoretical preliminaries for the presentation. Section 3 describes the digital signature, blind signature and RSA blind scheme. Section 4 describes the proposed blind signature based on Niederreiter PKC. Section 5 formally analyses the proposal scheme and proves that the scheme is secure and efficient. We conclude in Section 6.

2. Preliminaries

We now recapitulate some essential concepts from coding theory and security notions for signature schemes.

2.1 Coding Theory

The idea is to add redundancy to the message in order to be able to detect and correct the errors. We use an encoding algorithm to add this redundancy and a decoding algorithm to reconstruct the initial message, as is showed in Fig1, a message of length k is transformed in a message of length n with $n > k$.

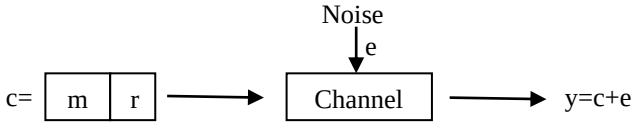

Fig1. Encoding Process

Definition 1(*Linear Code*). An (n, k)-code over F_q is a linear subspace $\mathbb{C}$ of the linear space F_q^n. Elements of F_q^n are called words, and elements of $\mathbb{C}$ are codewords. We call n the length, and k the dimension of $\mathbb{C}$.

Definition 2(*Hamming Distance, Weight*). The Hamming distance d(x, y) between two words x, y is the number of positions in which x and y differ. That is, $d(x,y) = |\{i: x_i \neq y_i\}|$, where $x = (x_1, \cdots, x_n)$ and $y = (y_1, \cdots, y_n)$. Here, we use $|S|$ to denote the number of elements, or cardinality, of a set S. In particular, d(x, 0) is called the Hamming weight of x, where 0 is the vector containing n 0's. The minimum distance of a linear code $\mathbb{C}$ is the minimum Hamming distance between any two distinct codewords.

Definition 3(*Generator Matrix*). A generator matrix of an (n, k)-linear code $\mathbb{C}$ is a $k \times n$ matrix G whose rows form a basis for the vector subspace $\mathbb{C}$. We call a code systematic if it can be characterized by a generator matrix G of the form $G = (I_{k\times k}|A_{k\times(n-k)})$, where $I_{k\times k}$ is the $k \times k$ identity matrix and A, an $k \times (n-k)$ matrix.

Definition 4(*Parity-check Matrix*). A parity-check matrix of an (n, k)-linear code $\mathbb{C}$ is an $(n-k) \times n$ matrix H whose rows form a basis of the orthogonal complement of the vector subspace $\mathbb{C}$, i.e. it holds that, $\mathbb{C} = \{c \in F_q^n : Hc^T = 0\}$.

2.2 SDP and GDP

A binary linear error-correcting code of length n and dimension k, denoted $[n,k]$-code for short, is a linear subspace of F_2^n having dimension k. If its minimum distance is d, it is called an $[n,k,d]$-code. An $[n,k]$-code $\mathbb{C}$ is specified by either a generator matrix $G \in F_2^{k\times n}$ or by parity-check matrix $H \in F_2^{(n-k)\times n}$ as $\mathbb{C} = \{mG \in F_2^n | m \in F_2^k\} = \{c \in F_2^n | Hc^T = 0\}$.

The syndrome decoding problem(SDP), as well as the closely related general decoding problem(GDP), are classical in coding theory and known to be NP-complete[11].

Definition 5(*Syndrome decoding problem*). Let r,n, and w be integers, and let (H,w,s) be a triple consisting of a matrix $H \in F_2^{r\times n}$, an integer w<n, and a vector $s \in F_2^r$. Does there exist a vector $e \in F_2^n$ of weight $wt(e) \leq w$ such that $He^T = s^T$?

Definition 6(*General decoding problem*). Let k,n, and w be integers, and let (G,w,c) be a triple consisting of a matrix $G \in F_2^{k\times n}$, an integer $w < n$, and a vector $c \in F_2^n$. Does there exist a vector $m \in F_2^k$ such that $wt(mG + c) \leq w$?

2.3 Niederreiter Public Key Cryptosystem

A dual encryption scheme is the Niederreiter[10] cryptosystem which is equivalent in terms of security to the McEliece cryptosystem[12]. The main difference between McEliece and Niederreiter cryptosystems lies in the description of the codes.

The Niederreiter encryption scheme describes codes through parity-check matrices. But both schemes have to hide any structure through a scrambling transformation and a permutation transformation. The Niederreiter cryptosystem includes three algorithms.

KegGen$(\mathbf{1^k})$

1.Choose n, k and t according to $\mathcal{K}$;

2.Randomly pick a parity-check matrix H_0 of an [n, k, 2t+1] binary Goppa code;

3.Randomly pick a $n \times n$ permutation matrix P;

4.Randomly pick a $(n-k) \times (n-k)$ invertible matrix M;

5.Calculate $H = M \times H_0 \times P$;

6.Output $pk = (H, t)$, and $sk = (M, H_0, P, \gamma_H)$ where γ_H is an efficient syndrome decoding algorithm.

Encrypt$(\mathbf{pk}, \mathbf{m} \in \boldsymbol{W_{2,n,t}})$

$\boldsymbol{W_{2,n,t}}$ algorithm maps any bit strings to codewords of length n and constant weight t.

1.Calculate $c = H \times m^T$;

2.Output c.

Decrypt$(\mathbf{sk}, \mathbf{c} \in \boldsymbol{F_2^{n-k}})$

1.Calculate $z = M^{-1} \times c$;
2.Calculate $y = \gamma_H(z)$;
3.Output $m = y \times P^{-1}$.
The security of the Niederreiter PKC and the McEliece PKC are equivalent. An attacker who can break one is able to break the other and vice versa [12]. In the following, by "Niederreiter PKC" we refer to the dual variant of the McEliece PKC and to the proposal by Niederreiter to use GRS codes by "GRS Niederreiter PKC".
The advantage of this dual variant is the smaller public key size since it is sufficient to store the redundant part of the matrix H. The disadvantage is the fact, that the mapping algorithm slows down encryption and decryption. In a setting, where we want to send random strings, only, this disadvantage disappears as we can take h(e) as random string, where h is a secure hash function.

3. Digital Signatures and Blind Signatures

3.1 Digital Signature

Under a protocol among all related parties, the digital signatures are used in private communication. All messages are capable of being encrypted and decrypted so as to ensure the integrity and non-repudiation of them. The concept of digital signatures originally comes from cryptography, and is defined to be a method that a sender's messages are encrypted or decrypted via a hash function number in keeping the messages secured when transmitted. Especially, when a one-way hashing function is performed to a message, its related digital signature is generated called a message digest. A one-way hash function is a mathematical algorithm that makes a message of any length as input, but of a fixed length as output. Because its one-way property, it is impossible for the third party to decrypt the encrypted messages. Two phases of the digital signature process is described in the following.
1. Signing Phase:
A sender firstly makes his message or data as the input of a one-way hashing function and then produces its corresponding message digest as the output. Secondly, the message digest will be encrypted by the private key of the sender. Thus, the digital signature of the message is done. Finally, the sender sends his message or data along with its related digital signature to a receiver.
2. Verification Phase:
Once the receiver has the message as well as the digital signature, he repeats the same process of the sender does, letting the message as an input into the one-way hashing function to get the first message digest as output. Then he decrypts the digital signature by the sender's public key so as to get the second message digest. Finally, verify whether these two message digests are identical or not.

When data are transmitted through the Internet, it is better that the data are protected by a cryptosystem beforehand to prevent them from tampering by an illegal third party. Basically, an encrypted document is sent, and it is impossible for an unlawful party to get the contents of the message, except he gets the sender's private key to decrypt the message. Under a mutual protocol between the senders and receivers, each sender holds a private key to encrypt his messages to send out, and a public key used by the receiver to decrypt his sent-out messages. When the two message digests are verified to be identical, the recipient can have the true text message. Thus, the security of data transmission can be made sure.

3.2 Blind Signature

The signer signs the requester's message and knows nothing about it; moreover, no one knows about the correspondence of the message-signature pair except the requester. A short illustration of blind signature is described in the following.
1. Blinding Phase:
A requester firstly chooses a random number called a blind factor to mess his message such that the signer will be blind to the message.
2. Signing Phase:
When the signer gets the blinded message, he directly encrypts the blinded message by his private key and then sends the blinding signature back to the requester.
3. Unblinding Phase:
The requester uses his blind factor to recover the signer's digital signature from the blinding signature.
4. Signature Verification Phase:
Anyone uses the signer's public key to verify whether the signature is valid.

3.3 RSA Blind System

The first blind signature protocol proposed by Chaum is based on RSA system [2]. For each requester, he has to randomly choose a blind factor r first and supplies the encrypted message α to the signer, where $\alpha \equiv r^e m \pmod n$. Note that n is the product of two large secret primes p and q, and e is the public key of the signer along with the corresponding secret key d such that $ed \equiv 1 \bmod (p-1)(q-1)$. The integer r is called a blind factor because the signer will be blind to the message m after the computation of $r^e m \pmod n$. While getting α, the signer makes a signature β on it directly, where $\beta \equiv \alpha^d \pmod n$ and then returns the signed message to the requester. The requester strips the signature β to yield an untraceable signature s, where $s \equiv r^{-1}\beta \pmod n$, and announces the pair (m, s) . Finally, anyone uses the signer's public key e to verify whether the signature is valid by checking the formula $s^e \equiv m \ (mod\ n)$ holds.

4. Proposed Blind Signature Scheme

4.1 Initialization Phase

We randomly choose a t degree irreducible polynomial g(x) in the finite field GF(q), and we get an irreducible Goppa code (n, k, t). The generating matrix of the Goppa code is G of order $k \times n$, the corresponding parity check matrix is H_0 of order $(n-k) \times n$. We then choose invertible matrix M of order $(n-k) \times (n-k)$ and permutation matrix P of order $n \times n$. Let $R = (M^T)^{-1}(H_0{}^T)^{-1}(P^T)^{-1}$. The private key is (M, H_0, P), the public key is (R, t).

4.2 Proposed Blind Signature Scheme

There are two parties in the proposed blind signature scheme, the requester and the signer. The requester who wants the signature of a message, the signer who can sign the message into a signature. Before signing the message, the requester has to hash the message in order to hide the information of the message.

1. Hash Phase

Assume the message m is of n dimension sequences, denoted as $m = (m_1, m_2, \cdots, m_n)$. We can use a secure hash function, for example, MD5, to obtain message digest h(m), where h is a selected secure hash function.

2. Blinding Phase

The requester randomly chooses a invertible matrix B as blinding factor, computes $B(m) = Bh(m)$. Then sends the blinding message B(m) to the signer.

3. Signing Phase

After the signer has received the blinding message B(m), computes $\sigma' = B(m)P^T H_0^T M^T$, then sends the signature σ' to the user.

4. Unblinding Phase

After the requester has received the signature σ', the requester uses invertible B to recover signature, computes as the following:

$\sigma = B^{-1}\sigma' = B^{-1}B(m)P^T H_0^T M^T = h(m)P^T H_0^T M^T$

So, σ is the real signature of the message digest h(m).

5. Verification Process

Anyone can verify whether the signature is valid by computing σR, R is the public key of the signer. If $\sigma R = h(m)$, then σ is the valid blind signature of the message m, otherwise, reject.

5. Performance Analysis

5.1 Correctness

If the requester and the signer execute the process according to the above protocol, then the signature σ is the exact correct signature of message m signed by the signer, and anyone can verify the correctness by computing the following:

$$\begin{aligned}&\sigma R\\&= h(m)P^T H_0^T M^T R\\&= h(m)P^T H_0^T M^T (M^T)^{-1}\left(H_0{}^T\right)^{-1}(P^T)^{-1}\\&= h(m)\end{aligned}$$

Because equation σR is equal to h(m), σ is the valid signature of the message m.

5.2 Security Analysis

The blind signature scheme is based on Niederreiter PKC, so the security of the proposed signature scheme is up to the security of Niederreiter PKC. There have been several methods proposed for attacking McEliece's system,[13],[14],etc. Among them, the best attack with least complexity is to repeatedly select k bits at random from the n-bit ciphertext vector c to form c_k in hope that none of the selected k bits are in error. If there is no error in them, then $c_k G_k^{-1}$ is equal to m where G_k is the $k \times k$ matrix obtained by choosing k columns of G according to the same selection of c_k. If anyone can decomposite public key R, he will get M, H_0 and P, therefore the blind signature scheme is invalid. However, there are too many ways in decompositing R, it's about $2^{2(n-k)}\prod_{i=1}^{n-k}(1-2^i)$, $\frac{1}{t}2^{mt}$, n! numbers of M, H_0 and P respectively[15]. When n and t are large, it's impossible to calculate, so the decomposition method is unfeasible.

At present, the most efficient method on attacking the Niederreiter PKC is solving linear equations. Under such an attack, the work factor is $W = \alpha k^3 \binom{n}{k} / \binom{n-t}{k}$, when $n = 1024, t = 50$, $\alpha = 1$,the work factor of Niederreiter PKC is approximately $2^{80.7}$, so we consider the Niederreiter PKC is secure enough. That is to say, the blind signature scheme is secure because the bind signature scheme is based on the Niederreiter PKC, they have the same security.

5.3 Blindness

The blind factor B is choosed randomly by the requester, only the requester knows B, others can't obtain from any other ways, the blinding process is computed as the following:

$B(m) = Bh(m)$

Because of the privacy and randomness of B, the blinding message B(m) is unknown to the signer.

5.4 Unforgeability

From the signature process, we can see that anyone else can't forge the signer's signature. If someone wants to forge the signer's signature, firstly, he must get the blinding message B(m) from the requester, then forges a

signature. In order to forge a signature, the adversary will encounter two handicap, one is the blind factor B which is random and secret, only the requester knows B. The other problem is that even the adversary obtains the blinding message B(m), because he doesn't know the private key M, H_0 and P of the signer, it's impossible to forge a message to satisfy the equation σR = h(m). The requester himself can't forge the signer's signature, in the first step, we use the hash function to hash the message and get h(m), the process of the hash function is invertible.

5.5 Non-repudiation

The signature of the signer is signed by his private key M,H_0 and P, no others can obtain his private key, so, at any time, the signer can't deny his signature.

5.6 Untraceability

After the signature message pair (m, σ) is published, even the signer has the signature information, he can't connect the blinding signature σ' with the blinding message $B(m)$, that is to say, he can't trace the original message m.

5.7 Compared with RSA

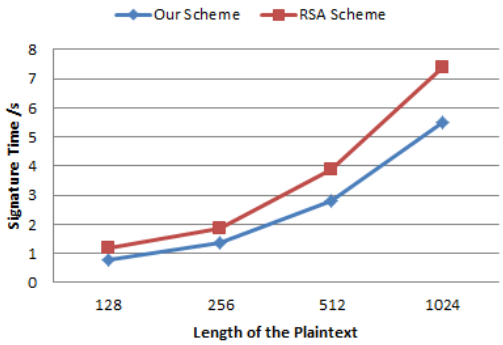

Fig2 Signature Time

We compare the blind signature time between RSA and our scheme, as is showed in Fig2. We compare four different situations, when the length of the plaintext is 128 bits, 256 bits, 512 bits and 1024 bits. From the Fig2, we can draw the conclusion that the signature time of our scheme is smaller than the signature time of the RSA shceme. So, our blind signature scheme based on Niederreiter PKC is very efficient.

6. Conclusions

We propose a blind signature scheme based on Niederreiter PKC whose security based on the security of Niederreiter PKC. Firstly, we use hash function to hash the message m to get the message digest h(m), then select randomly an invertible matrix B as blind factor to blind h(m) and get blinding message B(m). After the signer has received B(m), he will sign the B(m) by his private key. The user then unblinds what he receives, he will get the signature. By constructing the invertible matrix B cleverly, we can assure the signature is correct and is verifiable. Through performance analysis, the blind signature scheme is correct, also it has the characteristic of blindness, unforgeability and non-repudiation. The security of our scheme is the same as the security of Niederreiter PKC scheme, in addition, it's efficiency is higher than the signature scheme based on RSA scheme. The code-based cryptography can resist the attack of post-quantum computers, so the scheme is very applicable and considerable. In the near future, we will focus our research on the group signature and threshold ring signature based on the error-correcting code.

Acknowledgments

We are grateful to the anonymous referees for their invaluable suggestions. This work is supported by the National Natural Science Foundation of China (Nos. 61472472). This work is also supported by JiangXi Education Department (Nos. GJJ14650 and GJJ14642).

References

[1] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J.SCI.STATIST.COMPUT., 26:1484, 1997.
[2] Chaum D. Blind Signatures system. Advances in cryptology:proceedings of Crypto 1982, Heidelberg: Springer-Verlag, 1982:199-203.
[3] Okamoto T. Provable secure and practical identification schemes and corresponding digital signature schemes. CRYPTO'92. 1992: 31-52.
[4] C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In Advances in Cryptology – CRYPTO '89, LNCS, pages 239–252. Springer, 1989.
[5] Chien H Y, Jan J K, and Tseng Y M. RSA-Based partially blind signature with low computation. IEEE 8sth International Conference on Parallel and Distributed Systems. Kyongju : Institute of Electrical and Electronics Engineers Computer Soeiety, 2001: 385-389.
[6] Zheng Cheng, Guiming Wei, Haiyan Sun. Design on blind signature based on elliptic curve. Chongqing University of Posts and Telecommunications, 2007, (1):234-239.
[7] T.Okamoto. An efficient divisible electronic cash scheme. In CRYPTO, pages 438-451, 1995.
[8] I.Damgard. A design principle for hash functions. Crypto 89, LNCS 435, 416–427.
[9] Overbeck, R.: A Step Towards QC Blind Signatures. IACR Cryptology ePrint Archive 2009: 102 (2009).

[10]Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory[J]. Problems of Control and Information Theory, 1986, 15 (2) :159-166.
[11]E. Berlekamp, R. McEliece, and H. van Tilborg. On the Inherent Intractability of Certain Coding Problems. IEEE Transactions on Information Theory, IT-24(3), 1978.
[12]Li, Y., Deng, R., and Wang, X. the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Transactions on Information Theory, Vol.40, pp.271-273(1994).
[13]T.R.N. Rao and K.-H. Nam. Private-key algebraic-coded cryptosystems. Proc.Crypt0 '86, pp.35-48, Aug, 1986.
[14]C. M. Adams and H. Meijer. Security-related comments regarding McEliece's public-key cryptosystem. Roc. Crypto '87, Aug,1987.
[15]P. J. Lee and E. F. Brickell. An Observation on the Security of McEliece's Public-Key Cryptosystem. j-LECT-NOTES-COMP-SCI, 330:275–280, 1988.

Junyao Ye is a Ph.D. student in Department of Computer Science and Engineering, Shanghai JiaoTong University, China. His research interests include information security and code-based cryptography.

Fang Ren received his M.S. degree in mathematics from Northwest University, Xi'an, China, in 2007. He received his Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2012. His research interests include Cryptography, Information Security, Space Information Networks and Internet of Things.

Dong Zheng received his Ph.D. degree in 1999. From 1999 to 2012, he was a professor in Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. Currently, he is a Distinguished Professor in National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, China. His research interests include subliminal channel, LFSR, code-based systems and other new cryptographic technology.

Kefei Chen received his Ph.D. degree from Justus Liebig University Giessen, Germany, in 1994. From 1996 to 2013, he was a professor in Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. Currently, he is a Distinguished Professor in School of Science, Hangzhou Normal university, China. His research interests include cryptography and network security.