Proxy signature scheme based on McEliece public key cryptosystem

ZHAO Cheng-cheng
Communication Engineering Institute
Xidian University
Xi'an, China
e-mail: chengcheng.0612@163.com

YANG Ya-tao，LI Zi-chen
Beijing Electronic Science and Technology Institute
Beijing, China
e-mail: yyt2011@gmail.com

Abstract ***—Due to the threat of quantum computer, the public key cryptosystem which against quantum computing has became the focus of research. This paper applies a proxy signature scheme based on McEliece public key cryptosystem, aiming at hidden danger exists in current proxy signatures. It is designed by finding the matrices that are different but equivalent to original private keys to implement proxy signature. In addition, public key matrices are well constructed to ensure the correctness of proxy signature. Analysis shows that this scheme not only has general basic properties of digital signatures, but also inherits the security of McEliece public key cryptosystem. Therefore it has much higher security.***

Key words —Public key cryptography**; Quantum attacks;** ***McEliece public key cryptosystem*****;** ***Digital signature*****;** ***Proxy signature***

I. INTRODUCTION

Computer forensics is the technology of applying computer technology to access, investigate and analyze the evidence of computer crimes. It mainly includes the processes of determining and obtaining digital evidence, analyzing and taking data, filing and submitting result. Hence, digital signature is very useful for computer forensics. As we all know, the security of digital signature base on difficult problem, eg. RSA-PSS(R) base on Fatoriza-tion Problem, DSA and ECDSA base on Discrete Logarithm Problem. However, Peter Shor proposed a Quantum Algorithm, which can solve Fatorization Problem and Discrete Logarithm Problem within $(\lg n)^{2+o(1)}$ polynomial time, where n is module of RSA or Discrete logarithm. With quantum computer, Peter Shor algorithm can break all digital signature schemes that based on Fatorization Problem or Discrete Logarithm Problem. Therefore, the security of digital signature is faced with serious threat. McEliece public key cryptosystem is one of the post-quantum public key cryptosystem.

In daily life, a manager often needs to delegate his signature right to reliable proxies, who perform this right on manager's behalf, during his absence. This is what is called proxy signature.Proxy signature was first introduced by Mambo, Usuda and Okamoto[1][2] in 1996. It is a special class of digital signature which allows an original signer to delegate his signature right to a so-called proxy signer to sign on specified documents on behalf of the original signer. A perfect proxy signature scheme should meet verifiability, distinguishability, non-repudiation and non-forgeability[3][4]. The wide applications of proxy signature make scholars do further research on it. For example, Mambo, Usuda and Okamoto proposed complete proxy signature and part proxy signature, later Hwang defined multi-proxy signature scheme[5], etc.

At present, there are many proxy signature schemes have put forward. One of the most meaningful fields for study is to design a new proxy signature based on McEliece public key cryptosystem. In this paper, we first look for matrices that are different but equivalent to original private key to sign. Then construct public key matrices to ensure the correctness of signature when it is verified. Result shows that the proxy signature based on McEliece public key cryptosystem not only has the basic properties of general proxy signature, such as verifiability, distinguishability, non-repudiation and non-forgeability, but also inherited the safety of McEliece public key cryptosystem which can resist quantum attack. So it has higher safety and can solve privacy issues better than other public key cryptosystems.

In section 2, we review the McEliece public key cryptosystem including parameter selection, encryption and decryption processes. In section 3, we show the proxy signature scheme based on McEliece public key cryptosystem in detail. Section 4 is the security analysis of this proxy signature and the end part is the conclusion of this paper.

II. MCELIECE PUBLIC KEY CRYPTOSYSTEM

2. McEliece public key cryptosystem

The McEliece public key cryptosystem[6] using irreducible binary Goppa codes, which are a class of linear error correcting codes, so we will restrict ourselves to this subclass. As for any error correcting code, there exists a generator matrix *G* and a parity check matrix *H*. Given these matrices, a message *m* can be encoded into a codeword *c* of the code by computing $c = mG$.

2.1 Key generation:

The Public Keys

The public key is given by the public $n \times k$ generator matrix $G_p = SG_sP$ over binary field F_2 , where G_s is a generator matrix of the secret code Γ .

The Private Keys

The McEliece secret key consists of the Goppa polynomial $g(Y)$ of degree t defining the secret code Γ, an $n \times n$ permutation matrix P and a non-singular $k \times k$ matrix S over binary field F_2.

2.2 The Encryption Process

To encrypt a message $m \in F_2$, where F_2 is binary field, the user choose a random vector $e \in F_2$ with hamming weight $\mathrm{w}_H(e) = t$, and compute that $c = mG_p + e$, where e is a random error vector, then obtain the ciphertext c.

2.3 The Decryption Process

First, we calculate that

$$c^{'} = cP^T H^T = mSGPP^T H^T + eP^T H^T ,$$

then we use the rapid Goppa code decoding algorithm to the $eP^T H^T$. Since the hamming weight of eP^T and e are equal that is $W_H(eP^T) = W_H(e) = t$, we can get mS by decoding. Finally, the plaintext m can be recovered from calculating mSS^{-1}.

If the matrix S is chosen in such way that the public generator matrix is in reduced row echelon form, i.e., $G_p = [\prod | G_2]$, then, in the decryption processing, m can be recovered by extracting the first k bits of mSG_s. This would be a security problem if the McEliece public-key cryptosystem was used as proposed in [7].

2.4 Advantages

The biggest advantage of McEliece public key cryptosystem is encrypt and decrypt much faster than RSA. It is because binary addition and binary multiplication on 0 1 sequence in McEliece algorithm is much easier than big integer multiplication of RSA. From the encryption process above we can find vector e is select randomly every time, so there are different ciphertexts for the same plaintext. This kind of encryption belongs to probability encryption [8], can effectively resist attacker get plaintext from comparing the same ciphertext.

III. PROXY SIGNATURE BASED ON MCELIECE PUBLIC KEY CRYPTOSYSTEM

At the beginning, we choose appropriate parameters, i.e., construct public key matrices. It is very important to design the whole proxy signature.

3.1 Parameter Selection

Original signer A choose a error-correcting binary Goppa codes C_A. As for C_A, there exists a $k \times n$ generator matrix G_A and a $(n-k) \times n$ parity check matrix H_A. Then choose an $n \times n$ permutation matrix P and a non-singular $k \times k$ matrix S over F_2. Our main task is looking for the matrix G_A^* to make $G_A G_A^* = I_k$ be established, where I_k is a unit matrix.

Let $J_A = P_A^{-1} G_A^* S_A^{-1}$, $W_A = G_A^* S_A^{-1}$ and $T_A = P_A^{-1} H_A^T$.

Suppose original signer A is honest, choose another corresponding $k \times n$ generator matrix G_B for code C_A and generate a non-singular $k \times k$ matrix S_B to make $S_B G_B = S_A G_A$ satisfied. We keep S_B and G_B secret as private key and give it to proxy signer B.

List 1. Parameter List of Proxy Signature

	Public key	Private key
Original Signer A	J_A, W_A, T_A, H_A, t_A and $t^{'}$ (where $t^{'}$ are integers less than t_A)	S_A, G_A, P_A
Proxy Signer B		S_B, G_B, P_A

3.2 Signature Process

Proxy signer B sign message m_j as follows:

1) Randomly select a binary vector e_j with the length of n, and hamming weight is $W(e_j) = t^{'}$;

2) Signature c_j calculate by

$$c_j = (e_j + m_j S_B G_B) P_A$$

3.3 Verification Process

Because the whole signature process may be disturbed by noise, thus signature may make a mistake. Therefore let received signature be $c_j^{'}$, then the verification process is as follows:

First, we compute

$$\begin{aligned} D_1(c_j^{'}) &= c_j^{'} T_A \\ &= [(e_j + m_j S_B G_B) P_A]^{'} P_A^{-1} H_A^T \\ &= e_j^{'} H_A^T + m_j S_B G_B H_A^T \end{aligned}$$

From the above, we will get $e_j^{'}$ through Berlekamp-Massey algorithm. Compare the hamming weight of $e_j^{'}$ and e_j, if $W(e_j^{'}) \neq t^{'}$ or generate decoding error, the receiver will request retransmit the signature. If $W(e_j^{'}) = W(e_j) = t^{'}$, then go on the next step.

Let $D_2(c_j^{'}) = D_2(c_j) = c_j J_A$, then receiver calculate

$D_3(c_j^{'}) = D_3(c_j) = D_2(c_j) + e_j W_A = c_j J_A + e_j W_A$ and verify whether the value of $D_3(c_j^{'})$ is equal to m_j. The signature is effective if the answer is yes, or it is invalid.

IV. Security analysis

4.1 Correctness Analysis

Let $D_2(c_j^{'}) = D_2(c_j) = c_j J_A$, substitute $e_j + m_j S_B G_B$ and $P_A^{-1} G_A^* S_A^{-1}$ for c_j and J_A respectively, we get

$$\begin{aligned} D_2(c_j^{'}) &= D_2(c_j) \\ &= c_j J_A \\ &= [(e_j + m_j S_B G_B) P_A] P_A^{-1} G_A^* S_A^{-1} \\ &= e_j G_A^* S_A^{-1} + m_j S_B G_B G_A^* S_A^{-1} \end{aligned}$$

And then we compute that

$$\begin{aligned} D_3(c_j^{'}) &= D_3(c_j) \\ &= D_2(c_j) + e_j W_A \\ &= e_j G_A^* S_A^{-1} + m_j S_B G_B G_A^* S_A^{-1} + e_j G_A^* S_A^{-1} \\ &= e_j G_A^* S_A^{-1} + m_j S_A G_A G_A^* S_A^{-1} + e_j G_A^* S_A^{-1} \\ &= m_j \end{aligned}$$

Receiver verify $D_3(c_j^{'})$ by public key to see whether it is equal to m_j . The sign is effective if it is, otherwise the sign is invalid.

4.2 Security Analysis

1) Verifiability

All the needed parameters for verification are open. Such as identity authentication, message *m*, public keys, etc. Therefore any verifier can verify the effectiveness of proxy signature [9].

2) Distinguishability

Since the private keys of original signer and proxy signer are different, verifier can verify the validity of signature easily.

3) Non-repudiation

Once there is a dispute, verifier could judge by equation $D_3(c_j^{'}) = e_j G_A^* S_A^{-1} + m_j S_B G_B G_A^* S_A^{-1} + e_j G_A^* S_A^{-1}$. If $D_3(c_j^{'}) = m_j$, it is proxy signature, or it is original signature.

4) Non-forgeability

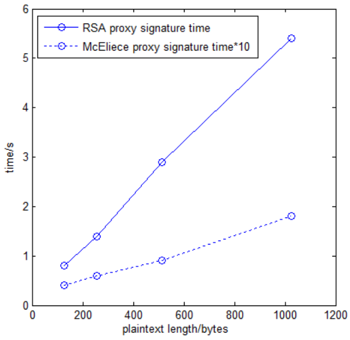
It is difficult for attackers to find proxy signer's private key according to the generation of keys. It is equivalent to the matrix decomposition NPC problem[10][11]. Attacker can't obtain private key, neither can he forge proxy signature. At the beginning, we suppose the original signer is honest, so he couldn't forge proxy signature, either.

5) Prevent the abuse of signature

Every time, original signer select private key and give it to proxy signer secretly, i.e., original signer authorize to proxy signer. Therefore, proxy signer not allowed signing unauthorized document. Of course, the original signer not permit to transfer signature right illegally.

4.2 Efficiency Analysis

To evaluate the efficiency of McEliece proxy signature, we compare the proxy signature time of RSA and McEliece. We choose different length of plaintexts and sign them respectively. Plaintexts are 128bytes, 256bytes, 512bytes and 1024bits.



Graph 1. Compare signature time of RSA and McEliece

From the graph1 above we can find that McEliece proxy signature is much faster than RSA proxy signature. So McEliece proxy signature is superior to RSA proxy signature in efficiency.

V. Conclusion

In this paper, we design a proxy signature scheme based on McEliece public key cryptosystem. We construct appropriate parameters not only complete the signature but also ensure the correctness of the signature verification.

There are two ways to attack McEliece public key cryptosystem. On the one hand, attackers can decipher private key S、G、P in order to decipher cryptosystem. On the other hand, attackers can decipher ciphertext directly. According to security analysis, to solve private keys is equivalent to matrix decomposition NPC problem. Therefore, it is impossible to decipher private keys. Neither can he decipher ciphertext. It shows McEliece proxy signature is superior to RSA proxy signature in efficiency.

Different kinds of signature e.g. threshold signature, group signature and blind signature based on McEliece public key cryptosystem need to do further research. Meanwhile, we should focus on data protection and leakage problem of privacy information. We hope to design better scheme can prevent privacy information from leaking out.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grants No. 61070219.

REFERENCES

[1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature for delegating signing operation[A]. Proc. 3rd ACM Conference on Computer and Communications Security (CCS96)[C]. [S.1.]: ACM Press, 1996:48-57

[2] MAMBOM M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Trans. Fundamentals, 1996, E79-A(9): 1338-1353

[3] LI Zi-chen, YAN Yun-sheng, ZHANG Juan-mei. An Attack on Libert et al's ID-Based Undeniable Signature [J]. Chinese Journal of Electronics, 2008, 17(4): 748 - 750.

[4] YANG Ya-tao, CAO Ru-lin, LI Zi-chen. A Novel Direct Anonymous Attestation Protocol Based on Zero Knowledge Proof for Different Trusted Domains [J]. China Communications, 2010, 7(4): 172 - 175.

[5] HWANG S J, CHEN C C. A new multi-proxy multi-signature scheme[A]. National Computer Symposium: Information Security[C]. Taibei:[s.n.],2001.

[6] McEliece R, Miller J.A Public-key Cryptosystem Based on Algebraic Coding Theory[D].CA,USA: Jet Propulsion Laboratories, California Institute of Technology,1978:114-116

[7] ZHU Hui-jun. Research and Implementation of direct anonymous authentication base on Goppa codes[D]. Henan Polytechnic University,2007.

[8] HAN Mou. Research into Seceral Issues in Code-based Post-Quantum Public Key Cryptography[D]. Nanjing, Nanjing Polytechnic University, 2011,05.

[9] P Gaborit, M Girault. Lightweight code-based authentication and signature [A]. In Proceedings of IEEE International Symposium on Information Theory [C]. Limoges, France, 2007. 191 - 195.

[10] K Kobara, H Imai. On the one-wayness against chosen-plaintext attacks of the Loidreaus modified McEliece PKC [J]. IEEE Transactions on Information Theory, 2003, 49(12): 3160 - 3168.

[11] C Wieschebrink. An attack on a modified Niederreiter encryption scheme [A]. In Proceedings of the 9th International Conference on Theory and Practice of Public-Key Cryptography [C]. New York, NY, USA, 2006. (3958), 14 - 26.