Code-based Ring Signature Scheme

Dong Zheng[1], Xiangxue Li[2], and Kefei Chen[1]
(Corresponding author: Dong Zheng)

Department of Computer Science and Engineering, Shanghai Jiaotong University[1]
School of Information Security Engineering, Shanghai Jiaotong University[2]
Shanghai 200030, P. R. China (Email: dzheng@sjtu.edu.cn)

(Received Nov. 20, 2005; revised and accepted Dec. 31, 2005 & Jan. 27, 2006)

Abstract

McEliece is one of the oldest known public key cryptosystems, however it was not quite as successful as RSA. One main reason is that it is widely believed that code-based cryptosystems like McEliece do not allow practical digital signatures. Although X.M. Wang presented a code-based signature scheme in 1990, some authors find that it is not secure. Recently, T.Courtois *et al.* show a new way to build a practical signature scheme based on coding theory (simply, Courtois et al.s scheme). The security is reduced to the well-known *syndrome decoding problem* and the distinguishability of permuted binary Goppa codes from a random code. This shows that error correct codes can be used to construct some other cryptosystems. In this paper, we present, for the first time, a code-based ring signature scheme with signature length of $144 + 126l$ bits (l is the number of ring members), which is one of the most short ring signature among all the presented ring signature schemes up to now.

Keywords: Goppa codes, McEliece cryptosystem, ring signature, syndrome decoding

1 Introduction

RSA and McEliece are the oldest public key cryptosystems. They are based on intractability of factorization and syndrome decoding problem respectively. However, McEliece was not quite as successful as RSA, partially due to its large public key and another main handicap of the belief that McEliece could not be used in signature. Recently, Nicolas T. Courtois, Matthieu Finiasz, and Nicolas Sendrier (CFS) show a new way to build practical signature schemes with the McEliece public key cryptosystem. They are based on the well-known hard syndrome-decoding problem that after 30 years of research is still exponential. Thus it would be very interesting to dispose of some other cryptosystems (such as ring signature and blind signature schemes) based on such hard decoding problems. In this letter, we propose an approach of constructing ring signature that is based on the coding theory. The main motivation for the suggested cryptosystem comes from previous studies of McEliece-Based digital signature scheme [4] and ring signature [8].

Ring signature allows a member of an Ad Hoc collection of users U to prove that a message is signed by one of U without revealing the identity of the actual signer. Unlike group signatures, ring signature has no group managers, no setup procedures, no revocation procedures, and no coordination: any user can choose any set of possible signers that includes himself, and sign any message by using his secret key and the others' public keys without their consent. Since the notion of ring signature was first formalized by Rivest *et al.* in [8], numerous ring signature schemes have been proposed [1, 3, 6, 10, 11], all of those schemes are based on the intractability of factorization, discrete logarithms problems (DLP) or elliptic curve discrete logarithms problems (ECDLP).

The rest of this paper is organized as follows. In Section 2, we introduce the properties of ring signature scheme and the security properties that such a scheme must satisfy. In Section 3, we review the McEliece-based signature scheme proposed by N.T. Courtois, M.Finiasz, and N.Sendrier. In Section 4, we present our new ring signature. In Section 5, we discuss the signature cost and length, and in Section 6, we discuss the security of the proposed scheme, and finally we give a conclusion.

2 Ring Signature

Following the formalization about ring signatures proposed in [8], we explain in this section the basic definitions and the properties eligible to ring signature schemes.

A regular ring signature scheme consists of the following three-tuple (*Key-Gen, Sign and Verify*):

- **Key-Gen** is a probabilistic polynomial algorithm that takes a security parameter(s) and returns the parameters (system parameters, private parameters and public parameters).
- **Sign** is a probabilistic polynomial algorithm that takes system parameters, a private parameter, a list

of public keys $p_{k1}, \cdots, p_{kl}$ of the ring, and a message M, the output of this algorithm is a ring signature σ for the massage M.

- **Verify** is a deterministic algorithm that takes as input a message M ,a ring signature σ, and the public keys of all the members of the corresponding ring, then outputs "True" if the ring signature is valid, or "False" otherwise.

The resulting ring signature scheme must satisfy the following properties:

- **Correctness:** any verifier with overwhelming probability must accept a ring signature generated in a correct way.
- **Anonymity:** any verifier should not have probability greater than $1/l$ to guess the identity of the real signer who has computed a ring signature on behalf of a ring of l members. If the verifier is a member of the ring distinct from the actual signer, then his probability to guess the identity of the real signer should not have greater than $1/(l-1)$.
- **Unforgeability:** any attacker must not have non-negligible probability of success in forging a valid ring signature for some message M on behalf of a ring that does not contain him, even if he knows valid ring signatures for messages, different from M, that he can adaptively choose.

3 Review of Courtois et al.'s McEliece-based Signature Scheme [4]

Let F_2 be the field with two elements $\{0,1\}$, and C be a t-error correcting Goppa codes of dimension $k(k = n - tm)$ and length $n = 2^m$, (there are about $2^{tm}/t$ such codes [7]). G^0 is a generating matrix of code C, H^0 is the parity check matrix of C, and it is a dual form of the generating matrix G^0. An element of F_2^n is called a word, and elements of C are called codewords. The product of a word and the parity check matrix H^0 is called a *syndrome*, it has a length of $n-k$ bits and is characteristic of the error added to the codeword.

Let U and V are non-singular matrices ($k \times k$ and $(n-k) \times (n-k)$ respectively) and P is an $n \times n$ permutation matrix. Let $G = UG^0P$ and $H = VH^0P$, h is a hash function returning a binary word of length $n-k$. The private keys are G, U, P and the public key is H.

Syndrome-Decoding (SD) Problem:
Instance: A binary $r \times n$ matrix H, a word s of F_2^n, and an integer $w > 0$
Problem: Is there a word x in F_2^n of weight $\leq w$ such that $H_{x^T} = s$?

Signature Algorithm:

- Hash the document M into $s = h(M)$;
- Compute $s_i = h([\cdots s \cdots | i])$ for $i = 1, 2, 3 \cdots$;
- Find i_0 the smallest value of i such that s_i is decodable;
- Use the trapdoor function to compute z such that $Hz^T = s_{i_0}$;
- Compute the index I_z of z in the space of words of weight 9;
- Use $[\cdots I_z \cdots | i_0]$ as a signature for M, where I_z is the index of z by $I_Z = 1 + \binom{i_1}{1} + \binom{i_2}{2} + \cdots + \binom{i_9}{9}$, and $i_1 < i_2 < \cdots < i_9$ denote the positions of the non-zero bits of z.

Verification Algorithm:

- Recover z from its index I_z;
- Compute $s_1 = Hz^T$ with the public key H;
- Compute $s_2 = h([\cdots h(M) \cdots | i_0])$ with the public hash function h;
- Compare s_1 and s_2: if they are equal the signature is valid.

4 Our Proposed Ring Signature Scheme

As we know, the SD problem is NP-hard, all among several known attacks for SD are fully exponential and nobody has ever proposed an algorithm that behaves differently for complete decoding and the bounded decoding problems within a distance accessible to the owner of the trapdoor. In this section, we will extend T.Courtois *et al.*'s signature scheme to a practical ring signature scheme, which is also based on *syndrome decoding problem*. The three-tuple of our ring signature is as follows.

Key-Gen (Key generating Algorithm):
Each potential signer A_i selects a t-error correcting Goppa code C_i of dimension $n - tm$ and length $n = 2^m$, chooses a generating matrix G_i^0 and chooses a generating matrix H_i^0, selects randomly two non-singular matrixes U_i, V_i and a permutation matrix P_i, computes $G_i = U_i G_i^0 P_i$ and $H_i = V_i H_i^0 P_i$, then makes H_i as A_i's public key and G_i, U_i, V_i, P_i as A_i's private keys.

As discussed in [4], the average number of tries needed to find a decodable syndrome is approximately $t!$. Consider the signature time, we have to take a t not greater than 10. If we want our scheme to be secure we will need a large n (the code length) of at least 2^{16} for $t = 9$ or 2^{15} for $t = 10$.

In the following ring signature scheme, the signer is user A_r.

Sign:

1) Hash the massage M into $h(M)$;

2) (Initialization): Choose randomly words $\bar{s}_q \in F_2^{n-k}$, and compute $s_{r+1,q} = h(L|h(M)|\bar{s}_q)$ for $q = 0, 1, 2, \cdots$;

3) (Generate forwarding ring sequence): For $i = r+1, \cdots, l-1, 0, 1, \cdots, r-1$, choose randomly $z_{i,q} \in F_2^n$ (of weight t) and compute $s_{i+1,q} = h(L|h(M)|H_i z_{i,q}^T \oplus s_{i,q})$;

4) Find $\bar{q}$ the smallest value of q such that $s_{r,\bar{q}} \oplus \bar{s}_{\bar{q}}$ is decodable;

5) Use the trapdoor function to compute $z_{r,\bar{q}}$ such that $H_r z_{r,\bar{q}}^T = s_{r,\bar{q}} \oplus \bar{s}_{\bar{q}}$;

6) Compute the index $I_{Z_{i,\bar{q}}}$'s of $z_{i,\bar{q}}$'s in the space of words of weight 9'as follows: $I_{z_{i,\bar{q}}} = 1 + \binom{i_1}{1} + \binom{i_2}{2} + \cdots + \binom{i_9}{9}$, Where $i_1 < i_2 < \cdots < i_9$ denote the positions of the non-zero bits of $z_{i,\bar{q}}$;

7) Output the ring signature: select 0 as the glue value, the resulting signature for M and L is the $l+1$ -tuple: $(s_{0,\bar{q}}, I_{z_{0,\bar{q}}}, I_{z_{1,\bar{q}}}, \cdots, I_{z_{l-1,\bar{q}}})$. For simplicity, let $s_i = s_{i,\bar{q}}, z_i = z_{i,\bar{q}}, I_{z_i} = I_{z_{i,\bar{q}}}, i = 0, \cdots, l-1$, then the resulting signature is denoted as $(s_0, I_{z_0}, I_{z_1}, \cdots, I_{z_{l-1}})$.

Verify:
Given $(s_0, I_{z_0}, I_{z_1}, \cdots, I_{z_{l-1}})$, M, and L:

1) Recover z_i from the index $I_{z_i}, i = 0, 1, \cdots, l-1$;

2) Compute $s_{i+1} = h(L|h(M)|H_i z_i^T \oplus s_i)$ for $i = 0, 1, \cdots, l-1$, Accept if $s_l = s_0$, and reject otherwise.

Analysis of the Proposed Scheme:
From the procedure of ring signature generation, we have:

$$\begin{aligned}
s_{r+1} &= h(L|h(M)|\bar{s}_{\bar{q}}) \\
s_{r+2} &= h(L|h(M)|H_{i+1} z_{i+1}^T \oplus s_{l+1}) \\
&\vdots \quad\quad \vdots \\
s_l &= h(L|h(M)|H_{l-1} z_{l-1}^T \oplus s_{l-1}) = s_0 \\
s_1 &= h(L|h(M)|H_0 z_0^T \oplus s_0) \\
s_2 &= h(L|h(M)|H_1 z_1^T \oplus s_1) \\
s_r &= h(L|h(M)|H_{r-1} z_{r-1}^T \oplus s_{r-1}).
\end{aligned}$$

Since $H_r z_r^T = s_r \oplus \bar{s}_{\bar{q}}$, we have

$$\begin{aligned}
s_{r+1} &= h(L|h(M)|H_r z_r^T \oplus s_r) \\
&= h(L|h(M)|\bar{s}_{\bar{q}}).
\end{aligned}$$

5 Cost and Length

Signature Cost:
The essential operation in our ring signature is to make $t!$ decoding attempts, as in the CFS signature scheme [4], for each of these attempts we need the following:

1) Compute the syndrome: we need to compute l hash functions and $l-1$ multiplication $H_i z_{i,q}$, and then we have a syndrome.

2) Solve the key equation: the signer needs to apply Berlekamp-Massey algorithm to obtain the locator polynomial, with the costs $O(t^2)$ operations in F_{2^m}.

3) Find the roots of the locator polynomial. If the syndrome is decodable, the locator polynomial splits in $F_{2^m}[z]$ and its roots give the error positions. It costs $t^2 m$ operations in F_{2^m}.

In Step 1 of our scheme, the signer has to compute l hash functions and $l-1$ multiplication $H_i z_{i,q}$, in Step1 of CFS signature scheme, the signer only needs to compute one hash functions and no multiplication $H_i z_{i,q}$. In Steps 2 and 3 of our scheme, the signer does the same thing as one does in the Steps 2 and 3 on CFS scheme. Due to the fact that the head cost in the signature generation of our signature scheme or CFS scheme are Steps 2 and 3, we may say the total cost of our signature generation is approximate to that of CFS.

Verification Cost:
The verifier needs to recover z_i's from I_{z_i}, computes l multiplication $H_i z_i^T$, and $l+1$ hash functions. Each multiplication $H_i z_i^T$ can be computed by adding the t corresponding columns. The total cost of this verification is lt column operations and $l+1$ hash computations.

Ring Signature Length:
The signature for massage M and ring L is $(s_0, I_{z_0}, I_{z_1}, \cdots, I_{z_{l-1}})$, if we take $m = 16$ and $t = 9$, then the length of s_0 is 144 bits ($n-k$ bits $= tm$ bits$= 16 \times 9 = 144$ bits), the length required to store I_{z_i} is about 126 bits, the total length of our signature is about $144 + 126l$. For the discrete logarithm based ring signature schemes [5, 8], the signature length is more than $160 + 1024l$ bits, for the ECC or pairing based ring signature schemes [11], the signature length is at least $160 + 160l$ bits.

6 Security

Anonymity: For the anonymity, We have that any attacker outside a ring of l possible users has probability $1/l$ to guess which member of the ring has actually computed a given signature on behalf of this ring, because all z_i but z_r are taken randomly from F_2^n, in fact, $z_r = \bar{z} \oplus \bar{z}_r$, because $\bar{z}$ is distributed uniformly over

F_2^n, this results in that z_r is uniformly over F_2^n.

Unforgeability:
When $n = 1$, our ring signature scheme degenerates into the McEliece-Based signature proposed by N.T. Courtois *et.al* (let $H_0 z_0^T \oplus s_0 = i_0$ in N.T.Courtoiss scheme). N.T.Courtois's scheme is non-forgeability under the two assumptions:

- Solving an instance of decoding problem is difficult.
- Recovering the underlying structure of the code is difficult.

For $n > 1$, we denote L a fix set of ring members, and suppose that an attacker A's public key does not belong to L, he may do the following:

- $A1$ Choose randomly a word $s_0 \in F_2^{n-k}$;
- $A2$ Do the same as "*generate forward ring sequence*" of **Sign** for $i = 0, 1, \cdots, l-2$;
- $A3$ Assign s_0 to $h(L|h(M)|H_{l-1}z_{l-1}^T \oplus s_{l-1})$;
- $A4$ Output the ring signature $(s_0, z_0, z_1, \cdots, z_{l-1})$.

Since h acts as a random oracle and z_i's are taken randomly from F_2^n, the probability of $s_0 = h(L|h(M)|H_{l-1}z_{l-1}^T \oplus s_{l-1})$ is $1/2^n$. So we say that our proposed ring signature is unforgeable.

7 Conclusion

We presented a code-based ring signature scheme. The security is based on the well-known hard *syndrome-decoding problem* that is still exponential. The signature length and the verification cost will always remain extremely small. The unique features make our coding-based ring signature scheme an exclusive choice for some applications while excluding other.

Acknowledgment

This work is partially supported by NSFC under the grant 60473020 and 60303026.

References

[1] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys", in *ASIACRYPT'02*, LNCS 2501, pp. 415-432, Springer-Verlag, 2002.
[2] E. R. Berlekamp, R. J. McEliece, and H. C. van Tilborg, "On the inherent intractability of certain coding problems", *IEEE Transactions on Information Theory*, vol. 24, no. 3, May. 1978.
[3] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups", in *CRYPTO'02*, LNCS 2442, pp. 465-480, Springer-Verlag, 2002.
[4] N. T. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme", *ASIACRYPT'01*, LNCS 2248, pp. 157-174, Springer-Verlag, 2001.
[5] J. Herranz and G. Saez, "Forking lemmas for ring signature schemes", in *Indocrypt'03*, LNCS 2904, pp. 266-279, Springer-verlag, 2003.
[6] J. K. Liu, V. K. Wei, and D. S. Wong, "A separable threshold ring signature scheme", in *ICISC'03*, LNCS 2971, pp. 7-22, Springer-Verlag, 2004.
[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
[8] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret", *Asiacrypt'01*, LNCS 2248, pp.552-565, Springer-Verlag, 2001.
[9] X. M. Wang, "Digital signature scheme based on error-correcting codes", *IEE Electronics Letters*, vol. 26, no. 13, pp. 898-899, 1990.
[10] D. Wong, K. Fung, J. Liu, and V. Wei, "On the RS-code construction of ring signature schemes and a threshold setting of RST", in *5th International Conference on Information and Communication Security (ICICS'03)*, LNCS 2836, pp. 34-36, Springer-Verlag, 2003.
[11] F. Zhang and K. Kim. "ID-based blind signature and ring signature from pairings", in *ASIACRYPT'02*, LNCS 2501, pp. 533-547, Springer-Verlag, 2002.

Dong Zheng received his Ph.D. degree in 1999. Now, he is a professor of department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include subliminal channel, LFSR, code-based systems and other new cryptographic technology.

Xiangxue Li is with Shanghai Jiaotong University. His research interests include provable security and pairing-based cryptography.

Kefei Chen received his Ph.D. degree from Justus-Liebig University, Germany, in 1994. Now, he is a professor of department of Computer Science and Engineering, deputy director of school of Information Security Engineering, Shanghai JiaoTong University. He concentrates his work in cryptography and information security.