Designated Verifier Signature Scheme Based on Braid Groups

Zou Shi-hua[*] Zeng Ji-wen Quan Jun-jie

September 7, 2006

Abstract

Artin's braid groups have been recently suggested as a new source for public-key cryptography. In this paper we first propose the designated verifier group signature scheme based on the conjugacy search problem and the root problem in the braid groups which are believed to be hard problems. Furthermore, our scheme can conceal the message to be signed so that it can be applied to E-voting and calling for tenders.

key words : braid groups, conjugacy search problem, root problem, designated verifier signature scheme.

1 Introduction

1.1 Braid Cryptography

A lot of popular public-key encryption systems are based on number-theoretic problems such as factoring of large integers or finding discrete logrithms (Discrete Logrithm Problem, DLP). The most underlying algebraic structure are abelian groups. Since computational power increases permanently, the required key length for a desired level of security needs to be enlarged permanently. It is therefore desirable to look for techniques in more complex algebraic settings. Combinatorial group theory provides a new platform to construct cryptosystem. Many people have investigated non-communicative algebraic structure in hope of finding a new alternative. Braid groups are deemed to hold a great deal of promise. Braid groups are more complicated than abelian groups, and are not complicated to worked with. The braid groups is useful to construct cryptosystem because: (1) it provides numerous mathematical hard problems such as the

[*]School of Mathematical Sciences,Xiamen University,Xiamen 361005

conjugacy search problem,the root problem and the braid decomposition problem; (2) the group operations and generation of the parameters can be implemented quickly by efficient algorithms; (3) the word problem is solved via a fast algorithm which can be used computer the canonical form . Recently Anshel-Anshel-Goldfeld proposed in [3] a key agreement system and a Public Key Cryptosystem (PKC) using the braid group where the word problem is easy but the conjugacy search problem is intractable. They noted that the usage of braid groups is particular promising. The braid group was first introduced to construct a Diffie-Hellman type key agreement protocol and a public-key encryption scheme at CRYPTO 2000 by Ko. *et al.* [1]. In the recent years many cryptographic protocols based on braid groups have been proposed. In this direction ,there are many positive results such as a construction of pseudorandom number generator by Lee *et al.*in2001 [2], key agreement protocols by Anshel *et al.*in2001 [3], an implementation of braid computations by Cha *et al.* in 2001 [4], digital signature schemes by Ko *et al.*in2002 [5],an entity authentication scheme by Sibert *et al.*in 2002 [6] , a provably-secure identification scheme by Kim *et al.*in 2004 [7] and three group signature schemes by Thomas *et al.*in 2006 [8]. However, to the best of our knowledge, there is no designated verifier group signature scheme based on both conjugacy search problem and root problem over braid groups in the open literitures.

1.2 Designated Verifier Group Signature Scheme

A designated verifier signature scheme is a signature scheme in which signature can only be verified by a single designated verifier chosen by the signer. This concept was first introduced by Jakobsson SaKo and Impayliazzo at Eurocrypt 96 [10]. In a designated verifier group signature scheme, any member of the group can sign a message on behalf of the group, the designated verifier can check whether the signer come from the group or not but cannot identify the actual signer, and only the designated verifier can verify the valid signature.

Designated verifier signatures are very useful in various situations . Let us consider the following example. Supposed that a public institution initiates a call for tenders, asking some companies to propose their prices for a set of instruments and tasks to be accomplished. The institution may require the companies to sign their offers in order to make sure that they are actually authentic and originated from whom they claim to be. But no company involved in this process desires its offer to affect other tenders' decisions. That is, a company may capture a competitor's signed offer on the transmission line (to the institution) and prepares its offer consequently in order to increase its chance to be selected by the institution. To prevent this, the companies may obviously encrypt their offers and signatures in order that they may only be read and verified by the institution. But nothing prevents the latter to reveal them once decrypted. Indeed, since the institution's goal is to obtain a good price (as low as possible). It could show some signed offers to some other companies to influence them in making "good" offers. Designated verifier signature is a solution to this problem. With such signatures, while the institution is convinced about the origin and the authenticity of an offer, it cannot transfer this conviction to others unless it reveal its own secret key used in verification.

1.3 Our Contribution

In this paper, we construct a designated verifier signature scheme based on both the conjugacy search problem(CSP)and root problem(RP)over a braid group. We prove this scheme is secure against active attack if the CSP and RP is intractable. In this scheme, only the designated verifier can recover the message and verify the signature, non-designated verifiers neither recover the message nor verify the signature unless they gain the secret key of the designated verifier. The designated verifier can check whether the signer is a valid group member or not, but he cannot identify the actual signer. The trust authority (T) knows the secret keys of all members, but he cannot forge signatures . In our scheme, T can identify the signer easily in case of a dispute. Furthermore, the opponent cannot operate the existential forgery under chosen message attack. Our proof is based on the fact that CSP and RP is hard in braid groups.

1.4 Outline of Paper

The rest of this paper is organized as follows: in section 2 ,we state some preliminaries , in section 3 we present our group signature scheme, in section 4, we state our definition of security and give a proof of security. Finally, we end with the conclusion.

2 Preliminaries

2.1 Braid Groups: The n-braid group is presented by the Artin generators $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ and relations

$$\sigma_i \sigma_j = \sigma_j \sigma_i \qquad |i-j| > 1$$

$$\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \qquad |i-j| = 1$$

Thus an n-braid b can be written as a word of$\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ and the word-length of b is the number of letters in a word equivalent to b. A positive braid is characterized by the fact that at each crossing point the string going from left to right undercrosses the string going from right to left. A positive braid is called a permutation braid if any two of its strings cross at most once. The braid

$$\triangle = (\sigma_1 \sigma_2 \ldots \sigma_{n-1})(\sigma_1 \sigma_2 \ldots \sigma_{n-2}) \ldots (\sigma_1 \sigma_2)\sigma_1$$

is called the fundamental braid. Permutation braids are subwords of the fundamental braid and the set of all permutation braids is one to one correspondence with the set S_n of permutations on $\{1, 2, \dots, n\}$, thus a permutation braid can be denoted by a permutation $\pi : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$, for example, the fundamental braid is the permutation sending i to $n - i$.

For two braids v and w in B_n, we say that $v \leq w$, if $w = avb$, a and b are positive braids. A braid b satisfying $e \leq b \leq \triangle$ is called a canonical factor. For a positive braid P, we say that the decomposition $P = A_0 P_0$ is left-weighted if A_0 is a canonical factor, $P_0 \geq e$, and A_0 has the maximal word length among all such decompositions. A left-weighted decomposition$P = A_0 P_0$ is unique, any braid x can be uniquely decomposed as $x = \triangle^u A_1 A_2 \dots A_p$, where $u \in \mathbf{Z}$, $A_i (\neq e, \triangle)$ is a canonical factor and the decomposition $A_i A_{i+1}$ is left-weighted for each $1 \leq i \leq p-1$. This unique decomposition is called the left canonical form of x and it solved the word problem. Since each canonical factor corresponds to a permutation braid, x can be denoted as $x = \pi_{\triangle}^u \pi_1 \pi_2 \dots \pi_p$ uniquely. Hence for implementation purposes the braid x can be represented as the triple $(u, \pi_1, \pi_2, \dots, \pi_p)$ which can be processed by the computer.

We use the following hard problems in our signature scheme:

1 Conjugacy Search Problem (CSP)

Let $(x, y) \in B_n \times B_n$, such that $y = axa^{-1}, a \in B_m, m \leq n$. The conjugacy search problem is to find a braid $b \in B_m$, such that $y = bxb^{-1}$.

Although CSP in the braid group B_n is solvable, it believed to be infeasible as the braid index n increases, all the known attacks need exponential time to computer a from the data (axa^{-1}, x).

2 Root Problem (RP)

Let$(x, y) \in B_n \times B_n$, such that $y = x^c, c \in N, c \geq 2, N$ denotes the set of all positive integers. The root extraction problem (for the exponent c) is to find a braid $b \in B_n$, such that $y = b^c, c \in N, c \geq 2$.

2.2 Cryptographic Assumption

In our scheme, we consider the braid group B_{2n} generated by $\sigma_1, \sigma_2, \cdots, \sigma_{2n-1}$, and its subgroups:

$$LB_{2n} =< \sigma_1, \sigma_2, \cdots, \sigma_{n-1} >, \ RB_{2n} =< \sigma_{n+1}, \sigma_{n+2}, \cdots, \sigma_{2n-1} >$$

The relation of all these groups is defined by

$$\sigma_i \sigma_j = \sigma_j \sigma_i, |i - j| > 1, \qquad \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j, |i - j| = 1$$

Let $h_1 : B_{2n} \rightarrow \{0, 1\}^k$ be an ideal hash function from the braid group to$\{0, 1\}^k$, this function has been used in [1].

Let $h_2 : \{0, 1\}^k \rightarrow B_{2n}$ be an ideal hash function. A way to construct the function is given in [5].

the security of our group signature scheme is based on the difficulty of the following problems.

[Base problem 1]

Instance: The triple (x, y_1, y_2) of elements in B_{2n} such that $y_1 = axa^{-1}$ and $y_2 = bxb^{-1}$ for some hidden $a \in LB_{2n}$and $b \in RB_{2n}$

Objective: Find $by_1b^{-1}(= ay_2a^{-1} = abxa^{-1}b^{-1})$

Ko.noted in[1]that base problem and CSP seem to have the almost same complexity and this phenomenon is similar to the case of the Diffie-Hellman problem and the discrete logarithm problem.

[Base problem 2]

Instance: Given$(y, c) \in B_{2n} \times N$ such that $y = x^c$ for some hidden $x \in B_{2n}$

Objective: Find x such that $y = x^c$

It is proved in [9] that base problem 2 is decidable but it is computationally infeasible when braids of a sufficient size are considered.

2.3 Attack Model

What a signature scheme is broken means that an adversary succeed in an impersonation attempt (making the verifier accept with non-negligible probability). We consider the scenario: the adversary forge a signature under chosen message attack, and T forge a signature impersonating the signer. We consider the strongest form of the attack: active attack.

3 Our Proposed Scheme

In this section, we present our designated verifier group signature scheme. Let B_{2n} be a braid group such that CSP and RP over it are intractable.

3.1 Key Generation:

(1) The keys of signers:

(a) T (trust authority of the group) chooses a complex enough braid $x_1 \in B_{2n}$. T chooses an integer $c \in N, c \leq 2$ and published them in the open directory.

(b) T chooses a secret key of the group:$a \in LB_{2n}$, computers

$$y_1 = ax_1a^{-1}$$

T sends $y_1 = ax_1a^{-1}$ to all the group members $U_i(i = 1, 2, \ldots, k)$.

(c) Every signer $U_i(i = 1, 2, \ldots, k)$chooses randomly many secret braids $a_{ij} \in RB_{2n}, j = 1, 2, \ldots, l_i$, l_i is chosen by the signer, computers:

$$w_{ij} = a_{ij}x_1a_{ij}^{-1}$$

Then send $(w_{i1}, w_{i2} \ldots, w_{il_i}, U_i)$ to T in a secret channel.
(d)U_i computers: $x_{ij} = a_{ij} y_1 a_{ij}^{-1}, j = 1, 2, \ldots, l_i$ and keeps$\{x_{ij} | j = 1, 2, \ldots, l_i\}$as the secret key that can be used to sign the message.
(e) T computers $x_{ij} = a w_{ij} a^{-1}, j = 1, 2, \ldots, l_i$ for $i = 1, 2, \ldots, k$ and keeps

$$\{(x_{i1}, x_{i2} \ldots, x_{il_i}, U_i) | i = 1, 2, \ldots, k\}$$

so that it can identify the signer in case of a dispute.
(f) T computers $x_{i1}^c, x_{i2}^c \ldots, x_{i1_i}^c, i = 1, 2, \ldots, k$, and publishs the complete list of $\{x_{i1}^c, x_{i2}^c \ldots, x_{i1_i}^c, i = 1, 2, \ldots, k,\}$ in random order in a Trusted Public Directory. Let $x_{ij}^c = y_{ij}$ and the public key of the group is

$$PK_G = \{y_{ij} | i = 1, 2, \ldots, k, j = 1, 2, \ldots, l_i\}$$

(2) The keys of verifiers
Suppose the group of all verifiers is

$$\{V_j | j = 1, 2, \ldots, t, t \geq 1, t \in N\}$$

T chooses a complex enough braid $x_2 \in N^*, x_2 \neq x_1$and publishs it. The verifier$V_j (j \in \{1, 2, \ldots, t\}$chooses randomly a braid $b_j \in LB_{2n}$ such that CSP is intractable in B_{2n} and computers $y_j^{'} = b_j x_2 b_j^{-1}$. V_j carry out a usual identification scheme with T, T accepts $(y_j^{'}, V_j)$ as the public key of the verifier $V_j$and publish it in the Trust Public Directory followed by the identification scheme. V_j keeps b_j as the secret key used in the verification, suppose he never reveal the secret key.
3.2 Sign: $sig(m, PK_s, SK_s, PK_v) = s_m$
Suppose a member $U_i (i \in \{1, 2, \ldots, k\})$ want to sign the message $m \in \{0, 1\}^k$and designates $V_j (j \in \{1, 2, \ldots, t\}$ as the verifier. U_i make use of his secret key $x_{ij} \in \{x_{i1}, x_{i1}, \ldots, x_{il_i}\}$, where each key will be used only once. Without loss of generality, suppose U_i uses x_{i1} and the public key $(y_j^{'}, V_j)$ of $V_j (j \in \{1, 2, \ldots, t\})$. U_i knows a_{i1} which corresponds to the secret key x_{i1}, he computes:

$$\alpha = a_{i1} x_2 a_{i1}^{-1}$$

$$\beta = a_{i1} y_j^{'} a_{i1}^{-1}$$

$$\gamma = h_1(\beta) \oplus m$$

$$\delta = h_2(m) x_{i1}$$

Return the signature of the message m:

$$S_m = (w_{i1}, \alpha, \gamma, \delta)$$

Obviously, the signature conceal the message m.

3.3 Verify: $Ver(PK, SK_v, S_m) = \{accept|reject\}$

Firstly, the designated verifier checks whether $w_{i1}\alpha$ is conjugate to x_1x_2 or not, the Conjugacy Decision Problem (CDP) is feasible, an efficient algorithm has been constructed to solve CDP with overwhelming accuracy in [5]. If $w_{i1}\alpha \sim x_1x_2$, then computers:

$$\beta = b_j\alpha b_j^{-1}, m = h_1(\beta) \oplus \gamma$$

Secondly, the designated verifier checks whether $[h_2(m)^{-1}\delta]^c$be in the public key of the group: PK_G or not. The designated verifier accepts $S_m$as a valid signature if and only if S_m satisfys:

$$[h_2(\gamma \oplus h_1(b_j\alpha b_j^{-1}))^{-1} \cdot \delta]^c = y_{i1} \in PK_G$$

3.4 Completeness:

If the signer U_i follows the signature protocol then V_j always accept $S_m = (w_{i1}, \alpha, \gamma, \delta)$ as a valid signature. Let $S_m = (w_{i1}, \alpha, \gamma, \delta)$ be a valid signature, because $w_{i1} = a_{i1}x_1a_{i1}^{-1}$ and $\alpha = a_{i1}x_2a_{i1}^{-1}$, $w_{i1}\alpha = a_{i1}x_1x_2a_{i1}^{-1} \sim x_1x_2$. Nextly, for $b_j \in LB_{2n}$ and $a_{i1} \in RB_{2n}$, we know $b_ja_{i1} = a_{i1}b_j$. Thus

$$b_j\alpha b_j^{-1} = b_j(a_{i1}x_2a_{i1}^{-1})b_j^{-1} = a_{i1}(b_jx_2b_j^{-1})a_{i1}^{-1} = a_{i1}(y_j^{'})a_{i1}^{-1} = \beta$$

$$h_1(\beta) \oplus \gamma = m$$

and $[h_2(m)^{-1}\delta]^c = [h_2(m)^{-1} \cdot h_2(m)x_{i1}]^c = [x_{i1}]^c = y_{i1} \in PK_G$. The designated verifier accepts $S_m = (w_{i1}, \alpha, \gamma, \delta)$ as a valid signature.

3.5 Open:

In case of dispute, V_j can easily computers $\beta = b_j\alpha b_j^{-1}, m = h_1(\beta) \oplus \gamma$. T uses the equation $\delta = h_2(m)x_{i1}$, he computers $x_{i1} = h_2(m)^{-1}\delta$, he can easily identify the actual signer by $\{(x_{i1}, x_{i2}, \ldots, x_{il}, U_i)|i = 1, 2, \ldots, k\}$.

4 Security Analysis

4.1 Only the designated verifier can verify the signature.

Only the designated verifier can verify the signature, non-designated verifiers cannot verify the signature. Firstly, the designated verifier have secret key b_j, computering: $\beta = b_j\alpha b_j^{-1}, m = h_1(\beta) \oplus \gamma$, then checking whether$[h_2(\gamma \oplus h_1(\beta))^{-1} \cdot \delta]^c = [h_2(m)^{-1} \cdot \delta]^c$ is in PK_G or not to check whether S_m is a valid signature or not. Secondly, if non-designated verifiers want to verify S_m, they must compute m and β. But they do not hold the secret key b_j of the designated verifier. They can obtain $x_2, \alpha = a_{i1}x_2a_{i1}^{-1}, y_j^{'} = b_jx_2b_j^{-1}$, they try to computer $\beta = b_j\alpha b_j^{-1} = a_{i1}y_j^{'}a_{i1}^{-1}$ however, that is equivalent to the **base problem 1**:

Instance: The triple $(x_2, \alpha, y_j^{'})$ of elements in B_{2n} such that $\alpha = a_{i1}x_2a_{i1}^{-1}$ and $y_j^{'} = b_jx_2b_j^{-1}$for some hidden $a_{i1} \in LB_{2n}$and $b_j \in RB_{2n}$

Objective: Find $b_j\alpha b_j^{-1}(= a_{i1}y_j^{'}a_{i1}^{-1} = a_{i1}b_jx_2a_{i1}^{-1}b_j^{-1})$. Thus the computation of β is mathematical difficult because of the previous cryptographic assumption. Then non-designated verifiers can not compute the message, nor carry out the verification.

4.2 The opponent cannot operate existential forgery under chosen message attack.

Firstly, the opponent cannot obtain the secret key x_{ij} of U_i from PK_G form the previous assumption of base problem 2, because root extraction problem is intractable over B_{2n}.

Secondly, suppose that the opponent capture the signature $S_m = (w_{i1}, \alpha, \gamma, \delta)$, and that he want to forge another signature impersonate the actual signer U_i. Because each key used only once , the opponent must choose another secret key of U_i, for example, the opponent Oscar choose $x_{i2}^c \in PK_G$. If he want to compute x_{i2} from $x_{i2}^c \in PK_G$, he must face up with the root extraction problem.

He could forge w_{i2}^* and α^* such that $w_{i2}^*\alpha^* \sim x_1x_2$ firstly, but he do not hold the secret key b_j of the designated verifier and the secret key a_{i2}^* of U_i, so he can not computer $\beta^* = b_j\alpha^*b_j^{-1}$.

Even the opponent conspires with the designated verifier, he computes $\beta^* = b_j\alpha^*b_j^{-1}$ with the secret key b_j of the designated verifier, then compute $\gamma^* = h_1(\beta^*) \oplus m^*$, but he cannot compute $\delta^* = h_2(m^*)x_{i2}^*$ because he do not hold the secret key correspond to $y_{i2}^* \in PK_G$. It is a root extraction problem that compute x_{i2}^* from y_{i2}^*.

Suppose that the opponent try to operate the forgery from the condition of the verification: $[h_2(m)^{-1}\delta]^c \in PK_G$. He want to determine $h_2(m)^{-1}$ and δ such that the condition is satisfied. We consider another scenario: the opponent choose x_{ij} randomly such that $x_{ij}^c \in PK_G$, the probability of success of the former is not greater than that of the latter.

4.3 T knows the secret keys $x_{i1}, x_{i2}, \dots, x_{il_i}$ of any user U_i , but he cannot forge signature .

Because the designated verifier checks whether $w_{ij}\alpha \sim x_1x_2$ or not firstly, T knows: $w_{ij} = a_{ij}x_1a_{ij}^{-1}, j = 1, 2, \dots, l_i$. If he want to compute a_{ij} from the data $(x_1, a_{ij}x_1a_{ij}^{-1}), j = 1, 2, \dots, l_i,$, that is mathematical difficult, because that is a conjugacy search problem. Thus T cannot computer $\alpha(= a_{ij}x_2a_{ij}^{-1})$. Consequently, T cannot create signature impersonating any user U_i.

4.4 The opponent cannot obtain the secret key x_{ij} from the data $(x_1, ax_1a^{-1}, a_{ij}x_1a_{ij}^{-1})$.

Because $x_{ij} = a(a_{ij}x_1a_{ij}^{-1})a^{-1} = a_{ij}(ax_1a^{-1})a_{ij}^{-1}$, it is obviously that this computation is equivalent to base problem 1.

5 Conclusion

In this paper, we constructed a designated verifier group signature based on some hard problems in braid groups. Our scheme is the first in this direction using braid groups. It is open to use hard problems in braid groups for designing more group signature schemes and other cryptographic protocols.

Our signature scheme can conceal the message to be signed, only the designated verifier can recover the message and carry out the verification. We can use it in the bidding in which the bidders want to conceal the content of their offers and empower the institution which initiate a call for tenders to verify the signature. In our signature, the power of the trust authority T is limited, though he knows the secret keys of the signers, he can not create valid signature impersonating the signers.

References

[1] K.H.Ko, S.J.Lee, J.H.Cheon, J.W.Han, J.S.Kang, C.S.Park, New public-key cryptosystem using braid groups, Advances in Cryptology: Proceedings of CRYPTO 2000, Lecture Notes in Computer Science, Springer-Verlag,1880(2000),pp.166-183.

[2] E. K. Lee, S. J. Lee, S. G. Hahn, Pseudorandomness from braid groups, Advances in Cryptology: Proceedings of CRYPTO 2001, Lecture Notes in Computer Science, Springer-Verlag, 2139 (2001), pp. 486-502.

[3] I. Anshel, M. Anshel, B. Fisher, D. Goldfeld, New key agreement protocols in braid group cryptography, Progress in Cryptology- CT-RSA 2001, Lecture Notes in Computer Science, Springer-Verlag, 2020 (2001), pp. 13-27.

[4] J. C. Cha, K. H. Ko, S.J. Lee, J. W. Han, J. H. Cheon, An efficient implementation of braid groups, Advances in Cryptology: Proceedings of ASIACRYPT 2001, Lecture Notes in Computer Science, Springer-Verlag, 2248 (2001), pp.144-156.

[5] K. H. Ko, D. H. Choi, M. S. Cho, J. W. Lee, New signature scheme using conjugacy problem, Available at: http://eprint.iacr.org/2002/168.pdf.

[6] H. Sibert, P. Dehornoy, M. Girault, Entity authentication schemes using braid word reduction, Available at: http://eprint.iacr.org/2002/187.

[7] Z. Kim, K. Kim, Provably-secure identification scheme based on braid groups, SCIS 2004, The 2004 Symposium on Cryptography and Information Security, Sendai, Japan, Jan. 27-30, 2004.

[8] Tony Thomas, Arbind Kumar Lal Group Signature Scheme Using Braid Groups arXiv:cs.CR/0602063 v1 17 Feb 2006.

[9] V.B.Styshnev, The extraction of a root in a braid group. Math.USSR.Izv.13(1979).

[10] M.JaKobssm. K.SaKo and R.Impagliazzo. Designated Verifier Proofs and Their Applications In Ueli Maurer, editor, Advances in Cryptology-EUROCRYPT 1996. volume1070 of Lecture Notes in Computer Science, pages 143-145, Springer-Verlag, May, 1996.