A Certificate Revocable Anonymous Authentication Scheme with Designated Verifier

Keita Emura, Atsuko Miyaji, and Kazumasa Omote

Abstract—In IEEE ISI 2008, an anonymous attribute authentication scheme has been proposed using a self-blindable certificate scheme. This scheme enables the anonymity and certificate revocation. A Certificate Revocation List (CRL) is used in the revocation check. Even if an attacker can obtain a CRL, the attacker cannot execute the revocation check. This means that this scheme enables the designated revocation. However, this scheme is not secure, namely, a user can make a forged proof using a public value. In this paper, we propose a certificate revocable anonymous authentication scheme with designated verifier. Our scheme enables the anonymity and certificate revocation. Moreover, our scheme enables a designated verification and revocation.

Index Terms—Anonymous Authentication, Certificate Revocation, Designated Verifier Signature

I. INTRODUCTION

Recently, cryptographic protocols requiring the users’ anonymity have been proposed. In [15], an anonymous attribute authentication scheme has been proposed using a self-blindable certificate scheme [18]. The purpose of this scheme is to apply an attribute authentication with some modules (e.g., mobile phones, smart cards and so on) for some services (a dispenser, a ticket gate, and so on) without exposing any personal information. Therefore, anonymity (which requires the unlinkability between two authentication executions) is indispensable. Entities in this scheme are a user, a Service Provider (SP), and an Attribute Authority (AA). The AA issues an attribute certificate for a user. Moreover, the AA sends a SP a Certificate Revocation List (CRL) which includes the set of an attribute certificate of a revoked user. First, a user sends a request to a SP. The SP generates a random number, and returns this random value and his public key with the public key certificate PKCSP to the user. The user verifies PKCSP, and sends a proof. The SP verifies whether the user has a valid attributes certificate or not using the public values and the CRL. Moreover, the SP also verifies whether the certificate including the proof has already revoked or not using the SP’s secret key. This means that a previous scheme [15] provides the designated revocation. Even if an attacker can obtain the CRL from the AA, the attacker cannot execute the revocation check. These are the different point of other anonymous authentication schemes. For example, in group signature schemes [1], [3], [5], [14], all entities can verify a group signature. In group signature with verifier-local revocation schemes [5], [14], if an attacker can obtain a CRL, the attacker can execute the revocation check. However, a previous scheme [15] is not secure, namely, a user with the AA’s public key can make a forged proof. This is a serious problem. Moreover, a previous scheme [15] does not provide the designated verification.

In [10], [11], designated verifier signature schemes have been proposed which enables the signer’s anonymity from the view point of a third party. If an attacker can obtain a message and a designated verifier signature, then the attacker cannot determine a signer. On the verification phase, a designated verifier verifies a signature with a message, a public key of a signer and a secret key of the designated verifier. This means that these schemes do not provide the signer’s anonymity from the view point of the designated verifier.

In [7], a designated verifier signature scheme for electronic voting (e-voting) has been proposed. This scheme is based on a linkable ring signature scheme proposed in [12]. The linkability is used to provide the uniqueness for the e-voting. Therefore, this scheme does not provide the unlinkability from the view point of a designated verifier.

In [9], a ring signature scheme with designated linkability has been proposed. A ring signature can only be linked by a designated verifier, although the ring signature remain anonymous from the view point of undesigned verifiers. Therefore, this scheme does not provide the unlinkability from the view point of the designated verifier.

Some revocable group signature schemes have been proposed [3], [5], [14]. However, these revocable schemes do not provide the designation property.

Our Contribution: In this paper, we propose a certificate revocable anonymous authentication scheme with designated verifier. Our scheme enables the anonymity and certificate revocation. Moreover, our scheme enables a designated verification and revocation.

Organization: The paper is organized as follows. Definitions are given in Section II. A previous work proposed by [15] is
described in Section III. Our scheme is presented in Section I V. Security analysis is performed in Section V.

II. DEFINITIONS

A. Bilinear Groups and Complexity Assumptions

Definition 1: (Bilinear Groups) We use bilinear groups and a bilinear map defined as follows:

1) $G_1$, $G_2$ and $G_3$ are cyclic groups of prime order $p$.
2) $P$ and $Q$ are generators of $G_1$ and $G_2$, respectively.
3) $e$ is an efficiently computable bilinear map $e: G_1 \times G_2 \rightarrow G_3$ with the following properties:
   - Bilinearity: for all $P, P' \in G_1$ and $Q, Q' \in G_2$, $e(P, Q) = e(P, Q')e(P', Q) = e(P', Q)e(P, Q')$.
   - Non-degeneracy: $e(P, Q) \neq 1_{G_3}$ ($1_{G_3}$ is the $G_3$'s unit).

Our scheme is based on the Discrete Logarithm (DL), Computational Diffie-Hellman (CDH), $q$-Strong Diffie-Hellman (q-SDH) [2], and Symmetric eXternal Diffie-Hellman (SXDH) [1], [4] assumptions. For the security parameter $k$, let $\epsilon = \epsilon(k)$ be a negligible function, namely for every polynomial $poly()$ and sufficiently large $k$, $\epsilon(k) < 1/\text{poly}(k)$.

Definition 2: (DL assumption) The DL problem in $G_1$ is defined as follows: given a tuple $(Q = \xi Q', Q'' \in G_1^2$ as input, where $\xi \in Z_p$, which outputs a value $\xi$. An algorithm $A$ has advantage $\epsilon$ in solving the DL problem in $G_1$ if $Pr[A(Q, Q') = \xi] \geq \epsilon$. We say that the DL assumption holds in $G_1$ if no PPT algorithm has an advantage of at least $\epsilon$ in solving the DL problem in $G_1$.

Definition 3: (q-SDH assumption) The q-SDH problem in $(G_1, G_2)$ is defined as follows: given a tuple $(P, Q, Q', \cdots, Q^e) \in G_1$ as input, where $P \in G_1$, $Q \in G_2$ and $\xi \in Z_p$, which outputs a tuple $\xi$ as a result. An algorithm $A$ has an advantage $\epsilon$ in solving the q-SDH problem in $(G_1, G_2)$ if $Pr[A(P, Q, Q', \cdots, Q^e) = (x, x)] \geq \epsilon$. We say that the q-SDH assumption holds in $(G_1, G_2)$ if no PPT algorithm has an advantage of at least $\epsilon$ in solving the q-SDH problem in $(G_1, G_2)$.

Definition 4: (SDH assumption) The CDH problem in $G_2$ is as follows: given a tuple $(Q, uQ, vQ) \in G_2^3$ as input, where $Q \in G_2$ and $u, v \in Z_p^*$, which outputs $uvQ$. An algorithm $A$ has an advantage $\epsilon$ in solving the CDH problem in $G_2$ if $Pr[A(Q, uQ, vQ) = uvQ] \geq \epsilon$. We say that the CDH assumption holds in $G_2$ if no PPT algorithm has an advantage of at least $\epsilon$ in solving the CDH problem in $G_2$.

Definition 5: (DDH assumption) The DDH problem in $G_2$ is as follows: given a tuple $(Q, Q', uQ, vQ')$ as input, where $Q, Q' \in G_2$ and $u, v \in Z_p^*$, which outputs 1 if $u = v$ or 0 otherwise. An algorithm $A$ has an advantage $\epsilon$ in solving the DDH problem in $G_2$ if $Pr[A(Q, Q', uQ, vQ') = 1] \geq \epsilon$. We say that the DDH assumption holds in $G_2$ if no PPT algorithm has an advantage of at least $\epsilon$ in solving the DDH problem in $G_2$.

Definition 6: (SXDH assumption) Let $(G_1, G_2)$ be a bilinear group. The SXDH assumption requires that the DDH problem is hard in both $G_1$ and $G_2$. This implies that the efficiency computable isomorphisms $\psi: G_2 \rightarrow G_1$ and $\psi^{-1}: G_1 \rightarrow G_2$ do not exist.

Note that the SXDH assumption is a reasonable assumption [4], [8]. We can use a MNT curve [13] implementation, where no efficient isomorphism between $G_1$ to $G_2$ [19].

In this paper, we use the notation according to which, if $S$ is a set, then $x \in R S$ denotes the operation of picking an element $x$ of $S$ uniformly at random.

III. A PREVIOUS WORK

In this section, we show a previous work [15].

A. a previous scheme [15]

Let $(G_1, G_2)$ be a bilinear group, where $G_1 = \langle P \rangle$ and $G_2 = \langle Q \rangle$. Let $z \in Z_p$ be the AA's secret key, $zP$ the AA's public key associated with an attribute, $(x_1, x_2) \in Z_p \times Z_p$ a user's secret key, $(x_1, x_2)P$ a user's public key, $z(x_1 + x_2)P$ a user's attribute certificate, $y \in Z_p$ a SP's secret key, $yP$ a SP's public key, and $PKC_{SP}$ a public key certificate. Note that $x_1$ and $x_2$ are chosen for each user. To simplify, a user index is omitted. A certificate revocation list $CRL = \{Cert_i, RK_i\}$, where $Cert_i = z(x_1 + x_2)P$ and $RK_i = x_1P$. A previous scheme [15] is described in Fig. 1: Note that a bilinear map $e$ is symmetric (namely $G_1 = G_2$) because $e(Cert_i, Sig_i)$, where $Sig_i = f_{x_1}ryP \in G_1$ has to be computed on the revocation check phase. This means the DDH problem on $G_1$ and $G_2$ is easy.

B. Problems of a previous scheme [15]

In this subsection, we show that two problems of a previous scheme [15] as follows:

1) A user with the AA's public key $zP$ can make a forged proof.
2) The DDH problem is easy although the hardness of the DDH problem is required.

The problem 1 is as follows: Let $c = ryP$ be a challenge of a SP. A user with the AA's public key $zP$ and his private key $(x_1, x_2) \in Z_p^2$ selects $f \in R Z_p^*$ and $x_1', x_2' \in R Z_p \setminus \{x_1, x_2\}$, and computes $TPK' = f(x_1' + x_2')P$, $TPCert' = f(zx_1' + x_2')P = fx_1'(zP) + fx_2'(zP)$, $Sig_1' = fx_1'c$ and $Sig_2' = fx_2'c$. Then $\pi = \langle TPK', TPCert', Sig_1', Sig_2'\rangle$ is a valid proof. Moreover, $\pi$ does not be rejected on the revocation check because $(z(x_1' + x_2')P, x_1'P) \notin CRL$. Therefore, any users with the AA's public key $zP$ can make a forged proof. Although the user's secret key $(x_1, x_2)$ is stored on tamper resistant devices such as a self-blindable certificate scheme [18], the probability of $(z(x_1' + x_2')P, x_1'P) \notin CRL$ is non-negligible, where $x_1', x_2' \in R Z_p$.

The problem 2 is as follows: The hardness of the DDH problem is required in [15] (See Section II and IV of [15]). However, the DDH problem is easy in both $G_1$ and $G_2$ because a symmetric pairing is applied.
IV. THE PROPOSED SCHEME

In this section, we propose a certificate revocable anonymous authentication scheme with designated verifier to modify a previous scheme [15].

A. The proposed scheme

Let (G_1, G_2) be a bilinear group, where G_1 = ⟨P⟩ and G_2 = ⟨Q⟩. Let z ∈ Z_p be the AA’s secret key, W = zQ ∈ G_2 the AA’s public key associated with an attribute, x ∈ Z_p a user’s secret key, y ∈ Z_p a user’s attribute certificate, yQ a SP’s secret key, yQ a SP’s public key, PKC_{SP} a public key certificate, H : {0,1}^* → Z_p a hash function, and NIZK a Non-Interactive Zero-Knowledge proof. A certificate revocation list CRL = {Cert_i, RK_i} such that Cert_i = xP for some user and RK_i = αP, where α ∈ Z_p. Note that α is chosen for each user. The attribute certificate yQ is a membership certificate of a group signature scheme proposed in [5]. The proposed scheme is shown in Fig. 2:

The proposed scheme:

1) A user sends a request to a SP.

2) The SP generates a random number r ∈ {0,1}^k, computes c = ryQ and π_r = NIZK{r : c = r(yQ)}, and returns c and his public key yQ with public key certificate PKC_{SP} to the user. Concretely, compute π_r as follows:

a) Select r_r ∈ Z_p.
b) Compute R = r_r(yQ), C = H(yQ, R) and s_r = r_rC.r.
c) π_r = (s_r, C)

3) The user verifies PKC_{SP}.

4) The user verifies π_r as follows:
   a) Compute R' = s_rQ + C(yQ).
   b) Check C = H(yQ, R').

5) The user selects f ∈ Z_p^* and computes T Cert = \frac{f}{\text{Cert}_i}, Sig_1 = fW, Sig_2 = fx_c, Sig_3 = fc and \frac{f}{\text{Cert}_i}, Sig_4 = fP.

6) The user sends a proof (T Cert, Sig_1, Sig_2, Sig_3, Sig_4) to the SP.

7) [Verification] : The SP verifies that e(Sig_4, W) = e(P, Sig_1), e(Sig_4, c) = e(P, Sig_3) and e(T Cert, rySig_1 + Sig_2) = e(Sig_4, Sig_3).

8) [Revocation Check] : The SP verifies that e(Cert_i, rySig_1 + Sig_2) = e(RK_i, Sig_3), where \forall (Cert_i, RK_i) ∈ CRL.

Note that both the verification and the revocation check have to be used the SP’s secret key y. Therefore, both the verification and the revocation check are only executed by the designated SP.

B. Efficiency

Our scheme uses pairing computations. Recently, an efficient paring computation on power restricted modules (e.g., mobile phones) has been proposed such as [17]. Let |CRL| = R. Our scheme requires 7 scalar multiplications and 1 multiplication as a user, and 3 scalar multiplications, 1 multiplication and 6 + 2R paring computations as a SP. The computational costs of a SP depends on the number of revoked members R. There is room for argument regarding the revocation costs. This is a common problem concerning some revocable
authentication schemes such as a revocable group signature scheme [5], [14].

V. SECURITY ANALYSIS

In this section, we consider the security of our scheme. The correctness is easy confirmed.

\[ e(Sig_4, W) = e(P, Sig_1) \]  
(1)

\[ e(Sig_4, c) = e(P, Sig_3) \]  
(2)

\[ e(TCert, rySig_1 + Sig_2) = e(Sig_4, Sig_3) \]  
(3)

Equations (1) and (2) obviously hold. In equation (3),

\[ e(TCert, rySig_1 + Sig_2) = e(P, ryf(z + x)Q) = e(\frac{1}{\alpha x^2} P, \alpha P) = e(\frac{1}{\alpha x^2} P, ryfxz + ryfxQ) = e(\frac{1}{\alpha x^2} P, ryfx(z + x)Q) = e(\frac{1}{\alpha x^2} P, ryfxz + ryfxQ) = e(\alpha P, ryfxQ) = e(RK, Sig_3) \]

Next, we discuss the designatnability. Both the verification and the revocation check have to be used the SP’s secret key \( y \). Therefore, both the verification and the revocation check are only executed by the designated SP. If an attacker can compute \( rySig_1 \) from the public values \( ryQ \) and \( Sig_1 \), then the attacker can solve the CDH problem. Therefore, even if an attacker can obtain a CRL from the AA, the attacker cannot execute both the verification and the revocation check.

Next, we discuss the unforgeability. From equations (1) and (2), \( Sig_1 = fW \), \( Sig_4 = fc \) and \( Sig_4 = fP \) for the same \( f \in \mathbb{Z}_p^* \). These are the same forms as the BLS signature scheme [6]. First, an attacker \( A \) attempts to forge \( TCert \).

If \( A \) can compute a forgeable certificate \((x', \frac{1}{\alpha x^2} P') \in \mathbb{Z}_p \times \mathbb{G}_1 \), then \( A \) can solve the q-SDH problem [5]. Second, \( A \) attempts to forge \( Sig_2 \). Let \( TCert = sP \) for \( s \in \mathbb{Z}_p \) chosen by \( A \). \( A \) also selects \( f \in \mathbb{Z}_p^* \) and computes \( Sig_1 = fW \), \( Sig_4 = fc \) and \( Sig_4 = fP \). From the verification equation, \( e(sP, ryfzQ + Sig_2) = e(fP, ryQ) \) and \( e(P, ryfzQ + sSig_2) = e(P, f^2ryQ) \) hold. Then, \( sryfzQ + sSig_2 = f^2ryQ \) and \( Sig_2 = s^{-1}f^2c - fryQ \) hold. So, (TCert, Sig1, Sig2, Sig3, Sig4) is a valid proof, where \( Sig_2 = s^{-1}f^2c - fryQ \).

\( A \) can distinguish whether two signers are same or not from two authentication executions. As group signature schemes [1], [3], [5], [14]. Let \((TCert, Sig_1, Sig_2, Sig_3, Sig_4) = (\frac{1}{\alpha x^2} P, fW, fxc, fP) \) and \((TCert', Sig_1', Sig_2', Sig_3', Sig_4') = (\frac{1}{\alpha x'2} P, fW', fxc', fP) \) be two authentication executions. We set \( t := t' \) and \( \frac{1}{\alpha x^2} := \frac{1}{\alpha x'^2} \). Then \( x = x' \) if and only if \( t \neq t' \).

We set \( fP := P \in \mathbb{G}_1, f'P := P' \in \mathbb{G}_1, fc := Q' \in \mathbb{G}_2 \) and \( f'c' := Q'' \in \mathbb{G}_2 \). If \( A \) can distinguish \( t = t' \) or \( t \neq t' \) from \( (Sig_4, Sig_4', TCert, TCert') = (P, P', tP', t'P') \in \mathbb{G}_1 \).
then $A$ can solve the DDH problem on $G_1$. Similarly, if $A$ can distinguish $x = x'$ or $x \neq x'$ from $(\text{Sig}_1, \text{Sig}_2, \text{Sig}_3, \text{Sig}_4) = (Q', Q'', xQ', x'Q'') \in G_2$, then $A$ can solve the DDH problem on $G_2$. Note that $\text{Sig}_1 = fW$ is not included a user's secret value $x$. Therefore, our scheme satisfies the anonymity under the SXDH assumption.

From these considerations, the proofs containing some reductions can be constructed easily using a sequence of games in the same way as in [16].

VI. CONCLUSION

In this paper, we propose a designated verifier anonymous authentication scheme with certificate revocation. Our scheme can be applied many kind of services. For example, dispensers of alcoholic drinks have to check a customer’s age. Then, a dispenser does not require other information, e.g., name, address and so on. We assume that a membership certificate with an attribute “age” is preserved on a module (e.g., mobile phones, smart cards and so on). Then, these dispensers can verify a customer’s age without exposing extra personal information.

REFERENCES