2009 International Conference on Availability, Reliability and Security

A Certificate Revocable Anonymous Authentication Scheme with Designated Verifier

Keita Emura, Atsuko Miyaji, and Kazumasa Omote

School of Information Science,
Japan Advanced Institute of Science and Technology,
1-1, Asahidai, Nomi, Ishikawa, 923-1292, Japan

Email: {k-emura,miyaji,omote}@jaist.ac.jp

***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 extra 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 PKC_{SP} to the user. The user verifies PKC_{SP}, 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 undesignated 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 is Section II. A previous work proposed by [15] is

978-0-7695-3564-7/09 $25.00 © 2009 IEEE
DOI 10.1109/ARES.2009.146

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) $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ are cyclic groups of prime order p.
2) P and Q are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively.
3) e is an efficiently computable bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$ with the following properties.
   - Bilinearity : for all $P, P' \in \mathbb{G}_1$ and $Q, Q' \in \mathbb{G}_2$, $e(PP', Q) = e(P, Q)e(P', Q)$ and $e(P, QQ') = e(P, Q)e(P, Q')$.
   - Non-degeneracy : $e(P, Q) \neq 1_{\mathbb{G}_3}$ ($1_{\mathbb{G}_3}$ is the $\mathbb{G}_3$'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 $poly(\cdot)$ and for sufficiently large k, $\epsilon(k) < 1/poly(k)$.

Definition 2: (**DL assumption**) The DL problem in $\mathbb{G}_1$ is defined as follows: given a $(Q = \xi Q', Q') \in \mathbb{G}_1^2$ as input, where $\xi \in \mathbb{Z}_p^*$, which outputs a value ξ. An algorithm $\mathcal{A}$ has advantage ϵ in solving the DL problem in $\mathbb{G}_1$ if $\Pr[\mathcal{A}(Q, Q') = \xi] \geq \epsilon$. We say that the DL assumption holds in $\mathbb{G}_1$ if no PPT algorithm has an advantage of at least ϵ in solving the DL problem in $\mathbb{G}_1$.

Definition 3: (**q-SDH assumption**) The q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$ is defined as follows: given a $(q+2)$ tuple $(P, Q, \xi Q, \cdots, \xi^q Q)$ as input, where $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ and $\xi \in \mathbb{Z}_p^*$, which outputs a tuple $(x, \frac{1}{(\xi+x)}Q)$, where $x \in \mathbb{Z}_p^*$. An algorithm $\mathcal{A}$ has an advantage ϵ in solving the q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$ if $\Pr[\mathcal{A}(P, Q, \xi Q, \cdots, \xi^q Q) = (x, \frac{1}{(\xi+x)}Q)] \geq \epsilon$. We say that the q-SDH assumption holds in $(\mathbb{G}_1, \mathbb{G}_2)$ if no PPT algorithm has an advantage of at least ϵ in solving the q-SDH problem in $(\mathbb{G}_1, \mathbb{G}_2)$.

Definition 4: (**CDH assumption**) The CDH problem in $\mathbb{G}_2$ is as follows: given a tuple (Q, uQ, vQ) as input, where $Q \in \mathbb{G}_2$ and $u, v \in \mathbb{Z}_p^*$, which outputs uvQ. An algorithm $\mathcal{A}$ has advantage ϵ in solving the CDH problem in $\mathbb{G}_2$ if $|\Pr[\mathcal{A}(Q, uQ, vQ) = uvQ]| \geq \epsilon$. We say that the CDH assumption holds in $\mathbb{G}_2$ if no PPT algorithm has an advantage of at least ϵ in solving the CDH problem in $\mathbb{G}_2$.

Definition 5: (**DDH assumption**) The DDH problem in $\mathbb{G}_2$ is as follows: given a tuple (Q, Q', uQ, vQ') as input, where $Q, Q' \in \mathbb{G}_2$ and $u, v \in \mathbb{Z}_p^*$, which outputs 1 if $u = v$ or 0 otherwise. An algorithm $\mathcal{A}$ has advantage ϵ in solving the DDH problem in $\mathbb{G}_2$ if $|\Pr[\mathcal{A}(Q, Q', uQ, uQ') = 0] - \Pr[\mathcal{A}(Q, Q', uQ, vQ') = 0]| \geq \epsilon$. We say that the DDH assumption holds in $\mathbb{G}_2$ if no PPT algorithm has advantage at least ϵ in solving the DDH problem in $\mathbb{G}_2$.

Definition 6: (**SXDH assumption**) Let $(\mathbb{G}_1, \mathbb{G}_2)$ be a bilinear group. The SXDH assumption requires that the DDH problem is hard in both $\mathbb{G}_1$ and $\mathbb{G}_2$. This implies that the efficiency computable isomorphisms $\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ and $\psi^{-1} : \mathbb{G}_1 \rightarrow \mathbb{G}_2$ 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 $\mathbb{G}_1$ to $\mathbb{G}_2$ [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 $(\mathbb{G}_1, \mathbb{G}_2)$ be a bilinear group, where $\mathbb{G}_1 = \langle P \rangle$ and $\mathbb{G}_2 = \langle Q \rangle$. Let $z \in \mathbb{Z}_p$ be the AA's secret key, zP the AA's public key associated with an attribute, $(x_1, x_2) \in \mathbb{Z}_p \times \mathbb{Z}_p$ 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, $y \in \mathbb{Z}_p$ 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 $RK_i = x_1 P$. A previous scheme [15] is described in Fig. 1: Note that a bilinear map e is symmetric (namely $\mathbb{G}_1 = \mathbb{G}_2$) because $e(Cert_i, Sig_1)$, where $Sig_1 = fx_1 ryP \in \mathbb{G}_1$ has to be computed on the revocation check phase. This means the DDH problem on $\mathbb{G}_1$ and $\mathbb{G}_2$ are 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 $c = ryP$ is a challenge of a SP. A user (with the AA's public key zP and his private key $x_1, x_2 \in \mathbb{Z}_p$) selects $f \in_R \mathbb{Z}_p^*$ and $x_1', x_2' \in_R \mathbb{Z}_p \setminus \{x_1, x_2\}$, and computes $TPK' = f(x_1' + x_2')P$, $TCert' = fz(x_1' + x_2')P = fx_1'(zP) + fx_2'(zP)$, $Sig_1' = fx_1'c$ and $Sig_2' = fx_2'c$. Then $\pi = (TPK', TCert', Sig_1', Sig_2')$ is a valid proof. Moreover, π 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 prover'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 $x_1', x_2' \in_R \mathbb{Z}_p$.

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 $\mathbb{G}_1$ and $\mathbb{G}_2$ because a symmetric pairing is applied.

User:		**SP:**
$x_1, x_2, (x_1+x_2)P, z(x_1+x_2)P, zP$		y, yP, PKC_{SP}, zP, CRT
		$r \in_R \{0,1\}^k$
	$\underleftarrow{r, yP, PKC_{SP}}$	
Verify PKC_{SP}		
$c \leftarrow ryP$		
$f \in_R \mathbb{Z}_p^*$		
$TPK \leftarrow f(x_1+x_2)P$		
$TCert \leftarrow fx(x_1+x_2)P$		
$Sig_1 \leftarrow fx_1 c$		
$Sig_2 \leftarrow fx_2 c$		
	$\underline{TPK, TCert, Sig_1, Sig_2}$	
		(1) Verification
		$e(TPK, zP) \stackrel{?}{=} e(TCert, P)$
		$c' \leftarrow ryP$
		$e(Sig_1, P)e(Sig_2, P) \stackrel{?}{=} e(TPK, c')$
		(2) Revocation Check
		For $^{\forall}(Cert_i, RK_i) \in CRL$ **do**
		$e(Cert_i, Sig_1) \stackrel{?}{=} e(TCert, ryRK_i)$

Fig. 1. A previous scheme [15]

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 $(\mathbb{G}_1, \mathbb{G}_2)$ be a bilinear group, where $\mathbb{G}_1 = \langle P \rangle$ and $\mathbb{G}_2 = \langle Q \rangle$. Let $z \in \mathbb{Z}_p$ be the AA's secret key, $W = zQ \in \mathbb{G}_2$ the AA's public key associated with an attribute, $x \in \mathbb{Z}_p$ a user's secret key, $\frac{1}{z+x}P$ a user's attribute certificate, $y \in \mathbb{Z}_p$ a SP's secret key, yQ a SP's public key, PKC_{SP} a public key certificate, $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$ a hash function, and $NIZK$ a Non-Interactive Zero-Knowledge proof. A certificate revocation list $CRL = \{Cert_i, RK_i\}$ such that $Cert_i = \frac{\alpha}{z+x}P$ for some user and $RK_i = \alpha P$, where $\alpha \in_R \mathbb{Z}_p^*$. Note that α is chosen for each user. The attribute certificate $\frac{1}{z+x}P$ 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 $r \in \{0,1\}^k$, computes $c = ryQ$ and $\pi_r = NIZK\{(r) : c = r(yQ)\}$, 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 $r_r \in_R \mathbb{Z}_p^*$.
   b) Compute $R = r_r(yQ)$, $C = H(yQ, R)$ and $s_r = r_r - Cr$.
   c) $\pi_r = (s_r, C)$
3) The user verifies PKC_{SP}.
4) The user verifies π_r as follows:
   a) Compute $R' = s_r Q + C(yQ)$.
   b) Check $C \stackrel{?}{=} H(yQ, R')$.
5) The user selects $f \in_R \mathbb{Z}_p^*$, and computes $TCert = \frac{f}{z+x}P$, $Sig_1 = fW$, $Sig_2 = fxc$, $Sig_3 = fc$ and $Sig_4 = fP$.
6) The user sends a proof $(TCert, Sig_1, Sig_2, Sig_3, Sig_4)$ to the SP.
7) **[Verification]** : The SP verifies that $e(Sig_4, W) \stackrel{?}{=} e(P, Sig_1)$, $e(Sig_4, c) \stackrel{?}{=} e(P, Sig_3)$ and $e(TCert, rySig_1 + Sig_2) \stackrel{?}{=} e(Sig_4, Sig_3)$.
8) **[Revocation Check]** : The SP verifies that $e(Cert_i, ryWSig_1 + Sig_2) \stackrel{?}{=} e(RK_i, Sig_3)$, where $^{\forall}(Cert_i, RK_i) \in CRL$.

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

User:		**SP:**
$x, \frac{1}{z+x}P, W = zQ$		$y, yQ, PKC_{SP}, W = zQ, CRT$
		$r \in_R \{0,1\}^k$
		$c \leftarrow ryQ$
		$\pi_r \leftarrow NIZK\{(r) : c = r(yQ)\}$
	$\underleftarrow{c, yQ, PKC_{SP}, \pi_r}$	
Verify PKC_{SP}, π_r		
$f \in_R \mathbb{Z}_p^*$		
$TCert \leftarrow \frac{f}{z+x}P$		
$Sig_1 \leftarrow fW$		
$Sig_2 \leftarrow fxc$		
$Sig_3 \leftarrow fc$		
$Sig_4 \leftarrow fP$		
	$\underrightarrow{TCert, Sig_1, Sig_2, Sig_3, Sig_4}$	
		(1) Verification
		$e(Sig_4, W) \stackrel{?}{=} e(P, Sig_1)$
		$e(Sig_4, c) \stackrel{?}{=} e(P, Sig_3)$
		$e(TCert, rySig_1 + Sig_2) \stackrel{?}{=} e(Sig_4, Sig_3)$
		(2) Revocation Check
		For $^{\forall}(Cert_i, RK_i) \in CRL$ **do**
		$e(Cert_i, rySig_1 + Sig_2) \stackrel{?}{=} e(RK_i, Sig_3)$

Fig. 2. The proposed scheme

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.

$$e(Sig_4, W) = e(P, Sig_1) \quad (1)$$

$$e(Sig_4, c) = e(P, Sig_3) \quad (2)$$

$$e(TCert, rySig_1 + Sig_2) = e(Sig_4, Sig_3) \quad (3)$$

Equations (1) and (2) obviously hold. In equation (3), $e(TCert, rySig_1 + Sig_2) = e(\frac{f}{z+x}P, (ryfz + ryfx)Q) = e(\frac{f}{z+x}P, ryf(z + x)Q) = e(fP, fryQ) = e(Sig_4, Sig_3)$ holds. Similarly, if the prover has already revoked, then $^{\exists}(Cert, RK) = (\frac{\alpha}{z+x}P, \alpha P) \in CRL$ such that $e(Cert, rySig_1 + Sig_2) = e(\frac{\alpha}{z+x}P, (ryfz + ryfx)Q) = e(\frac{\alpha}{z+x}P, ryf(z+x)Q) = e(\alpha P, ryfQ) = e(RK, Sig_3)$ holds.

Next, we discuss the designatability. 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), $Sig_1 = fW$, $Sig_3 = fc$ 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 $\mathcal{A}$ attempts to forge $TCert$. If $\mathcal{A}$ can compute a forge attribute certificate $(x', \frac{1}{z+x'}P) \in \mathbb{Z}_p \times \mathbb{G}_1$, then $\mathcal{A}$ can solve the q-SDH probrem [5]. Second, $\mathcal{A}$ attempts to forge Sig_2. Let $TCert = sP$ for $s \in_R \mathbb{Z}_p$ chosen by $\mathcal{A}$. $\mathcal{A}$ also selects $f \in_R \mathbb{Z}_p^*$, and computes $Sig_1 = fW$, $Sig_3 = fc$ and $Sig_4 = fP$. From the verification equation, $e(sP, ryfzQ + Sig_2) = e(fP, fryQ)$ and $e(P, sryfzQ + sSig_2) = e(P, f^2ryQ)$ hold. Then, $sryfzQ + sSig_2 = f^2ryQ$ and $Sig_2 = s^{-1}f^2c - fryzQ$ hold. So, ($TCert$, Sig_1, Sig_2, Sig_3, Sig_4) is a valid proof, where $Sig_2 = s^{-1}f^2c - fryzQ$. c is given by a verifier, and (s, f) is chosen by the attacker. However, $ryzQ$ cannot compute from $c = ryQ$ and $W = zQ$ under the hardness of the CDH problem. Moreover, any private values are not exposed from public values included authentication execution transcripts under the hardness of the DL problem.

Next, we discuss the anonymity. The anonymity requires that an adversary $\mathcal{A}$ cannot distinguish whether two signers are same or not from two authentication executions. This requiremnet is the same as group signature schemes [1], [3], [5], [14]. Let $(TCert, Sig_1, Sig_2, Sig_3, Sig_4) = (\frac{f}{z+x}P, fW, fxc, fP)$ and $(TCert', Sig_1', Sig_2', Sig_3', Sig_4') = (\frac{f'}{z+x'}P, f'W, f'x'c', f'P)$ be two authentication executions. We set $\frac{1}{z+x} := t$ and $\frac{1}{z+x'} := t'$. Then $x = x'$ if and only if $t = t'$. 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 $\mathcal{A}$ can distinguish $t = t'$ or $t \neq t'$ from $(Sig_4, Sig_4', TCert, TCert') = (P', P'', tP', t'P'') \in \mathbb{G}_1^4$,

then $\mathcal{A}$ can solve the DDH problem on $\mathbb{G}_1$. Similarly, if $\mathcal{A}$ can distinguish $x = x'$ or $x \neq x'$ from $(Sig_3, Sig_3', Sig_2, Sig_2') = (Q', Q'', xQ', x'Q'') \in \mathbb{G}_2^4$, then $\mathcal{A}$ can solve the DDH problem on $\mathbb{G}_2$. Note that $Sig_1 = fW$ 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

[1] G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros. Practical Group Signatures without Random Oracles Cryptology ePrint Archive: Report 2005/385.

[2] D. Boneh and X. Boyen. Short signatures without random oracles. In *EUROCRYPT 2004*, pages 56–73.

[3] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *CRYPTO 2004*, pages 41–55.

[4] L. Ballard, M. Green, B. de Medeiros, and Fabian Monrose. Correlation-Resistant Storage via Keyword-Searchable Encryption. Cryptology ePrint Archive, Report 2005/417.

[5] D. Boneh and H. Shacham. Group signatures with verifier-local revocation. In *ACM CCS 2004*, pages 168–177.

[6] D. Boneh, B. Lynn, and H. Shacham. Short signatures from theWeil pairing. Journal of Cryptology, 17(4):297–319, 2004. Extended abstract in Proceedings of Asiacrypt 2001, LNCS volume 2248.

[7] G. Chen, C. Wu, W. Han, X. Chen, H. Lee, and K. Kim. A New Receipt-Free Voting Scheme Based on Linkable Ring Signature for Designated Verifiers. In *International Conference on Embedded Software and Systems Symposia, ICESS 2008.*, pages 18–23.

[8] S. D. Galbraith and V. Rotger. Easy decision Diffie-Hellman groups. Journal of Computation and Mathematics, pages 201–218, 2004.

[9] J. K. Liu, W. Susilo, and D. S. Wong. Ring Signature with Designated Linkability. In International Workshop on Security, IWSEC 2006, pages 104–119.

[10] F. Laguillaumie and D. Vergnaud. Designated Verifier Signatures: Anonymity and Efficient Construction from Any Bilinear Map. In *Security and Cryptography for Networks, SCN 2004*, pages 105–119.

[11] F. Laguillaumie and D. Vergnaud. Multi-designated verifiers signatures: anonymity without encryption. In *Information Processing Letters, v.102 n.2-3, pages 127–132, 2007*

[12] J. Liu, V. Wei, and D. Wong. Linkable spontanrous anonymous group signature for ad hoc group (extended abstract). In *Australasian Conference on Information Security and Privacy, ACISP 2004*, pages 325–335.

[13] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for fr-reduction. *IEICE transactions*, 84(5):1234–1243, 2001.

[14] T. Nakanishi and N. Funabiki. A short verifier-local revocation group signature scheme with backward unlinkability. In *International Workshop on Security, IWSEC 2006*, pages 17–32.

[15] S. Kiyomoto and T. Tanaka. Anonymous Attribute Authentication Scheme Using Self-Blindable Certificates. IEEE Intelligence and Security Informatics, ISI 2008, pages 215–217.

[16] V. Shoup. Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint report 2004/332.

[17] M. Yoshitomi, T. Takagi, S. Kiyomoto, and T. Tanaka. Efficient Implementation of the Pairing on Mobilephones Using BREW. *IEICE transactions*, 91-D(5):1330–1337, 2008.

[18] Eric R. Verheul. Self-Blindable Credential Certificates from the Weil Pairing. *ASIACRYPT 2001*, pages 533–551.

[19] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. J. Cryptology, 17:pages 277–296, 2004.