Analysis of Bilinear Pairing-based Accumulator for Identity Escrowing

Christophe Tartary[1,2] Sujing Zhou[3] Dongdai Lin[3] Huaxiong Wang[1,4]
Josef Pieprzyk[4]

[1]Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Singapore

[2]Institute for Theoretical Computer Science
Tsinghua University
Beijing, 100084
People's Republic of China

[3]SKLOIS Lab, Institute of Software
Chinese Academy of Sciences
100080, Beijing
People's Republic of China

[4]Centre for Advanced Computing - Algorithms and Cryptography
Department of Computing
Macquarie University
NSW 2109 Australia

{zhousujing,ddlin}@is.iscas.ac.cn
{ctartary,HXWang}@ntu.edu.sg
josef@ics.mq.edu.au

Abstract

An accumulator based on bilinear pairings was proposed at CT-RSA'05. In this paper, we first demonstrate that the security model proposed by Lan Nguyen does lead to a cryptographic accumulator which is not collision resistant. Second we show that we can provide collision-resistance by updating the adversary model appropriately. Finally, we propose an improvement on Nguyen's identity escrow scheme with membership revocation based on the accumulator by removing the trusted third party.

Keywords: Bilinear Pairing, Collision Resistance, Cryptographic Accumulators, Identity Escrow, Group Signature.

1 Introduction

A cryptographic accumulator is an algorithm allowing the aggregation of a large set of elements into a single value of constant size. Accumulators were introduced by Belanoh and de Mare [5] in order to design distributed protocols without the presence of a trusted central authority. Such constructions are used in time-stamping [5], fail-stop signatures [4], ring signatures [11] and multicast stream authentication [12] for instance. Camenisch and Lysyanskaya introduced the notion of dynamic accumulators which allow the addition and deletion of values from the original set of elements [8]. In 2005, Nguyen [15] proposed a dynamic accumulator based on bilinear pairings to design ID-based ad-hoc anonymous identification schemes and identity escrow protocols with membership revocation.

In this work, we demonstrate that, contrary to what was claimed in [15], Nguyen's accumulator is not collision resistant. Following his advice [17], we demonstrate how to modify the security model so that collision resistance can be provided. Finally, we prove that it is possible to modify his identity escrow scheme based on the accumulator so that the presence of a trusted third party is not required any longer.

The remainder of this paper is organized as follows. In the next section, we recall the definitions and results from the original paper by Nguyen [15]. In Section 3, we introduce our attack against the collision resistance of Nguyen's accumulator. In Section 4, we demonstrate that the security model modification proposed by Nguyen [17] does lead to a collision resistant accumulator. Finally, we design our improvement on Nguyen's identity escrow scheme in Section 5.

2 Preliminaries

In this section, we recall the definitions and constructions as they appear in Nguyen's paper [15].

2.1 Notations and Terminology

Definition 1 *A function $f : \mathbb{N} \to \mathbb{R}^+$ is said to be negligible if:*

$$\forall \alpha > 0 \, \exists \ell_0 \in \mathbb{N} \, : \, \forall \ell > \ell_0 \quad f(\ell) < \ell^{-\alpha}$$

Definition 2 *A function $f : \mathbb{N} \to \mathbb{R}^+$ is said to be polynomially bounded if:*

$$\exists \alpha_0 > 0 \, : \, \forall \ell \in \mathbb{N} \quad f(\ell) < \ell^{\alpha_0}$$

We denote $\mathbb{Z}_p$ the set of residues $\{0, \ldots, p-1\}$ modulo p. We consider two additive cyclic groups $\mathbb{G}_1 = \langle P_1 \rangle$ and $\mathbb{G}_2 = \langle P_2 \rangle$ as well as a cyclic multiplicative group $\mathbb{G}_{\mathrm{M}}$. These three groups are assumed to have the same prime order p. We assume that we have a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_{\mathrm{M}}$ such that:

1. $\forall (P, Q) \in \mathbb{G}_1 \times \mathbb{G}_2 \; \forall (a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p \quad e(a\,P, b\,Q) = e(P, Q)^{a\,b}$
2. $e(\cdot, \cdot)$ is not degenerated: $e(P_1, P_2) \neq 1$
3. There exists a computationally efficient algorithm to compute $e(P, Q)$ for every couple (P, Q) from $\mathbb{G}_1 \times \mathbb{G}_2$.

As in [15], we consider $\mathbb{G}_1 = \mathbb{G}_2$ (and thus $P_1 = P_2$) in the remainder of this paper. We have the following definition:

Definition 3 *A bilinear pairing instance generator is a probabilistic polynomial-time (PPT) algorithm $\mathcal{G}$ taking as input a security parameter 1^ℓ and returning a uniformly random tuple $\mathbf{t} = (p, \mathbb{G}_1, \mathbb{G}_M, e(\cdot, \cdot), P)$ of bilinear pairing parameters defined as before where ℓ represents the length of the prime number p and $\mathbb{G}_1 = \langle P \rangle$.*

We now present the definition of accumulators and the collision resistance property as set by Nguyen in [15].

Definition 4 ([15]) *An accumulator is a tuple $(\{\mathbf{X}_\ell\}_{\ell \in \mathbb{N}}, \{\mathbf{F}_\ell\}_{\ell \in \mathbb{N}})$, where $\{\mathbf{X}_\ell\}_{\ell \in \mathbb{N}}$ is called the value domain of the accumulator and $\{\mathbf{F}_\ell\}_{\ell \in \mathbb{N}}$ is a sequence of pairs of functions such that each $(f, g) \in \mathbf{F}_\ell$ is defined as $f : \mathbf{U}_f \times \mathbf{X}_f^{ext} \to \mathbf{U}_f$ for some $\mathbf{X}_f^{ext} \supset \mathbf{X}_\ell$ and $g : \mathbf{U}_f \to \mathbf{U}_g$ is a bijective function. In addition, the following properties are satisfied:*

- (Efficient Generation) *There exists an efficient algorithm $\mathcal{G}$ taking as input a security parameter 1^ℓ and outputting a random element (f, g) from $\mathbf{F}_\ell$ possibly together with some auxiliary information a_f.*
- (Quasi-commutativity)$\forall (\ell, (f, g), u, x_1, x_2) \in \mathbb{N} \times \mathbf{F}_\ell \times \mathbf{U}_f \times \mathbf{X}_\ell \times \mathbf{X}_\ell \; f(f(u, x_1), x_2) = f(f(u, x_2), x_1)$. *For any $\ell \in \mathbb{N}, (f, g) \in \mathbf{F}_\ell$ and $\mathbf{X} := \{x_1, \ldots, x_{\mathrm{q}}\} \subset \mathbf{X}_\ell$, we call $g(f(\cdots f(u, x_1) \cdots, x_{\mathrm{q}}))$ the accumulated value of the set $\mathbf{X}$ over u. The element $f(\cdots f(u, x_1) \cdots, x_{\mathrm{q}})$ does not depend on the order of the elements to be evaluated and is denoted $f(u, \mathbf{X})$.*
- (Efficient Evaluation) *For any $(f, g) \in \mathbf{F}_\ell, u \in \mathbf{U}_f$ and $\mathbf{X} \subset \mathbf{X}_\ell$ with polynomially bounded size (as a function of ℓ), $g(f(u, \mathbf{X}))$ is computable in time polynomial in ℓ even without the knowledge of a_f.*

Nguyen set the previous definition to generalize the accumulator constructions by Camenisch and Lysyanskaya [8] and Dodis *et al.* [11] where $\mathbf{U}_f = \mathbf{U}_g$ and the bijective function g is the identity function. Then, he gave the following security definition.

Definition 5 ([15] Collision Resistant Accumulator) *An accumulator is said to be collision resistant if for every* PPT *algorithm $\mathcal{A}$, the function:*

$$\begin{aligned}\mathrm{Adv}_{\mathcal{A}}^{\text{col.acc.}}(\ell) := \quad & \mathrm{Prob}\Big((f, g) \xleftarrow{R} \mathbf{F}_\ell; u \xleftarrow{R} \mathbf{U}_f; (x, w, \mathbf{X}) \leftarrow \mathcal{A}(f, g, \mathbf{U}_f, u) \,| \\ & (\mathbf{X} \subset \mathbf{X}_\ell) \wedge (w \in \mathbf{U}_g) \wedge (x \in \mathbf{X}_f^{\text{ext}} \setminus \mathbf{X}) \wedge (f(g^{-1}(w), x) = f(u, \mathbf{X}))\Big)\end{aligned}$$

is negligible as a function of ℓ. We say that w is a witness for the fact that $x \in \mathbf{X}_\ell$ has been accumulated in $v \in \mathbf{U}_g$ whenever $g(f(g^{-1}(w), x)) = v$.

We now introduce the q-Strong Diffie Hellman (q-SDH) assumption as it was used by Nguyen to claim the security of his construction.

Definition 6 *The q-Strong Diffie Hellman (q-SDH) assumption states that for every* PPT *algorithm $\mathcal{A}$, the function:*

$$\mathrm{Adv}_{\mathcal{A}}^{q\text{-SDH}}(\ell) := \mathrm{Prob}\left(\left(\mathcal{A}(\mathbf{t}, P, s\,P, \ldots, s^{\mathrm{q}}\,P) = \left(c, \tfrac{1}{s+c}\,P\right)\right) \wedge (c \in \mathbb{Z}_p)\right)$$

is negligible as a function of ℓ where $\mathbf{t} = (p, \mathbb{G}_1, \mathbb{G}_M, e(\cdot, \cdot), P) \leftarrow \mathcal{G}(1^\ell)$ and $s \xleftarrow{R} \mathbb{Z}_p^*$.

2.2 Construction of the Accumulator

To generate an instance of the accumulator from the security parameter ℓ, we run the algorithm $\mathcal{G}$ on input 1^ℓ to obtain a tuple **t** and a uniformly chosen element s from $\mathbb{Z}_p^*$ as in Definition 6. We construct a tuple $\mathbf{t}' := (P, s\,P, \ldots, s^{\mathrm{q}}\,P)$ where q is an upper bound on the number of elements to be accumulated. The corresponding functions (f, g) for this instance $(\mathbf{t}, \mathbf{t}')$ are defined as:

$$\begin{array}{rccc} f: & \mathbb{Z}_p \times \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \\ & (v, x) & \longmapsto & (x+s)\,v \end{array} \qquad \begin{array}{rccc} g: & \mathbb{Z}_p & \longrightarrow & \mathbb{G}_1 \\ & v & \longmapsto & v\,P \end{array}$$

This construction involves that we have:

$$\mathbf{U}_f = \mathbf{X}_f^{\text{ext}} = \mathbb{Z}_p \qquad \mathbf{U}_g = \mathbb{G}_1 \qquad \mathbf{X}_\ell = \mathbb{Z}_p \setminus \{-s\}$$

It is clear that f is quasi-commutative. In addition, for $u \in \mathbb{Z}_p$ and a set $\mathbf{X} = \{x_1, \ldots, x_k\} \subset \mathbb{Z}_p \setminus \{-s\}$ where $k \leq q$, the accumulated value $g(f(u, \boldsymbol{X})) = \left(\prod_{i=1}^{k} (x_i + s)\,u\right) P$ is computable in time polynomial in ℓ from the tuple $\mathbf{t}'$ and without the knowledge of the auxiliary information s [15].

We now recall the security theorem demonstrated by Nguyen. Note that it is denoted as Theorem 2 in [15].

Theorem 1 ([15]) *The accumulator related to the pair (f, g) defined above provides collision resistance if the q-*SDH *assumption holds, where q is the upper bound on the number of elements to be accumulated.*

3 Breaking the Collision Resistance

In this section, we construct a PPT algorithm $\mathcal{A}$ which breaks the collision resistance property of the accumulator with non-negligible probability. Since this will contradict the result from Theorem 1, we will then show that the adversary reduction model to the q-SDH assumption given by Nguyen was incorrect.

3.1 Our Attack

Algorithm Construction. According to Definition 5, the adversary is given the functions f and g as well as u and the set $\mathbf{U}_f = \mathbb{Z}_p$. We build the following algorithm:

```
Algorithm $\mathcal{A}$
Input: The pair of functions $(f, g)$ and the value $u$.
1. Compute $s = f(1, 0)$
2. Let $k$ be any polynomial function of $\ell$. Choose uniformly at random $k+1$ elements of $\mathbb{Z}_p \setminus \{-s\}$ denoted $x_1, \ldots, x_k, x$ and set $\mathbf{X} := \{x_1, \ldots, x_k\}$.
3. Compute $\lambda := \prod_{i=1}^{k} (x_i + s)\,u \bmod p$ and $\mu := (x+s)^{-1} \bmod p$. Denote $\xi := \lambda\,\mu \bmod p$ and set $w := g(\xi)$.
Output: The triple $(x, w, X)$.
```

Correctness of the output. Due to Step 2, we have: $\mathbf{X} \subset \mathbf{X}_\ell$ and $x \in \mathbf{X}_f^{\text{ext}} \setminus \mathbf{X}$. From Step 3, we obtain: $w \in \mathbf{U}_g$.

By construction of **X** we have: $f(u, \mathbf{X}) = \prod_{i=1}^{k} (x_i + s)\,u \bmod p$. We also have $\xi = g^{-1}(w)$ since g is invertible. We obtain the following equalities:

$$\begin{array}{rcl} f(\xi, x) & = & (x+s)\,\xi \bmod p \\ & = & (x+s)\,\lambda\,\mu \bmod p \\ & = & (x+s)\,(x+s)^{-1}\,\lambda \bmod p \\ & = & \lambda \bmod p \\ & = & \lambda \\ & = & f(u, \mathbf{X}) \end{array}$$

Therefore, we have: $f(g^{-1}(w), x) = f(u, \mathbf{X})$. In addition, the construction of the triple $(x, w, \mathbf{X})$ is deterministic (the value μ always exists since $x \neq -s$). So, we obtain:

$$\text{Adv}_{\mathcal{A}}^{\text{col.acc.}}(\ell) = 1$$

Running time. First, it should be noticed that any operation (addition, multiplication, inversion) in $\mathbb{Z}_p$ can be done in quadratic time as a function of ℓ [14]. That is, any of these arithmetic operations can be performed in $O(\ell^2)$ bit operations.

Since k is a polynomial function of ℓ, we denote it as $\mathcal{K}(\ell)$. We can also assume that picking one random element from $\mathbb{Z}_p \setminus \{-s\}$ requires polynomial time $\mathcal{R}(\ell)$ (otherwise it would be computationally infeasible to construct a single family of elements from $\mathbb{Z}_p \setminus \{-s\} = \mathbf{X}_\ell$ which is not a realistic assumption). Thus, Step 2 is executed in $(\mathcal{K}(\ell) + 1)\,\mathcal{R}(\ell)$ bit operations.

Since s has been obtained at Step 1 (using $O(\ell^2)$ bit operations), one can get λ with k multiplications and k additions in $\mathbb{Z}_p$ representing $O(\mathcal{K}(\ell)\,\ell^2)$ bit operations. Each of the two elements, μ and ξ, also needs $O(\ell^2)$ bit operations to be computed while g can be run in polynomial time $\mathcal{G}(\ell)$. Therefore, the number of bit operations executed during Step 3 is $O(\mathcal{K}(\ell)\,\ell^2 + \mathcal{G}(\ell))$.

As a consequence, the running time of $\mathcal{A}$ is:

$$O(\ell^2) + (\mathcal{K}(\ell)+1)\,\mathcal{R}(\ell) + O(\mathcal{K}(\ell)\,\ell^2 + \mathcal{G}(\ell)) = O(\mathcal{K}(\ell)\,\mathcal{R}(\ell)\,\ell^2 + \mathcal{G}(\ell))$$

which is polynomial in the security parameter ℓ.

Therefore, $\mathcal{A}$ is a PPT algorithm breaking the collision resistance of the accumulator with non-negligible probability. Thus, the accumulator is not collision resistant. We point out that $\mathcal{A}$ enables to construct many such triples $(x, w, \mathbf{X})$.

3.2 Comments on the Original Security Proof

The issue in [15] is that the adversary is given access to f which enables him to break the computational assumption as follows. According to Definition 6, an adversary trying to break the q-SDH assumption should only be provided with $(\mathbf{t}, P, z\,P, \ldots, z^{\mathrm{q}}\,P)$. Nevertheless, the adversary model of the accumulator (Definition 5) allows to query both f and g. As a consequence, it is easy for the adversary to obtain z by a single query to f as in Step 1 of $\mathcal{A}$. Then, he can compute $(z+c)^{-1}$ mod p in $O(\ell^2)$ bit operations for *any* c. Finally, the adversary runs g on that inverse and obtain $\frac{1}{z+c}\,P$. This means that the adversary can break the q-SDH assumption.

4 Ensuring Collision Resistance

In order to be immune against our attack, Nguyen suggested to allow the adversary the use of the composition $g \circ f$ instead of both f and g [16, 17]. His proposed definition is as follows:

Definition 7 ([16]) *An accumulator is said to be collision resistant if for every* PPT *algorithm $\mathcal{A}$, the function:*

$$\begin{aligned}\mathrm{Adv}_{\mathcal{A}}^{\text{col.acc.}}(\ell) := \quad & \mathrm{Prob}\Big((f,g) \xleftarrow{R} \mathbf{F}_\ell; u \xleftarrow{R} \mathbf{U}_f; (x,w,\mathbf{X}) \leftarrow \mathcal{A}(g \circ f, \mathbf{U}_f, u) \,| \\ & (\mathbf{X} \subset \mathbf{X}_\ell) \wedge (w \in \mathbf{U}_g) \wedge (x \in \mathbf{X}_f^{\text{ext}} \setminus \mathbf{X}) \wedge (f(g^{-1}(w), x) = f(u, \mathbf{X}))\Big)\end{aligned}$$

is negligible as a function of ℓ. We say that w is a witness for the fact that $x \in \mathbf{X}_\ell$ has been accumulated in $v \in \mathbf{U}_g$ whenever $g(f(g^{-1}(w), x)) = v$.

In [15], the issue was that a PPT adversary $\mathcal{A}_{\text{col.acc.}}$ attacking the collision resistance of the accumulator had extra information (namely, a direct access to both f and g) with respect to a PPT adversary $\mathcal{A}_{q\text{-SDH}}$ trying to attack the q-SDH assumption directly. We now demonstrate that it is not the case any longer for the security model based on Definition 7.

Theorem 2 *Let $\mathcal{A}_{\text{col.acc.}}$ be a* PPT *adversary attacking the collision resistance of the accumulator and let $\mathcal{A}_{q\text{-SDH}}$ be a* PPT *adversary attacking the q-*SDH *assumption. Then, both adversaries have the same view of the q-*SDH *assumption.*

Proof.
According to Definition 6, a PPT adversary $\mathcal{A}_{q\text{-SDH}}$ attempting to break the q-SDH assumption is given the elements **t** and **t**′ where:

$$\begin{aligned}\mathbf{t} &= (p, \mathbb{G}_1, \mathbb{G}_{\mathrm{M}}, e(\cdot,\cdot), P) \\ \mathbf{t}' &= (P, s\,P, \ldots, s^{\mathrm{q}}\,P)\end{aligned}$$

According to Definition 7, a PPT adversary $\mathcal{A}_{\text{col.acc.}}$ attempting to break the collision resistance of the accumulator is provided with **t** (representing the construction parameters of the accumulator) as well as **t**″ where:

$$\mathbf{t}'' := (g \circ f, \mathbf{U}_f, u)$$

In the case of Nguyen's construction, we have: $\mathbf{U}_f = \mathbb{Z}_p$. So, we can write:

$$\mathbf{t}'' = (g \circ f, \mathbb{Z}_p, u)$$

We have to demonstrate that $\mathcal{A}_{\text{col.acc.}}$ (initially attacking the collision resistance of the accumulator) does not gain any benefits from receiving $\mathbf{t}'$ (i.e. $\mathcal{A}_{\text{col.acc.}}$ knows $\mathbf{t}, \mathbf{t}'$ and $\mathbf{t}''$) over $\mathcal{A}_{q\text{-SDH}}$ who attacks the q-SDH assumption directly (i.e. $\mathcal{A}_{q\text{-SDH}}$ only knows $\mathbf{t}$ and $\mathbf{t}'$). In other words, we must prove that the extra knowledge $\mathbf{t}''$ does not give $\mathcal{A}_{\text{col.acc.}}$ any advantage with respect to $\mathcal{A}_{q\text{-SDH}}$ when attacking the q-SDH assumption.

First, it should be noticed that $\mathcal{A}_{q\text{-SDH}}$ knows the group $\mathbb{Z}_p$ (second component of $\mathbf{t}'$) since he has knowledge of p as a part of the parameter $\mathbf{t}$.

Second, $\mathcal{A}_{q\text{-SDH}}$ can simulate the black-box $g \circ f$ from $\mathbf{t}$ and $\mathbf{t}'$. Indeed consider $(\mathcal{U}, \mathcal{X})$ from $\mathbb{Z}_p \times \mathbb{Z}_p$. We have:

$$(g \circ f)(\mathcal{U}, \mathcal{X}) = g(f(\mathcal{U}, \mathcal{X})) = (\mathcal{X} + s)\,\mathcal{U}\,P = (\mathcal{X}\,\mathcal{U})\,P + \mathcal{U}\,s\,P$$

Since $(P, s\,P)$ are the first two elements of $\mathbf{t}'$, $\mathcal{A}_{q\text{-SDH}}$ can compute $(g \circ f)(\mathcal{U}, \mathcal{X})$ in polynomial time for any input $(\mathcal{U}, \mathcal{X})$.

It remains to argue about the role of u. Assume that $\mathcal{A}_{\text{col.acc.}}$ designs an oracle $\mathcal{O}(\mathbf{t}, \mathbf{t}', \mathbf{t}'')$. The previous two observations allows us to rewrite this oracle as $\mathcal{O}(\mathbf{t}, \mathbf{t}', u)$. According to Definition 7, u has been chosen uniformly at random from $\mathbb{Z}_p$ and then given to $\mathcal{A}_{\text{col.acc.}}$. Nevertheless, $\mathbb{Z}_p$ is also known to $\mathcal{A}_{q\text{-SDH}}$. Thus, $\mathcal{A}_{q\text{-SDH}}$ can also draw elements uniformly at random from $\mathbb{Z}_p$. As a consequence, the advantage of the algorithm $\mathcal{O}(\mathbf{t}, \mathbf{t}', u)$ is equal to the advantage of the algorithm $\mathcal{O}(\mathbf{t}, \mathbf{t}', v)$ where v has been chosen uniformly at random from $\mathbb{Z}_p$ by $\mathcal{A}_{q\text{-SDH}}$.

Thus, the view of $\mathcal{A}_{\text{col.acc.}}$ (when he is given $\mathbf{t}'$) is identical to the view of $\mathcal{A}_{q\text{-SDH}}$.

□

The previous results shows that $\mathcal{A}_{q\text{-SDH}}$ can simulate the result of any algorithm $\mathcal{A}_{\text{col.acc.}}$ can design (since $\mathcal{A}_{q\text{-SDH}}$ can directly construct $g \circ f$ while u is chosen uniformly at random over the set $\mathbb{Z}_p$ which is also known to $\mathcal{A}_{q\text{-SDH}}$). We can now demonstrate the security of Nguyen's accumulator similarly to [15].

Theorem 3 *If the q-*SDH *assumption holds then the accumulator is collision resistant.*

Proof.
Assume that a PPT adversary $\mathcal{A}$ can break the collision resistance of the accumulator with non-negligible probability. As stated in [15], $\mathcal{A}$ can construct a set $\mathbf{X} = \{x_1, \ldots, x_k\} \subset \mathbb{Z}_p \setminus \{-z\}$, an element $x \in \mathbb{Z}_p \setminus (\mathbf{X} \cup \{-z\})$ and $W \in \mathbb{G}_1$ such that:

$$(x + z)\,W = \left[\prod_{i=1}^{k}(x_i + z)\,u\right] P \tag{1}$$

where the tuple challenge for the q-SDH assumption is $(P, z\,P, \ldots, z^{\mathrm{q}}\,P)$. We will show that the PPT adversary $\mathcal{A}$ can compute $(x, \frac{1}{x+z}\,P)$ with non-negligible probability.

Consider the formal polynomial $f(Z)$ defined as:

$$f(Z) := \sum_{i=0}^{k} f_i\,Z^i = \prod_{i=1}^{k}(x_i + Z)$$

Since $\mathbb{Z}_p[Z]$ is an Euclidean's ring, there exists a (unique) pair $(g(Z), c)$ from $\mathbb{Z}_p[Z] \times \mathbb{Z}_p$ such that: $f(Z) = (x + Z)\,g(Z) + c$. If we write $g(Z)$ as $\displaystyle\sum_{i=0}^{k-1} g_i\,Z^i$ then the previous equality is equivalent to the system:

$$\begin{pmatrix} 1 & x & 0 & 0 & \cdots & 0 \\ 0 & 1 & x & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & x & 0 \\ 0 & \cdots & \cdots & 0 & 1 & x \\ 0 & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} c \\ g_0 \\ \vdots \\ \\ g_{k-2} \\ g_{k-1} \end{pmatrix} = \begin{pmatrix} f_0 \\ \\ \vdots \\ \\ f_{k-1} - x \\ 1 \end{pmatrix}$$

The $(k+1) \times (k+1)$ matrix is invertible. Since the coefficients $f_0, \ldots, f_{k-1}$ only depend on $x_1, \ldots, x_k$, the adversary can compute the value c as well as the coefficients of $g(Z)$. We have:

$$\begin{aligned}(1) \quad &\iff \quad W = [g(z)\,u]\,P + \tfrac{c\,u}{x+z}\,P \\ (1) \quad &\iff \quad \tfrac{1}{x+z}\,P = \tfrac{1}{c}\left(\tfrac{1}{u}\,W - g(z)\,P\right)\end{aligned}$$

Since $k \leq q$, the elements $P, z\,P, \ldots, z^k\,P$ are public. Therefore, the adversary can compute $g(z)\,P$ since:

$$g(z)\,P = \sum_{i=0}^{k-1} g_i\,(z^i\,P)$$

which achieves the proof of construction of $\frac{1}{x+z}\,P$. As a consequence, the PPT adversary $\mathcal{A}$ was able to compute $(x, \frac{1}{x+z}\,P)$ with non-negligible probability which means that $\mathcal{A}$ broke the q-SDH assumption.

□

5 Improvement to Nguyen's Identity Escrow Scheme

In 1991, Chaum and van Heyst introduced group signatures to enable individual members to sign messages on behalf of the whole group [10]. An identity escrow scheme [13] is actually an interactive version of a group signature scheme. We propose an improvement on the modified version of Nguyen's construction as the original scheme was found flawed by Zhang and Chen [19]. Our proposed construction does not require the presence of a trusted third party while keeping the efficiency of the original scheme.

5.1 Design of Nguyen's Identity Escrow Scheme

An identity escrow scheme with membership revocation is a tuple $\mathcal{IE} = (\mathsf{GKg}, \mathsf{UKg}, \mathsf{Join}, \mathsf{Iss}, \mathsf{IEID}_P, \mathsf{IEID}_V, \mathsf{Open}, \mathsf{Judge}, \mathsf{Revoke}, \mathsf{Update}, \mathsf{CheckArchive})$ of polynomial time algorithms, where GKg generates public parameters and secret keys, UKg generates personal public and private keys for users (candidate members), the protocol (Join, Iss) allows a user to join the group and get a membership secret key and a membership certificate, where Join represent the part run by the user, Iss the part run by the *Group Manager* (GM) issuing certificates. The identity escrow's main protocol $\mathsf{IEID} = (\mathsf{IEID}_P, \mathsf{IEID}_V)$ allows a group member to anonymously prove his membership, Open revokes an IEID *transcript* to find the prover and Judge decides if the Open finds the right prover. The details of the notations are referred to [15].

This identity escrow scheme works as follows. Denote ℓ the security value. The construction parameters of the scheme $(p, \mathbb{G}_1, \mathbb{G}_\mathrm{M}, e(\cdot,\cdot), P)$ are obtained by querying the bilinear pairing instance generator $\mathcal{G}$ on input 1^ℓ (Definition 3). We also require the existence of a collision resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p$ [18]. The details can be found in [15].

GKg. A trusted third party uniformly chooses x, s, x' from $\mathbb{Z}_p^*$ and P_0, G, H from $\mathbb{G}_1$. He computes $P_\text{pub} := x\,P, \Theta := e(G,G)^{x'}$ and $Q_\text{pub} := s\,Q$. He publishes the group public key as $\{P, P_0, P_\text{pub}, H, G, \Theta, Q_\text{pub}\}$, and gives the GM the issuing key (x, s) as well as the opening key x'.

(Join, Iss). When a user U_i wants to join the group, he runs an interactive protocol with the GM to obtain his secret key x_i, his identity Δ_i as well as a pair (a_i, S_i) called *certificate*. That is, U_i selects his secret key x_i and sends a committed value $x_i P$ to the GM. The GM calculates $S_i = \frac{1}{x+a_i}(x_i P + P_0)$ and transfers it back to U_i. The detailed description is referred to [15]. These four elements satisfy $e(a_i\,P + P_\text{pub}, S_i) = e(P, x_i\,P + P_0)$ and $\Delta_i = e(P, S_i)$. Suppose the current group accumulated value is V_{j-1}. The GM computes the new accumulated value as $V_j := (a_i + s)\,V_{j-1}$. The witness of U_i is $W_{i,j} := V_{j-1}$.

$(\mathsf{IEID}_P, \mathsf{IEID}_V)$. User U_i computes $E := t\,G$ and $\Lambda := \Delta_i\,\Theta^t$. Then, he can show knowledge of $(a_i, S_i, x_i, W_{i,j})$ such that $e(a_i\,P + P_\text{pub}, S_i) = e(x_i\,P + P_0, P)$ and $e(a_i\,Q + Q_\text{pub}, W_{i,j}) = e(Q, V_j)$.

Open. To open an IEID transcript $(E, \Lambda, \ldots)$, the GM computes $\Delta_i = \Lambda\,e(E,G)^{-x'}$ and a non-interactive zero-knowledge proof of knowledge of x' so that $\Theta = e(G,G)^{x'}$ and $\Lambda/\Delta_i = e(E,G)^{x'}$.

5.2 Our Improvement

The properties an identity escrow (group signature) scheme must exhibit are unforgeability, anonymity, unlinkability, traceability, collision resistance and exculpability [1, 9]. The latter means that neither a group member nor the GM can sign any message on the behalf of another group member. At Asiacrypt'06, Cao [9] proposed an attack breaking the exculpability of the Ateniese-Camenisch-Joye-Tsudik's (ACJT) group signature [1]. In his attack, the GM can forge a valid group signature on the behalf of U_i (for any i) since the GM can intentionally choose $t := \log_{a_0} a$ (see [9] for details). The reader may be aware of a recent reply to Cao by the designers of the ACJT scheme [3]. As they emphasize, the attack by Cao only works when the GM is dishonest and the public parameters not verifiable (which was excluded in their original work [1]).

Consider the case where the scheme parameters are non-verifiable and the GM is untrusted. To reveal the underlying problem of Cao's attack, let's see another attack on the ACJT scheme as follows. Let $\hat{e}$ and $\hat{x}$ be as $\hat{e} := k_1\,\phi(n)$ and $\hat{x} := -t^{-1} + k_2\,\phi(n)$ (for an appropriate selection of k_1, k_2 so that $\hat{e} \in \Gamma$ and $\hat{x} \in \Lambda$, where Γ and Λ are integer intervals defined in [1]). Thus, we have $A_i^{\hat{e}} \equiv 1 \equiv a^{\hat{x}}\,a_0$ mod n where A_i represents the identity of user U_i. The GM can generate group signatures on behalf of U_i using $(\hat{e}, \hat{x})$.

In [15], this attack is not possible since the scheme parameters are set up by a trusted third party who distributes them to the GM. Nonetheless, the security analysis there does not consider the behavior of the trusted third party which, as pointed out in [6], will expose the scheme to unexpected attacks. Intuitively, there may be a simple method to foil such attacks, i.e., to generate public parameters P and P_0 as output of some hash function mapping a binary string to a group element [7]. In this case, however, a security proof of Nguyen's scheme has not been provided. We propose below a simple improvement requiring less calculation than querying such a hash function along with a proof of security. Our idea is to identify user U_i by $x_i\,P$ instead of S_i, as representing U_i by a^{x_i} rather than A_i in the unpublished version of the ACJT scheme [2]. This approach makes the construction resistant against an attack like Cao's.

(Join, Iss). When a user U_i wants to join the group, he runs an interactive protocol with the GM to obtain his secret key x_i, his identity Δ_i as well as a pair (a_i, S_i) called *certificate*. These four elements satisfy $e(a_i\,P + P_{\text{pub}}, S_i) = e(P, x_i\,P + P_0)$ and $\Delta_i = e(P, x_i P)$. Suppose the current group accumulated value is V_{j-1}. The GM computes the new accumulated value as $V_j := (a_i + s)\,V_{j-1}$. The witness of U_i is $W_{i,j} := V_{j-1}$.

(IEID_P, IEID_V). User U_i computes $E := t\,G$ and $\Lambda := \Delta_i\,\Theta^t$. Then, he can show knowledge of $(a_i, S_i, x_i, W_{i,j})$ such that $e(a_i\,P + P_{\text{pub}}, S_i) = e(x_i\,P + P_0, P)$ and $e(a_i\,Q + Q_{\text{pub}}, W_{i,j}) = e(Q, V_j)$. Formally, this proof of knowledge is as below:

$$\begin{aligned}
&PK\{(a_i, x_i, t, r_w, r_s) : \\
&\quad e(P, U_s)^{a_i} e(P, H)^{-r_s a_i} e(P_{pub}, U_s) e(P_{pub}, H)^{-r_s} = e(P, P)^{x_i} e(P_0, P), \\
&\quad e(Q, U_w)^{a_i} e(Q, H)^{-r_w a_i} e(Q_{pub}, U_w) e(Q_{pub}, H)^{-r_w} = e(Q, V_j), \\
&\quad E = tG, \Lambda = e(P, P)^{x_i}\Theta^t, R_w = r_w G, a_i R_w = r_w a_i G, R_s = r_s G, a_i R_s = r_s a_i G\},
\end{aligned}$$

where $U_w = W_{i,j} + r_w H$, $U_s = S_i + r_s H$, $R_w = r_w G$, $R_s = r_s G$, H is also part of the public key.

Here are the details of the construction. In Step 2 (See Page 14, Section 6.1 of [16]) do:

(a) IEID_P generates $r_s, r_w, k_1, k_2, k_3, k_4, k_5, k_6, k_7 \in_R \mathbb{Z}_p$ and computes the following:

$$\begin{aligned}
&U_w = W_{i,j} + r_w H, \quad R_w = r_w G, \quad U_s = S_i + r_s H, \quad R_s = r_s G, \quad T_1 = k_3 G \\
&T_2 = k_1 R_w - k_5 G, \quad T_3 = k_1 R_s - k_7 G, \quad T_4 = k_4 G, \quad T_5 = k_6 G \\
&\Pi_1 = e(P, U_s)^{k_1} e(P, H)^{-k_7} e(P_{pub}, H)^{-k_6} e(P, P)^{-k_2} \\
&\Pi_2 = e(Q, U_w)^{k_1} e(Q, H)^{-k_5} e(Q_{pub}, H)^{-k_4} \\
&\Pi_3 = e(P, P)^{k_2}\Theta^{k_3}
\end{aligned}$$

(b) $\mathsf{IEID}_P \longrightarrow \mathsf{IEID}_V$: $E, \Lambda, U_w, R_w, U_s, R_s, T_1, T_2, T_3, T_4, T_5, \Pi_1, \Pi_2, \Pi_3$.

(c) $\mathsf{IEID}_P \longleftarrow \mathsf{IEID}_V$: $c \in_R \mathbb{Z}_p$.

(d) IEID_P computes in $\mathbb{Z}_p$: $s_1 = k_1 - c a_i$, $s_2 = k_2 - c x_i$, $s_3 = k_3 - ct$, $s_4 = k_4 - c r_w$, $s_5 = k_5 - c r_w a_i$, $s_6 = k_6 - c r_s$, $s_7 = k_7 - c r_s a_i$.

(e) $\mathsf{IEID}_P \longrightarrow \mathsf{IEID}_V$: $s_1, s_2, s_3, s_4, s_5, s_6, s_7$.

(f) IEID_V verifies if the following equalities are satisfied:

$$\begin{aligned}
&T_1 = s_3 G + cE, \quad T_2 = s_1 R_w - s_5 G, \quad T_3 = s_1 R_s - s_7 G \\
&T_4 = s_4 G + c R_w, \quad T_5 = s_6 G + c R_s \\
&\Pi_1 = e(P, U_s)^{s_1} e(P, H)^{-s_7} e(P_{pub}, H)^{-s_6} e(P, P)^{-s_2} [e(P_0, P)/e(P_{pub}, U_s)]^c \\
&\Pi_2 = e(Q, U_w)^{s_1} e(Q, H)^{-s_5} e(Q_{pub}, H)^{-s_4} [e(Q, V_j)/e(Q_{pub}, U_w)]^c \\
&\Pi_3 = e(P, P)^{s_2}\Theta^{s_3}\Lambda^c
\end{aligned}$$

Open. To open an IEID transcript $(E, \Lambda, ...)$, the GM computes $\Delta_i = \Lambda\, e(E, G)^{-x'}$ and a non-interactive zero-knowledge proof of knowledge of x' so that $\Theta = e(G, G)^{x'}$ and $\Lambda/\Delta_i = e(E, G)^{x'}$.

The security of this proof of knowledge is easy to check given two $(s_1, s_2, s_3, s_4, s_5, s_6, s_7, c)$ and $(s'_1, s'_2, s'_3, s'_4, s'_5, s'_6, s'_7, c')$ where $s_i \neq s'_i$ for $i = 1, ..., 7$ and $c' \neq c$.

Lemma 1 *Under the Discrete Logarithm assumption on $\mathbb{G}_1$, the above IEID protocol is an honest-verifier perfect zero-knowledge proof of knowledge of $(a_i, S_i, x_i, W_{i,j}, t)$ that $E = t\,G$ and $\Lambda = e(P, P)^{x_i}\,\Theta^t$, and $e(a_i\,P + P_{pub}, S_i) = e(x_i\,P + P_0, P)$ and $e(a_i\,Q + Q_{pub}, W_{i,j}) = e(Q, V_j)$.*

Proof.
Soundness: The goal is to show that if the protocol accepts with non-negligible probability the proof of knowledge, then a PPT prover must have the knowledge of $(a_i, S_i, x_i, W_{i,j})$ satisfying the stated relations, under the Discrete Logarithm assumption on $\mathbb{G}_1$.

Suppose the protocol accepts for the same commitment $U_w, R_w, U_s, R_s, T_1, T_2, T_3, T_4, T_5, \Pi_1, \Pi_2, \Pi_3$ with two different pairs of challenges and responses $c, s_1, s_2, s_3, s_4, s_5, s_6, s_7$ and $c', s'_1, s'_2, s'_3, s'_4, s'_5, s'_6, s'_7$. Let $f_i = \frac{s_i - s'_i}{c - c'}, i = 1, ..., 7$, then the following equations are obtained according to the verification algorithms of the protocol:

$$f_3 G + E = 0 \tag{2}$$
$$f_1 R_w = f_5 G \tag{3}$$
$$f_1 R_s = f_7 G \tag{4}$$
$$f_4 G + R_w = 0 \tag{5}$$
$$f_6 G + R_s = 0 \tag{6}$$
$$e(P, U_s)^{f_1} e(P, H)^{-f_7} e(P_{pub}, H)^{-f_6} e(P, P)^{-f_2} e(P_0, P)/e(P_{pub}, U_s) = 1 \tag{7}$$
$$e(Q, U_w)^{f_1} e(Q, H)^{-f_5} e(Q_{pub}, H)^{-f_4} e(Q, V_j)/e(Q_{pub}, U_w) = 1 \tag{8}$$
$$e(P, P)^{f_2} \Theta^{f_3} \Lambda = 1 \tag{9}$$

From Equation (2) to Equation (9), we get:

$$E = -f_3 G, \Lambda = e(P, P)^{-f_2} \Theta^{-f_3}. \tag{10}$$

From Equations (3), (4), (5) and (6), we obtain: $-f_1 f_4 G = f_5 G$, $-f_1 f_6 G = f_7 G$. Then:

$$-f_1 f_6 = f_7, \tag{11}$$
$$-f_1 f_4 = f_5 \tag{12}$$

since G is a generator of $\mathbb{G}_1$.

From Equation (7), we get:

$$e(P, -f_1 U_s + f_7 H) e(P_{pub}, f_6 H + U_s) = e(-f_2 P + P_0, P),$$

Applying Equation (11), we obtain:

$$e(-f_1 P + P_{pub}, f_6 H + U_s) = e(-f_2 P + P_0, P), \tag{13}$$

Similarly, from Equation (8) and Equation (12), we get:

$$e(-f_1 Q + Q_{pub}, f_4 H + U_w) = e(Q, V_j). \tag{14}$$

From Equations (10), (13) and (14), it is easy to see that if we set $t = -f_3$, $x_i = -f_2$, $a_i = -f_1$, $S_i = f_6 H + U_s$, $W_{i,j} = f_4 H + U_w$, they satisfy the relations stated in the lemma.

Zero-knowledge: The simulator chooses $c, s_1, s_2, s_3, s_4, s_5, s_6, s_7 \in \mathbb{Z}_p$ and computes

$$T_1 = s_3 G + cE, \quad T_2 = s_1 R_w - s_5 G, \quad T_3 = s_1 R_s - s_7 G$$
$$T_4 = s_4 G + c R_w, \quad T_5 = s_6 G + c R_s$$
$$\Pi_1 = e(P, U_s)^{s_1} e(P, H)^{-s_7} e(P_{pub}, H)^{-s_6} e(P, P)^{-s_2} [e(P_0, P)/e(P_{pub}, U_s)]^c$$
$$\Pi_2 = e(Q, U_w)^{s_1} e(Q, H)^{-s_5} e(Q_{pub}, H)^{-s_4} [e(Q, V_j)/e(Q_{pub}, U_w)]^c$$
$$\Pi_3 = e(P, P)^{s_2} \Theta^{s_3} \Lambda^c$$

It is easy to see that the distribution of the simulation is the same as the distribution of the real transcript.

□

Theorem 4 *The above scheme provides non-frameability under the Discrete Logarithm assumption on* $\mathbb{G}_1$.

Proof.
The corresponding theorem in [15] states that the original Identity Escrow scheme provides non-frameability if the Discrete Logarithm assumption on $\mathbb{G}_1$ holds and the digital signature scheme $(K_s, Sign, Ver)$ is existentially unforgeable against chosen message attack. In our improvement, we simplify the description by omitting the digital signature scheme, whose purpose is to bind (in a non-repudiable manner) the transcript and the identity Δ_i. We just assume this is the case, i.e., $\Delta_i = e(P,P)^{x_i}$ and the transcript are bound together. Then, we proceed to prove that if there is a PPT adversary $\mathcal{A}$ breaking non-frameability of the above scheme, we can construct a PPT adversary $\mathcal{B}$ breaking the Discrete Logarithm assumption over $\mathbb{G}_1$.

Suppose $\mathcal{B}$ is given a challenge $P^* = zP$ randomly chosen from group $\mathbb{G}_1 = \langle P \rangle$. The goal of $\mathcal{B}$ is to calculate z. $\mathcal{B}$ constructs an instance of the above scheme by generating $x, s, x' \in_R \mathbb{Z}_p^*$ and $P_0, G, H \in_R \mathbb{G}_1$ ensuring G is also a generator of $\mathbb{G}_1$. $\mathcal{B}$ gives $\mathcal{A}$ the group public key $\{P, P_0, P_{\text{pub}} = x\,P, H, G, \Theta, Q_{\text{pub}} = s\,Q\}$, the issuing key (x, s) and the opening key x'.

$\mathcal{B}$ simulates a set of possible users $\{1, ..., q\}$ where q is the upper bound on the group size. $\mathcal{B}$ chooses $i^* \in_R \{1, ..., q\}$ and provides $\mathcal{A}$ access to the following simulated oracles the definitions of which can be found in [16]:

- $\mathsf{SndToU}(i, M_{in})$. If $i \neq i^*$, $\mathcal{B}$ just plays as an honest user i by executing Join as specified in M_{in}. If $i = i^*$, $\mathcal{B}$ simulates the (Join, Iss) protocol so that $\Delta_i = e(P, P^*)$.
- WReg, GSig, USK, CrptU, $\mathsf{RevokeU}$, and $\mathsf{Witness}$. $\mathcal{B}$ can simulate all these oracles because the knowledge of the secret keys, except the case when $\mathsf{USK}(i^*)$ is queried.

If $\mathcal{A}$ succeeds with probability ϵ, then the probability that he can impersonate i^* is at least ϵ/q. From the soundness of the protocol (Lemma 1), $\mathcal{B}$ can extract $(a_i, S_i, x_i, W_{i,j}, t)$ so that $E = t\,G$, $\Lambda = e(P, P^*)\Theta^t$, $e(a_i\,P + P_{\text{pub}}, S_i) = e(x_i\,P + P_0, P)$ and $e(a_i\,Q + Q_{\text{pub}}, W_{i,j}) = e(Q, V_j)$, i.e., $z = x_i$.

□

The security properties with regard to anonymity and traceability, as discussed in [15], also hold in the above scheme, because the encryption part and the GM's algorithms are identical.

6 Conclusion

In this work, we first constructed an algorithm breaking the collision resistance of the accumulator as defined in [15]. We showed that the original accumulator security model proposed by Nguyen allowed an adversary to break the q-SDH assumption. Second, we demonstrated that the new security model suggested by Nguyen [17, 16] did not allow the adversary to break the mathematical assumption so that the collision resistance of the accumulator is ensured. Finally, we proved that it possible to remove the trusted third party of Nguyen's identity escrow scheme based on the accumulator while being safe against an attack similar to Cao's.

Acknowledgment

The authors would like to thank Doctor Lan Nguyen for his comments related to the security of his construction. We are grateful to the recommendations from the anonymous reviewers in order to improve the quality of this paper. This work was supported in part by the National Natural Science Foundation of China Grant 60553001, 60673069, the National Basic Research Program of China Grant 2007CB807900, 2007CB807901 and 973 Project of China (No. 2004CB318004). The research of Christophe Tartary and Huaxiong Wang is also partially supported by the Ministry of Education of Singapore under grant T206B2204. Christophe Tartary did some of his work while being a PhD student at Macquarie University where his research was also funded by an iMURS scholarship as well as by the Australian Research Council under ARC Discovery Projects DP0558773 and DP0665035.

References

[1] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *Advances in Cryptology - Crypto'00*, volume 1880 of *Lecture Notes in Computer Science*, pages 255 – 270, Santa Barbara, USA, August 2000. Springer - Verlag.

[2] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. Private communication, March 2006.

[3] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. Remarks on "*Analysis of One Popular Group Signature Scheme*" in asiacrypt 2006. Cryptology ePrint Archive, Report 2006/464, December 2006. Available online at: http://eprint.iacr.org/2006/464.pdf.

[4] Niko Barić and Birgit Pfitzmann. Collision-free accumulators and fail-stop signature schemes without trees. In *Advances in Cryptology - Eurocrypt'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 480 – 494, Konstanz - Germany, May 1997. Springer - Verlag.

[5] Josh Benaloh and Michael de Mare. One-way accumulators: A decentralized alternative to digital signatures. In *Advances in Cryptology - Eurocrypt'93*, volume 765 of *Lecture Notes in Computer Science*, pages 274 – 285, Lofthus, Norway, May 1993. Springer - Verlag.

[6] Alexandra Boldyreva, Marc Fischlin, Adriana Palacio, and Bogdan Warinsch. A closer look at PKI: Security and efficiency. In *PKC 2007*, volume 4450 of *Lecture Notes in Computer Science*, pages 458 – 475, Beijing, China, April 2007. Springer - Verlag.

[7] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In *Advances in Cryptology - Asiacrypt'01*, volume 2248 of *Lecture Notes in Computer Science*, pages 514 – 532, Gold Coast, Australia, December 2001. Springer - Verlag.

[8] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *Advances in Cryptology - Crypto'02*, volume 2442 of *Lecture Notes in Computer Science*, pages 61 – 76, Santa Barbara, USA, August 2002. Springer - Verlag.

[9] Zhengjun Cao. Analysis of one popular group signature scheme. In *Advances in Cryptology - Asiacrypt'06*, volume 4284 of *Lecture Notes in Computer Science*, pages 460 – 466, Shanghai, China, December 2006. Springer - Verlag.

[10] David Chaum and Eugène van Heyst. Group signatures. In *Advances in Cryptology - Eurocrypt '91*, volume 547 of *Lecture Notes in Computer Science*, pages 257 – 265, Brighton, UK, April 1991. Springer - Verlag.

[11] Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous identification in ad hoc groups. In *Advances in Cryptology - Eurocrypt'04*, volume 3027 of *Lecture Notes in Computer Science*, pages 609 – 626, Interlaken, Switzerland, May 2004. Springer.

[12] Chris Karlof, Naveen Sastry, Yaping Li, Adrian Perrig, and J. D. Tygar. Distillation codes and applications to DoS resistant multicast authentication. In *11th Network and Distributed Systems Security Symposium (NDSS)*, San Diego, USA, February 2004.

[13] Joe Kilian and Erez Petrank. Identity escrow. In *Advances in Cryptology - Crypto'98*, volume 1462 of *Lecture Notes in Computer Science*, pages 169 – 185, Santa Barbara, USA, August 1998. Springer-Verlag.

[14] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[15] Lan Nguyen. Accumulators from bilinear pairings and applications. In *Topics in Cryptology CT-RSA 2005*, volume 3376 of *Lecture Notes in Computer Science*, pages 275 – 292, San Francisco, USA, February 2005. Springer - Verlag.

[16] Lan Nguyen. Accumulators from bilinear pairings and applications to id-based ring signatures and group membership revocation (revised version). Available online at: http://eprint.iacr.org/2005/123.pdf, November 2006.

[17] Lan Nguyen. Private communication, November 2006.

[18] Josef Pieprzyk, Thomas Hardjono, and Jennifer Seberry. *Fundamentals of Computer Security*. Springer, 2003.

[19] Fangguo Zhang and Xiaofeng Chen. Cryptanalysis and improvement of an ID-based ad-hoc anonymous identification scheme at CT-RSA 05. Available online at: http://eprint.iacr.org/2005/103.pdf, March 2005.