Cryptanalysis and improvement of an ID-based ad-hoc anonymous identification scheme at CT-RSA 05 ⋆

Fangguo Zhang[1] and Xiaofeng Chen[2]

[1] Department of Electronics and Communication Engineering,
Sun Yat-sen University, Guangzhou 510275, P.R.China
isdzhfg@zsu.edu.cn
[2] Department of Computer Science,
Sun Yat-sen University, Guangzhou 510275, P.R.China
isschxf@zsu.edu.cn

Abstract. An ad-hoc anonymous identification scheme is a new multi-user cryptographic primitive that allows participants from a user population to form ad hoc groups, and then prove membership anonymously in such groups. Recently, Nguyen [11] proposed an ID-based ad-hoc anonymous identification scheme from bilinear pairings. However, in this paper, we propose an attack on Nguyen's ID-based ad-hoc anonymous identification scheme. We show that any one can impersonate a valid group member to perform the anonymous identification protocol successfully. Furthermore, we propose a solution to improve this scheme against our attack.

Keywords: *Bilinear pairings, Ad-hoc anonymous identification, Attack*

1 Introduction

Identification schemes allow a prover (say Alice) to securely identify herself to a verifier (say Bob). Secure identification schemes were introduced by Feige, Fiat and Shamir [9, 7, 8].

In an anonymous group identification scheme, a member A of a group $\mathcal{G}$ can convince B that she is a member of $\mathcal{G}$ without revealing any information about her identity. This is a very useful primitive which enables A to control her privacy while enjoying privileges of the groups. For example, being able to enter an office building by proving that she is an employee while ensuring that her entrance to the building will not be logged. Secure group identification systems have been be designed in [2, 10, 12, 13] using public key cryptography.

Ad-hoc anonymous identification was introduced by Dodos *et al.* at EUROCRYPT 2004 [6]. An ad-hoc anonymous identification scheme is a new multi-user

⋆ This work is supported by the National Natural Science Foundation of China (No. 60403007) and Natural Science Foundation of Guangdong Province, China (No. 04205407).

cryptographic primitive that allows participants from a user population to form ad hoc groups, and then prove membership anonymously in such groups. An accumulator with one-way domain is the main tool in construction of ad-hoc anonymous identification scheme. Dodos *et al.* demonstrated the relationship between the accumulator with one-way domain and ad-hoc anonymous identification scheme by presenting a generic construction based on any accumulator with one-way domain.

Recently, Nguyen [11] proposed a dynamic accumulator scheme from bilinear pairings and used it to construct an ID-based ad-hoc anonymous identification scheme and identity escrow scheme with membership revocation. However, in this paper, we propose an attack on Nguyen's ID-based ad-hoc anonymous identification scheme. We show that any one can impersonate a valid group member to perform the anonymous identification protocol successfully. Furthermore, we propose a proposal to repair this scheme.

The rest of this paper is organized as follows. After introducing bilinear pairings in next section, we review Nguyen's ID-based ad-hoc anonymous identification scheme in brief in Section 3. We propose our attack in Section 4. In section 5, we propose a solution to improve this scheme against our attack. Section 6 concludes the paper.

2 Bilinear Pairings

The bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, are important tools for researching on algebraic geometry. In the last couple of years, the bilinear pairings have been found various applications in cryptography. They can be used to realize some cryptographic primitives that were previously unknown or impractical [1]. More precisely, they are basic tools for construction of ID-based cryptographic schemes [3].

Let $\mathbb{G}_1$ be a cyclic additive group generated by P, whose order is a prime p, and $\mathbb{G}_M$ be a cyclic multiplicative group with the same order p. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_M$ be a bilinear pairing with the following properties:

1. **Bilinearity:** $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1, a, b \in \mathbb{Z}_p^*$;
2. **Non-degeneracy:** There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$, in other words, the map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_1$ to the identity in $\mathbb{G}_M$;
3. **Computability:** There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

We consider the following problems in the additive group $(\mathbb{G}_1; +)$.

– **Discrete Logarithm Problem (DLP):** Given two group elements P and Q, find an integer $n \in \mathbb{Z}_p^*$, such that $Q = nP$ whenever such an integer exists.
– **Computational Diffie-Hellman Problem (CDHP):** For $a, b \in \mathbb{Z}_p^*$, given P, aP, bP, compute abP.

3 Review of Nguyen's ID-based ad-hoc anonymous identification scheme

We first review Nguyen's ID-based ad-hoc anonymous identification scheme in brief using the same notation as [11].

Nguyen's identity-based ad-hoc anonymous identification scheme is defined as a tuple $\mathcal{IA}$ =(**Setup, KeyGen, Make-GPK, Make-GSK,** $\mathbf{IAID_P}$, $\mathbf{IAID_V}$) of PT (polynomial-time) algorithms, which are described as follows.

- **Setup**, on a security parameter l, generates the public parameters $params = (l, t, t', f, g, Q, Q_{pub}, u, \mathcal{H})$, here $t = (p, \mathbb{G}_1, \mathbb{G}_M, e, P)$, $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_M$ is a bilinear pairing and P is a generator of $\mathbb{G}_1$. $t' = (P, P_{pub} = sP, \dots, s^q P)$, where $s \in_R \mathbb{Z}_p^*$ and q is the upper bound on the number of identities to be aggregated. The auxiliary information s can be safely deleted, as it will never be used later. f and g are two functions defined as:
$$f : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \quad f(u, x) \to (x + s)u$$
$$g : \mathbb{Z}_p \to \mathbb{G}_1 \quad g(u) \to uP$$
$Q \in_R \mathbb{G}_1, u, s_m \in_R \mathbb{Z}_p^*$ and $Q_{pub} = s_m Q$. $\mathcal{H}$ is a collision-free function $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_p$. The master key is $mk = s_m$.
- **KeyGen** extracts a private key $s_{id} = R_{id}$ for an identity id as $R_{id} = \frac{1}{\mathcal{H}(id)+s_m}Q$. The user can verifies the private key by checking
$$e(\mathcal{H}(id)Q + Q_{pub}, R_{id}) = e(Q, Q).$$
- **Make-GPK**, given a set of identities $\{id_i\}_{i=1}^k$, computes the set $\mathbf{X}= \{\mathcal{H}(id_i)\}_{i=1}^k$ and generates the group public key for the set $gpk = V = g(f(u, \mathbf{X}))$.
- **Make-GSK** generates the group secret key gsk for a user id and a set of identities $\{id_i\}_{i=1}^k$ by computing the set $\mathbf{X}' = \{\mathcal{H}(id_i)\}_{i=1}^k$, $h_{id} = \mathcal{H}(id_i)$ and the witness $W = g(f(u, \mathbf{X}'))$. The group secret key is $gsk = (h_{id}, s_{id}, W)$.
- ($\mathbf{IAID_P}, \mathbf{IAID_V}$). This protocol **IAID** has the common input $params$ and gpk and the prover (user id) also has gsk. It is a combination of the proof that an identity is accumulated and a proof of knowledge of the user private key corresponding to that identity. The protocol proves the knowledge of (h_{id}, R_{id}, W) satisfying equations $e(h_{id}Q + Q_{pub}, R_{id}) = e(Q, Q)$ and $e(h_{id}P + P_{pub}, W) = e(P, V)$. The details of the identification protocol are shown in Fig. 1.

About the correctness and the security analysis of the scheme, please refer to [11].

4 Cryptanalysis of Nguyen's ID-based ad-hoc anonymous identification scheme

In this section, we propose an attack on Nguyen's ID-based ad-hoc anonymous identification scheme. We show that any one can impersonate a valid group member to perform the anonymous identification protocol successfully. This means that the scheme is totally broken.

$IAID_P$ $\qquad\qquad\qquad\qquad$ $IAID_V$

$r_1, r_2, r_3, r_4, k_1, k_2, k_3, k_4 \in_R \mathbb{Z}_p^*$

$U_1 = r_1(h_{id}Q + Q_{pub}),\ U_2 = r_1^{-1}R_{id}$

$U_3 = r_2U_1 + r_3H,\ S_1 = r_1r_2(h_{id}P + P_{pub});$

$S_2 = (r_1r_2)^{-1}W; T_1 = k_1Q + k_2Q_{pub} + k_3H;$

$T_2 = k_4U_1 + k_3H,\ T_3 = k_1P + k_2P_{pub}$

$\xrightarrow[T_1, T_2, T_3]{U_1, U_2, U_3, S_1, S_2}$

$e(U_1, U_2) \stackrel{?}{=} e(Q,\ Q)$

$e(S_1, S_2) \stackrel{?}{=} e(P,\ V)$

$s_1 = k_1 + cr_1r_2h_{id} \mod p$ $\qquad \xleftarrow{c}$ $\qquad c \in_R \mathbb{Z}_p^*$

$s_2 = k_2 + cr_1r_2 \mod p$

$s_3 = k_3 + cr_3 \mod p$

$s_4 = k_4 + cr_2 \mod p$ $\qquad \xrightarrow{s_1, s_2, s_3, s_4}$

$T_1 \stackrel{?}{=} s_1Q + s_2Q_{pub} + s_3H - cU_3$

$T_2 \stackrel{?}{=} s_4U_1 + s_3H - cU_3$

$T_3 \stackrel{?}{=} s_1P + s_2P_{pub} - cS_1$

Fig. 1. The anonymous identification protocol

Assume that $\mathcal{A}$ is an adversary, who does not have any valid group member's secret key. However, we show that he can impersonate a valid group member to perform the anonymous identification protocol. The details of the attack are described as follows:

The **(Setup, KeyGen, Make-GPK,** and **Make-GSK** are same as above description. For the anonymous identification protocol, $\mathcal{A}$ can impersonate a valid group member to perform it with $IAID_V$ successfully without any secret key as show in Fig. 2.

$IAID_V$ will accept $\mathcal{A}$, this is because:

$$\begin{aligned}
& s_1Q + s_2Q_{pub} + s_3H - cU_3 \\
&= (k_1 + crr')Q + k_2Q_{pub} + (k_3 + cr'')H - c(r'U_1 + r''H) \\
&= k_1Q + k_2Q_{pub} + k_3H + crr'Q + cr''H - c(r'rQ + r''H) \\
&= k_1Q + k_2Q_{pub} + k_3H \\
&= T_1
\end{aligned}$$

$\mathcal{A}$		$IAID_V$
$r, r', r'', k_1, k_2, k_3, k_4 \in_R \mathbb{Z}_p^*$		
$U_1 = rQ,\ U_2 = r^{-1}Q$		
$U_3 = r'U_1 + r''H,\ S_1 = rr'P;$		
$S_2 = (rr')^{-1}V; T_1 = k_1Q + k_2Q_{pub} + k_3H;$		
$T_2 = k_4U_1 + k_3H,\ T_3 = k_1P + k_2P_{pub}$		
	$\xrightarrow[T_1, T_2, T_3]{U_1, U_2, U_3, S_1, S_2}$	$e(U_1, U_2) \stackrel{?}{=} e(Q,\ Q)$
		$e(S_1, S_2) \stackrel{?}{=} e(P,\ V)$
$s_1 = k_1 + crr' \mod p$	$\xleftarrow{\quad c \quad}$	$c \in_R \mathbb{Z}_p^*$
$s_2 = k_2 \mod p$		
$s_3 = k_3 + cr'' \mod p$		
$s_4 = k_4 + cr' \mod p$	$\xrightarrow{s_1, s_2, s_3, s_4}$	$T_1 \stackrel{?}{=} s_1Q + s_2Q_{pub} + s_3H - cU_3$
		$T_2 \stackrel{?}{=} s_4U_1 + s_3H - cU_3$
		$T_3 \stackrel{?}{=} s_1P + s_2P_{pub} - cS_1$

Fig. 2. The impersonation attack

$$\begin{aligned}
&s_4U_1 + s_3H - cU_3 \\
&= (k_4 + cr')U_1 + (k_3 + cr'')H - c(r'U_1 + r''H) \\
&= k_4U_1 + k_3H + cr'U_1 + cr''H - cr'U_1 - cr''H \\
&= k_4U_1 + k_3H \\
&= T_2
\end{aligned}$$

$$\begin{aligned}
&s_1P + s_2P_{pub} - cS_1 \\
&= (k_1 + crr')P + k_2P_{pub} - crr'P \\
&= k_1P + k_2P_{pub} + crr'P - crr'P \\
&= k_1P + k_2P_{pub} \\
&= T_3
\end{aligned}$$

From the above impersonation attack, $\mathcal{A}$ can convince $IAID_V$ that he is a valid group member without any secret key. This means that the scheme is totally broken.

In [11], the author also designs an ID-based ring signature scheme and an identity escrow scheme with membership revocation using his ID-based ad-hoc anonymous identification scheme. Because of the above attack on the ID-based ad-hoc anonymous identification scheme, both the ID-based ring signature scheme and the identity escrow scheme with membership revocation are insecure.

5 Improvements

At the anonymous identification phase, the prover will convince a verifier that she has a valid group certificate without revealing any information about her certificate. The identification protocol proves the knowledge of (h_{id}, R_{id}, W) satisfying the equations $e(h_{id}Q + Q_{pub}, R_{id}) = e(Q, Q)$ and $e(h_{id}P + P_{pub}, W) = e(P, V)$. In Nguyen's ID-based ad-hoc anonymous identification scheme, $\mathbf{IAID_P}$ provides U_1, U_2, U_3, S_1, S_2 to $\mathbf{IAID_V}$ which satisfy $e(U_1, U_2) = e(Q,\ Q)$ and $e(S_1, S_2) = e(P,\ V)$. Meanwhile, $\mathbf{IAID_P}$ provides $\mathbf{IAID_V}$ a proof that he knows the representations of U_3 about Q, Q_{pub} and H, U_3 about U_1 and H, S_1 about P and P_{pub}.

Our attack on Nguyen's ID-based ad-hoc anonymous identification scheme is based on follow facts:

- The commitments $U_1, U_2, U_3, S_1, S_2, T_1, T_2, T_3$ in the anonymous identification phase are not fixed, they can be different and random at each performance.
- Even the representation of U_3 about Q_{pub} is zero, we still can give a proof that we know the representations of U_3 about Q, Q_{pub} and H.

Our attack is due to these facts. To avoid such an attack, a simple solution is to employ a proof that the representation of U_3 about Q_{pub} (and/or S_1 about P_{pub}) is not zero, or it lies in an interval $[1, q-1]$, i.e.,

$$ZKP\{(\alpha, \beta, \gamma)|U_3 = \alpha Q + \beta Q_{pub} + \gamma H \wedge \beta \in [1, p-1]\}.$$

Such protocols can be found at [4, 5].

6 Conclusion

Ad-hoc anonymous identification scheme is a new and very useful cryptographic primitive. In this paper, we propose an attack on Nguyen's ID-based ad-hoc anonymous identification scheme. We show that any one can impersonate a valid group member to perform the anonymous identification protocol successfully. This means that the scheme is broken. Meanwhile, we propose a solution to improve the scheme against our attack.

References

1. P. S. L. M. Barreto, *The Pairing-Based Crypto Lounge*. Available at http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html.
2. D. Boneh and M. Franklin, *Anonymous authentication with subset queries*, In Proceedings of 6th ACM-CCS, pp.73-82. ACM press, 1999.
3. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
4. F. Boudot, *Efficient proofs that a committed number lies in an interval*, Advances in Cryptology-Eurocrypt 2000, LNCS 1807, pp.431-444, Springer-Verlag, 2000.
5. A. Chan, Y. Frankel, and Y. Tsiounis, *Easy come – easy go divisible cash*, Advances in Cryptology-Eurocrypt 1998, LNCS 1403, pp. 561-575, Springer-Verlag, 1998.
6. Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, *Anonymous identification in Ad Hoc groups*, Advances in Cryptology-Eurocrypt 2004, LNCS 3027, pp. 609-626, Springer-Verlag, 2004.
7. U. Feige, A. Fiat, and A. Shamir, *Zero knowledge proofs of identity*, In Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing (STOC'87), pp. 210-217, New York City, 1987.
8. U. Feige, A. Fiat, and A. Shamir, *Zero knowledge proofs of identity*, Journal of Cryptology. 1: 77-94. 1988.
9. A. Fiat and A. Shamir, *How to prove yourself: practical solutions to identification and signature problems*, Advances in Cryptology-Crypto 1986, LNCS 263, pp. 186-194, Springer-Verlag, 1987.
10. C. H. Lee, X. Deng, and H. Zhu, *Design and security analysis of anonymous group identification protocols*, PKC 2002, LNCS 2274, pp. 188-198, Springer-Verlag, 2002.
11. L. Nguyen, *Accumulators from bilinear pairings and applications*, CT-RSA 2005, LNCS 3376, pp. 275-292, Springer-Verlag, 2005.
12. A. D. Santis, G. D. Crescenzo and G. Persiano, *Communication-efficient anonymous group identification*, In Proceedings of 5th Conference on Computer and Communications Security, 1998, pp.73-82. ACM press, 1998.
13. A. D. Santis, G. D. Crescenzo, G. Persiano and M. Yung, *On monotone formula closure of SZK*, in Proceedings of 35th IEEE Symposium on Foundations of Computer Science (FOCS'94), pp.454-465, 1994.