Cryptanalysis of an Anonymous Identity-based Identification Scheme in Ad-Hoc Group without Pairings

Sook Yan Hue[a], Jason Chia[a], Ji-Jian Chin[a]

[a]*Multimedia University Cyberjaya, Malaysia*

Abstract

Anonymous identity-based identification scheme in the ad-hoc group is a multi-party cryptographic primitive that allows participants to form an ad-hoc group and prove membership anonymously in such a group. In this paper, we cryptanalyze an ad-hoc anonymous identity-based identification scheme proposed by Barapatre and Rangan and show that the scheme is not secure against key-only universal impersonation attack. We note that anyone can impersonate as a valid group member to convince the honest verifier successfully, even without knowing the group secret key. Moreover, we proposed a fix on the scheme and provide a security proof for our fixed scheme. The fixed scheme we proposed fulfills the security requirements of an ad-hoc anonymous identity-based identification scheme that are correctness, soundness, and anonymity.

Keywords: anonymity, cryptanalysis, identification protocol

1. Introduction

Identification schemes allow an entity (Prover) who is holding the secret key to show her identity to another entity (Verifier) who is holding the corresponding public key but without leaking her identity. The concept was first introduced by Fiat and Shamir [1] in 1986.

An ad-hoc anonymous identification scheme is a cryptographic primitive first introduced by Dodis *et al.* [2]. The concept of an anonymous identification scheme in an ad-hoc group allows participants to form an ad-hoc group from a user population without the help of a group manager, and is able to prove membership anonymously in such a group. Particularly, this cryptographic primitive allows the user to prove herself that she belongs to the group but without revealing her own identity. In addition, users can enjoy the privileges as one of the group members while protecting the privacy of her identity.

In the year 2005, Nguyen further extended the concept of anonymous identification into an identity-based setting and formalized the construction of the ad-hoc anonymous identity-based identification schemes and its security requirements in [3]. In the same paper [3], Nguyen proposed an instantiation of the ad-hoc anonymous identity-based identification scheme. Later, Zhang and Chen found out a flaw in Nguyen's scheme [3] and proposed a fix towards the scheme in [4]. Subsequently, Nguyen presented a full version of the paper [5] in 2005. Independently, Tartary and Wang [6] proposed a fix on Nguyen's scheme [3] in 2006. In this paper, we consider [3, 4, 5, 6] as the same scheme since they originated from the same paper.

Thereafter, Gu *et al.* [7] proposed an efficient ad-hoc anonymous identity-based identification scheme based on pairings in 2008. In the year 2013, Barapatre and Rangan [8] proposed an ad-hoc anonymous identity-based identification without pairings.

In this paper, we propose an attack on Barapatre and Rangan's ad-hoc group anonymous identity-based identification scheme [8]. We show that anyone who does not belong to the ad-hoc group can impersonate as a valid group member to perform the ad-hoc anonymous identity-based identification protocol successfully. Lastly, we propose a solution to correct this scheme that is provably secure utilizing [8]'s originally defined security model.

1.1. Our Contribution

In this paper, we conduct an attack namely the key only universal impersonation attack on the ad-hoc anonymous identity-based identification scheme proposed by Barapatre and Rangan [8].

We reveal that the scheme is vulnerable against our attack. The adversary can impersonate as a valid group member and able to convince the verifier successfully even without the group secret key. The reason for this problem is because the adversary violates the soundness property in the security proof of the scheme since he can convince an honest verifier with non-negligible probability.

Lastly, we propose a fix to our attack and prove it secure by conducting the relevant modifications on the original security proof.

1.2. Organization

The structure of this paper is organized as follows: The paper begins with the introduction in Section 1. Then, we recall the formal definition and security requirement of identity-based ad-hoc anonymous identification in Section 2. The scheme proposed by Barapatre and Rangan [8] is revisited in Section 3 and the attack conducted towards the scheme is proposed in the same section. Then, the fix is proposed in Section 4. Finally, we conclude our paper in Section 5.

2. Formal Definition and Security Models

We first describe the hardness assumption of RSA problem that used in the scheme proposed by Barapatre and Rangan [8] and the basic concept of standard identification scheme. Then, we recall the formal definition of the ad-hoc anonymous identity-based identification and its security requirement that was formalized by Nguyen [5].

2.1. Rivest-Shamir-Adleman (RSA) Assumption

RSA Generator. $\mathcal{K}_{RSA}(1^k)$ is a RSA-based key generator which returns the tuple (N, e, d) upon invocation where $d = e^{-1} \mod \phi(N)$ and $\gcd(e, \phi(N))$ $= 1$. The generator takes in the security parameter 1^k which determines the size of the prime numbers p and q used to generate the tuple. The RSA problem is defined as given $(N, e, X) \xleftarrow{\$} \mathcal{K}_{RSA}(1^k)$, compute x such that $X = x^d$ mod N where $ed = 1 \mod \phi(N)$.

2.2. Standard Identification

The standard identification scheme is a canonical three-move protocol as defined by Bellare and Palacio [9]. First, Prover $\mathcal{P}$ generates commitment Cmt and sends it as a message to $\mathcal{V}$. Verifier $\mathcal{V}$ selects a challenge Ch uniformly from a random set, called challenge set $ChSet_{\mathcal{V}}$ associated to its input, and sends the challenge to $\mathcal{P}$. Prover $\mathcal{P}$ generates a response Rsp and sends it to $\mathcal{V}$. Lastly, $\mathcal{V}$ deterministically outputs a value $d \leftarrow Veri(Cmt, Ch, Rsp)$ such that $d = 1 (accept)$ while $d = 0 (reject)$.

Prover $\mathcal{P}$		Verifier $\mathcal{V}$
Initial State $St = (q, R)$		
$(Cmt, St) \leftarrow \mathcal{P}(\epsilon; St)$		
	$\xrightarrow{Cmt}$	
		$Ch \stackrel{R}{\leftarrow} ChSet_{\mathcal{V}}$
	$\xleftarrow{Ch}$	
$(Rsp, St) \leftarrow \mathcal{P}(Ch; St)$		
	$\xrightarrow{Rsp}$	
		$d \leftarrow Veri(Cmt, Ch, Rsp)$

Figure 1: Standard Identification (A Canonical Protocol) [9]

2.3. Identity-based Ad-Hoc Anonymous Identification

The formal definition of the identity-based ad-hoc anonymous identification scheme that was formalized by Nguyen [5] is revisited as follows:

An identity-based ad-hoc anonymous identification scheme consists of six probabilistic polynomial time algorithms (PPT) which are *Setup*, *KeyGen*, *MakeGPK*, *MakeGSK*, *Prove* and *Verify* based on [5, 8].

Setup is first executed by the Private Key Generator (PKG) and outputs the public parameters `param` and master secret key *msk* to itself. *KeyGen* creates user-secret keys σ from a public `ID` string using the *msk*.

MakeGPK and *MakeGSK* generate the group public key *GPK* and group secret key *GSK*, respectively.

Prove and *Verify* together form the anonymous identity-based identification protocol (*IAID*). Both of the prover $IAID_P$ and the verifier $IAID_V$ takes as input `param` and a group public key. $IAID_P$ is also given a group secret key that is corresponding to the group public key. Finally, $IAID_V$ outputs $\{0, 1\}$ where 1 is accept and 0 is reject.

2.4. Security Requirements

There are three security requirements for an ad-hoc anonymous IBI scheme. The requirements mentioned by [2, 5, 8] are listed under Table 1 along with a brief description and attacker goals.

Table 1: Security Requirements for an ad-hoc anonymous IBI scheme [2, 5, 8]

Requirement	Description	Attacker Goal
Correctness	Any *honest prover* will always be able to convince a *verifier* with the *IAID* protocol.	Deny
Soundness	Any *dishonest* entity not possessing the private key will only be able to convince an *honest verifier* with negligible probability.	Impersonation
Anonymity	An adversary is unable to distinguish the identity-private key pair on a valid transcript with *honest* parties from two distinct identity-private key pairs, where one of the two is the pair used in the transcript. The adversary has negligibly more advantage as guessing the outcome of an unbiased coin toss. If this condition holds even against an adversary with unlimited computing power at their disposal, then the scheme satisfies *unconditional anonymity*	Deanonymization, Linkability

Honest describes an actor which strictly follows the protocol.

3. Cryptanalysis

3.1. Instantiation by Barapatre and Rangan

In 2013, Barapatre and Rangan instantiated an ad-hoc anonymous IBI scheme that is pairing free [8]. The six algorithms along with the IAID protocol are shown in Algorithm 1, 2, 3, 4 and Figure 2.

Algorithm 1 Setup.

```
procedure SETUP(1^k)
    (N, e, d) ← K_RSA(1^k)
    Select H_1 : {0,1}^* → Z_N^*
    Select H_2 : {0,1}^* → {0,1}^l where 2^l < e < 2^(l+1)
    param ← (N, e, H_1, H_2, l)
    msk ← d
return (param, msk)
end procedure
```

Algorithm 2 KeyGen.

```
procedure KEYGEN(msk, param, ID_i)
    σ_i ← H_1(ID_i)^d
return σ_i
end procedure
```

Algorithm 3 MakeGPK.

```
procedure MAKEGPK(param, ID_1...ID_n)
    U ← {ID_1...ID_n}
    Find s ∈ Z_n where ID_s ∈ U                ▷ Run by user with ID_s
    for i ∈ {1...n} \ s do
        A_i ←$ Z_N^*
        R_i ← A_i^e mod N
        h_i = H_2(U, ID_i, R_i)
    end for
    A ←$ Z_N^*
    R_s ← A^e ∏_{i≠s} [H_1(ID_i)]^(−h_i) mod N
    if R_s = 1 mod N or R_s = R_i and i ≠ s then
        GOTO Step 9.
    end if
    GPK ← ({R_i}_{i=1}^n, {h_i}_{i=1}^n, U)
return GPK
end procedure
```

Algorithm 4 MakeGSK.

procedure MAKEGSK(`param`, $ID_1 ... ID_n, \sigma_s$) ▷ Run by user with ID_s
    Find $s \in \mathbb{Z}_N$ from $\{ID_1 ... ID_n\}$
    $GPK \leftarrow$ MAKEGPK(`param`, $ID_1 ... ID_n$)
    $(\{R_i\}_{i=1}^n, \{h_i\}_{i=1}^n, U) \leftarrow GPK$
    $h_s \leftarrow H_2(U, ID_s, R_s)$
return $GSK \leftarrow \sigma_s^{h_s}$
end procedure

$\mathcal{P}$ (Prover)		$\mathcal{V}$ (Verifier)
$(ID_i, GPK, \texttt{param}, GSK)$		$(ID_i, GPK, \texttt{param})$
$m \in_R \mathbf{Z}_N^*$ $U = [H_1(ID_s)^{h_s}] \cdot m$	$\xrightarrow{U}$	
	$\xleftarrow{x}$	$x \in_R \mathbf{Z}_N^*$
$\sigma_1 = [(GSK)^{x+1} \cdot A \cdot \prod_{i \neq s} A_i]$ $\sigma_2 = m^x$ $W = \sigma_1^e \cdot \sigma_2$	$\xrightarrow{W}$	
		$W \stackrel{?}{=} U^x \cdot \prod_{i=1}^{n} [R_i \cdot H_1(ID_i)^{h_i}]$

Figure 2: The *IAID* protocol, operations are carried out modulo N [8]

3.2. Attack

We mount a key-only universal impersonation attack on Barapatre and Rangan's ad-hoc anonymous IBI scheme [8] in *IAID* protocol and prove that it is not secure since anyone can impersonate a valid group member to perform the anonymous identity-based identification protocol *IAID* successfully. Our attack shows the *soundness* property is invalid from their instantiation.

Assume that I is an impersonator, who only has the group public key GPK and does not have **any** valid group secret key GSK. We show that I can impersonate a valid group member under the *IAID* protocol listed in Figure 2. The details of the attack are described as follows:

1. The impersonator $\mathcal{I}$ impersonates the prover $\mathcal{P}$ by selecting a random $\tilde{U} \in_R \mathbb{Z}_N^*$ and sends $\tilde{U}$ as commitment to the honest verifier $\mathcal{V}$.

2. $\mathcal{V}$ selects a random $x \in_R \mathbf{Z}_N^*$ as the challenge and sends it to $\mathcal{I}$.

3. $\mathcal{I}$ computes $W = \tilde{U}^x \cdot \prod_{i=1}^{n} [R_i \cdot H_1(ID_i)^{h_i}] \mod N$.

4. $\mathcal{V}$ will always authenticate $\mathcal{I}$ since W is a valid response.

From the above impersonation attack, $\mathcal{I}$ can convince $\mathcal{V}$ that he is a valid group member without knowing the group secret key GSK. Under the same definition (2.2) from their work [8], we see that Equation 1 does not reflect on the advantage of the impersonator I in the game because it can always obtain a valid transcript **even without** any query to the Corrupt Oracle O_{Corr}.

$$(\forall\ \lambda \in N)(\forall\ \text{PPT}\mathcal{A})[\text{Succ}_{\mathcal{A}}^{\text{snd}}(k) \leq v(k)] \tag{1}$$

where $v(t)$ is a negligible function in security parameter k

4. The Fix

In this section, we proposed a fix for [8] and the security proof of the fixed scheme.

4.1. The Fixed Scheme

In order to fix this vulnerability, we suggest to change the way of the response has constructed in *IAID* protocol of the scheme [8]. The algorithms *Setup*, *KeyGen*, *MakeGPK* and *MakeGSK* remains the same, while the *IAID* protocol is modified as illustrated in Figure 3 works as follows:

1. Prover $\mathcal{P}$ select $m \in_R \mathbb{Z}_N^*$ and compute $U = [H_1(ID_s)^{h_s}] \cdot m$.

2. $\mathcal{P}$ sends U as commitment to verifier $\mathcal{V}$.

3. $\mathcal{V}$ selects a random $x \in_R \mathbb{Z}_N^*$ as the challenge and sends it to $\mathcal{P}$.

4. $\mathcal{P}$ computes $\sigma_1 = [(GSK)^{x+1} \cdot A \cdot \prod_{i \neq s} A_i \mod N]$ and $\sigma_2 = m^x$.

5. $\mathcal{P}$ sends (σ_1, σ_2) as the response to $\mathcal{V}$.

6. $\mathcal{V}$ checks for consistency of (σ_1, σ_2) as: If $\sigma_1^e \cdot \sigma_2 = U^x \cdot \prod_{i=1}^{n} [R_i \cdot H_1(ID_i)^{h_i}]$ mod N. Then $\mathcal{V}$ *Accepts*, else it *Rejects*.

Prover $\mathcal{P}$		Verifier $\mathcal{V}$
$m \in_R \mathbf{Z}_N^*$ $U = [H_1(ID_s)^{h_s}] \cdot m$		
	$\xrightarrow{U}$	
		$x \in_R \mathbf{Z}_N^*$
	$\xleftarrow{x}$	
$\sigma_1 = [(GSK)^{x+1} \cdot A \cdot \prod_{i \neq s} A_i \mod N]$ $\sigma_2 = m^x$		
	$\xrightarrow{(\sigma_1, \sigma_2)}$	
		$\sigma_1^e \cdot \sigma_2 \stackrel{?}{=} U^x \cdot \prod_{i=1}^{n} [R_i \cdot H_1(ID_i)^{h_i}] \mod N$

Figure 3: The fixed *IAID* protocol

4.2. The Flawed Security Proof and A Fix

The attack is possible likely due to a flaw in the scheme's original security proof. We present the flaw from their proof and our fix corresponding to our modification to the IAID protocol. Referring to Section 4 (Security Proof) in their paper [8] under the proof for the soundness property, Equation 2 cannot be computed by the simulator because (σ_1/σ_1') is not available to it but only $(\sigma_1/\sigma_1')^e$ computation of Equation 2 is pivotal in solving the given RSA problem. As such, the simulator will fail.

Recall that $W = \sigma_1^e \cdot \sigma_2$ is sent from prover to verifier as a response. We note that the flaw arises because the way W_1 and W_2 is computed, which **necessarily** give rise to the value $(\sigma_1/\sigma_1')^e$ under division.

$$z = ((\sigma_1/\sigma_1') \cdot x_j^{(h_j'-h_j)})^b \cdot y^a \mod N \tag{2}$$

With our fix, since σ_1 and σ_2 is sent over instead of $W = \sigma_1^e \cdot \sigma_2$, this becomes possible. Therefore, our proof would replace W_1/W_2 with $(\sigma_1/\sigma_1')^e \cdot \sigma_2/\sigma_2'$ and the rest follows from "dividing two equations" from their security proof [8].

For the proof of anonymity in [8], there are two equations which are:

$$W_i = \sigma_{1_i}^e \cdot \sigma_{2_i} = [(GSK)^{x+1} \cdot A \cdot \prod_{i \neq s} A_i \mod N] \cdot m_1^x$$

and

$$W_j = \sigma_{1_j}^e \cdot \sigma_{2_j} = [(GSK)^{x+1} \cdot A \cdot \prod_{j \neq s} A_j \mod N] \cdot m_2^x.$$

We replace W_i and W_j with $\sigma_{1_i}^e \cdot \sigma_{2_i}$ and $\sigma_{1_j}^e \cdot \sigma_{2_j}$, respectively. Therefore, the two fixed equations are:

$$\sigma_{1_i}^e \cdot \sigma_{2_i} = [(GSK)^{x+1} \cdot A \cdot \prod_{i \neq s} A_i \mod N] \cdot m_1^x$$

and

$$\sigma_{1_j}^e \cdot \sigma_{2_j} = [(GSK)^{x+1} \cdot A \cdot \prod_{j \neq s} A_j \mod N] \cdot m_2^x.$$

With the addition of the two equations,

$$U_i = H_1(ID_i)^{h_i} \cdot m_1$$

and

$$U_j = H_1(ID_j)^{h_j} \cdot m_2,$$

We obtained that the values of U_i and U_j are indistinguishable. Similarly, $\sigma_{1_i}^e \cdot \sigma_{2_i}$ and $\sigma_{1_j}^e \cdot \sigma_{2_j}$ are also indistinguishable. Thus, we can conclude that the communication transcript gives no information on the identity of the prover amongst the n users of the ad-hoc ring.

5. Conclusions

In this paper, we showed an attack on Barapatre and Rangan's ad-hoc anonymous identity-based identification scheme [8] that is constructed based on the RSA assumption. The scheme is found to be vulnerable to the key-only universal impersonation attack.

Also, we presented a flaw in the security proof provided for the original scheme in [8]. Lastly, we proposed a solution to improve the scheme against our attack and presented the security proof of the fixed scheme.

Acknowledgement

The authors would like to thank the Ministry of Education of Malaysia in providing financial support for this work through the Fundamental Research Grant Scheme (FRGS/1/2019/ICT04/MMU/02/5). This work was done when the authors were doing industrial training at MIMOS Berhad.

References

[1] A. Fiat, A. Shamir, How to prove yourself: Practical solutions to identification and signature problems, in: A. M. Odlyzko (Ed.), Advances in Cryptology — CRYPTO' 86, Springer Berlin Heidelberg, Berlin, Heidelberg, 1987, pp. 186–194.

[2] Y. Dodis, A. Kiayias, A. Nicolosi, V. Shoup, Anonymous identification in ad hoc groups, in: C. Cachin, J. L. Camenisch (Eds.), Advances in Cryptology - EUROCRYPT 2004, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 609–626.

[3] L. Nguyen, Accumulators from bilinear pairings and applications, in: A. Menezes (Ed.), Topics in Cryptology – CT-RSA 2005, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 275–292.

[4] F. Zhang, X. Chen, Cryptanalysis and improvement of an id-based ad-hoc anonymous identification scheme at ct-rsa 05, Information Processing Letters 109 (2009) 846 – 849. URL: http://www.sciencedirect.com/science/article/pii/S0020019009001379.

[5] L. Nguyen, Accumulators from bilinear pairings and applications to ID-based ring signatures and group membership revocation., IACR Cryptology ePrint Archive 2005 (2005) 123.

[6] C. Tartary, H. Wang, The bilinear pairing-based accumulator proposed at ct-rsa'05 is not collision resistant., IACR Cryptology ePrint Archive 2006 (2006) 426.

[7] C. Gu, Y. Zhu, C. Ma, An efficient identity based anonymous identification scheme for ad-hoc groups from pairings, 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing (2008).

[8] P. Barapatre, C. Pandu Rangan, Anonymous identity-based identification scheme in ad-hoc groups without pairings, in: B. Gierlichs, S. Guilley, D. Mukhopadhyay (Eds.), Security, Privacy, and Applied Cryptography Engineering, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 130–146.

[9] M. Bellare, A. Palacio, GQ and Schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks, in: M. Yung (Ed.), Advances in Cryptology — CRYPTO 2002, Springer Berlin Heidelberg, Berlin, Heidelberg, 2002, pp. 162–177.