CRYPTANALYSIS OF AN IDENTITY-BASED AUTHENTICATED KEY EXCHANGE PROTOCOL

YOUNES HATRI, AYOUB OTMANI, AND KENZA GUENDA

Abstract

Authenticated Key Exchange (AKE) protocols represent an important cryptographic mechanism that enables several parties to communicate securely over an open network. Elashry, Mu and Susilo proposed an Identity Based Authenticated Key Exchange (IBAKE) protocol where different parties establish secure communication by means of their public identities.The authors also introduced a new security notion for IBAKE protocols called resiliency, that is, if the secret shared key is compromised, the entities can generate another shared secret key without establishing a new session between them. They then claimed that their IBAKE protocol satisfies this security notion.

We analyze the security of their protocol and prove that it has a major security flaw which renders it insecure against an impersonation attack. We also disprove the resiliency property of their scheme by proposing an attack where an adversary can compute any share secret key if just one secret bit is leaked.

1. INTRODUCTION

Key agreement protocols permit different parties to share a common secret key which in turn can be used for different cryptographic goals like communication encryption, data integrity, *etc*. The first practical solution to the problem of key-distribution is the famous Diffie-Hellman protocol [6]. However, it does not prevent from Man-In-The-Middle attacks because it does not authenticate the involved parties. A key agreement protocol provides key authentication if each entity involved in the exchange is assured that no other entity can learn the shared secret key. There exist several methods to broadcast authenticated keys. Classically it requires public-key certificates with public key infrastructures. Another very interesting approach is to use public data like identities to generate authenticated keys.

The idea of using identities in cryptography dates back to Shamir's paper [14] where he asks how to achieve a public key encryption scheme that allows to compute public keys from arbitrary strings like user's identity (an email, phone number, *etc*). Consequently, electronic certificates are no more required and more importantly it eliminates the need for large-scale public key infrastructure. Although Shamir introduced in [14] the concept of Identity-Based Encryption (IBE), he was not able to propose one. The construction remained an open problem until Boneh and Franklin [2] and Cocks [4] proposed IBE schemes in 2001. The Boneh-Franklin scheme [2] makes use of bilinear maps which then sparked a lot of works [1, 18]. Recently, lattices have also been used in the design of IBE schemes [8] which gave rise to a large number of schemes.

Cocks builds in [4] an IBE scheme based on the quadratic residuosity problem modulo an RSA integer. It is time-efficient compared with pairing-based IBE systems, but unfortunately ciphertexts are

`hatri.younes@hotmail.fr`. Université des Sciences et de la Technologie Houari Boumediene, Bab Ezzouar 16111, Algeria.

`ayoub.otmani@univ-rouen.fr`. Normandie Univ, France; UR, LITIS, F-76821 Mont-Saint-Aignan, France.

`ken.guenda@gmail.fr`. Université des Sciences et de la Technologie Houari Boumediene, Bab Ezzouar 16111, Algeria.

very long. Boneh, Gentry and Hamburg (BGH) solved the problem of Cocks' scheme by presenting a space-efficient scheme without pairings but at the cost of a less time-efficient scheme [3].

The concept of IBE was extended to authenticated key exchange (AKE) protocols. Smart [15] presented a two-pass Identity-Based AKE (IBAKE) using Weil pairings and merging the ideas of Boneh and Franklin [2] with tripartite Diffie-Hellman (DH) protocol of Joux [10]. This work was then followed by several works. Recently, Elashry, Mu and Susilo [7] proposed another IBAKE protocol and introduced a new security notion called *resiliency*. A key exchange protocol is said to be *resilient* when parties are able to generate new shared secret keys without establishing a new session between them, even if a secret shared key has been compromised. The IBAKE protocol proposed by [7] builds upon the IBE encryption scheme of [3] and it is claimed in [7] to be resilient.

1.1. **Our contribution.** In this paper, we analyze the security of Elashry, Mu and Sussilo (EMS) protocol [7] and prove that it has a major security flaw which renders it insecure against an impersonation attack. We are indeed able to prove that the protocol is insecure against a very simple man-in-the-middle attack.

We also disprove the resiliency property of the EMS scheme by proposing an attack where an adversary can compute in time quartic in the security parameter the secret shared key from the knowledge of a single secret bit. Our method is similar to the one given in [16] to attack an IBE encryption scheme proposed in [9].

The rest of this paper is organized as follows. In Section 2, we recall the definition and notion for IBAKE protocols. In Section 3, we present Elashry, Mu, Sussilo (EMS) IBAKE protocol [7]. In Section 4, we describe our attacks against this protocol. In Section 5, we discuss the question of repairing the scheme. Finally, in Section 6 we conclude the paper.

2. PRELIMINARIES

2.1. **IBAKE Protocol.** We shall assume that a trusted authority is responsible for the creation and distribution of users' private keys. An Identity-Based Authenticated Key Exchange protocol (IBAKE) [15, 13] is defined by three algorithms: $\mathtt{Setup}()$, $\mathtt{Extract}()$ and $\mathtt{KeyExchange}()$.

   (1) $(\mathsf{msk}, \mathsf{mpk}) \leftarrow \mathtt{Setup}(\lambda)$. The authority takes as input a security parameter λ and generates public parameters that are denoted by mpk and a *master secret key* msk.
   (2) $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathtt{Extract}(\mathsf{msk}, \mathsf{id})$. Given an identity id, the authority uses his master key msk to generate the private key $\mathsf{sk}_{\mathsf{id}}$ corresponding to id.
   (3) $\mathsf{ssk} \leftarrow \mathtt{KeyExchange}(\mathsf{id}_1, \mathsf{id}_2)$. Two parties P_1 and P_2 with system parameters $(\mathsf{id}_1, \mathsf{sk}_{\mathsf{id}_1})$ and $(\mathsf{id}_2, \mathsf{sk}_{\mathsf{id}_2})$ respectively generate a shared secret key ssk.

2.2. **Quadratic Residues and Jacobi Symbol.** For any integer $N \geqslant 2$ we denote by $\mathbb{Z}_N^\times$ the multiplicative group of integers modulo N. Let $y \in \mathbb{Z}_N^\times$ then we say that y is a *quadratic residue* in $\mathbb{Z}_N^\times$ if there exists $x \in \mathbb{Z}_N^\times$ such that:
$$y \equiv x^2 \mod N.$$
The set of quadratic residues in $\mathbb{Z}_N^\times$ is denoted by $\mathsf{QR}(N)$:
$$\mathsf{QR}(N) = \left\{ y \in \mathbb{Z}_N^\times \ : \ \exists x \in \mathbb{Z}_N^\times, \, y = x^2 \mod N \right\}.$$
Let p be an odd prime number, we define the Legendre symbol of $x \in \mathbb{Z}$ with respect to p as
$$\left(\frac{x}{p} \right) = x^{\frac{p-1}{2}} \mod p.$$

We recall that $\left(\dfrac{x}{p}\right)$ belongs to $\{-1, 0, 1\}$ and enables to determine if x is a quadratic residue since we have:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if} \quad x \in \mathsf{QR}(N) \\ -1 & \text{if} \quad x \notin \mathsf{QR}(N) \text{ and } x \neq 0 \mod p \\ 0 & \text{if} \quad x = 0 \mod p. \end{cases}$$

The Legendre symbol is extended to any odd positive integer $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where $p_1, \ldots, p_k$ are pairwise different prime numbers and $\alpha_1, \ldots, \alpha_k$ are positive integers. This generalization is called the Jacobi symbol and is defined as:

$$\left(\frac{x}{N}\right) = \left(\frac{x}{p_1}\right)^{\alpha_1} \cdots \left(\frac{x}{p_k}\right)^{\alpha_k}.$$

The subset of $\mathbb{Z}_N$ with symbol to equal 1 is denoted by $\mathsf{J}(N)$. Note that $\mathsf{QR}(N)$ is a subset of $\mathsf{J}(N)$.

The *quadratic residuosity assumption* states that, for any integer $N = pq$, where p and q are different prime numbers that are picked at random, there exists no probabilistic polynomial time algorithm that is able to distinguish between the distribution of samples drawn from $\mathsf{QR}(N)$ and the distribution of samples picked from $\mathsf{J}(N) \setminus \mathsf{QR}(N)$ (see [3] for more details).

2.3. **Solving** $Rx^2 + Sy^2 = 1 \mod N$. Assuming that $N = pq$ where p and q are different prime numbers, Boneh, Gentry and Hamburg presented in [3] an efficient algorithm to solve in $\mathbb{Z}_N$ an equation of the form:

$$Rx^2 + Sy^2 = 1 \mod N \tag{1}$$

where R and S are in $\mathbb{Z}_N$. They considered the following ternary quadratic form over $\mathbb{Z}$:

$$\widetilde{R}x^2 + \widetilde{S}y^2 - z^2 = 0. \tag{2}$$

with $\widetilde{R}, \widetilde{S}$ in $\mathbb{Z}$. A classical result of Legendre [3] says that (2) has a solution $(x, y, z) \in \mathbb{Z}^3$ if there exist $\widetilde{r}$ and $\widetilde{s}$ in $\mathbb{Z}$ such that

$$\widetilde{R} = \widetilde{r}^2 \mod \widetilde{S} \quad \text{and} \quad \widetilde{S} = \widetilde{s}^2 \mod \widetilde{R}. \tag{3}$$

Cremona and Rusin proposed in [5] an algorithm using lattice reduction to solve (2) assuming that (3) holds. Furthermore, if $\widetilde{R} = R \mod N$ and $\widetilde{S} = S \mod N$ then a solution to (2) also gives a solution to (1). Consequently, solving (1) consists in finding prime numbers $\widetilde{R}, \widetilde{S}$ and integers $\widetilde{r}, \widetilde{s}$ such that $\widetilde{R} = R \mod N$, $\widetilde{S} = S \mod N$ and $\widetilde{r}, \widetilde{s}$ satisfy (3). There exist several possible candidates $(\widetilde{R}, \widetilde{S})$ from a given couple (R, S) but Boneh and Franklin proposed a *deterministic* polynomial-time algorithm that finds a specific $(\widetilde{R}, \widetilde{S})$ which leads to a solution to (1). For more details we refer the reader to [3].

Finally we state an important lemma that shows an important property used in [3] and [7].

Lemma 1. *Assume that R and S belong to $\mathsf{QR}(N)$ and let (x, y) be a solution to* (1)*. Then we have the following equality:*

$$\left(\frac{1 + x\sqrt{R}}{N}\right) = \left(\frac{2 + 2y\sqrt{S}}{N}\right).$$

Proof. We have in $\mathbb{Z}_N$ the following equality:

$$\left(x\sqrt{R}+1\right)\left(2y\sqrt{S}+2\right) = 2xy\sqrt{RS} + 2x\sqrt{R} + 2y\sqrt{S} + 2$$
$$= \left(x\sqrt{R} + y\sqrt{S} + 1\right)^2.$$

The last equality is obtained by using (1). $\square$

3. ELASHRY-MU-SUSILO (EMS) IBAKE SCHEME

EMS scheme [7] is specified by the following algorithms (Fig. 1):

(1) $(\mathsf{msk}, \mathsf{mpk}) \leftarrow \mathtt{Setup}(\lambda)$. The authority generates two prime numbers p and q according to security parameter λ. It also picks $\mu \in \mathsf{J}(N) \setminus \mathsf{QR}(N)$ and chooses a hash function $\mathcal{H} : \{0,1\}^* \longrightarrow \mathsf{J}(N)$. The master public key is then $\mathsf{mpk} = \{N, \mu, \mathcal{H}\}$ where $N = pq$ and the master secret key is $\mathsf{msk} = (p, q)$.

(2) $\mathsf{sk}_{\mathsf{id}} \leftarrow \mathtt{Extract}(\mathsf{msk}, \mathsf{id})$. Given an identity id, the authority generates $R = \mathcal{H}(\mathsf{id})$. Since R is in $\mathsf{J}(N)$ then either R or μR belongs to $\mathsf{QR}(N)$. The authority chooses a in $\{0,1\}$ such that $\mu^a R$ belongs to $\mathsf{QR}(N)$. It then picks at random one of the four possible square roots of $\mu^a R$. We denote it by $\sqrt{\mu^a R}$. The private key for identity id is then $\mathsf{sk}_{\mathsf{id}} = (a, \sqrt{\mu^a R})$.

(3) $\mathsf{ssk} \leftarrow \mathtt{KeyExchange}(\mathsf{id}_1, \mathsf{id}_2)$. Party P_1 with identity id_1 and system parameter $R_1 = \mathcal{H}(\mathsf{id}_1), \mathsf{sk}_{\mathsf{id}_1}$ chooses two random values s_1 and α_1 in $\mathbb{Z}_N^\times$ such that[1]

$$\mu^{\alpha_1} R_1 \in \mathsf{QR}(N).$$

P_1 then sends $(\mathsf{id}_1, \mu^{\alpha_1}, S_1)$ to P_2 where $S_1 = s_1^2 \mod N$ and keeps secret (α_1, s_1). P_2 with identity id_2 and system parameter $R_2 = \mathcal{H}(\mathsf{id}_1), \mathsf{sk}_{\mathsf{id}_2}$ also performs the same procedure by choosing two random values s_2 and α_2 in $\mathbb{Z}_N^\times$ such that

$$\mu^{\alpha_2} R_2 \in \mathsf{QR}(N).$$

Then P_2 sends $(\mathsf{id}_2, \mu^{\alpha_2}, S_2)$ to P_1 with $S_2 = s_2^2 \mod N$, and keeps secret (α_2, s_2).

Each party P_1 and P_2 solves independently for each $i = 1, \ldots, \ell$ the equation:

$$\mu^{\alpha_1} R_1 S_1^{2i+1} x_i^2 + \mu^{\alpha_2} R_2 S_2^{2i+1} y_i^2 = 1 \mod N. \qquad (4)$$

From *the* solution (x_i, y_i) and its private key P_1 is then able to compute the quantity $k_{i,1} \in \{-1, 1\}$ where

$$k_{i,1} = \left(\frac{1 + x_i s_1^{2i+1} \sqrt{\mu^{\alpha_1} R_1}}{N}\right).$$

P_2 computes $k_{i,2} \in \{-1, 1\}$ from *the* solution (x_i, y_i) and its private as the following:

$$k_{i,2} = \left(\frac{2 + 2y_i s_2^{2i+1} \sqrt{\mu^{\alpha_2} R_2}}{N}\right).$$

By Lemma 1 we know that $k_{i,1} = k_{i,2}$ and therefore the shared secret key ssk is

$$\left(k_{1,1}, k_{1,1}, \ldots, k_{\ell,1}\right) = \left(k_{1,2}, k_{1,2}, \ldots, k_{\ell,2}\right) = \mathsf{ssk}.$$

---

[1]P_1 can easily find $\alpha_1 \in \mathbb{Z}$ such that $\mu^{\alpha_1} R_1 \in \mathsf{QR}$ and can even compute $\sqrt{\mu^{\alpha_1} R_1}$ from its private key $\mathsf{sk}_{\mathsf{id}_1} = (a_1, \sqrt{\mu^{a_1} R_1})$. Indeed, P_1 chooses α_1 to be equal to $2t + a_1$ for a random integer $t \in \mathbb{Z}$ so that

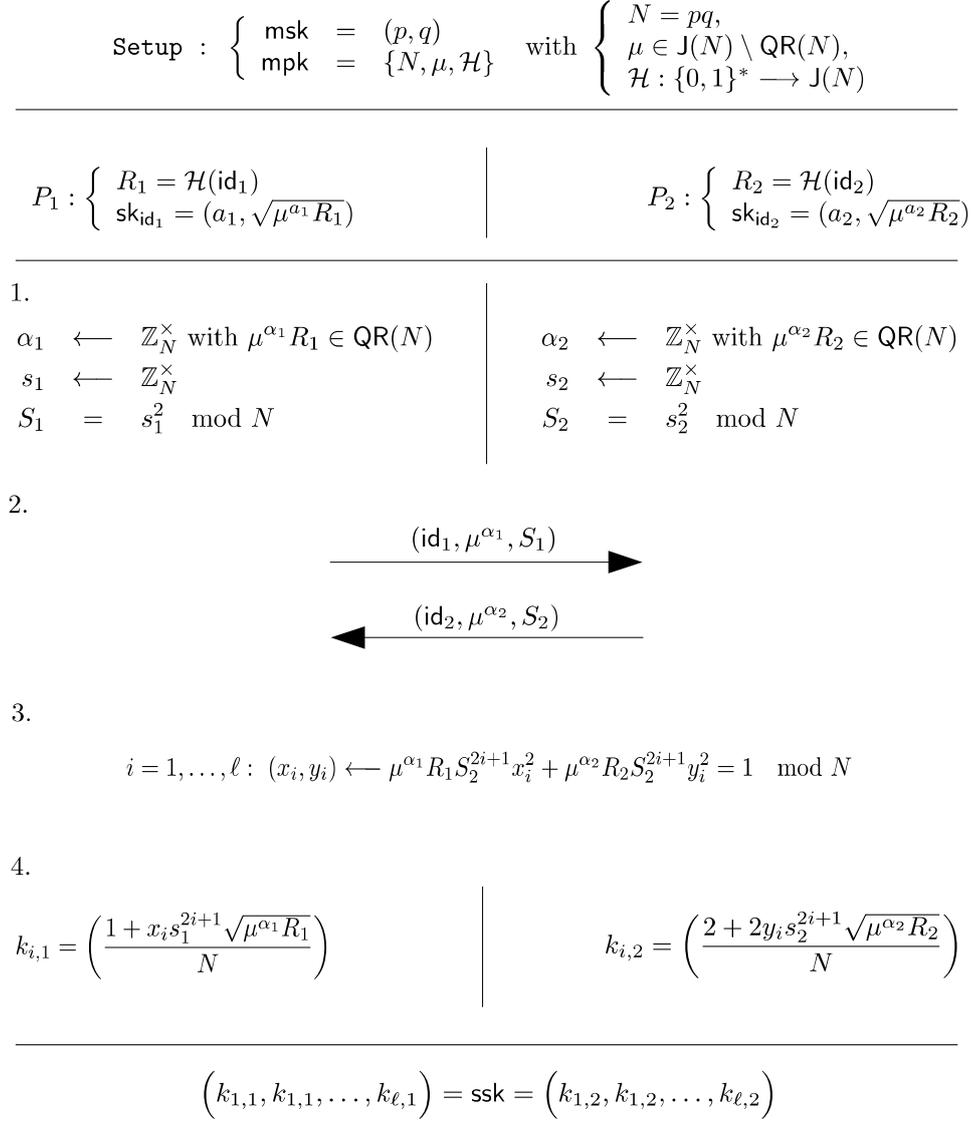$$\mu^{\alpha_1} R_1 = \mu^{2t+a_1} R_1 = \left(\mu^t \sqrt{\mu^a R_1}\right)^2.$$

$$\text{Setup} : \begin{cases} \mathsf{msk} &= (p,q) \\ \mathsf{mpk} &= \{N, \mu, \mathcal{H}\} \end{cases} \quad \text{with} \begin{cases} N = pq, \\ \mu \in \mathsf{J}(N) \setminus \mathsf{QR}(N), \\ \mathcal{H} : \{0,1\}^* \longrightarrow \mathsf{J}(N) \end{cases}$$

$$P_1 : \begin{cases} R_1 = \mathcal{H}(\mathsf{id}_1) \\ \mathsf{sk}_{\mathsf{id}_1} = (a_1, \sqrt{\mu^{a_1} R_1}) \end{cases} \qquad\qquad P_2 : \begin{cases} R_2 = \mathcal{H}(\mathsf{id}_2) \\ \mathsf{sk}_{\mathsf{id}_2} = (a_2, \sqrt{\mu^{a_2} R_2}) \end{cases}$$

1.

$$\begin{aligned}
\alpha_1 &\longleftarrow \mathbb{Z}_N^{\times} \text{ with } \mu^{\alpha_1} R_1 \in \mathsf{QR}(N) \\
s_1 &\longleftarrow \mathbb{Z}_N^{\times} \\
S_1 &= s_1^2 \mod N
\end{aligned}
\qquad
\begin{aligned}
\alpha_2 &\longleftarrow \mathbb{Z}_N^{\times} \text{ with } \mu^{\alpha_2} R_2 \in \mathsf{QR}(N) \\
s_2 &\longleftarrow \mathbb{Z}_N^{\times} \\
S_2 &= s_2^2 \mod N
\end{aligned}$$

2.

$$\xrightarrow{\quad (\mathsf{id}_1, \mu^{\alpha_1}, S_1) \quad}$$

$$\xleftarrow{\quad (\mathsf{id}_2, \mu^{\alpha_2}, S_2) \quad}$$

3.

$$i = 1, \ldots, \ell : \ (x_i, y_i) \longleftarrow \mu^{\alpha_1} R_1 S_2^{2i+1} x_i^2 + \mu^{\alpha_2} R_2 S_2^{2i+1} y_i^2 = 1 \mod N$$

4.

$$k_{i,1} = \left(\frac{1 + x_i s_1^{2i+1} \sqrt{\mu^{\alpha_1} R_1}}{N} \right) \qquad\qquad k_{i,2} = \left(\frac{2 + 2 y_i s_2^{2i+1} \sqrt{\mu^{\alpha_2} R_2}}{N} \right)$$

$$\left(k_{1,1}, k_{1,1}, \ldots, k_{\ell,1} \right) = \mathsf{ssk} = \left(k_{1,2}, k_{1,2}, \ldots, k_{\ell,2} \right)$$

FIGURE 1. Elashry-Mu-Susilo (EMS) IBAKE protocol.

4. CRYPTANALYSIS

4.1. **Impersonation Attack.** The EMS protocol displays from its definition a major security flaw: it does not prevent from parties to be impersonated by an adversary. The protocols does not ensure any authentication during the exchange. In the following we explain a simple man-in-the-middle attack.
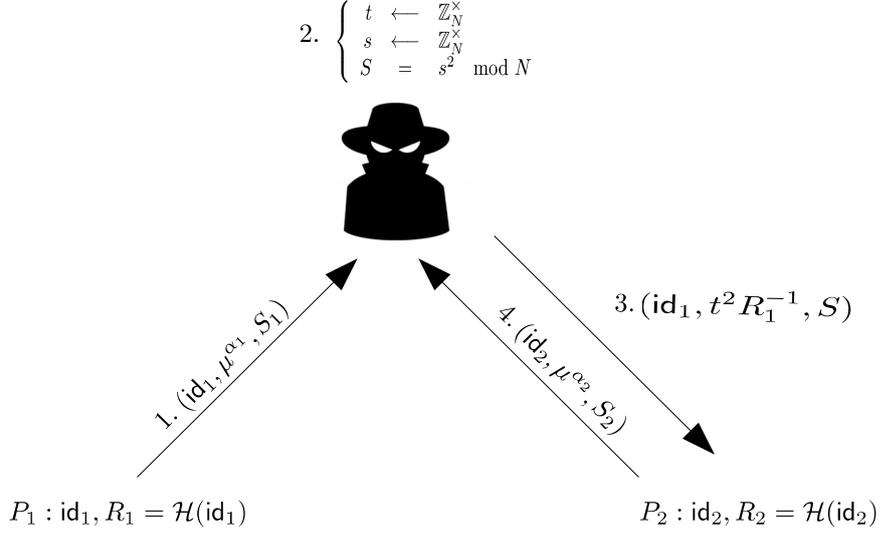
$$2. \begin{cases} t & \longleftarrow & \mathbb{Z}_N^\times \\ s & \longleftarrow & \mathbb{Z}_N^\times \\ S & = & s^2 \mod N \end{cases}$$

$3. \left(\mathsf{id}_1, t^2 R_1^{-1}, S\right)$

$1. \left(\mathsf{id}_1, \mu^{\alpha_1}, S_1\right)$

$4. \left(\mathsf{id}_2, \mu^{\alpha_2}, S_2\right)$

$P_1 : \mathsf{id}_1, R_1 = \mathcal{H}(\mathsf{id}_1)$

$P_2 : \mathsf{id}_2, R_2 = \mathcal{H}(\mathsf{id}_2)$

FIGURE 2. Impersonation attack.

Let us assume that an adversary $\mathcal{A}$ receives and forwards data exchanged between P_1 and P_2 whose parameters are respectively $(R_1 = \mathcal{H}(\mathsf{id}_1), \mathsf{sk}_{\mathsf{id}_1})$ and $(R_2 = \mathcal{H}(\mathsf{id}_2), \mathsf{sk}_{\mathsf{id}_2})$. We will now show how $\mathcal{A}$ can easily impersonate P_1.

When P_1 sends its session identifier $(\mathsf{id}_1, \mu^{\alpha_1}, S_1)$ to P_2, $\mathcal{A}$ intercepts it and chooses randomly t and s in $\mathbb{Z}_N^\times$, computes $S = s^2 \mod N$ then sends to P_2 the quantity $\left(\mathsf{id}_1, \frac{t^2}{R_1}, S\right)$. P_2 also sends its session identifier $(\mathsf{id}_2, \mu^{\alpha_2}, S_2)$ that is intercepted by $\mathcal{A}$. Upon receiving $(\mathsf{id}_1, \frac{t^2}{R_1}, S)$, P_2 computes first $T = \frac{t^2}{R_1} R_1 \mod N$ which turns out to be $t^2 \mod N$. Therefore $\mathcal{A}$ and P_2 have both to solve for $i = 1, \dots, \ell$ the (common) equations:

$$TS^{2i+1}x^2 + \mu^{\alpha_2} R_2 S_2^{2i+1} y^2 = 1 \mod N.$$

Then $\mathcal{A}$ and P_2 share the same secret key $\mathsf{ssk} = (k_1, \dots, k_\ell)$ since for any $i \geqslant 1$:

$$k_i = \left(\frac{1 + x_i t s^{2i+1}}{N}\right) = \left(\frac{2 + 2y_i \sqrt{\mu^{\alpha_2} R_2} s_2^{2i+1}}{N}\right).$$

The main reason why this attack is possible comes from the fact that each party in the protocol perform computations without involving data that identify the correspondent. Hence EMS protocol does not satisfy the basic property of authentication that any AKE protocol must satisfy. In the next section, we analyze further the security of the protocol by showing that EMS does not even ensure the resiliency property [7].

4.2. **Attack Against the Resiliency Property.** We assume that two parties P_1 and P_2 managed to share a secret key $\mathsf{ssk} = (k_1, \ldots, k_\ell)$ by means of EMS protocol as described in Section 3. We will prove that if an attacker $\mathcal{A}$ only knows one bit, let us say k_i with $i \in \{1, \ldots, \ell\}$, then $\mathcal{A}$ is able to recompute any bit k_j with $j \neq i$. This proves that EMS protocol does not satisfy the resiliency property unlike what is claimed by the authors in [7]. But before presenting our attack, we need an important lemma.

Lemma 2. [3, Lemma 5.1] *Let A, B_1 and B_2 be elements from $\mathbb{Z}_N$, and for each i in $\{1, 2\}$ let (x_i, y_i) be a solution to*

$$Ax^2 + B_i y^2 = 1 \mod N.$$

If $Ax_1 x_2 + 1$ belongs to $\mathbb{Z}_N^\times$ then (x_3, y_3) with $x_3 = \frac{x_1 + x_2}{1 + Ax_1 x_2}$ and $y_3 = \frac{y_1 y_2}{1 + Ax_1 x_2}$ is solution to

$$Ax^2 + B_1 B_2 y^2 = 1 \mod N.$$

We now describe how an adversary $\mathcal{A}$ can break the EMS protocol if $\mathcal{A}$ only knows k_i for some $i \in \{1, \ldots, \ell\}$ from a shared key $(k_1, \ldots, k_\ell)$. For the sake of simplicity, we will only describe how $\mathcal{A}$ can recover k_{i+1} from k_i and data publicly exchanged by P_1 and P_2. By induction, the attack can be generalized to any bit k_j.

Firstly, $\mathcal{A}$ solves (4) for i and $i+1$ to get (x_i, y_i) and (x_{i+1}, y_{i+1}) such that:

$$\begin{cases} \mu^{\alpha_1} R_1 S_1^{2i+1} x_i^2 & + & \mu^{\alpha_2} R_2 S_2^{2i+1} y_i^2 & = & 1 \mod N \\ \mu^{\alpha_1} R_1 S_1^{2i+3} x_{i+1}^2 & + & \mu^{\alpha_2} R_2 S_2^{2i+3} y_{i+1}^2 & = & 1 \mod N. \end{cases}$$

As explained in Section 2.3, $\mathcal{A}$ gets the *same* solutions to these equations as P_1 and P_2 would have during the protocol. Furthermore, $\mathcal{A}$ knows $(S_1 x_{i+1}, y_{i+1})$ which is a solution to the following equation:

$$\mu^{\alpha_1} R_1 S_1^{2i+1} (S_1 x_{i+1})^2 + \mu^{\alpha_2} R_2 S_2^{2i+3} y_{i+1}^2 = 1 \mod N.$$

From solutions (x_i, y_i) and $(S_1 x_{i+1}, y_{i+1})$, the adversary $\mathcal{A}$, by using Lemma 2, derives (x_*, y_*) that is solution to the equation

$$\mu^{\alpha_1} R_1 S_1^{2i+1} x_*^2 + \mu^{\alpha_2} R_2^2 S_2^{4i+4} y_*^2 = 1 \mod N \tag{5}$$

where

$$x_* = \frac{x_i + S_1 x_{i+1}}{1 + \mu^{\alpha_1} R_1 S_1^{2i+2} x_i x_{i+1}} \text{ and } y_* = \frac{y_i y_{i+1}}{1 + \mu^{\alpha_1} R_1 S_1^{2i+2} x_i x_{i+1}}.$$

The next lemma proves that k_i and k_{i+1} are related and an adversary can easily compute k_{i+1} from k_i and y_* and the public data exchanged between P_1 and P_2.

Lemma 3. *Let (x_*, y_*) be the solution to (5). We then have the equality:*

$$k_{i+1} = k_i \cdot \left(\frac{1 + \mu^{\alpha_1} R_1 S_1^{2i+2} x_i x_{i+1}}{N} \right) \cdot \left(\frac{2 + 2y_* \mu^{\alpha_2} R_2 S_2^{2i+2}}{N} \right)$$

Proof. We start by observing that

$$
\begin{aligned}
1 + x_* \sqrt{\mu^{\alpha_1} R_1 S_1^{2i+1}} &= 1 + x_* \sqrt{\mu^{\alpha_1} R_1} s_1^{2i+1} \\
&= 1 + \frac{(x_i + S_1 x_{i+1})}{1 + \mu^{\alpha_1} R_1 S_1^{2i+2} x_i x_{i+1}} \sqrt{\mu^{\alpha_1} R_1} s_1^{2i+1} \\
&= \frac{1 + \mu^{\alpha_1} R_1 S_1^{2i+2} x_i x_{i+1} + x_i \sqrt{\mu^{\alpha_1} R_1} s_1^{2i+1} + x_{i+1} \sqrt{\mu^{\alpha_1} R_1} s_1^{2i+3}}{1 + \mu^{\alpha_1} R_1 S_1^{2i+2} x_i x_{i+1}} \\
&= \frac{\left(1 + x_i \sqrt{\mu^{\alpha_1} R_1} s_1^{2i+1}\right)\left(1 + x_{i+1} \sqrt{\mu^{\alpha_1} R_1} s_1^{2i+3}\right)}{1 + \mu^{\alpha_1} R_1 S_1^{2i+2} x_i x_{i+1}}
\end{aligned}
$$

Since $k_i = \left(\frac{1 + x_i \sqrt{\mu^{\alpha_1} R_1} s_1^{2i+1}}{N}\right)$ and $k_{i+1} = \left(\frac{1 + x_{i+1} \sqrt{\mu^{\alpha_1} R_1} s_1^{2i+3}}{N}\right)$, this implies in particular that:

$$
k_{i+1} = k_i \cdot \left(\frac{1 + \mu^{\alpha_1} R_1 S_1^{2i+2} x_i x_{i+1}}{N}\right) \cdot \left(\frac{1 + x_* \sqrt{\mu^{\alpha_1} R_1 S_1^{2i+1}}}{N}\right)
$$

Since (x_*, y_*) is solution to (5) and $\mu^{\alpha_1} R_1 S_1^{2i+1} \in \mathsf{QR}(N)$ then by Lemma 1 we also have that:

$$
\left(\frac{2 + 2y_* \mu^{\alpha_2} R_2 S_2^{2i+2}}{N}\right) = \left(\frac{1 + x_* \sqrt{\mu^{\alpha_1} R_1 S_1^{2i+1}}}{N}\right)
$$

which terminates the proof of the lemma. $\square$

This attack is as efficient as the scheme since it only requires to compute the Jacobi symbol and the solving of (1). The computation of the Jacobi symbol can be performed [17] in $O\left(\log N \mathsf{M}\left(\log N\right)\right)$ operations where $\mathsf{M}(\lambda)$ is the cost of the multiplication of two integers of size λ bits (for large integers $\mathsf{M}(\lambda) = \lambda \log \lambda \log \log \lambda$). The equation (1) can be solved with $O\left(\log^4 N\right)$ operations ([3]). The total cost of the attack is therefore $O\left(\log^4 N\right)$ operations.

5. DISCUSSION ON A REPARATION

Our work raises also the question of whether the EMS protocol can be repaired. Our attack exploits the fact that the shared secret bits are related (see Lemma 3). One possible reparation would be to generate ℓ *independent* identity values $R_{i,1}, \ldots, R_{i,\ell}$ for a party P_i. For instance, one solution is to set $R_j = \mathcal{H}(\mathsf{id}, j)$ for all $j \in \{1, \ldots, \ell\}$, and the authority creates the secret key as $\mathsf{sk} = ((a_j)_{1 \leqslant j \leqslant \ell}, (r_j)_{1 \leqslant j \leqslant \ell})$ with $r_j = \sqrt{\mu^{a_j} R_j}$. Next, when two parties P_1 and P_2 wish to authenticate, they just have to solve the equations:

$$
R_{1,i} x_{i,j}^2 + R_{2,j} y_{i,j}^2 = 1 \mod N. \tag{6}
$$

The secret shared bit associated to this equation is now $k_{i,j} = \left(\frac{1 + x_{i,j} \sqrt{R_{1,i}}}{N}\right) = \left(\frac{2 + 2y_{i,j} \sqrt{R_{2,j}}}{N}\right)$.

Hence, they do not require anymore the values μ^{α_1} and μ^{α_2} which introduced the weaknesses (in particular for the impersonation attack). Unfortunately, this new protocol can (only) produce ℓ^2 secret bits, and the secret and public keys becomes ℓ times larger, which leads to an inefficient protocol for realistic applications.

6. Conclusion

In this paper, we have studied the security of the IBAKE protocol in introduced in [7]. The authors claimed that their protocol is provably secure when during the key exchange session some secret bits are leaked.

We showed that this protocol has two major weaknesses. First, it is vulnerable to a simple man-in-the-middle attack. Secondly, we propose an efficient attack where an adversary can easily compute any bit of a shared key if just one secret bit is known, which contradicts authors' claim.

Acknowledgments

References

[1] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In Christian Cachin and Jan L. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings*, pages 223–238, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[2] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings*, pages 213–229, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[3] Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryption without pairings. *2007 48th Annual IEEE Symposium on Foundations of Computer Science*, 00:647–657, 2007.

[4] Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, pages 360–363, London, UK, UK, 2001. Springer-Verlag.

[5] John Cremona and David Rusin. Efficient solution of rational conics. *Mathematics of Computation*, 72(243):1417–1441, 2003.

[6] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, 22(6):644–654, September 1976.

[7] Ibrahim Elashry, Yi Mu, and Willy Susilo. A resilient identity-based authenticated key exchange protocol. *Security and Communication Networks*, 8(13):2279–2290, 2015. sec.1172.

[8] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 197–206, New York, NY, USA, 2008. ACM.

[9] Mahabir Prasad Jhanwar and Rana Barua. A variant of boneh-gentry-hamburg's pairing-free identity based encryption scheme. In Moti Yung, Peng Liu, and Dongdai Lin, editors, *Information Security and Cryptology: 4th International Conference, Inscrypt 2008, Beijing, China, December 14-17, 2008, Revised Selected Papers*, pages 314–331, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[10] Antoine Joux. A one round protocol for tripartite diffie–hellman. *Journal of Cryptology*, 17(4):263–276, 2004.

[11] Xiong Li, Jian-Wei Niu, Jian Ma, Wen-Dong Wang, and Cheng-Lian Liu. Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*, 34(1):73 – 79, 2011.

[12] Xiong Li, Jianwei Niu, Muhammad Khurram Khan, and Junguo Liao. An enhanced smart card based remote user password authentication scheme. *Journal of Network and Computer Applications*, 36(5):1365 – 1371, 2013.

[13] Noel McCullagh and Paulo S. L. M. Barreto. A new two-party identity-based authenticated key agreement. In Alfred Menezes, editor, *Topics in Cryptology – CT-RSA 2005: The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005. Proceedings*, pages 262–274, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[14] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in Cryptology*, volume 196, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[15] N. P. Smart. An identity based authenticated key agreement protocol based on the weil pairing. *Electronics Letters*, 38:630–632, 2001.

[16] Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, and Anca-Maria Nica. Security of identity-based encryption schemes from quadratic residues. In Ion Bica and Reza Reyhanitabar, editors, *Innovative Security Solutions for*

Information Technology and Communications: 9th International Conference, SECITC 2016, Bucharest, Romania, June 9-10, 2016, Revised Selected Papers, pages 63–77, Cham, 2016. Springer International Publishing.

[17] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2013.

[18] Brent Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings*, pages 114–127, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.