On Security Proof of McCullagh-Barreto's Key Agreement Protocol and its Variants

Zhaohui Cheng
School of Computing Science, Middlesex University
The Burroughs, Hendon, London, UK
E-mail: m.z.cheng@mdx.ac.uk

Liqun Chen
Hewlett-Packard Laboratories
Filton Road, Stoke Gifford, Bristol, UK
E-mail: liqun.chen@hp.com

Abstract: McCullagh and Barreto presented an identity-based authenticated key agreement protocol in CT-RSA 2005. Their protocol was found to be vulnerable to a key-compromise impersonation attack. In order to recover the weakness, McCullagh and Barreto, and Xie proposed two variants of the protocol respectively. In each of these works, a security proof of the proposed protocol was presented. In this paper, we revisit these three security proofs and show that all the reductions in these proofs are invalid, because the property of indistinguishability between their simulation and the real world was not held. As a replacement, we slightly modify the McCullagh and Barreto's second protocol and then formally analyse the security of the modified scheme in the Bellare-Rogaway key agreement model.

1 Introduction

An identity-based authenticated key agreement protocol is a key agreement protocol where each of two (or more) parties uses an identity-based asymmetric key pair instead of a traditional public/private key pair for authentication and determination of the established key, which at the end of the protocol is shared by these parties.

The concept of identity-based cryptography was first formulated by Shamir (1985) in which a public key is the identity (an arbitrary string) of a user, and the corresponding private key is created by binding the identity string with a master secret of a trusted authority (called key generation center). In the same paper, Shamir provided the first identity-based key construction that was based on the RSA problem, and presented an identity-based signature scheme. By using varieties of the Shamir key construction, a number of identity-based key agreement schemes were proposed (e.g., ISO/IEC 11770-3 (1999); Okamoto (1986); Tanaka and Okamoto (1991)).

In 2000, Sakai et al. (2000) introduced an identity-based key agreement scheme based on bilinear pairings over elliptic curves. Their protocol made use of an interesting identity-based key construction with pairings, in which an identity string is mapped to a point on an elliptic curve and then the corresponding private key is computed by multiplying the mapped point with the master private key that is a random integer. A similar key construction is also used by Boneh and Franklin (2001) in their well-known security-provable identity-based encryption scheme. After that, many other identity-based key agreement schemes using this key construction were presented, such as Chen and Kudla (2004); Scott (2002); Smart (2002); Wang (2005). A more completed collection of the identity-based key agreement protocols from pairings is given in Chen et al. (2006b). The security of these key agreement schemes were scrutinized (although some errors in a few reductions have been pointed out recently but fixed as well, e.g., Cheng et al. (2004)).

In 2003, Sakai and Kasahara (2003) presented a new identity-based key construction using pairings (SK key construction for short), which can be tracked back to the work by Mitsunari et al. (2002). This key construction has the potential to improve performance, where an identity string is mapped to an element h of the cyclic group $\mathbb{Z}_q^*$ instead of a point on an elliptic curve directly. The corresponding private key is generated by first computing an inverse of the sum of the master secret (a random integer from $\mathbb{Z}_q^*$) and the mapped value h, and then multiplying a point of the elliptic curve (which is the generator of an order q subgroup of the group of points on the curve) with the inverse.

Based on the SK key construction, McCullagh and Barreto (2005) (MB) presented an identity-based authenticated key agreement protocol on CT-RSA 2005, which appears to be more efficient on computation than the above mentioned schemes (Chen and Kudla (2004); Scott (2002); Smart (2002); Wang (2005)). However, as pointed out by Cheng (2004) and Xie (2004), the scheme is vulnerable to a key-compromise impersonation attack, i.e., if an adversary knows a party A's long-term private key, the adversary can impersonate any other party to A. In order to recover this security weakness, McCullagh and Barreto (2004) and Xie (2005) proposed two fixes respectively. Meanwhile, they provided a security reduction for each protocol in the Bellare-Rogaway's key agreement formulation (Bellare and Rogaway (1993); Blake-Wilson et al. (1997)).

In this paper, we revisit the security proofs in McCullagh and Barreto (2005, 2004); Xie (2005) and show that all these three proofs are problematic. More specifically, in their security reductions, the property of indistinguishability between their simulation and the real world was not held. We observe an interesting feature when simulating an identity-based cryptographic world. In any identity-based cryptographic scheme, given a certain identity string, system parameters and key generation center's master public key, it is universally verifiable whether the private key corresponding to the identity string is correctly constructed or not. Therefore, if a simulator is not able to offer an adversary necessary evidence, which allows the adversary to verify the correction of a simulated key construction, the simulation fails, because the adversary can immediately notice the inconsistency between the simulation and the simulated real world. All the three proofs failed to provide this feature.

As pointed out in Li et al. (2005), Xie's scheme still suffers from the key-compromise impersonation attack, hence here we do not formally analyse it. Instead, we slightly modify McCullagh and Barreto's second protocol in McCullagh and Barreto (2004) and then present a formal reduction for the scheme in the Bellare-Rogaway key agreement model. The new reduction demonstrates the security strength of the scheme.

The paper is organized as follows. First, we recall the existing primitives, some related assumptions and the security model of a key agreement scheme in next section. Then, in Section 3 we revisit the three protocols. In our specification, we refer to these protocols as the MB protocol and its variants. We give a sketch of the three security proofs and point out the flaws in the proofs in Section 4. After that, in Section 5 we further modify McCullagh and Barreto's second protocol and present a new reduction for the modified scheme. At the end, we conclude the paper.

2 Preliminaries

Before revisiting the protocols and their proofs, we recall some related pairing primitives, assumptions and the security model of an authenticated key agreement (AK) scheme.

2.1 Bilinear Groups and Some Assumptions

Definition 1. *A pairing is a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with two cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q, which has the following properties:*

1. *Bilinear: $\hat{e}(sP, tR) = \hat{e}(P, R)^{st}$ for all $P, R \in \mathbb{G}_1$ and $s, t \in \mathbb{Z}_q$.*
2. *Non-degenerate: for a given point $Q \in \mathbb{G}_1$, $\hat{e}(Q, R) = 1$ for all $R \in \mathbb{G}_1$ if and only if $Q = 1$.*
3. *Computable: $\hat{e}(P, Q)$ is efficiently computable for any $P, Q \in \mathbb{G}_1$.*

Some researchers have recently worked on varieties of pairings, such as asymmetric pairings in Smart and Vercauteren (2005), where two inputs from two (possibly) different groups are mapped into an element in the third group, i.e., $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$. For the purpose of analysing security of the key agreement protocols based on the SK key construction, in the remaining of this paper, we will focus on a symmetric pairing, i.e., $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

The following Bilinear Diffie-Hellman assumption has been used to construct many exciting cryptography schemes.

Assumption 1. (BDH) *For $x, y, z \in_R \mathbb{Z}_q$, $P \in \mathbb{G}_1^*$, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, given (P, xP, yP, zP), computing $\hat{e}(P, P)^{xyz}$ is hard.*

In McCullagh and Barreto (2005, 2004); Xie (2005), the authors reduced the security of their protocols to the following Bilinear Inverse Diffie-Hellman assumption. The assumption was proved to be equivalent to the BDH assumption in Zhang et al. (2004).

Assumption 2. (BIDH) *For $x, y \in_R \mathbb{Z}_q$, $P \in \mathbb{G}_1^*$, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, given (P, xP, yP), computing $\hat{e}(P, P)^{y/x}$ is hard.*

The decisional variant of the above assumption is as follow:

Assumption 3. (DBIDH) *For $x, y, r \in_R \mathbb{Z}_q$, $P \in \mathbb{G}_1^*$, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, distinguishing $(P, xP, yP, \hat{e}(P, P)^{y/x})$ and $(P, xP, yP, \hat{e}(P, P)^r)$ is hard.*

There are a few related assumptions which have been used in the literature to construct cryptography systems (see Chen and Cheng (2005) for a summary and relations among these assumptions). The decisional variant of the following k-BDHI assumption was used in Boneh and Boyen (2004a) to construct a selective identity-based encryption without random oracles. and in Chen and Cheng

(2005); Chen et al. (2006a) the k-BDHI was used to prove the security of identity-based encryption schemes using SK key construction by Sakai and Kasahara (2003).

Assumption 4. (k-BDHI) *For an integer k, and $x \in_R \mathbb{Z}_q^*$, $P \in \mathbb{G}_1^*$, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, given $(P, xP, x^2P, \ldots, x^kP)$, computing $\hat{e}(P,P)^{1/x}$ is hard.*

Assumption 5. (k-DBDHI) *For an integer k, and $x, r \in_R \mathbb{Z}_q^*$, $P \in \mathbb{G}_1^*$, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, distinguishing between the distributions $(P, xP, x^2P, \ldots, x^kP, \hat{e}(P,P)^{1/x})$ and $(P, xP, x^2P, \ldots, x^kP, \hat{e}(P,P)^r)$ is hard.*

The following k-BCAA1 is a variant of k-BDHI, as discussed in Chen and Cheng (2005).

Assumption 6. (k-BCAA1) *For an integer k, and $x \in_R \mathbb{Z}_q^*$, $P \in \mathbb{G}_1^*, \hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, given $(P, xP, h_0, (h_1, \frac{1}{h_1+x}P), \ldots, (h_k, \frac{1}{h_k+x}P))$ where $h_i \in_R \mathbb{Z}_q^*$ and different from each other for $0 \le i \le k$, computing $\hat{e}(P,P)^{1/(x+h_0)}$ is hard.*

The relationship between k-BDHI and k-BCAA1 has been proved in Chen and Cheng (2005) by the following theorem.

Theorem 1. *If there exists a polynomial time algorithm to solve (k-1)-BDHI, then there exists a polynomial time algorithm for k-BCAA1. If there exists a polynomial time algorithm to solve (k-1)-BCAA1, then there exists a polynomial time algorithm for k-BDHI.*

We shall use the gap variant of k-BCAA1 in this work; that is

Assumption 7. (k-Gap-BCAA1) *For an integer k, and $x \in_R \mathbb{Z}_q^*$, $P \in \mathbb{G}_1^*, \hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, given $(P, xP, h_0, (h_1, \frac{1}{h_1+x}P), \ldots, (h_k, \frac{1}{h_k+x}P))$ where $h_i \in_R \mathbb{Z}_q^*$ and different from each other for $0 \le i \le k$ and the access to a decision BIDH oracle (DBIDH) which given $(P, aP, bP, \hat{e}(P,P)^r)$ returns 1 if $\hat{e}(P,P)^r = \hat{e}(P,P)^{b/a}$, else returns 0, computing $\hat{e}(P,P)^{1/(x+h_0)}$ is hard.*

2.2 Security Model of Key Agreement

In this paper, we use Blake-Wilson *et al.*'s key agreement formulation which extends the Bellare and Rogaway (1993) model to public key construction to test the security strength of a protocol.

In the Bellare-Rogaway model, each party involved in a session is treated as an oracle. An adversary can access the oracle by issuing some specified queries. An oracle $\Pi_{i,j}^s$ denotes an instance s of a party i involved with a partner party j in a session where the instance of the party j is $\Pi_{j,i}^t$ for some t. The oracle $\Pi_{i,j}^s$ executes the prescribed protocol Π and produces the output as $\Pi(1^k, i, j, S_i, P_i, P_j, conv_{i,j}^s,\ r_{i,j}^s, x) = (m, \delta_{i,j}^s, \sigma_{i,j}^s)$ where x is the input message; m is the outgoing message; S_i and P_i are the private/public key pair of party i; P_j is the public key of j; $\delta_{i,j}^s$ is the decision of the oracle (accept or reject the session or no decision yet) and $\sigma_{i,j}^s$ is the generated session key (please see Bellare and Rogaway (1993); Blake-Wilson et al. (1997) for the details). At the end of Π, the conversation transcript $conv_{i,j}^s$ is updated as $conv_{i,j}^s.x.m$ (where "$a.b$" denotes the result of the concatenation of two strings, a and b).

The security of a protocol is tested by a game with two phases. In the first phase, an adversary E is allowed to issue queries as follows in any order.

1. Send a message query: $Send(\Pi_{i,j}^s, x)$. $\Pi_{i,j}^s$ executes $\Pi(1^k, i, j, S_i,\ P_i,\ P_j,\ conv_{i,j}^s,\ r_{i,j}^s, x)$ and responds with m and $\delta_{i,j}^s$. If the oracle $\Pi_{i,j}^s$ does not exist, it will be created. Note that x can be λ in the query which causes an oracle to be generated as an initiator, otherwise as a responder.

2. Reveal a session key: $Reveal(\Pi_{i,j}^s)$. $\Pi_{i,j}^s$ reveals the private output of the session $\sigma_{i,j}^s$ if the oracle accepts.

3. Corrupt a party: $Corrupt(i)$. The party i responds with the private key S_i.

Once the adversary decides that the first phase is over, it starts the second phase by choosing a *fresh oracle* $\Pi_{i,j}^s$ and issuing another query:

4. Test an oracle $Test(\Pi_{i,j}^s)$. Oracle $\Pi_{i,j}^s$, as a challenger, randomly chooses $b \in \{0,1\}$ and responds with $\sigma_{i,j}^s$, if $b = 0$; otherwise it returns a random sample generated according to the distribution of the session secret $\sigma_{i,j}^s$.

After this point the adversary can continue querying the oracles except that it cannot reveal the test oracle $\Pi_{i,j}^s$ or its partner $\Pi_{j,i}^t$ (if it exists), and it cannot corrupt party j. Finally the adversary outputs a guess b' for b. If the adversary guesses the correct b, we say that it wins. Define

$$Advantage^E(k) = \max\{0, \Pr[E \text{ wins}] - \tfrac{1}{2}\}.$$

The fresh oracle in the game is defined as below, which is particularly defined to address the key-compromise impersonation resilience property by Cheng et al. (2004).

Definition 2. (fresh oracle) *An oracle $\Pi_{i,j}^s$ is fresh if (1) $\Pi_{i,j}^s$ has accepted; (2) $\Pi_{i,j}^s$ is unopened (not being issued the* Reveal *query); (3) j is not corrupted (not being issued the* Corrupt *query); (4) there is no opened oracle $\Pi_{j,i}^t$, which has had a matching conversation to $\Pi_{i,j}^s$.*

We stress that in this work, it is required that $i \neq j$ for the chosen fresh oracle in the game (note that the model allows a party to engage in a session with itself).

We use session ID to define **matching conversations**. Two oracles $\Pi_{i,j}^s$ and $\Pi_{j,i}^t$ have a matching conversation to each other if both of them have the same session ID. In this work, we shall use the concatenation of the messages in a session (the transcript of an oracle) to define the session ID.

A secure authenticated key (AK) agreement protocol is defined as below.

Definition 3. Blake-Wilson et al. (1997) *Protocol Π is a secure AK if:*

1. *In the presence of the benign adversary, which faithfully conveys the messages, on $\Pi^s_{i,j}$ and $\Pi^t_{j,i}$, both oracles always accept holding the same session key σ, and this key is distributed uniformly at random on $\{0,1\}^k$;*

and if for every polynomial time adversary E:

2. *If two oracles $\Pi^s_{i,j}$ and $\Pi^t_{j,i}$ have matching conversations and both i and j are uncorrupted, then both accept and hold the same session key σ;*
3. *Advantage$^E(k)$ is negligible.*

3 The MB Protocol and its Variants

In this section, we recall McCullagh and Barreto's protocol and its variants. These protocols use the same key construction (the SK key construction) and exchange the same message flows. However, in the last step of the protocols, each protocol has a different scheme to compute an established session key.

Setup. Given the security parameter k, the algorithm randomly chooses $s \in \mathbb{Z}_q^*$ and generates the system **params** $(\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, sP, H_1, H_2)$ where $P \in \mathbb{G}_1^*$ and $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_2 : \mathbb{G}_2 \to \{0,1\}^n$ for some integer n. The **master key** is s which is kept secret by the center.

Extract. The schemes employ the SK key construction by Sakai and Kasahara (2003). Given an identity ID_A, the **master key** s, and the system **params**, the algorithm computes $H_1(ID_A) = \alpha \in \mathbb{Z}_q^*$ and the corresponding private key $d_A = \frac{1}{s+\alpha}P$ for ID_A. $\alpha P + sP$ will be treated as the real public key corresponding to ID_A.

Protocol. Suppose $H_1(A) = \alpha$ and $H_1(B) = \beta$. Party A and B randomly choose x and y from $\mathbb{Z}_q^*$ respectively. The protocol proceeds as follow.

$$A \to B : T_1 = x(\beta P + sP)$$
$$B \to A : T_2 = y(\alpha P + sP)$$

On completion of the protocol, there are three ways to compute the agreed secret which have different security strength. Here we slightly change the protocols in McCullagh and Barreto (2005, 2004); Xie (2005) by employing an extra hash function on the agreed secret to generate the session keys.

Scheme 1 (McCullagh-Barreto's first scheme in McCullagh and Barreto (2005)). A computes $K = \hat{e}(T_2, d_A)^x = \hat{e}(P, P)^{xy}$ and B computes $K = \hat{e}(T_1, d_B)^y = \hat{e}(P, P)^{xy}$. The agreed session key is $SK = H_2(\hat{e}(P, P)^{xy})$. This scheme *appears* to provide an interesting security property: the perfect forward secrecy (PFS, i.e., if the private keys of both parties are compromised, the agreed session keys between these two parties cannot be recovered by the adversary). However, this scheme does not achieve the key-compromise impersonation resilience as pointed out in Cheng (2004); Xie (2004). To defeat this attack, McCullagh-Barreto and Xie attempted the following two variants respectively.

Scheme 2 (McCullagh-Barreto's second scheme in McCullagh and Barreto (2004)). A computes $K = \hat{e}(T_2, d_A) \cdot \hat{e}(P, P)^x = \hat{e}(P, P)^{x+y}$ and B computes $K = \hat{e}(T_1, d_B) \cdot \hat{e}(P, P)^y = \hat{e}(P, P)^{x+y}$. The agreed session key is $SK = H_2(\hat{e}(P, P)^{x+y})$. Although now the protocol achieves the key-compromise impersonation resilience property, this scheme looses another desirable security attribution: the perfect forward secrecy.

Scheme 3 (Xie's scheme in Xie (2005)). A computes $K = \hat{e}(T_2, d_A)^{x+1} \cdot \hat{e}(P, P)^x = \hat{e}(P, P)^{xy+x+y}$ and B computes $K = \hat{e}(T_1, d_B)^{y+1} \cdot \hat{e}(P, P)^y = \hat{e}(P, P)^{xy+x+y}$. The agreed session key is $SK = H_2(\hat{e}(P, P)^{xy+x+y})$. Unfortunately this modification is still vulnerable to the key-compromise impersonation attack and further suffers from a trivial man-in-the-middle attack as pointed out in Li et al. (2005).

Note that in the original schemes described in McCullagh and Barreto (2005, 2004); Xie (2005), the use of H_2 is not explicitly required. It will result in a potential security problem, which will be discussed in the security proof of Section 4.2.

4 Their Security Proofs

4.1 A Sketch of Their Proofs

In this subsection, we give a sketch of three security proofs from McCullagh and Barreto (2005, 2004); Xie (2005) respectively, each for one variant of the MB protocol as described in Section 3. The proofs were intended to adopt the security model proposed by Bellare and Rogaway (1993) and extended by Blake-Wilson et al. (1997).

All of the three proofs are based on the bilinear inverse Diffie-Hellman (BIDH) problem, described in Assumption 3, i.e., given $(P, \alpha P, \beta P)$, computing $\hat{e}(P, P)^{\beta/\alpha}$ is computationally infeasible. Each proof involves two algorithms: an adversary $\mathcal{A}$ and a challenger (i.e., a simulator of the real world) $\mathcal{B}$. $\mathcal{A}$'s goal is to break a specified protocol, and $\mathcal{B}$'s goal is to solve the BIDH problem with the help of $\mathcal{A}$.

Each proof includes a set of parties, each modelled by an oracle. The notation $\Pi^s_{i,j}$ denotes an oracle i believing that it is participating in the s-th run of the protocol with another oracle j. $\mathcal{A}$ can access any oracle by issuing the queries of Create, Corrupt, Send, and Test. All queries by $\mathcal{A}$ pass through $\mathcal{B}$. Before the game starts, $\mathcal{B}$ randomly selects a pair of oracles, $\Pi^s_{i,j}$ and $\Pi^t_{j,i}$. $\mathcal{B}$ expects that $\mathcal{A}$ is going to attack the oracle $\Pi^s_{i,j}$ by playing the role of $\Pi^t_{j,i}$. In the three proofs, $\mathcal{A}$ and $\mathcal{B}$ play the game described in Section 2.2 in the following three slightly different ways.

Proof 1 (for Scheme 1 in McCullagh and Barreto (2005)). To answer a Create/Corrupt query for any oracle m where $m \neq j$, $\mathcal{B}$ chooses a random integer $y_m \in \mathbb{Z}_q^*$, and answers $y_m P$ as m's public key and $y_m^{-1}P$ as m's private key. $\mathcal{B}$ answers αP as j's public key and does not know j's private key $\alpha^{-1}P$. To answer a Send query for any oracle except $\Pi_{i,j}^s$, $\mathcal{B}$ follows the protocol properly. To answer a Send query for $\Pi_{i,j}^s$, $\mathcal{B}$ chooses a random integer $x_i \in \mathbb{Z}_q^*$ and answers $x_i P$. The proof relies on that an input from $\mathcal{A}$ as $\Pi_{j,i}^t$'s response is exactly the value of βP. After a Test query for $\Pi_{i,j}^s$, if $\mathcal{A}$ successfully breaks Scheme 1 by distinguishing the established key, $K = \hat{e}(P,P)^{x_i\beta/y_i\alpha}$, from a random number, $\mathcal{B}$ can get $\hat{e}(P,P)^{\beta/\alpha}$ by computing K^{y_i/x_i}.

Proof 2 (for Scheme 2 in McCullagh and Barreto (2004)). $\mathcal{B}$ answers Create/Corrupt queries in the same way as it did in Proof 1. To answer a Send query for any oracle except $\Pi_{i,j}^s$, $\mathcal{B}$ follows the protocol properly. To answer a Send query for $\Pi_{i,j}^s$, $\mathcal{B}$ answers βP. The input from $\mathcal{A}$ as $\Pi_{j,i}^t$'s response is an arbitrary value δP. After a Test query for $\Pi_{i,j}^s$, if $\mathcal{A}$ successfully breaks Scheme 2 by distinguishing the established key, $K = \hat{e}(P,P)^{\beta/\alpha+\delta/y_i}$, from a random number, $\mathcal{B}$ can get $\hat{e}(P,P)^{\beta/\alpha}$ by computing $K/\hat{e}(P,P)^{\delta/y_i}$.

Proof 3 (for Scheme 3 in Xie (2005)). To answer a Create/Corrupt query for any oracle m where $m \notin \{i,j\}$, $\mathcal{B}$ chooses a random integer $y_m \in \mathbb{Z}_q^*$, and answers $y_m P$ as m's public key and $y_m^{-1}P$ as m's private key. $\mathcal{B}$ answers αP as i's public key and does not know i's private key $\alpha^{-1}P$. $\mathcal{B}$ answers βP as j's public key and does not know j's private key $\beta^{-1}P$. To answer a Send query for any oracle except $\Pi_{i,j}^s$, $\mathcal{B}$ follows the protocol properly. To answer a Send query for $\Pi_{i,j}^s$, $\mathcal{B}$ chooses a random integer $x_i \in \mathbb{Z}_q^*$ and answers $x_i\beta P$. The proof relies on that an input from $\mathcal{A}$ as $\Pi_{j,i}^t$'s response is exactly the value of βP (i.e., $y_j\alpha P = \beta P$ for some y_j). After a Test query for $\Pi_{i,j}^s$, if $\mathcal{A}$ successfully breaks Scheme 3 by distinguishing the established key, $K = \hat{e}(P,P)^{(x_i+1)\beta/\alpha} \cdot \hat{e}(P,P)^{x_i}$, from a random number, $\mathcal{B}$ can get $\hat{e}(P,P)^{\beta/\alpha}$ by computing $(K/\hat{e}(P,P)^{x_i})^{1/(x_i+1)}$.

4.2 Analysis of Their Proofs

We now show that all the three reductions described in the last subsection are invalid. More specifically, the reductions have following three problems (independently Choo et al. (2005) pointed out some similar errors of McCullagh and Barreto (2005)).

Problem 1: From $\mathcal{A}$'s point view, the simulation offered by $\mathcal{B}$ is distinguishable from the real world of an identity-based authenticated key agreement protocol.

In any identity-based cryptographic world, the correctness of a public/private key pair derived from a chosen identity string, ID, is verifiable, given system parameters and the key generation center's master public key. In those security reductions based on a standard model (e.g., Boneh and Boyen (2004a,b)), an adversary can use ID directly as the public key to verify the result of a private key generation query (i.e., Corrupt query). In those security reductions based on a random oracle model, such as Boneh and Franklin (2001); Chen and Kudla (2004), to verify a correct key deriving can be done with a query of ID to the random oracle. This is acceptable in the random oracle model based reductions, although it is not as ideal as the first case.

It is addressed in McCullagh and Barreto (2005, 2004); Xie (2005) that the identity map function H_1 in the MB protocol and its variants is by means of the random oracle model. However, how to respond to the H_1 query is not specified in these three proofs. Another related missing part is that these three proofs do not specify either which entity has the access to the value of s, or what the system parameters that $\mathcal{A}$ would get access to should be. We can see that $\mathcal{B}$ is not able to answer the H_1 query by following the Create and Corrupt queries specified in these three proofs. As a result, $\mathcal{A}$ cannot verify correctness of either Create or Corrupt query result from ID and the system parameters. $\mathcal{A}$ can then immediately notice that $\mathcal{B}$ is a simulator, instead of the real world. We discuss this issue in the following two cases, dependent on whether or not $\mathcal{B}$ knows the value of s.

1. The value s is not known to $\mathcal{B}$. Following the three proofs, to answer the Create/Corrupt query to an oracle with the identity ID_m, $\mathcal{B}$ assigns a random element pair, $y_m P$, $y_m^{-1}P \in \mathbb{G}_1^*$, as the public/private key pair. However, $\mathcal{B}$ is not able to give the value of $u_m = H_1(ID_m)$, satisfying $u_m P = y_m P - sP$, because to solve the discrete logarithm problem in $\mathbb{G}_1$ is computational infeasible, which is implied by the used BIDH assumption. Therefore, $\mathcal{B}$ is not able to answer the oracle query $H_1(ID_m)$, and $\mathcal{A}$ then cannot verify correctness of the received $y_m P$ and $y_m^{-1}P$ from ID_m and sP.

2. The value s is chosen by $\mathcal{B}$. Following the reductions, to answer the Create query to an oracle with the identity ID_j in Proof 1 and Proof 2 (or ID_i in Proof 3), $\mathcal{B}$ assigns $\alpha P \in \mathbb{G}_1^*$, as the public key to the party j (or i). However, again $\mathcal{B}$ is not able to give the value of u_j (or u_i), satisfying $u_j P$ (or $u_i P$) $= \alpha P - sP$, because to solve the discrete logarithm problem in $\mathbb{G}_1$ is supposed to be computational infeasible. Therefore $\mathcal{B}$ is not able to answer the oracle query $H_1(ID_j) = u_j$ (or $H_1(ID_i) = u_i$) and $\mathcal{A}$ then cannot verify correctness of the received public key αP for ID_j (or ID_i) under the master public key sP.

In conclusion, since $\mathcal{B}$ cannot answer some H_1 queries, $\mathcal{A}$ can immediately notice the inconsistency between the simulation and the real world.

Problem 2: $\mathcal{B}$ in Proof 1 and Proof 3 requires that $\mathcal{A}$ provides an expected value as a response to a specific oracle. This is not a reasonable requirement.

This is because $\mathcal{A}$ is not controlled by $\mathcal{B}$. Even the assumption that the adversary would follow the protocol strictly to generate messages is too strong to cover many dangerous attacks. A sound reduction can only require that messages from the adversary are in the specified message space at most.

Problem 3: H_2 is not clearly required in the MB protocol and its variants. This results in that the reduction to the computational BIDH assumption does not follow.

The simulation $\mathcal{B}$ cannot be created based on the BIDH assumption for the original protocols in McCullagh and Barreto (2005, 2004); Xie (2005). Instead, even if both Problem 1 and 2 are solved, a simulation could only be created based on the decision BIDH for the original protocols if they are secure. Otherwise, the adversary can win the game with the probability to differentiate a random element of $\mathbb{G}_2$ from the true value. This is the reason why we employ an extra hash function on the agreed secret to generate a session key SK.

5 The Modified Scheme and Its Security Analysis

As pointed in Choo (2004), Scheme 2 does not achieve the known-session key security (i.e., the compromise of one session key would not affect other session keys' security), and so cannot be proved in the Bellare-Rogaway key agreement model with the Reveal query allowed (note that the reduction in McCullagh and Barreto (2004) proceeds in the model with the Reveal query disallowed, though it is invalid). However, we can slightly tweak the session key generation method in Scheme 2 to recover from the attack, furthermore the modification enables us to reduce the security of the scheme to the k-Gap-BCAA1 assumption in the full Bellare-Rogaway model. The modified scheme, which we refer to as **Scheme** $2'$, is as follow:

$$SK = H_3(A, B, T_1, T_2, \hat{e}(P, P)^{x+y}),$$

where $H_3 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{G}_2 \to \{0,1\}^n$ is a hash function. As the original protocol, the new scheme still cannot achieve PFS.

Before presenting the detailed proof, we should note that as pointed out in Cheng et al. (2006), when receiving a message T a party in general should check that T is in the specified message space, in this case, $\mathbb{G}_1^*$, then to accept the session. Otherwise, potential attacks are feasible, for example, if T is with small order, so could K be, and the adversary can enumerate the result group to compromise K.

Theorem 2. *Scheme $2'$ is a secure AK, provided that H_1, H_3 are random oracles and the k-Gap-BCAA1 assumption is sound. Specifically, suppose that there is an adversary $\mathcal{A}$ against the protocol with non-negligible probability $n(k)$ and in the attack H_1 has been queried q_1 times and q_o oracles have been created. Then there exists an algorithm $\mathcal{B}$ solve the (q_1-1)-Gap-BCAA1 problem with advantage*

$$Adv_{\mathcal{B}}^{(q_1-1)-Gap-BCAA1}(k) \geq \frac{1}{q_1 \cdot q_o} n(k).$$

Proof. We shall use the message transcript $T_1 \| T_2$ as the session ID to define matching conversations. The conditions 1 and 2 directly follow from the protocol specification. In the sequel we prove that the protocol satisfies the condition 3. We show that if $\mathcal{A}$ exists, we can construct an algorithm $\mathcal{B}$ to solve a $(q_1 - 1)$-Gap-BCAA1 problem with non-negligible probability.

Given an instance of the $(q_1 - 1)$-Gap-BCAA1 problem $(\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, (P, sP, \ h_0, \ (h_1, \ \frac{1}{h_1+s}P), \ \ldots, (h_{q_1-1}, \frac{1}{h_{q_1-1}+s}P))$ where $h_i \in_R \mathbb{Z}_q^*$ for $0 \leq i \leq q_1 - 1$ and the DBIDH oracle $\mathcal{O}_{\mathtt{DBIDH}}$, $\mathcal{B}$ simulates the **Setup** algorithm to generate the system **params** $(\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, sP, H_1, H_3)$ (i.e., using s as the **master key** which it does not know). H_1 and H_3 are two random oracles controlled by $\mathcal{B}$.

In the proof, we slightly abuse the notation $\Pi_{i,j}^s$ as the s-th oracle among all the oracles created during the attack, instead of the s-th instance of i. This change does not affect the soundness of the model because s originally is just used to uniquely identify an instance of party i. $\mathcal{B}$ randomly chooses $u \in_R \{1, \ldots, q_o\}$ and $I \in_R \{1, \ldots, q_1\}$ and interacts with $\mathcal{A}$ in the following way:

H_1-queries (ID_i)**:** $\mathcal{B}$ maintains a list of tuples (ID_i, h_i, d_i) as explained below. We refer to this list as H_1^{list}. The list is initially empty. When $\mathcal{A}$ queries the oracle H_1 at a point on ID_i, $\mathcal{B}$ responds as follows:

- If ID_i already appears on the H_1^{list} in a tuple (ID_i, h_i, d_i), then $\mathcal{B}$ responds with $H_1(ID_i) = h_i$.
- Otherwise, if the query is on the I-th distinct ID, then $\mathcal{B}$ stores $(ID_I, h_0, \perp)$ into the tuple list and responds with $H_1(ID_I) = h_0$.
- Otherwise, $\mathcal{B}$ selects a random integer $h_i (i > 0)$ from the $(q_1 - 1)$-Gap-BCAA1 instance which has not been chosen by $\mathcal{B}$ and stores $(ID_i, h_i, \frac{1}{h_i+s}P)$ into the tuple list. $\mathcal{B}$ responds with $H_1(ID_i) = h_i$.

H_3-queries $(ID_i, ID_j, T_i, T_j, K_t)$**:** At any time $\mathcal{A}$ can issue queries to the random oracle H_3. To respond to these queries $\mathcal{B}$ maintains a list of tuples called H_3^{list}. Each entry in the list is a tuple of the form $(ID_i, ID_j, T_i, T_j, K_t, \zeta_t, O_t)$ indexed by $(ID_i, ID_j, T_i, T_j, K_t)$. To respond to a query, $\mathcal{B}$ does the following operations:

- If on the list there is a tuple indexed by $(ID_i, ID_j, T_i, T_j, K_t)$, then $\mathcal{B}$ responds with ζ_t.
- Otherwise, $\mathcal{B}$ goes through the list Λ built in the Reveal query to find tuples of the form $(ID_i, ID_j, T_i, T_j, r^t, \zeta^t, O^t)$ and proceeds as follow:

– Compute $D = K_t/(P,P)^{r^t}$.

– Access $\mathcal{O}_{\texttt{DBIDH}}(P,(h_0+s)P,T_j,D)$ if $O^t = 0$ or access $\mathcal{O}_{\texttt{DBIDH}}(P,(h_0+s)P,T_i,D)$ otherwise. If $\mathcal{O}_{\texttt{DBIDH}}$ returns 1, $\mathcal{B}$ inserts $(ID_i, ID_j, T_i, T_j, K_t, \zeta^t)$ into H_3^{list} and responds with ζ^t to the query and removes the tuple from Λ.

- Otherwise, $\mathcal{B}$ randomly chooses a string $\zeta_t \in \{0,1\}^n$ and inserts a new tuple $(ID_i, ID_j, T_i, T_j, K_t, \zeta_t)$ into the list H_3^{list}. It responds to $\mathcal{A}$ with ζ_t.

Corrupt($\mathbf{ID}_i$): $\mathcal{B}$ looks through list H_1^{list}. If ID_i is not on the list, $\mathcal{B}$ queries $H_1(ID_i)$. $\mathcal{B}$ checks the value of d_i: if $d_i \neq \perp$, then $\mathcal{B}$ responds with d_i; otherwise, $\mathcal{B}$ aborts the game (**Event 1**).

Send$(\Pi^t_{j,i}, T)$**:** $\mathcal{B}$ maintains a list with tuples of $(\Pi^t_{j,i}, r^t_{j,i}, tran^t_{j,i})$ and responds to the query as follow:

- $\mathcal{B}$ looks through the list H_1^{list}. If ID_i is not on the list, $\mathcal{B}$ queries $H_1(ID_i)$. After that, $\mathcal{B}$ checks the value of t.
- If $t \neq u$, $\mathcal{B}$ honestly follows the protocol to respond the query by randomly sampling $r^t_{j,i} \in \mathbb{Z}_q^*$ and generating the message $r^t_{j,i}(H_1(ID_i)P + sP)$.
- If $t = u$, $\mathcal{B}$ further checks the value of d_i, and then responds the query differently as below depending on this value.

  – If $d_i \neq \perp$, $\mathcal{B}$ aborts the game (**Event 2**). We note that there is only one party's private key is represented as $\perp$ in the whole simulation.

  – Otherwise, $\mathcal{B}$ randomly chooses $y \in \mathbb{Z}_q^*$ and responds with yP. Note that $\Pi^t_{j,i}$ can be the initiator (if $T = \lambda$) or the responder (if $T \neq \lambda$).

Reveal$(\Pi^t_{j,i})$**:** $\mathcal{B}$ maintains an initially empty list Λ with tuples $(ID_i, ID_j, T_i, T_j, \ r^t, \zeta^t, O^t)$. $\mathcal{B}$ responds to the query as follow:

- If $t = u$ or if the u-th oracle has been generated as $\Pi^u_{a,b}$ and $ID_a = ID_i, ID_b = ID_j$ and two oracles have the same session ID, then abort the game (**Event 3**).
- Go through $H_1^{list}(ID_j)$ to find the private key d_j of party j with identity ID_j.
- If $d_j \neq \perp$, compute $K = \hat{e}(T_i, d_j) \cdot \hat{e}(P,P)^{r^t_{j,i}}$ where T_i is the incoming message and $r^t_{j,i}$ is the random flips of the oracle $\Pi^t_{j,i}$. $\mathcal{B}$ responds with $H_3(ID_j, ID_i, T_j, T_i, K)$ if the oracle is the initiator, otherwise $H_3(ID_i,\ ID_j,\ T_i,\ T_j,\ K)$.
- Otherwise, $\mathcal{B}$ goes through H_3^{list} to find tuples indexed by (ID_j, ID_i, T_j, T_i) (if $\Pi^t_{j,i}$ is the initiator) or by (ID_i, ID_j, T_i, T_j) (if $\Pi^t_{j,i}$ is the responder). For each (K_t, ζ_t) in the found tuples,

  – Compute $D = K_t/\hat{e}(P,P)^{r^t_{j,i}}$.

  – Access $\mathcal{O}_{\texttt{DBIDH}}(P,(h_0+s)P,T_i,D)$. If $\mathcal{O}_{\texttt{DBIDH}}$ returns 1, then $\mathcal{B}$ responds to the query with ζ_t. Note that there can be at most one K_t meeting the test.

- Otherwise (no K_t is found in the last step), randomly choose $\zeta^t \in \{0,1\}^n$ and insert $(ID_j, ID_i, T_j, T_i, r^t_{j,i}, \zeta^t, 0)$ if the oracle is the initiator, or $(ID_i,\ ID_j,\ T_i,\ T_j,\ r^t_{j,i},\ \zeta^t, 1)$ into Λ. $\mathcal{B}$ responds with ζ^t.

Test$(\Pi^t_{j,i})$**:** If $t \neq u$ or $(t = u$ but) there is an oracle $\Pi^w_{i,j}$ with the same session ID with $\Pi^t_{j,i}$ that has been revealed, $\mathcal{B}$ aborts the game (**Event 4**). Otherwise, $\mathcal{B}$ randomly chooses a number $\zeta \in \{0,1\}^n$ and gives it to $\mathcal{A}$ as the response.

Once $\mathcal{A}$ finishes the queries and returns its guess, $\mathcal{B}$ goes through H_3^{list} and for each K_ℓ,

- Compute $D = (K_\ell/\hat{e}(T, d_j))^{1/y}$, where T is the incoming message to the tested oracle $\Pi^u_{j,i}$.
- Access $\mathcal{O}_{\texttt{DBIDH}}(P,(h_0+s)P,P,D)$. If $\mathcal{O}_{\texttt{DBIDH}}$ returns 1, $\mathcal{B}$ returns D as the response of the (q_1-1)-Gap-BCAA1 challenge.
- If no K_ℓ meets the test, fail the game.

Claim 1. *If algorithm $\mathcal{B}$ does not abort during the simulation, then algorithm $\mathcal{A}$'s view is identical to its view in the real attack.*

Proof. $\mathcal{B}$'s responses to H_1 queries are uniformly and independently distributed in $\mathbb{Z}_q^*$ as in the real attack. H_3 is modelled as a random oracle which requires that for each unique input, there should be only one response. We note that the simulation substantially makes use of the programmability of random oracle and the access to the DBIDH oracle to guarantee the unique response for every H_3 query. The responses in other types of query are valid as well. Hence the claim follows. □

Now let us evaluate the probability that $\mathcal{B}$ did not abort the game. $\mathcal{B}$ aborts the game only when at least one of following events happens: (1) **Event 1**, denoted as $\mathcal{H}_1$: $\mathcal{A}$ corrupted party i whose private key is represented by $\perp$ at some point; (2) **Event 2**, denoted as $\mathcal{H}_2$: in the u-th session, if $\mathcal{A}$ impersonated a party, it did not impersonate party i whose private key is represented by $\perp$ (recall that oracle $\Pi^u_{j,i}$ was simulated by $\mathcal{B}$ in the game. It is not important who sent the message T to $\Pi^u_{j,i}$. It could be the adversary who impersonated party i or an oracle $\Pi^v_{i,j}$ for some v); (3) **Event 3**, denoted as $\mathcal{H}_3$: $\mathcal{A}$ revealed the u-th oracle or its partner oracle. (4) **Event 4**, denoted as $\mathcal{H}_4$: $\mathcal{A}$ did not choose the u-th oracle as the challenge fresh oracle.

Note that according to the rules of the game, the adversary would not corrupt party i if it chose $\Pi^u_{j,i}$ as the fresh oracle. Hence $\neg\mathcal{H}_4 \wedge \neg\mathcal{H}_2$ implies $\neg\mathcal{H}_1$ (recall that in this work, we require that $j \neq i$ for the chosen fresh oracle

$\Pi^t_{j,i}$, i.e., in the attacked session the victim party did not establish the session with itself. This is not an unusual requirement in the real practice) and $\neg\mathcal{H}_4$ implies $\neg\mathcal{H}_3$. Let $\mathcal{F}$ be the event that $\mathcal{B}$ did not abort the game. Then, we have

$$\begin{aligned}\Pr[\mathcal{F}] &= \Pr[\neg\mathcal{H}_1 \wedge \neg\mathcal{H}_2 \wedge \neg\mathcal{H}_3 \wedge \neg\mathcal{H}_4] \\ &= \Pr[\neg\mathcal{H}_2 \wedge \neg\mathcal{H}_4] \\ &\geq \tfrac{1}{q_1} \cdot \tfrac{1}{q_o}.\end{aligned}$$

Claim 2. *The adversary has computed the agreed secret K in the challenge session with non-negligible probability $n(k)$ if the game did not abort.*

Proof. Suppose in the game, the chosen fresh oracle for the Test query is $\Pi^t_{j,i}$ and party j is the initiator (the result holds if party j is the responder for the similar reason). Let $\mathcal{H}$ be the event that $(ID_j, ID_i, T^t_j, T^t_i, *)$ has been queried on H_3 where T^t_j is the message from j and T^t_i is the message from party i or the adversary $\mathcal{A}$. Now let us consider the following situations:

- Situation 1. $\mathcal{A}$ reveals $\Pi^w_{u,v}$ where $u \notin \{i,j\}$ or $v \notin \{i,j\}$ or $u = v = i$ or $u = v = j$, i.e., IDs are different from the fresh oracle. Because ID_u and ID_v, instead of ID_j and ID_i, will be queried as the identifier to H_3, event $\mathcal{H}$ will not be caused by such Reveal queries. Recall that for the chosen fresh oracle as the challenge, it is required that $i \neq j$.

- Situation 2. $\mathcal{A}$ reveals $\Pi^w_{i,j}$ where i is the initiator (if j is the responder for the chosen fresh oracle, then i is the responder, i.e., party i has the same role in the w-th session as j in the t-th session). The Reveal query will only query in the form of $H_3(ID_i, ID_j, *, *, *)$, so event $\mathcal{H}$ will not be caused by this type of Reveal query.

- Situation 3. $\mathcal{A}$ reveals $\Pi^w_{i,j}$ where i is the responder (if j is the responder for the chosen fresh oracle, then i is the initiator, i.e., party i and j have matching roles in the sessions). In this case, H_3 could be queried on $(ID_j, ID_i, T^w_j, T^w_i, *)$. Because of the rule of the game, $\Pi^w_{i,j}$ has no matching conversation to $\Pi^t_{j,i}$, which means either $T^t_j \neq T^w_j$ or $T^t_i \neq T^w_i$ (recall that the session ID which is the message transcript of the session, is used to define matching conversations. Two oracles have matching conversation to each other if both have the same message transcript). Hence event $\mathcal{H}$ will not be caused by this type of Reveal query.

- Situation 4. $\mathcal{A}$ reveals $\Pi^w_{j,i}$ for $w \neq t$ and party j has the different roles in the t-th and w-th session. As analysed in Situation 2, event $\mathcal{H}$ will not be caused by this type of Reveal query.

- Situation 5. $\mathcal{A}$ reveals $\Pi^w_{j,i}$ for $w \neq t$ and party j has the same role in the t-th and w-th session. Because for both oracles $\Pi^t_{j,i}$ and $\Pi^w_{j,i}$, j is not controlled by the adversary, it is only negligibly likely that $T^t_j = T^w_j$ if the used random flips are generated uniformly. Hence event $\mathcal{H}$ will not (or with only negligible probability) be caused by this type of Reveal query.

Let $\mathcal{H}'$ be the event that $H_3(ID_j, ID_i, T^t_j, T^t_i, K^t_{j,i})$ was queried where $K^t_{j,i}$ is the agreed secret of $\Pi^t_{j,i}$. We note here there are two possibilities that event $\mathcal{H}'$ happens in the proof of using random oracles.

- Case 1. The simulator which could not compute $K^t_{j,i}$ but was forced to respond with a random sample ζ^t in some Reveal query. Hence though the oracle H_3 was not explicitly queried with the tuple value, in this case, we regard that $\mathcal{H}'$ has happened, as the random oracle should return a unique result corresponding to each unique input and if H_3 is later explicitly queried on $(ID_j, ID_i, T^t_j, T^t_i, K^t_{j,i})$, then ζ^t should be returned.

- Case 2. The adversary queried H_3 with $(ID_j, ID_i, T^t_j, T^t_i, K^t_{j,i})$.

As analysed above, we know that the Reveal queries won't cause $\mathcal{H}$ with non-negligible probability. Hence Case 1 will only happen with negligible probability at most. In other words, event $\mathcal{H}'$ happens with non-negligible probability only if $\mathcal{A}$ has queried $H_3(ID_j, ID_i, T^t_j, T^t_i, K^t_{j,i})$.

As H_3 is a random oracle, we have $\Pr[\mathcal{A} \text{ wins}|\neg\mathcal{H}'] = \frac{1}{2}$. Then we have

$$\begin{aligned}n(k) + \tfrac{1}{2} = \;& \Pr[\mathcal{A} \text{ wins}] \\ = \;& \Pr[\mathcal{A} \text{ wins}|\mathcal{H}'] \Pr[\mathcal{H}'] \\ & + \Pr[\mathcal{A} \text{ wins}|\neg\mathcal{H}'] \Pr[\neg\mathcal{H}'] \\ \leq \;& Pr[\mathcal{H}'] + \tfrac{1}{2}.\end{aligned}$$

So, $\Pr[\mathcal{H}'] \geq n(k)$, which means, $\mathcal{A}$ has computed $K^t_{j,i}$ with probability $n(k)$ and queried it on H_3. □

Note the agreed secret in the chosen fresh oracle $\Pi^t_{j,i}$ should be $K = \hat{e}(T, d_j) \cdot \hat{e}(P, P)^r$ where $r(h_0P + sP) = yP$ (recall that party i's public key is $h_0P + sP$ and the private key is unknown to $\mathcal{B}$ and represented by $\perp$), i.e., $r = \frac{y}{h_0+s}$ and $K = \hat{e}(T, d_j) \cdot \hat{e}(yP, \frac{1}{h_0+s}P)$. From Claim 2 we have

$$\Pr[\mathcal{B} \text{ wins}] = \Pr[\mathcal{F} \wedge \mathcal{H}'] \geq \frac{1}{q_1 \cdot q_o} \cdot n(k).$$

This completes the security analysis of the protocol. □

6 Conclusion

In this paper, we have revisited the security proofs of three identity-based authenticated key agreement schemes using the Sakai and Kasahara key construction and pointed out the flaws in the reductions. We have also slightly modified McCullagh and Barreto's second protocol and provided a new reduction for the modified scheme based on the k-Gap-BCAA1 assumption in the Bellare-Rogaway's key agreement formulation.

REFERENCES

Bellare, M. and Rogaway, P. (1993) 'Entity authentication and key distribution', In *Proceedings of Advances in Cryptology - Crypto '93*, LNCS 773, pp. 232–249, 1993.

Bellare, M., Pointcheval, D. and Rogaway, P. (2000) 'Authenticated key exchange secure against dictionary attacks', In *Proceedings of Proceedings of Advances in Cryptology - Eurocrypt 2000*, LNCS 1807, pp. 139–155, 2000.

Blake-Wilson, S., Johnson, D. and Menezes, A (1997) 'Key agreement protocols and their security analysis', In *Proceedings of the Sixth IMA International Conference on Cryptography and Coding*, LNCS 1355, pp. 30–45, 1997.

Boneh, D. and Franklin, M. (2001) 'Identity based encryption from the Weil pairing', In *Proceedings of Advances in Cryptology - Crypto 2001*, LNCS 2139, pp. 213–229, 2001.

Boneh, D. and Boyen, X. (2004) 'Efficient selective-ID secure identity based encryption without random oracles', In *Proceedings of Advances in Cryptology - Eurocrypt'2004*, LNCS 3027, pp. 223–238, 2004.

Boneh, D. and Boyen, X. (2004) 'Secure identity-based encryption without random oracles', In *Proceedings of Advances in Cryptology - Crypto 2004*, LNCS 3152, pp. 443–459, 2004.

Chen, L. and Kudla, C. (2004) 'Identity based authenticated key agreement from pairings', In *Proceedings of the 16th IEEE Computer Security Foundations Workshop*, pp. 219–233, June 2003.

Chen, L. and Cheng, Z. (2005) 'Security proof of the Sakai-Kasahara's identity-based encryption scheme', In *Proceedings of Cryptography and Coding 2005*, LNCS 3706, pp. 442–459, 2005.

Chen, L., Cheng, Z., Malone-Lee, J. and Smart, N. (2006) 'An efficient ID-KEM based on the Sakai-Kasahara key construction', *IEE Proceedings of Information Security*, **153**, pp. 19–26 2006.

Chen, L., Cheng, Z., and Smart, N. (2006) 'Identity-based key agreement protocols from pairings', Cryptology ePrint Archive, Report 2006/199, 2006.

Cheng, Z., Nistazakis, M., Comley, R. and Vasiu, L. (2004) 'On the indistinguishability-based security model of key agreement protocols-simple cases', In *Proceedings of ACNS 2004 (technical track)*. The full paper available on Cryptology ePrint Archive, Report 2005/129.

Cheng, Z. (2004) 'Private communication', 2004.

Cheng, Z., Chen, L., Comley, R. and Tang, Q. (2006) 'Identity-based key agreement with unilateral identity privacy using pairings', In *Proceedings of Information Security Practice and Experience 2006*, LNCS 3903, pp. 202–213, 2006.

Choo, K.-K. R. (2004) 'Revisit of McCullagh–Barreto two-party ID-based authenticated key agreement protocols', Cryptology ePrint Archive, Report 2004/343.

Choo, K.-K. R., Boyd, C. and Hitchcock, Y. (2005) 'On session key construction in provably-secure key establishment protocols: revisiting Chen & Kudla (2003) and McCullagh & Barreto (2005) ID-based protocols', In *Proceedings of Mycrypt 2005*, LNCS 3715, pp. 116–131, 2005.

ISO/IEC 11770-3:1999 'Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques'.

Li, S., Yuan, Q. and Li, J. (2005) 'Towards security two-party authenticated key agreement protocols', Cryptology ePrint Archive, Report 2005/300.

McCullagh, N. and Barreto, P.S.L.M. (2004) 'A new two-party identity-based authenticated key agreement', Cryptology ePrint Archive, Report 2004/122.

McCullagh, N. and Barreto, P.S.L.M. (2005) 'A new two-party identity-based authenticated key agreement', In *Proceedings of CT-RSA 2005*, LNCS 3376, pp. 262–274, 2005.

Menezes, A., van Oorschot, P. and Vanstone, S. (2001) 'Handbook of applied cryptography', CRC Press, 2001.

Mitsunari, S., Sakai, R. and Kasahara, M. (2002) 'A new traitor tracing', *IEICE Trans. Fundamentals*, E85-A(2):481–484, 2002.

Okamoto, E. (1986) 'Proposal for identity-based key distribution system', *Electronics Letters*, 22:1283–1284, 1986.

Sakai, R., Ohgishi, K. and Kasahara, M. (2000) 'Cryptosystems based on pairing', In *Proceedings of 2000 Symposium on Cryptography and Information Security*, Okinawa, Japan, 2000.

Sakai, R. and Kasahara, M. (2003) 'ID based cryptosystems with pairing on elliptic curve', Cryptology ePrint Archive, Report 2003/054.

Scott, M. (2002) 'Authenticated ID-based key exchange and remote log-in with insecure token and PIN number', Cryptology ePrint Archive, Report 2002/164, 2002.

Shamir, A. (1985) 'Identity-based cryptosystems and signature schemes', In *Proceedings of Advances in Cryptology - Crypto '84*, LNCS 196, pp.47–53, 1985.

Smart, N. P. (2002) 'An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairing', *Electronics Letters* 38 (2002), pp. 630–632.

Smart, N. and Vercauteren, F. (2005) 'On computable isomorphisms in efficient piaring based systems', Cryptology ePrint Archive, Report 2005/116.

Tanaka, K. and Okamoto, E. (1991) 'Key distribution system for mail systems using ID-related information directory', *Computers & Security*, 10:25–33, 1991.

Wang, Y. (2005) 'Efficient identity-based and authenticated key agreement protocol', Cryptology ePrint Archive, Report 2005/108.

Xie, G. (2004) 'Cryptanalysis of Noel McCullagh and Paulo S. L. M. Barreto's two-party identity-based key agreement', Cryptology ePrint Archive, Report 2004/308.

Xie, G. (2005) 'An ID-based key agreement scheme from pairing', Cryptology ePrint Archive, Report 2005/093.

Zhang, F., Safavi-Naini, R. and Susilo, W. (2004) 'An efficient signature scheme from bilinear pairings and its applications', In *Proceedings of International Workshop on Practice and Theory in Public Key Cryptography - PKC 2004*, LNCS 2947, pp. 277–290, 2004.