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

Zhaohui Cheng[1] and Liqun Chen[2]

[1]School of Computing Science, Middlesex University
White Hart Lane, London N17 8HR, UK
m.z.cheng@mdx.ac.uk
[2]Hewlett-Packard Laboratories, Bristol, UK
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 present a new reduction for the McCullagh and Barreto modified protocol in the weaker Bellare-Rogaway key agreement model. Our reduction is based on a new assumption, which is at least as weak as some well-explored assumptions in the literature.

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 in 1984 [23] 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 setting that was based on the RSA problem, and presented an identity-based signature scheme. By using varieties of the Shamir key setting, a number of identity-based key agreement schemes were proposed (e.g., [13, 14, 19, 26]).

In 2000, Sakai et al. introduced an identity-based key agreement scheme based on bilinear pairings over elliptic curves [21]. Their protocol made use of an interesting identity-based key setting 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 setting is also used by Boneh and Franklin in their well-known provable identity-based encryption scheme [7]. After that, many other identity-based key agreement schemes using this key setting were presented, such as [9, 22, 24, 27]. 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., [11]).

In 2003, Sakai and Kasahara presented a new identity-based key setting using pairings (SK key setting for short) [20], which can be tracked back to the work in [18]. This key setting 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 setting, McCullagh and Barreto (MB) presented an identity-based authenticated key agreement protocol on CT-RSA 2005 [15], which appears to be more efficient on computation than the above mentioned schemes [9, 22, 24, 27]. However, as pointed out by Cheng [10] and Xie [29], 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 [16], and Xie [30] proposed two fixes respectively. Meanwhile, they provided a security reduction for each protocol in a weaker model of Bellare-Rogaway's key agreement formulation [2, 4].

In this paper, we revisit the security proofs in [15, 16, 30] 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 a public/private key pair 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 setting, 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 a replacement, we present a new reduction for the McCullagh and Barreto modified protocol [16] in the weaker Bellare-Rogaway key agreement model. Our reduction is based on a new assumption, which as shown in the paper is weaker (or at least as weak as) some well-explored assumptions in the literature. Unfortunately, we can not find replacements to prove the MB original protocol [15] and Xie's modification [30]. We leave them as an open problem.

The paper is organized as follows. First, we recall the existing primitive, 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 present a new reduction for McCullagh-Barreto's modified protocol. Before concluding the paper in Section 7, we give a few comments on the new reduction in Section 6.

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 [7]:*

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 $Q \in \mathbb{G}_1$, $\hat{e}(Q, R) = 1_{\mathbb{G}_2}$ for all $R \in \mathbb{G}_1$ if and only if $Q = 1_{\mathbb{G}_1}$.*
3. *Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}_1$.*

Some researchers have recently worked on varieties of pairings, such as asymmetric pairings [25], 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 analyzing security of the key agreement protocols based on the SK key setting, 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 [7]) *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 $\langle P, xP, yP, zP \rangle$, to compute $\hat{e}(P, P)^{xyz}$ is hard.*

In [15, 16, 30], 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 [31].

Assumption 2 (BIDH [31]) *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 $\langle P, xP, yP \rangle$, to compute $\hat{e}(P, P)^{y/x}$ is hard.*

There are a few related assumptions which have been used in the literature to construct cryptography systems (see [8] for a summary and relations among these assumptions). The following decision k-BDHI assumption was used in [5] to construct a selective identity-based encryption without random oracles, and in [8] to prove the security of Sakai et al.'s identity-based encryption scheme [20].

Assumption 3 (k-BDHI [5]) *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 $\langle P, xP, x^2P, \ldots, x^kP \rangle$, to compute $\hat{e}(P,P)^{1/x}$ is hard.*

Assumption 4 (k-DBDHI [5]) *For an integer k, and $x, r \in_R \mathbb{Z}_q^*$, $P \in \mathbb{G}_1^*$, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, to distinguish between the distributions $\langle P, xP, x^2P, \ldots, x^kP, \hat{e}(P,P)^{1/x} \rangle$ and $\langle P, xP, x^2P, \ldots, x^kP, \hat{e}(P,P)^r \rangle$ is hard.*

Assumption 5 (k-BCAA1 [8]) *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 $\langle P, xP, h_0, (h_1, \frac{1}{h_1+x}P), \ldots, (h_k, \frac{1}{h_k+x}P) \rangle$ where $h_i \in_R \mathbb{Z}_q^*$ and different from each other for $0 \le i \le k$, to compute $\hat{e}(P,P)^{1/(x+h_0)}$ is hard.*

The relationship between k-BDHI and k-BCAA1 has been proved in [8] by the following theorem.

Theorem 1 ([8]) *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.*

Assumption 6 (k-sCAA1 [31]) *For an integer k, and $x \in_R \mathbb{Z}_q^*$, $P \in \mathbb{G}_1^*$, given $\langle P, xP, (h_1, \frac{1}{h_1+x}P), \ldots, (h_k, \frac{1}{h_k+x}P) \rangle$ where $h_i \in_R \mathbb{Z}_q^*$ and different from each other for $1 \le i \le k$, to compute $(h, \frac{1}{h+x}P)$ for some $h \in \mathbb{Z}_q^*$ but $h \notin \{h_1, \ldots, h_k\}$ is hard.*

Here we propose a new assumption. We call it k-EBCAA1 which is the variant of the k-BCAA1 assumption presented in [8].

Assumption 7 (k-EBCAA1) *For an integer k, and $x, y \in_R \mathbb{Z}_q^*$, $P \in \mathbb{G}_1^*, \hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, given $\langle P, xP, h_0, (h_1, \frac{1}{h_1+x}P), \ldots, (h_k, \frac{1}{h_k+x}P), yP \rangle$ where $h_i \in_R \mathbb{Z}_q^*$ and different from each other for $0 \le i \le k$, to compute $\hat{e}(\frac{1}{h_0+x}P, yP)$ is hard.*

We argue that the assumption k-EBCAA1 is weaker or at least as weak as the k-BDHI assumption (we note here that a weaker assumption implies a harder problem). The relation can be easily established from Theorem 1 and the fact that if there exists a polynomial time algorithm to solve k-EBCAA1, then there exists a polynomial time algorithm for k-BCAA1. This fact follows obviously.

2.2 Security model of key agreement

In this paper, we use Blake-Wilson et al.'s key agreement formulation which extends the Bellare-Rogaway (BR) model [2] to public key setting to test the security strength of a protocol. In the BR model [2], each party involved in a session is treated as an oracle. An adversary can access the oracle by issuing some specified queries. An oracle $\Pi^s_{i,j}$ 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 $\Pi^t_{j,i}$. The oracle $\Pi^s_{i,j}$ executes the prescribed protocol Π and produces the output as $\Pi(1^k, i, j, S_i, P_i, P_j, conv^s_{i,j}, r^s_{i,j}, x) = (m, \delta^s_{i,j}, \sigma^s_{i,j})$ 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; $\delta^s_{i,j}$ is the decision of the oracle (accept or reject the session or no decision yet) and $\sigma^s_{i,j}$ is the generated session key (please see [2, 4] for the details). At the end of Π, the conversation transcript $conv^s_{i,j}$ is updated as $conv^s_{i,j}.x.m$ (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: $Send(\Pi^s_{i,j}, x)$. $\Pi^s_{i,j}$ executes $\Pi(1^k, i, j, S_i, P_i, P_j, conv^s_{i,j}, r^s_{i,j}, x)$ and responds with m and $\delta^s_{i,j}$. If the oracle $\Pi^s_{i,j}$ 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's agreed session key: $Reveal(\Pi^s_{i,j})$. $\Pi^s_{i,j}$ reveals the session's private output $\sigma^s_{i,j}$ if the oracle accepts.
3. Corrupt a party: $Corrupt(i)$. The party i responds with the private key S_i. Here, the adversary is not allowed to replace a party's private key because the attack is impossible in the identity-based schemes.

Once the adversary decides that the first phase is over, it starts the second phase by choosing a *fresh oracle* $\Pi^s_{i,j}$ and issuing another query: $Test(\Pi^s_{i,j})$. Oracle $\Pi^s_{i,j}$, as a challenger, randomly chooses $b \in \{0, 1\}$ and responds with $\sigma^s_{i,j}$, if $b = 0$; otherwise it returns a random sample generated according to the distribution of the session secret $\sigma^s_{i,j}$. 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 [11].

Definition 2 (fresh oracle) *An oracle $\Pi^s_{i,j}$ is fresh if (1) $\Pi^s_{i,j}$ has accepted; (2) $\Pi^s_{i,j}$ 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 $\Pi^t_{j,i}$, which has had a matching conversation to $\Pi^s_{i,j}$.*

We stress that in this paper, 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 [1], which is the concatenation of the messages in a session (the transcript of an oracle), to define matching conversations. Two oracles $\Pi^s_{i,j}$ and $\Pi^t_{j,i}$ have the matching conversations if both of them derive the same session ID from (each own) conversation transcript.

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

Definition 3 [4] *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 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 setting (the SK key setting) 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** $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, sP, H_1, H_2 \rangle$ 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 setting [20]. 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 used as the public key corresponding to ID_A.

Note that the result of the SK key setting is a short signature d_A on the identity string ID_A signed under the private signing key s. As proved in Theorem 3 of [31], this short signature is secure against adaptive chosen message attacks in the secure signature notation by Bellare and Rogaway [3] provided that the k-sCAA1 assumption is sound.

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 [15, 16, 30] by employing an extra hash function on the agreed secret to generate the session keys).

Scheme 1 (McCullagh-Barreto's original scheme [15]). 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 two interesting security properties: the perfect forward secrecy (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) and the master-key forward secrecy (i.e., even if the master-key is compromised, the session keys of previous sessions are still safe). However, this scheme does not achieve the key-compromise impersonation resilience [10, 29]. To defeat this attack, Xie and McCullagh-Barreto proposed the following two fixing variants respectively.

Scheme 2 (McCullagh-Barreto's modified scheme [16]). 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 *appears* to achieve the key-compromise impersonation resilience property, this scheme looses two other desirable security attributions obtained in Scheme 1: the perfect forward secrecy and the master-key forward secrecy.

Scheme 3 (Xie's scheme [30]). 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 $SK = H_2(\hat{e}(P, P)^{xy+x+y})$. This scheme *appears* to be the strongest among three schemes and achieves the key-compromise impersonate resilience property, the perfect forward secrecy and the master-key forward secrecy as well.

Note that in the original schemes described in [15, 16, 30], the use of H_2 is not clearly 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 [15, 16, 30] 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 [2] and extended by Blake-Wilson et al. [4].

All of the three proofs are based on the bilinear inverse Diffie-Hellman (BIDH) problem, described in Assumption 2, i.e., given $\langle P, \alpha P, \beta P \rangle$, to compute $\hat{e}(P, P)^{\beta/\alpha}$ 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 modeled 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 [15]). 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 $\Pi^s_{i,j}$, $\mathcal{B}$ follows the protocol properly. To answer a Send query for $\Pi^s_{i,j}$, $\mathcal{B}$ 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 $\Pi^t_{j,i}$'s response is exactly the value of βP. After a Test query for $\Pi^s_{i,j}$, 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 [16]). $\mathcal{B}$ answers Create/Corrupt queries in the same way as it did in Proof 1. To answer a Send query for any oracle except $\Pi^s_{i,j}$, $\mathcal{B}$ follows the protocol properly. To answer a Send query for $\Pi^s_{i,j}$, $\mathcal{B}$ answers βP. The input from $\mathcal{A}$ as $\Pi^t_{j,i}$'s response is an arbitrary value δP. After a Test query for $\Pi^s_{i,j}$, 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 [30]). 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 $\Pi^s_{i,j}$, $\mathcal{B}$ follows the protocol properly. To answer a Send query for $\Pi^s_{i,j}$, $\mathcal{B}$ 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 $\Pi^t_{j,i}$'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 $\Pi^s_{i,j}$, 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.

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., [5, 6, 28]), 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 [7, 9], 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 [15, 16, 30] 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 the H_1 query, $\mathcal{A}$ 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.

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 [15, 16, 30]. 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 A New Proof

Although the reduction for the MB's modified protocol (Scheme 2) in [16] is invalid, this does not mean the protocol is insecure. Instead, we can present a new reduction based on the k-EBCAA1 assumption which reflects the security strength of this protocol. Now we present a new proof for Scheme 2 based on the k-EBCAA1 assumption but with the *Reveal* query disallowed. Obviously the reduction can be based on any assumption stronger than k-EBCAA1, including k-BDHI. A discussion on effect from disallowing the reveal query will be given in the next section.

Theorem 2 *McCullagh-Barreto's protocol using Scheme 2 as the session key generation function is a secure AK with respect to the Bellare-Rogaway's model with the* Reveal *query disallowed, provided that H_1, H_2 are random oracles and the k-EBCAA1 assumption is sound.*

Proof: The conditions 1 and 2 directly follow from the protocol specification. In the sequel we prove that the protocol satisfies the condition 3 if the *Reveal* query is disallowed.

Suppose that there is an adversary $\mathcal{A}$ against the protocol with non-negligible probability. Let q_1 and q_2 be the number of the distinct queries to H_1 and H_2 respectively (note that H_1 could be queried directly by an H_1-query or indirectly by a *Corrupt* query or a *Send* query). With the help of $\mathcal{A}$, we can construct an algorithm $\mathcal{B}$ to solve a q_1-EBCAA1 problem with non-negligible probability.

Given an instance of the q_1-EBCAA1 problem $(\mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, \langle P, sP, h_0, (h_1, \frac{1}{h_1+s}P), \ldots, (h_{q_1-1}, \frac{1}{h_{q_1-1}+s}P), yP\rangle$ where $h_i \in_R \mathbb{Z}_q^*$ for $0 \leq i \leq q_1 - 1)$, $\mathcal{B}$ simulates the **Setup** algorithm to generate the system **params** $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, q, P, sP, H_1, H_2\rangle$ (i.e., using s as the **master key** which it does not know). H_1 and H_2 are two random oracles controlled by $\mathcal{B}$. Suppose, in the game, there are T_1 oracles created by the engaged parties and $\mathcal{A}$. Here, 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 $u \in_R \{1, \ldots, T_1\}$ 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 $\langle ID_j, h_j, d_j\rangle$ 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 ID_i, $\mathcal{B}$ responds as follows:

1. If ID_i already appears on the H_1^{list} in a tuple $\langle ID_i, h_i, d_i\rangle$, then $\mathcal{B}$ responds with $H_1(ID_i) = h_i$.
2. Otherwise, if the query is on the I-th distinct ID, then $\mathcal{B}$ stores $\langle ID_I, h_0, \perp\rangle$ into the tuple list and responds with $H_1(ID_I) = h_0$.
3. Otherwise, $\mathcal{B}$ selects a random integer $h_i(i > 0)$ from the q_1-EBCAA1 instance which has not been chosen by $\mathcal{B}$ and stores $\langle ID_i, h_i, \frac{1}{h_i+s}P\rangle$ into the tuple list. $\mathcal{B}$ responds with $H_1(ID_i) = h_i$.

H_2-queries (X_i)**:** At any time $\mathcal{A}$ can issue queries to the random oracle H_2. To respond to these queries $\mathcal{B}$ maintains a list of tuples called H_2^{list}. Each entry in the list is a tuple of the form $\langle X_i, H_i\rangle$ indexed by X_i. To respond to a query on X_i, $\mathcal{B}$ does the following operations:

1. If on the list there is a tuple indexed by X_i, then $\mathcal{B}$ responds with H_i.
2. Otherwise, $\mathcal{B}$ randomly chooses a string $H_i \in \{0, 1\}^n$ and inserts a new tuple $\langle X_i, H_i\rangle$ to the list. It responds to $\mathcal{A}$ with H_i.

Corrupt(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$(\Pi_{j,i}^t, M)$**:** $\mathcal{B}$ first 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 $t \neq u$, $\mathcal{B}$ responds the query by honestly following the protocol. If $t = u$, $\mathcal{B}$ further checks the value of d_i, and then responds the query differently as below dependending 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, $\mathcal{B}$ responds with yP obtained from the q_1-EBCAA1 instance. Note that $\Pi_{j,i}^t$ can be the initiator (if $M = \lambda$) or the responder (if $M \neq \lambda$).

Test($\Pi^t_{j,i}$)**:** If $t \neq u$, $\mathcal{B}$ aborts the game (**Event 3**). Otherwise, $\mathcal{B}$ randomly chooses a number $\zeta \in \{0,1\}^n$ and gives it to $\mathcal{A}$ as the response. When $\mathcal{A}$ responds, $\mathcal{B}$ randomly chooses a tuple from H_2^{list} with value X_ℓ. $\mathcal{B}$ responds to the q_1-EBCAA1 challenger with the value of $X_\ell / \hat{e}(d_j, M)$ where M is the incoming message to oracle $\Pi^t_{j,i}$.

Note that if the game did not abort, the adversary cannot find the inconsistency between the simulation and the real world. The agreed secret in oracle $\Pi^t_{j,i}$ should be $K = \hat{e}(d_j, M) \cdot \hat{e}(P,P)^r$ 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 $K = \hat{e}(d_j, M) \cdot \hat{e}(yP, \frac{1}{h_0+s}P)$.

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 M 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 $\mathcal{H}_3$: $\mathcal{A}$ 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 $\Pi^t_{j,i}$ as the *fresh oracle*. Hence $\neg\mathcal{H}_3 \wedge \neg\mathcal{H}_2$ implies $\neg\mathcal{H}_1$ (recall that in this report, we require that $j \neq i$ for the chosen fresh oracle $\Pi^t_{j,i}$, i.e., in the attacked session the victim party establish the session with itself. This is not an unusual requirement in real environments). Let $\mathcal{F}$ be the event that $\mathcal{B}$ did not abort the game. Then, we have

$$Pr[\mathcal{F}] = Pr[\neg\mathcal{H}_1 \wedge \neg\mathcal{H}_2 \wedge \neg\mathcal{H}_3] = Pr[\neg\mathcal{H}_2 \wedge \neg\mathcal{H}_3] \geq \frac{1}{q_1} \cdot \frac{1}{T_1}.$$

Let $\mathcal{H}$ be the event that $\hat{e}(d_j, M) \cdot \hat{e}(yP, \frac{1}{h_0+s}P)$ has been queried to H_2. Since H_2 is a random oracle and all the oracles are *unopened*, $\Pr[\mathcal{A} \text{ wins} | \neg\mathcal{H}] = \frac{1}{2} + \epsilon(k)$ for some negligible function $\epsilon(k)$. Suppose $\mathcal{A}$ wins the game with non-negligible advantage $n(k)$. Then we have

$$n(k) + \tfrac{1}{2} = Pr[\mathcal{A} \text{ wins}] \leq Pr[\mathcal{A} \text{ wins}|\mathcal{H}]Pr[\mathcal{H}] + \tfrac{1}{2} + \epsilon(k) \leq Pr[\mathcal{H}] + \tfrac{1}{2} + \epsilon(k).$$

So, $Pr[\mathcal{H}] \geq n(k) - \epsilon(k) > n'(k)$ which is non-negligible. Let $\mathcal{E}$ be the event that $\mathcal{B}$ finds the correct $\hat{e}(d_j, M) \cdot \hat{e}(yP, \frac{1}{h_0+s}P)$ on the list H_2^{list}, and so computes the correct $\hat{e}(yP, \frac{1}{h_0+s}P)$. Overall, we have

$$Pr[\mathcal{B} \text{ wins}] = Pr[\mathcal{F} \wedge \mathcal{H} \wedge \mathcal{E}] \geq \frac{1}{q_1 \cdot T_1} \cdot n'(k) \cdot \frac{1}{q_2}.$$

□

6 Discussions about the Reduction

The reduction presented in the previous section does not allow the adversary to query the session keys generated in other sessions (different from the challenge session). Obviously, such reduction cannot guarantee that the scheme is secure against the known-session key attacks in general (see [11] for some examples). However, in the scheme H_2, which is treated as a random oracle in the game, is employed to generate the real session key (for later communication) from the agreed secret K. H_2 should be replaced by some cryptographic hash function which should at least achieve the preimage resistance property (Chapter 9 [17]). Hence, even given a session key $H_2(K)$ (which could possibly be recovered by some means from the later communication using the key), the adversary still cannot recover K. That means, the adversary cannot make use of its knowledge of $H_2(K)$ to launch any attack requiring the knowledge of K. Moreover, in the protocol, one party cannot totally control the generation of K in a session, and so, K and $H_2(K)$ will vary on each session because at least one party will behave honestly following the protocol.

So, intuitively, the *Reveal* query (in one session) does not help the adversary guess the session key of another session to win the game. Meanwhile, as suggested in [11] and employed in [27], to include the exchanged messages in a session or the identity of the engaged parties, known-session key attacks can be defeated.

Claim 1 *If the session key in Scheme 2 is generated in the following way:*

$$SK = H_2(A, B, T_1, T_2, \hat{e}(P, P)^{x+y}),$$

and H_2 is modelled as a random oracle, the Reveal query does not help the adversary win the game.

Proof (sketch): Suppose in the game, the chosen fresh oracle for the Test query is $\Pi^t_{j,i}$. Then to win the game through the Reveal query, the adversary has to at least reveal the session key of an oracle $\Pi^u_{i,j}$ or $\Pi^v_{j,i}$ because two parties' identifiers are used in H_2, and H_2 supposes to be a random oracle. If $\Pi^u_{i,j}$ is revealed, then it must not have the identical transcript with $\Pi^t_{j,i}$ because the rule of the game requires that $\Pi^u_{i,j}$ is not an oracle with a matching conversation with $\Pi^t_{j,i}$ (recall that a matching conversation is determined by the session ID which is the transcript of the oracle). Hence, an allowed reveal query on $\Pi^u_{i,j}$ does not help the adversary either, because the transcript is used in H_2. As $\Pi^v_{j,i}$ would have the same transcript with $\Pi^t_{j,i}$ (it requires at least that both oracles randomly choose the same integer r_j to generate the outgoing message $r_j(H_1(i)P + sP)$) with only negligible probability, the reveal query on this oracle does not provide any advantage to the adversary.

We have only provided a reduction for McCullagh-Barreto's modified protocol (Scheme 2). It seems that the reduction cannot be adapted for Xie's modification (Scheme 3). A formal reduction is still required for Xie's protocol, even though Xie's protocol seems stronger than McCullagh-Barreto's, which appears to achieve the perfect forward secrecy and the master-key forward secrecy.

7 Conclusion

In this paper, we have revisited the security proofs of three identity-based authenticated key agreement schemes using the SK key setting and pointed out the flaws in the reductions. We have also provided a new reduction for one of the three schemes. Our reduction is based on the k-EBCAA1 assumption in a weaker model of Bellare-Rogaway's key agreement formulation. We leave the formal security analysis of the other two schemes as an open problem.

References

1. M. Bellare, D. Pointcheval and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Proceedings of Advances in Cryptology - Eurocrypt 2000*, LNCS 1807, Springer-Verlag, 2000.
2. M. Bellare and P. Rogaway. Entity authentication and key distribution. In *Proceedings of Advances in Cryptology - Crypto '93*, LNCS 773, pp. 232-249, Springer-Verlag, 1993.
3. M. Bellare and P. Rogaway. The exact security of digital signatures - how to sign with RSA and Rabin. In *Proceedings of Advances in Cryptology - Eurocrypt '96*, LNCS vol. 1070, pp. 399–416, Springer-Verlag, 1996.
4. S. Blake-Wilson, D. Johnson and A. Menezes. Key agreement protocols and their security analysis. In *Proceedings of the Sixth IMA International Conference on Cryptography and Coding*, Springer-Verlag, 1997.
5. D. Boneh and X. Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In *Proceedings of Advances in Cryptology - Eurocrypt 2004*, LNCS 3027, pp. 223–238, Springer-Verlag, 2004.
6. D. Boneh and X. Boyen. Secure identity-based encryption without random oracles. In *Proceedings of Advances in Cryptology - Crypto 2004*, Springer-Verlag, 2004.
7. D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In *Proceedings of Advances in Cryptology - Crypto 2001*, LNCS 2139, pp.213–229, Springer-Verlag, 2001.
8. L. Chen and Z. Cheng. Security proof of the Sakai-Kasahara's identity-based encryption scheme. Manuscript.
9. L. Chen and C. Kudla. Identity based authenticated key agreement from pairings. In *Proceedings of the 16th IEEE Computer Security Foundations Workshop*, pages 219-233, June 2003. See also Cryptology ePrint Archive, Report 2002/184.
10. Z. Cheng. Private communication. 2004.
11. Z. Cheng, M. Nistazakis, R. Comley and L. Vasiu. On the indistinguishability-based security model of key agreement protocols-simple cases. In *Proceedings of ACNS 2004*. Full version available on Cryptology ePrint Archive, Report 2005/129.
12. K.-K. R. Choo. Revisit of McCullagh–Barreto two-party ID-based authenticated key agreement protocols. Cryptology ePrint Archive, Report 2004/343.
13. M. Girault and J.C. Paills. An identity-based scheme providing zero-knowledge authentication and authenticated key exchange. In *Proceeedings of ESORICS '90*, pages 173-184, 1990.
14. ISO/IEC 11770-3:1999. Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques.

15. N. McCullagh and P. S. L. M. Barreto. A new two-party identity-based authenticated key agreement. In *Proceedings of CT-RSA 2005*, LNCS 3376, pp. 262-274, Springer-Verlag, 2005.
16. N. McCullagh and P. S. L. M. Barreto. A new two-party identity-based authenticated key agreement. Cryptology ePrint Archive, Report 2004/122.
17. A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 2001.
18. S. Mitsunari, R. Sakai and M. Kasahara. A new traitor tracing. *IEICE Trans. Fundamentals*, E85-A(2):481–484, 2002.
19. E. Okamoto. Proposal for identity-based key distribution system. *Electronics Letters*, 22:1283-1284, 1986.
20. R. Sakai and M. Kasahara. ID based Cryptosystems with Pairing on Elliptic Curve. Cryptology ePrint Archive, Report 2003/054.
21. R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing. *The 2000 Symposium on Cryptography and Information Security*, Okinawa, Japan, January 2000.
22. M. Scott. Authenticated ID-based key exchange and remote log-in with insecure token and PIN number. Cryptology ePrint Archive, Report 2002/164, 2002. http://eprint.iacr.org/2002/164.
23. A. Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of Advances in Cryptology - Crypto '84*, LNCS 196, pp.47–53, Springer-Verlag, 1985.
24. N. P. Smart. An identity based authenticated key agreement protocol based on the Weil pairing. *Electronics Letters*, 38:630-632. See also Cryptology ePrint Archive, Report 2001/111.
25. N. Smart and F. Vercauteren. On computable isomorphisms in efficient pairing based systems. Cryptology ePrint Archive, Report 2005/116.
26. K. Tanaka and E. Okamoto. Key distribution system for mail systems using ID-related information directory. *Computers & Security*, 10:25-33, 1991.
27. Y. Wang. Efficient identity-based and authenticated key agreement protocol. Cryptology ePrint Archive, Report 2005/108.
28. B. R. Waters. Efficient identity-based encryption without random oracles. In *Proceedings of Advances in Cryptology - Eurocrypt 2005*, Springer-Verlag, 2005. See also Cryptology ePrint Archive, Report 2004/180.
29. G. Xie. Cryptanalysis of Noel McCullagh and Paulo S. L. M. Barreto's two-party identity-based key agreement. Cryptology ePrint Archive, Report 2004/308.
30. G. Xie. An ID-based key agreement scheme from pairing. Cryptology ePrint Archive, Report 2005/093.
31. F. Zhang, R. Safavi-Naini and W. Susilo. 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*, 2004.