International Journal of Computational Intelligence Research (IJCIR).
ISSN: 0973-1873 Volume 13, Number 8 (2017), pp. 1917–1930
© Research India Publications
http://www.ripublication.com/ijcir.htm

Provable Secure Identity Based Key Agrement Protocol With Perfect Forward Secrecy

Shaheena Khatoon
School of Studies in Mathematics,
Pt. Ravishankar Shukla University,
Raipur - 492010 (C.G.), India.

Tejeshwari Thakur
School of Studies in Mathematics,
Pt. Ravishankar Shukla University,
Raipur - 492010 (C.G.), India.

Abstract

In this paper we propose an efficient identity based authenticated key agreement (AKA) protocol based on bilinear pairing. The proposed protocol is evaluated as well as analyzed in term of efficiency, security and compared with the existing protocol. Further, the security is proved by modular proof technique given by Kudla and Paterson in the random oracle model under the Gap Bilinear Diffie Hellman (GBDH) assumption.

AMS subject classification: Primary: 94A60; Secondary: 94A62.
Keywords: identity based, key agrement, bilinear pairing, modular security technique,perfect forward secrey.

1. Introduction

Key agreement is one of the fundamental cryptographic primitives for establishing a secure communication in hostile environment. It is a process in which two or more parties establishes a common session key in such a way that not a single party can predetermine the resulting value. Authenticated key agreement (AKA) protocol allows sharing of the session key as well as provides authenticity of the users [6]. An AKA protocol can be obtained by combining key agrement protocols with digital signatures.Diffie - Hellman in 1976 [19] was first to propose the concept of key agrement protocol. But it suffers from man-in-middle attack and it does not provide authenticity. After this seminal paper, many key agrements were proposed but they all requires the traditional public key infrastructure (PKI) which is expensive to use and have a complex key management mechanism.

The pioneer work of Adi Shamir in 1984 [1] gave the notion of identity (ID) based cryptography. In ID based cryptography users public key is generated by users identities like user's email address and the private key is generated by trusted private key generator (PKG). This greatly simplifies the key management mechanism. The formally proved identity - based cryptosystem based on Weil pairing was given by Boneh and Franklin [10] and in the year 2000 [20] gave the construction of key agreement protocol from pairing but it also suffers from the man-in-middle attack. Nevertheless it became a breakthrough since then many ID based AKA protocols employing pairing has been proposed some of them are in [12, 23, 25, 26, 28].

In this paper, we propose an efficient and secure ID-based AKA protocol using bilinear pairing. Formal security is given by using the modular proof technique of Kudla and Paterson in random oracle model under Gap Bilinear Diffie Hellman (GBDH) assumption. Furthermore, we prove that the proposed protocol achieves perfect forward secrecy (PFS) under Bilinear Diffie-Hellman (BDH) assumption. And we also compare our scheme with other existing scheme in term of efficiency. The structure of the paper is as follows: In section 2 preliminaries are given in section 3 modular proof approach for ID based AKA protocol is discussed. Proposed protocol is given in section 4 followed by its security proof in section 5, section 6 performance comparison. TheConclusion is given in section 7 followed by acknowledgement and bibliography.

2. Preliminaries

This section briefly gives the fundamental background needed in this paper:

Definition 2.1. [Bilinear Pairing] Suppose G_1 and G_2 be two group of same prime order q, where G_1 be an additive groups and G_2 be a multiplicative group and P be generators of G_1.Then the map $e : G_1 \times G_1 \to G_2$ is a bilinear map, with the following properties:

1. Bilinear: $e(aR, bS) = e(R, S)^{ab}$, for any $a, b \in Z_q^*$ and for all $R, S \in G_1$.
2. Non-degenerate: $e(P, P_1) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(R, S)$ for all $R, S \in G_1$.

Weil or Tate pairing on an elliptic curve over finite field are the admissible pairing. References [8, 9] gives the detail description of these pairing.

Now we define the following computational problem which are used in the security proof of the ID bases AKA protocols. Let G_1, G_2, P, e be as above, then computational problem are defined in the following way:

Definition 2.2. [Computational Diffe–Hellman (CDH) Problem] Given a tuple $(P, aP, bP) \in G_1$, for some random values $a, b \in Z_q^*$ the Computational Diffe-Hellman (CDH) Problem, consists of computing the element abP.

Definition 2.3. [Divisible Computational Diffe-Hellman (DCDH) Problem] Given a tuple $(P, aP, bP) \in G_1$, for some random values $a, b \in Z_q^*$ the Divisible Computational Diffe-Hellman (DCDH) Problem, consists of computing the element $ab^{-1}P$.

Definition 2.4. [Bilinear Diffe-Hellman (BDH) Problem] Given $(P, aP, bP, cP) \in G_1$ for some random values $a, b, c \in Z_q^*$, the Bilinear Diffie-Hellman (BDH) Problem, consists of computing $e(P, P)^{abc} \in G_2$.

Definition 2.5. [Decisional Bilinear Diffe-Hellman (DBDH) Problem] Given $(P, aP, bP, cP) \in G_1$ for some random values $a, b, c \in Z_q^*$, and $W \in G_2$ the Decisional Bilinear Diffe-Hellman (DBDH) Problem, is to determine if $e(P, P)^{abc} = W$.

Definition 2.6. [Gap Bilinear Diffe-Hellman (GBDH) Problem] Given $(P, aP, bP, cP) \in G_1$ with uniformly random choices of $a, b, c \in Z_q^*$, as well as an oracle the solves the DBDH problem in G_1, G_2,the GBDH problem, is to compute $e(P, P)^{abc}$.

Now we state a theorem given by Bao et al. [11] which establish relation between CDH problem and DCDH problem.

Theorem 2.7. DCDH problem is equivalent to CDH problem, i.e., by solving two instances of DCDH problem, one can solve an instance of CDH problem.

3. Modular Proof approach for ID based AKA Protocols

In this section, we will present our refined modular proof technique called cNR-ID-mBR (Computational No Reveal-ID based modified Bellare-Rogaway model game). This model is a modified version of Kudla and Paterson model [21, 22], we will make following two modification in the Kudla and Paterson model. Firstly, we will use the notion of SID(session identifier) as in [13] instead of matching conversation. And secondly, we will extend the model in ID based setting. Noting that SID of any oracle is defined as the concatenation of all the message sent and received by oracle. Bellare and Rogaway [2, 3] were first to give the formal security notion for key agrement protocols. Later on, a number of modification and extension have been made the noteworthy being [4] and [7] by Wilson et al. and Bellare et al. respectively. "Modular" approach was advocated by Bellare, Canetti and Krawczyk [5]. Kudla and Paterson gave the modular technique for those protocol which are not designed in modular form. Firstly we define the ID based modified Bellare-Rogaway(ID-mBR) model.

3.1. The ID-based modified Bellare-Rogaway model(ID-mBRM)

The model includes a set of participants U modeled by a collection of oracles. Each participant has a long-term ID-based public/private key pair and the unique ID.We use $\prod\limits_{I,J}^{n}$ denotes the oracle in the nth instance of participant I having communicating with another participant J. There exist an adversary E which has access to all the oracles. Further, each oracle maintains a transcript $T_{\Pi^n_{I,K}}$ which records all message they have sent or received in reply to queries made to them.

3.2. Some Definitions

Definition 3.1. [Open Oracle] If an oracle $\prod\limits_{I,J}^{n}$ reveals the accepted session key in any state, then oracle is considered opened in that state.

Definition 3.2. [Partner Oracles] Two oracles $\prod\limits_{I,J}^{n}$ and $\prod\limits_{I,J}^{n'}$ are called partner if they have the same SID.

Definition 3.3. [Fresh Oracle] An oracle $\prod\limits_{I,J}^{n}$ is unfresh if it is opened or its partner oracle $\prod\limits_{I,J}^{n'}$ is opened or corrupted, otherwise it is fresh oracle.

3.3. The ID-mBR Game

A two phase adaptive game (called ID-mBR game) between a challenger C and an adversary E defines the security of a key agreement protocol. C simulates the PKG and generates public parameter, also generates master secret s through which it generates the private key d_{ID} of a participant with identity ID.

- **Phase1** : In this phase adversary E issues following queries in any order.

  Send(I,J,n,M) E sends message M to oracle $\prod\limits_{I,J}^{n}$. Oracle runs the protocol and sends back message M to E or sends the decision to E specifying acceptance or rejection of the session.

  Reveal($\prod\limits_{I,J}^{n}$) In response to this query,oracle return the accepted session key (if any) or return the empty string ($\perp$). In this case oracle is considered to be opened.

Corrupt(I) In response to this query C sends the private key d_{ID} of any participant I. In this case, participant is considered as corrupted.

Test ($\prod_{I,J}^{n}$) E can make test query to some fresh oracle at any time. C response to test query in this way: C flips a fair coin $b \in 0, 1$ if answer is 1, C outputs a random chosen session key. Otherwise it outputs the agreed session key of the test oracle.

- **Phase2** : In this phase, E continues to issue the above queries to oracle except the test query at the same time E is not allowed to corrupt any other participant J.

Output Finally, E output b and wins the game if $b = b'$ and the advantage of A in wining game is defined as $Adv^{E}(L) =\mid Pr[b =' b] - 1/2 \mid$.

A benign adversary is one who simply communicate messages between participants without modifying it.

Definition 3.4. [ID-mBR secure protocol] An authenticated key agrement protocol is said to be ID-mBR secure if:

- If in the presence of any benign adversary, two oracles say $\prod_{I,J}^{n}$ and $\prod_{I,J}^{m}$ who runs the given protocol agreed upon holding the same session key, and this session key is distributed uniformly at randomly on $\{0, 1\}^{k}$.
- And the advantage of any adversary E is negligible in ID- mBR game i.e. $Adv^{E}(k)$ is negligible.

3.4. Kudla and Paterson's modular approach

As stated by Chen et al. [15], Kudla and Paterson's modular approach [21, 22] is one of the most efficient way to proof the security of any AKA protocol. Further, from references [21, 22] it is noted that modular proof approach works only on key agrement protocol which generates hashed session key at the end of the protocol.The proposed protocol also derives session key using a key derivative function (kdf), and kdf is implemented via a hash function. Basically, modular proof approach consist of following three steps:

1. Protocol Π is proved to have strong partnering.
2. The related protocol π is showed to be secure in a highly reduced security model.
3. With the help of Gap assumption [24] the security of π is translated into the security proof of Π in the full model.

Now we define the following term used above:

Definition 3.5. [Session string] Let Π produces a hashed session key through a hash function H, then the session string $(ss_{\prod^{i}_{I,J}})$ of an oracle $\prod\limits_{I,J}^{i}$ is the string which is hashed to produce session key $SK\prod\limits_{I,J}^{i}$ i.e. $SK\prod\limits_{I,J}^{i} = H(ss_{\prod^{i}_{I,J}})$.

Definition 3.6. [Strong Partnering] When an adversary E attacks, a protocol Π in a mBR game with non negligible probability in the security parameter k, in such a way that it makes two different oracles (which are not partner to accept the same session key. Then we say that Pi has weak partnering, otherwise it has strong partnering.

Definition 3.7. [Reduced Game/(cNR-mBR Game)] A reduced game is equivalent to mBR game except that adversary E is not allowed to make reveal query and to win the game.Rather E is allowed to accept a fresh oracle on which E makes a modified test query at the end of its attack and output the session key held by this oracle. And the advantage of E in the mBR model is the probability that E output a session key sk such that $sk = sk\prod\limits_{I,J}^{i}$ $(\prod\limits_{I,J}^{i}$ is the oracle on which E puts the modified test query).

Definition 3.8. [cNR-ID-mBR secure protocol] An authenticated key agrement protocol is said to be cNR-ID-mBR secure if:

- If in the presence of any benign adversary, two oracles say $\prod\limits_{I,J}^{n}$ and $\prod\limits_{I,J}^{m}$ who runs the given protocol agreed upon holding the same session key, and this session key is distributed uniformly at randomly on $\{0, 1\}^{k}$.
- And the advantage of any adversary E is negligible in cNR-ID-mBR game i.e. $Adv^{A}(k)$ is negligible.

As noted in [16] the above definition 2.2 capture all the security attributes desired for a protocol including Known-key secrecy (K-KS), Perfect forward secrecy (PFS),Key-compromise impersonation (K-CI) resilience,Unknown key-share (UK-S) resilience and No key control. As the adversary in the above game is modeled in such a way that it includes all the attacks in the real world.

4. Proposed ID based AKA Protocol

In this section we describe our proposed identity based authenticated key agrement (ID-AKA) protocol. Let their be a trusted PKG (Private key generator) which generates and distributes the private key of the user. The proposed protocol consist of following steps:

1. Setup: Let $e : G_1 \times G_1 \rightarrow G_2$ be an admissible pairing where G_1 and G_2 are two group of same order $q(q$ is prime). The PKG does the following:

   - Randomly chooses a generator P of G_1, a secret master key $s \in_R Z_q^*$ and evaluates the master public key $P_{pub} = sP$.
   - Chooses a collision resistant hash function $H_1 : \{0, 1\}^* \times G_1 \rightarrow Z_q^*$.
   - Publishes the public parameters $(G_1, G_2, e, q, P\ and\ sP, H_1)$.

2. Private Key Extraction: For a given user with identity ID_i, PKG randomly selects $r_i \in_R Z_q$ and compute:

   (a) $R_i = r_i P$

   (b) $h = H_1(ID_i||R_i)$

   (c) $S_i = \dfrac{1}{(r_i + hs)}$

3. Key Agreement: Let their be two users A and B with the private key as (S_A, R_A) and (S_B, R_B) respectively. To establish a shared session key A and B proceed in the following way:

   (a) Both A and B generates an ephemeral private key a and b $\in Z_q^*$.

   (b) A sends (ID_A, R_A) to B, B send back (ID_B, R_B, T_{BA}) to A where $T_{BA} = b[R_A + H_1(ID_A||R_A)P_{pub}]$, then A computes $T_{AB} = a[R_B + H_1(ID_B||R_B)P_{pub}]$ and communicates it to B

   (c) A computes:
   $$K_{AB}^1 = aP + S_A T_{BA}$$
   and
   $$K_{AB}^2 = e(S_A T_{BA}, P_{pub})^a$$
   Similarly B computes
   $$K_{BA}^1 = bP + S_B T_{AB}$$
   and
   $$K_{BA}^2 = e(S_B T_{AB}, P_{pub})^b$$

Correctness: By the property of Bilinear Pairing we can easily verify:

$$\begin{aligned} K_{AB}^1 &= aP + S_A T_{BA} \\ &= aP + (r_a + hs)^{-1} b(r_a P + hsP) \\ &= aP + (r_a + hs)^{-1} b(r_a + hs)P \\ &= aP + bP \\ &= (a + b)P \end{aligned}$$

$$\begin{aligned}K_{BA}^1 &= bP + S_B T_{AB}\\ &= bP + (r_b + hs)^{-1} b(r_b P + hsP)\\ &= bP + (r_b + hs)^{-1} b(r_b + hs)P\\ &= bP + aP\\ &= (a+b)P\end{aligned}$$

$$\begin{aligned}K_{AB}^2 &= e(S_A T_{BA}, P_{pub})^a\\ &= e[(r_a + hs)^{-1} b(r_a P + hsP), sP)]^a\\ &= [(r_a + hs)^{-1} b(r_a + hs)P, sP)]^a\\ &= e(bP, sP)^a\\ &= e(P, P)^{sab}\end{aligned}$$

$$\begin{aligned}K_{BA}^2 &= e(S_B T_{AB}, P_{Pub})^b\\ &= e[(r_b + hs)^{-1} a(r_b P + hsP), P_{pub})]^b\\ &= e[(r_b + hs)^{-1} a(r_b + hs)P, P_{pub})]^b\\ &= e(aP, sP)^b\\ &= e(P, P)^{sab}\end{aligned}$$

Hence, we have $K_{AB}^1 = K_{BA}^1 = K^1$ and $K_{AB}^2 = K_{BA}^2 = K^2$. Thus, A and B calculate the shared session key as:

$$sk = H(ID_A || ID_B || Trans || K^1 || K^2)$$

here, $Trans = (T_{AB} || T_{BA})$ and H is a key derivation function (kdf) such that $H : \{0, 1\}^* \times \{0, 1\}^* \times (G_1)^2 \times (G_2)^4 \rightarrow \{0, 1\}^k$ (in which $k = |sk|$).

Table 1: The Proposed Protocol

User A		User B
$a \in_R Z_q^*$		$b \in_R Z_q^*$
	$\longrightarrow (ID_A, R_A)$	
		$T_{BA} = b[R_A + H_1(ID_A \| \| R_A)P_{pub}]$
	$\longleftarrow (ID_B, R_B, T_{BA})$	
$T_{AB} = b[R_B + H_1(ID_B \| \| R_B)P_{pub}]$		
$K_{AB}^1 = aP + S_A T_{BA}$		$K_{BA}^1 = bP + S_B T_{AB}$
$K_{AB}^2 = e(S_A T_{BA}, P_{pub})^a$		$K_{BA}^2 = e(S_B T_{AB}, P_{pub})^b$
$sk = H(ID_A \| \| ID_B \| \| Trans \| \| K_{AB}^1 \| \| K_{AB}^2)$		$sk = H(ID_A \| \| ID_B \| \| Trans \| \| K_{BA}^1 \| \| K_{BA}^2)$

5. Security Proof

In order to adopt the modular proof technique given by Kudla and Paterson, in [21, 22], firstly we convert the given protocol Π in to a related protocol π, so we assume $\pi = (ID_A||ID_B||Trans||K^1||K^2)$. Thus $\Pi = H(ID_A||ID_B||Trans||K^1||K^2)$.

From the references [21, 22] we state the following theorem which converts the security of related protocol into the security of full protocol.

Theorem 5.1. Suppose that key agreement protocol Π produces a hashed session key on completion of the protocol (via hash function H) and that Π has strong partnering. If the cNR-mBR security of the related protocol π is probabilistic polynomial time reducible to the hardness of the computational problem of some relation f, and the session string decisional problem for Π is polynomial time reducible to the decisional problem of f, then the mBR security of Π is probabilistic polynomial time reducible to the hardness of the Gap problem of f, assuming that H is a random oracle.

Now we prove that that the related protocol π is cNR-ID-mBR secure:

Theorem 5.2. If for related protocol π, there is an an adversary E who can win a cNR-ID–mBR game with non-negligible probability n(k) in polynomial time t(k), then the CDH problem can be solved with non-negligible probability within time t(k), where k is the security parameter for protocol π.

Proof. Assume challenger A is provided with two groups G_1 and G_2, the bilinear mapping e, a generator P of G_1 and the tuple $(P, aP, bP) \in G_1$ for some random $a, b \in Z_p$ and A task is to compute $c = abmodP$. For this A simulates a challenger C in the game with an adversary E:

Setup: A first chooses $x \in Z_q^*$ at random sets the PKG's master key as x, A will simulates all oracle required during the game and replies queries in the following way:

$H_1(ID_i, R_i)$: A stipulates the hash function H_1 and maintain an empty list H_1 list. Here, $n_p(k)$ denotes the total number of participant in the game and $n_s(k)$ denotes the total number of sessions each participant may be involved. Let the private key of the i-th participant with the identity ID_i be (S_i, R_i), so in order to generate (S_i, R_i) A proceed in the following way: A first randomly selects $I \in \{1, \dots, n_p(k)\}$ after that selects $R_I \in_R G$ and sets $(\perp, R_I) = (S_i, R_i)$ and sets master public key as $P_{pub} = H_1(ID_I, R_I)^{-1}(bP - R_I)$ this implies $S_I^{-1}P = bP$. Now in order to set the private key of all $i \in \{1, \dots, n_p(k)\}\ and\ i \neq I$, A randomly selects $(S_i, h_i) \in_R Z_p^*$ then evaluates $R_i = S_i^{-1}P - h_i P_{pub}$ and sets (S_i, R_i) as the private key of the participant with Identity ID_i and accordingly adds $(ID_i, R_i, S_i, h_i), i \in \{1, \dots, n_p(k)\}$ in the H_1 list.

Now A randomly selects $J \neq I \in \{1, \dots, n_p(k)\}$ and $v \in \{1, \dots, n_s(k)\}$ and replies to E's query in the following ways:

- If (ID_i, R_i) already exist in H_1 list then A sends h_i to A.

- Otherwise randomly selects $h_i \in_R Z_p^*$ and adds (ID_i, R_i, S_i, h_i) to the H_1 list and sends h_i to E.

Corrupt(ID_i)**:** When A receives corrupt query on ID_i, A simulates as follows:

- If $ID_i \neq ID_I$ A looks for the tuple (ID_i, R_i, S_i, h_i) in the H_1 list and sends S_i, R_i to E.
- Otherwise,if $ID_i = ID_I$ A aborts the query.

Send$(\prod_{I,J}^{s}, M)$**:** If $\prod_{I,J}^{s} \neq \prod_{I,J}^{v}, M$ then A acts according to the protocol specification, otherwise responds with tuple ID_j, upk_j, R_j, aP. The probability that $\prod_{I,J}^{v}$ is chosen as test oracle by E and that $ID_i = ID_I$ and $ID_j = ID_k$ is $\frac{1}{n_s(k)n_p(k)}$. This means A could not have corrupted TD_I and C would not have aborted the Corrupt query.If A wins such game then at the end of this game A will output its guess of the session key of the form $\{0, 1\}^* \times (G_1)^2 \times (G_2)^4$ and C output $A - S_jM$ where M is the input message of the send query.This implies C can solve DCDH problem with non-negligible probability $\frac{\epsilon}{n_s(k)n_p^2(k)}$,hence from theorem 2.7 one can solve CDH with advantage at least $[\frac{\epsilon}{n_s(k)n_p^2(k)}]^2$. ■

Theorem 5.3. The protocol Π has strong partnering in the random oracle model.

Proof. It is easy to verify, as we can see that partnering information namely protocol transcript and identity of participant are already included in the session string and we model kdf via hash function and if two different oracle ends up holding same session key, then the probability of weak partnering is negligible. Hence Π has strong partnering. ■

Now we prove the security of the proposed protocol with the help of following theorem:

Theorem 5.4. The proposed protocol Π is secure in the random oracle model assuming the hardness of Gap Diffie-Hellman (GDH) problem.

Proof. The theorem 5.1 5.2 and 5.3 directly establishes the security of the of the proposed protocol in cNR-ID-mBR model under the assumption that GDH is hard. ■

Theorem 5.5. Our protocol has the perfect forward secrecy property if the BDH problem is hard.

Proof. Let the private key of A and B be S_A, R_A and S_B, R_B respectively. Suppose A and B establishes a session key K using the proposed protocol. Let a and b be the random number chosen by A and B during key establishment and let their private key S_A, R_A and S_B, R_B be compromised, then an adversary E can easily compute $S_A T_{AB} = aP$ and $S_B T_{BA} = bP$.So aP, bP,and sP forms the BDH tuple and to compute the value of $e(P, P)^{sab}$ without the knowledge of a,b,and s the adversary must have the ability to solve the BDH problem.Under BDH assumption this probability is negligible hence the proposed protocol has perfect forward secrecy. ■

6. Comparison With Other Protocols

In this section we compare the proposed protocol with other existing protocols namely [12, 14, 23, 25, 28]. We also use MIRACL [27] a standard cryptographic library to compare computational efficiency. The hardware platform as per reference [17] is a PIV 3 GHz processor with 512 M bytes memory and the Windows XP operating system. For the pairing-based protocols, the Tate pairing defined over the supersingular elliptic curve $E/F_p : y^2 = x^3 + x$, with embedding degree 2 is used to achieve 1,024-bit RSA level security, q is a 160-bit Solinas prime $q = 2^{159} + 2^{17} + 1$ and p a 512-bit prime satisfying $p + 1 = 12qr$. For the ECC-based protocols, to achieve the same security level, the ECC group on Koblitz elliptic curve $y_2 = x^3 + ax + b$ defined on F_2^{163} with $a = 1$ and b a 163-bit random prime. To evaluate the computation efficiency of different protocols, we use the simple method from [18]. Table 1 gives Cryptographic operation time (in milliseconds) as per reference [17] and table 2 shows the efficiency comparison of our protocol with other existing protocols.

Table 2: Cryptographic operation time (in milliseconds).

Pairing	Multiplication in G_1	Exponentiation in G_2
20.01	6.38	11.20

Table 3: Efficiency Comparision

protocols	PFS	Reduction	Computation	Computation (in ms)
Smart [25]	No	-	2P + 2M	52.78
Chen-kudla [12]	No	CBDH	1P + 2M	32.77
McCullagh-Barreto [23]	No	BIDH	1P + 2M + 1E	43.97
Wang et al. [28]	yes	DBDH	2P + 1M + 2E	68.82
Chen et al. [14]	yes	GBDH	1P + 2M + 1E	43.97
Our scheme	yes	GBDH	1P + 3M	39.15

In the table BIDH is Bilinear Inverse Deffie Hellman assumption and DBDH is Decisional Bilinear Deffie Hellman assumption. P stands for bilinear pairing, M is scalar multiplication in G_1 and E is exponentiation in G_2. Here we have considered only expensive operations.From table 2 we draw the following conclusion: Smart's,Chen-kudla's and McCullagh-Barreto's protocols do not provide perfect forward secrecy. Only Wang et al.'s, Chen et al's and proposed protocol provides perfect forward security. But the proposed protocol has lower computation cost. The computation time of Chen-kudla and McCullagh-Barreto are less then our scheme but they do not provide perfect forward secrecy. Hence we can claim that our proposed scheme is more secure and efficient.

7. Conclusion

Key agrement protocol plays vital role for secure communication over open network. In the paper we have presented an ID based authenticated key agrement (AKA) protocol and proved its security in more efficient and widely accepted modular proof technique given by [21, 22]. The scheme also captures all the security properties like Known-key secrecy (K-KS), Perfect forward secrecy (PFS), Key-compromise impersonation (K-CI) resilience, Unknown key-share (UK-S) resilience and No key control with a reduced computational overhead and improved efficiency.

Acknowledgement

The authors would like to thanks the anonymous reviewers for their valuable comments and review.

References

[1] A. Shamir, Identity-based cryptosystems and signature schemes, in: Advances in Cryptology - CRYPTO'84, Springer, New York, 1985, pp. 47–53.

[2] M. Bellare and P. Rogaway. Entity authentication and key distribution. In Advances in Cryptology - CRYPTO '93, volume 773 of LNCS, pages 232–249. Springer-Verlag, 1994.

[3] M. Bellare and P. Rogaway. Provably secure session key distribution: The three party case. In Proceedings of the 27th Annual ACM Symposium on Theory of Computing STOC, pages 57–66. ACM, 1995.

[4] Blake-Wilson S, Johnson C, Menezes A. Key agreement protocols and their security analysis. In: Proc of the sixth IMA International Conference on Cryptography and Coding, LNCS vol. 1355. New York: Springer-Verlag, 1997. 30–45

[5] M. Bellare, R. Canetti, and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In Proceedings of the 30th Annual Symposium on the Theory of Computing, pages 419–428. ACM, 1998.

[6] Blake-Wilson S, Menezes A. Authenticated Diffie-Hellman key agreement protocols. In: Proc of SAC 1998, LNCS vol. 1556. New York: Springer-Verlag, 1999. 339–361.

[7] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In B. Preneel, editor, Advances in Cryptology - EURO-

CRYPT 2000, volume 1807 of Lecture Notes in Computer Science, pages 139–155. Springer-Verlag, 2000.

[8] Barreto P S L M, Kim K Y, Lynn B. Efficient algorithms for pairing-based cryptosystems. In: Proc CRYPTO 2002, LNCS vol. 2442. New York: Springer-Verlag, 2002. 354–368

[9] Galbraith S D, Harrison K, Soldera D. Implementing the Tate pairing. In: Proc of ANTS-V, LNCS vol. 2369. New York: Springer-Verlag, 2002. 324–337

[10] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, SIAM J. Comput. 32 (3) (2003) 586–615.

[11] Bao F,DengR,ZhuH.VariationsofDiffie-HellmanProblem.In:5thinternational conference of information and communications security-ICICS 2003. Lecture notes in computer science, vol. 2836, 2003. p. 301–12.

[12] L. Chen, C. Kudla, Identity based authenticated key agreement protocols from pairings, in: Computer Security Foundations Workshop, IEEE, USA, 2003, pp. 219–233.

[13] [choo]Choo K-K R, Boyd C, Hitchcock Y, et al. On session identifiers in provably secure protocols: The Bellare-Rogaway threeparty key distribution protocol revisited. In: Proc of SCN 2004, LNCS vol. 3352. New York: Springer-Verlag, 2005. 351–366.

[14] Cheng Z, Chen L, Comley R, Tang Q. Identity-based key agreement with unilateral identity privacy using pairings. In: Proc of ISPEC 2006, LNCS vol. 3903. New York: Springer-Verlag, 2006. 202–213.

[15] L. Chen, Z. Cheng, N.P. Smart, Identity-based key agreement protocols from pairings, Int. J. Inf. Secur. (6) (2007) 213–241.

[16] Cao X, KouW, DuX. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Information Sciences 2010; 180(15):2895–903.

[17] Cao X, Kou W, Du X (2010) A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Inf Sci 180:2895–2903

[18] Ren K, Lou W, Zeng K, Moran PJ (2007) On broadcast authentication in wireless sensor networks. IEEE Trans. Wirel. Commun 6(11):4136–4144.

[19] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (6) (1976) 644–654.

[20] A. Joux, A one round protocol for tripartite Diffie-Hellman, in: 4th International Symposium on Algorithmic Number Theory, in: Lecture Notes in Comput. Sci., vol. 1838, Springer, New York, 2000, pp. 385–394.

[21] Kudla C, Paterson K G. Modular security proofs for key agreement protocols. In: Proc of ASIACRYPT'05, LNCS vol. 3788. New York: Springer-Verlag, 2005. 549–565.

[22] Kudla C. Special signature schemes and key agreement protocols. PhD Thesis, Royal Holloway University of London, 2006.

[23] N. McCullagh, P.S.L.M. Barreto, A new two-party identity-based authenticated key agreement, Cryptology ePrint Archive Report 2004/122, 2004.

[24] Okamoto T, Pointcheval D. The Gap-problems: a new class of problems for the security of cryptographic schemes. In: Proc of PKC 2001, LNCS vol. 1992. New York: Springer-Verlag, 2002. 104–118.

[25] N.P. Smart, Identity-based authenticated key agreement protocol based on Weil pairing, Electronics Lett. 38 (13) (2002) 630–632.

[26] K. Shim, Efficient ID-based authenticated key agreement protocol based on Weil pairing, Electronics Lett. 39 (8) (2003) 653–654.

[27] Shamus Software Ltd., Miracl library. <http://www.shamus.ie/index.php?page=home>.

Cryptology ePrint Archive Report2005/108, 2005.

[28] Wang S B, Cao Z F, Cheng Z H, et al., Perfect forward secure identity-based authenticated key agreement protocol in the escrow mode. Sci China Ser F-Inf Sci, 2009, 52: 1358–1370.