A New Efficient ID-Based Authenticated Key Agreement Protocol

Quan Yuan
yq2uan@pku.edu.cn

Songping Li
lsp@pku.edu.cn
School of Mathematical Sciences,
Peking University,Peoples Republic of China

Mar. 1, 2005

Abstract

Recently Eun-Kyung Ryu, Eun-Jun Yoon, and Kee-Young Yoo proposed an efficient ID-based authenticated key agreement with paring[11]. They argued that it is secure and efficient. In this paper, we show this protocol is doesn't satisfy the Key-Compromise Impersonate property and it is not secure against key reveal attack. Then we propose our protocol from this protocol and shim's protocol[15], its security and efficiency was analyzed.
Keywords: ID-Based, Key Agreement, Key Compromise Impersonation, Key Reveal Attack.

1 Introduction

The key agreement, which allows two parties to establish a shared secret by exchanging messages over an open channel, was first proposed by Diffie and Hellman[5]. However this protocol is not secure against man-in-the-middle attack. Then many authenticated key agreement with protocols were proposed. But all of them need a public key infrastructure(PKI), which is requires high computational and storage efforts.

To simplify the PKI system, Shamir introduced the new idea of ID-Based system[13]. In such cryptosystems the public key of a user is derived from his identity information and his private key is generated by a trusted third party called Key Generation Center (KGC). The advantage of ID-based cryptosystems is that it simplifies the key management process which is a heavy burden in PKI based cryptosystems. In these cryptosystems, Alice can send an encrypted message to Bob by using Bob's identity information (Bob ,for example) even before Bob obtains his private key from the KGC. This idea is also provide a way to construct authenticated key agreement protocol.

The first ID-Based authenticated key agreement based on Weil pairing was constructed by Smart who make use of Shamir's ID-based concept[13], the construction of the D. Boneh and M. Franklin[2] and the idea of A. Joux's tripartite protocol. However, Shim point out this protocol is not full forward security[14] and proposed his protocol. Nonetheless, Shims protocol still suffers from an important security flaw because it is not protected from a man-in-the-middle attack[16]. After that, many protocols was proposed in[3], [4], [9], [12] and [19]. Recently Ryu, Yoon and Yoo proposed a new ID-based protocol[11], which is more efficient, required only one pairing computation and two point multiplication. But in this paper, we will show this protocol is insecure under the Key Compromise Impersonation Attack, which was descirbe in[18], and key reveal attack describe in [8]. Then we propose our protocol which was satisfy several desirable security attributes describe in[17].

The rest of this paper is organized in the following. In Section 2, we briefly review the bilinear group and secure property of the key agreement protocol. In Section 3, we review the protocol of Eun-Kyung Ryu, Eun-Jun Yoon, and Kee-Young Yoo's and show Key Compromise Impersonate attack and key reveal attack against the protocol. In section 4 we review shim's protocol and man-in-the-middle attack. then we propose our modified protocol, the efficiency and security are analyzed. Then we conclude the paper.

2 Preliminaries

2.1 Bilinear Group

we briefly review the necessary facts about bilinear map. We use the following notations:

1. G_1 is a additive group and G_2 is a multiplicative group, and both are cyclic groups of prime order p.
2. P is generator of G_1.
3. e is bilinear map $e : G_1 \times G_1 \to G_2$.

Let G_1 and G_2 is defined above. A map $e : G_1 \times G_1 \to G_2$ is called bilinear map if e satisfy the following properties.

Bilinear: $\forall Q, R \in G_1$ and $\forall x, y \in \mathbb{Z}$ we have $e(xQ, yR) = e(Q, R)^{xy}$.

Non-degeneracy: $e(P, P) \neq 1$.

Computable: There exists an efficient algorithm to compute $e(Q, R)$, $\forall Q, R \in G_1$

For example, let G_1 be a subgroup of the additive group of the points of an supersingular elliptic curve E/F_p and G_2 be a subgroup of the multiplicative group of a finite field F_{p^2} . Then the Weil pairing (respectively, Tate pairing) could be used to construct bilinear maps between these two groups.

The Bilinear Diffie-Hellman(BDH) problem about $e : G_1 \times G_1 \to G_2$ is as follows: given a tuple $P, aP, bP, cP \in G_1$ as input, we want to get $e(P, P)^{abc}$ as output. The Computational Diffie-Hellman(CDH) problem in Group G_1 is: given a tuple $P, aP, bP \in G_1$ as input, we want to get abP as output. For the remainder of the paper we assume that BDH problem was hard about $e : G_1 \times G_1 \to G_2$, and CDH problem was hard in G_1

2.2 Security Property

For get a sound key agreement protocol, we need define some Property. We show these property in detail,which were defined in[17].Here we assume Alice and Bob are two honest entities.

Known-Key Security: In each round of key agreement protocol, Alice and Bob should generate a unique secret key. Each key generated in one protocol round is independent and should not be exposed if other secret keys are compromised.

Forward Secrecy: The Forward Secrecy property is that if Alice and Bobs secret keys are compromised, the session keys used in the past should not be recovered.

Key-Compromise Impersonation: A protocol which is secure against the key compromise impersonation attack means that if Alices secret key is compromised, the adversary who knows the value can not impersonate others to Alice.

Unknown Key-Share: After the protocol, Alice ends up believing he shares a key with Bob, and Bob mistakenly believes that the key is instead shared with an adversary. Therefore, a sound authenticated key agreement protocol should prevent the unknown key-share situation.

No Key Control: The key should be determined jointly by both Alice and Bob. Neither Alice nor Bob can control the key alone.

In some case, in the ID-Based system, we need

Perfect Forward Security:(Non-Escrow) Even the KGC is compromised, the previously established session keys are not compromised.

3 Review and Attack of Ryu, Yoon and Yoo's Protocol

3.1 Ryu, Yoon and Yoo's Protocol

Setup: The KGC select G_1, G_2, $e : G_1 \times G_1 \to G_2$, P as described in 2.1, and also select $H_1 : \{0,1\}^* \to G_1$, $s \in \mathbb{Z}_p^*$, $s \in \mathbb{Z}_p^*$ and H which is a key derivation function. Then KGC computes $P_{pub} = sP$, publishes $< G_1, G_2, e, P, P_{pub}, H_1, H >$, and keep s for master key.

Extract: For a user with identity ID the public key is given by $Q_{ID} = H_1(ID)$ and the KGC generates the associated private key as $S_{ID} = sQ_{ID}$.

Key Agreement: The key agreement are the following steps:

1. A picks $a \in \mathbb{Z}_p^*$ at random, computes $T_A = aP$, and sends T_A to B.
2. B picks $b \in \mathbb{Z}_p^*$ at random, computes $T_B = bP$, and sends T_B to A.
3. A computes the session key $K_{AB} = H(A, B, aT_B, e(S_A, Q_B))$ and B computes $K_{BA} = H(A, B, bT_A, e(Q_A, S_B))$.
4. If both A and B follow the protocol they will compute the same session key $K_{AB} = K_{BA} = H(A, B, abP, e(Q_A, Q_B)^s)$.

3.2 Key Compromise Impersonate Attack On this protocol

Here, we assume A and B are two honest entities. One adversary Adv has A's private key. Then Adv can impersonate any entities to sand message to A. For example, if Adv want to impersonate B. He can do as follow:

1. Adv selects $b \in \mathbb{Z}$ and send bP to A.
2. Adv receives $T_A = aP$ from A.
3. because Adv knows S_A, so he can get the session key from $H(A, B, bT_A, e(S_A, Q_B))$.

So this protocol is non satisfies the Key Compromise Impersonation. Let us check the protocol, it is not secure because the $e(Q_A, Q_B)^s$ is symmetry of Q_A and Q_B. So either S_A or S_B can be used to get $e(Q_A, Q_B)$.

3.3 Reveal Attack on this protocol

Key reveal Attack means the adversary have a access to a key reveal oracle which can reveal an old session key that has been previously accepted. So the adversary can derive something from other established session key. This attack is define in the security model in [1]. As [17] had correctly pointed out, two-flow authenticated key establishment protocols that do not contain asymmetry in the formation of the session key will not meet the security requirements in the [1] security model. Unfortunately this protocol is symmetric. So it can't against reveal attack. We will show if Adv want to share a session key with A, he can first initiate a protocol with B, then he use the key reveal oracle to get the session key, finally he will get a session key with A form his session key shared with B. The detail follows:

1. Adv intercepts $T_A = aP$ from A. Then he choose $c \in \mathbb{Z}$, and impersonate A to send acP to B.
2. Adv intercepts $T_B = bP$ from B. He impersonate B to send bcP to A.
3. A computes the session key
$K_{ab} = H(A, B, a(bcP), e(Q_A, Q_B)) = H(A, B, abcP, e(Q_A, Q_B)^s)$.
Similarly, B computes the session key $K_{ab} = H(A, B, b(acP), e(Q_A, Q_B)) = H(A, B, abcP, e(Q_A, Q_B)^s)$.
4. Adv ask the the reveal oracle the session key between Adv and B. Then he also know the session key between he and A.

4 Our modified Protocol

To prevent the key compromise attack and key reveal attack on Ryu, Yoon and Yoo's Protocol, we should use some asymmetric information to replace $e(Q_A, Q_B)^s$, we find if this protocol is combined with Shim's protocol in [14] we can get a protocol with high security, which not only prevent the man-in-the-middle attack on shim's protocol, but also prevent the key compromise attack and key reveal attack on Ryu, Yoon and Yoo's Protocol. And the new protocol only need one more point multiplication.

4.1 Review of Shim's protocol

The **Setup** and **Extract** algorithms are same as the previous protocol and **Key Agreement protocol** is as follows:

1. A picks $a \in \mathbb{Z}_p^*$ at random, computes $T_A = aP$, and sends T_A to B.
2. B picks $b \in \mathbb{Z}_p^*$ at random, computes $T_B = bP$, and sends T_B to A.
3. A computes the shared security $K_{AB} = e(aP_{pub} + S_A, , T_B + Q_B)$.
4. Similarly, B computes the shared security $K_{AB} = e(T_A + Q_A, bP_{pub} + S_B)$
5. If both A and B follow the protocol they calculate the same shared secret: $K_{AB} = K_{BA} = e(P, P)^{abs} e(P, Q_B)^{as} e(Q_A, P)^{bs} e(Q_A, Q_B)^s$, the session key is $H(A, B, K_{AB})$

The man-in-the-middle attack on this protocol [16]is as follows:

1. one adversary Adv intercepts T_A from A. He sends $T'_A = a'P - Q_A$ to B, where a' is selected by Adv.
2. Adv intercepts T_B from B. He and sends $T'_B = b'P - Q_B$ to A, where b' is selected by Adv.
3. then Adv share the secret
   $K_{AB'} = e(aP_{sub} + S_A, T'_B + Q_B) = e(P, P)^{ab's} e(Q_A, P)^{sb'} = e(T_A + Q_A, b'P_{pub})$ with A
   and share $K_{A'B} = e(T'_A + Q_A, bP_{sub} + S_B,) = e(P, P)^{a'bs} e(P, Q_B)^{a's} = e(a'P_{pub}, T_B + Q_B)$ with B.

4.2 Our modified protocol

The **Setup** and **Extract** algorithms are same as the previous protocol and **Key Agreement protocol** is as follows:

1. A picks $a \in \mathbb{Z}_p^*$ at random, computes $T_A = aP$, and sends T_A to B.
2. B picks $b \in \mathbb{Z}_p^*$ at random, computes $T_B = bP$, and sends T_B to A.
3. A computes $h = aT_B = abP$ and the shared security $K_{AB} = e(aP_{pub} + S_B, T_B + Q_B)$.
4. Similarly, B computes $h = aT_A = abP$ and the shared security $K_{AB} = e(T_A + Q_A, bP_{pub} + S_B)$
5. If both A and B follow the protocol they calculate the same shared secret: $K_{AB} = K_{BA} = e(P, P)^{abs} e(P, Q_B)^{as} e(Q_A, P)^{bs} e(Q_A, Q_B)^s$, the session key is $H(A, B, h, K_{AB})$

protocol	weakness	pairing	point multiplication	blocks
Smart[15]	Forward security	2	2	1
Shim[14]	Man-in-the-middle	1	2	1
Chen-Kudla[3]		1	4	2
Choie-Jeong-Lee 1[4]		2	3	2
Choie-Jeong-Lee 2[4]		2	4	1
Ryu-Yoon-Yon[11]	Key compromise impersonate Reveal attack	1	2	1
McCullagh-Barreto[9]	Key compromise impersonate Reveal attack	1	2	1
McCullagh-Barreto Revised	Reveal attack	2	2	1
Xie[19]		2	3	1
our		1	3	1

Table 1

4.3 Analysis of Efficiency

Our protocol is role symmetric, meaning both communication entities execute the same operations. For each user, one paring computation and three point multiplication are required. We compare our protocol with others in Table 1. Because the calculation of a bilinear pairing is a computationally expensive process, so our protocol are more efficient than Smart's Choie-Jeong-Lee's, Xie's and McCullagh-Barreto's protocol. Compare to Chen-Kundla's protocol, our protocol need only one large data block exchange. Although our protocol are not as efficient as Shim's and Ryu-Yoon-Yoo's, we use only one more point multiplication to make up these protocol's flaw.

4.4 Analysis of Security

The security of this protocol is based on BDH assume and CDH assume. In fact, our protocol include DH protocol as a part of itself, so it is easy to show its security. In this section, we use heuristic proof to show our protocol satisfies the following properties:

Against Passive Attack: If an adversary who eavesdrops on a successful protocol run can compute a session key using only information obtainable over network, then the adversary could also break the Diffie-Hellman Problem(DHP) in G1. This is because computing the session key involves deriving the keying material abP from the values $T_A = aP$ and $T_B = bP$. Thus, we claim that it is no less difficult to break the DHP in G1 even though the adversary knows the long-term secret key s of the KGC. Therefore our protocol resists passive attack at least as well as the Diffie-Hellman scheme.

Against Man-in-the-middle attack: If an adversary want to implement man-in-the-middle attack, he replaces $T_A = aP$ with $a'P$ and substitutes $T_B = bP$ with $b'P$, Then $K_{AB'} = e(P,P)^{ab's}e(P,Q_B)^{as}e(Q_A,P)^{b's}e(Q_A,Q_B)^s$. The adversary knows b' and aP, so he can compute $e(Q_A,P)^{b's}$,and$e(P,P)^{ab's}$ but if he want to compute $e(P,Q_B)^{as}e(Q_A,Q_B)^s$ he must know S_B,or know the asP from aP and sP, which is CDH problem. If the adversary want to implement man-in-the-middle-attack like attack on Shim's protocol, he can replace $T_A = aP$ with $a'P - Q_B$. But he need to compute $b(a'P - Q_B)$, so he need to get b from bP, or he need to know the discrete logarithm $\log_P Q_B$.

Against Reveal Attack: This is true because K_{AB} has some asymmetric of a and b, so we can avoid reveal attack like previous section.

Known key security: This is true since each run of the protocol computes a unique session key that depends on the ephemeral private keys a and b. If the adversary know some other session keys, he also need to computer abP, this is CDH problem. There does not appear to be any easier way for him to carry out an expensive brute-force attack. This means he can gain no more information from other session keys.

Forward Security: If the private keys are compromised, the adversary also need to compute abP form aP and bP, which is CDH problem and is independent of private keys. So even adversary know the private key, he can't get previous session key.

Perfect Forward Security: Even adversary knows master key s, abP, part of session key is relevant to s. So the adversary con't get session key yet.

Key Compromise Impersonate: If adversary knows private key of A, he want to impersonate someone else like B to share key with A. He impersonate B, so he know aP,b and S_A, so he can computer $e(P,P)^{abs}$,$e(Q_A,P)^{bs}$ and$e(Q_A,Q_B)^s$. But $K_{AB} = e(P,P)^{abs}e(P,Q_B)^{as}e(Q_A,P)^{bs}e(Q_A,Q_B)^s$, so if he can get K_AB, he must con compute $e(P,Q_B)^{as}$. However, he only knows Q_B not S_B, he must compute asP, which is CDH problem.

Unknown Key Share: Because we use B's public key Q_B to compute session key. So we know who we share key with.

Imperfect Key Control: Obviously, no entity can decide the key separately. But we must note the fact that one entity, say B, in practice will receive the key component of the other party, say A, before B sends its component back to A [10]. This puts B at an unfair advantage on controlling the value of the shared session key. Therefore, every protocols observed in this paper does not possess the full key control, as mention in [3].

5 Conclusion

We derive a new ID-Base key agreement protocol based on pairing from two protocol. We first show some attack to Ryu-Yoon-Yoo's protocol, and then, we combine this protocol with Shim's protocol. We need only one more point multiplication and two point additive, but our protocol satisfies some secure properties which these two protocol don't satisfy. Then we analyze our protocol in detail.

References

[1] Mihir Bellare and Phillip Rogaway, *Entity Authentication and Key Distribution*, In Advances in Cryptology - Crypto 1993, pages 110C125. Springer-Verlag, 1993. Volume 773 of Lecture Notes in Computer Science.

[2] D. Boneh and M. Franklin, *Identity-based Encryption from the Weil pairing*, SIAM J. of Comput- ing, 32(3):586-615, 2003. Extended abstract in Proceedings of Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.

[3] L. Chen and C. Kudla, *Identity based authenticated key agreement protocols from pairing*, In: Proc. 16th IEEE Security Foundations Workshop, pages 219C233, IEEE Computer Society Press, 2003.

[4] Young Ju Choie, Eunkyung Jeong, Eunjeong Lee, *Efficient identity-based authenticated key agreement protocol from pairings*, Applied Mathematics and Computation 162 (2005) 179C188.

[5] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, 6(1976), 644C654.

[6] M. Choudary Gorantla, Raju Gangishetti and Ashutosh Saxena, *A Survey on ID-Based Cryptographic Primitives*, Cryptology ePrint Archive, Report 2005/094, 2003.

[7] A. Joux, *A one round protocol for tripartite Diffe-Hellman*, In Proc. of ANTS, LNCS 1838, pp. 385-394, 2000.

[8] K. Kwang and R. Choo, *Revisit Of McCullagh-Barreto Two-Party ID-Based Authenticated Key Agree- ment Protocols*, Cryptology ePrint Archive, Report 2004/343, 2004. http://eprint.iacr.org/2004/343.

[9] N. McCullagh and P. S. L. M. Barreto, *A New Two-Party Identity-Based Authenticated Key Agreement*, Cryptology ePrint Archive, Report 2004/122, 2004. In Proceeding of CT-RSA 2005. http://eprint.iacr.org/2004/122.

[10] C. Mitchell, M. Ward, P. Wilson, *Key control in key agreement protocols*, Electronics Letters 34 (10) (1998) 980C981.

[11] Eun-Kyung Ryu, Eun-Jun Yoon, and Kee-Young Yoo, *An Efficient ID-Based Authenticated Key Agreement Protocol*, Networking 2004 Volume 3042,2004.

[12] M. Scott, *Authenticated ID-based key exchange and remote log-in with insecure token and PIN number*, http://eprint.iacr.org/2002/164.pdf

[13] A. Shamir, *Identity-based Cryptosystem s and Signature Schemes,* In Advances in Cryptology- Crypto'84, LNCS 196, pp. 47-53, Springer-Verlag, 1984.

[14] K. Shim, *Effient ID-based authenticated key agreement protocol based on the Weil pairing*, Electron. Lett., 39(8), pp. 653-654, 2003.

[15] N. P. Smart, *An ID-based authenticated key agreement protocol based on the Weil pairing*, Electron. Lett., 38(13), pp. 630-632, 2002.

[16] Hung-Min Sun and Bin-Tsan Hsieh, *Security Analysis of Shim's Authenticated Key Agreement Protocols from Pairings*, Cryptology ePrint Archive, Report 2003/113, 2003. http://eprint.iacr.org/2003/113.

[17] Simon Blake-Wilson, Don Johnson, and Alfred Menezes, *Key Agreement Protocols and their Security Analysis*, In 6th IMA International Conference on Cryptography and Coding, pages 30C 45. Springer-Verlag, 1997. Volume 1355 of Lecture Notes in Computer Science.

[18] 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, 2004, http://eprint.iacr.org/2004/308.

[19] G. Xie, *An ID-Based Key Agreement Scheme from pairing*, Cryptology ePrint Archive, Report 2005/093, 2005, http://eprint.iacr.org/2005/093.