Cryptanalysis of Two ID-based Authenticated Key Agreement Protocols from Pairings

Kyung-Ah Shim

Department of Mathematics, Ewha Womans University
11-1, Daehyun-dong, Seodaemun-gu, Seoul, 120-750, Korea
kashim@ewha.ac.kr

Abstract. Recently, a number of ID-based two-party authenticated key agreement protocols which make of bilinear pairings have been proposed [3, 8, 12, 11, 14]. In this paper, we show that the Xie's protocol [14] does not provide implicit key authentication and key-compromise impersonation resilience. Also, we point out the vulnerability of the Choi *et al*'s protocol [3] against signature forgery attacks.

Key words: ID-based system, bilinear pairing, authenticated key agreement protocol.

1 Introduction

In 1984, Shamir [10] introduced the concept of identity-based cryptography. In traditional public key cryptosystem, Alice's public key is a random string. When Bob wishes to send a message to Alice, he must first obtain her authenticated public key in public directories. The main idea in ID-based cryptosystems is to eliminate the public key distribution problem by making Alice's public key derivable from some known aspect of her identity, such as her email address. When Bob wants to send a message to Alice, he merely derives Alice's public key directly from her identifying information. Public key directories are unnecessary. Such cryptosystems alleviate the certificate overhead and solve the problems of PKI technology: certificate management including storage and distribution and the computational cost of certificate verification. Over the years a number of researchers tried to propose secure and efficient ID-based encryption schemes, but with little success. This state of affairs changed in 2001 when an ID-based encryption scheme based on Weil pairing was proposed by Boneh and Franclin [2]. In fact, the existence of bilinear pairings such as Weil and Tate pairings was thought to be a bad thing in cryptography; the MOV attack [9] and the FR attack [6] reduce the discrete logarithm problem on some elliptic curves or hyperelliptic curves to the discrete logarithm problem in a finite field via Weil pairing and Tate pairing, respectively. These led some family of elliptic curves to be avoided from cryptographic use. Since the Boneh-Franclin's ID-based encryption scheme, the bilinear pairings of algebraic curves have initiated some completely new fields in cryptography, making it possible to realize cryptographic primitives that were previously unknown or impractical.

At first, Joux [7] proposed a one-round tripartite Diffie-Hellman key agreement protocol based on the Weil pairings. However, like the basic Diffie-Hellman key agreement protocol [5], Joux's protocol also suffers from the man-in-the-middle attack because it does not attempt to authenticate the communicating entities. Smart [11] proposed an ID-based two-party authenticated key agreement protocol. But, Shim [12] pointed out that the Smart's protocol does not provide full forward secrecy and proposed a new protocol which achieves full forward secrecy. However, it turns out that the protocol is insecure against a man-in-the-middle attack [13]. Recently, Xie [14] and Choi *et al* [3] proposed ID-based two-party authenticated key agreement protocols from pairings. The authors argued that the protocols satisfy all the required security attributes described in [1]. In this paper, we show that the Xie's protocol and Choi *et al*'s protocol are insecure against impersonation attacks and signature forgery attacks, respectively.

The rest of this paper is organized as follows. In the following section, we describe admissible pairings and ID-based public key infrastructure. In section 3, we describe desirable security attributes of authenticated key agreement protocols. In section 4, we point out the vulnerabilities of two protocols against impersonation attacks and signature forgery attacks and . Concluding remarks are given in section 5.

2 Security Attributes of Authenticated Key Agreement Protocols

Let A and B be two honest entities, i.e., legitimate entities who execute the steps of a protocol correctly. A key agreement protocol is said to provide *implicit key authentication* of B to A if entity A is assured that no other entity aside from a specifically identified second entity B can possibly learn the value of a particular secret key. A key agreement protocol which provides implicit key authentication to both participating entities is called an *authenticated key agreement* (AK) protocol. In addition to the fundamental security goal such as implicit key authentication, a number of desirable security attributes of AK protocols have been identified [1].

- **Known-Key Security.** Each run of a key agreement between A and B should produce a unique secret key, such a key is called a *session key.* A protocol should achieve its goal in the face of an adversary who has learned some other session keys.
- **Forward Secrecy.** If long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities is not affected.
- **Key-Compromise Impersonation Resilience.** Suppose A's long-term private key is disclosed. Clearly an adversary that knows this value can now impersonate A, since it is precisely this value that identifies A. This loss does not enable an adversary to impersonate other entities as well and obtain the session key.

- **Unknown Key-Share Resilience.** Entity B cannot be coerced into sharing a key with entity A without B's knowledge, i.e., when B believes the key is shared with some entity $C \neq A$, and A believes the key is shared with B.

3 Bilinear Pairings and ID-based Public Key Infrastructure

3.1 Bilinear Pairings

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of a large prime order q. We write $\mathbb{G}_1$ additively and $\mathbb{G}_2$ multiplicatively. We assume that the discrete logarithm problems in both $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard.

Admissible Pairing: We call e an *admissible pairing* if $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a map with the following properties:

1. Bilinearity: $e(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and for all $a, b \in \mathbb{Z}$.
2. Non-degeneracy: There exists $P \in \mathbb{G}_1$ such that $e(P,\ P) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such admissible pairing, as in [2, 7].

3.2 ID-based Public Key Infrastructure

Now, we describe ID-based public key infrastructure based on pairing. ID-based public key infrastructure involves a Key Generation Center (KGC) and users. It consists of **Setup** and **Private Key Extraction** algorithms. Let P be a generator of $\mathbb{G}_1$. Remember that $\mathbb{G}_1$ is an additive group of prime order q and $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is the bilinear pairing. Let $H : \{0,1\}^* \rightarrow \mathbb{Z}_q$ and $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$ be two cryptographic hash functions.

• **Setup**: KGC chooses a random $s \in \mathbb{Z}_q^*$ and set $P_{KGC} = sP$. KGC publishes the system parameters $< \mathbb{G}_1, \mathbb{G}_2, q, e, P, P_{KGC}, H(\text{or } H_1) >$ and keep s as a master secret key.

• **Private Key Extraction I**: For a given string $ID \in \{0,1\}^*$, this algorithm do;

1. Compute the user's public key as $Q_{ID} = H_1(ID) \in \mathbb{G}_1$,
2. Set the private key S_{ID} to be sQ_{ID}, where s is a master secret.

• **Private Key Extraction II**: For a given string $ID \in \{0,1\}^*$, this algorithm do;

1. Compute $\alpha = H(ID) \in \mathbb{Z}_q$.
2. Set the private key d_{ID} to be $\frac{1}{\alpha+s}P$ and $\alpha + sP$ is the public key corresponding to ID.

4 Cryptanalysis of ID-based Two-party AK protocols

4.1 Xie's ID-based AK Protocol with Escrow

Recently, Xie [14] showed that the McCullagh and Barreto's ID-based AK protocol is insecure against the key-compromise impersonation attack. And proposed an improved protocol to defeat the attack. They argue that its protocol satisfies all the security attributes described in § 2. First, we review the Xie's protocol.

■ **Xie's Protocol**

$$\begin{array}{ll} (1) & A \longrightarrow B \ : \ A_{KA} = x(bP + sP) \\ (2) & A \longleftarrow B \ : \ B_{KA} = y(aP + sP). \end{array}$$

This protocol follows the **Private Key Extraction II** algorithm. Let $H_1(ID_A) = a$ and $H_1(ID_B) = b$. First, A and B exchange the ephemeral public keys A_{KA} and B_{KA}. Then, A computes

$$K_A = e(B_{KA}, d_A)^{x+1} e(P, P)^x$$

and B computes

$$K_B = e(A_{KA}, d_B)^{y+1} e(P, P)^y.$$

The resulting session key is $K = K_A = K_B = e(P, P)^{xy+x+y}$.

Now we show that the Xie's protocol is insecure against impersonation attacks, i.e., an adversary can impersonate A to B at any time. The attack on the protocol is mounted as follows;

• **Impersonation Attacks:** Suppose that an adversary E wants to impersonate A to B. $E(A)$ denotes E masquerade as A. First, $E(A)$ sends $A_{KA} = -(bP+sP)$ to B impersonating A. After receiving the message, B sends $B_{KA} = y(aP+sP)$ and computes the session key

$$K_B = e(-(bP + sP), d_B)^{y+1} e(P, P)^y = e(P, P)^{-y-1} e(P, P)^y = e(P, P)^{-1}.$$

By bilinearity of e, the value $e(P, P)^y$ disappears in the resulting session key. Thus, E is also able to compute $K_B = e(P, P)^{-1}$ from known value. Finally, E succeeds to impersonate A to B as well as the knowledge of the session key K_B.

In above attack, an adversary can generate an ephemeral public key to confine the shared secret to a predictable value. Thus, the Xie's protocol does not provide implicit key authentication attribute. From the attack, we can easily see that the protocol is insecure against man-in-the-middle attacks and key-compromise impersonation attacks. The same attacks can be applied to the Xie's ID-based AK protocol without escrow and AK between members of distinct domains.

4.2 Choi *at al*'s ID-based AK Protocol

Choi *et al* [3] proposed two ID-based authenticated key agreement protocols satisfying forward secrecy. Their protocol I adapts a signature scheme to provide authentication; the authenticity of the ephemeral public keys in the protocol I are assured by each user's signature. We show that the protocol I does not achieve authentication as intended, i.e., anyone can forge each user's signature.

■ **Choi** *et al*'s **Protocol I**

$$\begin{array}{ll} (1) & A \longrightarrow B \;:\; U_A = aP_{KGC},\; V_A = aS_A \\ (2) & A \longleftarrow B \;:\; U_B = bP_{KGC},\; V_B = bS_B. \end{array}$$

This protocol follows the **Private Key Extraction I** algorithm. First, A sends (U_A, V_A) to B. On the receipt of the message from A, B verifies $e(V_A, P) = e(Q_A, U_A)$. If the equation holds, B sends $(U_B V_B)$ to A and computes $K_B = bU_A$. After receiving the message from B, A verifies $e(V_B, P) = e(Q_B, U_B)$. If the equation holds, A computes $K_A = aU_B$. The resulting session key is $K = kdf(K_A, Q_A, Q_B) = kdf(K_B, Q_A, Q_B) = kdf(absP, Q_A, Q_B)$, where kdf is a key derivation function.

• **Signature Forgery Attack:** In the protocol I, anyone can generate a valid pair (U_A, V_A) satisfying $e(V_A, P) = e(Q_A, U_A)$ as follows; an adversary chooses a at random and then computes $U_A = aP$ and $V_A = aQ_A$. Then the pair satisfies the verification equation $e(V_A, P) = \hat{e}(Q_A, U_A)$;

$$e(V_A, P) = e(aQ_A, P) = e(Q_A, aP) = e(Q_A, U_A).$$

Therefore, an adversary can forge each user's signature on the ephemeral public key without the knowledge of corresponding long-term private key. Although this attack does not allow the adversary to gain any knowledge of the agreed session key, the signature scheme adapted to cryptographic protocols should be secure.

5 Conclusion

We have shown that the Xie's protocol is insecure against impersonation attacks including man-in-the-middle attacks and key-compromise impersonation attacks and the Choi *et al*'s protocol is also insecure against the signature forgery attacks

References

1. S. Blake-Wilson and A. Menezes, "Authenticated Diffie-Hellman key agreement protocols", Proc. of the 5th Annual Workshop on Selected Areas in Cryptography, SAC'98, LNCS 1556, Springer-Verlag, pp. 339-361, 1999.

2. D. Boneh and M. Franclin, “Identity-based encryption from the Weil pairing”, Advances in cryptology; Crypto’01, LNCS 2139, Springer-Verlag, pp. 213-229, 2001.
3. Y. J. Choie, E. Jeong and E. Lee,“Efficient identity-based authenticated key agreement protocol from pairings”, Applied Mathematics and Computation, vol. 162(1), pp. 179-188.
4. C. Cocks, “An identity-based encryption schme based on the quadratic residues”, Cryptography and Coding, LNCS 2260, Springer-Verlag, pp. 360-363, 2001.
5. W. Diffie, and M. Hellman, “New Directions in Cryptography”, IEEE Transactions on Information Theory, Vol. 22(6), pp. 644-654, 1976.
6. G. Frey, and H. Ruck, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”, Math. of Computaions, 62, pp. 865-874, 1994.
7. A. Joux, “A one round protocol for tripartite Diffie-Hellman”, Proc. of ANTS IV, LNCS 1838, Springer-Verlag, pp. 385-394, 2000.
8. N. McCullagh, P. S. L. M. Barreto, “A new two-party identity-based authenticated key agreement”, CT-RSA’05, LNCS 3376, Springer-Verlag, pp. 262-274, 2005.
9. A. Menezes, T. Okamoto and S. Vanstone, “Reducing elliptic curve logarithms in a finite field”, IEEE Trans. on Information Theory, vol. 39(5), pp. 1639-1646, 1993.
10. A. Shamir, “Identity-based cryptosystems and signature schemes”, Advances in cryptology; Crypto’84, LNCS 196, Springer-Verlag, pp. 47-53, 1884.
11. N. Smart, “An ID-based authenticated key agreement protocol based on the Weil pairing”, Elec. Lett., vol. 38(13), pp. 630-632, 2002.
12. K. Shim, ”Efficient ID-based authenticated key agreement protocol from the Weil pairing,” Elect. Lett., vol. 39, pp. 653-654, 2003.
13. H. Sun and B. Hsieh, “Security analysis of Shim’s authenticated key agreement protocols from pairings”, Cryptogarphy ePrint Archive, Report 2003/113, available at http://eprint.iacr.org/2003/113, 2003.
14. G. Xie, “An ID-based key agreement scheme from pairing”, Cryptology ePrint Archive: Report 2005/093, available at http://eprint.iacr.org/2005/093, 2005.