An Efficient ID-Based Authenticated Key Agreement Protocol from Pairings

Eun-Kyung Ryu, Eun-Jun Yoon, and Kee-Young Yoo

Department of Computer Engineering, Kyungpook National University,
Daegu 702-701, South Korea
{ekryu,ejyoon}@infosec.knu.ac.kr, yook@knu.ac.kr

Abstract. In this paper, we describe a new ID-based authenticated key agreement protocol that makes use of bilinear pairings. We then discuss the security properties of our scheme, including known-key security, perfect forward secrecy and no key control. It is also able to withstand both passive and active attacks. An important advantage of our scheme is that it preserves the perfect forward secrecy even though the long-term secret key of a trusted key generation center is compromised. We also show that it is more efficient than Chen and Kudla's protocol with same security properties as ours.

1 Introduction

Key agreement is one of the fundamental problems considered in cryptography. The best-known protocol for key agreement is the Diffie-Hellman protocol, which allows two parties to establish a shared secret by exchanging messages over an open channel without the need for any prior communication. However, the basic Diffie-Hellman protocol is susceptible to a man-in-the-middle attack because it does not authenticate the communicating parties.

Many solutions to this vulnerability in the Diffie-Hellman scheme have been developed over the years; recently, the identity-based (ID-based) approach has been the subject of much interest. In ID-based schemes, a public key is calculated directly from the user's identity rather than being extracted from a certificate that is issued by a trusted third-party. Such schemes can potentially provide the benefits of public key cryptography without the need for certificates and their attendant public key infrastructure.

One of the first feasible solutions for ID-based encryption was Boneh and Franklin's scheme[3], which is based on pairings on elliptic curves. Other feasible ID-based key agreements based on the pairing technique were then developed; in particular, Smart[8] proposed an ID-based authenticated key agreement protocol based on a combination of the ideas from [1] and [2].

All ID-based key agreement protocols require a Key Generation Center (KGC) that is relied upon to create and deliver private keys to entities and to not abuse its knowledge of those keys. However, a property that should be required of ID-based protocols is that if two entities are communicating, then the KGC cannot derive the established session key. In addition, if at any stage the

N. Mitrou et al. (Eds.): NETWORKING 2004, LNCS 3042, pp. 1458–1463, 2004.

KGC's key is compromised, this should not compromise the previously established session keys. This property is called *full forward secrecy* or *perfect forward secrecy*, which should be an important consideration when designing ID-based authenticated key agreement protocols.

However, Shim[6] pointed out that Smart's scheme does not have the property of perfect forward secrecy, which we believe to be an important security requirement for authenticated key agreement protocols. Shim proposed an alternative ID-based authenticated key agreement protocol, which is claimed to be efficient and to provide many security properties such as known-key security, perfect forward secrecy, key compromise impersonation resilience, and unknown key-share resilience. Nonetheless, Shim's protocol still suffers from an important security flaw because it is not protected from a man-in-the-middle attack, as described in [5]. After that Chen and Kudla in [7] introduced a ID-based authenticated key agreement protocol which includes the property of the perfect forward secrecy by increasing communication and computation overhead.

In this paper, we describe a new ID-based authenticated key agreement protocol in which computation and communication overheads for computing a session key are significantly reduced, while it provides same security propertis with Chen and Kulda's protocol. This new protocol combines the idea of ID-based cryptosystems from pairing on elliptic curve with the basic Diffie-Hellman key agreement scheme.

2 Bilinear Pairings

In this section, we briefly describe the basic definition of the bilinear pairing that is necessary for the description of our protocol. Let G_1 be a cyclic additive group generated by P whose order is a prime number q, and let G_2 be a cyclic multiplicative group of the same order q. Typically G_1 will be a subgroup of the group of points on an elliptic curve over a finite field, and G_2 will be a subgroup of the multiplicative group of a related finite field. A mapping

$$\hat{e} : G_1 \times G_1 \to G_2$$

is called a *bilinear pairing* which has the following properties:

- *Bilinearity*: $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q) \cdot \hat{e}(P_2, Q)$ and $\hat{e}(P, Q_1 + Q_2) = \hat{e}(P, Q_1) \cdot \hat{e}(P, Q_2)$, or $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$;
- *Non-degeneracy*: If P is a generator of G_1, then $\hat{e}(P, P)$ is a generator of G_2. In other words, $\hat{e}(P, P) \neq 1$;
- *Computability*: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in G_1$.

We note that the Weil and Tate pairings associated with supersingular elliptic curves or Abelian varieties can be modified to create such bilinear maps; details can be found in [3,4].

For the remainder of the paper, we will use G_1 to refer to an additive group and G_2 to refer to a multiplicative group. We assume that the Discrete Logarithm Problem in both G_1 and G_2 is hard.

3 The Protocol

In this section we demonstrate a new ID-based authenticated key agreement protocol. This protocol consists of two phases: system setup and authenticated key agreement.

3.1 System Setup

As stated previously, an ID-based system requires a Key Generation Center(KGC) that is relied upon to create and deliver private keys to entities and to not abuse its knowledge of those keys. A KGC constructs two groups, G_1 and G_2, and a mapping $\hat{e} : G_1 \times G_1 \rightarrow G_2$ that is a bilinear pairing, as described in the preceding section. The KGC publishes $\{G_1, G_2, \hat{e}, P, H_1, H\}$, where P is a primitive root of G_1 and H_1 is a cryptographic hash function $H_1 : \{0,1\}^* \rightarrow G_1$ that maps a message of arbitrary length into a nonzero point of G_1, as described in [8]. H is a key derivation function, typically a secure hash function. The KGC then chooses a random integer $s \in Z_q^*$ as the secret key. Note that without the use of the key derivation function H, an adversary might be able to gain partial information about the session key despite the hardness of the underlying problem.

For an entity with identity information ID, the public key is given by $Q_{ID} = H_1(ID)$, and the KGC computes the private key as $S_{ID} = sQ_{ID}$. The KGC then issues S_{ID} to the entity via a secure channel. Thus, an ID-based key pair is defined as (Q_{ID}, S_{ID}), where $Q_{ID}, S_{ID} \in G_1$.

3.2 Authenticated Key Agreement

Suppose two communication entities, Alice and Bob want to establish a secret session key. To achieve this, they perform an instance of the protocol run. We denote their respective private keys as

$$S_A = sQ_A \text{ and } S_B = sQ_B$$

that have been obtained from the KGC.

Alice(A) and Bob(B) each randomly choose an ephemeral private key $a, b \in Z_q^*$, and compute the values of corresponding public keys, $T_A = aP$ and $T_B = bP$. Then they exchange the public keys as follows:

1. A $\rightarrow$ B: T_A
2. B $\rightarrow$ A: T_B

After that, Alice computes the session key $K_{AB} = H(A, B, K_A, V_A)$, where $K_A = a \cdot T_B$ and $V_A = \hat{e}(S_A, Q_B)$. Bob also computes the session key $K_{BA} = H(A, B, K_B, V_B)$, where $K_B = b \cdot T_A$ and $V_B = \hat{e}(S_B, Q_A)$.

Note, that both parties have the secret key $K_{AB} = K_{BA} = H(A, B, abP, \hat{e}(Q_A, Q_B)^s)$. Therefore the share secret key depends on the identities Q_A, Q_B of two parties, the secret key s of the key generation center and the two ephemeral

keys a, b. For the process of key confirmation it can easily be added to our protocol in the same manner as described in [8,2].

The strength of our protocol depends only on the difficulty of the well-known Discrete Logarithm Problem in G_1 and on the classical Diffie-Hellman assumption. The protocol makes use of the bilinearity property, but this does not require any additional assumptions to be made.

4 Security Analysis

In this section, we argue that our scheme has the following security properties.

- **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 G_1. 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 G_1 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.
- **Man-in-the-middle attack:** A man-in-the-middle attack, which requires an adversary to fool both sides of a legitimate conversation, cannot be carried out by an adversary who does not know Alice or Bob's private key. For example, suppose that an adversary, Eve, wants to fool Bob into thinking he is talking to Alice. First, Eve can compute $A' = a'P$ and send A' to Bob. Conversely, Bob computes $B = bP$ and send them to Eve, believing her to be Alice. The adversary must then compute $\hat{e}(Q_A, Q_B)^s$ to derive a correct session key. Therefore, it is argued that an adversary with no knowledge of S_A or S_B, is not in a position to launch a classical man-in-the-middle attack against it.
- **Known-key security:** Suppose that an adversary learned a key $K_{AB} = H(A, B, abP, \hat{e}(Q_A, Q_B)^s)$ from a past session. The adversary does not gain any additional information from combining the past key with publicly visible data for the purpose of deducing future session keys. This is true since each run of the protocol computes a unique session key that depends on the ephemeral private keys a and b. There does not appear to be any easier way for him to carry out an expensive brute-force attack. It means that the adversary, having obtained some past session keys, gains no advantage toward computing future session keys. Thus, it the protocol resists the known-key attack.
- **Perfect Forward secrecy:** Suppose that an adversary has learned a long-term private key, either S_A or S_B, or both of the entities involved in a conversation. To extract the past session keys, the adversary must compute abP from aP and bP. However, this is assumed to be a hard problem equivalent to solving the DHP in G_1. In our scheme, any previous session key will not be compromised even if the long-term key s of the KGC may be corrupted. Therefore, it preserves the property of perfect forward secrecy. This property is one advantage of our scheme over the Smart's protocol[8] in which the

Table 1. Efficiencies of ID-based authenticated key agreement protocols

Protocol	Pairng	Point multiplication	Large blocks
Smart's protocol	2	2	2
Chen and Kudla's protocol	1	4	4
Ours	1	2	2

compromise of the long-term private keys or the KGC's secret key allows past session keys to be computed.

- **Key-compromise impersonation attack:** Suppose that Alice's long-term private key S_A is revealed to an adversary, Eve. Then, Eve can of course impersonate Alice in any protocol in which Alice is identified by this key. However, in our protocol, the compromise of one entity's long-term private key does not imply that the private key of the other entity will also be compromised. That is, possession of this key does not allow Eve to impersonate Bob to Alice, nor can she impersonate any entities besides Alice to Bob. To achieve this goal, the adversary would have to solve the Discrete Logarithm Problem in G_1. Thus, our protocol resists the key-compromise impersonation attack.
- **No key control:** The session keys in our protocol are determined jointly by both parties, so that neither party alone can control the outcome of the session key by restricting it to lie in some predetermined small set. Therefore, there is no key control in our protocol.

5 Efficiency

The proposed protocol is role symmetric, meaning both communication entities execute the same operations. We compare our protocol with Smart's protocol[8] and Chen and Kudla's[7], which are also role-symmetric ID-based schemes.

The factors that most affect the overall performance of authenticated key agreement protocols include the number of rounds, the communication overhead, and the computational overhead; therefore it is desirable to minimize these properties of the protocol used. In this section, we thus compare our protocol with them in terms of computation overhead and exchanged large message blocks except the number of rounds. Since message flows in our protocol are identical with the message flows of the two pass elliptic curve based unauthenticated Diffie-Hellman protocol as well as Smart's protocol and Chen and Kudla's.

Table 1 shows efficiencies of ID-based authenticated key agreement protocols for each user. In our protocol, each user requires to compute only one pairing and two elliptic curve point multiplications for establishing session key. The calculation of a bilinear pairing is a computationally expensive process; therefore reducing the number of pairing operations in a pairing-based protocol leads to significantly greater efficiency.

As we see from Table 1, our scheme and Chen and Kudla's protocol require only one pairing while Smart's needs two pairings. Furthermore, Smart's protocol does not preserve the security property of perfect forward secrecy. In Chen

and Kudla's protocol, each entity needs more two elliptic curve point multiplications and two large data blocks exchanged than ours by allowing their scheme to include the perfect forward secrecy. Therefore, the proposed scheme can be expected as the most efficient one in terms of computation and communication overhead.

6 Conclusion

Recently, many cryptographic schemes from pairings have been proposed. In this paper, we presented a new ID-based authenticated key agreement protocol that makes use of bilinear pairings. The security of our scheme is based on the difficulty of the well-known Discrete Logarithms Problem over an elliptic curve and on the classical Diffie-Hellman assumption. We argued that the proposed scheme has the properties of known-key security, perfect forward secrecy and no key control; it is also able to withstand both passive and active attacks, including key compromise impersonation and man-in-the-middle. We have also shown that our protocol is more efficient than Chen and Kudla's protocol with same security properties as ours.

Acknowledgement. We would like to thank anonymous reviewers for the helpful comments.This work was supported by the Brain Korea 21 Project in 2003.

References

1. A. Joux: A one-round protocol for tripartite Diffie-Hellman. Algorithm Number Theory Symposium, Lecture Notes in Computer Science 1838 (2000), pp. 385-394
2. A. Menezes, M. Qu, J. Solinas and S. Vanstone: Some new key agreement protocols providing mutual implicit authentication. In proceedings of the second workshop on Selected Area in Cryptography. (1995), pp. 22-32
3. D. Boneh, and M. Franklin: Identity-based encryption from the Weil pairing. Advances in Cryptology(Crypto'2001), Lecture Notes in Computer Science 2139 (2001), pp. 213-229
4. D. Boneh, B. Lynn, and H. Shacham: Short signatures from the Weil pairing. Advances in Cryptology(Asiacrypt'2001), Lecture Notes in Computer Science 2248 (2002), pp. 514-532
5. H. Sun and B. Hsieh: Security Analysis of Shim's Authenticated Key Agreement Protocols from Pairings. (available on eprint.iacr.org)
6. K. Shim: Efficient ID-based authenticated key agreement protocol from the Weil pairing. Electronics Letters 39 (2003), pp. 653-654
7. L. Chen and C. Kudla: Identity based authenticated key agreement protocols from pairings, Computer Security Foundations Workshop, (2003), pp.219-233
8. N.P. Smart: An identity based authenticated key agreement protocol based on the Weil pairing. Electronics Letters 38 (2002), pp. 630-632