Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 166 (2005) 523–530
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Weakness in ID-based one round authenticated tripartite multiple-key agreement protocol with pairings

Kyungah Shim *, Sungsik Woo

Department of Mathematics, Ewha Womans University, 11-1 Daehyun-dong, Seodaemun-gu, Seoul 120-750, Republic of Korea

Abstract

In this paper, we show that the ID-based tripartite authenticated multiple-key agreement protocol by Liu et al. [ID-based tripartite key agreement protocol with pairing, 2003 IEEE International Symposium on Information Theory, 2003, pp. 136–143, or available at Cryptology ePrint Archive, Report 2002/122] is insecure against an unknown key-share attack. And then we propose a more efficient ID-based tripartite authenticated multiple-key agreement protocol to overcome the attack.

1. Introduction

Recently, there have been proposed several new cryptosystems based on bilinear pairings. The existence of bilinear pairings such as Weil pairing and Tate pairing was thought to be a bad thing in cryptography; it was shown that

* Corresponding author. Address: Department of Mathematics, Ewha Womans University, 11-1 Daehyun-dong, Seodaemun-gu, Seoul 120-750, Republic of Korea.
E-mail address: shimkah@hanmail.net (K. Shim).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2004.06.104

the discrete logarithm problem in supersingular curves was reducible to that in an extension of underlying field via Weil pairing [6]. This led supersingular curves to be avoided from cryptographic use. This situation changed with the work of Boneh–Franclin's ID-based encryption scheme [2] and Joux's one round tripartite Diffie–Hellman protocol [4]. However, like the basic Diffie–Hellman key agreement protocol, Joux's protocol also suffers from the man-in-the-middle attack [7] because it does not attempt to authenticate the communicating entities. Recently, Liu et al. [5] proposed an ID-based one round authenticated tripartite key agreement protocol (LZC protocol) which results in eight session keys per one instance. The authenticity of the protocol is assured by a certain signature scheme so that messages carrying the information of two ephemeral public keys can be broadcasted by an entity. They argue that their protocol satisfies all the security attributes; implicit key authentication, known-key security, perfect forward secrecy, key-compromise impersonation resilience and unknown key-share resilience. However, this paper shows that the protocol is still vulnerable to an unknown key-share attack. And then we propose a new ID-based one round authenticated tripartite multiple-key agreement protocol to overcome the attack.

2. Bilinear pairings and some assumptions

Let $\mathbb{G}_1$ be a cyclic group generated by P, whose order is a prime q and $\mathbb{G}_2$ be a cyclic multiplicative group of the same order q. We assume that the discrete logarithm problem (DLP) in both $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a pairing which satisfies the following conditions:

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

We note that the Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear pairings [2].

- *Bilinear Diffie–Hellman (BDH) problem*: For a bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, given P, aP, bP, cP, compute $\hat{e}(P,P)^{abc}$, where a, b, c are randomly chosen from $\mathbb{Z}_q^*$.
- *Computational Diffie–Hellman (CDH) problem*: Given P, aP, bP, compute abP, where a and b are randomly chosen from $\mathbb{Z}_q^*$.
- *Square computational Diffie–Hellman (SCDH) problem*: Given P, aP, compute a^2P, where a is randomly chosen from $\mathbb{Z}_q^*$.