Mathematical and Computer Modelling 54 (2011) 3143–3152

Contents lists available at SciVerse ScienceDirect

Mathematical and Computer Modelling

journal homepage: www.elsevier.com/locate/mcm

A new two-round certificateless authenticated key agreement protocol without bilinear pairings

Debiao He [a,b], Yitao Chen [a,*], Jianhua Chen [a], Rui Zhang [a], Weiwei Han [c]

[a] *School of Mathematics and Statistics, Wuhan University, Wuhan, People's Republic of China*

[b] *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences,Beijing, People's Republic of China*

[c] *School of Mathematics & Computer Science, Guangdong University of Business Studies, Guangzhou, People's Republic of China*

ARTICLE INFO

Article history:
Received 28 April 2011
Received in revised form 30 July 2011
Accepted 1 August 2011

Keywords:
Certificateless cryptography
Authenticated key agreement
Provable security
Bilinear pairings
Elliptic curve

ABSTRACT

Certificateless public key cryptography (CLPKC), which can simplify the complex certificate management in the traditional public key cryptography and resolve the key escrow problem in identity-based cryptography, has been widely studied. As an important part of CLPKC, certificateless two-party authenticated key agreement (CTAKA) protocols have also received considerable attention. Recently, many CTAKA protocols using bilinear pairings have been proposed. But the relative computation cost of the pairing is approximately twenty times higher than that of the scalar multiplication over elliptic curve group. To improve the performance, several CTAKA protocols without pairings have been proposed. In this paper, we will show a latest CTAKA protocol is not secure against a type 1 adversary. To improve the security and performance, we also propose a new CTAKA protocol without pairing. At last, we show the proposed protocol is secure under the random oracle model.

Published by Elsevier Ltd

1. Introduction

Public key cryptography is an important technique to realize network and information security. Traditional public key cryptography requires a trusted certification authority to issue a certificate binding the identity and the public key of an entity. Hence, the problem of certificate management arises. To solve the problem, Shamir [1] defined a new public key cryptography called identity-based public key cryptography. However, identity-based public key cryptography needs a trusted key generation center (KGC) to generate the private key for every entity according to his identity. So we are confronted with the key escrow problem. Fortunately, the two problems in traditional public key infrastructure and identity-based public key cryptography can be prohibited by certificateless public key cryptography (CLPKC) [2], which can be conceived as an intermediate between traditional public key infrastructure and identity-based cryptography.

The first certificateless two-party authenticated key agreement (CTAKA) protocol appears in the seminal paper by Al-Riyami and Paterson [2]. However, no formal security model or proof for the CTAKA protocol is provided. Some other CTAKA protocols (e.g., [3–6]) were also proposed with heuristic security analysis. In order to improve the security, Swanson [7] proposed the first formal security model for the CTAKA protocol. Swanson also pointed that several early proposed CTAKA protocols [3–6] are insecure in his model. In [8], Lippold et al. proposed a new security model for CTAKA protocol. They also proposed a CTAKA protocol and prove its security under their model. Compared with Swanson's model, Lippold et al.'s model is stronger in the sense that after the adversary replaces the public key of a user, the user will use the new public/private key pair in the rest of the game, while in Swanson's model, the user keeps using his/her original public/private key pair. However,

[*] Corresponding author.
E-mail address: chenyitao.math@gmail.com (Y. Chen).

0895-7177/$ – see front matter. Published by Elsevier Ltd
doi:10.1016/j.mcm.2011.08.004