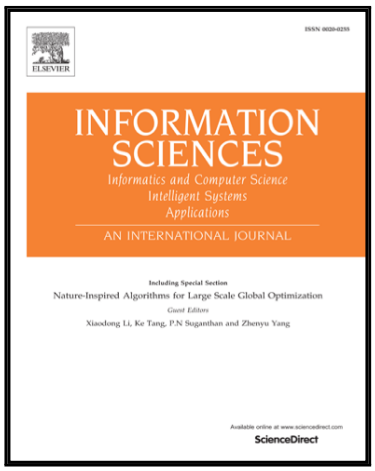

Comment on a Certificateless One-Pass and Two-Party Authenticated Key Agreement Protocol

Yang Lu , Quanling Zhang , Jiguo Li , Jian Shen

PII: S0020-0255(16)30462-5
DOI: 10.1016/j.ins.2016.06.041
Reference: INS 12315

To appear in: *Information Sciences*

Received date: 3 August 2015
Revised date: 2 June 2016
Accepted date: 23 June 2016

Please cite this article as: Yang Lu , Quanling Zhang , Jiguo Li , Jian Shen , Comment on a Certificateless One-Pass and Two-Party Authenticated Key Agreement Protocol, *Information Sciences* (2016), doi: 10.1016/j.ins.2016.06.041

Comment on a Certificateless One-Pass and Two-Party Authenticated Key Agreement Protocol

Yang Lu[a], Quanling Zhang[a], Jiguo Li[a], Jian Shen[b]

[a]College of Computer and Information, Hohai University, Nanjing, China
[b]School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China
[E-mail: luyangnsd@163.com, zhangquanling99@163.com, ljg1688@163.com, s_shenjian@126.com]
*Corresponding author: Yang Lu

Abstract: Authenticated key agreement protocol is a useful primitive which allows two or more entities to securely establish a shared secret key for their communications over an insecure public network. Recently, Zhang proposed an efficient certificateless one-pass and two-party authenticated key agreement protocol. The proposed protocol meets all the security requirements that a one one-pass and two-party authenticated key agreement protocol should satisfy. To achieve the standard key-compromise impersonation security, Zhang provided a general idea to convert the proposed protocol to the one with key-compromise impersonation property. However, Zhang may omit some detailed inputs in the description of the extended certificateless one-pass and two-party authenticated key agreement protocol. We show that the extended protocol achieves the standard key-compromise impersonation security if and only if some public inputs are well included.

***Keywords*:** Authenticated key agreement protocol, Certificateless public key cryptography, One-pass, Key-compromise impersonation, Bilinear pairing

1. Introduction

Key agreement protocol is a basic cryptographic primitive for building secure communication channels over the insecure public networks. It allows two or more users to securely set up a shared secret key for their communications in the present of an adversary. Key agreement protocols are usually implemented over public key cryptography (PKC). The first practical key agreement solution is the well-known Diffle-Hellman protocol [3]. However, the Diffle-Hellman protocol suffers from the man-in-the-middle attack because it does not provide authentication to the participants. This kind of key agreement protocols are only secure against the passive adversaries. In the real world, the adversary may mount more powerful attacks such as by impersonating one party to communicate with another party. Hence, the research in this field has been concentrating on the authenticated key agreement (AKA) protocols that can provide authentication to the participants. Over the years, numerous AKA protocols have been proposed over traditional PKC or identity-based cryptography (IBC), *e.g.* [2, 4, 6, 8, 9, 10, 12].

To eliminate the key escrow problem in IBC while retaining the implicit authentication property, Al-Riyami and Paterson [1] introduced the notion of certificateless public key cryptography (CL-PKC) in Asiacrypt 2003. In CL-PKC, a user's private key is generated by combining a partial private key from a partially trusted authority named key generation center (KGC) with a secret value selected by the user himself. In this way, KGC does not know any user's private key. Therefore, CL-PKC solves the key escrow problem inherent in IBC. In addition, CL-PKC provides an effective implicit authentication mechanism so that a user does not need to obtain a certificate from the certificate authority for the authenticity of his public key. Since its advent, CL-PKC has aroused great interest in the research community and many certificateless AKA protocols have been presented [7,11,13,14].

In a one-pass and two-party AKA protocol, only one participant is required to send information to the other during the protocol. Thus, the one-pass and two-party AKA protocols are more efficient than the common two-party AKA protocols in terms of communication overhead. Recently, Zhang [15] proposed an efficient one-pass and two-party AKA protocol in the setting of CL-PKC and proved it to achieve all the security requirements that a one-pass and two-party AKA protocol should satisfy. Considering that the proposed protocol only satisfies the weak sender's key compromise impersonation security attribute, Zhang [15] further proposed a general idea to convert the proposed certificateless one-pass and two-party AKA protocol to the one with the standard key-compromise impersonation property. However, Zhang described the extended protocol at a high level and may omit some detailed