An Efficient Signcryption Scheme with Key Privacy

Chung Ki Li[1], Guomin Yang[1], Duncan S. Wong[1,⋆], Xiaotie Deng[1], and Sherman S.M. Chow[2]

[1] Department of Computer Science
City University of Hong Kong
Hong Kong, China
{travisli,csyanggm,duncan,deng}@cs.cityu.edu.hk
[2] Department of Computer Science
Courant Institute of Mathematical Sciences
New York University, NY 10012, USA
schow@cs.nyu.edu

Abstract. In Information Processing Letters 2006, Tan pointed out that the anonymous signcryption scheme proposed by Yang, Wong and Deng (YWD) in ISC 2005 provides neither confidentality nor anonymity. However, no discussion has been made on whether YWD scheme can be made secure. In this paper, we propose a modification of YWD scheme which resolves the security issues of the original scheme without sacrificing its high efficiency and simple design. Indeed, we show that our scheme achieves confidentiality, existential unforgeability and anonymity with more precise reduction bounds. In addition, our scheme further improves the efficiency when compared with YWD, with reduced number of operations for both signcryption and de-signcryption.

Keywords: Signcryption, Key Privacy, Ciphertext Anonymity, Gap Diffie-Hellman.

1 Introduction

Signcryption, introduced by Zheng in 1997 [24], is a cryptographic primitive targeting to provide unforgeability and confidentiality simultaneously as typical signature-then-encryption technique does but with less computational complexity and lower communication cost. Due to these advantages, signcryption is suitable for many applications which require secure and authenticated message delivery using resource limited devices.

There have been many signcryption schemes proposed after Zheng's publication (e.g. [2,11,16,19,23,9,10,15,13,14]). In 2002, Baek *et al.* [3] first formally defined the security notions of signcryption, which are similar to the traditional semantic security against adaptive chosen ciphertext attack (IND-CCA2) [17]

⋆ The author was supported by a grant from CityU (Project No. 7001959).

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 78–93, 2007.

and existential unforgeability against adaptive chosen message attack (EUF-CMA) [12]. The notion of *insider security*[1] was first defined by An *et al.* [1]. The notion allows an adversary to not only access the public keys of both sender and receiver but does also know the sender's private key. For example, a signcryption scheme is said to be 'insider secure' if the adversary cannot compromise the confidentiality of a ciphertext even the adversary knows the sender's private key. Similar notion has later been extended to other security properties for signcryption [9,13,14]. Those properties include unforgeability, anonymity, etc.

In [9], Boyen proposed a new set of security models for signcryption schemes (under the identity-based setting [18]). In particular, a new requirement called *ciphertext anonymity* was proposed. It requires that a ciphertext should appear anonymous to anyone but the actual recipient. It hides the identities of both the sender and the recipient of the ciphertext. This notion can be viewed as an extension of *key privacy* introduced by Bellare et al. [4] for public key encryption. A signcryption scheme with ciphertext anonymity or key privacy, the identities of both sender and recipient are protected from being known from a ciphertext.

In [14], Libert and Quisquater proposed a signcryption scheme with ciphertext anonymity. However, [20] and [22] independently demonstrated that it is neither semantically secure nor anonymous under chosen plaintext attack. In [22], Yang, Wong and Deng also proposed an improvement (hereinafter referred as the YWD scheme) based on [14]. YWD scheme has a special merit on efficiency as it is computationally efficient and supports parallel processing which may help improving the performance further. However, a recent result by Tan [21] showed that the YWD scheme is not semantically secure and does not satisfy ciphertext anonymity, under insider's chosen-ciphertext attack. However, no improved scheme was proposed by Tan.

Our Contribution. It is still not known if the YWD scheme can be improved to a secure one, while maintaining the advantages of the original scheme being highly efficient and simple. In this paper, we propose a modification of the YWD scheme. The modified scheme not only solves the security issues of the original scheme, but also maintains its efficiency. In particular, we show that our scheme achieves confidentiality, existential unforgeability and anonymity with more precise reduction bounds. In addition, our scheme further improves the efficiency with reduced number of operations for both signcryption and de-signcryption.

Organization. We give the definition and security models of a signcryption scheme with ciphertext anonymity (or key privacy) in Sec. 2. It is then followed by the review and discussion of YWD signcryption scheme and Tan's attacks in Sec. 3. This leads us to the description of our method for solving the security issues of the YWD scheme. Our construction and its security analysis are given in Sec. 4. We conclude the paper in Sec. 5.

[1] The original paper of An, *et al.* [1] only presents the insider attack against the integrity of a signcryption. The idea has later been extended to confidentiality and other security properties [9,14].