Efficient Signcryption Without Random Oracles*

Qianhong Wu[1], Yi Mu[1], Willy Susilo[1], and Fangguo Zhang[2]

[1] Center for Information Security Research
School of Information Technology and Computer Science
University of Wollongong, Wollongong NSW 2522, Australia
{qhw, wsusilo, ymu}@uow.edu.au
[2] Department of Electronics and Communication Engineering
Sun Yat-sen University, Guangzhou 510275, P.R. China
isszhfg@mail.sysu.edu.cn

Abstract. Signcryption is an asymmetric cryptographic method that simultaneously provides confidentiality and authenticity at a lower computational and communication overhead. A number of signcryption schemes have been proposed in the literature, but they are only proven to be secure in the random oracle model. In this paper, under rational computational assumptions, we propose a signcryption scheme from pairings that is proven secure *without* random oracles. The scheme is also efficient and comparable to the state-of-the-art signcryption schemes from pairings that is secure in the random oracle model.

1 Introduction

One of the most important applications of cryptography is to build a trusted computing environment by providing confidentiality and authenticity. Usually, these properties are achieved by independent cryptographic primitives such as public key encryption and signature. However, in many applications, both security services are required. A simple combination is usually an inefficient solution. Moveover, such a simple combination may potentially be insecure.

To address such issues, a separate primitive, named signcryption, has been introduced by Zheng in [19]. The original motivation is to achieve a tailored, more efficient solution than a simple composition. Most of these initial work on signcryption are lacking of formal definition and analysis. In [1,9], the formal definitions of signcryption were independently presented. Subsequently, a number of signcryption schemes (e.g. [7,15,11,16,17]) have been proven secure in the random oracle models introduced in [8].

Although the random oracle methodology leads to the construction of efficient and provably secure schemes, it has received a lot of criticism, that the proofs in the random oracle model are *not* proofs. They are simply a design validation methodology capable of spotting defective or erroneous designs when they fail

* This work is supported by ARC Discovery Grant DP0557493 and the National Natural Science Foundation of China (No. 60403007).

L.T. Yang et al. (Eds.): ATC 2006, LNCS 4158, pp. 449–458, 2006.

[2,3,10,13]. Hence, due to the importance of signcryption, it is essential to have signcryption schemes that are secure in the standard model.

We also note that it is possible to construct a signcryption scheme in the standard model by combining signature schemes with the Cramer-Shoup encryption schemes [12] by using one of the suitable generic composition methods considered by An, Dodis and Rabin in [1]. In fact, another generic construction suggested by Malone-Lee [14] does not make use of random oracles. However, such generic constructions mainly concentrate on a secure combination of encryptions and signatures and hence, such generic constructions are usually not more efficient than a simple combination of the underlying signature and encryption schemes.

Following the original work due to Zheng's signcryption scheme [19], we investigate special effort into designing a more efficient solution than a mere composition of signature and encryption. The main contribution of this paper is an efficient signcryption scheme from pairings. Our construction is based on variants of the Boneh-Boyen signature [4] and the ElGamal encryption. Under the q-Strong Diffie-Hellman (q-SDH) assumption and a candidate Double Decision Diffie-Hellman (DDDH) assumption, the confidentiality and authenticity of the signcryption scheme are proven *without* using random oracles. For performance evaluation, compared to the underlying original ElGamal cryptosystem, the scheme requires only 2 more modular exponentiations in the sender side and 3 more modular exponentiations plus a pairing computation in the receiver side. The ciphertext is about 2 times of that of the original ElGamal cryptosystem. The performance is comparable to the state-of-the-art signcryption scheme from pairings in the random oracle model.

2 Security Definitions

We review the security definitions of signcryption in [1] with a slight extension. In [1], the user's key to produce signature can also be used to receive and decrypt ciphertext. In the following, we distinguish the key to signcrypt messages from the key to de-signcrypt ciphertext.

Definition 1. *A signcryption scheme $\mathcal{SC}$ consists of four algorithms: $\mathcal{SC} = (\mathtt{Gen}_S(\cdot), \mathtt{Gen}_R(\cdot), \mathtt{SigEnc}(\cdot), \mathtt{VerDec}(\cdot))$:*

- $(SK_S, PK_S) \leftarrow \mathtt{Gen}_S(1^\lambda)$ *is a polynomially probabilistic time (PPT) algorithm which, on input a security parameter λ, outputs the sender's private/public key pair (SK_S, PK_S).*
- $(SK_R, PK_R) \leftarrow \mathtt{Gen}_R(1^\lambda)$ *is PPT algorithm which, on input a security parameter λ, outputs the receiver's private/public key pair (SK_R, PK_R).*
- $\sigma \leftarrow \mathtt{SigEnc}(m, SK_S, PK_R)$ *is a PPT algorithm which, on input a message m from the associated message space M, the sender's private key SK_S and the receiver's public key PK_R, outputs a signcryption ciphertext σ.*
- $m/\perp \leftarrow \mathtt{VerDec}(\sigma, SK_R, PK_S)$ *is a polynomial-time deterministic algorithm which, on input a signcryption ciphertext σ, the receiver's private key SK_R and the sender's public key PK_S, outputs $m \in M$ or $\perp$, where $\perp$ indicates that the message was not encrypted or signed properly.*