# Universally Composable Signcryption

Kristian Gjøsteen and Lillian Kråkmo

Dept. of Mathematical Sciences, NTNU

**Abstract.** One of the challenges within public-key based cryptosystems is providing the user with a convenient interface, while retaining security. In the universal composability framework, we propose an ideal functionality for secure messaging, with a user-friendly interface. We also propose an ideal functionality for signcryption, and we show that, given a public key infrastructure and a secure signcryption protocol, we can construct a protocol that securely realizes the secure messaging functionality. Moreover, we show that a signcryption protocol realizes the signcryption functionality if and only if the corresponding signcryption scheme is secure.

**Keywords:** Secure messaging, universal composability, signcryption.

## 1 Introduction

Signcryption was first proposed by Zheng [7] as a primitive for achieving both confidentiality and authenticity of message delivery/storage in a logically single step, with the aim of reducing the cost compared to the standard "sign-then-encrypt" method. Regarding security definitions for signcryption schemes, several approaches have been taken. An overview of the different models is provided in [5].

In general, composing several (possibly identical) protocols into a larger protocol may not preserve security. Universally composable security is a framework proposed by Canetti [3] as a way to define security for protocols such that security-preserving composition is possible. This allows for a modular design and analysis of protocols.

For each cryptographic task, an *ideal functionality* can be defined, which incorporates the required properties of a protocol for the task and the allowed actions of an adversary. A protocol is said to *securely realize* the ideal functionality if, loosely speaking, any effect caused by an adversary attacking the protocol can be obtained by an adversary attacking the ideal functionality. When designing complex protocols, one can allow the involved parties to have secure access to ideal functionalities. Then, when implementing the protocol, each ideal functionality is replaced by a protocol securely realizing the functionality. The *composition theorem* then guarantees security. We refer to [3] for a complete overview of this framework.

In Sect. 2 of this paper, we review the properties of a signcryption scheme and define what it means for a signcryption scheme to be secure. Based on these security requirements, we construct an ideal functionality for signcryption, which

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 346–353, 2007.

is defined in Sect. 3. This section also presents a natural ideal functionality for secure messaging, which is a suitable model for applications such as secure email and secure instant messaging. Given functionalities for public key infrastructure and signcryption, we construct a protocol that integrates these services and securely realizes the secure messaging functionality.

Finally, in Sect. 4 we claim that a signcryption scheme satisfies our security definitions if and only if the corresponding protocol securely realizes the signcryption functionality. We note that our results are only valid in the static corruption case. This is discussed further in Sect. 5.

Proofs are omitted due to space limitations, but will appear in the full version of this paper.

## 2 Signcryption

Our definition of a signcryption scheme is identical to the one given in [5].

**Definition 1.** *A signcryption scheme $\mathcal{SC}$ is a 5-tuple of algorithms $(\mathcal{C}, \mathcal{K}_s, \mathcal{K}_r, \mathcal{S}, \mathcal{U})$ with the following properties:*

- *$\mathcal{C}$ is a probabilistic algorithm, taking as input a security parameter $\tau$ (encoded as $1^\tau$) and returning the global information $I$ needed by users of the scheme.*
- *$\mathcal{K}_s$ is a probabilistic algorithm, taking as input the global information $I$ and returning a pair $(sk^s, pk^s)$ of secret and public keys for the sender.*
- *$\mathcal{K}_r$ is a probabilistic algorithm, taking as input the global information $I$ and returning a pair $(sk^r, pk^r)$ of secret and public keys for the receiver.*
- *$\mathcal{S}$, the signcryption algorithm, is probabilistic. Its inputs are a sender's private key $sk^s$, a receiver's public key $pk^r$ and a plaintext $m$, and its output is a ciphertext $c$.*
- *$\mathcal{U}$, the unsigncryption algorithm, is deterministic. Its inputs are a sender's public key $pk^s$, a receiver's secret key $sk^r$ and a ciphertext $c$. Its output is a plaintext $m$ or the symbol $\perp$, indicating that the signcryption is invalid.*

*It is required that $\mathcal{U}(pk^s, sk^r, \mathcal{S}(sk^s, pk^r, m)) = m$ for all plaintexts $m$ and all key pairs $(sk^s, pk^s)$ and $(sk^r, pk^r)$ output by $\mathcal{K}_s$ and $\mathcal{K}_r$.*

Our security model for signcryption schemes is similar to the ADR model presented in [5]. Since non-repudiation is not always required, we do not consider it here due to space constraints. Therefore we need only consider unforgeability between honest users. We need two experiments described in Fig. 1.

The first experiment $\mathbf{Exp}^{\text{ind-cca2}}_{\mathcal{SC},A}$ concerns privacy of messages, and adapts the notion IND-CCA2 from public-key encryption. In the beginning of the experiment, the adversary $A$ is given two public keys $pk^s$ and $pk^r$ belonging to the target sender and the target receiver, respectively. $A$ is composed of a *find*-stage algorithm $A_1$ and a *guess*-stage algorithm $A_2$. $A_1$ finds two messages $m_0$ and $m_1$ of the same length, while $A_2$ is given a challenge ciphertext $c$ and guesses whether $c$ is a signcryption of $m_0$ or $m_1$.