Theoretical Computer Science 618 (2016) 1–20

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

A reduction of security notions in designated confirmer signatures

Yingjie Xia [a], Xuejiao Liu [b], Fubiao Xia [c,*], Guilin Wang [d]

[a] College of Computer Science and Technology, Zhejiang University, Hangzhou, China
[b] Institute of Service Engineering, Hangzhou Normal University, Hangzhou, China
[c] Philips Research Asia, Shanghai, China
[d] Huawei International Pte Ltd, Singapore

ARTICLE INFO

Article history:
Received 18 April 2014
Received in revised form 2 December 2015
Accepted 16 December 2015
Available online 29 December 2015
Communicated by X. Deng

Keywords:
Designated confirmer signature
Security reduction
Fully verification

ABSTRACT

Since the invention of designated confirmer signatures (DCS), a number of schemes with various properties and different underlying mathematical problems have been developed. Although a considerable amount of work has been dedicated to the design of DCS schemes, the confusions of the security notions in the existing DCS models have not been formally discussed and clarified to achieve a proper level of confirmer's security. In order to achieve provable security, we propose a reduced security model and prove that a DCS cryptosystem only requires transcript-simulatability or alternatively invisibility plus non-transferability from a modelling perspective. Accompanied by the reduced DCS model, a generic DCS scheme is also constructed that still retains the feature of full verification, i.e., either the signer or the confirmer can interactively verify arbitrary signatures by providing a convincing proof. Our proposed scheme employs a computationally binding commitment scheme, together with an IND-CCA2 secure public encryption scheme, to achieve a provable security in the standard model. Meanwhile, we present an efficient concrete instantiation by using BLS signatures, CS-Paillier encryption scheme with labels, and Perdesen commitment scheme.

1. Introduction

Digital signatures are one of the most significant achievements of public-key cryptography and constitute a fundamental tool to ensure data authentication. However, the public verifiability of digital signatures may have undesirable consequences when manipulating sensitive and private information. Undeniable signatures, whose verification requires the cooperation of the signer in an interactive way, were invented due to that considerations.

However, in many practical applications, if the signer becomes unavailable, or refuses to cooperate, the recipient cannot make use of the signature. Due to this reason, **designated confirmer signatures** (DCS) are introduced by Chaum and van Antwerpen [1] to overcome this weakness, as an extension of undeniable signatures. In a designated confirmer signature scheme, the signer is still able to interactively verify the signature with the verifier. However, if the signer is unavailable, a semi-trusted third party called the designated confirmer can also confirm the (in)validity of an alleged signature by running some interactive protocols with the verifier. In general, such a verifier cannot transfer the signature's (in)validity

* Corresponding author.
E-mail address: xiafb@hotmail.com (F. Xia).

http://dx.doi.org/10.1016/j.tcs.2015.12.025
0304-3975/

to other parties by convincing them of the same fact. Furthermore, the designated confirmer can selectively convert a designated confirmer signature into a standard signature, so that it becomes a publicly verifiable signature.

Since the invention of designated confirmer signatures, a number of schemes with various properties and different underlying mathematical problems have been developed. Although a considerable amount of work has been dedicated to the design of DCS schemes, the confusions of the security notions in the existing DCS models have not been formally discussed and clarified to achieve a proper level of security.

In this paper, we prove that to get provable security, a DCS cryptosystem only requires transcript-simulatability or alternatively invisibility plus non-transferability. In other words, the security model proposed by Camenisch and Michels [2] and the security model proposed by Gentry et al. [3] are equivalent under a practical assumption. Also, we prove that unimpersonation is implied by invisibility, which concludes that Goldwasser and Waisbard's security model [4] is weaker than Camenisch and Michels' security model [2].

Then, we propose a generic DCS scheme that achieve the reduced security notion and still supports full verification, i.e., either the signer or the confirmer can interactively verify arbitrary signatures by providing a convincing proof. The main idea of our construction is, to issue a DCS, the targeted message is initially sealed in a commitment φ. Then the randomness r used to open the commitment is doubly encrypted, that is, two ciphertexts say c_1 and c_2 will be generated as part of the DCS which are the encryptions on the randomness with regard to the signer or the confirmer's public key. The final output DCS is a combination of φ, c_1, c_2 and σ, where σ is an ordinary signature on φ by using the signing key. To confirm or disavow such a DCS, either the signer or the confirmer can simply decrypts one of the ciphertexts using his private key to get the witness, i.e., the randomness. By checking the correctness of the commitment, the prover can later provides a ZK proof of knowledge for the equality of the randomness existed in the commitment and in the ciphertext.

Organizations. The rest of the paper is organized as follows. In Section 2 we discuss related work. We introduce the basic knowledge of bilinear maps in Section 3, together with two cryptographic primitives which are used to construct our generic scheme. A reduced security model of DCS is presented in Section 4, including unforgeability, invisibility and non-transferability-1. Then we give a formal discussion of the reduced security notions in Section 5. Later we propose a generic DCS based on the reduced model in Section 6. We show how to efficiently instantiate the proposed scheme by choosing specific building blocks in Section 7. Section 8 concludes our work of this paper.

2. Related works

Designated confirmer signatures (DCS) are introduced by Chaum and van Antwerpen [1] as an extension of undeniable signature. More specifically, in a designated confirmer signature scheme, if the signer is unavailable, a semi-trusted third party called *the designated confirmer* can confirm the (in)validity of an alleged signature by running some interactive protocols with a verifier. However, such a verifier cannot transfer the signature's (in)validity to other parties by convincing them of the same fact. Furthermore, the designated confirmer can selectively convert a designated confirmer signature into a standard signature so that it can be publicly verifiable. A number of related work have been presented in the last two decades, like [4,2,5,6,3,7,8], though most of them are either insecure or inefficient. For example, Michels and Stadler [6] identify attacks against the two concrete DCS scheme proposed in [5], Camenisch and Michels [2] show the insecurity of [6], Wang et al. [7] point out security flaws in the schemes proposed by [4,3], while the solutions given in [2,8] are not efficient as they rely on general zero-knowledge protocols.

Apart from unforgeability which is a common security requirement for variants of digital signatures, the unique security property of a DCS scheme is called *invisibility* [2], which requires that any probabilistic polynomial adversary *cannot* feasibly determine the (in)validity of an alleged signature against adaptive attacking environment.

Since the introduction by Chaum and van Antwerpen [1], various generic DCS schemes have been produced from ordinary digital signatures and other cryptographic primitives such as public key encryptions, commitment schemes, and/or zero-knowledge protocols. We briefly review the most important attempts in chronological order:

- Chaum and van Antwerpen (1994) [1]: The first proposition of designated confirmer signatures to solve the weakness of undeniable signatures, with an example of DCS based on RSA scheme.
- Okamoto (1994) [5]: Okamoto gave the first formal definition of designated confirmer signatures in the sense of rigorous concept, and proposed a practical construction by using digital signatures, public key encryptions, bit-commitment schemes and pseudo-random functions. Also it novelly shows that the existence of public-key encryption is the necessary and sufficient assumption for constructing designated confirmer signatures.
- Michels and Stadler (1998) [6]: They pointed out a certain weakness of the DCS schemes by Okamoto [5] that the confirmer can forge a valid signature on behalf of the signer. Realizing this problem, they further proposed a new security model and introduced an efficient DCS scheme in that model by using signatures with the Fiat–Shamir paradigm and commitment schemes.
- Camenisch and Michels (2000) [2]: The authors identified an attack against the DCS schemes proposed in [1,5,6], where the validity of a DCS issued by a signer S can be linked to that of a DCS issued by another signer S'. As a result, those schemes are insecure if multiple signers share the same confirmer, and such multi-signer settings seem to be natural in e-commerce applications. Based on that observation, they proposed a new security model to cover this variant of