Computers and Electrical Engineering 38 (2012) 1647–1657

Contents lists available at SciVerse ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Efficient ID-based non-malleable trapdoor commitment ☆

Chunhui Wu [a,*], Xiaofeng Chen [b], Qin Li [c], Dongyang Long [d]

[a] Department of Computer Science, Guangdong University of Finance, Guangzhou 510521, PR China
[b] State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, PR China
[c] College of Information Engineering, Xiangtan University, Xiangtan 411105, PR China
[d] Department of Computer Science, Sun Yat-sen University, Guangzhou 510275, PR China

ARTICLE INFO

Article history:
Received 13 November 2010
Received in revised form 26 June 2012
Accepted 26 June 2012
Available online 21 July 2012

ABSTRACT

Non-malleability is an important property in commitment schemes, which can resist to the person-in-the-middle (PIM) attacks within the interaction. In this paper, we focus on the non-malleability of ID-based trapdoor commitment. We first point out some weakness of the definition for Fischlin's ID-based trapdoor commitments, which we call the *partial* ID-based trapdoor commitments. Moreover, we present the formal definition for the *full* ID-based trapdoor commitment and give a concrete construction based on the computational Diffie–Hellman (CDH) assumption. Finally, we use the idea of multi-trapdoor commitments and the technique of non-malleability to propose two efficient interactive full ID-based non-malleable trapdoor commitments in discrete logarithm (DL) system, with/without random oracle respectively.

1. Introduction

A commitment scheme is an interactive protocol between two parties, the sender $\mathcal{S}$ holding a message, and the receiver $\mathcal{R}$. It can be divided into two phases as the commitment phase and opening phase. In the commitment phase, the sender gives some jumbled information about the message to the receiver such that, on one hand, even a malicious receiver $\mathcal{R}^*$ cannot gain any information about the message (hiding), and on the other hand, a malicious sender $\mathcal{S}^*$ cannot ambiguously open a commitment given to $\mathcal{R}$ (binding). In the opening phase, the sender transmit the original message and some evidence that the commitment really jumbles this message. Due to the computation power of the adversary, the two properties of binding and hiding can either be perfect (statistical) or computational ones. However, a commitment scheme cannot be perfect (statistical) hiding and perfect (statistical) binding at the same time [1]. Therefore, we mainly consider the commitment schemes of perfect (statistical) hiding (resp., binding) and computational binding (resp., hiding). Loosely speaking, a commitment scheme is perfect (statistical) hiding and computational binding if the distribution of the commitments of any message are identical (statistical close) for any arbitrary powerful malicious $\mathcal{R}^*$, and opening a valid commitment ambiguously contradicts the hardness of some cryptographic assumption. A commitment scheme is perfect (statistical) binding and computational hiding if a valid commitment can be opened ambiguously with probability zero (negligible) for any arbitrary powerful malicious $\mathcal{S}^*$, and two commitments are computationally indistinguishable for any probably polynomial time (PPT) malicious $\mathcal{R}^*$.

Trapdoor commitment is a commitment scheme with special properties, that is, one with the trapdoor key can open his commitment in different ways. Trapdoor commitment is also called equivocable commitment or chameleon commitment. It has many applications in modern cryptography. One important application is in constructing zero-knowledge proof [2],

☆ Reviews processed and approved for publication by Editor-in-Chief Dr. Manu Malek.

* Corresponding author. Tel.: +86 02037216133.
E-mail address: chunhuiwu@163.com (C. Wu).

0045-7906/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compeleceng.2012.06.013

constant-round zero-knowledge [3–5] in which the prover and verifier exchange only a constant number of messages, concurrent zero-knowledge [6,7] where the verifier talks to several instances of the prover in parallel, and resettable zero-knowledge [8] where the verifier is even allowed to reset the prover to some previous step of the protocol. Additionally, trapdoor commitments play an important role for the construction of secure signature schemes such as chameleon signatures [9–13], and on-line/off-line signatures [14–16].

Shamir [17] firstly introduced the notion of ID-based cryptosystem, where a trusted authority, called the private key generation center (PKG), is responsible for the generation of private key for the user. Private key generation, also known as Extract(·) algorithm, applies the PKG's master secret key *MSK* to the user's identity. For security, the adversary is allowed to query the Extract(·) oracle polynomial many times on inputting id_i, and obtain the corresponding secret keys sk_{id_i}, while keeping *MSK* secret. However, in the definitions of ID-based trapdoor commitment [1], the public parameters are generated w.r.t. a specific identity and compromise of two users will expose the *MSK* and thus break the binding property for other users. So, it cannot satisfy the requirement of ID-based cryptosystem and we call it the *partial* ID-based trapdoor commitment.

The concept of non-malleability was introduced by Dolev et al. [18]. They also presented a non-malleable public-key encryption scheme (based on any trapdoor permutation) and a non-malleable commitment scheme with logarithmically many rounds based on any one-way function. Nevertheless, their solutions involve cumbersome non-interactive or interactive zero-knowledge proofs. Di Crescenzo et al. [19] presented a non-interactive and non-malleable commitment scheme based on any one-way function in the common random string model. Though being non-interactive, their construction is rather theoretical as it excessively applies an ordinary commitment scheme to non-malleably commit to a single bit. Fischlin and Fischlin [20,21] presented efficient interactive non-malleable commitment schemes based on standard assumptions (such as DL and RSA assumptions) in the common reference string model.

1.1. Our contribution

In this paper, we focus on the ID-based non-malleable trapdoor commitment. Our contributions are two folds:

(1) We point out the weakness of the definitions for Fischlin's ID-based trapdoor commitment [1], and then introduce the notion of (*full*) ID-based trapdoor commitment. We also give a concrete construction based on the CDH assumption.
(2) We propose the first two constructions of efficient interactive ID-based non-malleable trapdoor commitments, with/without random oracle respectively.

1.2. Organization

The rest of the paper is organized as follows: We give some preliminaries in Section 2. In Section 3, we introduce the notion of *full* ID-based trapdoor commitment and then give a concrete construction based on the CDH assumption. In Section 4, we extend the scheme to a non-malleable one and prove its security in the random oracle model. We also propose a new commitment scheme without the random oracles in Section 5. Finally, we conclude in Section 6.

2. Preliminaries

In this section, we first introduce some well-known number-theoretic problems in the discrete logarithm systems. We also give some notations related to commitment schemes.

2.1. Number-theoretic problems

Let $\mathbb{G}$ be a cyclic multiplicative group generated by g with prime order q. We introduce the following problems in $\mathbb{G}$.

- Discrete Logarithm Problem (DLP): Given two elements g and h, to find an integer $a \in \mathbb{Z}_q^*$, s.t. $h = g^a$.
- Computation Diffie–Hellman Problem (CDHP): Given (g, g^a, g^b) for $a, b \in \mathbb{Z}_q^*$, to compute g^{ab}.
- l-Strong Diffie–Hellman Problem (l-SDHP): Given $(g, g^a, g^{a^2}, \cdots, g^{a^l})$ for $a \in \mathbb{Z}_q^*$, to compute (e, h), $e \in \mathbb{Z}_q$, $h \in \mathbb{G}$, s.t. $h^{e+a} = g$.
- Decision Diffie–Hellman Problem (DDHP): Given (g, g^a, g^b, g^c) for $a, b, c \in \mathbb{Z}_q^*$, to decide whether $c = ab \bmod q$.

It is proved that the CDHP and DDHP are not equivalent in the GDH groups. More precisely, we call $\mathbb{G}$ a GDH group if the DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve the CDHP with non-negligible probability. Such groups can be found in supersingular elliptic curves or hyper elliptic curves over finite fields. Moreover, we call $\langle g, g^a, g^b, g^c \rangle$ a valid Diffie–Hellman tuple if $c = ab \bmod q$.

2.2. Interactive protocols and commitment schemes

We follow the notations in [1] to describe interactive protocols and commitment schemes.