Computers and Electrical Engineering 37 (2011) 614–623

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Discrete logarithm based chameleon hashing and signatures without key exposure ☆

Xiaofeng Chen [a,*], Fangguo Zhang [b], Haibo Tian [b], Baodian Wei [b], Kwangjo Kim [c]

[a] *Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University, Xi'an 710071, PR China*
[b] *School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510275, PR China*
[c] *Computer Science Department, KAIST, Taejon 305-714, South Korea*

ARTICLE INFO

Article history:
Received 8 April 2010
Received in revised form 18 March 2011
Accepted 28 March 2011
Available online 6 May 2011

ABSTRACT

Chameleon signatures simultaneously provide the properties of non-repudiation and non-transferability for the signed message. However, the initial constructions of chameleon signatures suffer from the key exposure problem of chameleon hashing. This creates a strong disincentive for the recipient to compute hash collisions, partially undermining the concept of non-transferability. Recently, some constructions of discrete logarithm based chameleon hashing and signatures without key exposure are presented, while in the setting of gap Diffie–Hellman groups with pairings.

In this paper, we propose the first key-exposure free chameleon hash and signature scheme based on discrete logarithm systems, without using the gap Diffie–Hellman groups. This provides more flexible constructions of efficient key-exposure free chameleon hash and signature schemes. Moreover, one distinguishing advantage of the resulting chameleon signature scheme is that the property of "message hiding" or "message recovery" can be achieved freely by the signer, i.e., the signer can efficiently prove which message was the original one if he desires.

1. Introduction

Chameleon signatures, introduced by Krawczyk and Rabin [1], are based on well established hash-and-sign paradigm, where a chameleon hash function is used to compute the cryptographic message digest. A chameleon hash function is a trapdoor one-way hash function, which prevents everyone except the holder of the trapdoor information from computing the collisions for a randomly given input. Chameleon signatures simultaneously provide non-repudiation and non-transferability for the signed message as undeniable signatures [2–6] do, but the former allows for simpler and more efficient realization than the latter. In particular, chameleon signatures are non-interactive and less complicated. More precisely, the signer can generate the chameleon signature without interacting with the designated recipient, and the recipient will be able to verify the signature without the collaboration of the signer. On the other hand, if presented with a forged signature, the signer can deny its validity by only revealing some certain values. That is, the forged-signature denial protocol is also non-interactive. Besides, since the chameleon signatures are based on well established hash-and-sign paradigm, it provides more generic and flexible constructions.

One limitation of the original chameleon signature scheme is that signature forgery (i.e., collision computation) results in the signer recovering the recipient's trapdoor information, i.e., the private key [7]. The signer then can use this information to deny other signatures given to the recipient. In the worst case, the signer could collaborate with other individuals to

☆ Reviews processed and approved for publication by Editor-in-Chief Dr. Manu Malek.
* Corresponding author.
E-mail address: xfchen@xidian.edu.cn (X. Chen).

0045-7906/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2011.03.011

invalidate any signatures which were designated to be verified by the same public key. This will create a strong disincentive for the recipient to compute the hash collisions and thus weakens the property of non-transferability.

Ateniese and de Medeiros [7] firstly addressed the key exposure problem of chameleon hashing and introduced the idea of identity-based chameleon hashing to solve this problem.[1] Due to the distinguishing property of identity-based system, the signer can sign a message to an intended recipient, without having to first retrieve the recipient's certificate. Moreover, the signer uses a different public key (corresponding a different private key) for each transaction with a recipient, so that signature forgery only results in the signer recovering the trapdoor information associated to a single transaction. Therefore, the signer will not be capable of denying signatures on any message in other transactions. We argue that this idea only provides a partial solution for the problem of key exposure since the recipient's public key is changed for each transaction.[2]

Chen et al. [11] proposed the first full construction of a key-exposure free chameleon hash function in the gap Diffie–Hellman (GDH) groups with bilinear pairings. Ateniese and de Medeiros [12] then presented three key-exposure free chameleon hash schemes, two based on the RSA assumption (the first constructions without using pairings), as well as a new construction based on pairings. Recently, Gao et al. [13] claimed to present a key-exposure free chameleon hash scheme based on the Schnorr signature. However, this scheme requires an interactive protocol between the signer and the recipient and thus does not meet the basic definition of chameleon hashing and signatures.

All of the existing discrete logarithm based chameleon hash schemes without key exposure [11,12] can only be constructed in the setting of GDH groups with pairings. Are there efficient (discrete-logarithm-based) constructions for key-exposure free chameleon hashing without using the GDH groups? To the best of our knowledge, there is no research work on this problem in the open literature.

Our contribution. In this paper, we propose two efficient constructions for discrete logarithm based chameleon hash schemes without key exposure. Our contribution is two folds:

(1) We proposed a new key-exposure free chameleon hash scheme in the GDH groups. Compared with the existing schemes in the GDH groups [11,12], the proposed chameleon hash scheme is not only based on the weaker assumption, but also more efficient in both hashing and collision computations.
(2) We propose the first discrete logarithm based key-exposure free chameleon hash scheme without using the GDH groups. One distinguishing advantage of the resulting chameleon signature scheme is that the property of "message hiding" or "message recovery" can be achieved freely by the signer.

Organization. The rest of the paper is organized as follows: Some preliminaries are given in Section 2. The definitions associated with chameleon hashing and signatures are introduced in Section 3. The proposed key exposure freeness chameleon hash and signature schemes in the GDH groups and non-GDH groups are given in Sections 4 and 5, respectively. Finally, conclusions will be made in Section 6.

2. Preliminaries

In this section, we first introduce some well-known number-theoretic problems in the discrete logarithm systems. We then present two proof systems for knowledge of discrete logarithms.

2.1. Number-theoretic problems

Let $\mathbb{G}$ be a cyclic multiplicative group generated by g with the 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 $a \in \mathbb{Z}_q^*$, such that $h = g^a$ whenever such an integer exists.
- Computation Diffie–Hellman problem (CDHP): Given (g, g^a, g^b) for $a, b \in \mathbb{Z}_q^*$, to compute g^{ab}.
- Decision Diffie–Hellman problem (DDHP): Given (g, g^a, g^b, g^c) for $a, b, c \in \mathbb{Z}_q^*$, to decide whether $c \equiv ab \bmod q$.

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 hyperelliptic curves over finite fields. For more details, see [14–16]. Moreover, we call $\langle g, g^a, g^b, g^c \rangle$ a valid Diffie–Hellman tuple if $c \equiv ab \bmod q$.

[1] Shamir and Tauman [8] firstly used the chameleon hash functions to design efficient generic on-line/off-line signature schemes. It also suffers from the key exposure problem of chameleon hashing. Chen et al. [9,10] firstly introduced a special double-trapdoor hash family to solve the problem in the on-line/off-line signatures.

[2] A trivial solution for the key exposure problem is that the signer changes his key pair frequently in the chameleon signature scheme. However, it is only meaningful in theoretical sense because the key distribution problem arises simultaneously.