International Journal of Innovative Computing, Information and Control
Volume **5**, Number **9**, September **2009**

 ISSN 1349-4198
pp. **2829–2836**

CHAMELEON SIGNATURE WITH CONDITIONAL OPEN VERIFICATION

Yu-Fang Chung[1] and Kuo-Hsuan Huang[2]

[1]Department of Electrical Engineering
Tunghai University, Taiwan
yfchung@thu.edu.tw

[2]Department of Computer Science and Engineering
Tatung University, Taiwan
kuohsuan1225@gmail.com

Received January 2008; revised August 2008

Abstract. *Chameleon signature was first proposed by Krawczyk and Rabin. It is based on the well known hash-and-sign paradigm; the chameleon hash function is used to calculate the message digest. The greatest feature of chameleon signature is non-transferability, that is, an unauthorized signature recipient can not verify validity of signatures. The initial chameleon hash scheme has key exposure problem, which is fixed in our proposed chameleon hash scheme. In addition, our proposed chameleon hash scheme is the first chameleon signature scheme that offers conditional open verification. At the time of generation of signature, the signer can specify the conditions under which signature verification can be performed by a third party. Normally, only the specified recipient can verify the signatures. The present chameleon signature loses its non-transferability attribute when it turns into a universally verifiable instance. This paper also attempts to tackle this problem and proposes a solution.*
Keywords: Chameleon hash, Chameleon signature, Non-transferability, Key exposure

1. **Introduction.** The studies on digital signature and its various extended models [1-3] have always been the subject to discuss in the applications of cryptographic techniques. Digital signature provides signed message with capabilities like integration, authentication and non-repudiation. Anyone can use the signer's public key to verify the authenticity of the signature, but sometimes, the signer may need to protect certain interest, and therefore, do not wish their signature to be checked by anyone other than the specified message recipient. Chaum and van Antwerpen [4] first proposed an undeniable signature to solve the above problem. Undeniable signature requires the collaboration of signers during its verification. Therefore, signer can control whether or not the signed message is open to verification by a recipient; this is known as non-transferability. Undeniable Signature and related topics [5-9] have been widely discussed in recent years.

Krawczyk and Rabin [10] proposed a new type of signature scheme called chameleon signature. Chameleon signatures are based on the well established hash-and-sign paradigm, where a chameleon hash function is used to calculate the message digest. A chameleon hash function is a trapdoor collision-resistant hash function. Without the trapdoor information, a chameleon hash function has the same characteristics, like pre-image and collision-resistance, as any cryptographic hash function. However, collisions and second pre-images can be easily computed once the trapdoor is known. Chameleon signature has the characteristics of an undeniable signature, that is, it is non-repudiable and non-transferable. It is, in fact, a variation of undeniable signature. The main difference between undeniable signature and chameleon signature is that undeniable signature interacts