# An efficient non-interactive deniable authentication protocol with anonymous sender protection

Shin-Jia Hwang *
Chien-Hung Chao †
*Department of Computer Science and Information Engineering*
*Tamkang University*
*Tamsui Township, Taipei County, 251*
*Taiwan, R.O.C.*

**Abstract**

Deniable authentication protocols satisfy two basic properties: Deniability and the specifiable receiver properties. However, the deniability also damages the sender right. To protect senders, Hwang and Ma first proposed deniable authentication with anonymous sender protection. The sender's anonymity is also used to protect the sender's privacy. To reduce the computation cost, an efficient deniable authentication protocol is proposed. Our new protocol not only achieves the two properties but also provides the protection of sender and receiver to keep the privacy of the sender and receiver. Though the sent message is forgeable by receivers, but the sender can provide evidence to prove the message was really sent by him/her. Due to the efficient performance, our protocol is more practical than the other protocols in the real world.

***Keywords and phrases :*** *Anonymous, deniable authentication protocol, Non-interactive protocol.*

## 1. Introduction

Deniable authentication protocol is first proposed by Dwork *et al.* [6] in 1998. A deniable authentication protocol should satisfy two basic properties. One is the deniability and another is the receiver specification property. By the deniability, the receiver cannot convince anyone that the received messages are indeed from the senders, even though the receiver is able to authenticate the sender's identity. By the receiver specification property, only the receiver can authenticate the received messages.

*E-mail*: sjhwang@mail.tku.edu.tw
†*E-mail*: 696410082@s96.tku.edu.tw

*Journal of Discrete Mathematical Sciences & Cryptography*
Vol. 13 (2010), No. 3, pp. 219–231