International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **3**, March **2011**

 ISSN 1349-4198
pp. 1499–1510

NEW SECRET KEY TRAITOR TRACING SCHEME WITH DISPUTE SETTLEMENT FROM BILINEAR MAPS

Kuo-Yu Tsai[1], Tzong-Chen Wu[1,2] and Chien-Lung Hsu[1,3]

[1]Taiwan Information Security Center
[2]Department of Information Management
National Taiwan University of Science and Technology
No. 43, Sec. 4, Keelung Rd., Taipei 106, Taiwan
nicklas@twisc.org

[3]Department of Electrical Engineering
Chang Gung University
No. 259, Wen-Hwa 1st Rd., Kwei-Shan, Tao-Yuan 333, Taiwan

Received November 2009; revised May 2010

Abstract. *We propose a new secret key traitor tracing scheme using bilinear maps, in which the size of the enabling-block in a broadcast message is independent of the number of subscribers. The proposed traitor tracing scheme can identify malicious subscribers (also called traitors) from a pirate decoder, which is collusively made by k or fewer traitors. Further, any malicious subscriber cannot falsify an unintended content for framing the broadcast center and cause all other personal keys to be exposed. We also give formal analyses to discuss the security of the proposed scheme in the random oracle model.*
Keywords: Traitor tracing, Dispute settlement, Bilinear map

1. **Introduction.** *Broadcast encryption* [1] is one of the mechanisms to securely tackle the distribution of digital content to a specific set of authorized subscribers [2, 3, 4, 5, 6, 7]. In various well-known practical and useful applications of broadcast encryption, such as pay-per-view or subscription television broadcasts, online database publicly accessible on the Internet, or distribution of multimedia (e.g., files in MP3 or JPEG), a subscriber is in possession of a decoder that allows them to access the broadcast. The roles of a broadcast encryption mechanism can be categorized as a *broadcast center* and a set of *subscribers* each equipped with a *decoder*. Initially, the broadcast center assigns an authorized key, stored in a decoder, for each subscriber. Thereafter, the broadcast center encrypts an intended content with an encryption key and broadcasts the encrypted content. Only the authorized subscribers can reconstruct the encryption key with their authorized keys, and further, they recover the intended content with their encryption keys. Basically, a broadcast message is divided into two parts: an *enabling-block* and a *cipher-block*. The cipher-block is the ciphertext form of an intended content, which is encrypted by using the encryption key. The enabling-block contains the public information that is used by a decoder to reconstruct the encryption key for obtaining the intended content. Upon receiving the broadcast message, each authorized subscriber can use his/her authorized key to reconstruct the encryption key from the enabling-block and then use it to decrypt the cipher-block to obtain the intended content.

Consider such scenario in which some malicious subscribers (so-called *traitors*) may collude to create a pirate decoder with their authorized keys or copy intended content to non-subscribers in the above applications. Traitor tracing [8] is one of the important mechanisms to resist the piracy. Chor *et al.* [8] introduced the concept of a *traitor tracing*