Cryptology ePrint Archive: Report 2011/084

Traitor Tracing against Public Collaboration (Full Version)

Xingwen Zhao and Fangguo Zhang

Abstract: Broadcast encryption provides a convenient method to distribute digital content to subscribers over an insecure broadcast channel. Traitor tracing is needed because some users may give out their decryption keys to construct pirate decoders. There are many traitor tracing schemes based on collusion secure codes and identifiable parent property codes. However, these schemes are subject to public collaboration of traitors, which is presented by Billet and Phan in EUROCRYPT 2009 as an attack against code-based traitor tracing schemes. In this paper, we describe a generic collusion secure codes based scheme secure against such collaboration. Our scheme is motivated by the idea of identity-based encryption with wildcards (WIBE). We regard the collusion secure codeword for each user as his/her identity, and issue private key accordingly. When in broadcasting, we use a special pattern of WIBE, namely all bit positions in the codewords of intended receivers are set as wildcards. When in tracing, we use another special pattern of WIBE, namely all positions are set as wildcards except the tracing position. By using WIBE, each user is issued one decryption key which should be used as a whole and any incomplete part of the key is useless, while in previous codes based schemes each user holds a number of keys that can be used separately for different bit positions in the codeword. Thus our scheme is resistant to public collaboration, since if the decryption key is disclosed as a whole, it will immediately lead to the accusation of the very traitor. Our idea fits well for code based traitor tracing schemes, no matter collusion secure codes or identifiable parent property codes. We provide an instance based on Boneh-Boyen-Goh WIBE scheme, achieving constant private key storage cost for each user. We also present another instance achieving shorter ciphertexts, on the expense of increasing public keys and private keys. Our scheme presents an answer to the problem left open by Billet and Phan.

Category / Keywords: public-key cryptography / Broadcast encryption, traitor tracing, public collaboration.

Publication Info: This is the full version of a paper accepted for publication at ISPEC 2011

Date: received 18 Feb 2011, last revised 3 Mar 2011

Contact author: isszhfg at mail sysu edu cn