Cryptology ePrint Archive: Report 2011/576

Efficient Multicast Key Distribution Using HOWF-based Access Control Structures

Jing Liu, Qiong Huang, Bo Yang

Abstract: Both broadcast encryption (BE) protocols and multicast key distribution (MKD) protocols try to solve the same problem of private group communication. For the first time, we discuss fundamental differences between BE protocols and MKD protocols from multiple perspectives, and reveal subtle connections between them. Both efficient BE protocols and MKD protocols are usually based on some types of access control structures. Compared with the static access control structures employed by BE protocols, those employed by MKD protocols need be updated upon every single change in group membership, and thus are highly dynamic. It has been shown that instantiation of a dynamic access control structure that's based on one-way function (OWF) by using homomorphic one-way function (HOWF) helps improve the efficiency of these update operations. In this paper, we introduce two new HOWF-based access control structures — Bi-Directional Homomorphic One-way Function Chain (BD-HOFC) and Top-down Homomorphic One-way Function Tree (TD-HOFT), and two structure-preserving operations — chain product and tree product. Employing BD-HOFC and chain products, we propose a time-based MKD protocol and a user-based MKD protocol. Both protocols overcome the drawbacks with their corresponding "non-homomorphic" counterpart. We also introduce an operation called tree blinding for a particular type of TD-HOFT called exclusive key tree (EKT). Utilizing tree product and tree blinding operations, we design an MKD protocol called EKT+ that improves the original EKT protocol. We give rigorous security proofs for our protocols in a symbolic security model.

Category / Keywords: applications /

Date: received 25 Oct 2011

Contact author: liujing3 at mail sysu edu cn