© 2013 FIZ Karlsruhe

io-port 05172707

Lee, Deok-Gyu; Lee, Im-Yeong

A study on efficient key distribution and renewal in broadcast encryption.

Laganà, Antonio (ed.) et al., Computational science and its applications — ICCSA 2004. International conference, Assisi, Italy, May 14–17, 2004. Proceedings, Part IV. Berlin: Springer (ISBN 3-540-22060-7/pbk). Lecture Notes in Computer Science 3046, 66-76 (2004).

Summary: The method of broadcast encryption has been applied to the transmission of digital information such as multimedia, software, and paid TV on the open network. In this broadcast encryption method, only previously authorized users can gain access to digital information. When broadcast message is transmitted, authorized users can first decode the session key using the previously given private key and get digital information using this session key. This way, users retrieve a message or a session key using the key transmitted by broadcasters. For their part, broadcasters need to generate and distribute keys. Broadcasters should also carry out efficient key renewal when users subscribe or unsubscribe. This paper introduces how to generate and distribute key efficiently and how key renewal works. The proposal uses two methods: (1) the server generates keys without the consent of users by anticipating users, and; (2) the server and users generate keys by mutual agreement. The advantage of the two proposed methods is that the receiver can decode broadcast message using a secret key. Even if the key is renewed later, the user can efficiently renew using only a single set of information.

doi:10.1007/b98054