

AN EFFICIENT GENERALIZED GROUP-ORIENTED SIGNATURE SCHEME

CHIH-YING CHEN¹, HSIU-FENG LIN² AND CHIN-CHEN CHANG²

¹Department of Communications Engineering

²Department of Information Engineering and Computer Science

Feng Chia University

Taichung 40724, Taiwan

{chihchen; hflin}@fcu.edu.tw; ccc@cs.ccu.edu.tw

Received February 2007; revised June 2007

ABSTRACT. *The concept of universal modulus, meaning that the modulus used by each authorized member of a group is identical, is a significant way to simplify the generation and verification of a group-oriented signature. Since most existing group-oriented signature systems using universal modulus are discrete logarithm based, RSA based solutions become more significant because of its widely spread use. In this paper, based upon a proper set of distributed RSA parameters produced by a key generation center, we first propose an (r, r) threshold signature scheme in which all authorized signers of a group can cooperate to sign a message on behalf of the group with a universal modulus. And the security of the scheme is guaranteed because of the computational infeasibility of factoring the used modulus. A generalized group-oriented signature scheme is subsequently proposed from elaborately modifying the (r, r) threshold signature scheme. Also, the modulus used by each authorized signer is universal and the security can be ensured in the same way.*

Keywords: Group-oriented signature, Threshold signature, Generalized group-oriented signature, Universal modulus

1. Introduction. Since group-oriented communications activities are becoming more and more popular, group-oriented digital signature plays a very important role in internet applications. A group-oriented signature system allows a group to decide its signing policy in such a way that only the authorized members of this group can cooperate to sign a message on behalf of the group. It is sometimes referred as a distributed signature system if all the authorized signers cooperate in a distributed manner [1,4,5,8,9,13,18]. If the set of authorized signers is any sets of t or more signers of this group, it is called a threshold signature scheme. And if the authorized subset can be arbitrarily specified, it is called a generalized signature scheme. In this scheme, the clerk of the group can specify, according to the classified grade of the message and the group signature policy, a certain set of distinct combinations of authorized signers such that the group signature for the message can be produced when and only when all signers in a specified combination work cooperatively.

However, a threshold scheme is not robust enough to realize any group-oriented signature policy in real applications because, implicitly, it assumes that each authorized signer in the group has equal privilege to sign every message [11,12]. Accordingly, a generalized scheme is more significant than a threshold scheme in practical applications of group-oriented signature [11,12]. Nevertheless, so far most of group-oriented signature schemes proposed are threshold schemes [2,5-8,11,12,14,17,19,22,23]; only a few are generalized schemes [2,6,11,12,17].