



Short Paper

An Improved Threshold Scheme Based On Modular Arithmetic

REN-JUNN HWANG AND CHIN-CHEN CHANG⁺

*Department of Computer Science and Information Engineering
Chung Cheng Institute of Technology
Taoyuan, Taiwan 335, R.O.C.*

E-mail: victor@ccit.edu.tw

⁺*Department of Computer Science and Information Engineering
National Chung Cheng University*

Chiayi, Taiwan 621, R.O.C.

E-mail: ccc@cs.ccu.edu.tw

An efficient threshold scheme is proposed in this paper. It overcomes the weakness of Asmuth et al.'s scheme. The (r, n) -threshold scheme proposed below only takes $O(r)$ operations to recover the shared secret while Shamir's scheme takes $O(r \log^2 r)$ operations. We show that our scheme is perfect. Further, we also propose a method to generate a pairwise relatively prime integer set which satisfies the requirements of Asmuth et al.'s and our schemes.

Keywords: Chinese remainder theorem, cryptography, key safeguarding, secret sharing, threshold scheme

1. INTRODUCTION

Threshold schemes are mainly used to keep a secret from being lost, destroyed or modified. They are also called secret sharing schemes or key safeguarding schemes. In 1979, Shamir[7] and Blakley[2] first proposed the threshold scheme independently. An (r, n) -threshold scheme consists of a trust dealer and n participants. The dealer divides the important shared secret into n shadows and distributes them to these n participants. The shadows should be distributed secretly so that no participant knows the shadow given to another participant. The shared secret can only be recovered by any r or more participants while it can not be determined by any $r-1$ or fewer participants. In our society, there are many "real-world" examples of this situation, such as the military, banks and high technology companies.

Definition: An (r, n) -threshold scheme is perfect if the conditional entropy of a shared secret is

Received December 27, 1996; accepted November 13, 1997.
Communicated by Jhing-Fa Wang.