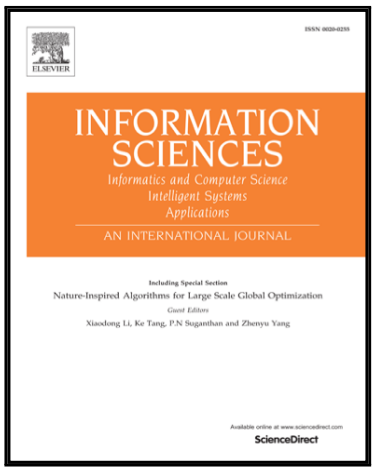

A New Threshold Changeable Secret Sharing Scheme Based on the Chinese Remainder Theorem

Xingxing Jia, Daoshun Wang, Daxin Nie, Xiangyang Luo, Jonathan Zheng Sun

PII: S0020-0255(18)30724-2
DOI: https://doi.org/10.1016/j.ins.2018.09.024
Reference: INS 13935

To appear in: *Information Sciences*

Received date: 10 May 2018
Revised date: 7 September 2018
Accepted date: 16 September 2018

Please cite this article as: Xingxing Jia, Daoshun Wang, Daxin Nie, Xiangyang Luo, Jonathan Zheng Sun, A New Threshold Changeable Secret Sharing Scheme Based on the Chinese Remainder Theorem, *Information Sciences* (2018), doi: https://doi.org/10.1016/j.ins.2018.09.024

A New Threshold Changeable Secret Sharing Scheme Based on the Chinese Remainder Theorem

Xingxing Jia[a,1,*], Daoshun Wang[b], Daxin Nie[a], Xiangyang Luo[c,*], Jonathan Zheng Sun[d]

[a]*School of Mathematics and Statistics, Lanzhou University, Lanzhou, Gansu, China*
[b]*School of Computing, Tsinghua University, Beijing, China*
[c]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Science and Technology Institute, Zhengzhou, Henan, China*
[d]*Department of Mathematics and Computer Science, Citadel Military College of South Carolina, Charleston, South Carolina, USA*

Abstract

A general (t, n) secret sharing (SS) scheme with fixed threshold allows a secret to be shared without considering the time dynamic nature of the security environment. In this paper, we propose a threshold changeable secret sharing scheme whose threshold can be changed in an integer interval $[t, t']$ without updating the shares. In this scheme, a different threshold can be activated at any time through the public broadcast channel. At the heart of the proposed scheme is a novel matrix of primes. The validity of the share generation and secret reconstruction is provided by the Chinese Remainder Theorem (CRT). We prove the existence of the proposed matrix and present a method to efficiently construct it, which makes use of a proposed sequence of nested closed intervals generated by large co-prime numbers. We further use the structure to propose a scheme with computational security, without maintaining online dealer. Compared with previous methods, the proposed scheme has short share size and low complexity for recovery. For any changeable threshold in $[t, t']$, the increase in share size is at most $\frac{1}{t-1}$ of that from previous methods. Computational complexity for secret recovery is $O(t)$, compared with $O(t \log^2 t)$ of the best previous methods.

Keywords: Threshold changeability, secret sharing, Chinese Remainder Theorem, entropy

1. Introduction

1.1. Threshold secret sharing

A $(t, n)(2 \leq t \leq n)$ secret sharing (SS) scheme deals with the problem of concealing a secret in a group of n mutually suspicious participants with conflicting interests who must cooperate. An authority called dealer distributes a secret s to the n participants such that any set of t or more participants can reconstruct the secret from their shares, while any set of less than $t-1$ participants cannot obtain any information about the secret. The property of collective engagement in the recovery of the secret gives the (t, n) SS scheme strong robustness against less than $t-1$ share loss or corruption. Pioneered by

☆This work was supported in part by 2017 Teaching and Research Program of Lanzhou University under Grant No. 2017114, in part by the National Natural Science Foundation of China under Grant Nos. U1536102, U1536116, U1636219, and 61872289, in part by Plan for Scientific Innovation Talent of Henan Province (No. 2018JR0018 and the Science and Technology Program of Guangxi (No. 16380076), in part by China Mobile Research Fund Project (MCM20170407), and Key Laboratory of Digital Content Anti-Counterfeiting and Security Forensics of the state Administration of Press, Publication, Radio, Film and Television of the People's Republic of China.

*Corresponding author.
Email addresses: jiaxx@lzu.edu.cn (Xingxing Jia), xiangyangluo@126.com (Xiangyang Luo)