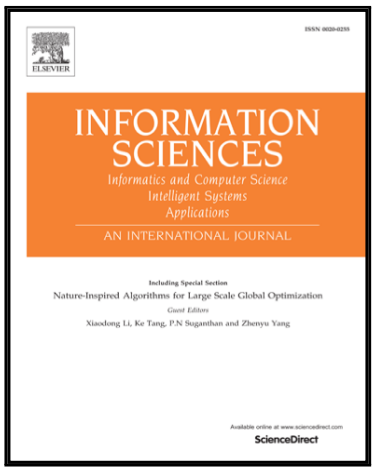

Attacks to some verifiable multi-secret sharing schemes and two improved schemes

Yanhong Liu, Futai Zhang, Jie Zhang

PII: S0020-0255(15)00695-7
DOI: 10.1016/j.ins.2015.09.040
Reference: INS 11804

To appear in: *Information Sciences*

Received date: 14 December 2011
Revised date: 1 December 2014
Accepted date: 16 September 2015

Please cite this article as: Yanhong Liu, Futai Zhang, Jie Zhang, Attacks to some verifiable multi-secret sharing schemes and two improved schemes, *Information Sciences* (2015), doi: 10.1016/j.ins.2015.09.040

Attacks to some verifiable multi-secret sharing schemes and two improved schemes

Yanhong Liu[1,3], Futai Zhang[1,2], Jie Zhang[1]

[1]*School of Computer Science and Technology, Nanjing Normal University, P.R. China*
[2]*Jiangsu Engineering Research Center on Information Security and Privacy Protection Technology, Nanjing, P.R. China*
[3]*Heilongjiang Research Center for Labor Safety Science and Technology, P.R. China*
Email: angelpray@126.com, zhangfutai@njnu.edu.cn, 464516929@qq.com

Abstract

Secret sharing plays an important role in protecting confidential information from being lost, destroyed, or falling into wrong hands. Verifiable multi-secret sharing enables a dealer to share multiple secrets among a group of participants such that the deceptive behaviors of the dealer and the participants can be detected. In this paper, we analyze the security of several recently proposed verifiable multi-secret sharing schemes. We show that these schemes cannot withstand some deceptive behaviors of the dealer, and hence fails to satisfy the basic requirement of secure verifiable secret sharing schemes. After that, we present two improved verifiable multi-secret sharing schemes. Our new schemes can not only resist cheating by the dealer or participants, but also remove the use of private channels.

Keywords: Secret sharing, verifiable multi-secret sharing scheme, private channel, shadow, RSA cryptosystem.

1. Introduction

Secret sharing plays an important role in protecting important information from getting lost, destroyed, or falling into wrong hands. It has many practical applications, such as safeguarding very confidential information, opening a bank vault, launching a missile, etc. In 1979, the first (t, n) threshold secret sharing schemes were proposed by Shamir [30] and Blakley [2] independently. In a (t, n) threshold secret sharing scheme, a secret can be shared among n participants such that t or more participants can reconstruct the secret, but $t-1$ or fewer participants can not. In real applications, it is known that traditional secret sharing schemes like Shamir's and Blakley's cannot solve the following problems:

(1) Only one secret can be shared during one secret sharing process, they cannot be used to share multiple secrets simultaneously.

(2) The shadows of participants are not reusable. Once the secret has been reconstructed, all shadows will no longer be private.

(3) Deceptive behaviors of a dishonest dealer cannot be detected. A dishonest dealer may distribute a fake shadow to a certain participant, and then that participant would subsequently never obtain the true secret.

(4) Deceptive behaviors of a malicious participant cannot be prevented in the process of reconstruction. A malicious participant may provided a fake shadow to cheat the other participants to prevent them from reconstructing the true secret.

(5) Private channels are required for the communications between the dealer and participants.

(6) The dealer knows all shadows of participants. The shadows of participants are not reusable for different dealers.