Information Sciences 453 (2018) 21–29

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Cheating identifiable secret sharing scheme using symmetric bivariate polynomial[☆]

Yanxiao Liu[a,*], Chingnung Yang[b], Yichuan Wang[a], Lei Zhu[a], Wenjiang Ji[a]

[a] *Department of computer science and engineering, XI'AN university of technology, 710048, China*
[b] *Department of CSIE, National Dong Hwa University, Hualien County, Taiwan*

ARTICLE INFO

Article history:
Received 1 February 2017
Revised 17 December 2017
Accepted 10 April 2018
Available online 10 April 2018

Keywords:
Secret sharing
Cheating identification
Bivariate polynomial
Symmetry

ABSTRACT

In (k, n) secret sharing scheme, any m out of the n users $(m \geq k)$ can reconstruct the secret and any less than k users cannot get any information on the secret. However, some cheaters can submit fake shares to fool other honest users during secret reconstruction. Cheating identification is an important technical to prevent such cheating behavior. In this paper, we consider cheating problem in bivariate polynomial based secret sharing scheme, and propose two cheating identification algorithms respectively. The first algorithm can identify cheaters by the m users who participate in secret reconstruction; the second algorithm can achieves stronger capability of cheater identification with the collaboration of the rest $n-m$ users who are not involved in secret reconstruction. In our scheme, the cheating identification is only based on the symmetry property of bivariate polynomial and linearity of interpolated polynomial. Both the two algorithms are efficient with respect of cheater identification capabilities.

© 2018 Elsevier Inc. All rights reserved.

1. Introduction

Since Shamir [18] and Blakley [1] introduced the concept of secret sharing to safely keeping secret information among a group of users in 1979, secret sharing schemes have attracted interests of scholars for almost four decades. In a (k, n) threshold secret sharing scheme, a dealer divides a secret into n shares, each share is send to a user through secure channels. Using their shares, k or more users can reconstruct the secret; but any $k-1$ or less users get no information on the secret at all.

In [21], Tompa and Woll proposed a cheating problem in secret sharing scheme such that cheaters submit fake shares during secret reconstruction. It results that other honest users reconstruct a forged secret, and the cheaters can get the real secret exclusively. Many works were proposed to prevent cheating problem in secret sharing schemes. Those schemes can be divided into two categories, cheating detection schemes [9,13,14,21] and cheating identification schemes [5,9–12,16,17,22]. In cheating detection schemes, honest users can detect the cheating behavior, but cannot identify cheaters; cheating identifiable schemes provide stronger technical to solving the cheating problem where honest users can not only detect the cheating behavior, but also identify the cheaters. The first cheater identifiable scheme was introduced in [16], and the discussion on capability of identifying cheaters is proposed in [11], however more than k users are needed to identify cheaters in that

[☆] Cheating identification secret sharing.
[*] Corresponding author.
E-mail address: liuyanxiao@xaut.edu.cn (Y. Liu).

https://doi.org/10.1016/j.ins.2018.04.043
0020-0255/© 2018 Elsevier Inc. All rights reserved.

scheme [11]. The schemes [8,12,17] can identify cheaters when k users participate in secret reconstruction. The cheater identification of [8,12] were based on linear error correcting code and universal hash functions, and the cheater identification of [17] was based on pairwise share authentication keys. In [5,10], two identifiable secret sharing schemes were proposed, where the cheating identification were only based on the linearity of interpolated polynomial. However the scheme [5] requires much more than k users to identify cheaters [3], and the capability of scheme [10] is weaker than other schemes [12,17].

Most previous cheating identifiable secret sharing schemes were based on Shamir's work [18], where all the shares are generated from a $k-1$ degree polynomial $f(x)$. However, bivariate polynomial $F(x, y)$ is also a fundamental tool to construct functional secret sharing schemes such as verifiable secret sharing schemes [2,6,7,15] where all users can verify the correctness of their shares before secret reconstruction. Both symmetric and asymmetric bivariate polynomial can be used in verifiable secret sharing schemes. Recently, bivariate polynomial based secret sharing were also extended to other cryptographic schemes, such as secure cloudy computing [19], multiple secrets reconstruction [4], and secret image sharing schemes [20,23]. Bivariate polynomial based secret sharing scheme has attracted more attention in the research of secret sharing schemes. However, there are few cheater identifiable secret sharing schemes based on bivariate polynomial. In [22], Wang et al. proposed a cheater identifiable scheme using bivariate polynomial, but their scheme is not secure against collusive cheaters.

In this paper, we propose two cheater identification algorithms in secret sharing schemes using symmetric bivariate polynomial. In our scheme, the shares of each user are generated from a symmetric bivariate polynomial, which is the same approach in those verifiable secret sharing schemes [7,15]. The cheating identification is only based on the symmetry property of bivariate polynomial and the linearity of interpolated polynomial. The first algorithm can identify cheaters from the m users who participate in secret reconstruction; the second algorithm can achieve stronger capability of cheater identification with the collaboration of the rest $n-m$ users who are not involved in secret reconstruction. Both the two algorithms are efficient with respect of the capabilities on cheating identification. Although most cheating identification schemes involves only the m users who participate in secret reconstruction, the rationality of inviting the rest $n-m$ users to identify cheaters is explained in Yang et al. 's work [23]. In that scheme, m out n users work together to reconstruct a secret image using their shadows, when the cheating is detected, all n users (including the rest $n-m$ users) collaborate to authenticate the validity of each shadow of the m users. There are also many applications where the integrity of users are the most important in the security, such as the intelligence department or the military department of government. If (k, n) secret sharing scheme is adopted in these applications, it is necessary to involve all the n users in cheating identification.

This paper is organized as follows. In Section 2, we prepare some preliminaries, which includes Shamir's secret sharing scheme, bivariate polynomial based secret sharing scheme and some results on cheater identifiable secret sharing schemes. In Section 3, we propose our scheme with two cheating identification algorithms, and analyze their securities and capabilities of cheating identification. In Section 4, four different examples are used to describe the cheating identification of proposed schemes. Comparison between our schemes and other cheater identifiable schemes are also shown in this section. Section 5 gives the conclusion of our work.

2. Preliminaries

In this part, we give a brief description of Shamir's (k, n) secret sharing scheme, which is also the fundamental of bivariate polynomial based (k, n) secret sharing scheme. Next, we introduce the model of cheater identifiable secret sharing scheme and list some previous works on it.

2.1. Shamir's (k, n) secret sharing scheme

A (k, n) secret sharing scheme is a method where a secret is divided into n pieces information, called shares, in such way that any k or more shares can reconstruct the secret and fewer than k shares get nothing on the secret. More formally, in secret sharing scheme, there exists n users $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ and a dealer $\mathcal{D}$. A (k, n) secret sharing scheme consists of two phases:

1. ***Sharing phase:*** During this phase, the dealer $\mathcal{D}$ divides the secret s into n shares $v_1, v_2, \ldots, v_n$, and sends each share v_i to a user P_i.
2. ***Reconstruction phase:*** During this phase, a group of at least k users submit their shares to reconstruct the secret.

In the ***Sharing phase***, the dealer $\mathcal{D}$ computes n shares in such a way that satisfies the following conditions:

1. ***Correctness:*** Any set of at least k shares can reconstruct the valid secret.
2. ***Secrecy:*** Any fewer than k shares have no information regarding the secret.

Shamir's (k, n) secret sharing scheme is shown in following Scheme 1.

Scheme 1. Shamir's (k, n) secret sharing scheme
Sharing phase :

1. The dealer $\mathcal{D}$ choose a $k-1-th$ degree polynomial $f(x) \in GF(q)[X]$ which satisfies $s = f(0) \in GF(q)$.

Download English Version:

https://daneshyari.com/en/article/6856398

Download Persian Version:

https://daneshyari.com/article/6856398

Daneshyari.com