Information Processing Letters 115 (2015) 851–857

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Dynamic threshold secret reconstruction and its application to the threshold cryptography

Lein Harn [a], Ching-Fang Hsu [b,*]

[a] Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City, 64110, MO, USA
[b] Computer School, Central China Normal University, 430079, Wuhan, China

ARTICLE INFO

Article history:
Received 18 April 2014
Received in revised form 16 June 2015
Accepted 20 June 2015
Available online 26 June 2015
Communicated by S.M. Yiu

Keywords:
Cryptography
Secret sharing scheme
Bivariate polynomial
Secure channel
Dynamic threshold

ABSTRACT

Shamir's (t, n) secret sharing scheme (SS) is based on a univariate polynomial and is the most cited SS in the literature. The secret in a (t, n) SS can be recovered either by exactly t or more than t shareholders. Most SSs only consider when there are exactly t shareholders participated in the secret reconstruction. In this paper, we examine security issues related to the secret reconstruction if there are more than t shareholders participated in the secret reconstruction. We propose a dynamic threshold SS based on a bivariate polynomial in which shares generated by the dealer can be used to reconstruct the secret but having a larger threshold which is equivalent to the exact number of participated shareholders in the process. In addition, we extend the proposed scheme to enable shares which can also be used to establish pairwise keys to protect the reconstructed secret from non-shareholders. Shamir's SS has been used in conjunction with other public-key algorithms in most existing threshold algorithms. Our proposed SS can also be applied to the threshold cryptography to develop efficient threshold algorithms.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

The (t, n) secret sharing scheme (SS) was propose by Shamir [1] and Blakley [2] separately in 1979. In a (t, n) SS, the dealer divides the secret into n shares such that (a) the secret can be recovered if there are t or more than t shares, and (b) the secret cannot be recovered if there are fewer than t shares. The (t, n) SS can be implemented by different mathematical tools. For example, Shamir's scheme is based on a univariate polynomial, Blakely's scheme [1] is based on the geometry, Mignotte's scheme [3], Asmuth–Bloom's scheme [4] are based on the Chinese remainder theorem (CRT) and McEliece et al. scheme [5] is based on Reed–Solomon codes.

SS has become one of most popular cryptographic tools in many protocols of multi-party computing. The secret reconstruction of Shamir's SS is very simple and is based on the Lagrange interpolation formula. However, in the secret reconstruction, additional mechanisms are needed to protect the secret; otherwise, non-shareholders (i.e., outside attackers) or dishonest shareholders' (i.e., inside attackers) can take advantage over honest shareholders.

In 1985, Chor et al. [6] proposed the first verifiable secret sharing (VSS). Verifiability is the property of a VSS which allows shareholders to verify their shares. Invalid shares may be caused by the dealer during generation or by channel noise during transmission. VSS is executed by shareholders after receiving their shares from the dealer but before using their shares to reconstruct the secret. If VSS has detected/identified invalid shares, shareholders can request the dealer to regenerate new shares. There are vast research papers on the VSS in the literature. Based to

* Corresponding author.
E-mail addresses: harnl@umkc.edu (L. Harn), cherryjingfang@gmail.com (C.-F. Hsu).

http://dx.doi.org/10.1016/j.ipl.2015.06.014
0020-0190/© 2015 Elsevier B.V. All rights reserved.

security assumptions, we can classify VSSs into two different types, schemes that are computationally secure and unconditionally secure. For example, Feldman [7] and Pedersen [8] developed non-interactive VSSs based on cryptographic commitment schemes. The security of Feldman's VSS is based on the hardness of solving discrete logarithm, while the privacy of Pedersen's VSS is unconditionally secure and the correctness of the shares depends on a computational assumption. Benaloh [9] proposed an interactive VSS scheme and it is unconditionally secure. Stinson et al. [10] proposed an unconditionally secure VSS and later, Patra et al. [11] proposed a generalized VSS scheme. In 1996, Stadler [12] proposed the first publicly verifiable secret sharing (PVSS) scheme. A PVSS scheme allows each shareholder to verify the validity of all shares, including both shares of his/her own and other shareholders. However, in most non-interactive VSSs [7,8], shareholders can only verify the validity of his/her own share; but not other shareholders' shares.

When shareholders present their shares in the secret reconstruction, dishonest shareholders (i.e., cheaters) can always exclusively derive the secret by presenting fake shares and thus the other honest shareholders get nothing but a fake secret. It is easy to see that Shamir's (t, n) secret sharing scheme does not prevent dishonest shareholders in the secret reconstruction. Cheater detection and identification are important functions in order to provide fair reconstruction of a secret. In 1989, Tompa and Woll [13] proposed the first cheater detection scheme. There are many research papers in the literature to propose algorithms for cheater detection and identification. Most of these algorithms [14–17] assume that there are exactly t shareholders participated in the secret reconstruction. The dealer needs to provide additional information to enable shareholders to detect and identify cheaters. Some algorithms [18,19] use error-correcting codes to detect and identify fake shares. In a recent paper, Harn and Lin [20] proposed a new approach to detect and identify cheaters. The algorithm uses shares to detect and identify cheaters. When there are more than t (i.e., the threshold) shares, for example j (i.e., $t < j$) shares in the secret reconstruction, the redundant shares can be used to detect and identify cheaters. In this approach, shares in a secret sharing scheme serve for two purposes; that are, (a) reconstructing the secret and (b) detecting and identifying cheaters. The detectability and identifiability of cheaters is proportional to the number of redundant shares in the secret reconstruction.

In this paper, we consider different security issues in the secret reconstruction. In particular, we examine problems if there are more than t shareholders participated in the secret reconstruction. We will discuss these problems in Section 3. Furthermore, we propose dynamic threshold SSs to overcome these problems. Our proposed SSs are based on a bivariate polynomial. Shares obtained from the dealer can serve for three different purposes, (a) reconstructing the secret, (b) reconstructing the secret having a dynamic threshold and (c) protecting exchange information in the secret reconstruction.

We summarize the contributions of our paper.

- A dynamic threshold SS based on a bivariate polynomial is proposed in which shares obtained from the dealer initially can be used to reconstruct the secret but having a larger threshold which is equivalent to the exact number of participants.
- An efficient (t, n) SS is proposed in which shares generated by the dealer can serve for three different purposes, (a) reconstructing the secret, (b) reconstructing the secret having a dynamic threshold and (c) protecting exchange information in the secret reconstruction.
- Our proposed SSs can be extended to the threshold cryptography to develop efficient threshold cryptographic algorithms (threshold signature/encryption).

The rest of paper is organized as follows. In Section 2, we review SSs based on polynomials. We discuss some security issues in the secret reconstruction in Section 3. A dynamic threshold SS and an efficient (t, n) SS based on a bivariate polynomial are proposed in Sections 4 and 5, respectively. The application of our proposed SS to the threshold cryptography is discussed in Section 6. The conclusion is given in Section 7.

2. Review of SSs based on polynomials

In Shamir's (t, n) SS [1], the dealer selects a univariate polynomial, $f(x)$, with degree $t-1$ and $f(0) = s$, where s is the secret. The dealer generates shares, $f(x_i)$, $i = 1, 2, \ldots, n$, for shareholders, where x_i is the public information associated with each shareholder, U_i. Each share, $f(x_i)$, is an integer in $GF(p)$. Shamir's (t, n) SS satisfies both security requirements of a (t, n) SS. That are, (a) with t or more than t shares can reconstruct the secret, and (b) with fewer than t shares cannot obtain any information of the secret. Shamir's SS is unconditionally secure.

Shamir's (t, n) SS does not provide the ability to allow shareholders to verify their shares obtained from the dealer. In 1985, Chor et al. [14] extended the notion of SS and proposed the first verifiable secret sharing (VSS). Verifiability is the property of a VSS which allows shareholders to verify their shares. Invalid shares may be caused by the dealer during generation or by channel noise during transmission. VSS is executed by shareholders after receiving their shares from the dealer but before using their shares to reconstruct the secret. If VSS has detected/identified invalid shares, shareholders can request the dealer to regenerate new shares. There are many (t, n) VSSs [21–27] based on bivariate polynomials, denoted them as BVSSs. A bivariate polynomial with degree $t-1$ is represented as $F(x, y) = a_{0,0} + a_{1,0}x + a_{0,1}y + a_{2,0}x^2 + a_{1,1}xy + a_{0,2}y^2 + \ldots + a_{t-1,0}x^{t-1} + a_{t-2,1}x^{t-2}y + \ldots + a_{0,t-1}y^{t-1} \bmod p$, where $a_{i,j} \in GF(p)$, $\forall i, j \in [0, t-1]$. If the coefficients satisfy $a_{i,j} = a_{j,i}$, $\forall i, j \in [0, t-1]$, it is a symmetric bivariate polynomial. Shares generated by a bivariate polynomial enable pairwise keys to be shared between any pair of shareholders. We can classify BVSSs into two types, the asymmetric BVSSs, denoted them as ABVSSs [21,22,24,26] and the symmetric BVSSs, denoted them as SBVSSs [24–27]. In all existing (t, n) SBVSSs, the dealer selects a bivariate polynomial,

Download English Version:

https://daneshyari.com/en/article/428845

Download Persian Version:

https://daneshyari.com/article/428845

Daneshyari.com