Information Sciences 294 (2015) 31–40

Contents lists available at ScienceDirect

Information Sciences

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

Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and LFSR public-key cryptosystem

Samaneh Mashhadi, Massoud Hadian Dehkordi *

Department of Mathematics, Iran University of Science & Technology, Narmak, Tehran 16846 13114, Iran

ARTICLE INFO

Article history:
Received 29 November 2007
Received in revised form 6 May 2014
Accepted 22 August 2014
Available online 26 September 2014

Keywords:
Verifiable secret sharing
Nonhomogeneous linear recursion
LFSR public-key cryptosystem
Public value
Secure channel

ABSTRACT

We shall propose two new efficient verifiable multi-secret sharing schemes based on linear feedback shift register (LFSR) public key and new nonhomogeneous linear recursions. Compared with previous schemes, these schemes have better performance and shorter private/public key length. Moreover, they have fewer public values and simpler construction, as well as various methods for the reconstruction phase. Altogether, they are easy to use and provide great capabilities for many applications.

1. Introduction

A (t,n) multi secret sharing scheme is a method which allows multiple secrets to be shared among a set of participants in such a way that in a subset of any size at least t participants can recover the shared secrets, but $(t-1)$ or fewer participants cannot obtain anything about the secrets [2–6,9–20].

In verifiable multi-secret sharing, there are multiple secrets to be shared during a secret sharing process, and any cheating by a dealer or by participants can be detected [5,6,9–13,19]. In 2005, Shao and Cao (SC)[17] presented an efficient verifiable multi-secret sharing based on Yang et al.'s (YCH) and Feldman's schemes [19,6]. In those schemes, the dealer, send the shadow of each participant through a secure channel. In 2006, Zhao et al. (ZZZ) [19] proposed a practical verifiable multi-secret sharing based on YCH and Hwang–Chang (HC) schemes [19,13]. As HC, ZZZ deployed RSA cryptosystem and Diffie–Helman (DH) key agreement method in the verification phase, so they did not require a secure channel. In addition, each participant chooses his secret shadow by himself. This not only cuts the dealer's amount of computing, but also makes it impossible for the dealer to cheat.

In 2008, we proposed two verifiable multi-secret sharing schemes based on homogeneous linear recursions [9]. There, for the first time, we deployed homogeneous linear recursions instead of polynomials in the distribution and the recovery phases. The schemes not only posses all of the advantages of the previous schemes, but also provides some new benefits including simpler distribution, alternative ways of reconstruction, the possibility of using a secret after an unsuccessful reconstruction, the possibility of increasing or decreasing of a secret in any time, and alternative ways of distribution. In

* Corresponding author.
E-mail addresses: smashhadi@iust.ac.ir (S. Mashhadi), mhadian@iust.ac.ir (M. Hadian Dehkordi).

http://dx.doi.org/10.1016/j.ins.2014.08.046
0020-0255/

addition, in the verification phase in [9], as in that of ZZZ and HC, RSA and DH are employed, so these schemes do not require a secure channel and each participant chooses his shadow by himself. In 2008, again for the first time, we proposed two new efficient and secure verifiable multi-secret sharing schemes based on nonhomogeneous linear recursions [10], having all the advantages of the previous schemes. Further, in the verification phase, elliptic curve discrete logarithm problem (ECDLP) and elliptic curve RSA (ECRSA) were employed, so those do not need secure channels.

In 2012, Hu et al. [12] proposed two verifiable multi-secret sharing schemes based on [7–9]. They employed homogeneous linear recursions in the distribution and reconstruction phase and the LFSR cryptosystem in the verification phase. The proposed method in [12] has shorter private/public key in comparison to the previous ones (more precisely, one-third of the previous schemes) because of the employed LFSR cryptosystem [7,8]. Thus, it also has better performance.

In this paper, we suggest two verifiable multi-secret sharing schemes based on LFSR cryptosystem and new nonhomogeneous linear recursions. These schemes pose all of the advantages of the previous schemes. According to the properties of linear recursions, these schemes have a simple construction, three different methods for the reconstruction phase, the possibility of using a secret after an unsuccessfully reconstruction, the possibility of increasing or decreasing of a secret in any time, and alternative ways of distribution. In addition, we employ the LFSR cryptosystem in the verification phase. Then the length of the private/public key of our scheme is only one-third of those of the previous ones. In addition, the security level of our method is the same as that of the previous ones. Since we have employed simpler nonhomogeneous linear recursions in comparison to those employed in [10], the present method has better performance and less number of public keys.

1.1. Nonhomogeneous linear recursion

In this section we will introduce the mathematical background of our schemes. At first we bring some preliminaries about homogeneous linear recursions. A detailed description of linear recursion can be found in [1].

Definition 1. Let t be a positive integer and $c_0, c_1, \ldots, c_{t-1}, a_1, a_2, \ldots, a_t$ be real numbers. A *homogeneous linear recursion of degree t* or a *homogeneous linear feedback shift register (HLFSR) sequence* (u_i) is defined by the equations

$$[\text{HLFSR}]\begin{cases} u_0 = c_0, u_1 = c_1, \ldots, u_{t-1} = c_{t-1}, \\ u_{i+t} + a_1 u_{i+t-1} + \cdots + a_t u_i = 0, \end{cases} \quad (i \geqslant 0)$$

where $c_0, c_1, \ldots, c_{t-1}$ and $a_1, a_2, \ldots, a_t$ are constants.

Definition 2. We define the *auxiliary equation* and the *characteristic polynomial* for [HLFSR] to be $x^t + a_1 x^{t-1} + \cdots + a_t = 0$ and $f(x) = x^t + a_1 x^{t-1} + \cdots + a_t$ respectively. We define the *generating function* for the HLFSR sequence (u_i) to be $U(x) = \sum_{i=0}^{\infty} u_i x^i$.

The following theorem, proved in [1], provides an explicit formula for calculating the terms of homogeneous LFSR sequence (u_i).

Theorem 3. *Suppose that the HLFSR sequence (u_i) is defined by [HLFSR], and the auxiliary equation has the roots $\alpha_1, \alpha_2, \ldots, \alpha_l$ with multiplicities $m_1, m_2, \ldots, m_l$, respectively. Then*

I. *The generating function for the sequence (u_i) is $U(x) = \frac{R(x)}{(1-\alpha_1 x)^{m_1}(1-\alpha_2 x)^{m_2}\cdots(1-\alpha_l x)^{m_l}}$, where $R(x)$ is a polynomial and deg $R(x) < t$;*

II. *$u_i = p_1(i)\alpha_1^i + p_2(i)\alpha_2^i + \cdots + p_l(i)\alpha_l^i$, where $p_j(i)$ is a polynomial function of i with degree at most $m_j - 1$.*

Thus, we have the following result.

Corollary 4. *Consider a typical fraction $\frac{R(x)}{(1-\alpha x)^m}$ where $h(x)$ is a polynomial and deg $R(x) < m$. Then we have*

$$\frac{R(x)}{(1-\alpha x)^m} = \sum_{i=0}^{\infty} u_i x^i,$$

where $u_i = p(i)\alpha^i$ and $p(x)$ is a $(m-1)$-degree polynomial.

We will use the above results in the sequel. Now, we bring some preliminaries about nonhomogeneous linear recursion.

Definition 5. Let t be a positive integer and $c_0, c_1, \ldots, c_{t-1}, a_1, a_2, \ldots, a_t$ be real numbers. A *nonhomogeneous linear recursion of degree t* or a *nonhomogeneous linear feedback shift register (NHLFSR) sequence* (u_i) is defined by the equations

$$[\text{NHLFSR}]\begin{cases} u_0 = c_0, u_1 = c_1, \ldots, u_{t-1} = c_{t-1}, \\ u_{i+t} + a_1 u_{i+t-1} + \cdots + a_t u_i = f(i), \end{cases} \quad (i \geqslant 0)$$

where $c_0, c_1, \ldots, c_{t-1}$ and $a_1, a_2, \ldots, a_t$ are constants.

This recurrence is said to have degree t since each term u_i depends on the previous t terms. It is also linear since u_{i+t} is a linear function of the previous terms, and nonhomogeneous because $f(i) \neq 0$.