A Nonlinear Secret Sharing Scheme

Ari Renvall and Cunsheng Ding

Department of Mathematics
University of Turku
Fin-20014 Turku, Finland

Abstract. In this paper, we have described a nonlinear secret-sharing scheme for $n$ parties such that any set of $k - 1$ or more shares can determine the secret, any set of less than $k - 1$ shares might give information about the secret, but it is computationally hard to extract information about the secret. The scheme is based on quadratic forms and the computation of both the shares and the secret is easy.

1 Introduction

In a secret-sharing scheme a number of parties share a secret. The information about the secret a party has is called a share or shadow. The earliest contributions on this topic are linear ones [1, 9]. There are many later contributions on this topic (see [2, 3, 4, 8, 10, 11, 12] for examples). Some nonlinear secret-sharing schemes can be found in [2, 11]. The most studied secret-sharing schemes are the $(k, n)$ threshold schemes in which the secret can be recovered with any set of $k$ shares while any set of $k - 1$ shares gives no information about the secret. By a proper formulation linear $(k, n)$ threshold schemes are equivalent to maximum distance separable (MDS) error-correcting codes, but there is only a very limited class of MDS linear codes. The progress in coding theory shows that finding more MDS linear codes, and therefore more linear $(m, n)$ threshold schemes, is not easy. This motivates the study of nonlinear secret-sharing schemes.

In secret-sharing schemes for $n$ parties the shares $t_i$ for $i = 1, 2, \ldots, n$ are often computed according to some arithmetic functions

$$t_i = f_i(s_1, s_2, \ldots, s_u),$$

where $s_1$ is the secret and $s_2, \ldots, s_u$ are randomly chosen elements of some fields. We call such a scheme linear if all $f_i$ are linear with respect to the variable $s = (s_1, \ldots, s_u)$, and nonlinear otherwise.

Most of the secret-sharing systems are designed so that when a subset of parties pools their shares together, they get either no information or all information about the secret. Thus, in such a scheme only authorized parties can get information about the secret. Such secret-sharing schemes are called perfect. An alternative could be that the unauthorized sets of shares are allowed to give a limited amount of information about the secret, but extracting the information by such a subset of parties is computationally hard. Thus, theoretically they can get some information about the secret, but computationally they cannot do so.
This is the case for many cipher systems in which a set of plaintext-ciphertext pairs usually gives information about the key, but finding the actual key by making use of the information provided by the set of plaintext-ciphertext pairs could be computationally infeasible. From practical point of view such a secret-sharing system with similar properties could be as good as a perfect scheme.

In this paper we describe a nonlinear secret sharing scheme for $n$ parties such that

- any $k - 1$ or more shares are enough to recover the secret;
- any $k - 2$ or fewer shares might give information about the secret, but it is computationally hard to extract the information.

Our secret-sharing system has the following properties:

1. it is nonlinear;
2. both computing the shares and recovering the secret are efficient;
3. with decoding techniques for Reed-Solomon codes it can correct cheatings when enough parties pool their shares together.

The secret-sharing scheme, based on the theory of quadratic forms, is nonperfect since it is nonlinear. It can be proved that all linear secret-sharing schemes are perfect, but nonlinear schemes are often nonperfect.

2 Designing the parameters

Let $p$ be a large prime of the form $p = 3 \mod 4$. Our secret is a number between 0 and $(p-1)/2$. We shall use $\mathbb{GF}(p)$ to denote the field consisting of the integers $\{0, 1, \cdots, p-1\}$ with addition and multiplication modulo $p$. We assume that each number between 0 and $(p-1)/2$ is equally likely to be the secret.

The secret-sharing scheme described in this paper is intended for key safeguarding, so we assume that the prime $p$ has at least 60 bits. The other parameters of the system are a set of distinct nonzero integers $a_1, \cdots, a_n$.

Before specifying the parameters we need some notations. In the sequel for each set of indices $1 < i_1 < \cdots < i_w < n$, where $1 \leq w \leq n$, let

$$M(i_1, \cdots, i_w) = \begin{bmatrix}
a_{i_1} & a_{i_1}^2 & \cdots & a_{i_1}^w \\
a_{i_2} & a_{i_2}^2 & \cdots & a_{i_2}^w \\
\vdots & \vdots & \ddots & \vdots \\
a_{i_w} & a_{i_w}^2 & \cdots & a_{i_w}^w
\end{bmatrix}$$

and $N(i_1, \cdots, i_w) = [n(i_1, \cdots, i_w)_{u,v}]$ be the inverse of $M(i_1, \cdots, i_w)$. Furthermore, let

$$\beta_2(i_1, \cdots, i_{k-2}) = 1 + \sum_{u=2}^{k-1} \left( \sum_{v=1}^{k-2} n(i_1, \cdots, i_{k-2})_{u,v} \right)^2$$