Information Sciences 181 (2011) 1403–1409

Contents lists available at ScienceDirect

Information Sciences

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

An ideal multi-secret sharing scheme based on MSP

Ching-Fang Hsu [a,*], Qi Cheng [b], Xueming Tang [a], Bing Zeng [a]

[a] *College of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan 430074, China*
[b] *Engineering Department, Institute of Wuhan Digital Engineering, Wuhan 430074, China*

ARTICLE INFO

Article history:
Received 9 October 2009
Received in revised form 21 June 2010
Accepted 27 November 2010
Available online 5 December 2010

Keywords:
Ideal linear multi-secret sharing schemes
Monotone span programs
Perfect multi-secret sharing schemes

ABSTRACT

A multi-secret sharing scheme is a protocol to share m arbitrarily related secrets $s_1,\ldots,s_m$ among a set of n participants. In this paper, we propose an ideal linear multi-secret sharing scheme, based on monotone span programs, where each subset of the set of participants may have the associated secret. Our scheme can be used to meet the security requirement in practical applications, such as secure group communication and privacy preserving data mining etc. We also prove that our proposed scheme satisfies the definition of a perfect multi-secret sharing scheme.

1. Introduction

Single-secret sharing schemes (SSSS). A secret sharing scheme is a protocol to distribute a secret among a set $\mathcal{P}$ of participants. This distribution is done in such a way that some authorized subsets of participants, pooling together their information, can reconstruct the secret; whereas, other unauthorized subsets of participants have no information about the secret.

Secret sharing schemes were first described by Blakley [3] and Shamir [30]. They analyzed (t,n) threshold schemes, which were the most practical and widely developed until now (see [1,7,13,15–17,35]). In such schemes any set of at least t out of n participants can recover the secret, but sets of cardinality less than t have no information about it. In [2,18,19] it has been shown how to realize a secret sharing scheme for any access structure, where the access structure is the family of all subsets of participants that are authorized to reconstruct the secret. For a unified description of results in the area of secret sharing schemes the reader can consult the survey articles by Simmons [31] and Stinson [32].

An important research direction in the area of secret sharing schemes is to establish bounds on the size of the shares to be given to participants, which, in turn, establishes bounds on both the storage complexity and the communication complexity of secret sharing schemes. Thus, it has received considerable attention by several researchers (see [8,9]). A secret sharing scheme is said to be ideal if the size of each share is the same as the size of the secret. This definition can be extended to multi-secret sharing, that is, a secret sharing scheme with multiple secrets is said to be ideal if all secrets and shares are the same size.

Multi-secret sharing schemes (MSSS). Many secret sharing applications, in particular those associated with key management, require the protection of more than one secret. As an example, consider the following situation, described by Simmons [31]: There is a missile battery in which each missile has a different launch enable code. The problem is to devise a scheme to protect these codes by using the same pieces of private information. This problem could be trivially solved by realizing different secret sharing schemes, one for each launch enable code, but in this case each participant should remember too much information. In order to reduce the amount of information given to participants it is interesting to investigate the possibility of constructing multiple sharing schemes without necessarily using different single sharing schemes.

[*] Corresponding author.
E-mail address: cherryjingfang@gmail.com (C.-F. Hsu).

0020-0255/$ - see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2010.11.032

Another scenario in which the sharing of many secrets is important was considered by Franklin and Yung [14]. They investigated the communication complexity of unconditionally secure multi-party computation and its relations with various fault-tolerant models. They presented a general technique for parallelizing non-cryptographic computation protocols, at a small cost in fault-tolerance. Their technique replaces polynomial-based (single) secret sharing with a technique allowing multiple secrets to be hidden in a single polynomial. The technique applies to all protocols for secure computation which use polynomial based threshold schemes.

Previous results. Specific models for the sharing of many secrets have already been considered in the literature. In [24] Karnin et al. considered the problem of sharing m secrets $s_1,\ldots,s_m$ among a set of n participants. In particular, they considered the situation in which, for a fixed value $k \leqslant n$ and for any $1 \leqslant j \leqslant m$, any set of k participants can reconstruct the secret s_j, whereas, any set of $k-1$ participants has no information about the secret s_j. These schemes are called (m,k,n) multi-secret sharing threshold schemes, which have been constructed by several researchers recently (see [10–12,27,28,34]). Schemes of this kind have been also considered by Jackson et al. [20,22]. In particular, they considered the situation in which, for a fixed value $t \in \{1,2,\ldots,n\}$, there is a secret associated with each set $\mathcal{P}' \subseteq \mathcal{P}$, such that $|\mathcal{P}'| = t$. For a fixed parameter $k \leqslant t$, this secret can be reconstructed by any k participants in $\mathcal{P}'$. They proved bounds on the size of the information that participants must hold in order to ensure that up to w participants $(0 \leqslant w \leqslant n-t+k-1)$ cannot obtain any information about a secret they are not associated with. Such schemes are referred to as w-secure (k,t,n) multi-threshold schemes.

In [5] the problem of sharing more than one secret among a set of participants has been generalized to the case where all the secrets are shared according to a fixed access structure. In the proposed model any qualified set of participants can recover all the secrets, whereas, any non-qualified set of participants has absolutely no information about each secret but, knowing some secrets, might have some information about the other secrets. Schemes of this kind have also been considered in [21], where some optimal constructions have been proposed. The problem of sharing many secrets according to different access structures has been considered in [4] and further investigated in [23], where a classification of ideal secret sharing schemes with multiple secrets has been proposed.

By using a multi-party computation protocol, [26] solved a secret-leaking problem in multi-secret sharing schemes, in which they also showed that the non-direct sum linear multi-secret sharing scheme was preferred in reducing share expansion, after comparing it with the associated "direct sum" scheme. A corresponding relation between monotone span programs and linear multi-secret sharing schemes has been studied in [33], where the optimal linear multi-secret sharing schemes have also been discussed. These results are fairly interesting to construct ideal multi-secret sharing schemes for general access structures.

Our results. However, very little is known about how to devise ideal multi-secret sharing schemes for general access structures. Due to the difficulty of finding general results, the construction of ideal multi-secret sharing schemes for families of access structures that may have interesting applications is worth considering. In this paper, we consider the security requirement of practical applications, such as secure group communication and privacy preserving data mining etc., where each subset of the set of participants need have the associated secret. We construct such an ideal linear multi-secret sharing scheme, in which each subset of $t\,(t \leqslant n)$ participants may have different target secret. In particular, we put forward a general and simple construction method for such a scheme based on monotone span programs. The correctness and security of the proposed scheme are proved.

The rest of the paper is organized as follows: In Section 2, the basic definitions of secret sharing schemes and monotone span programs (MSP) are reviewed. The MSP to permit more than one target vector is introduced in Section 3. In Section 4, based on the MSP, the proposed scheme is described. Section 5 proves the correctness and security of the proposed scheme and finally, conclusions are provided in Section 6.

2. Preliminaries

In this section we review some basic definitions concerning secret sharing schemes.

2.1. Access structures and adversary structures

Let $\mathcal{P} = \{1,\ldots,n\}$ be the set of participants. An access structure, denoted by Γ, is a collection of subsets of $\mathcal{P}$ satisfying the monotone ascending property: for any $A' \in \Gamma$ and $A \in 2^{\mathcal{P}}$, $A' \subseteq A$ implies $A \in \Gamma$. An adversary structure, denoted by $\mathcal{A}$, is a collection of subsets of $\mathcal{P}$ satisfying the monotone descending property: for any $A\prime \in \mathcal{A}$ and $A \in 2^{\mathcal{P}}$, $A \subseteq A'$ implies $A \in \mathcal{A}$. Because of the monotone properties, for any access structure Γ and any adversary structure $\mathcal{A}$, it is enough to consider the minimum access structure $\Gamma_{\min} = \{A \in \Gamma | \forall B \subset A \Rightarrow B \notin \Gamma\}$ and the maximum adversary structure $\mathcal{A}_{\max} = \{B \in \mathcal{A} | \forall A \supset B \Rightarrow A \notin \mathcal{A}\}$ respectively. In this paper, we consider the complete situation, i.e., $\mathcal{A} = 2^{\mathcal{P}} - \Gamma$.

2.2. Linear secret sharing schemes and monotone span programs

Suppose that S is the secret-domain and P_i is the share-domain of participant i, where $1 \leqslant i \leqslant n$. When a dealer D wants to share a secret $s \in S$ among a set of participants $\mathcal{P} = \{1,\ldots,n\}$, he will give each participant a share $p_i \in P_i$. The shares should be distributed secretly, so no participant knows the share given to another participant. At a later time, a subset of