Fully Dynamic Secret Sharing Schemes *

Carlo Blundo,[1] Antonella Cresti,[2] Alfredo De Santis,[1] and Ugo Vaccaro[1]

[1] Dipartimento di Informatica ed Applicazioni,
Università di Salerno, 84081 Baronissi (SA), Italy

[2] Dipartimento di Scienze dell' Informazione,
Università di Roma "La Sapienza", 00198 Roma, Italy

Abstract

We consider secret sharing schemes in which the dealer is able (after a preprocessing stage) to activate a particular access structure out of a given set and/or to allow the participants to reconstruct different secrets (in different time instants) by sending them the same broadcast message. In this paper we establish a formal setting to study secret sharing schemes of this kind. The security of the schemes presented is unconditional, since they are not based on any computational assumption. We give bounds on the size of the shares held by participants, on the size of the broadcast message, and on the randomness needed in such schemes.

1 Introduction

A secret sharing scheme is a method of dividing a secret s among a set $\mathcal{P}$ of participants in such a way that: if the participants in $A \subseteq \mathcal{P}$ are qualified to know the secret then by pooling together their information they can reconstruct the secret s; but any set A of participants not qualified to know s has absolutely no information on the secret. The collection of subsets of participants qualified to reconstruct the secret is usually referred to as the *access structure* of the secret sharing scheme.

Secret sharing schemes are useful in any important action that requires the concurrence of several designed people to be initiated, as launching a missile, opening a bank vault or even opening a safety deposit box. Secret sharing schemes are also used in management of cryptographic keys and multi-party secure protocols (see [11] for example). We refer the reader to the excellent survey papers [21] and [24] for a detailed discussion of secret sharing schemes and for a complete bibliography on the argument.

Simmons [21] first pointed out the practical relevance of secret sharing schemes having the feature of being able (after some preprocessing stage) to activate a particular access structure out of a given set and/or to allow the participants to reconstruct different secrets (in different time instants) simply by sending to all participants the same broadcast message. Harn, Hwang, Laih, and Lee [12] gave an algorithm to construct threshold secret sharing schemes (i.e., characterized by an access structure consisting of all subsets of participants of cardinality not less than some integer k), in which the dealer could enable participants

*Partially supported by Italian Ministry of University and Research (M.U.R.S.T.) and by National Council for Research (C.N.R.). A preliminary version of this paper has been presented at Crypto '93.

to recover different secrets in different time instants simply by sending the same broadcast message to all of them. However, the authors of [12] assumed that the access structure remained the same in each time instant. Martin [19] presented a technique to realize secret sharing schemes for general access structures in which, by sending a broadcast message to all participants, a new secret is activated and a participant is disenrolled from the scheme. Blakley, Blakley, Chan, and Massey [2] considered the problem of constructing threshold secret sharing schemes with disenrollment capability, but the value of the threshold of the secret sharing schemes is not changed at each disenrollment. Moreover, they gave a lower bound on the size of the shares held by each participant in such schemes.

The problem of evaluating the size of the shares to be given to participants is among the most important problems in the area of secret sharing schemes. Recently, the problem of estimating the amount of random bits necessary to set up the schemes has received considerably attention. The first problem is strictly related to the security of the schemes, since the security of any system degrades as the amount of secret information increases. The problem of estimating the number of random bits necessary to implement randomized algorithms is receiving considerable interest (see [13], [17], for example). This is due to the fact that the amount of randomness needed by an algorithm is to be considered a computational resource, analogously to the amount of time and space needed. The quantitative study of the number of random bits needed by secret sharing schemes has been initiated in [6], where the optimality of several secret sharing schemes according to this measure has been proved. Some other results on this topic can be found in [3].

In this paper we establish a formal setting to study secret sharing schemes in which different access structures and/or different secrets can be activated in subsequent time instants simply by sending the same broadcast message to all participants. Our approach is information–theoretic based. The security of the schemes presented in this paper is unconditional, since they are not based on any computational assumption. We first study the case in which we have different access structures and we want to enable one of them to reconstruct a predefined secret. In this model we show that the size of shares held by any participant and the size of the broadcast message are bounded from below by the size of the secret. We show that these bounds are optimal if one considers separately the problem of bounding the size of the share of the participant and that of the broadcast message (see Theorem 4.5 and Theorem 4.6). Motivated by this result we define *Ideal Secret Sharing Schemes with Broadcast Message* as schemes for which the size of the shares held by participants and the size of the broadcast messages are the same as the size of the secret. We analyze ideal secret sharing schemes with broadcast messages when the family of the access structures that can be activated contains threshold access structures only. In Section 7 we consider the general case in which one wants to activate different access structures to recover possibly different secrets at subsequent time instants. We give sufficient conditions for the existence of a participant whose share size is lower bounded by the sum of the sizes of the secrets. This result generalizes the result of [2]. In Section 8 we analyze the randomness needed to set up secret sharing schemes with broadcast message and we give protocols that are optimal to this respect.

2 Secret Sharing

A secret sharing scheme permits a secret to be shared among a set $\mathcal{P}$ of n participants in such a way that only qualified subsets of $\mathcal{P}$ can recover the secret, but any non-qualified