On Partial Anonymity in Secret Sharing

Vanesa Daza and Josep Domingo-Ferrer

Rovira i Virgili University
UNESCO Chair in Data Privacy
Department of Computer Engineering and Mathematics
Av. Països Catalans, 26, E-43007 Tarragona, Catalonia
{vanesa.daza,josep.domingo}@urv.cat

Abstract. Anonymous secret sharing schemes allow a secret to be recovered from shares regardless of the identity of shareholders. Besides being interesting in its own right, this property is especially appealing to guarantee the anonymity of participants when secret sharing is used as a building block of more general distributed protocols (*e.g.* to anonymously share the secret key corresponding to a public key). However, current constructions of anonymous secret sharing schemes are not very efficient (because of the number of shares that every participant must hold) and existing bounds do not leave much room for optimism. In this paper we propose to weaken the anonymity condition to partial anonymity, where by partial anonymity we mean that the identity of the participant is not made public, but he is known to belong to some subset. That is, the search for a participant narrows down to one in a set of possible candidates. Furthermore, we propose a general construction of partial anonymous secret sharing schemes.

Keywords: Privacy, Protocols, Secret sharing.

1 Introduction

Anonymous secret sharing schemes allow a secret to be recovered from a set of shares without knowledge of which participants hold which shares. That is, in such schemes the computation of the secret can be carried out regardless the identities of shareholders. Beyond its intrinsic interest, anonymous secret sharing is particularly attractive to guarantee the anonymity of participants in more general distributed protocols. A typical application is anonymous sharing of the secret key corresponding to a certain public key. Unfortunately, the constructions of anonymous secret sharing schemes in the literature are not very efficient (in terms of the number of shares that every participant must hold) and existing bounds [4,16] do not leave much hope for forthcoming efficient constructions.

Anonymous secret sharing schemes were introduced in 1988 by Stinson and Vanstone [22]. Phillips and Phillips [17] proved that only some specific access structures can yield anonymous secret sharing schemes where the size of the shares given to each participant is equal to the size of the secret (smallest possible size). Later on, Blundo and Stinson [4] gave general constructions of anonymous secret sharing schemes. They also gave lower bounds on the size of the set

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 193–202, 2007.

of shares (as a function of the size of the secret) both for threshold and non-threshold access structures. However, their constructions are not very efficient and their lower bounds preclude substantially improved forthcoming constructions. Since then, some authors have proposed constructions of anonymous secret sharing schemes, but either they are quite inefficient or they are restricted to the particular $(2, n)$ threshold case.

1.1 Contribution and Plan of This Paper

The lack of efficient constructions for anonymous secret sharing motivates us to weaken the anonymity condition in quest of efficiency, measured in terms of the number of shares that must be held by any participant. In that sense, we introduce the notion of partial anonymity with the aim of providing a tradeoff between the level of anonymity achieved by a scheme and its efficiency. Roughly speaking, in partial anonymous secret sharing the identity of the participant is not made public, but he is known to belong to some subset. In other words, the search for a participant narrows down to one in a set of possible candidates. This principle bears some vague resemblance to k-anonymity [18] used for privacy in databases and k-anonymity to preserve privacy in communication protocols [23,24]. On the practical side, we propose an efficient construction of a scheme fulfilling the partial anonymity property.

The rest of the paper is organized as follows. We introduce some basic concepts on secret sharing schemes in Section 2. In Section 3 we review the notion of anonymous secret sharing schemes and we introduce the notion of partially anonymous secret sharing schemes. In Section 4 we provide some constructions of partially anonymous secret sharing schemes. Finally, we conclude in Section 5.

2 Secret Sharing

Secret sharing schemes were independently introduced by Shamir [19] and Blakley [2] in 1979. A secret sharing scheme is a method whereby a special entity D, usually called dealer, distributes a secret s among a set $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n players. The dealer secretly sends to every player P_i his share s_i of the secret s in such a way that only authorized subsets can recover the secret whereas non-authorized subsets obtain no information on the secret s.

A basic principle when designing secret sharing schemes is to minimize the amount of secret material. Therefore, the length of the shares should be as small as possible. In a secret sharing scheme the length of any share of a participant is greater than or equal to the length of the secret. When they are equal, the scheme is called ideal.

The family Γ of the subsets of shares authorized to recover the secret is called access structure. Any access structure is assumed to be monotone, that is, any superset of an authorized subset is also an authorized subset. A particular case is an access structure formed by those sets of players with at least t players, that is,

$$\Gamma = \{A \subset \mathcal{P} \mid\mid A \mid \geq t\}$$