Information Sciences 339 (2016) 85–97

Contents lists available at ScienceDirect

Information Sciences

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

Distributive weighted threshold secret sharing schemes☆

Constantin Cătălin Drăgan, Ferucio Laurenţiu Ţiplea*

Department of Computer Science, "Alexandru Ioan Cuza" University of Iaşi, Romania

ARTICLE INFO

Article history:
Received 21 April 2013
Revised 22 December 2015
Accepted 3 January 2016
Available online 11 January 2016

Keywords:
Access structure
Secret sharing scheme
Chinese remainder theorem
Entropy

ABSTRACT

The concept of distributive weighted threshold access structure is introduced, which is an weighted threshold access structure where the participants are distributed on levels, the participants on the same level are assigned the same weight, and the threshold of the access structure is 1. The weight of the participants on the ith level is of the form $1/k_i$ and, therefore, the ith level induces a standard threshold access structure with threshold k_i.

We propose a CRT-based realization of distributive weighted threshold access structures, which is asymptotically perfect and perfect zero-knowledge. We also show that distributive weighted threshold access structures do not generally have ideal realizations. In case of just one level, our scheme can be viewed as an asymptotically perfect and perfect zero-knowledge variation of the Asmuth–Bloom secret sharing scheme.

1. Introduction

A secret sharing scheme is a method of partitioning a master secret among some users by providing each user with a share of the secret. The secret can be recovered only if a sufficient number of shares are combined together. Secret sharing schemes were independently proposed for the first time by Blakley [7] and Shamir [20]. Blakley's scheme is based on hyperplane intersections. The secret is an element of a k-dimensional vector space over a Galois field, and the shares are $(k-1)$-dimensional hyperplanes whose intersection is the secret. The secret can be obtained by intersecting any k shares. Shamir's scheme is based on polynomial interpolation. The secret is the free coefficient of a polynomial P of degree $k-1$ with coefficients in $\mathbb{Z}_p$ for some large prime p, and the shares are $P(i)$ for any $1 \leq i \leq n$, where $n \geq k$. Any k shares can recover the secret by computing the polynomial by interpolation.

Novel threshold secret sharing schemes based on the Chinese Remainder Theorem (CRT) have independently been proposed by Asmuth and Bloom [1] and Mignotte [16], and later by Goldreich et al. [11]. The schemes in this category, are based on sequences of co-prime positive integers with special properties. The shares are obtained by dividing the secret or a secret-dependent quantity by the numbers in the sequence and collecting the remainders. The secret can be recovered from any k shares, where k depends on the sequence, by using CRT.

Weighted threshold secret sharing schemes are natural generalizations of threshold secret sharing schemes, where each participant is assigned a weight depending on his importance (role) in the group of all participants. The secret can be reconstructed if and only if the sum of the weights assigned to a set of participants is greater than or equal to a fixed threshold. This idea was first proposed by Shamir [20] who also suggested a realization of it by using tuples of polynomial

☆ Work supported by the European Social Fund in Romania, under the responsibility of the Managing Authority for the Sectoral Operational Programme for Human Resources Development 2007–2013 [Grant POSDRU/CPP 107/DMI 1.5/S/78342].

* Corresponding author. Tel.: +40 742019593.
E-mail addresses: constantin.dragan@info.uaic.ro (C.C. Drăgan), fltiplea@info.uaic.ro, fltiplea@gmail.com (F.L. Ţiplea).

http://dx.doi.org/10.1016/j.ins.2016.01.019
0020-0255/

values associated to each participant. In 1999, Morilo et al. [17] proposed a complete characterization of the weighted threshold access structures of rank two by using graph theory (the rank of a weighted threshold access structure is the maximum cardinality of the minimal authorized sets). Later, Beimel et al. [3,4] have proposed a characterization of ideal weighted threshold access structures by showing that weighted threshold access structures are ideal if and only if they are either hierarchical threshold access structures of at most three levels, or tripartite access structures, or compositions of two ideal weighted threshold access structures.

As we have mentioned above, Shamir already suggested in [20] how weighted threshold secret sharing schemes can be obtained by using polynomial interpolation. Wang et al. [25] generalized Shamir's idea by proposing a weighted secret sharing scheme that creates the secret-dependent quantity in the same manner as Shamir, but computes the shares as the remainders obtain by polynomial reduction. The scheme uses a polynomial form of the CRT [8] to recover the secret (one may also see the last section in [1]). Another direction to design weighted threshold secret sharing schemes was to extend the Mignotte's and Asmuth–Bloom's schemes to weighted threshold access structures [13–15]. Unfortunately, [14,15] do not provide any security analysis of the proposed schemes and it is expected that these schemes are neither asymptotically perfect nor asymptotically ideal nor perfect zero-knowledge [18]. The scheme in [13] is somehow a direct translation of the Asmuth–Bloom scheme; it adds more public parameters and reaches the same security as the Asmuth–Bloom scheme (which is neither asymptotically perfect nor perfect zero-knowledge [2]). An extensive comparison between our work and the one in [13–15] is provided in the last section.

Another class of secret sharing schemes closely related to our work is that of *multilevel secret sharing schemes* [4,6,12,21,23] also called *hierarchical threshold secret sharing schemes* in [4,23]. In such schemes, participants are divided into disjoint levels according to their importance. These levels are totally ordered and participants on lower levels are more important than participants on higher levels. In a standard scenario regarding the employees of a bank, the lowest level may consists of the board of directors. Two types of access structures for multilevel secret sharing schemes have been proposed so far, namely *disjunctive multilevel access structures* [21] and *conjunctive multilevel access structures* [23] (the terms *disjunctive* and *conjunctive* were proposed in [6]). To understand the difference between these two types of access structures let $U_1, \ldots, U_q$ denote the levels, where U_1 is the lowest one. To each level U_i a threshold k_i is associated such that $k_1 < \cdots < k_q$. In disjunctive multilevel access structures a group of participants can reconstruct the secret if there exists i such that the group contains at least k_i participants taken from $\cup_{j=1}^{i} U_j$, while in conjunctive multilevel access structures the group of participants who want to reconstruct the secret must contain at least k_i participants taken from $\cup_{j=1}^{i} U_j$, for all i.

Contribution. To understand the motivation of our work let us consider the case of a disjunctive multilevel access structure with just two levels U_1 and U_2 and thresholds $k_1 = 2$ and $k_2 = 4$. Assume that U_1 consists of directors, and U_2 of senior tellers, of a bank. The choice of these parameters tells that a bank vault can be opened by either any two directors or four senior tellers. According to the definition of a disjunctive multilevel access structure, the bank vault can also be opened by three senior tellers together with one director, but not by two senior tellers together with one director. This is somewhat contrary to our intuition that, according to the choice of the parameters, one director can be replaced by any two senior tellers.

This small example leads us to consider multilevel access structures where each participant has associated a weight and where each participant in an authorized set can be replaced by any number of participants whose weights can compensate the weight of that participant. These new multilevel access structure are introduced via weighted threshold access structures and are called *distributive weighted threshold access structures*. With such a structure, all the participants are distributed over a fixed number of levels $U_1, \ldots, U_q$. The participants on the same level U_i are assigned the same weight which is of the form $1/k_i$ for some positive integer k_i. The scheme threshold is 1; that is, any set of participants whose sum of weights exceeds 1 should be able to recover the secret. In particular, any set of k_i participants on the level U_i are able to recover the secret. Therefore, the integer k_i acts as a threshold for the level U_i showing that distributive weighted threshold access structures can also be viewed as methods of combining disjoint threshold access structures. The authorized sets are either the authorized sets of the component threshold access structures or sets of participants on different levels whose sum of weights exceeds 1.

Distributive weighted threshold access structures are "extension" of disjunctive multilevel access structures in the sense that for any disjunctive multilevel access structure Γ one can construct a distributive weighted threshold access structure Γ' such that $\Gamma \subseteq \Gamma'$.

As distributive weighted threshold access structures are particular cases of weighted threshold access structures, they can be realized by the CRT-based secret sharing schemes proposed in [13–15] for weighted threshold access structures. Unfortunately, as we have already mentioned, the schemes in [13–15] appear to be neither asymptotically perfect nor asymptotically ideal nor perfect zero-knowledge (more on these will be provided in the last section). Therefore, we propose a CRT-based realization of the distributive weighted threshold access structures, different than those in [13–15], and we show that this realization is asymptotically perfect and perfect zero-knowledge. We also prove that distributive weighted access structures do not generally have ideal realizations. From this point of view, we may say that our scheme is all that can be achieved using CRT. In case of just one level, our CRT-based realization of the distributive weighted threshold access structures can be viewed as an asymptotically perfect and perfect zero-knowledge variation of the Asmuth–Bloom secret sharing scheme (recall that the Asmuth–Bloom secret sharing scheme is neither asymptotically perfect nor perfect zero-knowledge [2]).