Information Sciences 367–368 (2016) 209–220

Contents lists available at ScienceDirect

Information Sciences

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

Realizing secret sharing with general access structure

Lein Harn [a,b,1], Chingfang Hsu [c,1,*], Mingwu Zhang [a], Tingting He [c], Maoyuan Zhang [c]

[a] School of Computer Science and Technology, Hubei University of Technology, 430068, Wuhan, China
[b] Department of Computer Science Electrical Engineering, University of Missouri- Kansas City, MO 64110, USA
[c] Computer School, Central China Normal University, 430079, Wuhan, China

ARTICLE INFO

Article history:
Received 18 November 2015
Revised 11 April 2016
Accepted 8 June 2016
Available online 14 June 2016

Keywords:
General secret sharing
Chinese remainder theorem
Secret sharing policy
Monotone function
Integer optimization
Minimal positive access subset
Maximal negative access subset

ABSTRACT

Secret sharing (SS) is one of the most important cryptographic primitives used for data outsourcing. The (t, n) SS was introduced by Shamir and Blakley separately in 1979. The secret sharing policy of the (t, n) threshold SS is far too simple for many applications because it assumes that every shareholder has equal privilege to the secret or every shareholder is equally trusted. Ito et al. introduced the concept of a general secret sharing scheme (GSS). In a GSS, a secret is divided among a set of shareholders in such a way that any "*qualified*" subset of shareholders can access the secret, but any "*unqualified*" subset of shareholders cannot access the secret. The secret access structure of GSS is far more flexible than threshold SS. In this paper, we propose an optimized implementation of GSS. Our proposed scheme first uses Boolean logic to derive two important subsets, one is called *Min* which is the *minimal positive access subset* and the other is called *Max* which is the *maximal negative access subset,* of a given general secret sharing structure. Then, conditions of parameters of a GSS are established based on these two important subsets. Furthermore, integer linear/non-linear programming is used to optimize the size of shares of a GSS. The complexity of linear/non-linear programming is $O(n)$, where n is the number of shares generated by the dealer. This proposed design can be applied to implement GSS based on any classical SS. However, our proposed method is limited to be applicable to some general secret sharing policies. We use two GSSs, one is based on Shamir's weighted SS (WSS) using linear polynomial and the other is based on Asmuth-Bloom's SS using Chinese Remainder Theorem (CRT), to demonstrate our design. In comparing with existing GSSs, our proposed scheme is more efficient and can be applied to all classical SSs.

1. Introduction

The(t, n) SS was introduced by Shamir [24] and Blakley [2] independently in 1979 and then became one of the most important cryptographic primitives discussed by many researchers [10,17,18,22]. In a (t, n) SS, a dealer divides a secret s into n shares and s is shared among a set of n shareholders, $U = \{U_1, U_2, ..., U_n\}$, in such a way that any t or more than t shareholders can reconstruct the secret s; while fewer than t shareholders cannot reconstruct the secret s. In Shamir's (t, n)

[*] Corresponding author. Tel.: 86 18908625707.

E-mail addresses: harnl@umkc.edu (L. Harn), cherryjingfang@gmail.com (C. Hsu), csmwzhang@gmail.com (M. Zhang), tthe@mail.ccnu.edu.cn (T. He), zhangmyccnu@126.com (M. Zhang).

[1] Lein Harn and ChingFang Hsu contributed equally to this work.

http://dx.doi.org/10.1016/j.ins.2016.06.006
0020-0255/© 2016 Elsevier Inc. All rights reserved.

SS, a dealer generates n shares based on a linear polynomial having degree$t-1$. Secret reconstruction is based on Lagrange interpolating formula using any t or more than t private shares. Shamir's (t, n) SS is unconditionally secure. There are other types of SSs. For example, Blakely's scheme [2] is based on Geometry, Mignotte's scheme [19] and Asmuth-Bloom's scheme [1] are based on Chinese remainder theorem (CRT), and McEliece et al. scheme [20] is based on Reed-Solomon codes.

The weighted (t, n) secret sharing scheme (WSS) was originally proposed by Shamir [24]. In a WSS, each share of a shareholder has a positive weight. The secret can be recovered if the overall weight of shares is equal to or larger than the threshold; but the secret cannot be recovered if the overall weight of shares is smaller than the threshold value. In fact, Shamir's (t, n) SS is a special type of WSSs in which the weight of all shares is the same. One simple way to implement a WSS using Shamir's (t, n) SS is to assign multiple shares to each shareholder according to his/her weight. There are some papers to discuss properties and characteristics of a WSS. For example, Morillo et al. [21] discussed the property of information rate of a WSS. Beimel et al. [3] characterized all weighted threshold access structures that are ideal. They showed that a weighted threshold access structure is ideal if and only if it is a hierarchical threshold access structure, or a tripartite access structure, or a composition of two ideal weighted threshold access structures that are defined on smaller sets of users.

The secret sharing policy of the (*t, n*) threshold SS is far too simple for many applications because it assumes that every shareholder has equal privilege to the secret. Complicated sharing policies, in which shareholders have different privileges, can also be realized by other general SSs [4,11]. Ito et al. [11] have introduced the concept of general secret sharing (GSS). In a GSS, a secret is divided among a set of shareholders, U, in such a way that any "qualified" subset of Ucan access the secret, but any "unqualified" subset of Ucannot access the secret. Benaloh et al. [4] have shown that there is a correspondence between the set of general secret sharing functions and the set of monotone functions. Ito et al. [12] have introduced the *cumulative array technique* and used it to construct a GSS based on monotone access structures. In their scheme, multiple shares are needed for each shareholder. Benaloh et al. [4] have represented the access instances using formulae. According to monotone access instances of a secret, a set of formulae on a set of variables is used to share the secret. Their scheme shares the same problem as scheme proposed by Ito et al. That is, multiple shares are needed for each shareholder. Harn et al. [8] have proposed an *l*-span generalized SS in which the shares can be repeatedly used for *r* times to reconstruct *r* different secrets. However, the security of their scheme is based on RSA assumption. Horng [9] propose a method for constructing multiple assignment schemes which is a combination of the threshold scheme and the cumulative scheme. The *cumulative map* is a simple realization of the multiple assignment map based on a (t, n) SS [11] which utilized a GSS based on a WSS. However, the GSSs constructed by the cumulative map are inefficient. Iwamoto et al. [13] proposed an optimal multiple assignments based on integer programming to optimize the size of shares. The complexity of solving an integer programming problem is related to the cardinality of the constraint variables set. However, the number of variables in the integer programming is $O(2^n)$,where n is the number of shares generated by the dealer. Li et al. [15] proposed a method to reduce the number of constraint variables in the integer programming problem. Srinathan et al. [25] have considered the problem of non-perfect secret sharing (NSS) over general secret sharing policy and defined generalized monotone span programs (MSP) to facilitate the design of NSS schemes. However, their approach captures and addresses only NSS schemes that are linear. In 2007, Xu et al. [28] have studied new operations on secret sharing policy to construct large MSPs from small MSPs and proposed new design of GSS. Recently, Guo et al. [6] have proposed a scheme based on the key-lock-pair mechanism. The share of each shareholder is a pair of column vectors corresponding to the key-lock-pair. However, the number of elements of column vectors is determined by the number of terms in the secret access structure. Iftene [14] has proposed a GSS using CRT for special types of general access structures such as the compartmented and the weighted threshold SSs. In 2015, Li et al. [16] have proposed a type of secret sharing schemes called *ramp assignment schemes* (RAS's) to realize general access structures (AS's). In such a scheme, each participant is assigned a subset of primitive shares of an optimal *(k, L, m)*-ramp scheme in such a way that the number of primitive shares assigned to each qualified subset is not less than *k* whereas the one corresponding to any forbidden subset is not greater than *k* – *L*. RAS's can be viewed as a generalization of multiple assignment schemes. Very recently, Tochikubo [26] proposed a perfect GSS which is more efficient than schemes based on scheme proposed by Benaloh et al. [4] and Tochikubo [27].

In a GSS, there are two most important subsets, one is called *Min* which is the *minimal positive access subset* and the other is called *Max* which is the *maximal negative access subset,* which characterize any given general secret sharing structure. In this paper, we first uses Boolean logic to derive these two important subsets. Our proposed method is very simple and straightforward. Then, we propose to use these two subsets to implement a GSS. In particular, integer linear/non-linear programming is used to optimize the size of shares of a GSS. Our design is completely different from all existing schemes. This proposed design can be applied to implement GSS based on any classical SS. We use two GSSs, one is based on Shamir's weighted SS (WSS) using linear polynomial and the other is based on Asmuth-Bloom's SS using Chinese Remainder Theorem (CRT), to demonstrate our design. In comparing with existing GSSs, our proposed scheme is more efficient and can be applied to all classical SSs. Here, we summarize the contributions of our paper.

- We propose an optimized design to implement a GSS based on any classical SS.
- For any given general secret sharing policy, Boolean logic is used to derive *Min* and *Max*, then parameters of a GSS are determined based on *Min* and *Max*.
- Integer linear/non-linear programming can be used to minimize the size of shares. The complexity in the integer/non-linear programming is $O(n)$.