Chapter 2

Evolution of Secret Sharing Schemes

2.1 Introduction

In this chapter, we discuss the evolution of Secret Sharing Schemes. Some important advancements in this area are discussed and illustrated with suitable examples. The difficulties and limitations of the different schemes is also discussed.

In this section we recall some general notations used and basic definitions of secret sharing schemes.

Definition 2.1
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, and any non-qualified subset has

absolutely no information on the secret. In other words, a non-qualified subset knows only that the secret is chosen from a prespecified set (which we assume is public knowledge), and they cannot compute any further information regarding the value of the secret.

Definition 2.2

An *access structure* Γ is the set of all subsets of $\mathcal{P}$ that can recover the secret.

Definition 2.3

The collection of subsets of participants that cannot reconstruct the secret is called *prohibited access structure* or simply *prohibited structure* and is usually denoted by Δ.

Definition 2.4

Let $\mathcal{P}$ be a set of participants and $2^{\mathcal{P}}$ denotes the collection of all subsets of $\mathcal{P}$. A *monotone access structure* Γ on $\mathcal{P}$ is a subset $\Gamma \subseteq 2^{\mathcal{P}}$, such that,

$$A \in \Gamma, A \subseteq B \subseteq \mathcal{P} \Rightarrow B \in \Gamma.$$

i.e, if an access structure is monotone, then, any superset of an authorized subset must be authorized.

Definition 2.5

Let $\mathcal{P}$ be a set of participants and let $\mathcal{A} \subseteq 2^{\mathcal{P}}$. The *closure of* $\mathcal{A}$, denoted by *cl(*$\mathcal{A}$*)*, is the set

$$\mathrm{cl}(\mathcal{A}) = \{\, C \mid \exists\, B \in \mathcal{A} \text{ such that } B \subseteq C \subseteq \mathcal{P} \,\}.$$

That is, the closure of an access structure Γ is the smallest monotone access structure containing Γ.

For a monotone access structure Γ, we have, $\Gamma = cl(\Gamma)$. Suppose Γ is an access structure on $\mathcal{P}$. Then $B \in \Gamma$ is a *minimal* authorized subset, if $A \notin \Gamma$ whenever $A \subset B$. The set of *minimal* authorized subsets of Γ is denoted by Γ_{min} and is called the *basis* of Γ. Similarly, for a prohibited structure Δ on $\mathcal{P}$, $B \in \Delta$ is a *maximal* unauthorized subset, if $A \notin \Delta$ whenever $A \supset B$. It is easy to see that, for every monotone access structure, there is a corresponding set of maximal unauthorized access sets.

We can see that a monotone access structure Γ is completely characterized by the family of its minimal authorized subsets Γ_{min}, via, $\Gamma = cl(\Gamma_{min})$. Hence monotone access structures can be determined by the corresponding family of its minimal authorized subsets.

Obviously, it is hard to imagine a meaningful method of sharing a secret in which the access structure does not possess the monotone property. It is assumed that there is always at least one subset of participants who can reconstruct the secret, i.e., $\Gamma \neq \phi$, and also that every participant belongs to at least one minimal qualified subset.

For sets X and Y and for elements x and y, to avoid overburdening of the notations, we often write x for $\{x\}$, xy for $\{x, y\}$, and XY for $X \cup Y$.

Example 2.1

Let $\mathcal{P}$ *be* $P_1P_2P_3P_4$ *and* $\mathcal{A} = \{P_1P_2P_3,\ P_1P_2P_4,\ P_1P_3P_4,\ P_2P_3\}$. *The subset* $\mathcal{A}$ *is not a monotone subset, for both* P_2P_3 *and* $P_1P_2P_3 \in \mathcal{A}$, *where one is a subset of other.*

The *closure* of $\mathcal{A}$, $cl(\mathcal{A}) = \{P_1P_2P_3,\ P_1P_2P_4,\ P_1P_3P_4,\ P_1P_2P_3P_4,\ P_2P_3,\ P_2P_3P_4\}$ and the set of *minimal* subsets of $\mathcal{A}$ is, $\mathcal{A}_{min} = \{P_1P_2P_4,\ P_1P_3P_4,\ P_2P_3\}$.

Example 2.2

Consider the following monotone access structure on $\mathcal{P} = P_1P_2P_3P_4$*:*

$$\begin{aligned}\mathcal{A} \;=\; \{\; & P_1P_2,\ P_2P_3,\ P_3P_4,\ P_1P_4,\ P_1P_2P_3,\\ & P_1P_2P_4,\ P_1P_3P_4,\ P_2P_3P_4,\ P_1P_2P_3P_4\ \}.\end{aligned}$$

The set of *minimal* authorized subsets of $\mathcal{A}$ is given by $\mathcal{A}_{min} = \{P_1P_2,\ P_2P_3,\ P_3P_4,\ P_1P_4\}$ and the corresponding maximal unauthorized access sets are P_1P_3 and P_2P_4.

Definition 2.6

A Secret Sharing Scheme is called *ideal,* if the size of the shares is less than or equal to the size of the secret.

Definition 2.7

A Secret Sharing Scheme is called *perfect,* if, no information about the secret is obtained on pooling of shares of any unauthorized set of participants.

2.2 Evolution of the schemes

In the initial stages of work on secret sharing, Blakley [9] and Shamir [53] considered only schemes with a (k, n)-threshold access structure. Benaloh showed an interactive verifiable (k, n)-threshold secret sharing scheme which is zero knowledge [6]. In [61], D. R. Stinson and S. A. Vanstone introduced the anonymous threshold scheme. Informally, in an anonymous secret sharing scheme, the secret is reconstructed without the knowledge of, which participants hold which shares. In such schemes the computation of the secret can be carried out by giving the shares to a black box that does not know the identities of the participants holding those shares. The authors proved a lower bound on the size of the shares for anonymous threshold schemes and provided optimal schemes for certain classes of threshold structures by using a combinatorial characterization of optimal schemes. Further results can be found in [51] and in [26].

Phillips and Phillips [49] considered a different model for anonymous secret sharing schemes. In their model, different participants are allowed to receive the same shares. They proved the interesting result that a strongly ideal scheme for an access structure Γ on n participants can be realized, if and only if, Γ is either a $(1, n)$-threshold structure, a (n, n)-threshold structure, or the closure of the edge set of a complete bipartite graph. Further

results on this type of anonymous secret sharing schemes can be found in [16].

Non-anonymous secret sharing schemes for graph access structures have been extensively studied in several papers, such as [18] [19] [22] [15] [14] [59] [60].

Further works considered the problem of finding secret sharing schemes for more general access structures. D. R. Stinson [58] gives a comprehensive introduction to this topic.

Secret Sharing schemes based on Chinese Remainder Theorem was introduced by Mignotte [47]. Asmuth and Bloom [1] implemented a (k, n) threshold scheme based on Chinese Remainder Theorem in 1983.

A black-box secret sharing scheme for the threshold access structure is one which works over any finite Abelian group. G. Bertilsson and I. Ingemarsson [8] describes a construction method of practical secret sharing schemes using Linear Block Codes.

A more general approach has been considered by Karnin, Greene and Hellman [39], who invented the analysis (limited to threshold scheme) of secret sharing schemes when arbitrary probability distributions are involved.

Some other general techniques handling arbitrary access struc-

tures are given by Simmons, Jackson, and Martin [45] [56] and also suggested by Kothari [41].

In [17], Brickell introduced the *vector space construction* which provides secret sharing schemes for a wide family of access structures. In [58], Stinson proved that threshold schemes are vector space access structures.

During 1987 Ito, Saito, and Nishizeki [36] described a generalized method of secret sharing scheme whereby a secret can be divided among a set $\mathcal{P}$ of trustees such that any qualified subset of $\mathcal{P}$ can reconstruct the secret and unqualified subsets cannot. They have described a secret sharing scheme, for a generalized monotone access structure.

While in threshold schemes proposed by Blakley [9] and Shamir [53] and in the vector space schemes given by Brickell [17] the shares have the same size as the secret, in the schemes constructed by M. Ito, A. Saito, and T. Nishizeki [36] for general access structures, the shares are, in general, much larger than the secret.

An important issue in the implementation of secret sharing schemes is the size of shares, since the security of a system degrades as the amount of the information that must be kept secret increases. J. C. Benaloh and J. Leichter, proved that there exists an access structure (namely the path of length three) for

which any secret sharing scheme must give to some participant a share which is from a domain larger than that of the secret.

Subsequently, Benaloh and Leichter [5] gave a simpler and more efficient way to realize such schemes. They also proved that no threshold scheme is sufficient to realize secret sharing on general monotone access structures. In support of their claim, they have shown that there is no threshold scheme such that the access structure $((A \vee B) \wedge (C \vee D))$ can be achieved. [see Example 2.3.]

In [6], Benaloh describes a homomorphism property that is present in many threshold schemes which allows shares of multiple secrets to be combined to form "composite shares" which are shares of a composition of the secrets. This property, makes the entity best suitable in implementing the cases in which, one requires high confidentiality, such as e-voting. While casting the vote, each voter will take the role of dealer, and the votes casted will be recorded in terms of shares given to each contesting candidate. Because of the homomorphism property, (i.e., $h(ab) = h(a).h(b)$,) one can combine shares, and compute the votes scored by each contesting candidate.

Capocelli, De Santis, Gargano and Vaccaro [22] proved that, there exist access structures for which the best achievable information rate (i.e., the ratio between the size of the secret and that of the largest share) is bounded away from 1. An ideal

secret sharing scheme is a scheme in which the size of the shares given to each participant is equal to the size of the secret. Brickell and Davenport [18] showed a correspondence between ideal secret sharing schemes and matroids (see also [38]).The uniqueness of the associated matroid is established by Martin in [44]. Beimel and Chor [4] investigate the access structures for which an ideal scheme can be constructed for every possible size of the set of secrets.

The following are some "extended capabilities" of secret sharing schemes that have been studied.

- The idea of protecting against cheating by one or more participants is addressed in [46], [62], [50], [54], [20], [23]. The problem of identifying the cheater is solved by Tompa and Woll [62]. In a sense, it is an improvement on the works of Shamir [53]. A cheater might tamper with the content of a share and make the share unusable for combining, to retrieve the secret.

- Prepositioned schemes are studied in [55].

- Threshold schemes that permit disenrollment of participants are investigated and redistributing secret shares to new access structures has been considered in [10].

- Secret sharing schemes in which the dealer has the feature of being 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 to all participants the same broadcast message have been analyzed in [13].

- Schemes for sharing several non-independent secrets simultaneously have been analyzed in [14].
- Schemes where different secrets are associated with different subsets of participants are considered in [37].
- The question of how to set up a secret sharing scheme in the absence of a trusted party is solved in [35].

De Santis, Desmedt, Frankel, and Yung [31] introduced the notion of threshold sharing for functions and they described how to share a key to a cryptographically secure function f in such a way that:

- Any k shareholders can collectively compute f.
- Even after taking part in the computation of f on some inputs, no set of up to $k-1$ shareholders can compute f on other inputs.

B. Chor and E. Kushilevitz [27] investigated secret sharing systems on infinite domain with finite access structures.

1994, Naor and Shamir [48] described a new $(k,\ n)$ visual cryptographic scheme using black and white images, where the dealer distributes a secret into n participants. In this scheme, a shared secret information (printed text, handwritten notes, pictures, etc.) can be revealed without any cryptographic computations. For example, in a $(k,\ n)$ visual cryptography scheme, a dealer encodes a secret into n shares and gives each participant a share, where each share is a transparency. The secret is visible if any k(or more) of participants stack their transparencies together (in an arbitrary order), but none can see the shared secret if fewer than k transparencies are stacked together. It is clear that the visual secret sharing scheme needs no computation in decryption. This property distinguishes the visual secret sharing schemes from ordinary secret sharing schemes. In [3], G. Ateniese, C. Blundo, A. D. Santis, and D. R Stinson gave a construction method to extend the $(k,\ n)$ visual cryptography scheme to a general access structure which is specified by qualified sets and forbidden sets. The qualified set is a subset of n participants that can decrypt the secret image while a forbidden set is a subset of participants that can gain no information of the secret image. A more detailed discussion about visual cryptographic scheme with examples are given in the first part of chapter 3.

Until the year 1997, although the transparencies could be stacked to recover the secret image without any computation, the revealed secret images (as in [2] [3] [32] [48]) were all black

and white. In [63], Verheul and Van Tilborg used the concept of *arcs* to construct a colored visual cryptography scheme, where users could share colored secret images. The key concept for a c-colorful visual cryptography scheme is to transform one pixel to b sub-pixels, and each sub-pixel is divided into c color regions. In each sub-pixel, there is exactly one color region colored, and all the other color regions are black. The color of one pixel depends on the interrelations between the stacked sub-pixels. For example, if we want to encrypt a pixel of color c_i, we color region i with color c_i on all sub-pixels. If all sub-pixels are colored in the same way, one sees color c_i, when looking at this pixel; otherwise one sees black.

A major disadvantage of this scheme is that the number of colors and the number of sub-pixels determine the resolution of the revealed secret image. If the number of colors is large, coloring the sub-pixels will become a very difficult task, even though we can use a special *image editing package* to color these sub-pixels. How to stack these transparencies correctly and precisely by human beings is also a difficult problem. Another problem is that when the number of sub-pixels is b, the loss in resolution from the original secret image to the revealed image becomes b.

In [34], Hwang proposed a new visual cryptography scheme which improved the visual effect of the shares (the shares in their scheme were significant images, while those in the previous

scheme were meaningless images). Hwang's scheme is very useful when we need to manage a lot of transparencies; nevertheless, it can only be used in black and white images. For this reason, Chang, Tsai and Chen [24] proposed a new secret color image sharing scheme based on *modified visual cryptography*.

In that scheme, through a predefined Color Index Table (CIT) and a few computations they can decode the secret image precisely. Using the concept of modified visual cryptography, the recovered secret image has the same resolution as the original secret image in their scheme. However, the number of sub-pixels in their scheme is also proportional to the number of colors appearing in the secret image; i.e., the more colors the secret image has, the larger the shares will become. Another disadvantage is that additional space is needed to store the Color Index Table (CIT). In [25], Chang proposed a scheme wherein the size of the share is fixed and independent of the number of colors appearing in the secret image. Further, the pixel expansion was only 9, which was the least amongst the previously proposed methods. But this algorithm is applicable only for $(n,\ n)$ schemes. In paper [29], Tsai gives the concept of the sharing of the multiple secrets in the digital image.

2.3 General Secret Sharing Schemes

There are situations which require more complex access structures than the threshold ones. Shamir [53] discussed the case of sharing a secret between the executives of a company such that the secret can be recovered by any three executives, or by any executive and any vice-president, or by the president alone. This is an example of the so-called hierarchical secret sharing schemes. The Shamir's solution for this case is based on an ordinary $(3,\ n)-$ threshold secret sharing scheme. Thus, the president receives three shares, each vice-president receives two shares and, finally, every simple executive receives a single share.

The above idea leads to the so-called weighted (or multiple shares based) threshold secret sharing schemes. Benaloh and Leichter have proven in [5] that, there are access structures that cannot be realized using such schemes. We present next their example that proves this.

Example 2.3
Consider the access structure $\mathcal{A}$ defined by the formula $\mathcal{A}_{min} = \{AB, CD\}$, and assume that a threshold scheme is to be used to divide a secret value s among A, B, C, and D such that only those subsets of A, B, C, D which are in $\mathcal{A}$ can reconstruct s.

Let a, b, c, and d respectively denote the weight (number of shares) held by each of A, B, C, and D. Since A together with B

can compute the secret, it must be the case that $a + b \geq t$ *where* t *is the value of the threshold. Similarly, since* C *and* D *can together compute the secret, it is also true that* $c + d \geq t$*. Now assume without loss of generality that* $a \geq b$ *and* $c \geq d$*. (If this is not the case, the variables can be renamed.) Since* $a + b \geq t$ *and* $a \geq b, a+a \geq a+b \geq t$*. So* $a \geq t/2$*. Similarly,* $c \geq t/2$*. Therefore,* $a+c \geq t$*. Thus,* A *together with* C *can reconstruct the secret value* s*. This violates the assumption of the access structure.*

2.4 Applications

Most of the business organizations need to protect data from disclosure. As the world is more connected by computers, the hackers, power abusers have also increased, and most organizations are afraid to store data in a computer. So there is a need of a method to distribute the data at several places and destroy the original one. When a need of original data arises, it could be reconstructed from the distributed shares. Initially, when it was introduced, its goal was to present its customers a secure information storage media. Secret Sharing can provide confidentiality of the data base. For example, e-voting can be effectively implemented by secret sharing technique. It can ensure confidentiality. It aims to achieve the two somewhat divergent goals of data secrecy and data availability. If availability were the only goal, then simple duplication of the full data among n

places would prevent the loss of data upto $n-1$ places from erasing the secret. However, this would increase the threats also. Capturing any one place could disclose the secret to an adversary. If secrecy were the only goal, then solutions might include splitting the data into n pieces and storing each piece at each of the n places. This would require all n places accessible to get the secret. However, the destruction or alteration of any one piece would erase the distributed information. It ensures secrecy in the face of adversaries and yet achieves data integrity and availability with the cooperation of its shareholders. General concept of secret sharing is that, it doesn't want information to be centralized at one point. For example, in the preparation of plastic cards, such as ATM cards, it can provide good security. Presently, a vide range of its applications have been identified.

We present next the most important general secret sharing techniques.

2.5 Ito-Saito-Nishizeki Scheme

Ito, Saito, and Nishizeki [36] have introduced the so-called cumulative array technique for monotone access structures.

Definition 2.8

Let $\mathcal{A}$ be a monotone authorized access structure of size n and let $B_1, \ldots, B_m$ be the corresponding maximal unauthorized access

sets. The *cumulative array f*or the access structure $\mathcal{A}$, denoted by $\mathcal{C}^{\mathcal{A}}$, is the $n \times m$ matrix, $(\mathcal{C}^{\mathcal{A}}_{i,j})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$, where,

$$\mathcal{C}^{\mathcal{A}}_{i,j} = \begin{cases} 0, & \text{if } i \in B_j \\ 1, & \text{if } i \notin B_j \end{cases}$$

for all $1 \leq i \leq n$, and $1 \leq j \leq n$.

Let us consider now an arbitrary (m, m)-threshold secret sharing scheme with the secret S and the corresponding shares $s_1, \ldots, s_m$. In the $\mathcal{A}$-secret sharing scheme, the shares $I_1, \ldots, I_n$ corresponding to the secret S will be defined as

$$I_i = \{s_j | \mathcal{C}^{\mathcal{A}}_{i,j} = 1\},$$

for all $1 \leq i \leq n$.

Example 2.4

Let $n = 4$ *and* $\mathcal{A}_{min} = \{\{1, 2\}, \{3, 4\}\}$. *In this case, we obtain that* $\overline{\mathcal{A}}_{max} = \{\{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}\}$ *and* $m = 4$.

The cumulative array for the access structure $\mathcal{A}$ *is,*

$$\mathcal{C}^{\mathcal{A}} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

In this case, $I_1 = \{s_3, s_4\}$, $I_2 = \{s_1, s_2\}$, $I_3 = \{s_2, s_4\}$ *and* $I_4 = \{s_1, s_3\}$, *where* s_1, s_2, s_3, s_4 *are the shares of a (4, 4)-threshold secret sharing scheme with the secret* S.

2.6 Benaloh-Leichter Scheme

Benaloh and Leichter [5] have represented the access structures using formulae. More exactly, for a monotone authorized access structure $\mathcal{A}$ of size n, they defined the set $\mathcal{F}_{\mathcal{A}}$ as the set of formulae on a set of variables $\{v_1, v_2, \ldots, v_n\}$ such that for every $\mathcal{F} \in \mathcal{F}_{\mathcal{A}}$, the interpretation of $\mathcal{F}$ with respect to an assignation of the variables is true if and only if the true variables correspond to a set $A \in \mathcal{A}$. They have remarked that such formulae can be used as templates for describing how a secret can be shared with respect to the given access structure. Because the formulae can be expressed using only $\wedge$ operators and $\vee$ operators, it is sufficient to indicate how to "split" the secret across these operators.

Thus, we can inductively define the shares of a secret S with respect to a formulae $\mathcal{F}$ as follows:

$$Shares(S, F) = \begin{cases} (S, i), & \text{if } F = v_i,\ 1 \leq i \leq n; \\ \bigcup_{i=1}^{k} Shares(S, F_i), & \text{if } F = F_1 \vee \cdots \vee F_k; \\ \bigcup_{i=1}^{k} Shares(s_i, F_i), & \text{if } F = F_1 \wedge \cdots \wedge F_k, \end{cases}$$

where, for the case $F = F_1 \wedge F_2 \wedge \cdots \wedge F_k$, we can use any (k, k)-threshold secret sharing scheme for deriving some shares $s_1, \ldots, s_k$ corresponding to the secret S and, finally, the shares as $I_i = \{s | (s, i) \in Shares(S, F)\}$, for all $1 \leq i \leq n$, where, F is an arbitrary formula in the set $\mathcal{F}_{\mathcal{A}}$.

Example 2.5

Let $n = 3$ and an authorized access structure $\mathcal{A}$ given by

$\mathcal{A}_{min} = \{\{1,2\},\{2,3\}\}$. *For example, the formula* $F = (v_1 \wedge v_2) \vee (v_2 \wedge v_3)$ *is in the set* $\mathcal{F}_{\mathcal{A}}$. *In this case, Shares*$(S, F)$*, for some secret* S*, can be obtained as*

$$\begin{aligned} Shares(S,F) &= Shares(S, v_1 \wedge v_2) \cup Shares(S, v_2 \wedge v_3) \\ &= Shares(s_1, v_1) \cup Shares(s_{2,1}, v_2) \cup \\ &\quad Shares(s_{2,2}, v_2) \cup Shares(s_3, v_3) \\ &= \{(s_1,1),\ (s_{2,1},2),\ (s_{2,2},2),\ (s_3,3)\}, \end{aligned}$$

where, $s_1, s_{2,1}$ *and respectively,* $s_{2,2}, s_3$ *are shares of the secret* S *with respect to two arbitrary (2, 2)-threshold secret schemes. Thus, the shares corresponding to the secret* S *with respect to the access structure* $\mathcal{A}$ *are*

$$I_1 = \{s_1\},\ I_2 = \{s_{2,1}, s_{2,2}\} \text{ and } I_3 = \{s_3\}.$$

Example 2.6

Consider the access structure $\Gamma_{min} = \{P_1P_2P_3,\ P_1P_4\}$.
Let the secret $s \in GF(2^r)$.

A secret sharing scheme for Γ_{min}can be realized in the following way:
Randomly choose $x,\ y \in GF(2^r)$.
Compute z such that $s = (x + y + z) \pmod{2^r}$.
Let $a_1 = x;\ a_2 = y;\ a_3 = z$ and $a_4 = y + z \pmod{2^r}$.

Example 2.7

Consider the access structure $\Gamma_{min} = \{P_1P_2P_3,\ P_1P_2P_4\}$.
Let $s \in GF(2^r)$.

A secret sharing scheme for Γ_{min} can be realized in the following way:

Randomly choose $x, y \in GF(2^r)$.

Compute z such that $s = (x + y + z) \pmod{2^r}$.

Let $a_1 = x; a_2 = y; a_3 = z$ and $a_4 = z$.

Example 2.8

Consider the access structure $\Gamma_{min} = \{P_1P_2P_4,\ P_1P_3P_4,\ P_2P_3\}$.
Let $s \in GF(2^r)$.

A secret sharing scheme for Γ_{min} can be realized in the following way:

Randomly choose $x, y \in GF(2^r)$.

Let $a_1 = x; a_2 = s + y; a_3 = s - y$ and $a_4 = y - x$.

Remark 2.1

A share I_i may contain many sub-shares, one sub-share for every minimal access set to which i belongs. Thus, an ordering of these sub-shares is required in order to select the correct sub-share corresponding to a certain access set in the reconstruction phase.

Remark 2.2

They also proposed using general $threshold_{k,m}$[1] *operators in order*

[1]For $m \geq 1$, $1 \leq k \leq m$, $threshold_{k,m}$ denotes the formula

$$\bigvee_{1 \leq i_1 < i_2 < \ldots < i_k \leq i_k} \left(\bigwedge_{j=1}^{k} F_{i_j} \right).$$

Thus, $F_1 \vee F_2 \vee \ldots F_m = threshold_{1,m}(F_1, \ldots, F_m)$ and
$F_1 \wedge F_2 \wedge \ldots F_m = threshold_{m,m}(F_1, \ldots, F_m)$.

to construct smaller formulae, reducing in this way the size of the shares. In this case, the definition of $Shares(S, F)$ *can be extended for these operators as follows:*

$$Shares(S, F) = \cup_{i=1}^{m} Shares(s_i, F_i),$$

if $F = threshold_{k,m}(F_1, \ldots, F_m)$*, where* $s_1, \ldots, s_m$ *are the shares corresponding to the secret* S *with respect to an arbitrary* (k, m)*-threshold secret sharing scheme.*

Example 2.9

Let $n = 4$ *and a monotone authorized access structure* $\mathcal{A}$ *given by* $\mathcal{A}_{min} = \{\{2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}\}$*. For example, the formula* $F = (v_2 \wedge v_3) \vee (v_1 \wedge v_2 \wedge v_4) \vee (v_1 \wedge v_3 \wedge v_4)$ *is in the set* $\mathcal{F}_{\mathcal{A}}$*. Using the threshold operator, we can obtain a shorter formula, namely,* $(v_2 \wedge v_3) \vee threshold_{3,4}(v_1, v_2, v_3, v_4)$.

Example 2.10

Consider the access structure $\Gamma_{min} = \{P_1P_3P_4,\ P_1P_2,\ P_2P_3\}$.
Let $s \in GF(2^r)$.

A secret sharing scheme for Γ_{min} can be realized in the following way: Construct a (3,4) threshold scheme for the secret s and let $y_1, \ldots, y_4$ be the shares of this threshold scheme.
Let $a_1 = y_1;\ a_2 = y_2,\ y_4;\ a_3 = y_3$ and $a_4 = y_4$.

Example 2.11

Consider the access structure $\Gamma_{min} = \{P_1P_3P_4,\ P_1P_2,\ P_2P_3, P_2P_4\}$.
Let $s \in GF(2^r)$.

A secret sharing scheme for Γ_{min} can be realized in the following way:

Construct a (3, 5) threshold scheme for the secret s and let $y_1, \ldots, y_5$ be the shares of this threshold scheme.

Let $a_1 = y_1;\ a_2 = y_2,\ y_5;\ a_3 = y_3$ and $a_4 = y_4$.

Example 2.12

Consider the access structure $\Gamma_{min} = \{P_1P_2P_3,\ P_1P_2P_4,\ P_1P_3P_4\}$. *Let* $s \in GF(2^r)$.

A secret sharing scheme for Γ_{min} can be realized in the following way:

Randomly choose $x \in GF(2^r)$. Compute y such that $s = (x + y) \pmod{2^r}$. Construct a (2, 3) threshold scheme for the secret y and let $y_1, y_2 and y_3$ be the shares of this threshold scheme.

Let $a_1 = x; a_2 = y_1; a_3 = y_2$ and $a_4 = y_3$.

Example 2.13

Consider the access structure given by $\Gamma_{min} = \{P_1P_2, P_2P_3, P_3P_4, P_4P_5, P_5P_6, P_6P_7, P_7P_8, P_8P_1\}$. *Let* $s \in \{0, 1\}$.

Let the four distinct numbers $a, b, c, d \in B = \{0, 1, 2, 3\}$. Let $\mathcal{C}_0$ consists of all the 24 column matrices: [a a b b c c d d] and let $\mathcal{C}_1$ consists of all the 24 column matrices: [a b b c c d d a].

To share $s = 0$, the dealer randomly chooses one of the matrices in C_0, and to share $s = 1$, the dealer randomly chooses one of the matrices in C_1. The rows of chosen matrix defines shares given

to each one of the 8 participants.

Let $A = \{P_1P_2, P_3P_4, P_5P_6, P_7P_8\}$, and $B = \{P_2P_3, P_4P_5, P_6P_7, P_8P_1\}$. In this example, at the reconstruction stage, if $P_iP_j \in A$ and the value of the shares of P_i and that of P_j are equal or if $P_iP_j \in B$, and the value of the shares of P_i and that of P_j are not equal, the secret $s = 0$; otherwise secret $s = 1$.

2.7 Concluding remarks

In this chapter, the different research findings were analyzed and the efficiency aa well as the level of difficulty were brought out. Also discussed were, various examples to illustrate the secret sharing schemes in general.