Chapter 1

Secret Sharing Schemes

1.1 Introduction

Handling secret has been an issue of prominence from the time human beings started to live together. Important things and messages have been always there to be preserved and protected from possible misuse or loss. Some time secret is thought to be secure in a single hand and at other times it is thought to be secure when shared in many hands. Some of the formulae of vital combinations of medicinal plants or roots or leaves, in Ayurveda were known to a single person in a family. When he becomes old enough, he would rather share the secret formula to a chosen person from the family, or from among his disciples. There were times when the person with the secret dies before he could share the secret. Probably, similar incidents might have made the genius of those era to think of sharing the secrets with

more than one person so that in the event of death of the present custodian, there will be at least one other person who knows the secret.

Secret sharing in other forms were prevailing in the past, for other reasons also. Secrets were divided into number of pieces and given to the same number of people. To ensure unity among the participating people, the head of the family would share the information with respect to wealth among his children and insist that after his death, they all should join together to inherit the wealth.

To test the valor of the youth of a nation, a king, would hide treasure in some place in his kingdom and information about it would be placed in pieces at different places of varying grades of difficulty to reach. Only the brave and the intelligent would reach the treasure.

Military and defense secrets have been the subject matter for secret sharing in the past as well as in the modern days. Secret sharing is a very hot area of research in Computer Science in the recent past. Digital media has replaced almost all forms of communication and information preservation and processing. Security in digital media has been a matter of serious concern. This has resulted in the development of encryption and cryptography. Uniform secret sharing schemes form a part of this large study.

A Secret sharing scheme is a method of dividing a secret information into two or more pieces, with or without modifications, and retrieving the information by combining all or predefined sub collection of pieces.

The pieces of information are called **shares** and the process responsible for the division is called **dealer**. A predefined sub-collection of shares which contains the whole secret in some form is called an **allowed coalition**. The process responsible for the recovery of the secret information from an allowed coalition is called a **combiner**.

A share contains, logically, a part of the information, but will be of no use. Thus no single share is of any threat to the confidentiality of the secret information. It is also envisaged that after the dealer process is over, the original information can be destroyed forever. This would mean that even the person responsible for the dealer process will not be a threat, thereafter. The secret information is recovered from any allowed coalition using the recovery process called combiner. The combiner would be able to recover the secret information, only if, all shares in the allowed coalition is present and not with any fewer number of shares. Thus, in an allowed coalition, each member share is equally important such that without anyone of them, the secret information cannot be accessed.

Allowed coalition is also referred in the literature by other names too, such as, **authentic collection**, **qualified collection**

or **authorized set**. We, in our work, preferred to call the sub collection of shares as allowed coalition. The set of all allowed coalitions of participants is called the **access structure** and is usually denoted by Γ.

Secret Sharing is an important tool in Security and Cryptography. In many cases there is a single master key that provides the access to important secret information. Therefore, it would be desirable to keep the master key in a safe place to avoid accidental and malicious exposure. This scheme is unreliable: if master key is lost or destroyed, then all information accessed by the master key is no longer available. A possible solution would be that of storing copies of the key in different safe places or giving copies to trusted people. In such a case the system becomes more vulnerable to security breaches or betrayal [53], [30]. A better solution would be, breaking the master key into pieces in such a way that only the concurrence of certain predefined trusted people can recover it. This has proven to be an important tool in management of cryptographic keys and multi-party secure protocols (see for example [33]).

As a solution to this problem, Blakley [9] and Shamir [53] introduced $(k,\ n)$ threshold schemes. A $(k,\ n)$-threshold scheme allows a secret to be shared among n participants, in such a way that, any k of them can recover the secret, but $k-1$, or fewer, have absolutely no information on the secret.

Ito, Saito, and Nishizeki [36] described a more general method of secret sharing. An access structure is a specification of all subsets of participants who can recover the secret and it is said to be monotone if any set which contains a subset that can recover the secret, can itself recover the secret. Ito, Saito, and Nishizeki gave a methodology to realize secret sharing schemes for arbitrary monotone access structures.
Subsequently, Benaloh and Leichter [5] gave a simpler and more efficient way to realize such schemes.

An important issue in the implementation of secret sharing scheme is the size of the shares distributed to the participants, since the security of a system degrades as the amount of the information that must be kept secret increases. So the size of the shares given to the participants is a key point in the design of secret sharing schemes. Therefore, one of the main parameters in secret sharing is, the **average information rate** ρ, of the scheme, which is defined as the ratio between the average length (in bits) of the shares given to the participants and the length of the secret. Unfortunately, in all secret sharing schemes the size of the shares cannot be less than the size of the secret, and so the information rate cannot be less than one. Moreover, there are access structures, for which, any corresponding secret sharing scheme must give to some participant a share of size strictly bigger than the secret size. Secret sharing schemes with information rate equal to one are called **ideal**. A secret sharing

scheme is called efficient if the total length of the n shares is polynomial in n.

1.2 Principle of secret splitting

The simplest sharing scheme splits a message between two people. Consider the case where Daniel has a message M, represented as an integer, that he would like to split between two people Alice, and Bob, in such a way that neither of them alone can reconstruct the message. A solution to the problem readily lends itself: Choose a random number r. Then r and $M - r$ are independently random. He gives $M - r$ to Alice and r to Bob as their shares. Each share by itself means nothing in relation to the message, but together, they carry the message M. To recover the message, Alice and Bob have to simply add their shares together.

Here is another method in which Daniel splits a message between Alice and Bob:

1. Daniel generates a random-bit string R, of the same length as the message, M.
2. Daniel XORs M with R to generate S.
   i.e., $M \oplus R = S$.
3. Daniel gives R to Alice and S to Bob.
   To reconstruct the message, Alice and Bob have only one step to do:

4. Alice and Bob XOR their pieces together to reconstruct the message:

$$R \oplus S = M.$$

This technique is absolutely secure. Each piece, by itself, is absolutely worthless. Essentially, Daniel is encrypting the message with a one-time pad and giving the cipher text to one person and the pad to the other person. The one-time pad, which is an unbreakable cryptosystem, was developed by Gilbert Vernam and Joseph Mauborgne in 1917. It has perfect security [42]. No amount of computing power can determine the message from one of the pieces.

Shares can be constructed in several alternative forms using a random number. For example, $M - \frac{r}{2}$ and $M + \frac{r}{2}$ or Mr and $\frac{M}{r}$. Depending on the choice of constructing shares, suitable combiner has to be created.

It is easy to extend this scheme to more people:

Now let us examine the case where we would like to split the secret among three people. Any suitable splitting and combining method can be evolved. For example, the method employed for splitting the secret into two shares can be extended with the help of two random numbers r and s. For example, consider $M - r - s$, r and s as the three shares. To reconstruct the message M, simply add the shares. Similarly, we can evolve splitting and combining methods for a secret to be distributed as n shares with

the condition that only when all of them are combined together, the secret could be recovered.

Daniel divides up a message into $n(\geq 2)$ pieces:

1. Daniel generates $n-1$ random-bit strings $S_1, \ldots, S_{n-1}$ having the same length as the message, M
2. Daniel XORs M with $n-1$ random-bit strings to generate S_n:
   i.e., $M \oplus S_1 \oplus \ldots \oplus S_{n-1} = S_n$.
3. Daniel distributes the $S_i, (i = 1, \ldots, n)$ to the n participants.
4. The n participants working together can reconstruct the message:
   $S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1} \oplus S_n = M$.

Note: This protocol has a problem: If any of the pieces gets lost or is not available, the message cannot be reconstructed, since each piece is as critical to the message as every other piece.

1.3 History of Secret Sharing

In [43], Liu considered the following problem:

Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be

opened, if and only if, six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?

If we consider any five scientists together, there is a specific lock, which they cannot open. Consider a particular scientist. He must have the keys of those locks which cannot be opened by any five scientists from among the other ten scientists.

Among eleven scientists, five scientists can be selected in $\binom{11}{5} = 462$ ways, and among ten scientists, five scientists can be selected in $\binom{10}{5} = 252$ ways. (More details about one form of distribution of keys of the various locks to the scientists is included in Appendix 1.)

So, the minimal solution uses 462 locks and 252 keys per scientist. These numbers are clearly impractical, and they become exponentially worse when the number of scientists increases. Moreover, the secret documents are always as a single entity and is not being involved in the method. Since the secret is always in one piece, the level of security is low to that extent. The security in this case is solely depending on the locks and the keys. However, the cabinet with the document as a whole is at great risk.

1.3.1 Threshold scheme

In 1979 Shamir [53] and Blakley [9] introduced the concept of sharing of the secret message as a means and a method of making the message secure. Under this scheme, the message M is divided into n pieces $M_1, M_2, M_3, \ldots, M_n$, with or without transformation of the message, in such a way that, for a specified k, $(2 \leq k \leq n)$,

1. knowledge of any k or more pieces-M_i makes M computable;
2. knowledge of any $k-1$ or fewer M_i pieces leaves M completely undetermined (in the sense that all its possible values are equally likely).

Such a scheme is called a $(k,\ n)$-threshold scheme. The parameter $k \leq n$ is called the threshold value.

1.3.2 The Shamir Secret Sharing Scheme

Let $k,\ n \in \mathbb{Z}, k \leq n$. We will describe the $(k,\ n)$ Secret Sharing Scheme by Shamir. It uses a prime number, p, which is greater than n and the set of possible secret. The scheme is based on the following lemma.

Lemma 1.1

Let $k \in \mathbb{Z}$. Also let $x_i, y_i \in \mathbb{Z}/_p\mathbb{Z}, 1 \leq i \leq k$, where the

x_i are pairwise distinct. Then there is a unique polynomial $b \in (\mathbb{Z}/_p\mathbb{Z})[X]$ *of degree* $\leq k-1$ *with* $b(x_i) = y_i$, $1 \leq i \leq k$.

Proof: The Lagrange interpolation formula yields the polynomial

$$b(X) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{(x_j - X)}{(x_j - x_i)} \tag{1.1}$$

It satisfies $b(x_i) = y_i$, $1 \leq i \leq k$. This shows that at least one polynomial exists with the asserted properties. Now we determine the number of such polynomials.

Let $b \in (\mathbb{Z}/_p\mathbb{Z})[X]$ be such a polynomial. Write

$$b(X) = \sum_{j=0}^{k-1} b_j X^j, \quad where,\ b_j \in \mathbb{Z}/_p\mathbb{Z},\ 0 \leq j \leq k-1.$$

From $b(x_i) = y_i$, $1 \leq i \leq k$, we obtain the linear system

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_k & x_k^2 & \dots & x_k^{k-1} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{k-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{k-1} \end{bmatrix} \tag{1.2}$$

The coefficient matrix

$$U = \begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_k & x_k^2 & \dots & x_k^{k-1} \end{bmatrix}$$

is *Vandermonde matrix.* Its determinant is

$$det\, U = \prod_{1 \leq i < j \leq k} (x_i - x_j).$$

Since the x_i are distinct by assumption, the determinant is non zero. So the rank of U is k. This implies that the kernel of the coefficient matrix (1.2) has rank 0, and the number of solutions of our linear system is $p^0 = 1$. Hence the uniqueness. Now we are able to describe the scheme.

1.3.3 System Design

The dealer chooses a prime number p, which is greater than n and the set of possible secret and nonzero distinct elements $x_i \in \mathbb{Z}/_p\mathbb{Z}$, $1 \leq i \leq n$. Those elements in $\mathbb{Z}/_p\mathbb{Z}$ can, for example, be represented by their least nonnegative representative.

The shares

Let $S \in \mathbb{Z}/_p\mathbb{Z}$ be the secret.

1. The dealer secretly at random chooses elements $b_j \in \mathbb{Z}/_p\mathbb{Z}$, $1 \leq i \leq k-1$ and constructs the polynomial

$$b(X) = \sum_{i=1}^{k-1} b_i x^i + S. \tag{1.3}$$

   It is of degree $\leq k-1$.

2. The dealer computes the shares $y_i = b(x_i),\ 1 \leq i \leq n$.

3. The dealer distributes the share (x_i, y_i) to the i^{th} shareholder, $1 \leq i \leq n$.

So the secret is value $b(0)$ of the polynomial $b(X)$.

Reconstruction of the secret

Suppose that k shareholders collaborate. Without loss of generality assume that the shares are numbered, such that, $y_i = b(x_i)$, $1 \leq i \leq k$ with the polynomial b[X] from (1.3). Now we have

$$b(x) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{x_j - X}{x_j - x_i} \tag{1.4}$$

In fact this polynomial satisfies $b(x_i) = y_i$, $1 \leq i \leq k$ and by lemma 1.1 there is exactly one such polynomial of degree $\leq k-1$. Therefore, the shareholders can reconstruct the secret as

$$S = b(0) = \sum_{i=1}^{k} y_i \prod_{j=1, j\neq i}^{k} \frac{x_j}{x_j - x_i} \tag{1.5}$$

1.3.4 A method of solution

Now a secret is shared by computing points on a random polynomial in $(\mathbb{Z}/_p\mathbb{Z})[X]$. So first we must find a way of representing the "plaintext" secret as a set of class modulo p. This is not really part of secret sharing process; it is merely a way to prepare the secret so that it can be shared. To keep the things as simple as possible, we will assume that the "plaintext" secret contains only words written in uppercase letters. Thus the secret is ultimately a sequence of letters and blank spaces. The first step consists of

replacing each letter of the secret by a number, using the following correspondence:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

The blank space between words is replaced by 99. Having done that, we obtain a number, possibly a very large one, if the secret is large. However it is not a number we want, but rather classes modulo p. Therefore, we must break the numerical representation of the secret into a sequence of positive integers, each smaller than p. These are called the *blocks* of the secret.

For example, the numerical representation of the proverb "A SMALL LEAK WILL SINK A GREAT SHIP" is

$$1099282210212199211410209932182121992818232099109916271410299928171825$$

If we choose the prime $p = 9973$, the numerical representation of the proverb above must be broken into blocks smaller than 9973. One way to do this is as follows:

$$1099\text{-}2822\text{-}1021\text{-}2199\text{-}2114\text{-}1020\text{-}9932\text{-}1821\text{-}2199\text{-}$$
$$2818\text{-}2320\text{-}9910\text{-}9916\text{-}2714\text{-}1029\text{-}9928\text{-}1718\text{-}25$$

When secret is reconstructed, one obtains a sequence of blocks. The blocks are then joined together to give the numerical representation of the secret. It is only after replacing the numbers by letters, according to the table above, that one obtains the original secret.

Note that we have made each letter correspond to a *two-digit number* in order to avoid ambiguities. For example, if we had numbered the letters so that A corresponds to 1, B to 2, and so on, then we wouldn't be able to tell whether 12 stood for AB or for the letter L, which is the twelfth letter of the alphabet.

Of course, any convention that is unambiguous can be used instead of the one above. For example, one might prefer to use ASCII code, since the conversion of characters is automatically done by the computer.

Example 1.1

Let us return to the example we considered above. We choose $p = 9973$. *To construct a (3, 5)-threshold scheme, where any three of five people can reconstruct* S, *suppose the dealer chooses* $x_i = i, 1 \leq i \leq 5$. *Also assume that the randomly selected coefficients* b_2 *and* b_1 *are 1572 and 7583 respectively.*

Thus to share the first block of the secret, we must compute the polynomial,
$F(x) = 1572x^2 + 7583x + 1099 \pmod{9973}$ at each x_i. Thus the five shares of the first block are:

$$
\begin{aligned}
s_1 &= F(1) = 1572.1^2 + 7583.1 + 1099 \equiv \ \ 281 \pmod{9973} \\
s_2 &= F(2) = 1572.2^2 + 7583.2 + 1099 \equiv 2607 \pmod{9973} \\
s_3 &= F(3) = 1572.3^2 + 7583.3 + 1099 \equiv 8077 \pmod{9973} \\
s_4 &= F(4) = 1572.4^2 + 7583.4 + 1099 \equiv 6718 \pmod{9973} \\
s_5 &= F(5) = 1572.5^2 + 7583.5 + 1099 \equiv 8503 \pmod{9973}
\end{aligned}
$$

Sharing the whole secret, we have the following sequence of blocks:

$$
\begin{aligned}
s_1 &= 281\text{-}2004\text{-}203\text{-}1381\text{-}1296\text{-}202\text{-}9114\text{-}1003\text{-}1381\text{-} \\
&\quad 2000\text{-}1502\text{-}9092\text{-}9098\text{-}1896\text{-}211\text{-}9110\text{-}900\text{-}9180. \\
s_2 &= 2607\text{-}4330\text{-}2529\text{-}3707\text{-}3622\text{-}2528\text{-}1467\text{-}3329\text{-}3707\text{-} \\
&\quad 4326\text{-}3828\text{-}1445\text{-}1451\text{-}4222\text{-}2537\text{-}1463\text{-}3226\text{-}1533. \\
s_3 &= 8077\text{-}9800\text{-}7999\text{-}9177\text{-}9092\text{-}7998\text{-}6937\text{-}8799\text{-}9177\text{-} \\
&\quad 9796\text{-}9298\text{-}6915\text{-}6921\text{-}9692\text{-}8007\text{-}6933\text{-}8696\text{-}7003. \\
s_4 &= 6718\text{-}8441\text{-}6640\text{-}7818\text{-}7733\text{-}6639\text{-}5578\text{-}7440\text{-}7818\text{-} \\
&\quad 8437\text{-}7939\text{-}5556\text{-}5562\text{-}8333\text{-}6648\text{-}5574\text{-}7337\text{-}5644. \\
s_5 &= 8503\text{-}253\text{-}8425\text{-}9603\text{-}9518\text{-}8424\text{-}7363\text{-}9225\text{-}9603\text{-} \\
&\quad 249\text{-}9724\text{-}7341\text{-}7347\text{-}145\text{-}8433\text{-}7359\text{-}9122\text{-}7429.
\end{aligned}
$$

Let us see how a block of a secret can be reconstructed from the three shares. For example, the first block of S can be reconstructed from the first blocks of the shares s_2, s_3 and s_5 by using the formula (1.5):

$$
\begin{aligned}
b[0] &= \frac{2607.3.5}{1.3} + \frac{8077.2.5}{-1.2} + \frac{8503.2.3}{-3.-2} \pmod{9973} \\
&= 2607.5 + 8077.(-5) + 8503 \pmod{9973} \\
&= -18847 \pmod{9973} \\
&= 1099
\end{aligned}
$$

Similarly each block can be reconstructed.

It may be noted that, we are working with prime modulo p, in which, the numbers that appear in the denominators of formula (1.5), have inverses. We can use the Extended Euclidean Algorithm to find the inverse: $m^{-1} \pmod{p}$, where, $m \not\equiv 0 \pmod{p}$. The algorithm and an example are given as Appendix 2.

For example, suppose we want to construct the first block of the secret from s_1, s_2 and s_5. Here,

$$\begin{aligned}
b[0] &= \frac{281.2.5}{1.4} + \frac{2607.1.5}{-1.3} + \frac{8503.1.2}{-4.-3} \pmod{9973} \\
&= \frac{281.5}{2} + \frac{2607.5}{-3} - \frac{8503.1}{-6} \pmod{9973} \\
&= \frac{281.(15) - 2607.10 + 8503}{6} \pmod{9973} \\
&= \frac{-13352}{6} \pmod{9973} \\
&= -13352 * 8311 \pmod{9973} \\
&\qquad [because\, 6^{-1} \equiv 8311 \pmod{9973} \\
&= -110968472 \pmod{9973} \\
&= 1099 \pmod{9973}
\end{aligned}$$

1.4 Concluding remarks

We have seen the development of the subject from the simple case of (2, 2) sharing to the general $(k,\ n)$ sharing. Some examples

are also given. The chapter also contains an algorithm for the key allotment. We have included simple examples to highlight the various aspects of the existing sharing schemes.