

Cryptographic Secret Sharing: Shamir's and Blakley's Schemes

Jeremy Joseph Hanniel - 13510026¹

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganessa 10 Bandung 40132, Indonesia

¹evcrest@gmail.com

Abstract—Since long ago, sensitive information is made secret by traditional methods of preferring either great confidentiality and reliability; each having its own risk. In 1979, Adi Shamir and George Blakley independently addressed this problem by their invention of secret sharing, a method to keep sensitive information with distributed key and high confidentiality. This paper gives information regarding their secret sharing schemes that generalize into (k, n) -threshold scheme.

Index Terms—secret sharing, threshold scheme, Shamir's scheme, Blakley's scheme

I. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. The term cryptography itself is originated from Greek and has meanings of hidden or secret ^[2]. The principal of cryptography is to convert original information called *plaintext* through one of the many means into a concealed, incomprehensible form called *ciphertext* to make the information a secret. This act is called *encrypting*, while the act of converting the information from the *ciphertext* back into the *plaintext* is called *decrypting*. To either encrypt or decrypt the information, we need something that is called a *key*, which is also made secret. Such thing is done so that only two parties who know the key can learn of the information and not the unwanted third party.

When storing the encryption key, one must choose between keeping a single copy of the key in one location for maximum confidentiality and keeping multiple copies of the key in different locations for maximum reliability so that the key would not be easily lost. This is where traditional methods which can only fulfill one of the two become potentially dangerous for storing highly sensitive and confidential information such as missile launch codes and numbered bank accounts ^[3]. In both cases, if the key is obtained by the third party from either the first or second party, then the information would be easily unveiled. This means anyone can have access to the information as long as they know of the key. On one side, in the case where we prefer maximum confidentiality, all parties within the communication network have to refer to

the key from a single location which is of course, inefficient. On the other side, in the case where we aim for maximum reliability where numerous copies of the key exist and scattered, just for unwanted parties to get the key from one of the locations would reveal the whole piece of information. That way, additional attack vectors are created and the leakage of the key would all come down to how well a source guards it. Attacking only the least secure location would be sufficient to practically get their hands on the information. This is where secret sharing comes into play as it can address this problem, allowing arbitrarily high levels of confidentiality and reliability to be achieved ^[3].

II. CRYPTOGRAPHIC SECRET SHARING

Secret sharing refers to the method for distributing a secret amongst a group of participants, each of whom is allocated a share/part of the secret. The secret can be constructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. Formally put, in secret sharing there is one *dealer* and n *players*. Each of the players is by the dealer given a share of the key in secrecy so that any group of t or more players can together reconstruct the secret. However, the secret cannot be reconstructed by any number of shares below t . Such system is called a (t, n) -threshold scheme ^[3].

For example, let's take "cryptography" as the secret and 4 players from a total of 10 to be given 4 shares. The dealer gives a portion/share of the secret to each of the 4 players such that player 1 holds "cry-----" as his share, player 2 holds "---pto-----", and so on. This way, a player with no shares can only learn that the secret is 12 letters long. He has to figure out the secret by trying all combinations of 12 letters, which at worst counts to 26^{12} trials. A player with 1 share, however, only has to figure out the remaining 9 letters he does not know which at worst counts to 26^9 trials. We can see from this example that only if no less than 4 shares are combined that the secret would be exposed completely. This is what secret sharing is basically about. Methods used in secret sharing are called secret sharing schemes; and this example counts as one of them.

Even though the method applied in the above example is already better than traditional methods, it still is not a perfect and secure secret sharing scheme. Notice that a player with even no shares at all is able to obtain some significant information about the secret. The condition of a perfect and secure secret sharing scheme is that no information regarding the secret would be revealed even though a player is only missing one share. If applied in the example above, even a player with 3 shares would still have to try all combination of 12 characters, not the remaining 3 he does not know. Formally put, if any subset of 10 players that is not included in the 4 players with shares cannot determine any information about the secret, then the secret sharing method is said to be perfect^[3].

If we have a secret sharing method in which S is the set of possible secrets and T is the set of possible shares, we define the *information rate* ρ as

$$\rho = \frac{\log|T|}{\log|S|}$$

If the secret is a random element of $GF(q)$ and all shares are elements of $GF(q)$ too, then the information rate is 1. A secret sharing method is said to be *ideal* if it is perfect and has information rate 1^[6].

Though secret sharing schemes might look effective, there are limitations that come with them. The size of combined t shares that are needed to unlock the secret s must be of the same size as s itself. However, this does not mean that all shares must be of the same size as s as this would result in an imperfect secret sharing scheme as stated above. Also, all secret sharing schemes use random bits^[3].

III. THRESHOLD SCHEMES

There are many examples of (t, n) -threshold schemes. There are 2 cases of threshold schemes: one where $t = n$ and another where $t < n$. To better understand the 2 cases, let's look at the examples below.

Highly sensitive data such as the code to arm and launch a nuclear missile is usually distributed in fragments among high-ranking military officers. Only they know the code and no one else beside themselves can figure out the code. However, an officer would not know whatever fragments of the code that other officers possess. When the decision to launch the nuke is made, all of those officers must confirm to the idea and combine the fragments each of them hold to construct the full code to launch the nuke. This is one example of $t = n$ case where all n players are necessary to construct the secret s . Again, this is another example of perfect secret sharing scheme where the nuke will not be able to launch if not all n officers confirm to the idea. There is not even partial info that can be revealed from the $x < t$ shares regarding s .

Another example is when each share consists of random integer r_i where $1 \leq i \leq n$ and the secret s is constructed from the sum of all random integer r_i . This means that no less than $i = n$ players must participate to construct the secret. In this case, we cannot possibly guess

the secret s even if we are only missing one r_i since the possibility will be too large. The same case is when each share consists of random bit length b_i where again i ranges from 1 to n . We would not know how many bits the secret s consists of unless we know all b_i . Cases where all n is necessary to construct the secret s are called n -out-of- n sharing^[1].

Now let's assume that we need to cancel the nuke from launching after being armed. Since the launching can be fatal in many ways when the reason to do so becomes lacking, the cancellation of the launch must be done immediately and in the least complex way as possible. For example, only one fragment of the code is needed to cancel the launch. This can be done by distributing a common abort code to all n officers. We can see from this case that the not all n is necessary to cancel the nuke. This is one example of secret sharing schemes where $t < n$. In this particular case when one share is already enough to uncover the secret s , the secret sharing is called 1-out-of- n sharing. Moreover, the distribution of the common code (all n players have the same share as the secret s) made the case what is called trivial sharing^[1].

Let's take a look on the last example. Launching a tactical weapon such as a nuclear missile is a very hard decision and is used as the last resort and that is why in reality not all officers would simply agree to the idea. Even so, if the majority of them agree, then the nuclear missile will be launched. This means that not all n officers are needed to construct the code. Let's assume that the nuke will be launched when more than 60% of the officers from a total of 20 concur. That means $t \geq 12$ and $n = 20$. Remembering that the fragment of code given to each officer is unique, we realize that the code will be unique depending on which combination of $x \geq 12$ officers concur.

Threshold sharing is originally found by both Adi Shamir and George Blakley, independent of each other, in 1979^[4]. This is the reason why both of them has separate scheme to address the confidentiality vs. reliability problem at that time despite using the same principles. We will go into greater details of their schemes in the two chapters ahead.

IV. SHAMIR'S SECRET SHARING SCHEME

Shamir's secret sharing scheme follows the (k, n) -threshold scheme (k is different from t only in name) where knowing as few as k shares will construct the secret s whereas knowing at most $k - 1$ will reveal no information about secret S . The essential idea of Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points to define a parabola, 4 points to define a cubic curve, and so forth. That is, it takes k points to define a polynomial of degree $k - 1$ ^[3].

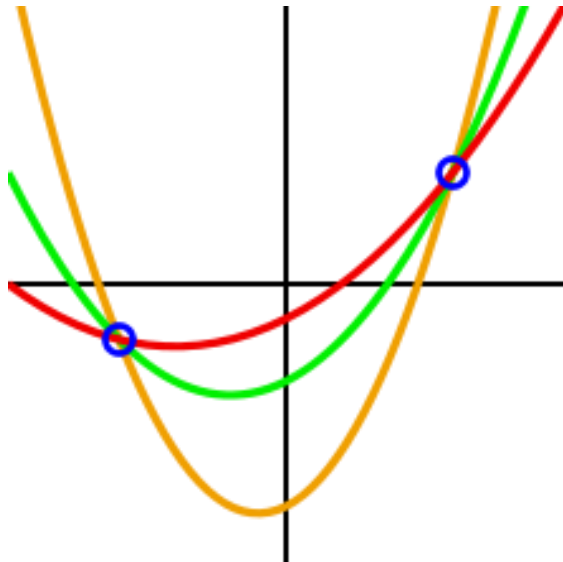


Figure 1 – Polynomials Building

One can draw an infinite number of polynomials of degree 2 through 2 points. 3 points are required to define a unique polynomial of degree 2. Not that this is not a representation of Shamir's scheme, but only an illustration to depict its principles over a finite field [4].

Shamir's scheme is based on the following observation. Let F_q be a finite field, that is, $(x_i, y_i) \in F_q \times F_q$ where $1 \leq i \leq k$ and all x_i 's are distinct. There is a unique polynomial $p(x)$ of degree $k - 1$ such that $p(x) = y_i$ for $1 \leq i \leq k$. Moreover, there are q polynomials of degree $k - 1$ satisfying $p(x_i) = y_i$ for $1 \leq i \leq k - 1$.

Assume that we represent the secret as an element a of F_q . We pick a random polynomial $p(x) \in F_q[x]$ such that $p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_{k-1}x^{k-1}$ where $a = a_0 = S$. If we want to share the secret with n shareholders, then we pick any $n \geq k$ distinct elements from F_q . The shares are calculated as pairs which is $K_i = (x_i, p(x_i)) = (x_i, y_i)$ [8]. Given any subset k of these pairs, we can find the coefficients of the polynomial using Lagrange interpolation [4].

Let's take a look at the example below. However, the example is not done through finite field arithmetic, but instead integer arithmetic so to better understand the scheme in a simple way. Therefore, it is not really a true example of Shamir's secret scheme and does not hold perfect secrecy [4].

- 1) First, we need to prepare the shares from the secret S .
- 2) Suppose that our secret is 1234, that is, $S = 1234$.
- 3) We wish to distribute the secret to 6 people so we pick $n = 6$, where any subset of 3 parts ($k = 3$) is sufficient to reconstruct the secret S .
- 4) We pick two random numbers, which is 166 and 94.
- 5) Therefore, our polynomial becomes:

$$p(x) = 1234 + 166x + 94x^2$$
- 6) Then, from above polynomial we construct 6 points of $(x, p(x))$ where $x \leq n$:
 - $x = 1$ yields $p(x) = 1494$, thus the 1st point is (1, 1494)

$x = 2$ yields $p(x) = 1942$, thus the 1st point is (2, 1942)
 $x = 3$ yields $p(x) = 2578$, thus the 1st point is (3, 2578)
 The same process is used to get the 3 remaining points which are (4, 3402); (5, 4414); (6, 5614).

- 7) We give each participant a different single point, both x and $p(x)$.
- 8) The next step is to reconstruct the secret. In order to do this, any 3 points of the above will suffice.
- 9) Let us choose 3 points out of the 6 points:

$$(x_0, y_0) = (2, 1942)$$

$$(x_1, y_1) = (4, 3402)$$

$$(x_2, y_2) = (5, 4414)$$

10) Then we will compute the Lagrange basis polynomials:

$$l_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 4}{2 - 4} \cdot \frac{x - 5}{2 - 5}$$

$$= \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$l_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{4 - 2} \cdot \frac{x - 5}{4 - 5}$$

$$= -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$l_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{5 - 2} \cdot \frac{x - 4}{5 - 4}$$

$$= \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

11) Therefore, we get

$$p(x) = \sum_{j=0}^2 y_j \cdot l_j(x)$$

$$= 1942 \cdot \left(\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3} \right) + 3402 \cdot \left(-\frac{1}{2}x^2 + \frac{7}{2}x - 5 \right) + 4414 \cdot \left(\frac{1}{3}x^2 - 2x + \frac{8}{3} \right)$$

$$= 1234 + 166x + 94x^2$$

12) Recall that the secret is the free coefficient, which means that $S = 1234$.

Here are some of the useful properties of Shamir's (k, n)-threshold scheme:

- 1) It is secure according to information theoretic security.
- 2) It is minimal: the size of each share does not exceed the size of the secret.
- 3) It is extensible in a way that when k is kept fixed, x_i shares can be dynamically added or deleted without affecting the other shares.
- 4) Security can be easily enhanced without changing the secret. It can be done by changing the polynomials occasionally or by constructing new shares.
- 5) We can distribute each player with different number of shares depending on their importance. For example, a high-ranking military officer can open a confidential file alone whereas normally it requires a few middle-ranking military officers.

Even so, the Shamir's secret sharing scheme which follows (k, n) -threshold scheme also has its drawbacks; one of which is the dense access structure of the system. Tracing it back to which players construct the secret using their shares are difficult to do. This is sometimes crucial to find out from where the secret happened to leak out. This weakness motivated the invention of other secret sharing schemes which have better access structures [7].

V. BLAKLEY'S SECRET SHARING SCHEME

Blakley's secret sharing scheme also follows the (k, n) -threshold scheme just like Shamir's. At least k shares are needed from a total of n shares to discover the secret S . One of its main differences from Shamir's secret sharing scheme is its geometric nature. The essential idea of Blakley's scheme is simple: the secret S is the intersection point of n -dimensional hyperplanes in an m -dimensional space. n shares are constructed with each share defining a dimensional hyperplane [5]. Each player is given enough information to define a hyperplane; the secret is recovered by calculating the planes' point of intersection and then taking a specified coordinate of that intersection [3]. For better understanding, let's look at Fig. II of 3-dimensional space below.

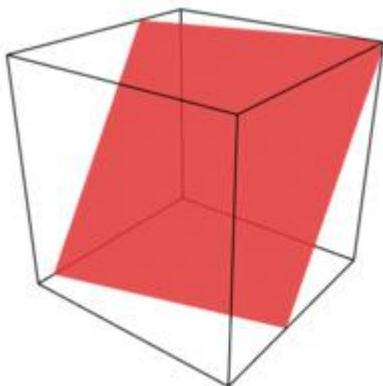


Figure II (a) – Each player is given enough information to define his dimensional hyperplane.

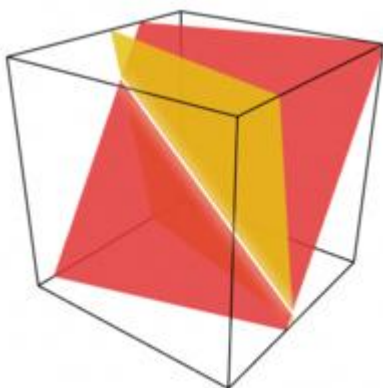


Figure II (b) – When 2 players combine their own 2 dimensional hyperplanes in the 3-dimensional space, the intersection between the two is formed as a line.

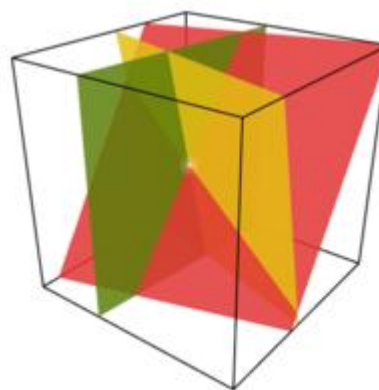


Figure II (c) – When threshold $k = 3$ is fulfilled, the intersection line becomes the intersection point, whose coordinates in the space is the secret S .

From Fig.II, we can learn that for any n shares in $m > 2$ dimensional space, the shareholder will directly know that the intersection point which is the secret S must be a point on his dimensional hyperplane [5]. It means that the shareholder can gain more knowledge than the outsider. This case is almost like our first example in chapter I where a player with even 0 shares is able to gain partial info about the secret. Therefore, it can be said that Blakley's secret sharing scheme is not perfect. This way, the system no longer has information theoretic security. Recall that a secret sharing scheme is perfect when the shareholders knows nothing more than non-shareholders; only when a number of sufficient shareholders combine their shares will they gain info of the secret. Then again, this scheme can be perfect for secrets in 2-dimensional space (i.e. the secret must lie on the y-axis). Let's examine Fig. III below for better comprehension [3].

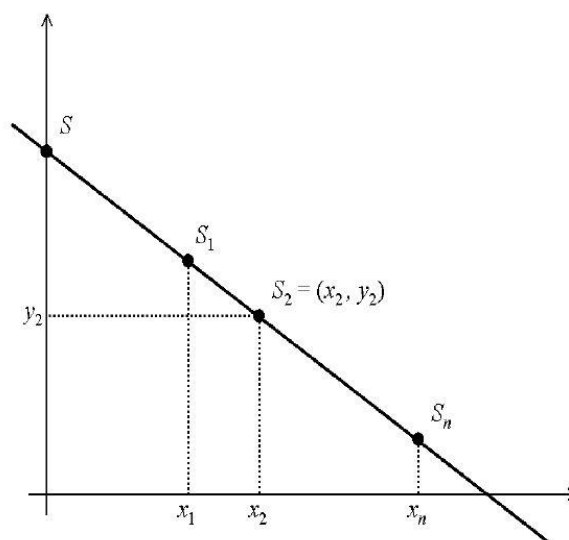


Figure III – In 2-dimensional space, the secret is defined only if 2 shares are combined. Any less than 2 shares will only conclude that the secret can be any point on y-axis.

Note that in an m -dimensional space, different

intersecting $n = k$ -dimensional hyperplanes also yields different intersection point. As Blakley's secret sharing scheme follows the (k, n) -threshold scheme, its drawbacks are very much alike with those of Shamir's scheme. One drawback special to the Blakley's scheme is that it is less space-efficient than Shamir's. Shamir's shares are each only as large as the original secret, Blakley's shares are k times larger. Blakley's scheme can be tightened by adding restrictions on which planes are usable as shares. The resulting scheme is equivalent to Shamir's polynomial system^[3].

VI. CONCLUSION

If we look from security perspective, it is obvious that secret sharing schemes are more favorable than traditional methods. By sharing secret using Shamir's and Blakley's scheme, we can maintain high levels of both confidentiality and reliability. Even so, the 2 schemes are now outdated and continually-expanding needs demands more versatile secret sharing schemes. Still, it is a starting point for developers in this subject to learn these 2 schemes before applying their creative idea into the world of cryptography.

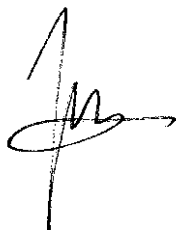
REFERENCES

- [1] <http://www.cs.berkeley.edu/~daw/teaching/cs276-s04/22.pdf>
Accessed on Dec 12th, 2011 at 06.00
- [2] <http://en.wikipedia.org/wiki/Cryptography>
Accessed on Dec 11th, 2011 at 15.25
- [3] http://en.wikipedia.org/wiki/Secret_sharing
Accessed on Dec 11th, 2011 at 11.41
- [4] http://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing
Accessed on Dec 11th, 2011 at 11.44
- [5] <http://x5.net/faqs/crypto/q105.html>
Accessed on Dec 11th, 2011 at 11.48
- [6] E. F. Brickell, *Some Ideal Secret Sharing Schemes*. Albuquerque: Springer-Verlag, 1998.
- [7] Hakan Ozadam, "Construction of Secret Sharing Schemes Using Linear Codes," unpublished.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Desember 2011



Jeremy Joseph Hanniel – 13510026