A Freely Modifiable Secret Sharing

An Extension to Shamir Secret Sharing for Achieving Independtly Modifiable Secret Share

Calvin Sadewa
IF-ITB
Bandung, Indonesia
Master23680@gmail.com

***Abstract*—This paper propose an extension to Shamir's secret sharing to support freely modifiable secret part, which mean a way to change one or more secret part without affecting other secret part. the key idea is to make a part which act as balancer to change that made**

Keywords—secret sharing, shamir secret sharing, public part, interpolation theorem, free modification.

I. Introduction

Secret sharing has become more popular since its introduction by Shamir, it deals on how to distribute secret to n participant in such way that k number of participant needed to reconstruct the secret. However, Shamir secret sharing does not provide a way to change one part of secret without changing others part of secrets. The property of changing one part maybe desirable in some, such as in password or changing the secret itself. A naïve idea is to separate the changeable part and the secret part, this idea may manifest as using password or a decryption key to get the secret part. this idea require space equal to the number of shared secret (n). another limitation that the secret part is not truly changeable. This paper describe an extension to Shamir secret sharing by adding public modifiable part to freely change a secret part.

II. Theory

A. *Secret sharing*

Secret sharing refers to any method for distributing a secret among a group of participants, each of which allocates a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. Threshold scheme (k,n) is a form of secret sharing, which distribute secret to n participant, and need at least k participant to reconstruct the secret.

B. *Shamir secret sharing*

Shamir secret sharing is a type of threshold scheme (k,n) that rely on polynomial interpolation, the algorithm is as followed :

1. Let s as secret, and choose any prime $p > \max(s,n)$
2. Choose $a_1, a_2, \dots a_{k-1}$, $0 > a_i > p$ for all i.
3. Let $q(x) = s + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}$
4. Let $D_i = q(i) \bmod p$, for all $0 < i < n+1$

The secret share is distributed in a tuple (i, D_i) to all participant. Based on interpolation theorem, to reconstruct q(x) (and subsequently s) needed k points (participant).

1. Secure: of any number of secret parts lesser than k, no information about secret s can be extracted.
2. Minimal: The size of each piece does not exceed the size of the original data.
3. Extensible: When k is kept fixed, secret share pieces can be dynamically added or deleted without affecting the other pieces.
4. Dynamic: Security can be easily enhanced without changing the secret, but by changing the polynomial occasionally (keeping the same free term) and constructing new shares to the participants.
5. Flexible: This scheme can be used in another scheme without much difficulties

III. Proposed Extension

Based on Shamir secret sharing, the extension add a modifiable public part. The algorithm for special case threshold(n,n) is as followed :

1. Let s as secret, and choose any prime $p > \max(s,n)$
2. Choose $a_1, a_2, \dots a_n$, $0 > a_i > p$ for all i.
3. Let $q(x) = s + a_1x + a_2x^2 + \dots + a_nx^n$
4. Let $D_i = q(i) \bmod p$, for all $0 < i < n+1$

5. Let public part be (n+1, q(n+1) mod p)

The polynomial in this scheme is in order n, rather than typical n-1 in Shamir's scheme, this is as direct consenquence of interpolation theorem which state to interpolate a k-order polynomial, one need to have k+1 points. In our case, we have n points and secret s (which can be treated as a point on x = 0), so we can interpolate a n-order polynomial. We can change a point (one of the n points or secret s) without affecting other point. Because the secret s is unknownable before the interpolation and we only have n points, we need additional point, which become the public part.

Modification of a secret part require n part, the algorithm is as followed :

1. Get the secret s by using Shamir secret reconstruction algorithm with n part and the public part.
2. Make the modification to the point, i.e (1,4) => (1,5). The modification is only allowed at the y component
3. Get q(x), the polynomial function, from interpolating the n point and secret point (0,s)
4. Let the new public part be (n+1, q(n+1) mod p)

In the modification, every change made do not affect other secret part, only the public part and the modified part.

From the special case of threshold (n,n), we can extend for a more general case of threshold (k,n), the algorithm is as followed :

1. Let s as secret, and choose any prime p > max(s,n)
2. Choose $a_1, a_2, \dots a_n, 0 > a_i > p$ for all i.
3. Let $q(x) = s + a_1x + a_2x^2 + \dots + a_nx^n$
4. Let $D_i = q(i*2+1) \bmod p, 0 < i < n+1$
5. Let public part $P_i = q(i*2), 0 < i < n-k+1$

The polynomial in this scheme is in order n, same as the special case of threshold (n,n), the difference is how the secret part and the public part generated, the amount of public part increase according to k because consequence of interpolation theorem and the threshold scheme, that one need a n + 1 points to interpolate n-order polynomial, with only k secret part, one need n-k+1 public part to interpolate the polynomial.

The modification step for this threshold scheme (k,n) can be derived from the special case, the algorithm is as followed :

1. Get the secret s by using Shamir secret reconstruction algorithm with k part and the public part.
2. Construct the n-order polynomial q(x) from interpolating of k part and the public part
3. Let the secret part $D_i = q(i*2+1) \bmod p, 0 < i < n+1$
4. Make the modification to the selected secret part, i.e D_3, (1,4) => (1,5). The modification is only allowed at the y component
5. Get q(x), the n-order polynomial function, from interpolating all of secret part and secret point (0,s)
6. Let new public part $P_i = q(i*2), 0 < i < n-k+1$

In the modification, one of the step is to search all the secret part, this is to ensure no information about secret part lost when one modify.

The extension scheme differ with shamir secret scheme in creating a new secret share (hence adding n), in shamir secret scheme one can easily make a new secret share. In this scheme, following step can be used:

1. Get the secret s by using Shamir secret reconstruction algorithm with k part and the public part.
2. Construct the n-order polynomial q(x) from interpolating of k part and the public part
3. Let the secret part $D_i = q(i*2+1) \bmod p, 0 < i < n+1$, where n is the old number of partcipant
4. Add any number of unique point (new participant) in secret part D_i.
5. Construct the polynomial q(x) from interpolating all of secret part and secret point (0,s)
6. Let new public part $P_i = q(i*2), 0 < i < n-k+1$, where n is the new number of participant

The extension scheme also differ in shamir secret scheme in changing k, in shamir scheme, one need to change the entire polynomial and secret share, in new scheme , we only need to add or delete the number of public part

IV. PROOF

Interpolation theorem : there is one k-order polynomial that can be interpolated by using k+1 unique points

Proof of polynomial existence as direct consequence of interpolation theorem: For k+1 random unique point, there is one k-order polynomial which can be interpolated.

Proof of space requirement of the general extension scheme: for scheme (k,n), we need n space for all of secret share, and n – k + 1 for all of public part. combining them, the total space requirement is 2n – k + 1, which is in order of n

Proof that modification step of general extension scheme in can be done in polynomial time : Step 1 of reconstructing secret can be done in polynomial time [1], step 2 and 5 consist of interpolating polynomial function can be done in O (n^2 log n) by [2]. Step 4 is trivial. Step 3 and 6 consist of evaluating a polynomial function n times and n-k+1 times , which is in O(n). overall the highest order of all step, which is the order of algorithm, is O (n^2 log n).

Proof of information security : Because the new scheme is derived from Threshold (n,n) scheme of Shamir secret sharing, the new scheme security directly follow Shamir secret sharing security.

Proof of anonymosity of change : for every modification made, the only direct consequence is the change of public part. Following public part treated as point, it is impossible to determine which secret share that changed because every secret share can be changed to make the public part become like that, this is the direct consequence of infinitifly many k-order polynomial can be fitted to n point where k > n.

V. Analysis

Much of the properties of this new scheme derived from shamir secret scheme, this new scheme properties is:

1. Secure: of any number of secret parts lesser than k, no information about secret s can be extracted.

2. Minimal: The size of each piece does not exceed the size of the original data.

3. Security extensible: When n is kept fixed, the number of k can easily be changed by adding or deleting public parts

4. Dynamic: Security can be easily enhanced without changing the secret, but by modify the secret share regulary

5. Modifiable: The secret share and secret can be easily modifiable without changing other secret

6. Flexible: This scheme can be used in another scheme without much difficulties

The property 3 is different than of shamir secret sharing, they differ in the context of usage. In shamir secret sharing, extensible means that for a given number of k, we can easily change the number of n. In new scheme it means that for a given number of n, one can easily change the number of k.

Another interesting property of this new scheme is anonymosity of change, that make no one outside the secret share changer to know that he is the one that change the secret share, unless the old public part collected and all other secret holder collaborating together. Which is ineffecient, considering they can get all information by having k secret holders.

Acknowledgment

The author thank Dr Rinaldi Munir for the lecture on sharing secrets.

References

[1] A. Shamir, How to share a secret. Comm. ACM, 22(11):612-613, November 1979

[2] Aho, A., Hopcroft, J., and Ullman, J. The Design and Analysis of Computer AIgorithms. Addison-Wesley, Reading, Mass., 1974.