Secret Sharing Schemes

Advanced Algorithms UE16CS302

Malaika Vijay
Dept. of Computer Science
PES University
malaika.vijay@gmail.com

Manasa Jagadeesh
Dept. of Computer Science
PES University
manasajagadeesh98@gmail.com

Mehul Garg
Dept. of Computer Science
PES University
mehulgarg14@gmail.com

***Abstract*—Secret Sharing schemes are methods by which a secret is split into shares and distributed amongst a set of users. Reconstruction of the secret is possible only when a certain number of shares satisfying certain conditions are available. In this work, we understand the worksing of, implement, and analyse six well known Threshold Secret Sharing Schemes.**

I. Introduction

Secret Sharing solves the problem of decomposing a key (the secret) into shares that are split amongst a set of users. The key can be recovered only when a sufficient number of shares, each of which contain partial information about the secret, are combined. Such schemes find use in secure storage of sensitive information, cryptography and distributed computing.

A Secret Sharing scheme consists of a dealer who has a key (the secret), a set of parties to which shares of the secret is distributed, and multiple subsets of the parties, called an access structure, each of which can determine the secret with their shares. Threshold Secret Sharing Schemes are those wherein the cardinality of the subset of shares determines whether or not a given subset is authorised to reconstruct the secret.

II. Definitions

Let *n* be an integer such that $n \geq 2, 2 \leq k \leq n$. A *k,n* threshold secret sharing scheme is one where a secret S is split into *n* shares. A set of *k* distinct shares can fully determine the secret.

A Perfect Threshold Secret Sharing scheme is one wherein the secret cannot be reconstructed with fewer than k shares

A verifiable Secret Sharing Scheme is one where it can be verified that the shares dealt out by the generator are untampered.

III. Secret Sharing Using the Chinese Remainder Theorem

Secret sharing based on the Chinese Remainder Theorem uses shares which are congruence classes of numbers associated with the key.

Theorem 1: (Chinese Remainder Theorem) Let $m_1, m_2, ..., m_k$ be a collection of pairwise relatively prime integers. The system of simultaneous congruences

$$x \equiv a_1 (mod m_1)$$
$$\text{x} \equiv a_2 (mod m_2)$$
$$\vdots$$
$$\text{x} \equiv a_k (mod m_k)$$

has a unique solution modulo M=$m_1, m_2, ..., m_k$ for any integers $a_1, a_2, ..., a_k$

A. Mignotte's Secret Sharing

Mignotte's Secret Sharing scheme makes use of a sequence of numbers, satsifying certain conditions called a Mignotte Sequence [3]

Definition 1: Let *n* and *k* be integers such that $n \geq 2, 2 \leq k \leq n$. A sequence of numbers $m_1, m_2, ..., m_n$ where $m_1 < m_2 < ... < m_n$ and gcd$(m_i, m_j) = 1, 1 \leq i < j \leq n$ and $\prod_{i=1}^{k} m_i > \prod_{i=n-k+1}^{n} m_i$ is a Mignotte Sequence.

- The secret S is chosen as a random number such that $\beta < S < \alpha, \alpha = \prod_{i=1}^{k} m_i, \beta = \prod_{i=n-k+1}^{n} m_i$
- The shares I_i are generated as $S(mod m_i), 1 \leq i \leq n$
- Given k distinct shares,$I_1, ..., I_k$ the secret S can be recovered as the unique solution modulo $m_1 ... m_k$ of the system

$$x \equiv I_{i_1} (mod m_{i_1})$$
$$\vdots$$
$$\text{x} \equiv I_{i_k} (mod m_{i_k})$$

If *k-1* shares are known, then the solution to the system of congruences modulo $m_{i_1}, ...m_{i_k}$ is found to be x_0. We only obtain that $S \equiv x_0 (mod p_{i_i} ... p_{i_{k-1}})$ but not S itself. For the secret to remain secure, the problem of finding the secret must be intractable by ensuring $\frac{\alpha - \beta}{\beta}$ is sufficiently large.

```
(n,k) (10, 3)
Secret:  1019996247
Mignotte Sequence:
[1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061]
Shares:
[165, 469, 684, 911, 110, 684, 596, 48, 747, 714]
Recovered Secret : 1019996247
```

Fig. 1. An Example of Mignotte Secret Sharing

B. Asmuth-Bloom Secret Sharing

Asmuth-Bloom Secret Sharing scheme [2] makes use of a sequence of numbers, satisfying certain conditions called an

Asmuth Bloom Sequence

Definition 2: Let *n* and *k* be integers such that $n \geq 2, 2 \leq k \leq n$. A sequence of numbers $m_0, m_1, m_2, ..., m_n$ where $m_0 < m_1 < m_2 < ... < m_n$ and gcd$(m_i, m_j) = 1, 1 \leq i < j \leq n$ and $\prod_{i=1}^{k} m_i > m_0 * \prod_{i=n-k+1}^{n} m_i$ is an Asmuth-Bloom Sequence.

- Let $M = \prod_{i=1}^{k} m_i$
- Compute $y = S + am_0$ where a is a random positive integer satisfying $0 \leq y < M$
- The shares of each user I_i are computed as $I_i = y(modm_i)$
- The secret can be recovered as the unique solution modulo $m_1...m_k$ of the system

$$y \equiv I_{i_1}(modm_{i_1})$$
$$\vdots$$
$$\text{y} \equiv I_{i_k}(modm_{i_k})$$

- $S = y(modm_0)$

If *k-1* shares were available, only *y´* i.e. the unique solution of the system modulo $m_{i_1}...m_{i_{k-1}}$ is known. Since M/$(m_{i_1}...m_{i_{k-1}}) > m_0$), and $gcd(m_0, \prod_{i=n-k+1}^{n} m_i) = 1$ the set of numbers n_i where $n_i \equiv y\acute{m}od(m_0)$ and $n_i < M$ covers all congruence classes modulo m_0. Since a is also unknown, no information is revealed by knowing fewer than k shares.

```
(n,k) : (5, 3)
Secret : 123456
Asmuth Bloom Sequence :
[123457, 370373, 370387, 370399, 370411, 370421]
Asmuth-Bloom Condition Satisfied
Shares:
[251098, 91663, 247599, 266467, 74487]
Recovered Secret 123456
```

Fig. 2. An Example of Asmuth-Bloom Secret Sharing

C. Shamir's Secret Sharing

Shamir's Secret Sharing is a *(n,k)* threshold scheme created by Adi Shamir [1]. A secret *S* is to be divided into n shares $S_1...S_n$ such that:

- Knowledge of *k* of these *n* shares is enough to fully recover the secret.
- Knowledge of any fewer than *k* shares will be equivalent to knowledge of 0 shares, and the secret *S* cannot be reconstructed at all.
- If *k=n* all the shares are required to reconstruct the secret.

This scheme uses the fact that it takes *k* points to define a polynomial of degree *k*-1. For example, it takes 2 points to define a line, 3 points to define a parabola and so on.

k-1 integers $a_1...a_{k-1}$ are chosen at random. The free coefficient a_0 is set to be equal to the secret *S*. These will form the coefficients of a polynomial.

$$\text{f(x)}=a_0+a_1*\text{x}+a_2*x^2$$

Now, *n* points are constructed that lie on this polynomial. For each *i* in set 1 to *n*, each one of the n points is of the form *(i,f(i))*. Each of these points constitute a share. Now, the polynomial, the secret are discarded. Only the threshold and the shares are retained. From these *n* shares, a minimum of *k* shares are required to reconstruct the secret.

1) Polynomial interpolation: In this scheme, Lagrange polynomials are used for polynomial interpolation.

Definition 3 (Lagrange polynomial): For a given set of (x_i,y_i) assuming no two x_i values are equal, then the Lagrange polynomial is the polynomial of the lowest degree that assumes at each value x_i the corresponding value of y_i.

The final interpolation polynomial is a linear combination of the Lagrange basis polynomial for each of the points in the set.

The free coefficient of the interpolated polynomial is the secret which has been reconstructed.

Some properties of Shamirs Secret Sharing Scheme are:

- Secure: It is information theoretically secure.
- Minimal: The size of each share does not exceed the size of the secret.
- Extensible: If the threshold *k* is fixed, the number of shares can be increased/decreased without affecting the other shares.
- Dynamic: The polynomial can be periodically changed, while keeping the free coefficient (the secret) same. This way new shares can be generated and distributed.
- Flexible: Different number of shares can be distributed to participants in the scheme, for e.g, based on hierarchy in the organisation.

A shortcoming of Shamirs Secret Sharing is that it is not verifiable. This means that there is a degree of trust involved with respect to the shares generated. It cannot be verified that the shares dealt out by the generator are untampered. It also cannot be verified that the shares submitted by the shareholders are untampered.

D. Feldman's Secret Sharing

This secret sharing scheme devised by Paul Feldman [4] aims to make Shamirs Secret Sharing verifiable. This is done by generating commitments for each of the coefficients of the randomly generated polynomial. It essentially combines Shamirs Secret Sharing scheme with any homomorphic encryption scheme.

Definition 4 (Commitment): A commitment is a cryptography primitive by which a user is allowed to commit to a chosen value while keeping it hidden from other parties, with the ability to reveal the committed value later.

A commitment essentially allows a participant to independently verify that the shares dealt out to the participants in the secret sharing scheme are valid. Such schemes which allow for commitments are essential in multi-party computation schemes.

Requirements for this scheme are:

- A cyclic group *G* of prime order *p* with a generator *g*
- A sub group of *G* of prime order *q* such that *q* divides *p*-1

- Computing discrete logarithms in this group must be computationally hard

In simpler terms, this scheme requires two prime numbers *p* and *q*, such that *q* divides *p*-1. Each of these primes will be used for modular arithmetic in a specific portion of the algorithm: computing the shares from the randomly generated polynomial will be done in the cyclic group Z_q, i.e, mod *q*; while the generation of commitments for the coefficients of the polynomial will be done in the cyclic group Z_p, i.e, mod *p*.

A commitment to a coefficient is computed as the generator of the cyclic group raised to the power of that coefficient. Thus for shares $s_1...s_n$ the corresponding coefficients are $g^{s_1}...g^{s_n}$

Now, to verify any given share, the check value if computed as the value of the product of each commitment raised to the power of the share itself raised to the power of the value it appears at. This check value is compared against the value of the share itself. If the values are equal, then the share is said to be valid.

Consider the following example

Example 1:

Share to be verified=1, Polynomial is $f(x)=0+3x+3x^2$, Commitments are 1,5,5

p=11, q=5, g=3.

Then the check value is computed as $1 * 5^1 * 5^{1^2}$ which is equal to 1

E. Blakley's Secret Sharing

Blakley's Secret Sharing [5] is an *(n,k)* threshold scheme created by George Blakley. It is based on two simple concepts:

- Any *n nonparallel n-1* dimensional hyperplanes intersect at exactly one point.
- Given one point on any n-dimensional plane it is almost computationally impossible to calculate the other *n - 1* points.

The secret may be encoded as any single coordinate of the point of intersection of the planes. If the secret is encoded using all the coordinates, even if they are random, then an insider (someone in possession of one or more of the $(n-1)$-dimensional hyperplanes) gains information about the secret since he knows that it must lie on his plane. This gives him more information than an outsider making this scheme insecure according to Information Theoretic Security. If any one coordinate is used the outsider knows no more than the insider. Each player is given enough information to define a hyperplane; the secret is recovered by calculating the point of intersection and then taking the specific coordinate of that intersection.

Example 2: Consider the following example:

Let n = 3. Since it's 3-dimensional it will have three coordinates *x, y, z*

- Let x_0 be the secret
- Let y_0, z_0 be generated randomly
- Pick *a, b* randomly and then set: $c \equiv ax_0 - by_0 - z_0$
- $a_i x + b_i y - z \equiv$-c$_i$, $k \leq i \leq n$

This yields the matrix equation

$$\begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \equiv \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix}$$

This equation can be solved provided the determinant of the coefficient matrix is not zero. The solution of this equation yields $\left(x_0, y_0, z_0\right)$, where x_0 is the solution.

The main disadvantage of this Scheme is that it is not space efficient as each user needs to store the other *k - 1* equations. Blakley's scheme can be tightened by restricting which planes can be used in shares. The reulting scheme is equivalent to Shamir's scheme.

F. Pedersen's Secret Sharing

Pedersen's scheme [6] is used in verifiable secret sharing, which is a critical building block of secure multiparty communication. Let p be a large prime number of the form p = 2q + 1 (where q is also prime). The subgroup order of q is inside $\mathbb{Z}^*{}_p$ A Pedersen commitment *Commit(a; r)* can be defined as Commit(a; r) = $g^a h^r$ mod p. For now g and h are public parameters. Three important properties of the commitment scheme:

- If h $\neq$ 1, the scheme is perfectly hiding.
- The scheme is computationally binding. In particular, breaking binding is equivalent to solving log_gh
- The dealer commits to the coefficients of the polynomial.

Dealing Protocol:

- Dealer D randomly chooses $a_1, ..., a_{t-1}, a'_0, ..., a'_{t-1} \in \mathbb{Z}^*{}_p$. Also defines $a_0 = v$.
- Define $q(x) = \sum_{i=0}^{t-1} a_i x^i$ and $q'(x) = \sum_{i=0}^{t-1} a'_i x^i$.
- The share (s_i, s_i) of P_i is $(q(i), q'(i))$.
- D broadcasts $y_i = g^{a_i} h a'^{i}_{i}$ for $i \in \{0, .., t-1\}$.

Verification:

- Each participant P_i gets a share (s_i, s'_i), he verifies $g^{s_i} h s'_i \stackrel{?}{=} \prod_{i=0}^{t-1} {y_i}^{j^i}$

Security of Pedersen's scheme:

- The broadcast value y_0 hides v unconditionally.
- Ability to change a share implies the knowledge of $log_g h$.
- Having less than t shares allows one to freely choose the secret v. Then there exists an a'_0 that is consistent with y_0.

IV. Conclusion

Secret sharing schemes are an interesting application of cryptography that aim to address relevant concerns in cyber security. Each scheme incrementally builds up to address concerns such as security, flexibility and verifiability. The drawbacks of each scheme have been studied, and attempts have been made to mitigate them in future versions of such secret sharing schemes.

REFERENCES

[1] A. Shamir, How to share a secret, Communications of the ACM, 1979

[2] C. Asmuth, J. Bloom, "A Modular approach to key safeguarding", IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 208-210, 1983.

[3] Iftene, S. (2006), General secret sharing based on the Chinese remainder theorem, Cryptology ePrint Archive, Report 2006/166.

[4] P. Feldman, A practical scheme for non-interactive verifiable secret sharing. IEEE Symposium on Foundations of Computer Science, pages 427–437. IEEE, 1987.

[5] Blakley G.R., Kabatianskii G.A. (1994) Linear algebra approach to secret sharing schemes. In: Chmora A., Wicker S.B. (eds) Error Control, Cryptology, and Speech Compression. ECCSP 1993. Lecture Notes in Computer Science, vol 829. Springer, Berlin, Heidelberg

[6] Pedersen T.P. (1992) Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In: Feigenbaum J. (eds) Advances in Cryptology CRYPTO 91. CRYPTO 1991. Lecture Notes in Computer Science, vol 576. Springer, Berlin, Heidelberg