More Versatile Secret Sharing

Meesa Shivaram Prasad

Department of CSE
Indian Institute of Technology Madras

B.tech Project, Even 2022

Research Guide: Dr.Aishwarya T

Secret sharing

Secret sharing is a method to divide the secret into many shares/parts such that secret can be constructed by authorized set of shares and unauthorized set of shares reveals least possible amount of information.

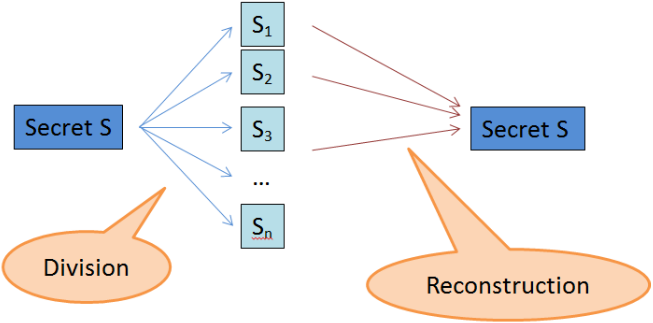


Figure: Illustration of Secret sharing

Secret sharing schemes are very helpful for storage of secure information such as cryptographic keys.

Figure: We may think of keeping keys in Secure Location

Figure: If the location got compromised?

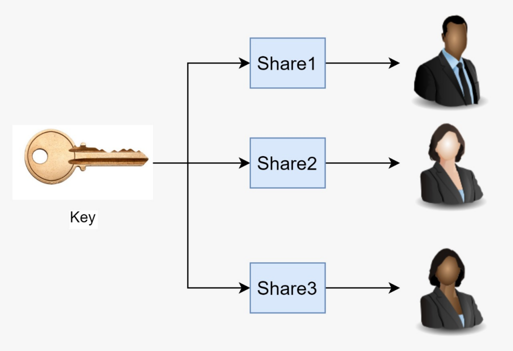


Figure: Secret Sharing

Solution: Divide the key into Shares and define only authorized set of people can reconstruct the key.

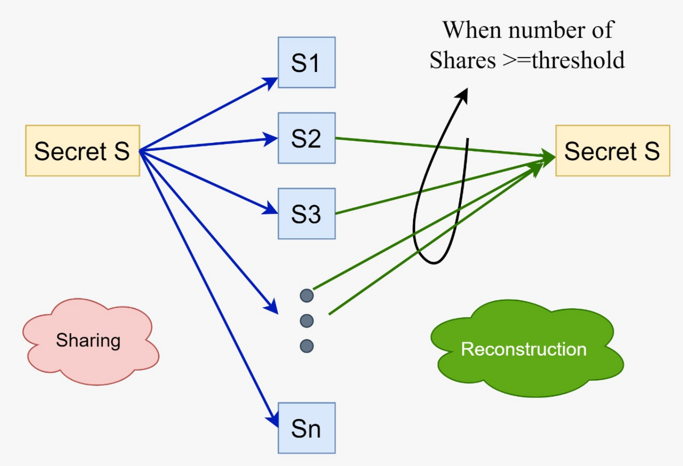


Figure: Secret can be reconstructed only if number of shares $\geq$ threshold shown up for reconstruction

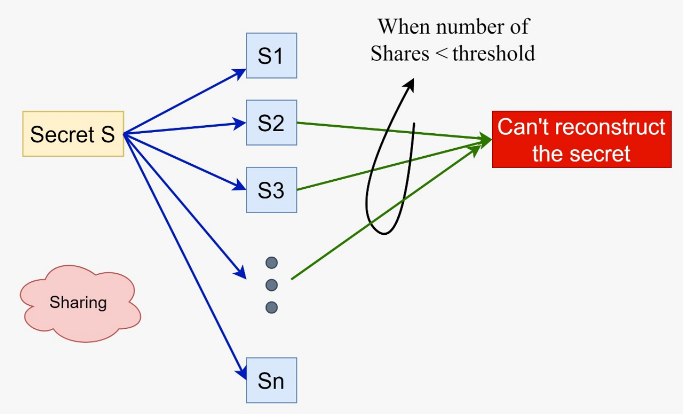


Figure: Secret can't be reconstructed if number of shares $<$ threshold

Shamir's secret sharing [1]

f is random $(t-1)^{th}$ degree polynomial with coefficients chosen at random, and constant term a_0 is secret.

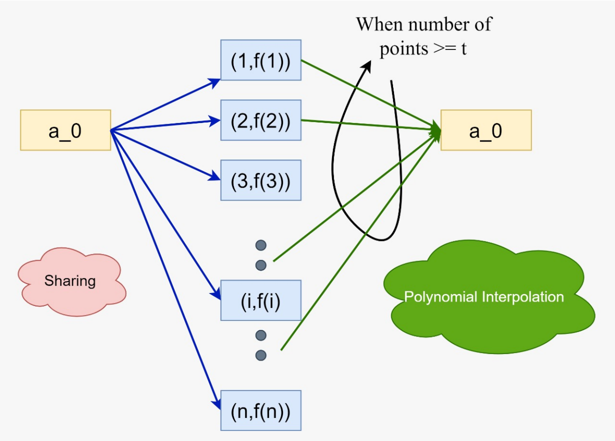


Figure: $(t-1)^{th}$ degree polynomial can be reconstructed uniquely with $\geq$ t points

Shamir's secret sharing [1]

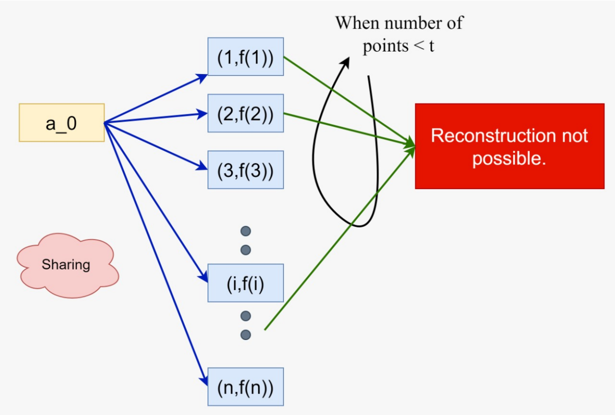


Figure: $(t-1)^{th}$ degree polynomial can't be reconstructed uniquely with $<$ t points

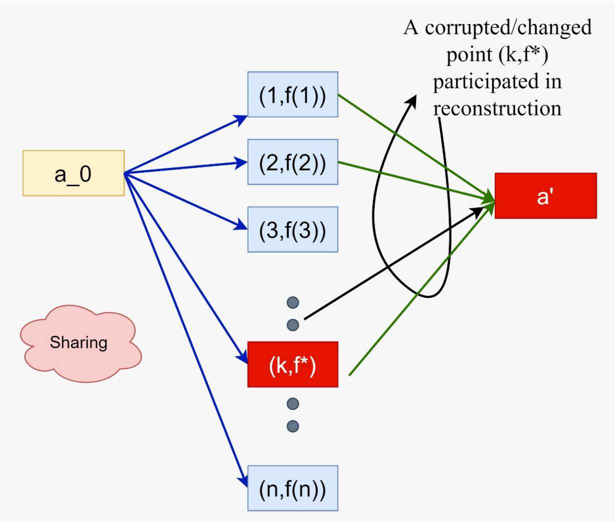


Figure: Some corrupted share participating in reconstruction resulting in $a' \neq a_0$

Bellare, Dai and Rogaway (2020) [2] augmented the classical notion with

1. Privacy when there is imperfect randomness.
2. Authenticity
3. Error Correction

error recovery definition [BDR]

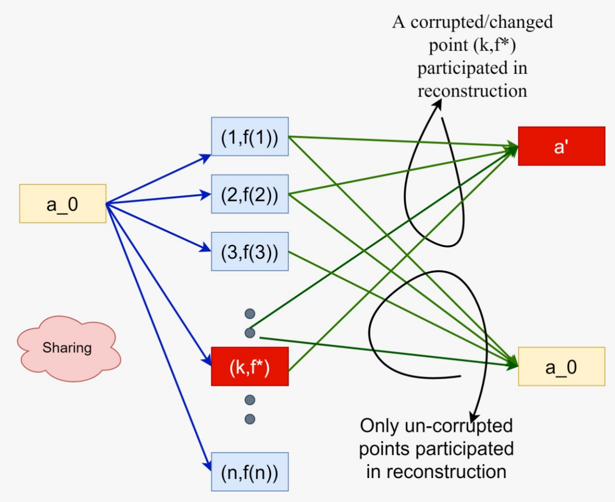


Figure: Recovery algorithm should output the secret only if an unique secret can be reconstructed from all possible subsets of input shares.

Error recovery algorithm [BDR]

1. Consider all elements of the power set of Input Shares S , let $(A_1, A_2, \ldots, A_r) \in P(S)$.
2. Sort these subsets in such a way that $A_i \subseteq A_j \implies i \geq j$
3. Now check in this order whether we can reconstruct a secret message or not using these subsets.

Error recovery algorithm [BDR]

1. If A_i is first subset with which we can reconstruct secret then exclude all subsets of A_i and continue searching in same order to find if we can reconstruct another different secret.
2. If we find another secret then return $\perp$, else return the Unique Secret Message

This error recovery algorithm takes exponential time in worst case.

My efficient error recovery Algorithm

Let $\mathbb{SS}$ be an ADSS scheme then

Sharing Algorithm :

1. Generate shares using $\mathbb{SS}.\mathit{Share}$
2. For each share concatenate the hash values of all other shares.

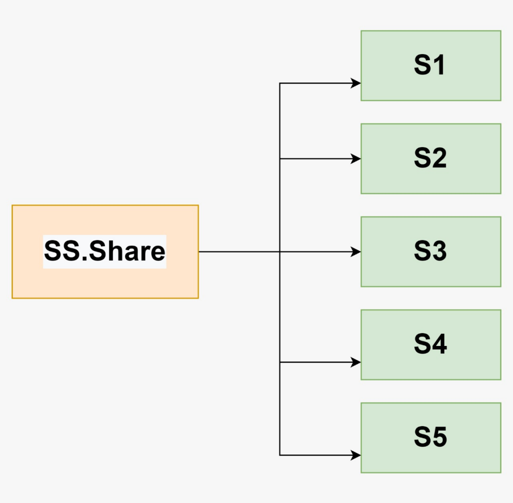


Figure: Shares generated from $\mathbb{SS}$

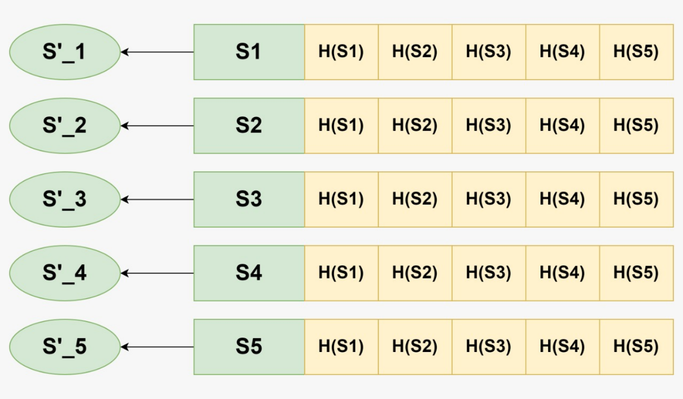


Figure: Concatenation of hash values to each share

Output the Shares $(S_1', S_2', S_3', S_4', S_5')$

We say B's share is corrupt according to A

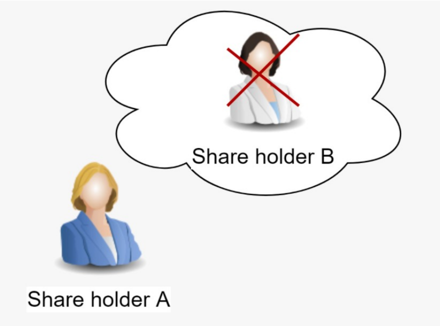


Figure: If H(B) doesn't match with hash value of B maintained by A

Recover Algorithm

Figure: Shares shown up for reconstruction.

Figure: Shares S_1, S_4 got corrupted by Adversary

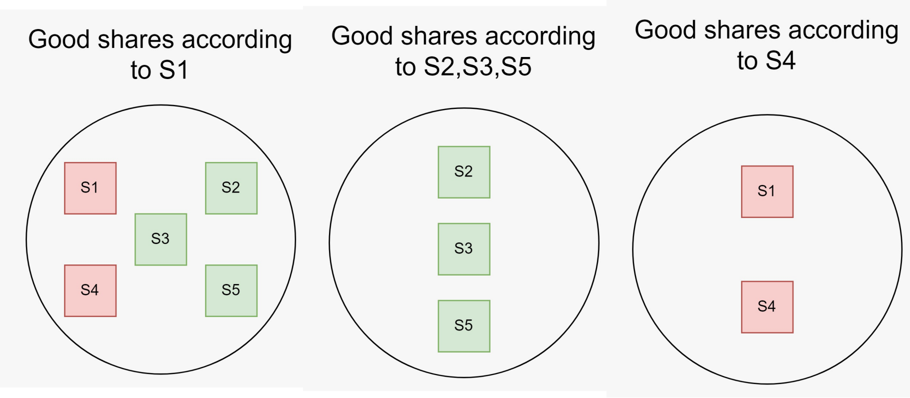
Recover Algorithm

1. Recoverer doesn't know which shares are corrupted.
2. Let threshold be 3 and known to Recoverer.

Recover Algorithm

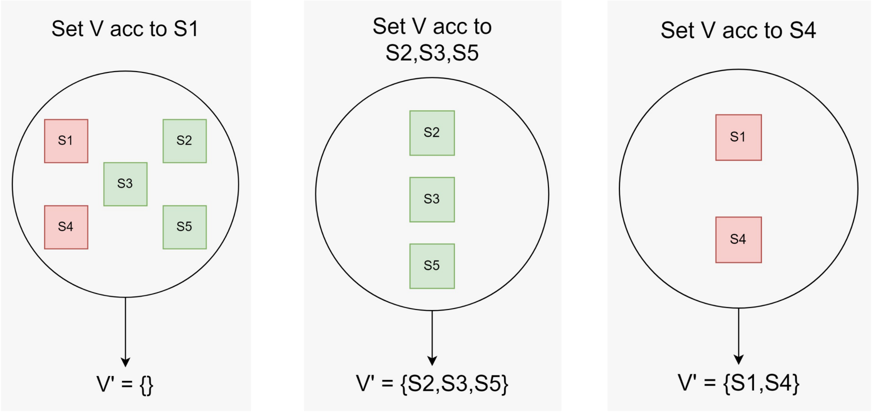
1. Initialize variable $Good\_Shares \leftarrow \{\}$
2. Now iterate through all shares $(S_1, S_2, S_3, S_4, S_5)$.

During iteration add set of all good shares according to current share to a set V.



1. Set V according to S_1, S_4 can be arbitrary as they're corrupt.
2. Set V according to S_2, S_3, S_5 are all good shares,as they're good shares

A variable $V' \leftarrow V$ if all shares in V agree each other that they're correct



We set $Good\_Shares \leftarrow V'$, if $|V'| \geq threshold$.

So in this example we'll be having $Good\_Shares = \{S_2, S_3, S_5\}$.

At the end we send Good_Shares to $\mathbb{SS}.Recover$ to get the original message back

Important Observations:

1. In the context of a good share the set V populated in the algorithm will be full of all good shares of S.
2. V' can't have a mix of good+corrupt shares.
3. If V' is all corrupt shares then $|V'|$ <threshold, as we know there can be at max $t-1$ corrupt shares
4. $Good\_Shares$ will be assigned only with set of all good shares.

Summary of Recover algorithm on input S

1. $Good\_Shares \leftarrow \{\}$
2. Iterate through each share of set S
    1. Add good shares according to current share into set V.
    2. $V' \leftarrow V$ if all shares in V agree each other that they're correct.
    3. $Good\_Shares \leftarrow V'$, if $|V'| \geq threshold$
3. Pass Good_Shares to $\mathbb{SS}.Recover$ to get the secret.

Results

If H is collison resistant then

- We can show Probability that this error recovery algorithm doesn't produce Unique secret message is negligible.

Time Complexity:

- The time complexity is $O(|shares|^4 + TC(\mathbb{SS}))$.
- There exists an ADSS scheme $\mathbb{SS}$ that runs in Polynomial time.
- Overall time complexity can be Polynomial time.

Future Goals

I aim to write efficient constructions for general set of access structures in near future , not just for threshold schemes.

Acknowledgements

I thank Aishwarya Madam who is my primary source of guidance through out my project and I also want to thank Yadu Vasudev sir for coordinating the B.tech project course.

I would like to thank Raghavendra, Simran (PhD scholars) for involving in good discussions relating to project.

Bibliography I

[1] Adi Shamir. "How to Share a Secret". In: (1979). URL: https://web.mit.edu/6.857/OldStuff/Fall03/ref/Shamir-HowToShareASecret.pdf.

[2] Bellare, Dai, and Rogaway. "Reimagining Secret Sharing: Creating a Safer and More Versatile Primitive by Adding Authenticity, Correcting Errors, and Reducing Randomness Requirements". In: (2020). URL: https://eprint.iacr.org/2020/800.pdf.