Ideal Secret Sharing - Observations of when and when not

Guido Ambasz, William Gasarch, Harikesh Kailad, Kyle Ryder, Rohan Vanga

June 11, 2021

1 Introduction

This paper will detail our findings of known ideal and non-ideal access structures for secret sharing schemes and ways of determining whether or not a scheme is ideal. We will use Dr. William Gasarch's Cryptography slides to define a (t, m) secret sharing scheme as a scheme which involves a "dealer" giving out shares of a predetermined secret to m parties, where $1 \leq t \leq m$. Any group of size $\geq t$ is able to discover the secret, but any group of size $< t$ is unable to determine the secret.

2 Definitions

We define an *access structure* as a monotone collection of subsets of parties [1, p. 786]. In other words, for a (t, m) secret sharing scheme, groups of size t and and subsets of that group are able to discover the secret. For example, if we have 3 parties, $\{0, 1, 2\}$ and a $(2, 3)$ secret sharing scheme, the sets $\{0, 1\}, \{1, 2\}, \{0, 2\}, \{0, 1, 2\}$ are able to discover the secret. Access structures give a broader definition of a secret sharing scheme. For example, schemes not defined by (t, m) can also be represented by access structures. An example is where you want to restrict a pair of participants from being able to reveal the secret. Then we would have an access structure of $\{\{0, 1\}, \{1, 2\}, \{0, 1, 2\}\}$.

A *perfect secret sharing scheme* is defined as a scheme where no information is leaked if any parties outside of the access structure gather together [3, p. 468]. For the example above, if party 2 tries to discover the secret, they will not gather any information from attempting, since they are not part of the access structure.

An *ideal secret sharing scheme* is a perfect scheme where all shares are in the domain of the secret [3, p. 468]. We define this as "if the secret is length s, then all shares are a maximum of length s." It could also be understood that all shares are part of the same set as the secret. Different papers have stated different definitions of ideal secret sharing schemes, but we have chosen the broader one.

In general, the definitions are one of these:

- |secret| = |share|
- |secret| $\geq$ |share|
- share $\in$ Dom(secret)

3 What access structures are known to be ideal

3.1 Threshold Access Structures (Blakely, Shamir)

We know these access structures are ideal and proven so by Shamir [9]. We will not mention much about them since they are covered in Dr. William Gasarch's lecture slides [5].

3.2 Multilevel Access Structure (Simmons)

This is a hierarchical sort of structure, proposed by Simmons and proven ideal by Brickell. It works as follows:

> "Each participant is assigned a level which is a positive integer and the access structure consists of those subsets which contain at least r participants all of level at most r." [3, p. 469]

For instance, look at the following examples [3, p. 469]. If two people with rank 2 can find the secret, then:

- Three people with rank 3 can find the secret.
- One person with rank 2 and two people with rank 3 can find the secret.

This access structure is a hierarchical one, in which different ranks can be used to use more or less people, depending on the requirements for reach secret. More information on this particular data structure can be found here.

3.3 Compartmented Access Structure (Simmons)

This access structure was also proven ideal by Brickell in the same paper [3, p. 469]. It works like so:

> "There are different "compartments" (groups), say $C_1, \ldots, C_u$, and positive integers $t_1, \ldots, t_u$ and a t. The access structure consists of all subsets containing at least t_i from C_i for $1 \leq i \leq u$, and a total of at least t participants." [3, p. 469]

4 What access structures are known not to be ideal

4.1 Vámos Matroids

Vámos Matroids are not ideal access structures. Brickell and Davenport detailed matroids in their study of secret sharing and questioned if all matroids were ideal access structures, given that some had been proven to be ideal [4, p. 126]. However, P.D Seymour proved that Vámos Matroids are not suitable for secret sharing, and therefore not an ideal access structure [8, p .5].

5 What makes secret schemes ideal

We found various ways in which one can determine whether access structures are ideal or not. These are:

- Monotone Circuits
- Matroids
- Graphs

5.1 Monotone Circuits

We understand monotone circuits to be circuits that can compute monotone formulas. These formulas and relationship to monotone access structure as described by Benaloh and Leichter. [2]

It turns out that monotone circuits can be used to determine whether an *access structure* is ideal or not. In essence, if you can represent an *access structure*'s subsets as a circuit with **two** inputs, and it consists of **only** AND and OR gates, and has a **single** output, then the access structure is **ideal** [3, p. 475].

5.2 Matroids

We use the following definition of Polymatroids from Padró:

> "A *polymatroid* is a pair (Q, f), where Q is a finite set, and f is a map $f : \mathcal{P}(Q) \to \mathbb{R}$ satisfying the following properties:

- $f(\emptyset) = 0$
- f is *monotone increasing*: if $A \subseteq B \subseteq Q$, then $f(A) \leq f(B)$
- f is *submodular*: $f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$ for all $A, B \subseteq Q$" [7]

It would seem that matroids can be used to determine whether an access structure is ideal. Brickel and Davenport showed that matroids are "closely related" to access structures [1, p. 786]. Furthermore, Padró claims that an access structure is ideal if and only if it is part of some polytropic matroid [7, p. 34].

5.3 Graphs

Graphs can also be used to determine whether an access structure is ideal or not. Considering the following definition:

> "For a graph $G = (V, E)$, consider access structure $\Gamma[G]$ in which the participants are identified to the vertices of G and the edges correspond to the minimal qualified subsets." [7, p. 35].

Given this definition, we can arrive at the following two propositions:

"Let G be a connected graph. Then access structure $\Gamma[G]$ is a matroid port if and only if G is a complete multipartite graph." [7, p. 36].
"If G is a complete multipartite graph, then the access structure $\Gamma[G]$ admits a vector space secret sharing scheme" [7, p. 36].

Which lead to the following equivalences [7, p. 37].:

- G is a complete multipartite graph
- $\Gamma[G]$ is a vector space access structure
- $\Gamma[G]$ is an ideal access structure
- $\Gamma[G]$ is a matroid port
- $\sigma(\Gamma[G]) < \frac{3}{2}$

6 Conclusion

Secret sharing refers to the method of splitting a secret (known as a share) and distributing it among a group. Only when a certain number of individuals come together can the secret be unraveled: individual shares on their own have no use. Ideal secret sharing schemes are perfect schemes where the size of each share is at most the size of the secret itself, or if the shares are taken from the same domain as the secret. These ideal schemes are sought after by researchers due to them being vital to information-theoretic secret sharing. Being information-theoretically secure implies that even with unlimited computing power, the system cannot be cracked or broken. The Threshold Scheme from Blakely and Shamir, Multilevel Access Structures as proposed by Simmons, and the random shares secret sharing scheme are all examples of ideal secret sharing schemes. However, all information-theoretic schemes have the common limitations of the shares being at least as long as the secret and they all require the distribution of random bits. There are many other schemes that give up some of the unconditional security found in information-theoretically secure ones to be more efficient. However, they still maintain enough security to be considered as secure as other common cryptographic primitives. These types of schemes fall under the computationally secure category.

Going forward, it may be worth looking into ideal secret sharing schemes which are computationally secure, rather than information-theoretic secure. Krawczyk touches on this in one of his papers regarding schemes with shares shorter than the secret, where the scheme relies on computational limits to create more efficiency in terms of space and communication due to the shorter amount of information necessary in the scheme [6, p .137]. These schemes would be very similar to the ideas of real-world encryption schemes, where computational limits such as discrete logarithm and factoring are assumed to be too hard and inefficient for computers to crack without extra information, and would provide a more realistic solution to secret sharing.

References

[1] A. Beimel and B. Chor. Universally ideal secret-sharing schemes. *IEEE Trans. Inf. Theory*, 40(3):786–794, 1994. https://doi.org/10.1109/18.335890.

[2] J. C. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In S. Goldwasser, editor, *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, volume 403 of *Lecture Notes in Computer Science*, pages 27–35. Springer, 1988. https://doi.org/10.1007/0-387-34799-2_3.

[3] E. F. Brickell. Some ideal secret sharing schemes. In J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology - EUROCRYPT '89,*

Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings, volume 434 of *Lecture Notes in Computer Science*, pages 468–475. Springer, 1989.
https://doi.org/10.1007/3-540-46885-4_45.

[4] E. F. Brickell and D. M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptol.*, 4(2):123–134, 1991.
https://doi.org/10.1007/BF00196772.

[5] W. Gasarch. Cryptography lecture slides - secret sharing.
https://www.cs.umd.edu/~gasarch/COURSES/456/F20/slides.html.

[6] H. Krawczyk. Secret sharing made short. In D. R. Stinson, editor, *Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference, Santa Barbara, California, USA, August 22-26, 1993, Proceedings*, volume 773 of *Lecture Notes in Computer Science*, pages 136–146. Springer, 1993.
https://doi.org/10.1007/3-540-48329-2_12.

[7] C. Padró. Lecture notes in secret sharing. *IACR Cryptol. ePrint Arch.*, page 674, 2012.
http://eprint.iacr.org/2012/674.

[8] P. D. Seymour. On secret-sharing matroids. *J. Comb. Theory, Ser. B*, 56(1):69–73, 1992.
https://doi.org/10.1016/0095-8956(92)90007-K.

[9] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
http://doi.acm.org/10.1145/359168.359176.