Vandermonde Matricies in Secret Sharing Schemes

Samuel Qin

March 2023

1 Abstract

The cryptographical problem of secure multiparty secret sharing is described as follows: a "dealer", d aims to share a secret s to n parties $P_1, P_2, \ldots, P_n$ by distributing an individual secret s_k to each party P_k. These individual secrets are designed so that any group of $i < n$ parties are able to reconstruct the secret s, while no number of parties $< i$ are able to to reconstruct the secret.

Shamir proposes a secret sharing scheme in which the dealer distributes $(x_1, s_1), (x_2, s_2), \ldots, (x_n, s_n)$ which are unique points on some i^{th} dimensional polynomial. As such, given i points (x_i, s_i), it is possible to compute the polynomial. However, as demonstrated by Halpern & Teague, there exists a Nash Equilibrium in which none of the i parties are motivated to share their given secrets; as such, each party will provide false information, leading to an incorrectly reconstructed secret.

Shamir's secret sharing scheme is an example of a linear secret sharing scheme. Such schemes are generalized through the use of matricies, especially Vandermonde matricies. A Vandermonde matrix is of the form of

$$Van^{u\times v}(\beta_1, \beta_2, \ldots \beta_u) = \begin{pmatrix} 1 & \beta_1^1 & \beta_1^2 & \ldots & \beta_1^{v-1} \\ 1 & \beta_2^1 & \beta_2^2 & \ldots & \beta_2^{v-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_u^1 & \beta_u^2 & \ldots & \beta_u^{v-1} \end{pmatrix}. \tag{1}$$

Then, such a matrix may be used to encode linear secret sharing schemes by multiplying by a column vector. Additionally, certain properties, such as invertibility and hyper invertibility, are used to create linear secret sharing schemes.

This paper aims to demonstrate the usage of these matricies in the use of linear secret sharing schemes which are both error resistant and resistant in the case of corrupted parties.

2 References

Joseph Halpern & Vanessa Teague (June 2004). Rational Secret Sharing and Multiparty Computation: Extended Abstract. In Proceedings of the 36th ACM on Theory of Computing.

Daniel Escudero (January 2022). An Introduction to Secret-Sharing-Based Secure Multiparty Computation.

3 Date Proposal

I believe I will be able to present sometime during the second or third week of April. However, I should be able to present earlier if need be.

4 Requests

As this is one of my first major presentations and term papers, I realize my unfamiliarity with writing formal, mathematical abstracts. I will ensure I utilize all received feedback.

Additionally, I would appreciate further references on multiparty secret sharing. While my current references are conclusive, they are difficult to read.