Threshold Secret Sharing with Geometric Algebra

David William Honorio Araujo da Silva[1], Luke Harmon[2], and Gaetan Delavignette[2]

[1]Algemetric, LLC
[2]Algemetric

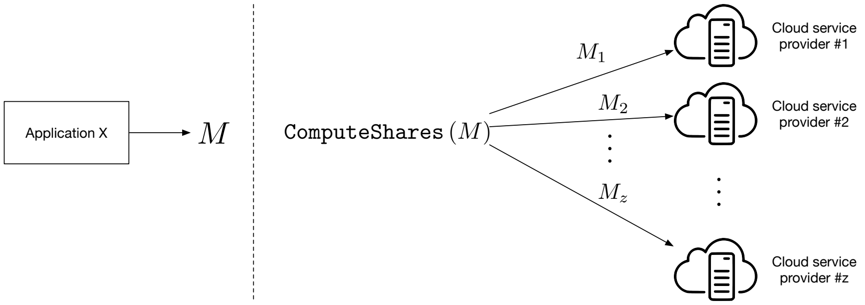
February 7, 2022

Abstract

As establishing a foundation for a new line of investigations on threshold secret sharing schemes with geometric algebra (GA), we propose a variation of a well-known threshold secret sharing scheme introduced by Adi Shamir in 1979, a cryptographic solution that allows a secret input to be divided into multiple random shares which are then sent, each one, to distinct parties. The computation of these shares is done so that there are proper subsets of these shares that allow reconstructing the secret input using polynomial interpolation. To reconstruct the secret input, Shamir's scheme requires a minimum number of shares, smaller than the total number of shares, referred to as a threshold. Any number of shares smaller than the threshold reveals nothing about the input secret. The random shares are generated such that each party can perform computations, generating a new set of shares that, when reconstructed, are equivalent to performing those exact computations directly on the secret input data. Our variant replaces the algebra in which the original secrets lie from integers to GA while preserving fundamental properties in Shamir's scheme, such as perfect secrecy and idealness (both secret and random shares are members of the same space). As a direct result, any application in GA dealing with multivectors can immediately add threshold security using our scheme. Non-GA applications can also benefit from our results by using multivectors as a vessel for sharing multiple secrets at once.

Hosted file

`Threshold_Secret_Sharing_with_Geometric_Algebra.pdf` available at https://authorea.com/users/459269/articles/555588-threshold-secret-sharing-with-geometric-algebra


Application X
M
ComputeShares (M)
M_1
M_2
M_z
Cloud service provider #1
Cloud service provider #2
Cloud service provider #z