Optimal Computational Secret Sharing

Rafael D'Oliveira

Clemson University

In (t, n)-threshold secret sharing, a secret S is distributed among n participants such that any subset of size t can recover S, while any subset of size $t-1$ or fewer learns nothing about it. For information-theoretic secret sharing, it is known that the share size must be at least as large as the secret, i.e., $|S|$. When computational security is employed using cryptographic encryption with a secret key K, previous work has shown that the share size can be reduced to $\frac{|S|}{t} + |K|$. In this paper, we present a construction achieving a share size of $\frac{|S|+|K|}{t}$. We further prove that, under reasonable assumptions on the encryption utilized, this share size is optimal.

In Special Session 47 on Mathematical Tools with Applications in Quantum and Genetic Coding at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS47-T08