The role of Mrs. Gerber's lemma for evaluating the information leakage of masked computations

Olivier Rioul

Joint work with Julien Béguinot, Yi Liu, Wei Cheng, and Sylvain Guilley

In the context of secret sharing computation in some finite Abelian group, given noisy observations of each share, how can one measure the information leakage of the secret? We show that in various instances of this problem, it boils down to establishing some variation of a "Mrs. Gerber's lemma". That is, find a lower bound on some randomness measure of a sum of discrete random variables in the Abelian group in terms of the product of individual randomnesses of each discrete random variable. It is an open problem to generalize these approaches in a suitable framework.