BILL MARTIN, Worcester Polytechnic Institute, MA

Selecting resilient functions for fault-tolerant random bit generation

Random number generation in constrained environments is a challenge of increasing importance in embedded security. High-security implementations call for hundreds of random bits per clock cycle. We need both high-rate physical entropy sources and robust post-processing tools that protect against adversaries.

This talk revisits a design of Sunar, Martin and Stinson which employs phase jitter in ring oscillators as entropy source and resilient functions in order to strengthen the output entropy. How gracefully do resilient functions fail when the entropy of the source is too low? What families of orthogonal arrays provide the best resilient functions to handle side-channel attacks?