NAU
NORTHERN
ARIZONA
UNIVERSITY

Department of Mathematics and Statistics
Colloquium
Tuesday September 24
AMB 164 4:00 - 5:00 pm

Statistical analysis of the response-based cryptography

Bertrand Cambou

Northern Arizona University (SICCS)

Abstract

Abstract: Response-based cryptographic methods use search engines to uncover erratic keys, generated by physical unclonable functions, which secure networks of low power cyber physical devices. However, when the defect densities are high, the latencies associated with search engines can be prohibitive. The statistical analysis developed, with Poisson distribution, shows how the fragmentation of keys can significantly reduce latencies, even when the error rates are large. The statistical models are validated experimentally with a 200MHz microcontroller development board, SHA-512 hash functions, and AES-256.

Refreshments at 3:45