Complexity Assessment of Analog Security Primitive Signals Using the Disentropy of Autocorrelation

Paul Jimmenez, Xavier Letatre, **Cédric Marchand**
Centrale Lyon, INSA Lyon, CNRS, Université Claude Bernard Lyon 1, CPE Lyon, INL, UMR5270, Ecully 69134, France
paul.jimenez@ec-lyon.fr

Fabio Pavanello
Univ. Grenoble Alpes, Univ. Savoie Mont Blanc, CNRS, Grenoble INP, CROMA, Grenoble, France

Speaker: Cédric Marchand

The analysis of regularity in signals holds significant importance across various fields most notably in medicine, where it is used to examine electrocardiogram (ECG) and electromyography (EMG) signals. However, this type of analysis also plays a important role in areas such as climate science, finance, and security. In this work, we focus on its relevance to security primitives, particularly Physical Unclonable Functions (PUFs) and Random Number Generators (RNGs). These primitives require a high degree of unpredictability or entropy in their outputs to ensure the security of their application.

There are multiple approaches to assess the complexity of their responses, especially in the binary domain. However, with the emergence of analog-based security primitives such as optical (photonic) PUFs and TRNGs it becomes increasingly valuable to assess complexity directly in the analog domain, ideally during the design phase, and before the analog-to-digital conversion.

In this numerical study, we investigate the potential of using the disentropy of autocorrelation as a metric for evaluating the complexity of security primitives working in the analog domain, including PUFs, True Random Number Generators (TRNGs), and PRNGs. We compare this metric against established measures of regularity in analog signals, such as Approximate Entropy and Fuzzy Entropy. Our results show that the disentropy of autocorrelation provides a clearer contrast between high-quality PRNGs and poorly designed or non-optimized ones in the analog domain. Furthermore, we demonstrate that this metric is sensitive enough to detect small patterns introduced into PUFs or RNGs responses.