Physical Unclonable Functions for Secure Communication

Roarke Horstmeyer¹, Benjamin Judkewitz¹, Ivo Vellekoop² and Changhuei Yang¹

¹Department of Electrical Engineering, California Institute of Technology, Pasadena, CA, USA ²University of Twente, Enschede, The Netherlands

Abstract: All encryption schemes rely on the use of suitably random keys to ensure security. Here, the feasibility of using an object’s microscopic randomness to generate these communication keys is experimentally investigated. The physical disorder of a volumetric material can be converted into a one-way hash function through a simple optical probe-and-detect setup. Benefits of physical randomness storage over algorithmic constructions include efficiency, resilience against characterization or modeling, and the near-impossibility of cloning. Noise is accounted for using a fuzzy commitment-based communication scheme. Future work is focused on jointly optimizing the physical and digital post-processing steps required of a successful device.

Background

- Sending coherent light through a volumetric scattering medium generates a highly randomized interference pattern — “speckle”.
- Slightly changing the incident light wave can create an equally random yet independent speckle pattern.
- Experiments indicate the total usefulness of randomness of a volumetric scatterer is on the order of $10^{10}$ bits in the absence of noise.

References


Acknowledgements

This work is supported in part by an NDSEG Scholarship Contact: Roarke Horstmeyer, roarke@caltech.edu Webiste: http://www.biophot.caltech.edu

Setup and Theory

- Randomly vary phase of input light with an SLM screen
- Digitally detect output interference pattern (intensity)
- Generate many random [Challenge, Response] key pairs

Example Communication Protocol

A. Register: Show same challenge, detect different response, build database

B. Communicate: Generate new responses (primed = noisy)

C. Experimental Noise Analysis

Adding grayscale content to remove noise

4-pixel error correction example

Error correction advantage

# pixels for error correction

NANSE

C. Removing correlation

1. Digital whitening methods
2. Piling up lemma:

\[ P(X_1 \oplus X_2 \oplus \cdots \oplus X_n = 0) = 1/2 + 2^{-n} \]

\[ \text{XOR} \rightarrow \text{Randomize} \]

\[ s_1 \oplus s_2 \oplus \cdots \oplus s_n \approx \text{speckle entropy} |i| \]