Optical Physical Unclonable Functions for Reconfigurable Public-Key Key Generation

Sid Assawaworrarit\(^1\), Roarke Horstmeyer\(^1\) and Changhuei Yang\(^1\)

\(^1\)Department of Electrical Engineering, California Institute of Technology, Pasadena, CA, USA

Correspondence to Sid Assawaworrarit (sca@caltech.edu) or Roarke Horstmeyer (roarke@caltech.edu)

Abstract: In this work, we experimentally demonstrate how random communication keys may be stored error-free in non-electronic memory over a period of several hours. We use an optical scattering Physical Unclonable Function (PUF) along with a suitably chosen error correction procedure to reproducibly generate gigabits of statistically verified randomness. This stability achievement is facilitated by a uniquely compact optical PUF construction, consisting primarily of a volumetric scattering medium sandwiched between a spatial light modulator (SLM) and digital detector. The spatial light modulator serves to pattern an incident light beam into a specific PUF challenge, the digital detector serves to measure the intensity of the resulting scattered optical field (i.e., the PUF response), and all optical components are fastened together with an epoxy to ensure the optical system is minimally effected by any mechanical movement. We also demonstrate how the entire random keyspace may be reset through device heating.

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.
- Digitally detecting many independent speckle patterns generates a large set of random numbers. Experiments indicate a volumetric scatterer can store $\sim10^{10}$ bits per mm$^3$ in the absence of noise.

Device achievements
- Non-electronic storage of PK communication keys
- Keys last several hours (e.g., typical session length)
- Ability to alter key-space quickly to prevent characterization of stolen devices.
- Large key space (gigabits) prevents direct characterization

References

Device setup and operation

Optical PUF key generation and storage pipeline

A. Key Generation
- Display random SLM screen $p$, detect speckle image $r$ (intensity)
- Generate a random sequence $k$ by removing correlation in $r$ with digital whitening method\(^d\)
- Create session key $a$ by truncating $k$ to desired length (e.g. 1024 bit)

B. Secure Storage of Session Key
- With another SLM screen $p$, generate random sequence $s(0)$
- Use fuzzy commitment\(^s\) and error correction to mix $a$ and $s(0)$ into a blob $B$, which can be securely stored in electronic memory

C. Key Retrieval
- With SLM screen $p$, generate sequence $s(t)$ at time $t$
- Use fuzzy commitment to un-mix $a$ from $s(t)$ and saved blob $B$

Results

A. Temporal Decorrelation of PUF Outputs

B. Error Correction Performance
We compare bit error rates of the following Error Correction Codes (ECCs) and show that the design of ECC affects key retrieval lifetime.

C. Resetting PUF with Sensor Heat Dissipation
We can induce reconfiguration of the PUF by:
- rapidly reading speckle data from the sensor (heating)
- putting the scatterer directly onto the sensor

Input

Optical PUF device

Output image and key

Mathematical model

W = Digital whitening

Experiment

Optical PUF key generation and storage pipeline

A. Temporal Decorrelation of PUF Outputs

B. Error Correction Performance

C. Resetting PUF with Sensor Heat Dissipation

A. Key Generation

B. Secure Storage of Session Key

C. Key Retrieval

We can induce reconfiguration of the PUF by:
- rapidly reading speckle data from the sensor (heating)
- putting the scatterer directly onto the sensor

Input

Optical PUF device

Output image and key

Mathematical model

W = Digital whitening

Experiment