Demo Abstract: CAMPUF: Physically Unclonable Function based on CMOS Image Sensor Fixed Pattern Noise

Yongwoo Lee, Kyuin Lee, and Younghyun Kim
University of Wisconsin–Madison

The past decade has witnessed a remarkable growth of services that rely on or involve mobile and wearable devices. The increasingly network-connected nature of these devices, coupled with more and more sensitive and confidential data placed online, has led to an unprecedented level of security and privacy concerns. As a promising measure to combat the security and privacy challenges, physically unclonable functions (PUFs) have been proposed. A PUF is a hardware component that exploits inherent manufacturing process variations to generate random numbers that are unique, unpredictable, and unreproducible. PUFs are a promising device authentication method to augment security as part of multi-factor user authentication. We propose a novel PUF design, named CAMPUF, based on commercial off-the-shelf CMOS image sensors, which are ubiquitously available in almost all mobile devices.

CMOS image sensor-based PUFs have emerged as an attractive option since image sensors are readily available in many mobile and wearable devices. The source of randomness in the image sensor-based PUFs is the imperfection of the pixel array and readout circuit manufacturing process, which manifests as fixed pattern noise (FPN) in the image. The FPN extracted from an image is unique from sensor to sensor and can, therefore, be used as the fingerprint of the sensors. The two main components of FPN are photo-response nonuniformity (PRNU) noise and dark signal non-uniformity (DSNU) noise. PRNU is due to the responsivity variation between pixels and is the dominant FPN in illuminated natural images. On the other hand, DSNU is mainly caused by the variations of dark current and is dominant in dark images.

CAMPUF uses DSNU as a fingerprint. Compared to other approaches that use PRNU, CAMPUF has two main advantages:
(i) Better security: PRNU can be extracted from high-quality illuminated natural images, which are often shared on social network services (SNSs). An adversary can easily obtain a PRNU-based fingerprint from the shared photos. On the other hand, DSNU is extracted only from dark images that are not shared publicly. Therefore, the DSNU-based fingerprint is more secure.
(ii) Better usability: To obtain PRNU, the user must take a picture of a flat object (e.g., plain wall), which may not be available at all times. On the other hand, DSNU can be obtained simply by covering the camera with any light-blocking object (e.g., hand). Therefore, CAMPUF is easier to use.

At the University Demonstration, we will demonstrate the performance of CAMPUF for device authentication. We implemented CAMPUF on an Android smartphone, Google Nexus 5X, with Sony IMX377 12-megapixel image sensor. Five identical sensors will be used for demonstration, as shown in Fig. 1. We developed an Android application to capture and transfer a raw image and a Matlab-based GUI to process and visualize the authentication process, as shown in Fig. 2. Our paper on CAMPUF will be presented at DAC 2018 [3].

- YouTube video link: https://youtu.be/N_RCLKh1DUA

![Google Nexus 5X](image1)

![Sony IMX377](image2)

**Fig. 1:** Smartphone and image sensors used for demonstration.

**Fig. 2:** CAMPUF GUI for visualizing authentication process.

**REFERENCES**

