# One Crossbar, Two Functions: Analogue Image Obfuscation and Feature Extraction via Memristors

Przemysław Janiszyn[1,2], Anna Wąsiak-Maciejak[1], Paweł Sitarz[1], Tomasz Matusiak[1]
[1] SEMIQA, Wroclaw, Poland
[2] Wroclaw University of Science and Technology, Wroclaw, Poland
p.janiszyn@semiqa.com

## SUMMARY

The rapid growth of the Internet of Things (IoT) and the increasing dependence on cloud-based data processing have heightened the need for security primitives that function directly at the edge, where computational and energy resources are highly limited. Conventional, well-established cryptographic protocols introduce substantial processing overhead that often exceeds the capabilities of resource-constrained edge imaging devices, prompting the investigation of hardware-based intrinsic alternatives. [1]

Physical Unclonable Functions (PUFs) offer a promising route in this regard, as they exploit the inherent manufacturing variability of integrated circuits to generate device-specific cryptographic signatures without the need for stored digital keys. [2]

This work introduces a memristor-based hardware architecture for secure and efficient edge-to-cloud image transmission. The system leverages a memristor crossbar to simultaneously achieve signal obfuscation and device authentication through a single analog-domain computation. We employed a Python-based framework integrating IBM's AIHWKit to model memristor process variation as a physical fingerprint, and MemTorch to simulate the filters and the entire circuit layout. We explore the impact of two complementary sources of variability: cycle-to-cycle variation for dynamic obfuscation and device-to-device conductance spread to create a persistent hardware-intrinsic security mechanism. We further demonstrate that the crossbar operation simultaneously serves as a feature extraction engine (Figure 1). Simulations confirm robust obfuscation, strong diffusion, and reliable reconstruction, highlighting a promising route toward low-power, hardware-intrinsic security in next-generation edge imaging.

## REFERENCES

[1] Ibrahim, H.M., Abunahla, H., Mohammad, B. et al. Memristor-based PUF for lightweight cryptographic randomness. Sci Rep.2022, 12, 8633.

[2] L.Yang, L.Cheng, Y.Li, H.Li, J.Li, T.-C.Chang, X.Miao, Cryptographic Key Generation and In Situ Encryption in One-Transistor-One-Resistor Memristors for Hardware Security. Adv. Electron. Mater.2021, 7, 2001182.

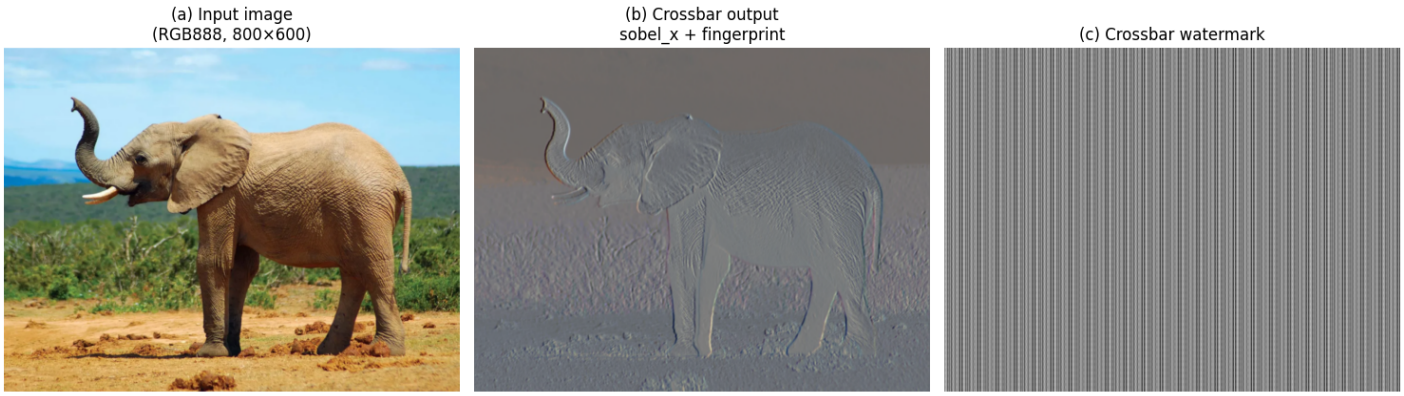


Figure 1. a) Original input image (RGB888, 800 × 600 px). b) Crossbar output with an embedded device fingerprint, utilizing a Sobel X edge detection filter to highlight horizontal intensity gradients. (c) Isolated device fingerprint recovered server-side from the stored key.