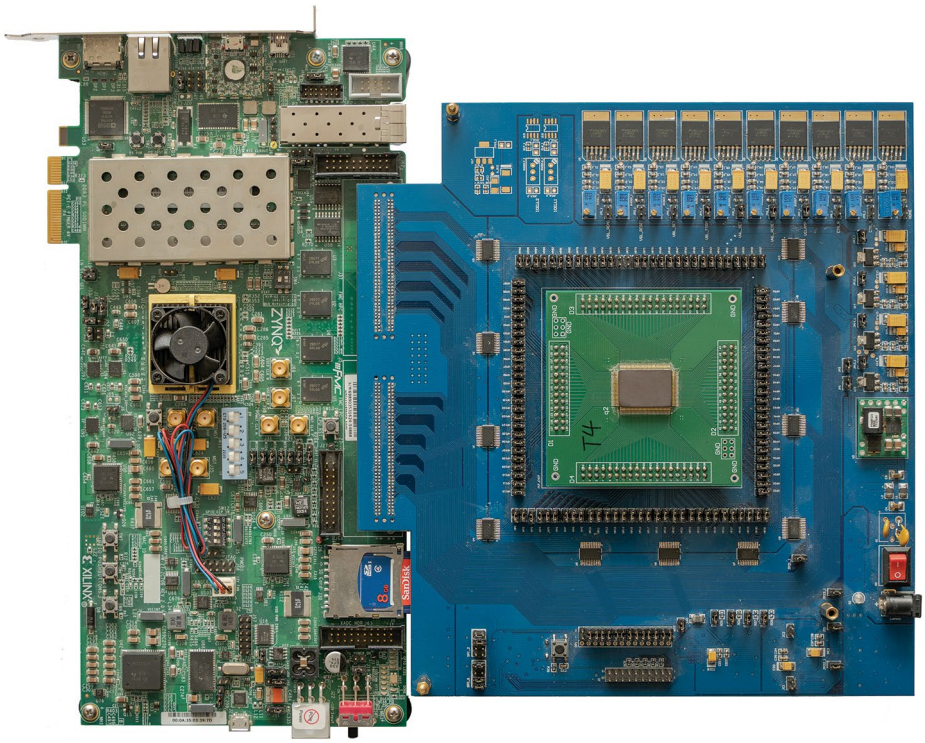
CRYPTOGRAPHIC HARDWARE

# Security in reconfigurability with resistive memories

*2019 Int. Solid-State Circuits Conf.* (in the press)




Credit: Huaqiang Wu, Tsinghua University

Physically unclonable functions (PUFs) are a class of hardware security primitives used for cryptographic applications such as key authentication. PUFs implemented in complementary metal–oxide–semiconductor (CMOS) technology typically exploit variations in the fabrication process (also known as process randomness) as the basis for their cryptographic keys. An alternative approach is to exploit the intrinsic variability of the device itself (also known as post-process randomness) as a source of stochasticity. Huaqiang Wu and colleagues at Tsinghua University, Georgia Institute of Technology, and National Tsing Hua University have now developed a PUF based on resistive memory that uses such ideas and can pass randomness tests set by the National Institute of Standards and Technology (NIST).

Wu and colleagues leveraged the inherent randomness of resistive random access memory (RRAM) cells to generate cryptographic keys. By applying a split-resistance technique they achieve a native bit-error-rate of less than $6 \times 10^{-6}$ and demonstrate a greater robustness to environmental changes (temperature and voltage) compared to PUFs implemented in CMOS technology. A key feature of their PUFs RRAM chip is the ability to reconfigure an entirely new PUF. To show the effectiveness of the approach, the researchers demonstrate 60 continuous reconfigured PUF keys with little correlation between the keys. The ability to reconfigure the PUF keys reduces the risks of key overuse and changing ownership of the hardware.

Michael Lee

Published online: 15 March 2019
https://doi.org/10.1038/s41928-019-0227-0