# Ag Conductive Bridge RAMs for Physical Unclonable Functions

**Bertrand Cambou**, **Fatemeh Afghah**, **Derek Sonderegger**
Northern Arizona University

**Jennifer Taggart**, **Hugh Barnaby**, **Michael Kozicki**
Arizona State University

*Abstract*— We are presenting a method to design reliable physical unclonable functions (PUFs), with silver based conductive-bridge random access memory (CB-RAM) arrays, to protect the internet of things (IoT). The arrays that we fabricated in our pilot line, and characterized, operate at extremely low power which is highly desirable for security applications, and to protect cryptographic primitives. The experimental data presented in this work supports the selection of the programming voltage, the Vset, as the parameter, to generate PUF challenge-response pairs (CRP). The median Vset voltage at 0.12V is orders of magnitude lower than other non-volatile memory technologies, which can reduce the threat of side channel analysis.

The level of stability, cell to cell, of the Vset that we characterized is acceptable when combined with methods based on ternary states, and resulted in low CRP error rates. Built-in-self-test capability (BIST) is used to differentiate unstable cells of the array, that carry the state “X”, from the solid cells carrying the states “0” and “1”, which are capable of generating reliable PUF CRPs. The use of machine learning algorithms can also compensate for the temperature drifts, noise, aging, and measurement instabilities normal variations. This research work is currently used to finalize and design a prototype with a custom state machine, and FPGA. We will fabricate various CB-RAM samples to optimize the quality of the PUFs.