Cryptographic Engineering Research Group
Presents

ECE DEPARTMENTAL SEMINAR

PUF designed with Resistive RAM and Ternary States

Bertrand Cambou, Ph.D.
School of Informatics, Computing, and Cyber-Systems
Northern Arizona University

Monday, April 4, 2016
3:15-4:15pm, ENGR 3507

Abstract:

The designs of Physically Unclonable Functions (PUFs) described in this presentation are based on Resistive RAMs incorporating ternary states with the objective to reduce false negative authentications (FNA) with low Challenge-Response-Pair (CRP) error rates. Unlike other error correction method, the method is not increasing false positive authentications (FPA). The ternary states, the "Xs", allow the blanking of all cells that are not characterized as consistently capable to generate stable and easy to read "1s" or "0s" PUF challenges. Experimental data extracted from Cu/TaOx/Pt Resistive RAM samples confirms that such a method can generate CRPs having error rates below 8 ppm useable for secure hardware authentication. Random Number Generators (RNG) can also be enhanced by the same ternary architecture.

Short bio:

A Professor of Practice at Northern Arizona University, Dr. Cambou primary research interests are in cyber-security, and how to apply nanotechnologies to strengthen hardware security. Previously he worked as CEO in Silicon Valley in nanotechnologies, where his organization won a contract with IARPA with applications related to quantum cryptography. He worked in the smartcard industry at Gemplus (now Gemalto), and in the POS/secure payment industry at Ingenico. He spent 15 years at Motorola Semiconductor (now NXP-Freescale), 5 years as CTO; he was named "Distinguished Innovator" and scientific advisor of the BOD. He is the author and co-author of 41 patents in microelectronics and cybersecurity with more than 400 citations. He holds a Doctorate degree from Paris-South University, France, and an Engineering degree from Supelec, France.