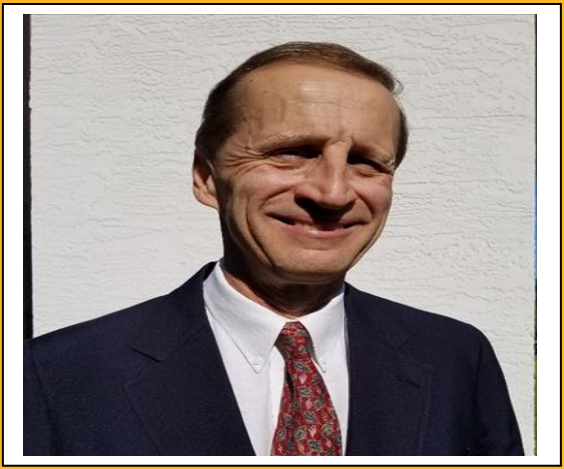
A Knight's Welcome To: Kevin A. Kwiat, Ph.D.



DATE: Friday November 30, 2018

TIME: 9:00AM-10:00AM

LOCATION: R1-307 (Research I Building)

HOSTED BY: Aziz Mohaisen

Associate Professor, Department of Computer Science

Bio: Kevin A. Kwiat, PhD, is formerly a Principal Computer Engineer with the U.S. Air Force Research Laboratory (AFRL) and has more than 34 years of service and has been awarded 5 patents during that time. While at AFRL, he conducted research and development in a wide scope of areas: high reliability microcircuit selection for military systems; testability; logic and fault simulation; rad-hard microprocessors; benchmarking of experimental designs; distributed processing systems; assured communications; FPGA-based computing; fault tolerance; survivable systems; game theory; cyber-security; and cloud computing. His PhD is in Computer Engineering from Syracuse University. He is co-founder and leader of Haloed Sun TEK of Sarasota, Florida, which is an LLC specializing in technology transfer and has joined forces with the Commercial Applications for Early Stage Advanced Research (CAESAR) Group.

"A Design Technique to Prevent Hardware Trojans from Leaking Sensitive Data"

Opportunities for entrepreneurs to capitalize on the U.S. Air Force's investment in technology has come to the forefront. An overview of such opportunities will be accompanied by a detailed technology example. Since the turn of the century many integrated circuit (IC) design houses have outsourced the production of their chips to other countries. This has created a new opening for cyber-attacks: when a firm sends out a design to be manufactured overseas, the trustworthiness of the manufactured IC can no longer be guaranteed. It is now possible to insert hardware Trojans directly into a chip during the design and manufacturing process. These hardware Trojans can destroy a chip, reduce performance or even leak sensitive data – including encryption keys. For many in the information assurance arena confidentiality is paramount, so the possibility of a hardware Trojan leaking data is of great concern. This presentation covers U.S. Air Force patent-pending methods of defending against data-leakage hardware Trojans in 2 forms: 1) combinational and 2) sequential logic. Both forms prevent data leakage through a randomized encoding and split manufacturing scheme. Experimental work revealed the power and area overheads associated with these techniques; yet, the Air Force's risk calculus can be such that these overheads become acceptable – especially when there is only a 3% decrease in performance.