Side Channel Resistant Lightweight Cryptography for the Internet of Things
Current and Future Research

PhD Seminar Presentation by William Diehl (Advisor: Dr. Kris Gaj)

Tuesday April 3, 2018
2:30 – 3:30 pm
ENGR 3507

Lightweight cryptography is an important topic in the emerging Internet of Things (IoT), since it provides moderate security at reduced cost in terms of circuit area, power, and energy. In particular, lightweight authenticated ciphers offer promise of lower-cost security solutions for certain embedded applications, since they combine the functionalities of confidentiality, integrity, and authentication into one algorithm. However, physical implementations of cryptography are vulnerable to side channel attack (SCA), where adversaries attempt to recover sensitive data by observing physical phenomena during cipher operations.

The CAESAR competition seeks to choose the best authenticated cipher candidates based on several criteria, including hardware performance and resistance to SCA. However, evaluation of the resistance to SCA and relative costs of protection against SCA is challenging, given the complexity of authenticated ciphers, and the large number of ciphers to be evaluated. In current research, we augment an open-source SCA test bench with leakage detection methodology for authenticated ciphers. We evaluate eleven authenticated cipher implementations for an SCA vulnerability called differential power analysis (DPA), protect them against 1st order DPA using threshold implementation (TI) countermeasures, and verify the effectiveness of countermeasures. We then benchmark the unprotected and protected ciphers in an FPGA, and compare the ciphers based on absolute and relative costs of protection against 1st order DPA in terms of area, throughput, throughput-to-area (TP/A) ratio, power, and energy per bit.

Since it is not always possible to distribute symmetric secret keys to all parties before use, key exchange protocols using public key solutions are also necessary for lightweight devices in the IoT. However, today's public key standards are vulnerable to future quantum computing. Accordingly, the National Institute of Standards and Technology (NIST) intends to issue standards for post-quantum-resistant cryptographic solutions. While there are several promising candidates for post-quantum-resistant solutions, most are difficult to implement in very-lightweight platforms, and all are potentially vulnerable to side channel attacks. In future research, we will build upon our research in authenticated ciphers to develop side channel resistant implementations of post-quantum-resistant public key cryptographic solutions in lightweight reconfigurable platforms, suitable for employment in security applications in the IoT.

William Diehl is a Doctoral Candidate in the Department of Electrical and Computer Engineering (ECE) at George Mason University. His interests include secure and efficient implementations of cryptography in hardware and software. His recent research topics include power analysis side channel attacks on lightweight authenticated ciphers, design and implementation of authenticated ciphers in Field Programmable Gate Arrays (FPGA), and implementation of lightweight cryptography in very low-cost, low-power reconfigurable microprocessors. William holds a B.A. degree in Computer Science from Duke University, and a M.S. degree in Electrical Engineering from the Naval Postgraduate School.