Notice and Invitation

Oral Defense of Doctoral Dissertation
The Volgenau School of Engineering, George Mason University

Ahmad Salman
Bachelor of Science, Arab Academy for Science and Technology, 2002
Master of Science, George Mason University, 2011

PUBLIC KEY CRYPTOGRAPHY USING HARDWARE/SOFTWARE CO-DESIGN FOR THE INTERNET OF THINGS

August 2, 2017, 1:00pm-3:00pm
Engineering Building, Room 3507
All are invited to attend.

Committee
Dr. Jens-Peter Kaps, Chair
Dr. Kris Gaj
Dr. Houman Homayoun
Dr. Angelos Stavrou

Abstract

Embedded electronic devices and sensors are playing a major role in bridging the gap between the physical world and the virtual world. Billions of devices such as smartphones, smart watches, wearables, medical implants, and Wireless Sensor Nodes (WSN) are considered building blocks in making "The Internet Of Things" (IoT) a reality. Such devices often carry sensitive data and are used in critical applications, making it essential to create a secure environment to protect the data they gather at rest and in transit. With these devices being limited in their power, energy, area, and memory, choosing a suitable cryptographic system to provide the necessary security services becomes a challenge. Pairing Based Cryptography (PBC) is among the leading candidates to bringing Public-Key Cryptography (PKC) to lightweight devices as it provides services that traditional PKC systems lack. Security services such as non-interactive key agreement, Identity-based Encryption (IBE), revoking of compromised keys and more, are all examples which show PBC benefit over PKC.

For these reasons and more, the area of creating lightweight implementations for different building blocks of PBC in software and hardware is an active research area and a hot topic among the cryptographic community. In this research, we studied bilinear pairings and their

lightweight implementations in software, hardware, and hardware/software co-design in efforts to create a design that is efficient, flexible, and lightweight. We also studied the effect of adding countermeasures to side-channel attacks on area usage and power consumption. Finally, we performed measurements on the power and energy consumption of the implemented designs. Our goal is to exploit the benefits of using PBC over classical public key for applications running on resource constraint devices and show that a lightweight PBC implementation on these devices is feasible and practical. The work was divided into two main phases. The first phase focused on the selection of pairing parameters (finite field, elliptic curve, embedding degree) that provide an acceptable security level while meeting efficiency requirements for resource constraint devices. The second phase focused on designing an efficient hardware accelerator for computationally intensive operations in pairing-based cryptography to achieve acceptable speed while minimizing area and power consumption.