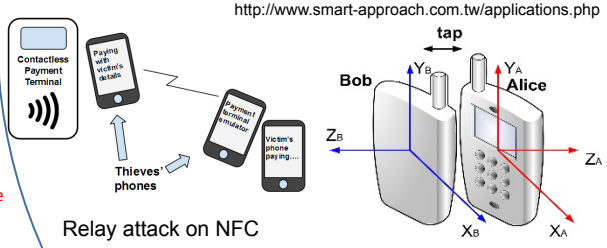
Secure Near Field Communications between Mobile Devices

Challenge:

- Ultra High Speed and Energy-Efficient Symmetric Key Generation for resource constrained NFC devices
- Providing communication confidentiality for largely deployed NFC devices without relying on encryption
- Defending against relay attacks on mobile payment and access control

Solution:

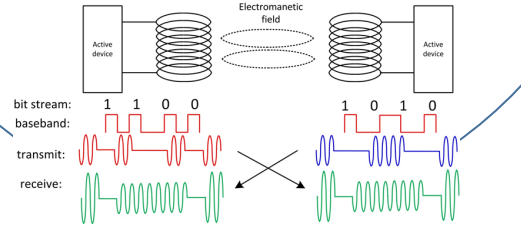
- Exploiting full-duplex capability of NFC to generate shared secret keys. Advantages over DH key exchange:
  - Faster speed with three orders of magnitude improvement
  - Lower energy consumption of one order of magnitude reduction
- Secure NFC by randomizing waveforms with friendly jamming
  - Providing confidentiality without encryption
  - Tackling synchronization offset, phase mismatch, and amplitude mismatch
- Using magnetometers to verify location proximity
  - High usability, strong security, transparent to user



Relay attack on NFC

Proximity verification using magnetometers

Testbed development



Key agreement using NFC full-duplex communication

Scientific Impact:

- Significantly improve the key generation efficiency, largely reduce energy consumption and key generation delay for resource constrained NFC devices
- Advance research on lightweight, energy-efficient, and usable security mechanisms in mobile networks for many IoT applications
- Promote the understanding of the advantage and capacity of physical layer security mechanisms
- Provide a more usable solution for location proximity verification and has a potential to be integrated with distance bounding protocols

Broader Impact:

- Applicable to important applications, such as mobile payment and access control
- Implementable in NFC readers to secure data reading from largely deployed NFC tags
- The newly established Cyber Security Engineering (CYSE) BS program at George Mason University will be enriched through this project
- High school and undergraduate students will be involved through university ASSIP summer internship program

Project No.: CNS-1619073

PI name: Kai Zeng
Institution: George Mason University