RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

NFC TECHNOLOGIES FOR SECURE MOBILE PAYMENT

Ciaran Fisher
NXP Semiconductors

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

Session Objectives

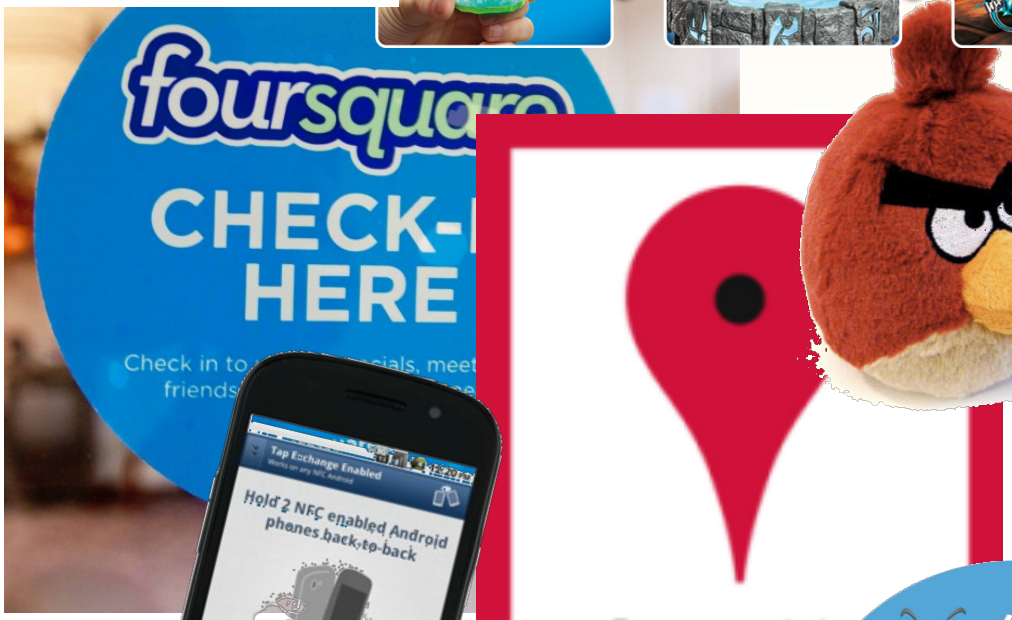
- NFC Basics and Market
- Crypto Introduction
- Secure Mobile Payments with NFC
- Questions
- Closing Thoughts

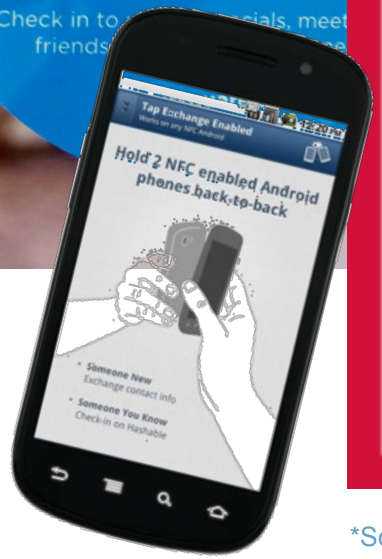
What is NFC

- Set of short-range wireless technologies, usually requiring a distance of 1 inch or less
- Operates at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s
- Very simple form factors such as tags or key fobs that do not require batteries
- Communication modes
  - Peer-to-peer
  - Tag reading/writing
  - Card emulation

Why NFC?: “Single Tap” Action

2.2B+ NFC Enabled Devices Shipping from 2011-2016*





*Source: ABI Research

- 5-6 second “single tap” check in/launch
- Connects online and physical experience
- Promotes mobile app downloads
- Showcases features in upcoming millions NFC phones
- Attribution for NFC innovation with consumers
- Leverage growing “NFC education” by ecosystem

Cryptology = Cryptography

Scope & Principles

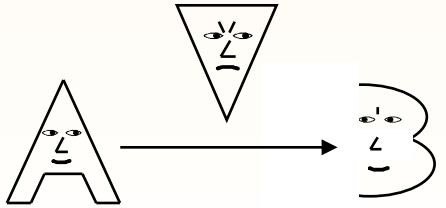
Symmetric (DES, AES) ☒ ☒

Asymmetric (RSA, ECC) ☒ ☒

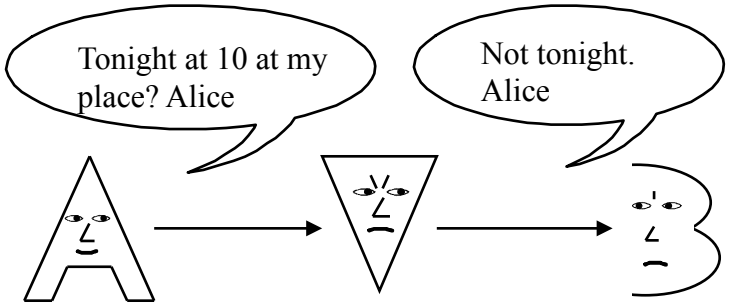
Protocols ☒

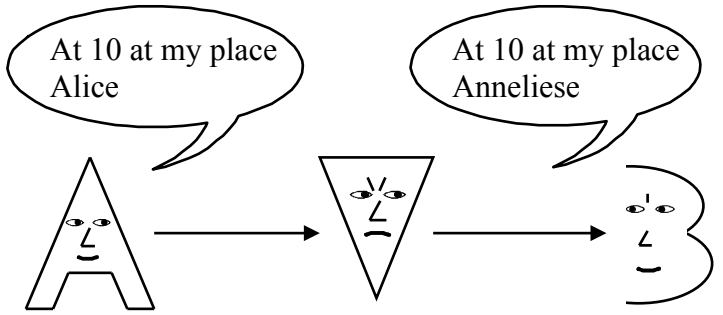
Random Numbers ☒

- The mathematical science of establishing trust
- Goal: Confidentiality
- Threat: Passive attacker eavesdrops a communication



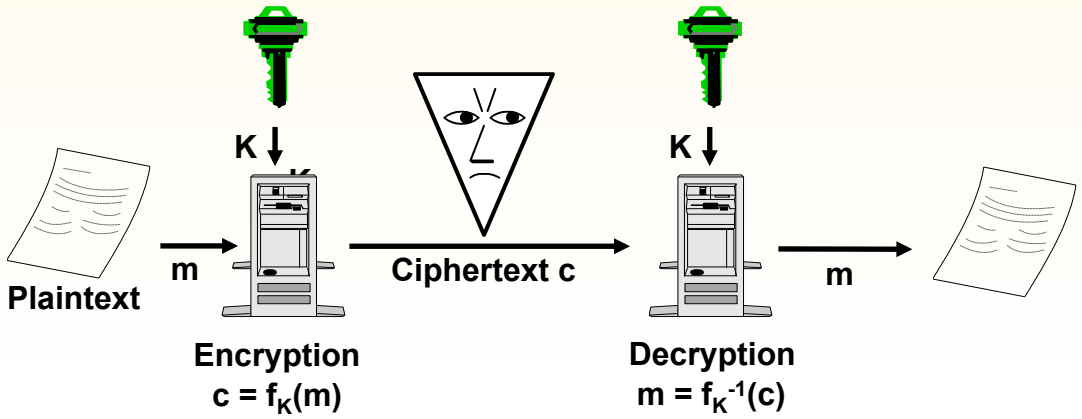
- Goals: Authenticity and Integrity
- Threat: Active Attacker influences



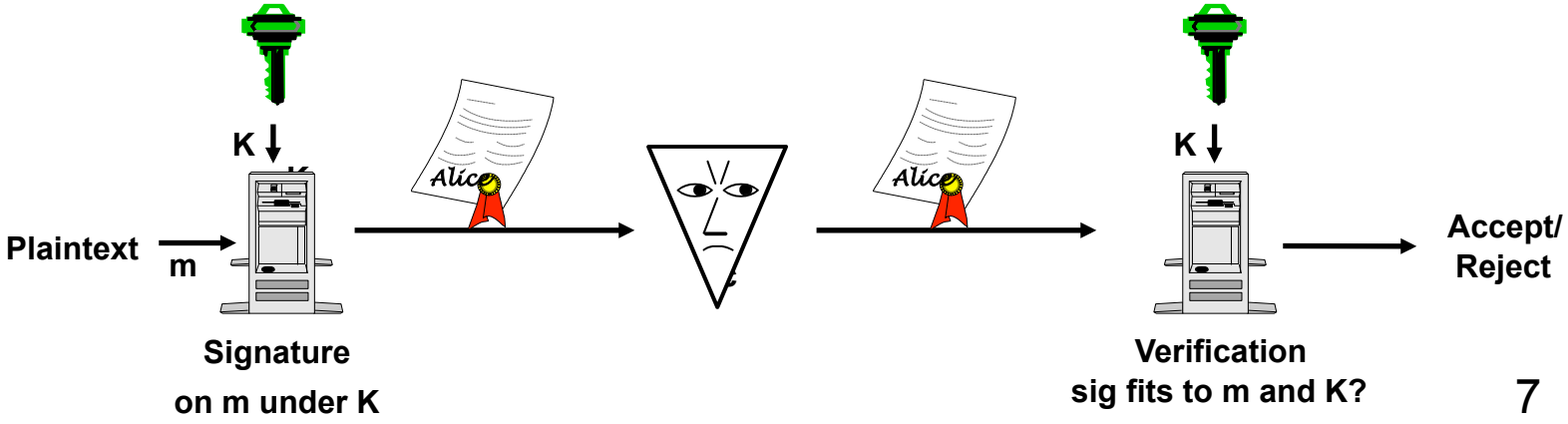


How to Achieve It

- **Confidentiality by Encryption**



- **Authenticity and Integrity by Signatures (Message Authentication Codes)**

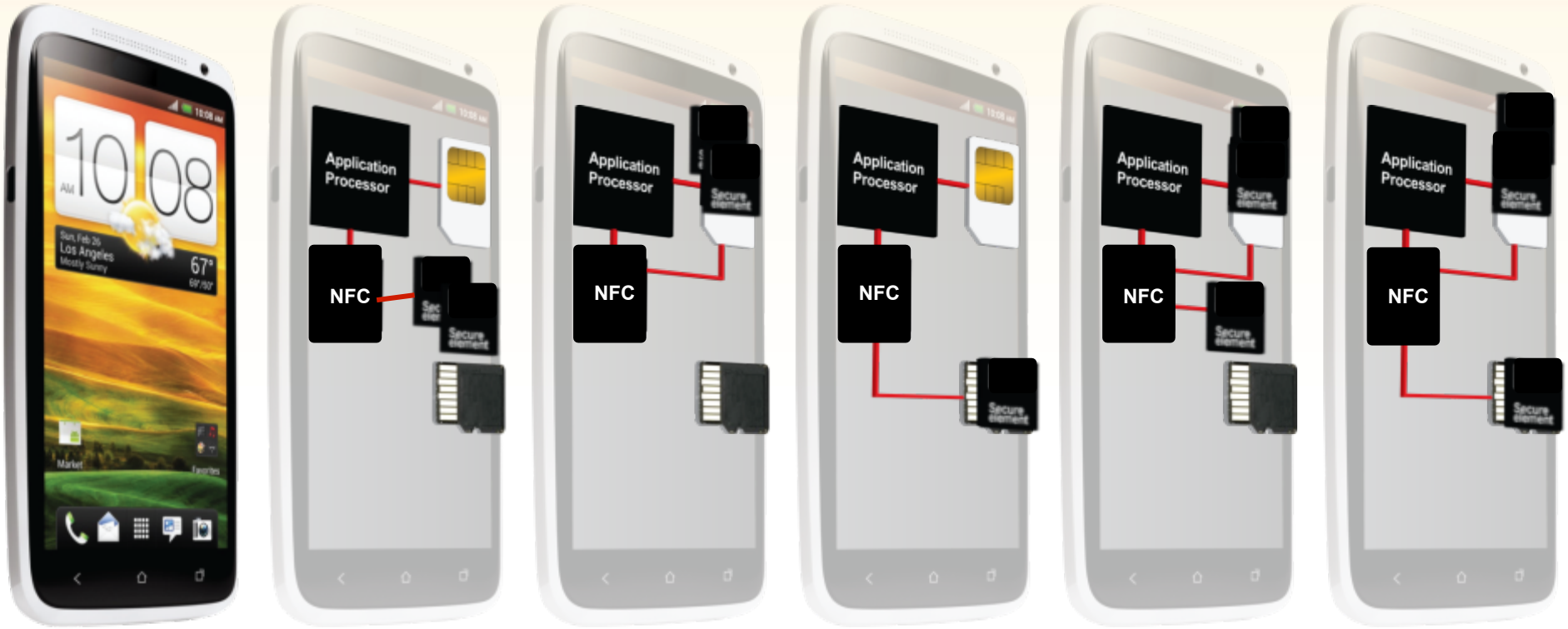


Scope of Cryptography

- Other goals
  - Non-repudiability (signatures)
  - Anonymity – Privacy Protection
- Not in scope
  - Hiding the existence of a message (e.g., in a picture or music file)
  - Coding of messages
  - Loss of data
  - Denial of Service

Ways to Implement Security in NFC

RSA CONFERENCE CHINA 2012



Secure Element Embedded (eSE)

Secure Element in the SIM socket (SWP-SIM)

Secure Element in the microSD (µSD)

Multiple Secure Elements

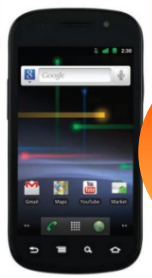
4 in 10 phones will have multiple SEs

Source: ABI Research

Embedded Secure Element (eSE)

- Chip component provides a tamper-proof environment for storing data and performing cryptographic functions
- Applications include payment services from banks, transit, ticketing, access control, and credential identifications
  - Highly secure environment needed for storing data and performing contactless transactions
- eSE plays an important role in non-NFC use cases
  - Protecting sensitive credentials for online payments
  - Authenticating enterprise applications

Benefits of eSE



Mobile OS App stores

Deploy scalable app store based services, flexible wallet with tight links to various apps and search engine (advertising)

Financial Inst.

Approve and promote phones as a full secure NFC solution

OEM

Differentiated phone offering
Secure mobile platform

MNO

Use phone differentiation attract customers and use SIM features on top if needed

End Customer

Choose a phone with available secure NFC and trusted look-and-feel

How eSE Secures Mobile Transactions

- Mobile transactions occur in Card Emulation mode
  - NFC device appears to an external reader much the same as a traditional contactless smart card
- This mode is **secure**
  - Supported by the Contactless Communication API
- Physical smart card is typically implemented as an applet and is installed in the Secure Element in either the Embedded Secure Element or UICC
- Service Provider Applications will interact with the applets in the Secure Element using ISO7816 APDU commands
- Applets will interact with the external contactless reader using ISO14443 APDU commands

Questions

Closing Thoughts

- NFC technology continues to be adopted by consumers
- Pervasive mobile lifestyle
- Payment transactions made with NFC need to be secure
- Importance of secure element

Thank You

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012