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

实现安全移动支付的 NFC 技术

Ciaran Fisher
NXP Semiconductors

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

专题会议目标

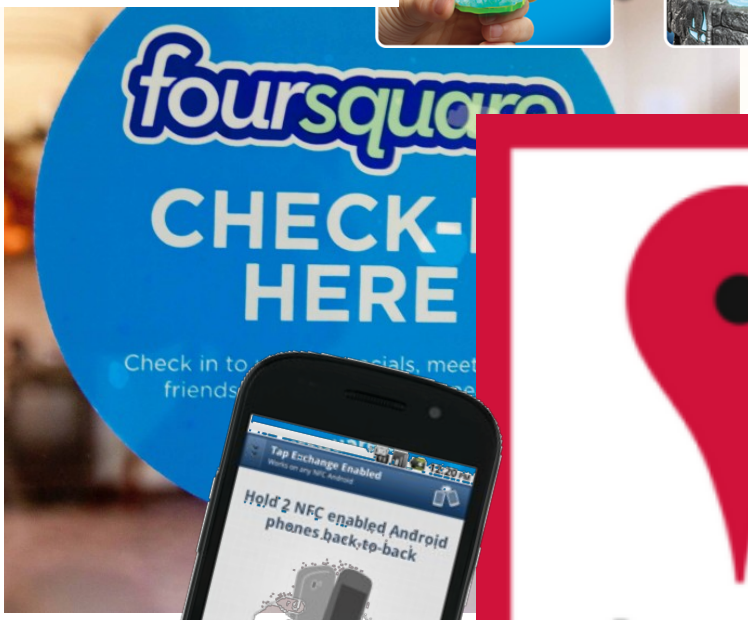
- NFC 基础知识和市场
- 加密简介
- 使用 NFC 的安全移动支付
- 问题
- 结论

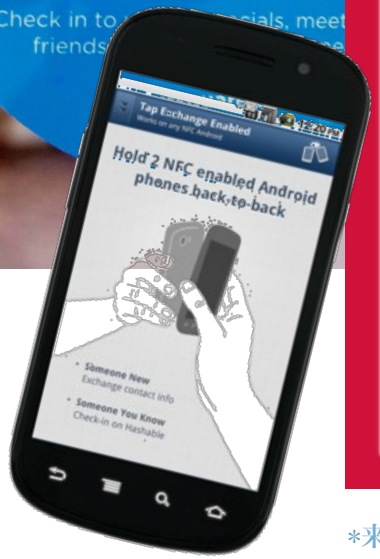
NFC 是什么

- 一组短程无线技术，通常要求距离不超过 1 英寸
- 在 ISO/IEC 18000-3 空中界面上以 13.56 MHz 频率工作，速率为 106 kbit/s 至 424 kbit/s
- 非常简单的机身结构，例如不需要电池的电子标签或钥匙扣
- 通信模式
  - 对等
  - 标签读取/写入
  - 卡模拟

为什么选择 NFC？：“单次点击”操作

2011-2016 年将推出 22 亿台支持 NFC 的设备*





*来源：ABI Research

- 5-6 秒“单次点击”签入/启动
- 提供联机和物理体验
- 促进移动应用程序的下载
- 展示即将推出的数百万部 NFC 电话中的功能
- 让消费者享受到 NFC 创新成果
- 利用生态系统提供的不断增加的 NFC 培训资源

密码学 = 密码术

范围和原则

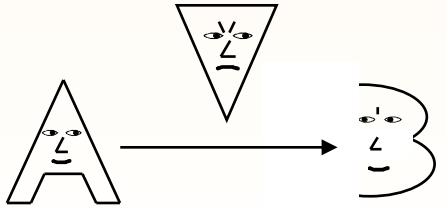
对称
（DES、AES）
☒ ☒

非对称
（RSA、ECC）
☒ ☒

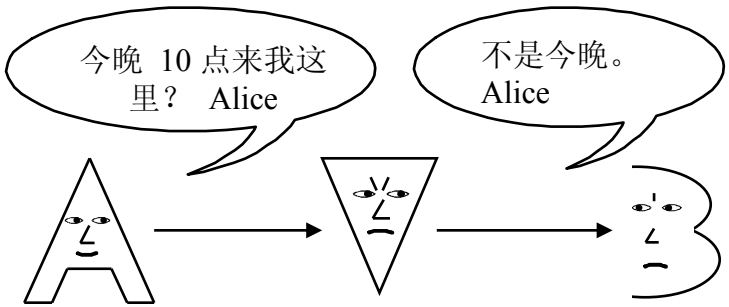
协议
☒

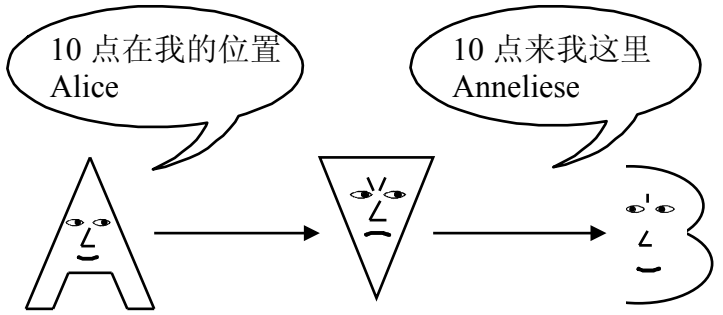
随机数字
☒

- 研究建立信任的数学科学
- 目标：机密性
- 威胁：被动攻击者窃听通信



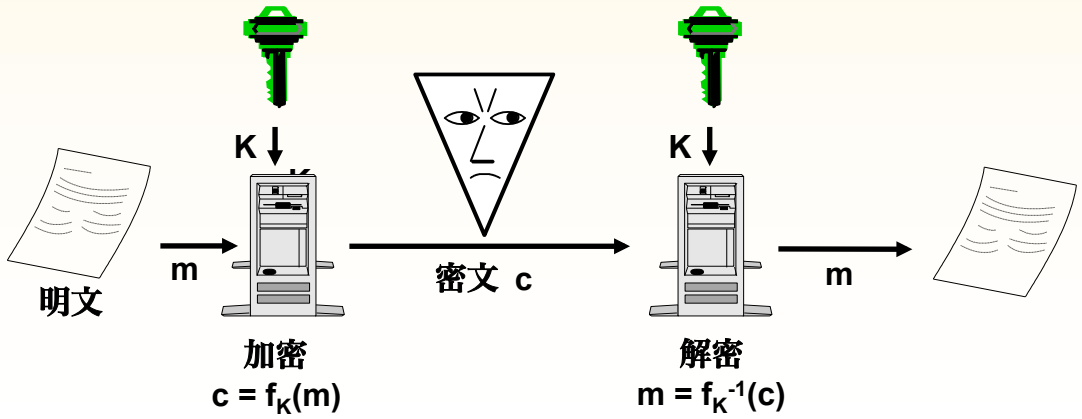
- 目标：真实性和完整性
- 威胁：主动攻击者影响



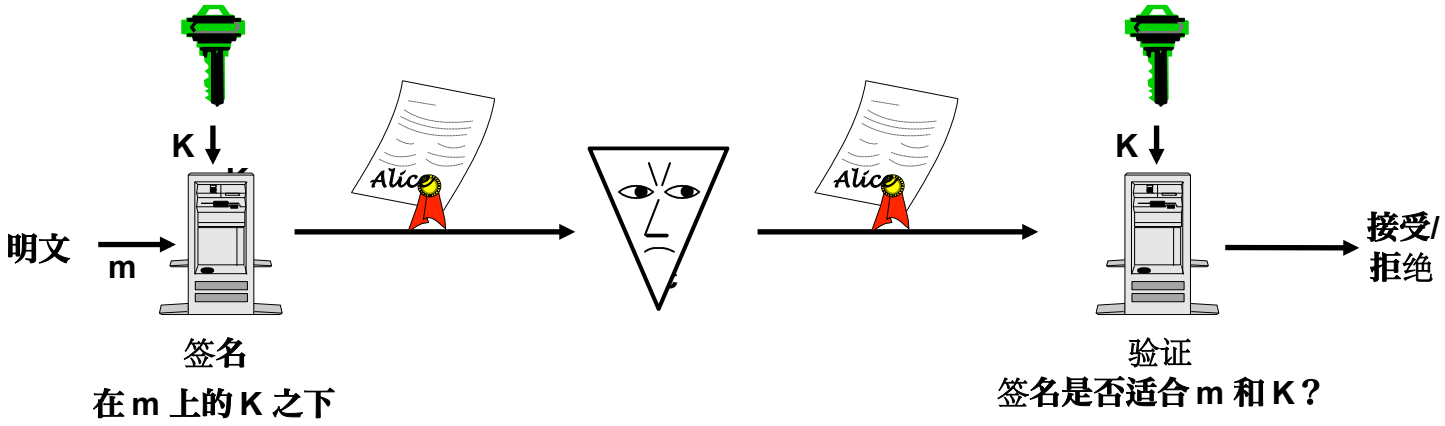


如何实现

- **通过加密实现机密性**



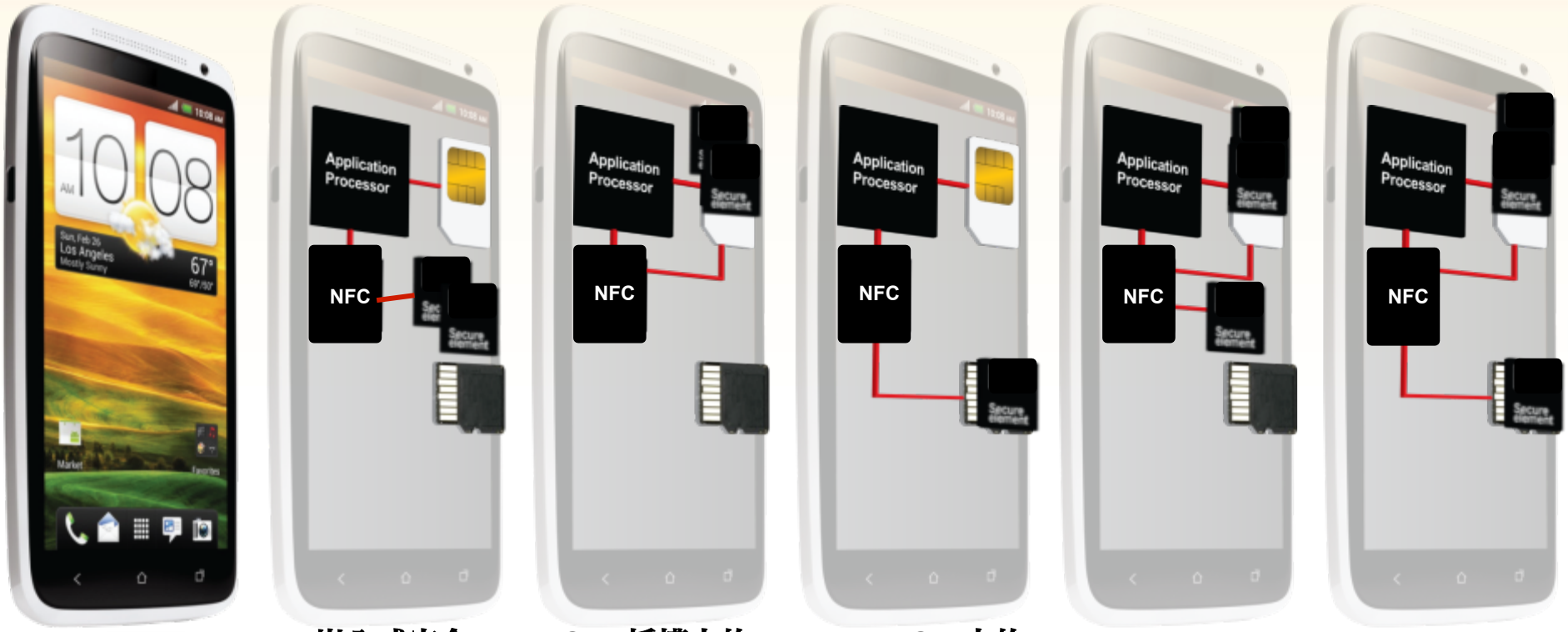
- **通过签名实现真实性和完整性（消息身份验证代码）**



密码术的作用范围

- 其他目标
  - 不可否认性（签名）
  - 匿名性 – 隐私保护
- 不在作用范围内
  - 隐藏消息的存在
    （例如，在图片或音乐文件中）
  - 消息的编码
  - 数据丢失
  - 拒绝服务

在 NFC 中实现安全性的方法



嵌入式安全要素 (eSE)

SIM 插槽中的安全要素 (SWP-SIM)

microSD 中的安全要素 (mSD)

多个安全要素

40% 的电话将具有多个 SE

来源：ABI Research

嵌入式安全要素 (eSE)

- 芯片组件提供了防篡改环境来存储数据和执行加密功能
- 应用包括银行的支付服务、传输、票证、访问控制和凭据标识
  - 存储数据和执行非接触式交易需要高度安全的环境
- eSE 在非 NFC 使用情形中发挥重要作用
  - 保护在线支付的敏感凭据
  - 对企业应用程序进行身份验证

eSE 的好处

移动 OS 应用商店

部署可扩展的基于应用商店的服务，紧密链接到各种应用程序和搜索引擎的灵活钱包（广告）

金融机构

批准并宣传手机是完全安全的 NFC 解决方案

OEM

提供安全移动平台的差异化手机

MNO

使用手机差异化来吸引客户并在需要时主要使用 SIM 功能

最终客户

选择具有可用的安全 NFC 和受信任外观的手机

eSE 如何保护移动交易

- 移动交易以卡模拟模式进行
  - 在外部阅读器看来，NFC 设备与传统的非接触式智能卡非常相似
- 此模式是安全的
  - 由非接触式通信 API 支持
- 物理智能卡通常作为小程序实现，并安装在嵌入式安全要素或 UICC 的安全要素中
- 服务提供商应用程序将使用 ISO7816 APDU 命令与安全要素中的小程序交互
- 小程序将使用 ISO14443 APDU 命令与外部非接触式阅读器交互

问题

结论

- NFC 技术不断被消费者采用
- 无处不在的移动生活方式
- 使用 NFC 进行的支付交易必须安全
- 安全要素的重要性

谢谢大家！

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012