“牵星”法：一种基于射频指纹的高频 RFID 克隆卡检测方法

张国柱[1,2,3,4], 夏鲁宁[1,2,3], 贾世杰[1,2,3,4], 嵇亚飞[1,2,3,4]

[1]中国科学院信息工程研究所 北京 100093
[2]中国科学院数据与通信保护研究教育中心 北京 100093
[3]中国科学院信息安全国家重点实验室 北京 100093
[4]中国科学院大学 北京 100049

摘要 射频识别(RFID)技术已在社会各领域得到了广泛应用, 如门禁系统、银行卡、居民身份证等。与此同时, 不断出现的 RFID 克隆卡时刻威胁着 RFID 应用系统的安全。尽管目前已提出了多种安全机制, 如基于密码学的认证协议, 并假设“密钥不出卡”, 但在侧信道分析等新型攻击手段下, 这类安全机制被绕过的风险显著增加。此外, 大量 RFID 卡的应用诸如门禁系统等并不使用密码技术, 使 RFID 卡被克隆的风险更大。本文提出了一种基于物理层特性的射频指纹识别方法—“牵星”法, 使高频 RFID 卡与其唯一且不可克隆的射频特征紧密绑定, 从而有效检测高频 RFID 克隆卡。我们对来自同厂家、同型号、同批次的 120 张高频 RFID 卡进行了测试, 识别精度可达等错误率 EER=2.5%。本方法可直接用于所有基于 ISO14443 Type A 协议的高频 RFID 克隆卡检测。同时, 由于该方法是对设备的射频指纹进行后期处理, 因此也支持其它标准定义的 RFID 克隆卡的检测。该识别系统仅由一个天线、一个读卡器和一个示波器组成, 是现有高频 RFID 卡识别系统中所需测量设备最少的一种。

关键词 射频指纹; 射频识别; 物理层; 克隆攻击; 安全
中图法分类号 TP309.1 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.04.004

“Star Drawing Operation”: A Method to Identify HF RFID Cloning Card Based on RF Fingerprinting

ZHANG Guozhu[1,2,3,4], XIA Luning[1,2,3], JIA Shijie[1,2,3,4], JI Yafei[1,2,3,4]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] Data Assurance and Communication Security Research Center of Chinese Academy of Sciences, Beijing 100093, China
[3] State Key Laboratory of Information Security, Beijing 100093, China
[4] University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Radio frequency identification (RFID) technology has been widely used in many fields, such as access control system, bank card, identification card and so on. At the same time, securities of the RFID application system are being threatened by the RFID cloning cards. A variety of security mechanisms have been proposed, such as authentication protocols based on cryptography assuming “the key is not out of the card”, however, the security mechanisms may be invalid under the new attack techniques of side channel analysis, and the risk seems to increase significantly. In addition, a lot of RFID applications, such as door forbidden system does not use password technology, then it makes the RFID cloning cards more threatening. In this work, we proposed a method to effectively identify the high-frequency RFID cloning card based on its physical characteristics-named “star drawing operation”method. In this method, the RFID card is closely bounded with its unique and cannot cloning physical characteristics. We evaluate our technique on a set of 120 cards from the same manufacturer, the same model, the same batch, and achieve EER=2.5%. This method can be directly applied to identify HF RFID cloning card based on ISO14443 type A protocol. Moreover, the method is just used to identify cards based on their RF fingerprints and does not affect the extraction process of the RF fingerprints, so it can identify all RFID cloning cards based on other standard protocols, and effectively improves the security of RFID application systems. The identification system consists of an antenna, a card reader and an oscilloscope, which has the least devices in current high frequency RFID identification system.

Key words radio frequency fingerprinting; radio frequency identification; physical layer; clone attack; security

通讯作者: 夏鲁宁, 博士, 高级工程师, Email: xialuning@iie.ac.cn。
本课题得到国家科技重大专项 973 计划(No.2014CB340603)和国家自然科学基金(No.61402470)资助。
收稿日期: 2016-06-02; 修改日期: 2016-09-23; 定稿日期: 2017-03-27

1 引言

射频识别(Radio frequency identification RFID)是一种无线通信技术, 由于其可通过无线信号识别特定目标并便捷地读写相关数据, 已在日常生活中得到了广泛应用。高频 RFID 卡更是在移动支付[1], 身份鉴别[2]和密钥管理[3]等领域得到大量应用并已成为日常生活中必不可少的一部分。与此同时, 各种针对高频 RFID 卡的安全问题也随之产生, 其中非法克隆[4,5,6]攻击可以绕过所有逻辑层面的安全机制, 严重威胁 RFID 应用系统的安全性。目前已有多类安全协议相继提出[7,8,9], 但存在一个不可忽视的事实是, 一旦 RFID 设备被成功地物理克隆, 现有的逻辑层面上的安全协议完全无法识别真伪。这是因为现有的逻辑安全协议多在传输层/应用层发挥作用, 而没有充分考虑物理层上的不可克隆属性。虽然通过假设“密钥不出卡”能够防范物理克隆, 但侧信道攻击[10]等新型攻击技术的出现使得这个假设并不十分可靠。换句话说, 逻辑安全协议确认的是“我知道什么”, 而不是“我是什么”。因此, 一旦非法设备通过物理克隆获得“我知道什么”的内容, 攻击就会成功。

近年来, 基于物理层射频特性的射频指纹识别技术得到学术界和工业界的关注。射频指纹识别意在通过提取无线通信系统发射的电磁波的射频特征来对无线设备的身份进行认证, 使设备身份与其物理特性相互绑定, 从而防范克隆攻击的发生。由于射频电子元器件的个体差异, 造成其发射出的电磁波包含自身的独特特征, 这些特征是在生产过程中产生的, 且不可人为控制, 我们将其称为“射频指纹”。射频指纹识别与人类生物特征识别技术相似, 目的是通过从无线信号中提取设备的唯一射频特征, 并用其对设备进行识别或分类[11]。现有研究表明射频指纹特征在不同的无线设备发射机中是唯一的[12]。由于射频指纹的特征与设备的物理层硬件特征紧密相关且不可人为控制, 从而可以据此检测克隆行为的发生。

目前, 有关射频指纹识别的研究主要集中在对远场信号(一个载波波长之外的空间范围)的识别上, 如 GSM 移动电话[13], ZigBee 设备[14],WiFi 设备[15]和 UHF 标签[16]等等。而对近场信号(一个载波波长之内的空间范围)的识别研究较少, 如在日常生活中广泛使用的 13.56 MHz 高频 RFID 卡。根据 ISO 14443 标准, 高频 RFID 卡在与读写器进行数据交换时, 其主要电磁传输机制是感应耦合(主要为磁耦合), 而不是远场中的辐射或后向散射, 这使得二者的射频指纹识别技术存在巨大差异。

在近场射频识别中, Romero 和 Danev 等分别对高频 RFID 卡的物理层电磁特性进行了研究。Romero[17]通过对特定谐波(载波的 3 次和 5 次谐波)的频率和相位分析, 对来自 4 个厂家的 20 张卡进行了分类, 分类准确率为 100%。实验中使用的设备包括: 两个耦合线圈, 一个读卡器和最大采样频率为 20 GHz 的示波器。随后, Romero[18]对来自同一厂家同一型号的高频 RFID 卡进行了单卡识别, 通过精确测量卡的无载谐振频率、品质因数与特定谐波(载波的 3 次谐波和 5 次谐波)的幅度相结合方法, 对 4 个不同厂家(5 张卡/厂家)的产品进行了识别, 等错误率 EER=4%。为了测量卡的谐振频率和品质因数, 实验中使用了一台带宽为 50 MHz 的矢量网络分析仪。

Danev 等[19]利用非标准载波频率(Fc =13.16 MHz)下卡响应的调制包络幅度, 对 4 种不同类型的高频 RFID 卡进行了分类, 分类准确率为 100%。在文中, Danev 等采用观察卡在冲击信号(一个持续时间为 10 个周期, 幅度为 10 V, 频率为 5 MHz 的正弦信号)和扫频信号(扫频范围为 100 Hz-15 MHz, 幅度为 10 V)下的响应特性, 对来自同一厂家同一型号的 50 张卡进行了单卡识别, 等错误率分别为 EER= 5.37%和 4.69%, 联合使用冲击和扫频信号下的响应特性, 等错误率降至 EER=2.43%。为产生非标准频率的载波信号, 实验中使用了一台包络信号生成器和一台调制信号生成器。随后, Danev[11]改进了采用冲击信号进行单卡识别的实验, 通过设置新的冲击信号(一个持续时间为 10 个周期, 幅度为 10 V, 频率为 12 MHz 的正弦信号)和改进的特征提取算法, 对来自同一厂家同一型号的 50 张卡进行了单卡识别, 等错误率 EER=0.5%。在实验中需要使用一台任意波形发生器产生所需的冲击信号。此外, 为确保提取信号的精度和稳定性必须保证任意波形发生器和示波器间的严格同步。

综上所述, 我们可以看到 Romero[17]和 Danev[11,19]的这三种单卡识别方法都存在以下问题: (1)识别过程无法在卡的正常工作状态下进行, 限制了其应用范围。文献[17]需要在卡离线状态下测量谐振频率和品质因数, 文献[11, 19]则需要在卡离线状态下测量对冲击信号和扫频信号的响应特性。(2)除了提取信号所必须的天线和示波器外, 还需要额外的测量设备。如文献[18]需要矢量网络分析仪, 文献[11,19]则需要任意波形发生器等。(3)测试过程复杂且条件要求较高。如文献[19]中的方法需要保证任意波形发生器和示波器间的严格同步。

在本文, 我们提出了一种可在正常工作状态下对 ISO14443 Type A 高频 RFID 卡进行单卡识别的方法, 其基本思想是在系统初始化阶段, 随机选取若干卡构成“星座”, 然后将待识别卡与“星座”中的每一张卡基于射频指纹建立一一对应关系对, 再通过对每个关系对的逐一判断进行单卡识别。由于这种方法跟古代航海定位导航技术“牵星术”[20]有某种程度的相似性, 我们将其形象地称为“牵星”法。通过对来自同一厂家同一型号同一批次的 120 张卡进行检测, 我们获得了等错误率 EER=2.5%的单卡识别精度。该方法是通过提取正常工作状态下卡的信号进行识别, 因此仅需天线和示波器就能完成信号的采样工作, 大大简化了识别系统的构成和测试过程。

本文的主要贡献如下:

(1) 提出了一种针对 ISO14443 Type A 高频 RFID 卡的射频指纹识别方法——“牵星”法。利用该方法不需要使用复杂的分类器如支持向量机[21]和概率神经网络[14]等就可进行单卡识别, 减少了训练样本的数量, 提高了计算效率,降低了识别难度。

(2) “牵星”法具有良好的适用性和可扩展性。原则上获得了同类设备的射频指纹之后, 都可以用该方法进行识别。因此其他标准定义的 RFID 设备(即: 非本文所针对的 ISO14443 Type A 类型的 RFID 设备)也可以基于本方法进行克隆检测。

(3) 在高频 RFID 卡的响应信号中, 发现任意一个高半位部分都可以作为提取射频指纹的区间, 并且仅需一个高半位就可进行单卡识别, 提高了识别效率。

(4) 克隆卡检测系统仅由一个天线、一个读卡器和示波器组成, 在现有的单卡识别系统中需要的测量设备最少。

本文结构如下: 第 2 节简要介绍了射频指纹和射频识别的背景知识; 第 3 节介绍了利用“牵星”法进行单卡识别的原理和过程; 第 4 节详细介绍了利用“牵星”法进行单卡识别的实现; 第 5 节给出了实验效果; 第 6 节讨论了阈值 T 对识别精度的影响, 以及错误接受率和错误拒绝率的波动性, 验证了卡响应信号的任意一个高半位都可以作为提取射频指纹的区间, 最后讨论了卡的不同摆放方式对射频指纹的影响; 第 7 节介绍了射频指纹识别的相关工作; 最后在第 8 节对全文进行了总结。

2 背景

本节首先介绍了射频指纹的概念、应用范围和识别过程, 然后简要介绍了射频识别技术以及在 ISO 14443 Type A 标准下读写器与高频 RFID 卡的交互过程。

2.1 射频指纹

射频指纹是指由于射频设备电子元器件的个体差异, 导致其发射出的电磁波包含设备的独特特征, 人们形象化地将这种与具体设备相关联的物理层上的模拟和数字信号特征, 称为“射频指纹”[12]。射频指纹可以用于入侵检测、身份认证、数据取证和保障监测等各个领域。简单的讲, 由于设备制造过程的差异性, 没有两个设备是完全相同的, 它们发射出的射频信号的特征也不完全相同,因此可以通过 “射频指纹”对设备进行识别和认证。

对于高频 RFID 卡, 射频指纹的识别过程主要包括以下 4 个步骤[22]: **(1)信号检测**。当高频卡与读写器通信时, 利用示波器捕获卡的响应信号, 根据检测的起始时刻对捕获信号进行对齐与截取,获得所需的兴趣区间(Region of Interesting ROI)。**(2)特征提取**。对(1)中获得的信号进行处理, 计算特征参量。**(3)特征选择**。此项为可选步骤, 它的主要任务是减少特征点数, 剔除无关数据, 以提高识别的准确率和效率。**(4)目标识别**。将提取的目标信号特征与数据库中的信号特征对应项进行比对判断。

2.2 RFID 技术

RFID 系统主要包括三个组成部分[23], 即读写器、卡(有时称为标签)和应用软件系统。读写器通过发送和接收射频信号与卡进行通信。卡一般由天线、微型芯片和外部封装组成。RFID 系统工作的频率范围非常广泛, 大致可以分为低频(Low Frequency LF)(30-300 kHz)、高频(High Frequency HF)(3-30 MHz)、超高频(Ultra High Frequency UHF)(868-928 MHz)和微波(2.45 GHZ、5.8 GHz)。根据卡内部是否有供电电源, 可将其分为无源卡和有源卡。无源卡不具有内置电源, 它通过磁耦合感应接收读写器发出的电磁场为内部电路供电,计算能力和硬件资源有限, 一般用在近距离识别场景。有源卡由于具有内置电源, 因此可一直保持在活动状态, 与无源卡相比有更多的计算能力和资源, 工作范围更大。但是, 由于内置电源的限制, 使它们较为笨重和昂贵, 时效性受到约束, 因此制约了其在高端设备上的广泛应用。

在本文中, 我们的目标是针对目前广泛使用的 ISO 14443 Type A 类型的无源高频(13.56 MHz) RFID 卡[24]进行基于射频指纹的单卡识别, 以检测被物理克隆的卡。根据 ISO 14443 Type A 标准, 读写器与卡进行数据交换时的初始速率为 106 kb/s。当数据由读写器发送到卡时, 采用 ASK 调制, 调制深度为 100%,

编码采用改进的米勒编码(Improved Miller encoding)。当数据由卡发送到读写器时, 调制方式为卡的负载调制, 调制频率为 848 kHz, 但是卡的负载调制对读写器射频场的幅度影响较小, 编码采用曼彻斯特编码(Manchester encoding)。因为, 在卡的响应信号中每个曼彻斯特编码的高半位都包含 4 个高频率的方波脉冲, 所以卡的响应信号中包含更多的物理层特征[24]。读写器与卡的数据交互过程如下: 读写器通过发出询问命令 REQA 识别工作范围之内是否有 Type A 类型的卡; 所有在工作范围之内的 Type A 卡收到命令之后均回复 16 位长的响应信号 ATQA。ATQA 中第 1-5 位中的某个位置 1 其它位置 0 用来防止比特帧冲突。如果在读写器的工作场中有多个响应信号回复, 读写器将检测到冲突的发生并选择与其中的一张卡进行单卡通信和交换信息。

文中后续描述中用到的主要符号和变量, 总结如下表:

表 1 文中用到的主要符号和变量

符号	含义	符号	含义
a(n)	瞬时幅度	φ(n)	瞬时相位
f(n)	瞬时频率	σ^2	方差
γ	偏度系数	κ	峰度系数
F	统计指纹	$SR_{(i)}$	第 i 个子区间
N_{SR}	子区间的个数	S_w	类内散射矩阵
S_b	类间散射矩阵	T	阈值
N_{gen}	真匹配次数	N_{imp}	假匹配次数
$ROI_{envelop}$	ROI 区间信号的包络		
w	通过 S_w 和 S_b 计算得到的投影矢量		
S_i	组成星座的第 i 个星卡		
I_j	需要识别的第 j 个发行卡		
T_j	需要识别的第 j 个测试卡		
Set_{S_i}	星卡 S_i 的训练样本投影之后的集合		
Set_{I_j}	发行卡 I_j 的训练样本投影之后的集合		
scr	测试卡 T_j 与发行卡 I_j 的相似度系数		
n_f	在对 n 个关系对评估时出现 0 的次数		

3 识别方法和过程

在本节我们将详细介绍“牵星”法的基本原理和利用该方法进行单卡识别的主要过程。

3.1 “牵星”法的基本原理

利用“牵星”法进行单卡识别的原理如图 1 所示。首先从所有待识别卡中随机取出若干卡 S_i (i=1, 2,…, n)作为“星卡”, 假设每个“星卡”的射频指纹在空间的分布如图 1 所示, 我们将此分布称为“星卡”S_i (i=1, 2,…, n)的射频指纹在空间组成的“星座”。发行卡 I_j (j=1, 2,…, m)在使用之前, 首先计算其射频指纹, 将发行卡 I_j 与每个“星卡” S_i 构成一个关系对(S_i, I_j), 通过线性判别式分析(Linear Discriminant Analysis LDA)算法对其进行训练。当 n 个关系对训练完成之后, 假设发行卡 I_j 的射频指纹在“星座”图中的位置如图 1 所示。

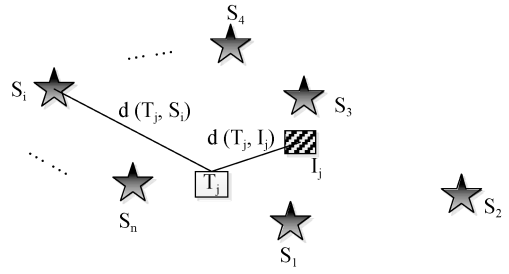


图 1 “牵星”法原理图

当需要验证测试卡 T_j 是否为发行卡 I_j 时, 分别计算 T_j 的射频指纹与 n 个关系对(S_i, I_j)中 S_i、I_j 的距离 d(T_j, S_i)、d(T_j, I_j)。如果 T_j 为真正的 I_j, 由于经过前期训练, 在每个关系对中 T_j 会离 I_j 比 S_i 更近一些, 即 d(T_j, I_j)<d(T_j, S_i) (i=1, 2,…, n)。如果 T_j 不是真正的 I_j, 那么在 n 个关系对中 T_j 离 I_j 近还是离 S_i 近会呈现随机分布, 即 d(T_j, I_j)不总是小于 d(T_j, S_i)。因此, 我们可以利用这个规律验证 T_j 是否为真正的 I_j。

在“牵星”法中, 我们将高频卡射频指纹测量的绝对值转化为与 n 个参考对象组成的关系对(S_i, I_j) (i=1, 2,…, n)中的相对值, 然后再利用测试卡 T_j 与 S_i、I_j 距离的规律进行识别。通过“牵星”法, 我们将高频卡的识别问题转化为它与 n 个参考对象的多次两两识别问题, 并且在 1 次两两识别过程中只涉及到 2 张卡, 只需要采用 LDA 法对卡进行训练之后, 就很容易地进行两两识别, 大幅降低了识别难度。因此利用该方法不需要使用复杂的分类器如支持向量机[21]和概率神经网络[14]等就可进行单卡识别, 减少了训练样本的数量, 提高了计算效率, 降低了识别难度。

虽然不同厂家生产的高频卡可以通过测量其信号的幅度直接进行分类识别[19], 但同一厂家、同一型号、同一批次的 RFID 卡的射频特征经常表现出高度的相似性, 直接使用测量值很难进行单卡识别。对相同测试样本使用“牵星”法和不使用“牵星”法的识别结果对比将在 5.3 节给出。

3.2 “牵星”法的识别过程

利用“牵星”法进行单卡识别的流程框图如图 2 所示。(1)通过示波器提取读写器与卡的第一个握手信号(REQA-ATQA); (2)从 ATQA 选择一个逻辑位的高半位作为 ROI; (3)采用希尔伯特变换提取 ROI 的

包络; (4)计算包络信号的统计指纹特征; (5)将所有待识别的卡分为两个子集: “星座”和“发行卡”; (6)通过射频指纹为两个子集中的卡建立一对一的“关系对”, 并设置阈值 T; (7)当检测时, 首先提取测试卡的统计指纹特征, 根据测试卡的惟一标识符(Unique Identifier UID)找到关系表中的对应卡, 并对 n 个关系对逐一判定, 计算出相似系数 scr;(8)判定。如果 $scr \geq T$, 判定为真; 否则判定为假并给出警告信息。整个识别过程除第一步信号采集外, 全部由软件实现。

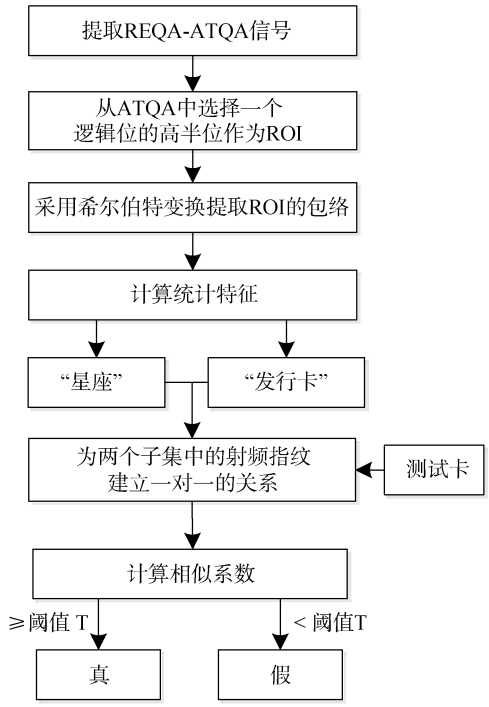


图 2　单卡识别流程框图

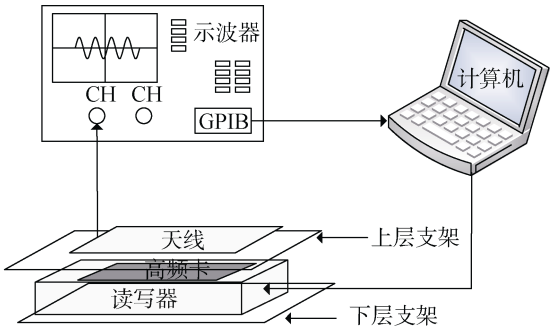
为评估识别系统的精度, 我们对来自同一厂家、同一型号、同一批次的 120 张 ISO14443 Type A 高频 RFID 卡行了检测。我们所使用的卡是具备典型意义的, 该类卡已在移动支付、访问控制和身份认证等方面得到了广泛应用, 出现在了日常生活中的各个方面。

4　实现

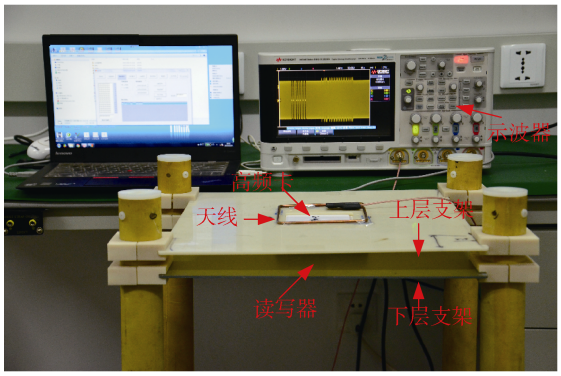
在本节我们给出了采集 REQA-ATQA 信号的测试设备, 并详细描述了利用“牵星”法进行单卡识别的过程。

4.1　测试设备和数据收集

图 3(a)和(b)分别给出了测试框图和对应的测试设备。测试设备组成如下: 带宽为 200 MHz 的示波器(型号 KEYSIGHT 3000), 读写器(Q-M8U2-N), 一个采样天线(紫铜线圈, 大小为 12 cm×12 cm)。为了测试方便, 我们搭建了一个塑料材质的两层支架结构, 如图 3 (b)所示。读写器放在下层支架上, 在上层支架的中央, 我们开了一个矩形槽, 通过矩形槽正好可将测试卡放到读写器上。天线放在上层支架上, 并与示波器相连。读写器和示波器均与电脑相连。测试所用的示波器带宽小, 价格低, 体型小, 并且所用的采样天线尺寸也较小。因此, 该识别系统可方便搭建并用于实际测试。



(a) 测试框图



(b) 测试设备

图 3　测试框图和测试设备

高频 RFID 卡主要由三部分组成: 芯片模块, 天线和外部封装组成。卡的参数如表 2 所示。其中, 卡的长度 L、宽度 W 和厚度 T 分别为 85.6 mm, 54 mm 和 0.84 mm。芯片模块为复旦 FM11RF08 芯片。卡中天线的形状为矩形, 最外层天线的尺寸为 70 mm×40 mm, 天线线圈数为 6, 线距为 1 mm,线径为 0.13 mm, 材料为铜丝。外层的封装材料为聚酯。

表 2　卡的参数

芯片模块	FM11RF08
卡的尺寸(L×W×T)	85.6 mm× 54 mm× 0.84 mm
天线尺寸(L×W)	70 mm×40 mm
天线圈数	6
线径	0.13 mm
线距	1 mm
天线材料	铜
封装	聚酯

测试时, 首先对每张卡编号(数字从 1 到 120)。每张卡的数据分三轮采集。每轮数据的采集过程如下:

(1) 将目标卡放置在读写器上, 计算机控制读写器发出寻卡命令 REQA, 卡回复响应命令 ATQA, 示波器记录整个握手过程并将数据传送至计算机用于分析, 每张卡重复 50 次信号采集过程。

(2) 然后, 用新卡替换旧卡并放置在读写器上, 再采集和存储 50 个握手信号。

对 120 个卡进行第一轮数据采集后, 我们可以获得 6000 个握手信号。因此, 经过三轮数据采集后, 每张卡可获得 150 个握手信号, 120 张卡总共可获得 18000 个握手信号。每轮测试结束时, 关闭所有设备, 在进行下一轮测试时重新开启。在信号采集过程中, 为避免影响卡与读写器的正常通信, 除正在测试的卡外, 其余卡都放在读写器的工作场之外。

图 4 给出了示波器采集到的读写器与卡的第一个握手信号 REQA-ATQA。读写器发出的 REQA 信号用来寻找读写器的工作场内是否有 type A 卡。卡的响应 ATQA 则通知读写器存在 type A 卡。根据 ISO 14443 type A 标准, 卡的响应信号 ATQA 的调制方式为负载调制, 采用曼彻斯特编码。该 ATQA 信号的曼彻斯特编码为 1001000000000000001。

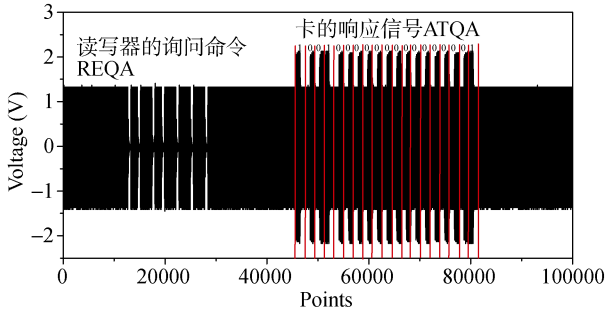


图 4 REQA-ATQA 握手信号

4.2 选择信号的 ROI

本节介绍如何选择生成射频指纹的信号区间 ROI。

根据曼彻斯特编码规则, 一个逻辑位由两部分组成: 逻辑高半位和逻辑低半位。图 5 给出了图 4 中 ATQA 信号第一个逻辑位的放大图。从图 5 中可以看出: (1)只有高半位被卡的负载调制过, 每个高半位都包含 4 个高频率的方波脉冲, 这些方波脉冲的调制频率为 848 kHz; (2)低半位为读写器发出的高频载波信号, 没有经过卡的负载调制。因此在一个逻辑位中高半位比低半位包含更多的可识别信息[24]。

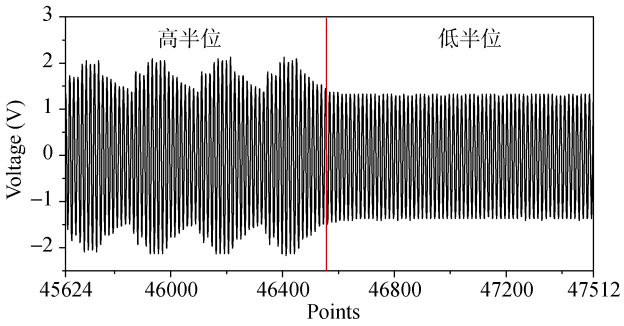


图 5 ATQA 信号中的第一个逻辑位

由图 4 可知, ATQA 响应信号中共有 19 个高半位。在实际识别过程中, 我们发现并不需要将 19 个高半位全部作为 ROI, 而只需选取其中任意一个高半位作为 ROI 来提取射频指纹。因此, 为最大程度上减少识别过程中的计算量, 我们只选择一个逻辑位的高半位作为提取射频指纹的信号区间 ROI。

4.3 提取 ROI 区间信号的包络

从 REQA-ATQA 握手信号中提取到的第一个高半位信号区间 ROI 如图 6(a)所示。载波信号和卡负载调制信号的幅度分别为 1.4 V 和 2 V。为去除载波信号对卡负载调制信号的干扰, 我们采用希尔伯特变换[31]提取 ROI 信号的包络, 并用 $ROI_{envelop}$ 表示。图 6(b)给出了采用希尔伯特变换后得到的 ROI 信号包络, 可见, 移除载波信号以后, 4 个包含负载调制的方波脉冲变得更加清晰。

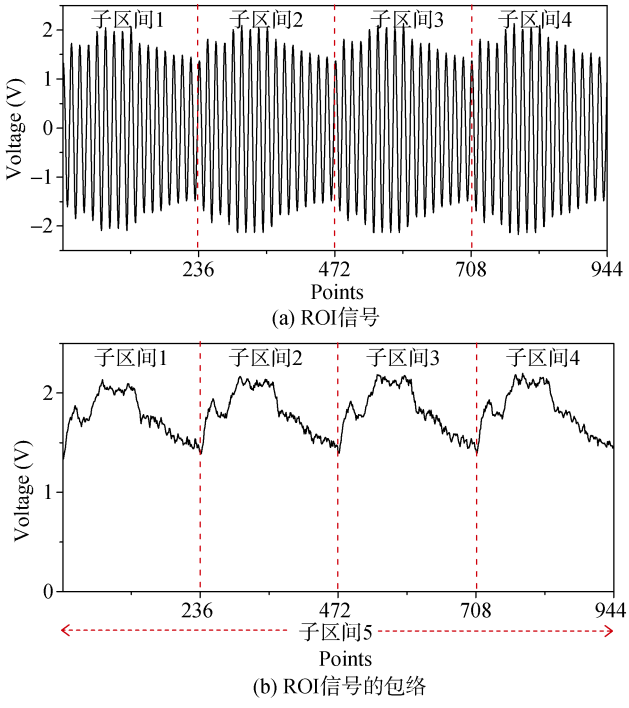


图 6 提取到的 ROI 和它的包络

4.4 生成高阶统计指纹

近年来使用高阶统计量提取无线设备射频指纹的文献逐渐增多。信号的高阶统计量[22]主要包括: 均值、最大互相关系数、标准差、方差、香农熵、二阶中心矩、偏度系数和峰度系数等。文献[14,22,28]中全部使用了标准差、方差、偏度系数和峰度系数这 4 个高阶统计量。

为进一步优化评估过程, 我们对 4 个常用的高阶统计量(标准差、方差、偏度系数和峰度系数)进行单独和组合使用“牵星”法时, 在阈值 T=100%时的识别效果进行了初步评估, 评估结果如表 3 所示。从表 3 中可以看到, 标准差、方差、偏度系数、峰度系数在单独使用时的等错误率 EER(代表了识别效果)分别为 7.9%、7.8%、16.6%和 13.6%。这表明标准差和方差的识别效果基本一致, 峰度系数次之, 偏度系数最次。根据 4 个高阶统计量单独使用时的识别效果, 我们对其进行了优化组合。当使用方差和峰度系数这两个高阶统计量时, 识别精度可以达到 EER=4.7%。当使用方差、偏度系数和峰度系数这 3 个高阶统计量时, 可以达到最高的识别精度 EER=4.2%。当 4 个高阶统计量全部使用时, 识别精度为 EER=4.5%。

表 3 4 个常用高阶统计量的识别效果评估

高阶统计量	“星卡”个数	EER (%)
标准差	11	7.9
方 差	11	7.8
偏度系数	5	16.6
峰度系数	6	13.6
方差 标准差	11	8.0
方差 偏度系数	14	6.2
方差 峰度系数	21	4.7
偏度 峰度系数	9	10.5
方差 偏度系数 峰度系数	22	4.2
标准差 方差 偏度系数 峰度系数	20	4.5

从以上讨论中可以看到, 使用方差、偏度系数和峰度系数这 3 个高阶统计量进行单卡识别时, 不但可以达到最高的识别精度, 并且与使用 4 个高阶统计量相比较, 可以减少 25%的计算量。因此, 本文没有与参考文献[14,22,28]一样采用 4 个高阶统计量, 而只采用方差、偏度系数和峰度系数 3 个高阶统计量提取高频 RFID 卡的射频指纹。

射频指纹的生成过程如图 7 所示, 主要由以下 4 个步骤组成:

(1) $\mathrm{ROI}_{envelop}$ 被划分为 5 个子区间

图 6(b)给出了 ROI 的子区间划分结果。因为一个高半位包含 4 个方波脉冲并且每个方波脉冲的长度都相同。因此, 我们将 ROI 按照方波脉冲的长度划分为 4 个长度相等的子区间, 每个子区间由 236 个数据点组成。整体的 ROI 作为另外一个子区间。因此, ROI 共被划分为 N_{SR}=(4+1)=5 个区间。

(2) 瞬时信号生成

在每一个子区间中, 需要生成三个瞬时信号: 瞬时幅度(IA)用 a (n)表示, 瞬时相位(IP)用 φ(n)表示, 瞬时频率(IF)用 f (n)表示。为了计算 φ(n)和 f (n), 首先通过希尔伯特变换将实值信号 a(n)变为正交的 I-Q 信号 $S_c(n)$。

$$S_c(n) = Hilbert(a(n)) = S_I(n) + j * S_Q(n) \tag{1}$$

其中 n=1, 2,…, N_x, N_x 为子区间中信号的总点数。

瞬时相位 IP 和瞬时频率 IF 的计算公式为:

$$\varphi(n) = \tan^{-1}[\frac{S_Q(n)}{S_I(n)}] \tag{2}$$

$$\mathrm{f}(n) = \frac{1}{2\pi}[\frac{d\varphi(n)}{dn}] \tag{3}$$

为去除系统采样的偏差, 瞬时幅度 IA 和瞬时频率 IF 进行“中心化”(减去均值)处理, 计算公式见式(4)和式(5)。其中 μ_a 和 μ_f 是子区间中 N_x 个点的幅度和频率均值。

$$\mathrm{a}_c(n) = \mathrm{a}(n) - \mu_a \tag{4}$$

$$\mathrm{f}_c(n) = \mathrm{f}(n) - \mu_f \tag{5}$$

最后, “中心化”后的信号 $a_c(n)$和 $f_c(n)$用各自幅度的最大值进行归一化处理, 以补偿功率的变化。

(3) 高阶统计特征计算

每一个子区间中的瞬时信号, 经“中心化”、归一化之后得到序列 $\bar{\mathrm{x}}_c(n)$, 计算序列 $\bar{\mathrm{x}}_c(n)$ 的 3 个统计参数: 方差 σ^2, 偏度系数 γ, 峰度系数 κ。

计算公式如下:

$$\sigma^2 = \frac{1}{\mathrm{N}_x}\sum_{n=1}^{\mathrm{N}_x}(\bar{x}_c(n) - \mu)^2 \tag{6}$$

$$\gamma = \frac{1}{\mathrm{N}_x\sigma^3}\sum_{n=1}^{\mathrm{N}_x}(\bar{x}_c(n) - \mu)^3 \tag{7}$$

$$\kappa = \frac{1}{\mathrm{N}_x\sigma^4}\sum_{n=1}^{\mathrm{N}_x}(\bar{x}_c(n) - \mu)^4 \tag{8}$$

(4) 指纹生成

每个子区间中每个瞬时信号的 3 个统计参数按照一定顺序级联在一起组成矢量 $\mathrm{F}_{SR(i)}$, 其中 i=1, 2, 3, 4, 5。

$$F_{SR(i)}=[\sigma^2_{SR(i)}\ \ \gamma_{SR(i)}\ \ \kappa_{SR(i)}]_{1\times3} \tag{9}$$

对每个选定的信号, 5 个子区间中的矢量 $F_{SR(i)}$ 按照一定的顺序级联组成新矢量 F^C:

$$F^C=[F_{SR(1)}\ F_{SR(2)}\ F_{SR(3)}\ F_{SR(4)}\ F_{SR(5)}]_{1\times5} \tag{10}$$

其中上标 C 表示一个具体的特征, 即: 幅度 a,相位 φ 或频率 f。

因此, 对一个高半位信号的 $ROI_{envelop}$, 综合考虑 IA、IP 和 IF, 得到的统计指纹 F 如公式 11 所示, 统计指纹 F 中的元素数为 3×5×3=45 个。

$$F=[F^a\ F^\varphi\ F^f]_{1\times45} \tag{11}$$

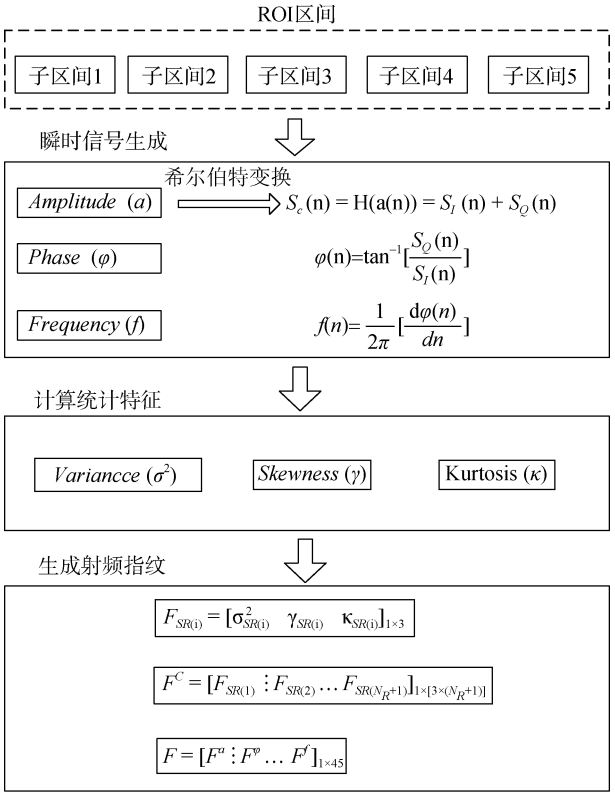


图 7 高阶统计指纹生成过程

4.5 建立“星座”与发行卡的关系

本节的目的是建立“星座”中的“星卡”和待识别卡之间的一一对应关系。

构建的过程如下:

(1) “星卡”的选择。从待识别的 N 个卡中随机选择 n 个卡作为“星卡”, 每个“星卡”记为 S_i (i=1, 2,…, n), 剩余的 m=(N-n)个卡作为发行卡用来评估识别效果, 记为 I_j (j=1, 2,…, m)。

(2) 构建“星卡”与发行卡之间的关系。对任意一张发行卡 I_j, 需要与“星座”中的 n 张“星卡”逐一建立关系(S_i, I_j) (i=1, 2,…, n)。对全部的 m 张发行卡进行类似的操作, 可得到(m×n)个关系对, 如表 4 所示。

表 4 “星卡”与发行卡的一一对应关系

发行卡 \ “星卡”	S_1	S_2	…	S_n
I_1	(S_1, I_1)	(S_2, I_1)	…	(S_n, I_1)
I_2	(S_1,I_2)	(S_2,I_2)	…	(S_n, I_2)
…	…	…	…	…
…	…	…	…	…
I_m	(S_1, I_m)	(S_2, I_m)	…	(S_n, I_m)

每一个关系对(S_i, I_j)的构建过程如下: 由于在每个关系对(S_i, I_j)中只有两张卡, 为增加两者之间在识别时的分隔距离, 我们采用经典的 LDA 方法[32], 将生成的统计指纹投影到 1 维空间上。给定两个卡的训练指纹样本之后, 采用 LDA 变换计算类内(每个卡的训练样本之间)散射矩阵 S_w 和类间(两个卡之间的训练样本)散射矩阵 S_b。S_w 和 S_b 的计算公式分别为式 12 和式 13。

$$S_w=\sum_{j=1}^{c=2}\sum_{i=1}^{N_j}(x_i^j-\mu_j)(x_i^j-\mu_j)^T \tag{12}$$

其中, c 代表卡的个数(类型数), 由于只有两张卡, 因此 c=2。x_i^j 是 j 卡的第 i 个样本, μ_j 是 j 卡所有训练样本的均值。N_j 是 j 卡中所有参加训练的样本数。

$$S_b=\sum_{j=1}^{c=2}(\mu_j-\mu)(\mu_j-\mu)^T \tag{13}$$

其中, μ 表示所有参加训练卡的统计指纹均值。

投影矢量 W 通过计算 $S_W^{-1}S_b$ 的最大特征值对应的特征矢量获得。因此, 每个关系对(S_i, I_j)中两张卡的统计指纹都可以通过投影矢量 W, 利用公式 14 投影到一维 LDA 空间上。

$$F^W=W^TF \tag{14}$$

对 S_i 和 I_j 的所有训练样本, 利用公式 14 分别投影得到集合 Set_{S_i} 和 Set_{I_j}。计算完成之后, 对每一个关系对(S_i, I_j)只需要存储投影矢量 W 和各自的投影集合 Set_{S_i} 和 Set_{I_j}, 利用发行卡 I_j 的 UID 作为索引以便于后续的查找使用。对 m 个发行卡重复上述过程, 最后可得到 m 行, n 列的矩阵形式, 如表 4 所示。

4.6 识别过程

本节介绍如何通过 4.5 节中建立的表 4 进行单卡识别。

具体的识别过程如下:

(1) 读写器与测试卡 T_j 的握手信号 REQA-ATQA 通过示波器抓取, 卡的 UID 通过读写器得到。如果

测试卡的 UID 没有在表 4 找到, 则此测试卡直接被判定为非法并给出警告, 如果测试卡的 UID 存在于表 4 中, 识别系统执行下一步。

(2) 根据图 7, 生成 T_j 的统计指纹 F_{T_j}, 根据 T_j 的 UID 找到表 4 中的相应行 I_j。

(3) 采用马氏距离逐一判断 F_{T_j} 属于关系对 (S_i, I_j) (i=1, 2,…, n)中 S_i 和 I_j 的训练样本产生的投影集合 Set_{S_i} 和 Set_{I_j} 中的哪一个。如果距离集合 Set_{I_j} 更近, 则记为“1”, 否则记为“0”。逐个评估 n 个关系对之后, 可得到由 n 个 0 和 1 组成的字符串, 并将此字符串记为 Str。

(4) 计算测试卡 T_j 与发行卡 I_j 的相似度系数 scr。scr 的值越接近 100%表示 T_j 与 I_j 的相似度越高。

$$\text{scr}=\frac{HW(Str)}{n}\times 100\% \tag{15}$$

其中 HW (•) 表示计算一个二进制字符串的汉明重量, n 表示”星座”的数量。

(5) 判定。如果 scr≥T, 则此测试卡被判为“真”, 否则被判为“假”。

计算 F_{T_j} 与关系对 (S_i, I_j) 中训练样本产生的集合 Set_{S_i} 和 Set_{I_j} 的距离过程如下:

(1) 通过公式 14, 将 F_{T_j} 投影到一维空间上并记为 $F_{T_j}^{W}$。

(2) 采用马氏距离分别计算 $F_{T_j}^{W}$ 到集合 Set_{S_i}、集合 Set_{I_j} 之间的距离。计算公式如下

$$d=\sqrt{(F_{T_j}^{W}-u)\ S^{-1}(F_{T_j}^{W}-u)^{T}} \tag{16}$$

其中, μ 表示集合 Set_{S_i} (Set_{I_j})的均值, S^{-1} 表示 Set_{S_i} (Set_{I_j})协方差矩阵的逆矩阵, 距离 d 表示 $F_{T_j}^{W}$ 与 Set_{S_i} (Set_{I_j})中元素的相似度, 距离越小表示相似程度越高。

5 评估结果

本节利用前面提出的“牵星”法对来自同厂家同型号同批次的 120 张高频 RFID 卡进行了评估。首先, 介绍了评估识别精度的指标, 随后介绍了基于交叉验证法的评估过程, 最后给出了评估结果。

5.1 评估指标

在本文中我们采用基于门限的身份认证方法对该识别系统进行了评估, 该方法已被广泛应用在对类似识别系统的评估上[32]。

基于门限的身份认证方法通常会有两种错误: 错误接受(False Accept FA)和错误拒绝(False Reject FR)。错误接受表示识别系统错误地将一个冒充者当作真实者接收。错误拒绝表示识别系统错误地将一个真实者当作冒充者拒绝。错误接受率(False Accept Rate FAR)和错误拒绝率(False Reject Rate FRR)表示错误接受和错误拒绝发生的频率。等错误率(Equal Error Rate EER)表示 FAR=FRR, 经常用来表示识别系统的识别精度。在随后的评估过程中, 我们主要用到 FAR、FRR 和 EER 这 3 个指标。

5.2 评估过程

我们采用基于交叉验证(cross-validation)的方法[11,18,19]来评估采集到的数据样本。交叉验证是指将数据样本分为若干个子集, 采用其中的一部分作为训练, 剩余部分作为测试对象来检测系统的性能。在本实验中, 我们对 120 张测试卡分别进行了三轮的数据采集。因此, 在交叉验证时我们将全部的数据样本分为 3 个子集, 将其中的 2 个子集作为训练样本, 剩余的 1 个子集作为测试样本, 即每一张卡的 150 个数据中, 取出 100 个数据作为训练样本, 剩余的 50 个数据作为检测样本。经过 3 轮交叉验证之后, 每一个子集中的数据不但做过训练样本, 同时也做过检测样本。

需注意的是, 在 4.6 节给出的识别过程中, 要先进行 UID 判断, UID 不同的卡直接被认定是不同的, 而无需进行“牵星”法判别。为了检验“牵星”法的判别效果, 我们选择忽略对 UID 的比对, 即假定所有的测试卡 T_j 都与对应的发行卡 I_j 拥有相同的 UID。

每一轮的检测过程如下: (1)确定“星座”中“星卡”的数量 n。“星卡”的数量 n 确定之后, 从 120 张测试卡中随机选出 n 张“星卡”组成“星座”, 剩下的 (120-n)张卡作为发行卡; (2)构建“星卡”与发行卡之间一一对应的关系。按照 4.5 节, 构建“星卡”与发行卡之间一一对应的关系对 (S_i, I_j), 见表 4; (3)识别。将发行卡中的每一张卡, 逐个与表 4 中的每一行进行比对, 并计算两者之间的相似系数, 如果 scr ≥ T, 则判断测试卡为真, 否则为假。经过三轮交叉验证之后, 统计识别过程中错误接受和错误拒绝出现的次数, 并计算 FAR 和 FRR。真正的匹配次数 N_{gen} 和错误的匹配次数 N_{imp} 的计算公式如下:

$$N_{gen}=(N\text{-}n)\times 50\times 3 \tag{17}$$

$$N_{imp}=(N-n)\times(N-n-1)\times 50\times 3 \quad (18)$$

为使评估结果更具有一般性, 当“星卡”的数量 n 为定值时, 我们重复(1)-(3)中的步骤 30 次并给出其平均值。

5.3 评估结果

由 4.5 节和 5.1 节可知错误率 FR(包括 FAR 和 FRR)与阈值 T 和“星座”中“星卡”的个数 n 有紧密联系。我们首先评估识别系统在**最严格阈值**条件下的识别精度, 即当 T=100%时。此时, 在对 n 个关系对(S_i, I_j)(i=1, 2,…, n)的评估中, 如果有一个结果为“0”, 则测试卡被判定为假。

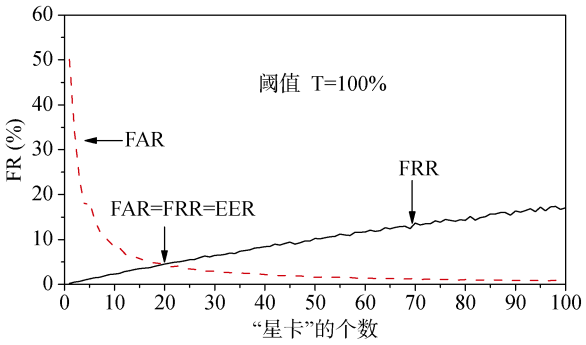


图 8 FR 与“星座”中“星卡”个数 n 的关系

图 8 给出了在阈值 T=100%的条件下，错误率 FR(FAR 和 FRR)与“星座”中“星卡”个数 n 的关系图。短划线和实线分别表示 FAR 和 FRR。可见，当“星卡”个数 n 从 1 增大到 100 时, FRR 呈现出线性增加的趋势, 当 n=100 时, FRR 达到最大值 16%。当 n 从 1 增大到 10 时, FAR 从 50%迅速下降到 8%。随后, 随着 n 的增大, FAR 下降速度逐渐变慢, 当 n=100 时, FAR 取得最小值 0.77%。当 n=22 时,FAR 与 FRR 两条曲线相交。此时, EER=FAR=FRR=4.2%。

我们对“牵星”法与其它方法的识别效果进行了对比。表 5 给出了对相同测试样本使用多元判别分析法(Multiple Discriminant Analysis MDA)[14]、匹配滤波器法[25]和功率谱密度法[26]的识别结果。当使用 MDA [14,28]时, 卡的射频指纹提取方法与“牵星”法相同。获得卡的射频指纹之后, 通过 MDA 对射频指纹进行投影以降低指纹特征维度同时增加不同卡之间的指纹分隔度, 采用公式 16 计算马氏距离, 最后利用比较距离的方法进行识别。

从表 5 中可以看出, 当使用 MDA 法时, 当识别卡的总数 N 从 10 增加到 45 时, 等错误率 EER 从 2.3%、3.9%、6.27%、8.8%, 迅速增加到 10.6%; 而使用“牵星”法时, 当识别卡总数 N=120 时, 即使在阈值 T=100%下, EER 仅为 4.2%。此外使用 MDA 方法时还有一个限制, 即要求待识别样本的数量不能超过射频指纹的维度[28]。从 4.4 节我们知道, 在 1 个高半位中采用 3 个高阶统计量生成的射频指纹维度为 45, 因此使用 MDA 法时最多只能识别 45 张卡。如果要提高识别样本的数量, 就需要选择更大的信号区间或更多的高阶统计量生成维度更高的射频指纹, 这样就会大幅提高运算量, 降低识别效率。而使用“牵星”法, 由于在每个关系对(S_i, I_j)的识别中使用 LDA 法[30], 因此每张卡射频指纹的维度大于或等于 2 就可进行识别, 这与 MDA 的要求相比是非常容易满足的, 因此在使用“牵星”法时不会受到指纹维度的限制, 适用性更强。

表 5 采用多元判别分析法、匹配滤波器和功率谱密度法与“牵星”法的单卡识别结果对比

识别方法	识别卡总数 N	EER (%)
多元判别分析法[14,28]	10	2.3
	20	3.9
	30	6.27
	40	8.8
	45	10.6
匹配滤波器法[25]	10	20
功率谱密度法[26]	10	30
“牵星”法	120	4.2%(T=100%)

如果直接使用测量值(如幅度、频率等)则识别结果更不理想。如使用文献[25]中的匹配滤波器法和文献[26]中的功率谱密度法, 当识别卡的总数为 N=10 时, 等错误率 EER 就达到 20%和 30%, 并且 EER 随着识别卡总数 N 的增大还会增大。

因此, 这些对其它设备能够成功识别的方法并不能直接地移植到对高频 RFID 卡的单卡识别中, 这是由于: (1)高频 RFID 卡仅由芯片模块和感应线圈组成, 较 WiFi、Zigbee 等其它有源射频器件要简单许多, 因此不同卡之间的射频指纹差异会更小, 识别更加困难; (2)以往的识别方法都是在获取设备的射频指纹之后, 通过各种算法或分类器将不同(类)设备的射频指纹投影到不同的空间中去，进行识别(分类)。因此, 这类方法的识别精度都不可避免地随着设备个数或种类的增加而减小。

表 6 比较了现有文献中采用不同的射频指纹识别方法对同一厂家同一型号的高频 RFID 卡的单卡识别结果。

表 6 采用射频指纹技术对高频 RFID 卡的单卡识别

文献	卡的工作状态	考察的特征	测试样本数量	EER(%)
Romero[18]2010	非正常	卡的无载谐振频率、品质因数与特定谐波的幅度相结合	20 张卡	4
Danev[19]2009	非正常	冲击信号/扫频信号下卡的响应	50 张卡	5.37/4.69
Danev[11]2012	非正常	改进的冲击信号下卡的响应	50 张卡	0.5
本文	正常	卡响应信号 1 个高半字节的高阶统计特征	120 张卡	4.2 (T=100%)

与 Romero 和 Danev 等提出的单卡识别方法比较, 采用“牵星”法进行单卡识别有两个最明显的优势: (1)可在正常工作状态下对克隆卡进行检测, 大大简化了识别系统的构成和测试过程; (2)该法具有良好的适用性和可扩展性。原则上获得了设备的射频指纹之后, 都可以用该方法进行识别。因此其它标准定义的 RFID 设备也可以基于本方法进行克隆卡检测。

在下节中我们可以看到, 通过选择合适的“星卡”个数 n 和阈值 T, 等错误率 EER 可下降到 2.5%。

6 讨论

在本节中首先讨论了阈值 T 对 FAR 和 FRR 的影响, 随后分析了由于随机选择“星卡”组成“星座”造成的 FAR 和 FRR 的波动性。最后证实了 ATQA 信号中的任意一个高半位都可以作为单卡识别的 ROI。

6.1 阈值 T 对 FAR 和 FRR 的影响

5.3 节给出了当阈值 T=100%时 FAR、FRR 与“星座”中“星卡”个数 n 的关系。当 T=100%时, 对 n 个关系对(S_i, I_j)(i=1,2,…, n)的评估中, 当值均为 1 时, 测试卡才能被判定为真卡。下面, 我们讨论在对 n 个关系对(S_i, I_j)(i=1,2,…, n)的评估中, 当分别出现 1 个和 2 个“0”时, FAR、FRR 与“星卡”个数 n 的关系。此时, 阈值 T 定义为:

$$T = \frac{n - n_f}{n} \times 100\% \tag{19}$$

其中, n_f 表示在对 n 个关系对评估时出现 0 的个数。

图 9 给出了当 n_f 分别为 0, 1, 2 时, 阈值 T 对 FAR 和 FRR 的影响。实线、短划线和点线分别对应 n_f 为 0, 1, 2 的结果。由图 9(a)可知, 当给定“星座”中“星卡”个数 n 时, 随着 n_f 从 0 增加到 2, FAR 增大, 不同 FAR 曲线之间的距离随着“星卡”个数 n 的增大而变小。由图 9(b)可知, FRR 的变化趋势与图 9(a)中 FAR 的变化规律正好相反。当 n_f 从 0 增加到 2 时, FRR 变小, 不同 FRR 曲线之间的距离随着“星卡”个数 n 的增大而变大。综合图 9(a)与图 9(b), 可得当

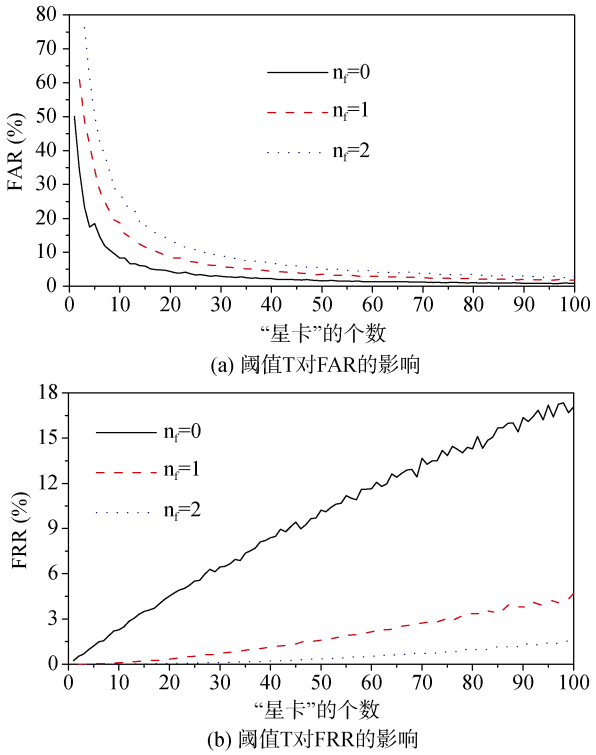


图 9 阈值 T 对 FAR 和 FRR 的影响

n_f=1 时, “星卡”数 n=72 时, FAR=FRR=EER=2.5%, 这意味着伪造者需要尝试使用同厂家同型号同批次的 100 张卡, 才可能获得不大于 2.5 次的成功机会。当 n_f=2 时, 在 n=1 到 100 的范围之内, FAR 与 FRR 无相交点, 当 n=100 时, FAR 取得最小值 3.0%, FRR 取得最大值 1.1%。

因此, 使用“牵星”法时可通过选择合适的阈值 T 和“星卡”个数 n 的组合得到最优的识别精度。

6.2 FAR 和 FRR 的波动性分析

在上面的识别过程中, “星座”是从所有待识别卡中随机选取生成的, 每次选择的“星座”集合一般不会完全相同。因此, 使用两个不同集合的“星座”进行单卡识别时, 两次计算的 FAR 与 FRR 数值不会完全相同, 这就产生了 FAR 与 FRR 的波动性。

下面我们以当 n_f=1 时为例, 分析 FAR 与 FRR 的波动性。分析过程如下: 当“星座”中“星卡”个数 n 给定时(n=10, 20,…, 100), 进行 30 次识别(即 30 次

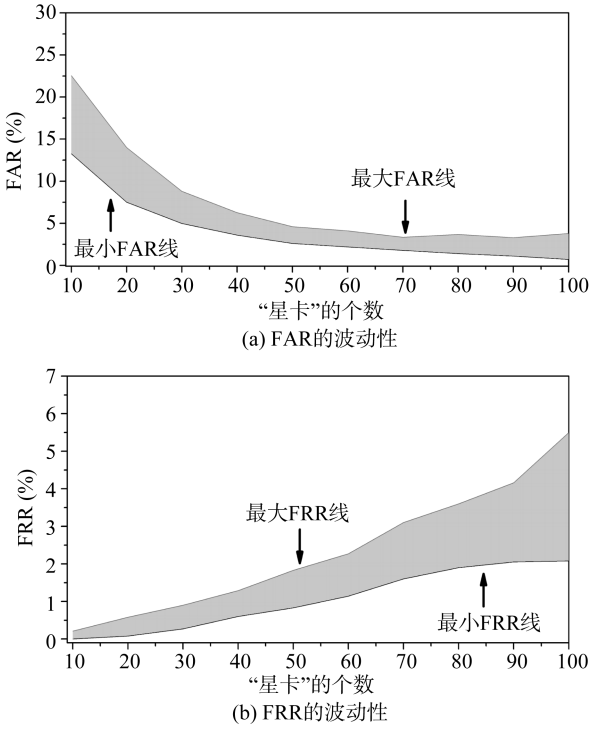


图 10　FAR 和 FRR 的波动性(n_f=1 时)

随机抽取的识别过程), 并记录 FAR 与 FRR 的最大值和最小值, 所得结果如图 10 所示。由图 10(a)可以看出 FAR 的最大值和最小值都随着 n 的增大而减小。当 n=10 时, 波动范围最大, 此时最大值为 FAR_{max}=22.54%, 最小值为 FAR_{min}=13.26%。由图 10(b)中可以看出, FRR 的最大值和最小值都随着 n 的增大而增大, 二者之间的距离也逐渐增大。当 n=10 时, 波动范围最小, 此时最大值为 FRR_{max}=0.21%,最小值为 FRR_{min}=0。实际上, 我们最感兴趣的点是当“星座”中“星卡”的个数 n=72 时的等错误率点, 即 FAR=FRR=EER=2.5%。此时, FAR 的最大值为 FAR_{max}=3.34%, 最小值为 FAR_{min}=1.78%, FRR 的最大值为 FRR_{max}=3.1%, 最小值为 FRR_{min}=1.6%。我们发现在等错误率 EER 点上, FAR 和 FRR 的最大值、最小值与 30 次平均值的差值在 1%之内, 这个差值是比较小的。因此, 在实际使用“牵星”法进行单卡识别时, 在确定了等错误点的阈值和相应的“星座”中“星卡”个数 n 之后, 不需要进行大量的重复测试就可以得到比较高的识别精度。当 n_f 为 0 或 2 时, 同样可得出类似的结论。

图 11 解释了在 5.2 节的评估当中为使评估结果更具有一般性而进行 30 次随机抽取识别的原因。图 11 给出了当“星座”中“星卡”个数 n=50 时, 错误率 FR(FAR、FRR)的平均值与重复次数的关系。图 11(a)、(b)和(c)分别对应 n_f 为 0,1 和 2 的结果, 实线和短划线分别代表 FRR 和 FAR 值。可见, 当重复次数小于 10 时, FAR 与 FRR 的波动相对较大, 当重复次数为 20 时, FAR 与 FRR 趋于稳定。因此, 为了使评估结果更具一般性, 当“星座”数量 n 为定值时, 我们选取当重复次数为 30 并给出了 FAR 和 FRR 的平均值。

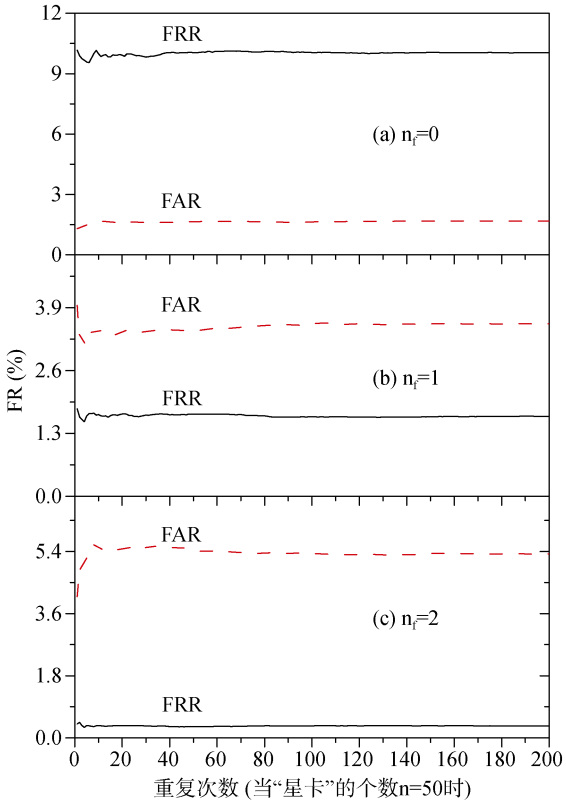


图 11　FR 的平均值与重复次数的关系

从 3.1 节介绍“牵星”法的基本原理和本节的讨论中我们可以看出, “星卡”的选择对识别结果具有直接影响, 某些 FAR 和 FRR 可以通过改变或添加“星卡”得到解决。因此, 如果能够选择表具有代表性的卡组成“星座”, 不但能够降低波动性而且还能进一步提升识别精度。但是, 同一厂家、同一型号、同一批次的 RFID 卡的射频指纹往往表现出高度的相似性, 并且每张卡的每个特征(幅度、相位、频率)在每个子区间(共有 5 个子区间)都有 3 个高阶统计量。因此, 每张卡的射频指纹包含的高阶统计量共有 3×5×3=45 个。这会给如何选择“有代表性的卡”造成很大困难。

6.3　ROI 的选择

由图 3 可以看出, 在卡响应的 ATQA 信号中共有 19 个高半位。在前面给出的结果和讨论中, 我们均以第一个高半位作为 ROI 并从中提取指纹进行识别。实际上, 我们通过计算发现 ATQA 信号中的每个高

半位都可以作为单卡识别的 ROI, 并获得几乎相同的 FAR 和 FRR 值。

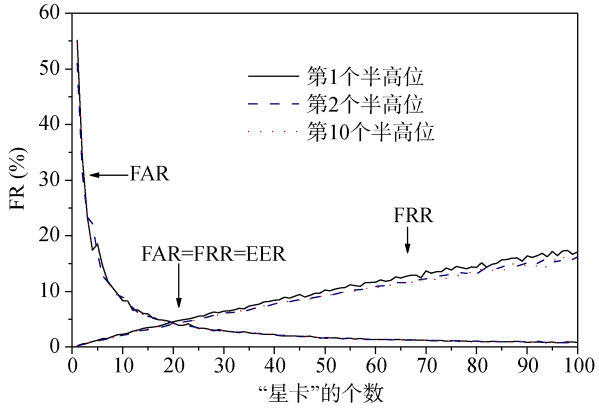


图 12　选择 1st, 2nd, 10th 高半位作为 ROI 时的 FAR 和 FRR(T=100%)

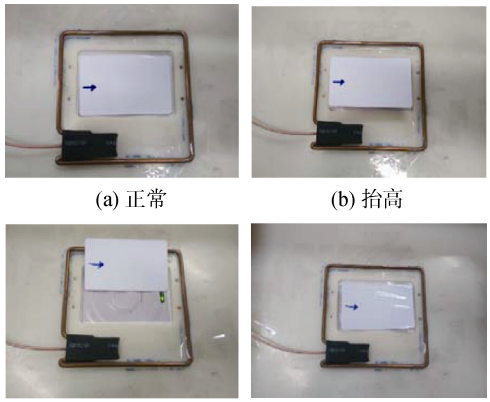
图 12 给出了从 ATQA 信号中选择第 1 个(1st)、第 2 个(2nd)和第 10 个(10th)高半位作为 ROI 时得到的 FAR 和 FRR 值(此时取阈值 T=100%)。实线、短划线和点线分别对应 1st、2nd 和 10th 高半位作为 ROI 的结果。对于 FAR 值, 当“星卡”个数 n 从 0 增加到 100 时, 3 个不同 ROI 对应的 FAR 曲线几乎完全重合。对于 FRR 值, 当“星卡”个数 n 从 0 增加到 40 时, 3 个不同 ROI 对应的 FRR 曲线重合度较好, 当 n 继续增大时, 3 个不同 ROI 对应的 FRR 曲线间的距离稍有增加。当 n=100 时, FRR 曲线间最大差值约为 2%。根据前面对 FRR 波动性的讨论, 这些差值是在允许的误差范围之内的。在 5.3 节中, 当阈值 T=100% 时,FAR=FRR=EER 对应“星座”的个数为 n=22<40。因此, ATQA 中任意一个高半位部分都可以作为提取统计指纹并进行单卡识别的 ROI。

6.4　卡的摆放方式对射频指纹的影响

在本节, 我们讨论了卡的摆放方式对射频指纹的影响。图 13(a)-(d)分别给出了同一卡的 4 种不同摆放方式: (a)正常(将卡直接放在读写器上), (b)抬高(卡与读写器的垂直距离为 15mm), (c)倾斜(卡沿着水平方向移动 27mm 并放在天线上), (d)弯折(弯折卡, 卡的长度由原来的 85mm 变为 83mm)。

信号的采样过程与 4.1 节相同, 每种摆放方式均收集 150 次数据, 射频指纹按照图 7 所示计算生成, 最后按照 4.6 节的识别过程进行检测。结果发现对同一卡的 4 种不同摆放方式, 只有图 13(a)中正常的摆放方式时才能够正确识别, 图 13(b)-(d)中的 3 种摆放方式均不能正确识别。

表 7 给出了对同一卡的 4 种不同摆放方式时, 幅度、相位和频率特征的 3 个高阶统计量在第 1 个子区间上平均值。从表 7 中可以看出幅度、相位和频率的方差、偏度系数或峰度系数随着摆放方式的不同大都发生了较大的变化。如幅度的统计特征, 图 13(b)-(d)相对于图 13(a)的正常摆放时, 方差的变化率分别为 8%、93%和 23%; 偏度系数的变化率分别为 232%、35%和 383%; 峰度系数的变化率分别为 1%、29%和 8%。其他子区间的变化率与此类似。因此, 当 5 个子区间的特征级联在一起时, 引起的差异会更大。这也说明高频 RFID 卡的射频指纹对通信的距离、天线的形状和摆放的角度等都是敏感的。



(a) 正常　(b) 抬高

(c) 倾斜　(d) 弯折

图 13　同一卡的 4 种不同摆放方式

表 7　同一卡的 4 种不同摆放方式时的幅度相位和频率的 3 个高阶统计量在第 1 个子区间上的平均值

信号特征	高阶量	正常	抬高	倾斜	弯折
幅度	方差	0.223	0.205	0.432	0.171
	偏度系数	0.056	0.186	0.036	–0.159
	峰度系数	1.845	1.867	1.296	1.690
相位	方差	0.011	0.009	0.008	0.002
	偏度系数	–0.203	–0.715	0.108	–0.347
	峰度系数	1.745	3.812	1.912	2.129
频率	方差	0.052	0.074	0.086	0.089
	偏度系数	–0.628	–0.398	–0.187	–0.106
	峰度系数	4.926	3.564	2.968	2.930

如引言中所述, ISO14443 所定义的高频 RFID 是一种近场通信方式, 感应耦合是它的主要电磁传输机制, 射频指纹对通信的距离、天线的形状和摆放的角度等都是敏感的。因此, 没有卡的密切配合很难提取有意义的指纹特征。

7　相关工作

在射频指纹识别中提取近场信号(1 个载波波长之内的空间范围)的方式主要为磁耦合, 提取远场信号(1 个载波波长之外的空间范围)的主要方式为电耦

合, 这是两种不同的电磁传输机制[19]。为此, 我们根据提取信号与发射源的距离, 将相关射频指纹识别的文献分为两类: 近场模式下的射频指纹识别和远场模式下的射频指纹识别。

7.1 近场模式下的射频指纹识别

正如第 1 节中所述, 近场模式下射频指纹识别相关的参考文献非常少, 主要有 4 篇[11,17-19], 由于在引言中已经进行了比较详细的介绍, 此处不再赘述。后面主要介绍远场模式下的射频指纹识别工作。

7.2 远场模式下的射频指纹识别

Periaswamy 等[33]提出利用标签的最小功率响应作为物理层指纹来识别甚高频 RFID(UHF RFID)标签。随后, 他们[34]又提取 UHF RFID 标签在多个频点下的最小功率响应作为物理层指纹对标签进行识别。通过对 50 个同种型号标签的评估, 识别的正确率为 94.4%(在 FAR=0.1%的条件下)和 90.7%(在 FAR=0.2%的条件下).

Periaswamy 等[16]和 Zanetti 等[35]利用信号的时隙特性对 UHF RFID 标签进行了识别。在文献[16]中, 通过对 3 个类型(10 个标签/类型)的测试, 分类成功率分别为 98.44%, 96.25%和 31.54%。在文献[35]中, 作者用实验证实了当标签离读写器 6 m 远处还能获得分类的准确率为 71%。在可控环境中, 利用信号的谱特征与时隙特征相结合的方法进行单卡识别并取得 EER=0。

Bertoncini 等[22]通过使用动态小波变换技术对 UHF RFID 标签的 EPC 码信号进行了研究, 采用有监督的模式分类技术, 获得的识别精度为 99%。

除了使用射频指纹技术之外, 还有其他的一些技术用来进行克隆卡的检测。文献[36]通过给 RFID 标签加装一种 PUF 电路来抵御非法克隆。PUF 是一种硬件结构, 难以复制和克隆。Lakafosis 等[37]还提出了一种 RF-CoA 结构用来抵御非法克隆, 这种物理结构通过测量入射信号的响应特性鉴别设备的真伪。

8 总结

本文提出了一种用于识别高频 RFID 卡的方法: “牵星”法。通过对来自同一厂家、同一型号、同一批次的 120 个高频 RFID 卡的测试, 获得了 EER=2.5%的识别精度。该识别方法可实现基于物理特征对卡的认证, 从而可以有效检测出克隆卡。该识别系统仅由一个天线、一个读卡器和示波器组成, 在现有的单卡识别系统中需要的测量设备最少。

虽然本文以社会应用最为广泛的 ISO14443 Type A 无源高频 RFID 卡为目标展开实验, 但识别原理与卡的底层标准并无必然联系。基于相同的原理可比较容易地推广到其他类型设备的射频识别中。本方法在防范 RFID 应用系统的克隆卡攻击, 提高应用安全性等方面都具有十分重要的意义。

参考文献

[1] K. Traub, G. Allgair, H. Barthel, L. Burstein, J. Garrett, B. Hogan, B. Rodrigues, S. Sarma, J. Schmidt, C. Schramek, et al, “The epc global architecture framework,” EPC global Ratified specification, 2005.

[2] C.-H. Huang and S.-C. Huang, “Rfid systems integrated otp security authentication design,” *in Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, pp. 1–8, 2013.

[3] S. Abughazalah, K. Markantonakis, and K. Mayes, “Enhancing the key distribution model in the rfid-enabled supply chains,” *In Advanced Information Networking and Applications Workshops (WAINA’14)*, pp.871–878, 2014.

[4] “Cracked it,” S. Boggan, http://www.guardian.co.uk/technology/2006/nov/17/news.homeaffairs/, May. 2016.

[5] L. Grunwald, “New attack to rfid-systems and their middleware and backends,” in Black Hat Briefings USA, 2006.

[6] J. van Beek, “epassports reloaded,” in Black Hat USA Briefings, 2008.

[7] L. Hui, D. Yahui, L. Dongsheng, L. Zilong, H. Dawei, and T. Hengqing, “A lattice-based public-key encryption scheme for rfid applications,” *in Solid-State and Integrated Circuit Technology (ICSICT)*, pp. 1–3, 2014.

[8] A. Miyaji and M. S. Rahman, “Aprap: Another privacy preserving rfid authentication protocol,” *in Secure Network Protocols (NPSec)*, pp. 13–18, 2010.

[9] M. Shuang and Y. Xiao-long, “An efficient authentication protocol for low-cost rfid system in the prensence of malicious readers,” *in Fuzzy Systems and Knowledge Discovery (FSKD)*, pp. 2111–2114, 2012.

[10] Kocher P, Jaffe J, Jun B.,“Differential power analysis”, *in advances in cryptology—CRYPTO’99*, pp. 388-397, 1999.

[11] B. Danev, S. Capkun, R. Jayaram Masti, and T. S. Benjamin, “Towards practical identification of HF RFID devices,” *ACM Transactions on Information and System Security (TISSEC)*,2（15）, July, 2012.

[12] H. L. Yuan and A. Q. Hu, “Fountainhead and uniqueness of RF fingerprint”, *Journal of Southeast University (Natural Science Edition)*, 39（2）：230-233, Mar. 2009.
(袁红林, 胡爱群, “射频指纹的产生机理与唯一性”, *东南大学学报(自然科学版)*, 39（2）：230-233, 2009 年 3 月。

[13] J. Hasse, T. Gloe, and M. Beck, “Forensic identification of gsm mobile phones,” *in Proceedings of the first ACM workshop on Information hiding and multimedia security*, pp. 131–140, 2013.

[14] H. J. Patel, M. A. Temple, and R. O. Baldwin, “Improving zigbee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting,” *IEEE Transactions on Reliability*,64(1): 221–233, 2015.

[15] Padilla J L, Padilla P, Valenzuela-Valdés J F, et al, “RF fingerprint measurements for the identification of devices in wireless communication networks based on feature reduction and subspace transformation”, Measurement 58, pp. 468-475, 2014.

[16] S. C. G. Periaswamy, D. R. Thompson, H. P. Romero, and J. Di, “Fingerprinting radio frequency identification tags using timing characteristics,” in Proc. *Workshop on RFID Security-RFID-sec Asia*, 2010.

[17] H. P. Romero, K. A. Remley, D. F. Williams, and C.-M. Wang, “Electromagnetic measurements for counterfeit detection of radio frequency identification cards,” *IEEE Transactions on Microwave Theory and Techniques*,57(5): 1383–1387, 2009.

[18] H. P. Romero, K. A. Remley, D. F. Williams, C.-M. Wang, and T. X. Brown, “Identifying rf identification cards from measurements of resonance and carrier harmonics,” *IEEE Transactions on, Microwave Theory and Techniques*, 58(7): 1758–1765, 2010.

[19] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, “Physical-layer identification of rfid devices,” *in Usenix Security Symposium*, pp. 199–214, 2009.

[20] Xun L. Study on the Features of Navigational Charts in China's Ming Dynasty[J]. 2016.

[21] Yuan, Y., Huang, Z., Wu, H., and Wang, X., “Specific emitter identification based on Hilbert-Huang transform-based time-frequency- energy distribution features”, *IET Commun*, 8(13): 2404–2412, 2014.

[22] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, “Wavelet fingerprinting of radio-frequency identification(rfid) tags,” *IEEE Transactions on Industrial Electronics*, 59(12): 4843–4850, 2012.

[23] Finkenzeller K. RFID, “Handbook: Radio-frequency identification fundamentals and applications”, Wiley, 1999.

[24] ISO/IEC, ”Identification cards - Contactless integrated circuit(s) cards -Proximity cards - Part 4: Transmission Protocol”, 2010.

[25] Gerdes, R. M., Daniels, T. E., Mina, M., & Russell, S. “Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach”, *in NDSS*, 2006.

[26] Suski, W. C., Temple, M. A., Mendenhall, M. J., & Mills, R. F., “Using spectral fingerprints to improve wireless network security”, *in Global Telecommunications Conference*, pp. 1-5, 2008.

[27] Ureten O, Serinken N., “Wireless security through RF fingerprinting”, *Electrical and Computer Engineering*, 32(1): 27-33, 2007.

[28] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, and Y. C. Kim, “Intrinsic physical-layer authentication of integrated circuits,” *IEEE Transactions on Information Forensics and Security*, 7(1): 14–24, 2012.

[29] Padilla J L, Padilla P, Valenzuela-Valdés J F, et al., “RF fingerprint measurements for the identification of devices in wireless communication networks based on feature reduction and subspace transformation”, Measurement, no. 58, pp.468-475, 2014.

[30] C.-h. Chen, L.-F. Pau, and P. S.-p. Wang, “Handbook of pattern recognition and computer vision,” volume 27, World Scientific, 2010.

[31] R. G. Lyons, “Understanding digital signal processing,” Pearson Education, 2010.

[32] R. M. Bolle, J. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, “Guide to biometrics,” Springer Science & Business Media, 2013.

[33] S. C. G. Periaswamy, D. R. Thompson, and J. Di, “Ownership transfer of rfid tags based on electronic Fingerprint,” in *Security and Management*, pp. 64–67, 2008.

[34] S. C. G. Periaswamy, D. R. Thompson, and J. Di, “Fingerprinting rfid tags,” *IEEE Transactions on Dependable and Secure Computing*, 8(6):938–943, 2011.

[35] D. Zanetti, B. Danev, et al, “Physical-layer identification of uhf rfid tags”. *In Proceedings of the sixteenth annual international conference on Mobile computing and networking*, pp. 353–364, 2010.

[36] P. Tuyls and L. Batina, “Rfid-tags for anticounterfeiting,” *in Topics in cryptology–CT-RSA*, pp. 115–131, Springer, 2006.

[37] V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. M. Tentzeris, G. R. DeJean, and D. Kirovski, “Rf fingerprinting physical objects for anticounterfeiting Applications,” *IEEE Transactions on Microwave Theory and Techniques*, 59(2): 504–514, 2011.

张国柱 于 2008 年在电子科技大学无线电物理专业获得硕士学位。现在中国科学院信息工程研究所攻读博士学位。研究领域为物理层安全, 嵌入式系统安全。研究兴趣包括: 无线通信安全和隐私。Email: zhangguozhu@iie.ac.cn

夏鲁宁 于 2008 年在中国科学院研究生院信息安全专业获得博士学位。现就职于中国科学院信息工程研究所, 高级工程师。研究领域为网络与信息系统安全, 嵌入式系统安全。研究兴趣包括: 射频指纹技术、固态存储安全技术等。Email: xialuning@iie.ac.cn

贾世杰 于中国科学院信息工程研究所攻读博士学位。研究领域为嵌入式系统安全。研究兴趣包括: 无线通信安全和隐私。Email: jiashijie@iie.ac.cn

嵇亚飞 于 2016 年在中国科学院大学信息安全专业获得博士学位。现任职于中国科学院信息工程研究所。研究领域为嵌入式系统安全。研究兴趣包括: 无线通信安全、电路设计等。Email: jiyafei@iie.ac.cn