RFID 系统密钥无线生成

鲁 力

(电子科技大学计算机科学与工程学院 成都 611731)

摘 要 随着无线射频识别(Radio Frequency Identification,RFID)系统发展,众多安全和隐私的相关应用对隐私保护认证(Privacy-Preserving Authentication,PPA)技术提出了强烈需求.而 PPA 应用的先决条件是合法读写器和标签之间存在共享密钥.但由于无线信道的开放性,读写器直接向标签写入的密钥会被敌手轻易窃听;此外,RFID 标签的计算、存储和通信能力极其有限,导致现有的密钥协商协议不能应用于 RFID 系统;再者,标签生产商在标签出厂时写入的密钥会带来密钥托管问题并且用户不能自定义密钥.上述原因导致 RFID 系统中密钥安全生成问题极具挑战性.该文创新性地利用 RFID 系统中信道不对称性,提出了一种 RFID 系统密钥无线生成方法 WiKey.WiKey 是一种轻量级协议可在现有的 RFID 系统中实现.通过全面的安全性分析,我们展示了 WiKey 能为 PPA 协议提供强有力的保护;在 WISP 标签上的原型实现以及实际测试表明 WiKey 在现有 RFID 系统中实现的可行性和高效性.

关键词 无线射频识别;密钥生成;隐私保护认证;RFID;物联网;密码学

中图法分类号 TP393 **DOI 号** 10.3724/SP.J.1016.2015.00822

Wireless Key Generation for RFID Systems

LU Li

(*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu* 611731)

Abstract As Radio Frequency Identification (RFID) systems have been enormously applied in fields like commerce and logistics, a wide spectrum applications call for Privacy-Preserving Authentication (PPA) in RFID systems, which require a legitimate reader to share secret keys with one or group of tags. With open wireless channels, an adversary can easily obtain keys sent to tags by the reader. Moreover, existing key-agreement approaches cannot be employed in RFIDs as tags are usually resource-constraint. Furthermore, keys implanted by manufacturer cannot be considered as secure due to two-fold reasons: the most trustworthy keys are those generated by users themselves and the key-escrow on the manufacturer incurs key-leaking problem. Hence, it is very challenging to generate shared secret keys among a valid reader and tags wirelessly and securely. In this paper, we propose an innovative wireless key generation scheme, called WiKey, with which a legitimate reader can generate secret keys among itself and tags by effectively utilizing the asymmetry of communication channels of RFID systems. WiKey is a very light-weighted protocol and can be implemented on current RFID systems. Through intensive security analysis, we show that WiKey is an efficient and strong protection for PPAs in RFID systems. Moreover, the implementation on WISP RFID tags and experiment results illustrate the feasibility and efficacy of WiKey.

Keywords radio frequency identification; key generation; privacy-preserving authentication; RFID; Internet of Things; cryptography

收稿日期:2013-10-04;最终修改稿收到日期:2014-10-13.本课题得到国家自然科学基金(61173171,61472068)、中央高校基本科研业务费项目(ZYGX2012J072)、博士后面上基金(2014M550466)资助.**鲁 力**,男,1978 年生,博士,副教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为无线系统安全、RFID 系统、应用密码学.E-mail:luli2009@uestc.edu.cn.

1 引　言

由于具有低成本、易部署的特点，无线射频识别(Radio Frequency Identification，RFID)技术已被广泛应用于物流[1-2]、仓库管理[3-4]、访问控制[5-6]和供应链管理系统[7-8]等方面.

最常用的标签为无源被动式标签，只能从读写器信号获得极少能量，并且其计算和存储资源极其有限.同时，标签在获得能量后通过反向散射读写器载波以传输信息，因此标签会自动响应所有提供能量的读写器访问.这种反向散射模式会暴露标签所储存的信息甚至会暴露读写器敏感的隐私信息.为了保护标签隐私，隐私保护认证(Privacy-Preserving Authentication，PPA)成为目前常用的保护读写器和标签之间交互的安全机制.PPA 的基本思想是在读写器和标签之间利用共享密钥进行认证和识别.然而，PPA 依赖于一个强假设：读写器和标签内存在共享密钥用于保护所传输的信息.

然而在 RFID 标签上安全生成密钥非常具有挑战性.首先，如果制造商预置密钥于标签中会造成密钥托管问题①，而用户也不能生成自己信任的密钥；第二，现有被动式无源标签没有物理接口(如 USB 等)与其它设备连接，因而通过物理连接生成密钥的方法不可行；第三，如果读写器以无线方式直接将密钥写入标签，由于读写器的发射功率较大，使得攻击者可以在远距离通过窃听获得密钥；最后，标签的计算能力非常有限，不能进行复杂的密码学运算，因此现有基于密码学的密钥协商方法均不能在标签上使用.

本文创新性地提出在 RFID 标签上进行密钥安全无线生成的方法(Wireless Key Generation，WiKey).WiKey 的基本思想是利用 RFID 系统前、后向信道(Forward Channel 和 Backward Channel[9])的非对称性.前向信道指从读写器到标签的信道，而后向信道是从标签到读写器的信道.由于读写器的发射功率较大，所以其通信半径较大，敌手可以很容易的监听该信道上的内容.而后向信道中，标签采用反向散射方式向读写器发送消息，标签由于自身缺乏电源，不能主动向读写器发送信号，只能反射读写器发出的载波，并通过幅移键控(Amplitude Shift Keying，ASK)调制加载数据.而反射信号与读写器发出的载波相比非常微弱，故其通信距离也较短，使得敌手的窃听非常困难.我们在第 3 节中通过理论分析和实验验证了后向信道不可窃听的特点.

WiKey 的基本思想是让没有初始密钥的标签向读写器发送密钥碎片，当接收到读写器生成的另一密钥碎片时，标签通过混合这些密钥碎片即可生成共享密钥.由于后向信道不可窃听，敌手不能获取标签生成的密钥碎片，即使听到读写器生成的密钥碎片也不能恢复共享密钥，这就实现了读写器和标签间密钥的无线生成.

WiKey 针对两种不同需求设计了密钥生成方案：(1)读写器对单个给定标签生成一个唯一的个体密钥；(2)读写器对一组标签生成一个群组密钥.对于个体密钥生成，WiKey 使用读写器获取给定标签的随机数并与读写器的随机数混合，在标签和读写器上产生共享密钥.基于个体密钥生成方案，WiKey 提出了在一组标签上生成共享群组密钥的方法.简单来说，由于 RFID 标签只能与读写器通信，WiKey 使用读写器作为群组控制者收集组内所有标签产生的密钥碎片，加以混合后对每个标签的密钥碎片产生对应的密钥生成因子，并发送给对应的标签，使之能产生正确的共享密钥.

WiKey 具有以下 4 项优点：(1)密钥无线生成，无需物理接口；(2)轻量级协议，适用于资源受限的 RFID 标签；(3)安全的密钥生成，能抵抗主动和被动攻击；(4)密钥生成可由终端非专业用户执行.

本文对 WiKey 的安全性进行了分析，并且在实际 RFID 系统中进行了实验以验证其可行性.性能评价和理论分析表明，WiKey 可在 RFID 系统中高效、安全地实现密钥无线生成.

本文第 2 节介绍无线系统中密钥生成的相关工作；第 3 节详细介绍 RFID 系统中信道特点并论证后向信道不可窃听的特性；第 4 节定义 RFID 系统及针对密钥无线生成的敌手模型；第 5 节详细描述 WiKey 的具体设计；第 6 节讨论 WiKey 在实际应用中可能遇到的问题；第 7 节对 WiKey 的安全性进行详细分析；第 8 节介绍在实际 RFID 系统上的原型实现；第 9 节对原型进行系统地评价；第 10 节总结全文.

2 相关工作

前无线设备中进行密钥生成的方法可分为以下两类：基于密码学和非密码学方法.

密码学方法：该类方法基于公钥密钥学的密钥

① Key Escrow. http://en.wikipedia.org/wiki/key escrow

协商方法，如 Diffie-Hellman 密钥协商协议[11]. 虽然该类方法可解决密钥生成问题，但需要进行复杂的计算(如大数操作)，因而并不适用于资源严重受限的 RFID 标签.

非密码学方法：该类方法不使用密码技术，而是采用物理方法或者基于通信信道的特征来生成密钥，详细描述如下.

物理方法：该方法主要包含两种方法：物理隔离和有线连接写入. 物理隔离利用法拉第笼[11]来保护无线设备之间的通信信道不被窃听. 法拉第笼是一个由金属网构成的用于屏蔽无线信号的容器，笼内的无线信号被法拉第笼屏蔽，因此，法拉第笼内的两个无线设备能以明文进行通信. 该方法受限于法拉第笼的空间，使得该类方法很难运用于 RFID 的实际应用中. 例如，法拉第笼无法容纳嵌入在如汽车、集装箱等大型物体里的 RFID 标签. 另外，终端用户可能不愿在使用 RFID 标签之前建造一个巨大的法拉第笼. 有线连接写入方法[12]中，两个设备需要硬件接口来建立物理电信号连接. 在该连接中，可进行密钥生成或交换. 但是由于 RFID 标签没有物理接口来支持这种电路连接，使得这种方法也不适用于 RFID 设备.

基于信道特征：方案[13]通过一个匿名信道在两个 CPU 资源受限的无线设备之间建立共享密钥. 简单而言，ID 为 A 的设备通过广播一个带有源字段为 A 的随机数据包，以代表发送比特 1 给 ID 为 B 的设备. 类似地，A 通过广播一个带有源字段为 B 的随机包，代表发送秘密比特 0. 由于只有 B 可以识别包真实源头恢复秘密比特(若源字段为 A，则为 1；否则为 0). 若数据包的源字段中包含 A 和 B 的概率相同，则窃听者无法确定包是由 A 或 B 发出，从而无法获取秘密比特. 该方法虽然计算开销较低，但是需要为每一秘密比特产生一个数据包，通信开销较大. 而且，目前被动式无源 RFID 标签只能反射读写器的信号作为应答，不能产生随机数据包. 因此读写器方法不适用于 RFID 系统.

方案[14-16]通过测量无线信道中的随机变量来产生密钥. 具体而言，当设备 A 向设备 B 发送数据包时，信号将通过不同的路径被发送，因此信号具有不同的延迟衰减，使得 B 接收到的信号是多路径信号的综合. 同样，B 向 A 发送的数据包将沿同样的路径到达 A. 由于信道的唯一性，窃听者无法从他所在的位置推断出信道的特征变量. 因此，这种方法可用于在两个无线设备中生成具有较高熵值的密钥. 但是，该方法需无线设备自主测量信道随机变量(如信号强度)，而 RFID 标签并不具备该能力.

鉴于现有方法的缺点，本文针对 RFID 系统提出了密钥无线生成方法 WiKey，与现有工作相比，WiKey 无需额外的硬件接口和复杂的密码算法；同时 WiKey 以无线方式生成密钥. 由于其轻量级的特点，WiKey 能在实际 RFID 系统中实现.

3 RFID 信道非对称性

大多数常用的 RFID 标签为被动式标签，即不能主动向读写器发送电磁波，而只能通过反向散射方式反射来自读写器的电磁波作为应答. 考虑到电磁波的传播衰减和标签天线的反射系数等原因，标签的反射信号强度(后向信道)相比读写器发射信号的强度(前向信道)极为微弱. 这意味着后向信道的通信距离相比前向信道其通信距离极其有限. 本节我们将研究前、后向信道的链路预算(即计算信号在信道中传播所遇到的所有衰减和增益)以揭示这一现象并提出后向信道信息不可窃听的事实观察.

3.1 前向信道链路预算

前向信道链路预算即当读写器以固定频率发射电磁波时，标签天线上所接收到的信号强度.

设 $P_{TX,\text{reader}}$、$P_{RX,\text{tag}}$、G_{reader}、G_{tag} 和 d_{for} 分别表示读写器发射功率、标签天线接收信号功率、读写器天线增益、标签天线增益和前向信道中标签天线到读写器的距离. 同时，设 λ 为 RFID 系统中信号的波长(目前北美和亚洲地区信号频段为 902～928 MHz). 由于读写器和标签在应用中常处于相互间目视范围内，因此电磁波传播服从自由空间模型[18]，则有

$$\frac{P_{RX,\text{tag}}}{P_{TX,\text{reader}}}=G_{\text{reader}}G_{\text{tag}}\left(\frac{\lambda}{4\pi d_{\text{for}}}\right)^2 \tag{1}$$

3.2 后向信道链路预算

后向信道链路预算是指接收方(如窃听者)天线上所能接收到标签反射信号的功率或信号强度. 在理想环境中(理想环境是指在标签和接收者之间不存在与波长在尺寸上可比的障碍物)，除了标签的反射系数外，后向信道链路预算与前向信道链路预算相似. 理论上来说标签反射能量可以达到吸收能量的 4 倍，但此时标签芯片不能获得足够多的能量用以启动标签. 因此，标签需要反射一部分入射能量并保留其余能量以启动标签芯片，反射能量占入射总能量的比值即为反射系数. 在实际被动式标签中，不同的设计导致不同的反射系数，因此反射系数没有

一个确定值，但是我们可以给出一个近似的估计，即反射信号能量占吸收能量的 1/3(−5 dB)[18]. 在本文中，记反射系数为 T_r，则标签反射信号能量为 $P_{TX,\text{tag}}=P_{RX,\text{tag}}T_r$.

基于自由空间传播模型，后向信道中链路预算为

$$\frac{P_{RX,\text{adv}}}{P_{TX,\text{tag}}}=G_{\text{tag}}G_{\text{adv}}\left(\frac{\lambda}{4\pi d_{\text{back}}}\right)^2 \tag{2}$$

这里 $P_{RX,\text{adv}}$、G_{adv} 和 d_{back} 分别表示窃听者天线所接收的信号强度、窃听者天线增益和窃听者到标签天线的距离. 在密钥无线生成的场景中，用户可在室内执行密钥生成，因此房间的混凝土墙和地板会进一步衰减窃听者的接收信号强度. 通常，混凝土墙对 900 MHz 频段电磁波每分米会带来 15～20 dB 衰减[19]. 我们记该衰减为 χ，则我们可以得到敌手在后向信道上的链路预算如下

$$\frac{P_{RX,\text{adv}}}{P_{TX,\text{tag}}}=\chi G_{\text{tag}}G_{\text{adv}}\left(\frac{\lambda}{4\pi d_{\text{back}}}\right)^2 \tag{3}$$

综合式(1)、(2)和(3)，得到窃听者的接收信号强度为

$$\frac{P_{RX,\text{adv}}}{P_{TX,\text{tag}}}=\chi T_r G_{\text{reader}}G_{\text{adv}}G_{\text{tag}}^2\left(\frac{\lambda}{4\pi}\right)^4\left(\frac{1}{d_{\text{for}}d_{\text{back}}}\right)^2 \tag{4}$$

将式(4)写为 dBm 形式，可得

$$\begin{aligned}P_{RX,\text{adv}}\text{dBm}=&P_{TX,\text{reader}}\text{dBm}+10\lg\chi+10\lg T_r+\\&10\lg G_{\text{reader}}+10\lg G_{\text{adv}}+20\lg G_{\text{tag}}+\\&40\lg\lambda-40\lg 4\pi-20\lg(d_{\text{for}}d_{\text{back}})\end{aligned} \tag{5}$$

由于被动式标签采用偶极天线，故不能确保天线主波束对准读写器，故 $G_{\text{tag}}\approx 1$. 若 $G_{\text{adv}}=G_{\text{reader}}=6$ dBi，$10\lg\chi=20$ dB，$10\lg T_r\approx -5$ dB，可将式(5)简化为

$$P_{RX,\text{adv}}\text{dBm}\approx P_{TX,\text{reader}}\text{dBm}-20\lg(d_{\text{for}}d_{\text{back}})-72.76 \tag{6}$$

式(6)表明窃听者所接收到的信号强度由 3 个因子决定：$P_{TX,\text{reader}}$、d_{for} 和 d_{back}. 举例来说，如果将合法读写器和标签放于一个 4 m×4 m 的房间中，标签置于读写器天线 2 m 处，设定读写器发射功率 $P_{TX,\text{reader}}\approx 0$ dBm，则标签反射的电磁波由于传播衰减和反射系数影响，其功率减至−35 dBm. 若窃听者距标签为 3 m，且混凝土墙存在其间，则窃听者所收到的标签反射信号功率约为−86 dBm，低于目前 RFID 商用读写器−75 dBm 的最高接收灵敏度[18].

此外，上述计算仅关注了链路预算，即接收信号强度，在实际环境中，窃听者若想获得后向信道中信息，还需对信号进行解调和解码，但由于 RFID 系统采用幅移键控(Amplitude Shift Keying，ASK)调制，极易受到噪声、多路径效应以及干扰的影响，导致解调和解码的误码率急速增大，导致窃听者的窃听能力进一步受限. 由于篇幅原因，我们在此不进行详细讨论，读者可参考文献[20].

3.3　实验验证

我们采用频谱仪测量了当读写器发射功率为 30 dBm 以及频谱仪接收天线增益为 8 dBi，到天线不同距离时的标签反射信号强度，如图 1 所示. 从图 1 中可以看出即使读写器发射功率达到 30 dBm，但距标签 6 m 处的反射信号强度小于−80 dBm，超出了现有 RFID 读写器的接收灵敏度，使得后向信道窃听极为困难. 需要说明的是，由于 WISP 能耗约为普通标签的 100 倍，所以读写器发射功率需要超过 23 dBm 以上才能使其获得足够能量，因此设定读写器发射功率为 30 dBm，但在 WiKey 实际应用时，可降低读写器发射功率以进一步缩短敌手可窃听距离.

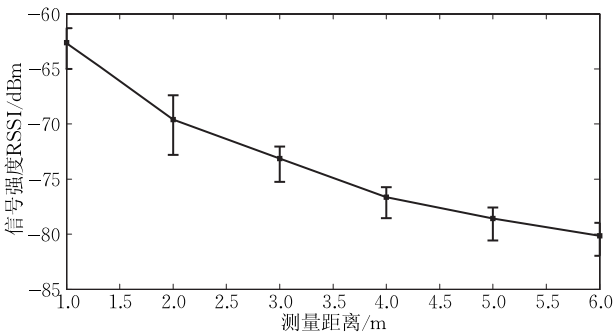

图 1　标签信号强度和距离关系

4　系统模型和设计目标

在本节，我们首先简要介绍 RFID 系统，再详细描述 RFID 信道的非对称性，并据此定义针对密钥无线生成的敌手能力，最后描述 WiKey 设计目标.

4.1　RFID 系统

典型的 RFID 系统主要由通过特定协议交互的两方组成：

读写器. 读写器与后台数据库通过安全信道连接，因此我们将两者看作一个整体，称为合法读写器或简称读写器. 读写器可向标签发送指令以获得标签中的数据.

标签. 标签响应来自读写器的指令. 对于被动式标签，由于没有电源，标签不能主动向读写器发射电磁波，所以采用反向散射模式通过幅度调制反射读写器载波来传输数据. 在反向散射通信中，发射信号极其微弱，即使读写器信号能在远至百米的范围内

被接收,标签的反射信号也仅能在有限的距离内被正确接收及解码.

协议. 读写器和标签通过特定协议通信. 现有的工业标准协议为 EPC Class 1 Generation 2(EPC C1G2)①,如图 2 所示. 该标准协议由两部分组成:"读取产品码"(Electronic Product Code,EPC)和"读/写用户区"操作. 在"读 EPC 操作"(或称为"盘存操作")中,标签收到查询指令后将返回一个 16 bits 的随机数(记为 RN16). 读写器收到 RN16 后,将该随机数作为应答返回给标签. 若标签验证 RN16 与之前所发送的一致,则向读写器发送其 EPC 或 TID(Tag ID,即标签 ID). 在"读/写用户区"操作中,读写器收到标签的 ID 后向标签发送指令以请求一个新的 RN16 作为读/写操作的会话句柄. 在用此句柄进行握手之后,读写器向标签发送读或写指令以对标签用户存储区读取或写入 16 bits 的数据,另外,读/写用户区的地址也包含在指令中.

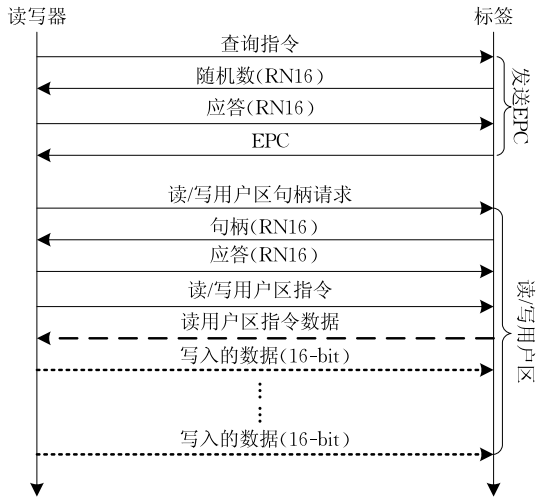

图 2 EPC C1G2 中定义的 RFID 通信协议

4.2 敌手模型和设计目标

在 RFID 标签密钥无线生成过程中,由于最终用户需要操作读写器向标签生成密钥,所以用户处于读写器和标签的通信区域. 如 4.1 节所述,标签到读写器的后向信道通信距离较短,所以用户可以目视发现进入该区域的敌手或敌手放置的设备. 因此,敌手不能在密钥生成过程中在读写器和标签通信区域内置入伪造的标签;另外,用户不会故意向读写器和标签的信道中注入错误数据或经常中断通信.

如 3.2 节中分析,由于后向信道中信号很弱,且敌手会在用户目视范围之外进行窃听,导致敌手距离标签较远,则敌手对后向信道窃听极为困难. 此外,若密钥生成过程在室内进行,而敌手只能在屋外窃听,则房屋的阻隔会进一步衰减标签信号 15~20 dB[19],这也增加了敌手窃听的难度.

综上所述,我们定义 RFID 系统密钥无线生成问题中敌手模型如下:

(1)敌手不能窃听后向信道;

(2)敌手可窃听前向信道或者向前向信道中注入错误信息,即向读写器发送伪造信息;

(3)敌手可向后向信道注入错误信息,即向合法标签发送伪造信息;

(4)敌手不能在密钥生成过程中在读写器和标签通信区域内置入伪造标签.

结合 RFID 系统密钥无线生成的需求以及敌手能力,定义 WiKey 设计目标如下.

密钥机密性. 敌手获取共享密钥的概率可忽略;

密钥可靠性. 标签能接收到读写器试图让其接收到的密钥;

群组密钥生成. 一个单独的读写器可同时为一组标签分配密钥.

5 WiKey 设计

本节针对密钥生成的两种场景描述 WiKey 的设计:(1)读写器为单个标签生成密钥. 其中包括读写器为一个标签生成一个共享密钥和为一批标签分别生成不同的共享密钥;(2)读写器为一组标签生成一个共同的组密钥.

5.1 概 述

WiKey 分为 3 个阶段:标签识别、密钥生成和隐私保护认证.

(1)标签识别. 在该阶段,若标签中不存在初始密钥,则读写器 R 对通信范围内的标签进行盘存操作,以识别每个需要生成密钥的标签 T_i. 本阶段用于发现标签,同时,在密钥生成之后于后台数据库记录标签的 ID. 由于标签识别过程在 EPC Gen2 空中接口标准中已定义,本文将不予详细阐述. 若标签中存在初始密钥,则读写器和标签可用此密钥进行双向隐私保护认证,认证成功后可执行密钥生成.

(2)密钥生成. 在该阶段,读写器 R 与标签执行 WiKey 协议生成密钥. 在本节剩余部分,我们将详细描述 WiKey 在 3 种不同场景下的协议:生成单个

① EPC Global Inc. EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz~960 MHz. http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g 2120-standard-20080511.pdf

标签的个体密钥生成、批量标签个体密钥生成以及群组标签的组密钥生成.

(3) 隐私保护认证. 在密钥生成之后，读写器与标签执行某个 PPA 协议进行双向隐私保护认证，以验证所生成的密钥在读写器和标签端是否一致；如果不一致，则再次执行密钥生成阶段. 由于目前隐私保护认证协议已经存在大量工作，所以本文将不对 WiKey 所使用的隐私保护认证协议进行描述，可参考的协议如 HashLock[21] 和 LAST[22].

5.2　个体密钥生成

生成个体密钥时存在两种情况：(1) 为单个标签生成密钥；(2) 为一批标签同时分别生成个体密钥.

(1) 单个标签密钥生成. 此时 WiKey 协议由两轮组成，如图 3(a)所示. 读写器 R 首先生成一个随机数 $r_R \in_R \{0,1\}^l$，之后将该随机数发送给标签 T_i，其中 l 是预定义的密钥长度. 当标签 T_i 收到 r_R 之后，首先生成另一个随机数 $r_{T_i} \in_R \{0,1\}^l$，之后计算共享密钥 $k_{T_i}=r_R \oplus r_{T_i}$. 之后标签 T_i 将 r_{T_i} 返回给读写器作为应答. 最后，读写器 R 计算所生成的共享密钥.

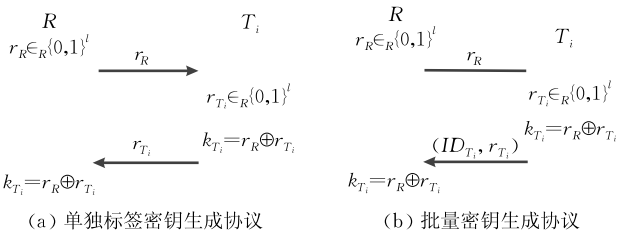

图 3　个体密钥生成协议

该协议为 WiKey 基本协议，其安全性依赖于如第 2 节所述，敌手不能窃听后向信道. 由于不能获得 r_{T_i}，即使敌手窃听读写器生成随机数 r_R 也无法正确地恢复所生成的共享密钥 k_{T_i}.

(2) 批量密钥生成. 作为单独标签密钥生成协议的扩展，批量密钥生成使得 RFID 读写器可以为大量不同标签同时独立地生成个体密钥. 该协议可用于大规模 RFID 系统.

与单个标签密钥生成相比，在批量密钥生成协议的第 2 轮(见图 3(b))，每个标签 T_i 回复中增加了标签 T_i 的身份 ID_{T_i}. 标签计算生成的共享密钥 $k_{T_i}=r_R \oplus r_{T_i}$. 一旦读写器 R 接收到 (ID_{T_i}, r_{T_i})，读写器为每个标签 T_i 计算共享密钥 $k_{T_i}=r_R \oplus r_{T_i}$ 并将其记录在后台数据库中.

5.3　群组密钥生成

群组密钥生成需在读写器 R 和一组标签 $T_1, \cdots, T_n$ 之间生成一个唯一的共享密钥 k，这里 n 为群组中标签的个数.

图 4 所示为群组密钥生成协议. 具体而言，在个体密钥生成协议中，共享的密钥由读写器和标签分别生成的随机数共同计算生成；而在群组密钥生成协议中，共享密钥则由同组中的不同标签选取的不同密钥碎片(随机数)共同生成，该协议由 3 轮组成. 读写器 R 首先向全组标签 $T_1, \cdots, T_n$ 广播一个“密钥生成请求”以通知所有标签开始进行群组密钥生成. 一旦组内标签 T_i 收到该“请求”，T_i 独立选取一个随机数 $r_{T_i} \in_R \{0,1\}^l$ 并将 (ID_{T_i}, r_{T_i}) 发送给读写器，ID_{T_i} 为标签 T_i 的 ID. 收到所有标签的回复之后，R 将接收到的标签响应中所有标签 $ID_{T_1}, \cdots, ID_{T_i}, \cdots, ID_{T_n}$ 与标签识别阶段所发现的标签 ID 进行对比并判断其是否一致，如果不一致则表明存在未应答标签(或称为“静默”标签)(详细讨论请见第 6 节)，则 R 重新发送“请求”以重启密钥生成. 若所有标签均已应答，可进行密钥生成. 此时，R 计算一个共享群组密钥 $k=\bigoplus_{i=1}^{n} r_{T_i}$，并为每个标签 T_i 计算密钥生成因子 $k_{T_i}=k \oplus r_{T_i}$，并广播 (ID_{T_i}, k_{T_i}). 当标签 T_i 收到 (ID_{T_i}, k_{T_i}) 之后，T_i 比较该消息中 ID_{T_i} 是否与自身 ID 一致，如不一致，T_i 丢弃该消息，否则计算共享组密钥 $k_{T_i}=k \oplus r_{T_i}$.

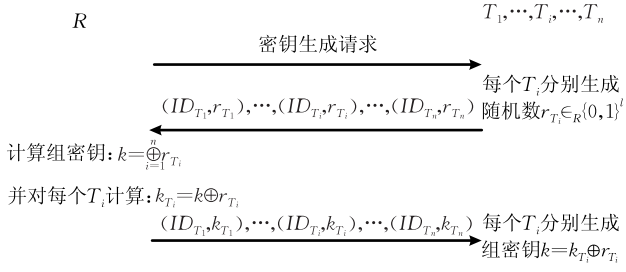

图 4　群组密钥生成协议

6　讨　论

本节讨论 WiKey 在实际应用中可能会遇到的问题.

(1) 标签存储限制. RFID 标签通常只有很小的用户存储区用于存储用户信息和密钥. 因此在设计 WiKey 时必须考虑标签存储效率. 在 WiKey 中，标签需要暂存标签和读写器生成的随机数以及最后生成的密钥. 对于目前的 RFID 应用，64 bits 密钥已经足以使用，因此标签上存储区须大于 128 bits，而目前市场上超过 90% 的标签(由 3 家公司生产：NXP、ALIEN 和 ImpinJ)的用户存储区均超过 512 bits.

(2) 标签计算能力. 由于计算能力有限，现在的普

通标签,如被动式标签,还不能执行 WiKey 中的所需操作.但是在现有标签上进行少量的修改以运行 WiKey 是可行的.详细来说,WiKey 中的主要操作是按比特异或以及随机数生成,均可用较少的门电路实现①.另外,现有的普通被动式标签也集成了 16 bits 的随机数发生器.在第 8 节,我们使用了一种具有一定计算能力的标签(Wireless Identification and Sensing Platform,WISP②)实现了 WiKey 原型.

(3)静默标签.在实际使用中,执行 WiKey 的标签可能被损坏或无应答(静默标签)导致 WiKey 无法执行.在个体密钥生成时读写器通过等待标签应答很容易发现静默标签.但当 WiKey 进行群组密钥生成时,读写器会一直等待静默标签的应答,这将导致 WiKey 无法继续执行.为解决这一问题,读写器在执行 WiKey 之前可初始化一个定时器,如果在定时器超时后还未收到某些标签的应答,则读写器将这些标签标记为静默标签并从群组中移除,再重新执行 WiKey.

(4)多群组标签.在一些应用中,一个标签可能会被多个群组所包含,可通过 WiKey 为标签生成多个群组密钥.但在使用这些多群组标签时,读写器需要通知标签使用哪个密钥.在考虑隐私保护的情况下,读写器可以用需要的群组密钥与标签进行一次隐私保护认证(如 HashLock[21] 和 LAST[22]),以通知标签应使用的密钥.由于篇幅限制,本文不对隐私保护认证进行详细阐述.

(5)用户错误.非专业用户在使用 WiKey 时可能会出现错误导致标签产生错误密钥,但 WiKey 的设计可检测用户错误.如 5.1 节所述,在 WiKey 生成密钥之后,隐私保护认证阶段将检查读写器和标签中密钥的一致性,若因为用户错误导致密钥不一致,则读写器不能通过密钥验证过程,此时用户可发现错误并重新执行 WiKey.

7 安全性

本节首先介绍了 WiKey 的安全目标,之后再给出安全分析.

7.1 安全目标

(1)抗被动攻击.在密钥植入之前,由于没有可信密钥来保护标签和读写器之间的消息,所以 WiKey 需抵抗敌手窃听,使得敌手不能通过窃听来推断所生成的密钥.如第 3.2 节所述,敌手不能窃听标签到读写器的后向信道,则当敌手仅能窃听前向信道时,WiKey 应使敌手不能推断所生成的密钥.

(2)抗主动攻击.敌手可以向前向和后向信道注入虚假信息.由于前向信道的通信范围较大,敌手可对前向信道较容易的注入或修改信息,其对应的攻击为读写器假冒.后向信道虽然不能被窃听,但敌手可以向后向信道注入信息,假冒标签以欺骗读写器获得生成的密钥.因此 WiKey 能够抵抗读写器和标签假冒.

7.2 安全性分析

7.2.1 被动攻击

WiKey 抗被动攻击的能力依赖于标签和读写器生成随机数的性质.若标签和读写器所生成的随机数中每比特为 0 或 1 的概率相等,则 WiKey 能抵抗被动攻击,而 EPC Gen 2 空中接口标准中已经定义了嵌入在 RFID 标签中的 16 bits 伪随机数生成器满足该性质.WiKey 中所用的随机数一般可大于 64 bits,仅需要对现有标签中的随机数生成器作简单并联即可获得.

为了获取所生成的共享密钥,敌手可窃听读写器和标签之间通信,但如 3.2 节所述,敌手不能窃听到从标签到读写器的后向信道上的消息,因此敌手仅能获得前向信道上读写器向标签发送的消息,即随机数或密钥生成因子(见 5.3 节群组密钥生成).但由于生成的密钥由读写器的随机数以及标签生成的随机数共同计算得到,缺少后向信道上标签生成的随机数,敌手不能恢复出所生成的密钥.另外,若敌手采用暴力攻击的方式猜测密钥,只需设置合适的密钥长度,即可增加敌手猜测的困难.具体而言,若采用 n 比特长度的随机数,则可产生 n 比特的密钥,则敌手猜测密钥的复杂度为 2^n,综合考虑 RFID 系统需求和标签能力,采用 64 bits 长度的密钥即可有效抵抗暴力攻击.

7.2.2 主动攻击

敌手可以向前向信道和后向信道中注入错误信息,以欺骗读写器和标签使得它们生成错误的密钥,因此我们对该种攻击进行详细分析.

(1)前向信道消息注入.敌手在合法读写器与标签执行 WiKey 之前、之时和之后均可向前向信道注入信息,从效果上可以看作敌手假冒合法读写器

① Docherty J, Koelmans A. Hardware implementation of sha-1and sha-2 hash functions. Technical Report in School of Electrical, Electronic and Computer Engineering, Newcastle University. http://async.org.uk/tech-reports/NCL-EECE-MSD-TR- 2011-170.pdf, 2011.

② WISP: Wireless Identification and Sensing Platform. http://www.seattle.intel-research.net/WISP/

与标签执行 WiKey 协议.

当攻击发生于 WiKey 执行之后，此时标签已经与合法读写器生成密钥，如 5.1 节所述，标签会使用所生成的密钥对读写器进行隐私保护认证，由于敌手不能获得该密钥，则攻击失败.

当攻击发生于 WiKey 执行之时，此时合法读写器正和标签进行密钥生成，由于没有初始共享密钥存在，标签不能分辨前向信道中消息来源. 若敌手注入了错误数据，会导致标签计算出与合法读写器端不一致的错误密钥. 而 WiKey 在密钥生成之后合法读写器会通过生成的密钥进行隐私保护认证以检测密钥一致性(如 5.1 节所述)，此时合法读写器会发现标签被敌手攻击.

当攻击发生于 WiKey 执行之前，敌手向标签发送随机数使得标签生成密钥，即使敌手不能获得后向信道中标签所产生的随机数从而不能计算出标签中所生成的密钥，但敌手依然可以让标签中产生错误密钥. 由于该错误密钥的存在，导致合法读写器与标签在执行 WiKey 时标签不能再重新产生合法密钥. 但是，合法读写器在执行密钥生成之前能发现该攻击，从而可对标签再次初始化.

综上所述，当敌手假冒合法读写器向前向信道注入消息时，即使能让 WiKey 不能生成合法密钥，也会被合法读写器发现.

(2) 后向信道消息注入. 在该攻击中，敌手虽然不能窃听到后向信道中的标签消息，但可以主动向合法读写器发送消息，以破坏密钥生成过程或获取读写器与标签所生成的密钥. 从攻击效果而言，等价于敌手假冒合法标签与读写器执行 WiKey 生成密钥. 由于在执行 WiKey 之前不存在共享密钥，合法的读写器无法区分合法标签和敌手假冒标签发送的消息. 我们对该攻击分为两类：针对个体密钥生成和群组密钥生成.

攻击个体密钥生成时，敌手与合法读写器执行 WiKey 可生成一个与读写器共享密钥，但无法获得其它合法标签与读写器生成的共享密钥，因此合法标签中所生成的密钥不会泄露. 攻击群组密钥生成时，敌手通过在合法标签群组中置入伪造标签，敌手可在 WiKey 执行之后生成获取该目标群组的共享组密钥. 但是，如 3.2 节所述，由于现实中密钥生成可处于一个私密空间，故敌手难以将伪造标签置入合法标签群组中. 进一步来说，假设敌手不放置伪造标签而是在远距离与读写器交换信息，敌手也能生成群组密钥. 但这种攻击会造成群组中增加不存在的标签，而 WiKey 在进行密钥生成之前需要先对标签进行识别，从而合法读写器和用户可以知道群组中标签数量. 这样，若群组中实际标签数少于 WiKey 执行时所发现的标签数，则用户可判断攻击发生.

8　原型实现

由于现有的商用被动式标签不具备 WiKey 所需的计算能力，并且不能编程，所以我们使用 ImpinJ Speedway Revolution 读写器和 10 个 WISP 标签来实现 WiKey 系统原型，如图 5 所示. WISP 是一种兼容 EPC C1G2 的超高频 RFID 被动式标签，相比于普通被动式商用标签，WISP 可编程且具有一定的计算能力. 在原型实现中，通过对固件的重编程实现对 WISP 的“读/写用户区”操作. 同时，选择 64 bits作为生产的密钥和随机数长度.

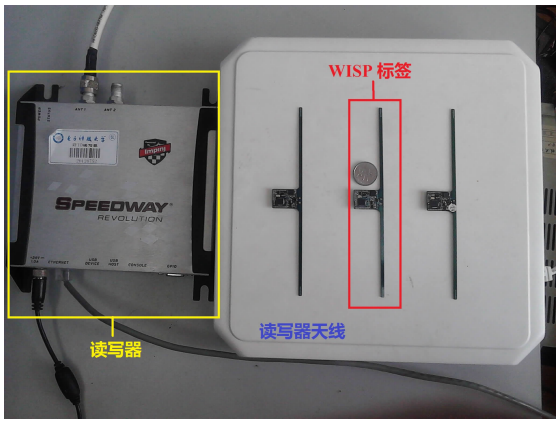

图 5　原型系统

根据 EPC C1G2 标准，读写器仅能通过“读用户区”操作来获取标签的非 ID 数据，也只能通过“写用户区”操作向标签发送数据，因此原型系统采用“读/写用户区”指令实现 WiKey 所需的读写器和标签消息交互.

使用 WISP 实现 WiKey 的最大挑战是解决标签能量限制. 对于被动式标签，其计算和通信的能量来自于读写器向标签发送查询指令和连续载波信号(见图 2). 标签能量由两个主要因素决定：第 1 个因素是标签和读写器之间的通信距离，越长的距离将导致在标签天线上越弱的信号强度；第 2 个因素是读写器同时操作的标签个数或群组中的标签个数. 由于读写器在操作标签时采用时分复用的方式，所以读写器只能以顺序方式访问标签，因此，在读写器读取范围内存在大量标签将导致每个标签的平均等

待时间延长.进一步而言,当读写器在向某个标签执行读/写操作时,其它标签只能等待并监听读写器信号,直到收到 RN16 应答或新的读/写操作指令,而长时间等待会使得标签掉电从而不能响应读写器指令.因此,读写器可操作的标签数量是受限的,特别是当读写器对标签执行高能耗的写操作时.

为克服能量限制,WiKey 采用了一种称为"多次盘存"的机制,即当读写器需要向标签写入大量数据(如 64 bits 随机数)时,该数据将被分为数个单元,每个单元包含 16 bits 数据,对于每个数据单元,读写器发起一次新的盘存操作发送查询指令和连续载波以对标签充电.通过该方式,读写器可以同时操作更多标签,即扩展 WiKey 中批量或群组密钥生成所支持的标签数量.

9 性能评价

我们基于原型系统对 WiKey 性能进行了评价.从原型实现的过程中我们发现,WiKey 性能主要由两个因素决定:(1)读写器和标签执行 WiKey 时的操作距离;(2)批量或群组密钥生成时 WiKey 所支持的标签数量.所以我们分别测试了 WiKey 在这两种指标下的性能.

9.1 操作距离

在本实验中,我们测试了 WiKey 操作距离和操作时间的关系,该实验包括 3 个部分:(1)读写器与一个标签生成个体密钥;(2)读写器不采用"多次盘存"方法(见第 7 节)时与多个标签生成密钥;(3)读写器采用"多次盘存"时与多个标签生成密钥.需注意的是由于批量个体密钥生成和群组密钥生成所需的运算和协议过程类似,其性能也类似,因此在第 2 和第 3 个实验中,我们将两种密钥生成方法统一测试.

在测试个体密钥生成时,我们在 0～1 m 范围内调整 WISP 标签到读写器天线的距离,在每个距离上,我们执行 WiKey 协议生成密钥并测量密钥生成所需的时间,每次测试重复 10 次,取均值为最终测试结果.

图 6 描述了读写器和 1 个标签运行 WiKey 时其操作时间和距离关系.从图 6 可以看出,随着距离增加,操作时间先在 80 cm 以内递减,之后开始持续增长.其原因如下:超高频 RFID 系统工作频率为 915 MHz,其波长 λ 约为 33.3 cm,在小于 $\lambda/2\pi$(约 5.2 cm)的近场范围内电磁波主要以磁场形式存在[①],由于标签只能接收电场能量,所以标签需要较长时间充电,导致在 10 cm 以内其操作时间较长;随着操作距离增加,电场能量逐渐增强,标签可更有效地获得能量,所以其操作时间相应减小;而超过 80 cm 之后,电磁波衰减效应导致标签在单位时间内获得能量开始减少,所以其操作时间开始增长.另外,从图中可以看出操作时间大于 640 ms,超过了商用被动式标签的响应时间,这是由于 WISP 标签所需能量约为商用标签的 100 倍,其能量采集时间更长,若对 WISP 进行一些修改,采用更加高效的能量采集电路,将会有效缩短 WiKey 操作时间.

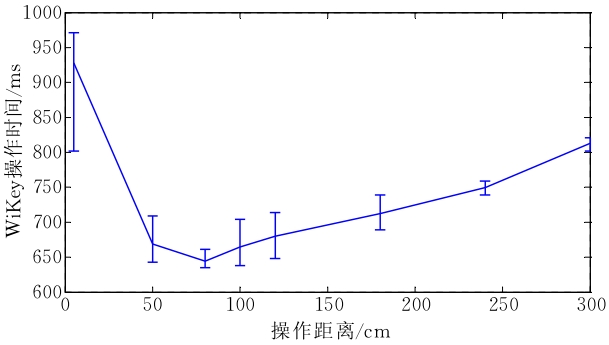

图 6 单个标签操作距离和操作时间

图 7 和图 8 描述了当读写器与多个标签运行 WiKey 时其操作时间和操作距离的关系.图 7 为不采用"多次盘存"机制的结果;图 8 为采用"多次盘存"后的结果.从两图中可以看出,WiKey 操作时间随操作距离和标签数目增长而增长,其原因是更多标签和信号传播衰减导致标签需要更多时间获取足够能量.另外,相比单个标签密钥生成,在多标签运行 WiKey 时,操作时间增长显著,这是由于目前的 RFID 空中接口标准规定读写器采用时分复用方式顺序访问标签,标签数量增长会导致操作时间相应增加.

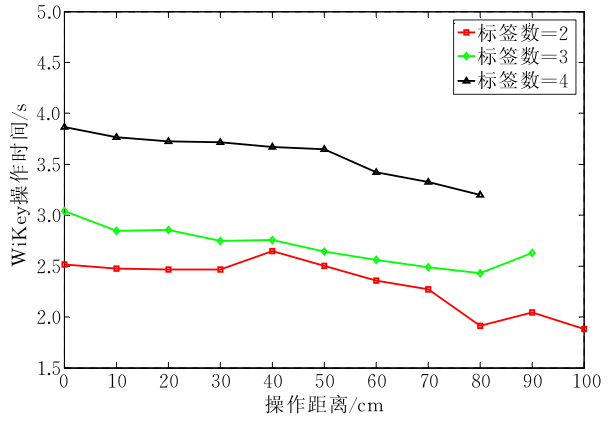

图 7 不使用"多次盘存"群组密钥生成

① Inductive Coupling. http://en.wikipedia.org/wiki/inductive coupling.

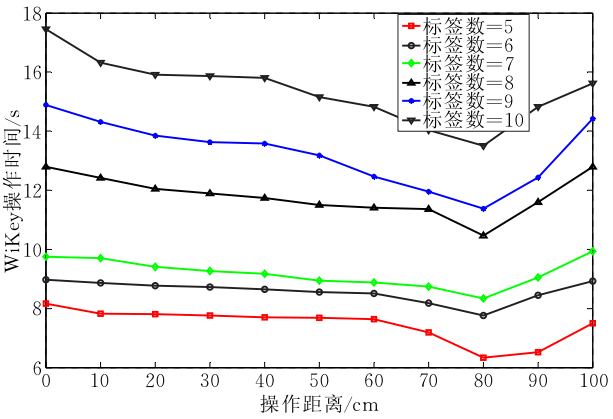

图 8　使用“多次盘存”群组密钥生成

9.2　标签数量

对比图 7 和图 8，可以看出 WiKey 操作时间与标签数量呈正比. 对于图 7，由于未采用“多次盘存”机制，多个标签在等待读写器访问时间过长导致掉电，使得标签不能响应读写器指令，因此 WiKey 所能支持的标签数量受到限制，从图 7 可以看出，此时 WiKey 所能支持的标签数量在 4 个以内. 而采用了“多次盘存”机制之后（如图 8 所示），虽然操作时间相比图 7 增大（10 个标签时约 14～18 s），但是能支持的标签数量显著增加. 而密钥生成是一次性工作，18 s 以内的操作时间可以接受. 另外，由于我们手中只有 10 个 WISP 标签，所以未能测试更多标签时的 WiKey 性能.

10　总　结

本文提出了一种 RFID 系统密钥无线生成方法（称为 WiKey）以支持 RFID 系统的安全应用. WiKey 针对标签个体密钥设计了基本密钥生成方法，并据此设计了群组密钥生成机制. 我们讨论并分析了 WiKey 在实际使用中可能遇到的问题并提出了相应的解决方法. 安全分析表明 WiKey 能抵抗被动窃听和主动信道消息注入. 同时我们在 WISP 和商用读写器上实现了 WiKey 并对性能进行了评价，结果显示 WiKey 能在 RFID 标签和读写器上高效的生成密钥，适用于 RFID 的安全应用.

参　考　文　献

[1] Ni L M, Liu Y, Lau Y C, et al. LANDMARC: Indoor location sensing using active RFID. Wireless Networks, 2004, 10(6): 701-710

[2] Tian Y, Chen G, Li J. A new ultra-lightweight RFID authentication protocol with permutation. IEEE Communications Letters, 2012, 16(5): 702-705

[3] Li Y, Ding X. Protecting RFID communications in supply chains//Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security. Singapore, 2007: 234-241

[4] Chen M, Luo W, Mo Z, et al. An efficient tag search protocol in large-scale RFID systems//Proceedings of the 32nd IEEE International Conferenceon Computer Communications. Turin, Italy, 2013: 899-907

[5] Kriplean T, Welbourne E, Khoussainova N, et al. Physical access control for captured RFID data. IEEE Pervasive Computing, 2007, 6(4): 48-55

[6] Agudo I, Rios R, Lopez J. A privacy-aware continuous authentication scheme for proximity-based access control. Computers & Security, 2013, 39(1): 117-126

[7] Moriyama D, Matsuo S, Ohkubo M. Relations among notions of privacy for RFID authentication protocols. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2014, 97(1): 225-235

[8] Alomair B, Clark A, Cuellar J, et al. Scalable RFID systems: A privacy-preserving protocol with constant-time identification. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(8): 1536-1550

[9] Finkenzeller K. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. 2nd Edition. John Wiley & Sons Ltd, 2003

[10] Diffie W, Hellman M E. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644-654

[11] Kuo C, Luk M, Negi R, et al. Message-in-a-bottle: User-friendly and secure key deployment for sensor nodes//Proceedings of the 5th International Conference on Embedded Networked Sensor Systems. Sydney, Australia, 2007: 233-246

[12] Stajano F, Anderson R. The resurrecting duckling: Security issues for ubiquitous computing. Computer, 2002, 35(4): 22-26

[13] Castelluccia C, Mutaf P. Shake them UP! A movement based pairing protocol for cpu-constrained devices//Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services. Seattle, USA, 2005: 51-64

[14] Bellot P, Dang M. Secret key agreement over a non-authenticated channel. IEEE Transactions on Information Theory, 2003, 49(4): 48-55

[15] Mathur S, Trappe W, Mandayam N, et al. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel//Proceedings of the 14th Annual International Conference on Mobile Computing and Networking. San Francisco, USA, 2008: 128-139

[16] Jana S, Premnath S, Clark M, et al. On the effectiveness of secret key extraction using wireless signal strength in real environments//Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. Beijing, China, 2009: 321-332

[17] Goldsmith A. Wireless Communications. Cambridge, UK: Cambridge University Press, 2005
[18] Dobkin D M. The RF in RFID: UHF RFID in Practice. Oxford, UK: Newnes Press, 2012
[19] Philippidis T P, Aggelis D G. Experimental study of wave dispersion and attenuation in concrete. Ultrasonics, 2005, 43(7): 584-595
[20] Fan Changxin. Principles of Communications. Beijing: Publishing House of Electronics Industry, 2010
[21] Weis S A, Sarma S E, Rivest R L, et al. Security and privacy aspects of low-cost radio frequency identification systems// Hutter D, Müller G, Stephan W, Ullmann M eds. Security in Pervasive Computing. Lecture Notes in Computer Science 2802. Springer Berlin Heidelberg, 2004: 201-212
[22] Lu L, Liu Y, Li X. Refresh: Weak privacy model for RFID systems//Proceedings of the 29th International Conference on Computer Communications. San Diego, USA, 2010: 1-9

LU Li, born in 1978, Ph. D., associate professor. His research interests include wireless system security, RFID systems and applied cryptography.

Background

Along with Radio Frequency Identification (RFID) systems being deployed in modern industries such as retail, logistics and supply chain management, the requirement for privacy and security in RFID systems has been addressed by academia and industry. Current security techniques employ shared secret keys to protect communications among the RFID reader and tags. Hence, without a secure secret key generation scheme, existing techniques in RFID systems cannot be proved as secure and private. The issue of secret key generation, however, is not well addressed due to severe resource-constraints of RFID tags as well as open wireless communications. Thus there's no solution suitable for key generation in RFID systems in the literature.

In this paper, we propose an innovative wireless key generation scheme, called WiKey, with which a legitimate reader can generate secret keys among itself and tags by effectively utilizing the asymmetry of communication channels of RFID systems. WiKey is a very light-weighted protocol and can be implemented on current RFID systems. Through intensive security analysis and prototype implementation, we show that WiKey can provide efficient and strong protection for RFID systems.

The author has done some works on the issue of privacy-preserving authentication for RFID systems and published over 5 papers on including IEEE Infocom, Percom, IPDPS and IEEE Transactions on parallel and distributed systems. From 2010 to 2012, the author was working on the project about privacy-preserving technology in RFID systems, which was support by National Natural Science Foundation of China under Grant No. 60903155.

This work is supported by National Natural Science Foundation of China under Grant Nos. 61173171, 61472068, the Fundamental Research Funds for the Central Universities under Grant No. ZYGX2012J072 and China Postdoctoral Science Foundation Funded project under Grant No. 2014M550466.