Journal of Computer Applications
计算机应用,2012,32(4):968-970,980
ISSN 1001-9081
CODEN JYIIDU
2012-04-01
http://www.joca.cn

文章编号:1001-9081(2012)04-0968-03
doi:10.3724/SP.J.1087.2012.00968

EPC Gen2 标准下强安全射频识别认证协议

唐拥政[1*],王明辉[1],王建东[2]
(1.盐城工学院 信息工程学院,江苏 盐城 224051; 2.南京航空航天大学 信息科学与技术学院,南京 210016)
(*通信作者电子邮箱 tyz@ycit.edu.cn)

摘 要:由于现在很多射频识别(RFID)认证协议不符合 EPC Class 1 Gen 2(EPC Gen2)标准的要求,同时对 RFID 系统的计算能力要求很高,因此很难在低端标签中实现。针对上述问题,通过分析已有协议的安全性,总结出不安全协议的缺陷,提出了一种新的基于 EPC Gen2 标准的 RFID 认证协议,并采用 BAN 逻辑对协议进行了安全性证明。通过安全性分析,新协议满足了信息机密性、数据完整性和身份真实性的 RFID 系统认证协议的安全需求。

关键词:无线射频识别;前向安全;认证协议;密钥;循环冗余校验
中图分类号:TP309 **文献标志码**:A

Enhanced secure RFID authentication protocol for EPC Gen2

TANG Yong-zheng[1*], WANG Ming-hui[1], WANG Jian-dong[2]
(1. *School of Information Engineering, Yancheng Institute of Technology, Yancheng Jiangsu* 224051, *China*;
2. *College of Information Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing Jiangsu* 210016, *China*)

Abstract: Many current Radio Frequency IDentification (RFID) authentication protocols cannot conform with the EPC Class 1 Gen 2 (EPC Gen2) standards or cannot meet the requirements of low-cost tags for the RFID authentication protocol. A new RFID authentication protocol based on the EPC Class 1 Gen 2 (EPC Gen2) standards was proposed and the security proof was given with BAN logic. After analyzing the security, the proposed protocol can meet the RFID security demands: information confidentiality, data integrity and identity authentication.

Key words: Radio Frequency IDentification (RFID); forward secrecy; authentication protocol; key; Cyclic Redundancy Check (CRC)

0 引言

射频识别技术(Radio Frequency IDentification,RFID)是一种非接触式的自动识别技术,在系统的前端主要由 RFID 标签和读写器组成。读写器向标签发出认证请求,并将标签返回的数据传输给后台进行数据处理。它通过射频信号自动识别目标并获取相关数据,使得系统无需任何物理接触就可以完成特定目标对象的自动识别。目前 RFID 技术已经被广泛应用于物流供应管理、生产制造和装配、航空行李处理、邮件、快运包裹处理及物联网等领域。

然而,在有些情况下,未授权读写器可以读取和收集用户的电子标签里的个人信息,通过信息处理和比对,在用户下次使用标签时就可以跟踪其位置信息,并且还可以获取用户的隐私信息,因此,RFID 系统的安全问题引起了人们的极大关注。但是,由于低成本电子标签在计算能力和存储上具有很大限制,目前很多的安全协议没有办法在其上面应用。本文通过比较分析目前比较典型的 RFID 安全协议,设计了一种低成本、高效率、安全的双向认证协议。并通过 BAN 逻辑分析了协议的安全性。

1 RFID 系统

1.1 RFID 系统的构成

RFID 系统由标签、读写器和数据处理系统三部分组成(如图 1 所示)。标签和读写器通过无线信号进行通信,读写器向 RFID 标签发出命令,标签根据接收到的命令做出响应。

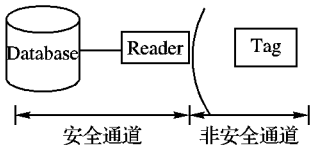

图 1 RFID 系统构成

1)标签(Tag)。

RFID 的标签是由用于无线通信的耦合线圈电路(天线)和计算、存储数据的逻辑门电路组成。天线用于无线通信,芯片的计算和存储能力十分有限。每个标签具有唯一的 ID。

2)读卡器(Reader)。

读卡器由无线收发模块、信号天线、控制单元及接口电路等组成,其计算能力和存储能力都比标签要大。当 RFID 读写器通过收发模块发出询问命令且接收到标签返回的信息后,将信息传送给后端数据库。

3)后端数据库(Database)。

后端数据库系统具有巨大的数据分析和存储能力,存储着包含读卡器和标签的所有相关的数据信息,并且接收来自 RFID 读写器的数据。

从 RFID 读写器到标签的信道是不安全信道;从 RFID 读写器和后端数据库之间是安全信道。

收稿日期:2011-10-13;**修回日期**:2011-12-11。
基金项目:盐城市 2009 年科技发展计划项目(YK2009092);盐城工学院 2010 年校级科研项目(XKY2010024)。
作者简介:唐拥政(1973-),男,江苏盐城人,副教授,硕士,主要研究方向:网络安全、密码学; 王明辉(1977-),男,黑龙江绥棱人,讲师,硕士,主要研究方向:信息安全、密码协议; 王建东(1945-),男,江苏南京人,教授,博士生导师,主要研究方向:人工智能、信息安全、计算复杂性理论。

1.2 安全需求

RFID 系统的安全类似于网络和计算机安全,其主要目的是为了保证数据传输和数据存储的安全,但是 RFID 系统中的读写器和标签所具有的运算能力极其有限,因此,根据信息系统安全的基本要求,结合 RFID 系统自身的实际情况,比较完善的 RFID 系统安全解决方案应当具备信息机密性、数据完整性和身份真实性等基本特征。

1)信息机密性。

一个 RFID 系统在运行过程中,电子标签不能向任何未经允许的读写器泄漏任何产品信息,RFID 电子标签中所包含的信息一旦被攻击者获取,将会泄露使用者的隐私,因而,一个完备的 RFID 安全方案必须能够保证标签中所包含的信息仅能被授权的读写器访问。

2)数据完整性。

在通信过程中,数据完整性能够保证接收者收到的信息在传输过程中没有被攻击者篡改或替换。在 RFID 系统中,通常使用循环冗余校验(Cyclic Redundancy Check,CRC)来进行数据完整性的检验,它使用的是一种带有共享密钥的散列算法,即将共享密钥和待检验的消息连接在一起进行散列运算,对数据的任何细微改动都会对消息认证码的值产生较大影响。

3)身份真实性。

电子标签的身份认证在 RFID 系统的许多应用中非常重要。攻击者可以伪造电子标签,也可以通过某种方式隐藏标签,使读写器无法获取该标签,从而成功地实施产品转移;读写器只有通过身份认证才能够确信消息是从正确的电子标签发送过来的;也有攻击者伪造读写器通过多次访问标签来获取标签中的信息。因此,标签也需要对读写器的身份进行认证,这称之为双向认证。

2 RFID 认证协议

2.1 相关协议分析

因为 RFID 系统应用广泛,很多学者在这方面投入很大精力,但由于每个学者对 RFID 系统能力的假设不同,所以提出的基于 RFID 的认证协议千差万别。有些协议中使用了哈希函数,其中比较典型的是 Hash 锁协议[1],随机 Hash 锁协议[2]和 Hash 链协议[3];有些协议使用了更加复杂的运算,这些协议对 RFID 系统的计算能力要求很高,在实际使用中的成本很高。为了促进 RFID 技术的推广,EPC Global 组织制订了 EPC Class 1 Gen 2 (EPC Gen2)[4]标准,这个标准利用了一个 16 位的伪随机数生成器(Pseudo Random Number Generator,PRNG)和一个 16 位的循环冗余校验码(CRC)为 RFID 协议提供基本的可靠性保证,符合该标准的标签只需采用硬件复杂度较低的 PRNG 和 CRC,而不采用加密函数和 Hash 函数,这样就可以很大程度地提高协议的执行效率。

近年来,研究者们提出了很多符合 EPC Gen2 标准的认证协议。2008 年,Burrow 等[5]提出一个新的符合 EPC Gen2 标准的协议,声称该协议能够抵抗标签跟踪和伪装攻击,在这个协议中使用了伪随机数生成器(PRNG),同时标签具有乘法和加法的运算能力。通过分析可以发现文献[5]协议的安全性取决于一个线性函数 $g()$,通过运算,攻击者能够得到标签中密钥的值,而且攻击者连续窃听同一个标签和读写器之间的回话,可以有效伪装一个标签,并且攻击者可以对标签进行跟踪[6]。

Chen 等[7]提出一个轻量级的 RFID 认证协议,在协议中,产品电子代码(Electronic Product Code,EPC)被用作标签的标识码,读写器和标签共享秘密信息 S_1,S_2 和 EPC。这个协议的致命缺陷是标签可以被模仿[8]。协议的运行过程如下:

首先读写器 R 向标签 T 发送认证请求,并发送随机数 r_R:$CRC(S_1,r_R)$。标签 T 验证 $CRC(S_1,r_R)$,生成随机数 r_T,通过计算 $X \leftarrow (S_2 \oplus EPC \oplus r_T)$,$Y \leftarrow CRC(r_T \oplus EPC \oplus X)$,再将$(r_T, X, Y)$ 发送给读写器 R。读写器 R 验证(X,Y) 后将结果返回标签 T。

攻击者能够被动监听读写器和标签之间的通信,并且保存它们之间的交换数据。在同一个标签第二次认证时,攻击者将协议中的(r_T,X,Y) 替换为(r,X',Y')。其中 $X' = X \oplus r_T \oplus r$($X$ 和 r_T 在上次通信中获得),$Y' = Y$,$Y = CRC(r_T \oplus EPC \oplus X) = CRC(r_T \oplus S_1 \oplus S_2 \oplus EPC \oplus r_T)$。这样,攻击者可以成功扮演标签 T[9]。

最近,邓淼磊等[10]提出一个新的基于 Gen2 标准的 RFID 认证协议。在协议中,读写器 R 向标签 T 发出认证请求,并发送 n_r。标签 T 计算 $M_1 = CRC(P \oplus (n_r \| n_t)) \oplus k$,并且发送$(M_1, n_t)$ 给读写器 R,读写器 R 转发(M_1,n_r,n_t) 给数据库 D。在协议中,CRC 被当成一个单项的加密函数,忽略了 CRC 的另外一个不安全属性,对于所有的 A,B,都有 $CRC(A \oplus B) = CRC(A) \oplus CRC(B)$[6]。再者,攻击者通过侦听,可以获得 n_r 和 n_t,因此,攻击者可以计算出 $CRC(n_r \| n_t)$,$M_1 \oplus CRC(n_r \| n_t) = CRC(P) \oplus k$,攻击者可以通过伪造 n_r,在不需要知道 P 和 k 的情况下,成功地冒充标签 T。

2.2 基于 EPC Gen2 认证协议中存在的问题

1)标签的 ID 以明文形式出现在认证协议中,没有对 ID 进行有效保护,致使标签容易受到跟踪,泄漏用户隐私信息。

2)错误地将 $CRC()$ 当成加密函数,致使攻击者能够推导出标签的 ID。

3)为了适应分布式环境,有些协议提供数据同步功能,但是标签和数据库的更新没有同时进行,或者受到攻击,导致数据不同步。

4)到目前为止,已经有很多的 RFID 安全协议被提出,但是大多缺乏严格的格式化分析和证明。

在总结上述问题的基础上,本文提出一个新的基于 EPC Gen2 标准的 RFID 认证协议,并采用 BAN 逻辑对上面所提出的协议进行形式化分析、证明。

3 强安全的 EPC Gen2 认证协议

3.1 协议设计

系统初始化之后,数据库 D 和标签 T 之间共享秘密随机数 k,数据库 D 和标签 T 之间共享标签的 ID(ID 在标签中称 ID_T,ID 在数据库中称 ID_D),数据库中存储记录(TID,k)。

$R \rightarrow T$:读写器 R 向标签 T 发出认证请求 Query。

$T \rightarrow R \rightarrow D$:标签 T 生成随机数 α,计算 $M_T = CRC(PRNG(ID_T \| \alpha) \oplus k, N_T = k \oplus \alpha$。并将$(M_T,N_T)$ 发送给

读写器 R。读写器 R 产生随机数 β,将 (M_T, N_T, β) 发送给数据库 D。

$D \rightarrow R \rightarrow T$:数据库 D 首先认证标签 T,数据库 D 本身存储有参数 m 的值,可以计算出 $\alpha = N_T \oplus m$。通过查询记录 (ID_D, k),看是否满足 $CRC(PRNG(ID_D \| \alpha) \oplus k = M_T$,如果找到这样的 ID_D,则数据库 D 完成对标签 T 的认证,否则放弃此次连接。标签 T 通过数据库 D 的认证以后,数据库 D 计算 $K = PRNG(ID_D) \oplus \alpha \oplus \beta, M_D = CRC(PRNG(ID_D \| \beta) \oplus k$,更新 $k = k \oplus K$。将 $(M_D, PRNG(ID_D))$ 发送给读写器 R,读写器 R 计算 $\alpha = N_T \oplus k, K = PRNG(ID_D) \oplus \alpha \oplus \beta$,更新 $k = k \oplus K$,并将 (M_D, β) 发送给标签 T。

T:标签 T 收到数据后,计算出 $K = (PRNG(ID_T) \oplus \alpha \oplus \beta)$,如果 $CRC(PRNG(ID_T \| \beta) \oplus k = M_D$,那么标签 T 完成对数据库 D 的认证,同时更新 $m = m \oplus K$。

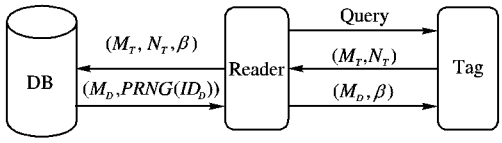

图 2 协议图

3.2 协议的 BAN 逻辑证明

这里采用 BAN 逻辑对上面提出的基于 EPC Gen2 标准的认证协议进行形式化的分析和证明。采用 BAN 逻辑[5]分析通信协议的安全性,能够在设计协议的过程中,揭示一些非形式化方法很难发现的缺陷和冗余。通过严格的数学推理,能够很好地解决协议的认证性问题。

1)协议理想化。

消息 1 $R \rightarrow T: N_a$

消息 2 $T \rightarrow R: \{M_T, N_T\}$

消息 3 $R \rightarrow D: \{M_T, N_T, \beta\}$

消息 4 $D \rightarrow R: \{M_D, PRNG(ID_D)\}$

消息 5 $R \rightarrow T: \{M_D, \beta\}$

2) 安全目标。

$D \models ID_T, T \models ID_D$

3) 初始假设。

$P1: D \models D \overset{k}{\leftrightarrow} T$

$P2: T \models T \overset{k}{\leftrightarrow} D$

$P3: D \models \#(\alpha)$

$P4: T \models \#(\beta)$

$P5: D \models T \mid\Rightarrow (ID_T \| \alpha)$

$P6: T \models D \mid\Rightarrow (ID_D \| \beta)$

4) 逻辑推理。

由消息 3 知 $D \lhd \{ID_T \| \alpha\}_K$,由假设 $P1$ 和规则 $\dfrac{P \models Q \overset{Y}{\leftrightarrow} P, P \lhd \{X\}_Y}{P \models Q \mid\sim X}$ 得到 $D \models T \mid\sim (ID_T \| \alpha)$;由假设 $P3$ 和规则 $\dfrac{P \models \#(X)}{P \models \#(X,Y)}$,可得 $D \models \#(ID_T \| \alpha)$;由公式 $\dfrac{P \models \#(X), P \models Q \mid\sim X}{P \models Q \models X}$ 可得 $D \models T \models (ID_T \| \alpha)$;再由规则 $\dfrac{P \models Q \mid\Rightarrow X, P \models Q \models X}{P \models X}$ 可得 $D \models (ID_T \| \alpha)$;最后由规则 $\dfrac{P \models (X,Y)}{P \models X}$ 得到 $D \models ID_T$。

由消息 5 知 $T \lhd \{ID_D \| \beta\}_K$,由假设 $P1$ 和规则 $\dfrac{P \models Q \overset{Y}{\leftrightarrow} P, P \lhd \{X\}_Y}{P \models Q \mid\sim X}$ 得到 $T \models D \mid\sim (ID_D \| \beta)$;由假设 $P4$ 和规则 $\dfrac{P \models \#(X)}{P \models \#(X,Y)}$,可得 $T \models \#(ID_D \| \beta)$;由公式 $\dfrac{P \models \#(X), P \models Q \mid\sim X}{P \models Q \models X}$ 可得 $T \models D \models (ID_D \| \beta)$;再由规则 $\dfrac{P \models Q \mid\Rightarrow X, P \models Q \models X}{P \models X}$ 可得 $T \models (ID_D \| \beta)$;最后由规则 $\dfrac{P \models (X,Y)}{P \models X}$ 得到 $T \models ID_D$。

4 安全性分析

4.1 安全性能比较

本文提出的协议与之前提出的协议进行了比较(详见表 1),通过比较可以看出,本协议具有很好的安全性能,满足了 RFID 认证协议的基本需求。其中,T 表示具备该项要求;F 表示不具备该项要求。

表 1 RFID 认证协议的比较

认证协议	密钥同步更新	相互认证	伪装攻击	重传攻击	流量分析	匿名	前向安全性
Hash 锁	F	F	F	F	F	F	T
随机 Hash 锁	F	T	F	F	F	T	T
Hash 链	F	F	F	F	T	T	T
文献[5]协议	T	T	F	T	F	T	T
文献[7]协议	T	T	F	T	T	T	T
本文协议	T	T	T	T	T	T	T

4.2 安全属性分析

1)抵抗跟踪攻击。

抵抗跟踪是用户隐私保护的基本需求,由于当前的协议中标签在每次通信中都没有直接使用 TID,传递的消息都不是固定的,并且每次的输出都有随机数的参与,也是不可预知,因此攻击者对标签的跟踪攻击很难实现。

2)抵抗冒充攻击。

攻击者可以被动地侦听读写器和标签之间的通信,并且有能力获得 N_T、N_R、M_D 和 M_T。但是攻击者没有能力通过计算它们的历史数据获得当前通信中的数值,因为每次认证过程之后秘密信息 m 都会得到更新,而 α 和 β 在每次认证过程中都是随机生成的,两次相同的概率可以忽略不计。因此,攻击者没有能力成功地冒充读写器或者标签。

3) 双向认证。

在本文协议中,服务器通过在数据库中查找 TID' 和 m 来验证 M_T,而 TID 和 m 为数据库和合法标签所共有。标签通过计算 K 和 m 来验证 M_D,K 和 m 只有数据库和合法的标签及读写器才能拥有。

4) 前向安全性。

即设攻击者获得了读写器和标签某次通信的秘密信息,仍然无法获得之前它们之间的通信信息。因为在每次认证完成之后都对读写器和标签的共有信息 m 进行了更新,而 α 和 β 是随机生成的,因此攻击者无法根据当前获得的输出回溯之前的认证数据,具有前向安全性。

结合上述分析,本文的协议完全达到了信息机密性、数据

(下转第 980 页)

篡改定位能力。但是,从图 6(d)来看,单从水印图像和 TAF 值,仅能定位篡改发生的位置,仍无法区分恶意攻击的类型。不过,可以通过对比遭到篡改音频段的波形,来进一步区分此段语音究竟是遭到了剪切,还是替换攻击。

定位了篡改位置后,可以进一步提取出篡改发生段音频的波形,如图 7 所示。

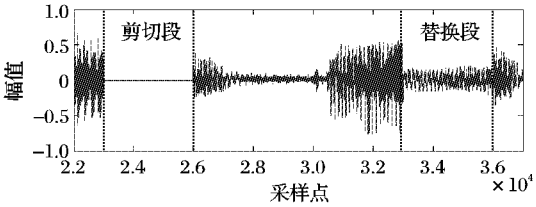

图 7 篡改发生段待测音频波形

图中两虚线间的音频段为发生篡改的音频段,对比两个篡改段可以看出,左边音频段的篡改比较彻底,幅度变成了零,可以推断该段音频遭到了剪切攻击;而右边的篡改段依然有一定的幅度,很可能是被替换成了另一段音频,可以推断该段音频遭到了替换攻击。由此,就能进一步对两种恶意攻击进行区分。

4 结语

本文提出一种可用于内容认证的半脆弱音频零水印算法,将自适应思想和零水印技术结合起来,采用图像分块、Arnold 变换和小波分解等方法完成了水印图像的嵌入和提取,并将分割的图像块和自适应分帧处理后的音频段一一对应起来,使得算法效率更高,篡改定位更加准确。其特点是在不改变载体音频的前提下,完成对载体音频的完整性认证,并准确定位篡改区域。实验结果说明,本算法不但对常规攻击具有较好的鲁棒性,而且对恶意攻击还具有较好的篡改定位能力,同时计算简单,易于实现,具有很高的应用价值。

参考文献:

[1] 杨晋霞, 马朝阳, 张雪英. 基于小波包分析的数字音频双水印算法[J]. 计算机应用, 2010, 30(5): 1218 - 1220.

[2] WU SHAO-QUAN, HUANG JI-WU, MEMBER S. Efficiently self-synchronized audio watermarking for assured audio data transmission [J]. IEEE Transactions on Broadcasting, 2005, 51(1): 69 - 76.

[3] MENDELZON A O, RIZZOLO F, VAISMAN A. Indexing temporal XML documents[C]// VLDB'04: Proceedings of the Thirtieth International Conference on Very Large Data Bases. [S. l.]: VLDB Endowment, 2004: 216 - 227.

[4] MARTIN S, PETITCOLAS F A P. Stirmark benchmark: Audio watermar-king attacks[EB/OL]. [2011 - 06 - 01]. http://private.sit.fhg.de/~steineba/publikationen-Dateien/itcc01_stirmark.pdf.

[5] 温泉, 孙锬锋, 王树勋. 零水印的概念和应用[J]. 电子学报, 2003, 31(2): 214 - 216.

[6] 张小华, 孟红云, 刘芳, 等. 一类有效的脆弱型数字水印技术[J]. 电子学报, 2004, 32(1): 114 - 117.

[7] 张兵路, 姜建国, 冯复科, 等. 基于 DWT 的音频零数字水印技术研究[J]. 计算机工程, 2005, 31(18): 148 - 152.

[8] 全笑梅, 张鸿宾. 用于篡改检测及认证的脆弱音频水印算法[J]. 电子与信息学报, 2005, 27(8): 1187 - 1191.

[9] 王向阳, 祁薇. 用于版权保护与内容认证的半脆弱音频水印算法[J]. 自动化学报, 2007, 33(9): 937 - 940.

[10] 桑军, 张之刚, 向宏. 基于人工神经网络的半脆弱零水印技术[J]. 计算机工程与应用, 2009, 45(16): 93 - 95.

[11] 廖琬名, 张玉贤, 李东晓, 等. 基于小波变换的脆弱 - 鲁棒双重音频水印[J]. 浙江大学学报: 工学版, 2009, 43(4): 722 - 726.

[12] 叶天语, 钮心忻, 杨义先. 多功能双水印算法[J]. 电子与信息学报, 2009, 31(3): 546 - 551.

(上接第 970 页)

完整性和身份真实性的 RFID 系统认证协议的安全需求。

5 结语

随着电子商务和物联网的发展,RFID 技术被广泛应用,人们越来越多地关注安全和隐私问题。现有的认证协议中,大多存在某些安全隐患或者不符合 EPC Gen2 标准的要求,无法成为实际可用的 RFID 系统安全机制。本文在对以往协议分析研究的基础上,总结以往协议存在漏洞的基本原因,提出新的认证协议,经安全性分析,新提出的协议符合 EPC Gen2 标准,并且能够满足 RFID 协议的各种安全需求。

参考文献:

[1] SARMA S E, WEIS S A, ENGELS D W. RFID systems and security and privacy implications[C]// Proceedings of CHES'02 Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems. London: Springer-Verlag, 2003: 454 - 469.

[2] SARMA S E, WEIS S A, ENGELS D W. Radio-frequency identification: Secure risks and challenges[J]. RSA Laboratories CryptoBytes, 2003, 6(1): 2 - 9.

[3] WEIS S A, SARMA S E, RIVEST R L. Security and privacy aspects of low-cost radio frequency identification systems[C]// Security in Pervasive Computing, LNCS 2802. Berlin: Springer-Verlag, 2004: 201 - 212.

[4] EPCglobal. The EPCglobal architecture framework[S/OL]. [2011 - 11 - 06]. http://www.epcglobalinc.org/standards/architecture/architecture_1_3-framework-20090319.pdf.

[5] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication [J]. ACM Transactions in Computer Systems, 1990, 9(1): 18 - 36.

[6] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR J E, *et al*. Weaknesses in two recent lightweight RFID authentication protocols[C]// Inscrypt'09: Proceedings of the 5th International Conference on Information Security and Cryptology. Berlin: Springer-Verlag, 2009: 383 - 392.

[7] CHEN C-L, DENG Y-Y. Conformation of EPC class 1 and generation 2 standards RFID system with mutual authentication and privacy protection[J]. Engineering Applications of Artificial Intelligence, 2009, 22(8): 1284 - 1291.

[8] BURMESTER M, de MEDEIROS B, MUNILLA J, *et al*. Secure EPC Gen2 compliant radio frequency identification[C]// ADHOC-NOW'09: Proceedings of the 8th International Conference on Ad-Hoc, Mobile and Wireless Networks. Berlin: Springer-Verlag, 2009: 227 - 240.

[9] PIRAMUTHU S. RFID mutual authentication protocols[J]. Decision Support Systems, 2011, 50(2): 387 - 393.

[10] 邓淼磊, 黄照鹤, 鲁志波. EPC Gen2 标准下安全的 RFID 认证协议[J]. 计算机科学, 2010, 37(7): 115 - 117.

[11] MITRA M. Privacy for RFID systems to prevent tracking and cloning [J]. International Journal of Computer Science and Network Security, 2008, 8(1): 1 - 5.