一种基于部分 ID 的新型 RFID 安全隐私相互认证协议

张 辉 侯朝焕 王东辉
(中国科学院声学研究所 北京 100190)

摘 要：在低成本电子标签中实现安全隐私功能是 RFID 研究领域需要解决的一项关键技术，该文采用部分 ID，CRC 校验以及 ID 动态更新的方法，提出一种新型 RFID 相互认证协议，该协议具有前向安全性，能够防止位置隐私攻击、重传攻击、窃听攻击和拒绝服务攻击，新协议有效地解决了 RFID 安全隐私问题，并且符合 EPC Class1 Gen2 标准，它的硬件复杂度较低，适用于低成本电子标签。

关键词：射频识别；安全；隐私；相互认证；部分 ID
中图分类号：TP391 **文献标识码**：A **文章编号**：1009-5896(2009)04-0853-04

A New Security and Privacy on RFID Mutual Authentication Protocol Based on Partial ID

Zhang Hui Hou Chao-huan Wang Dong-hui
(*Institute of Acoustics*, *Chinese Academy of Science*, *Beijing* 100190, *China*)

Abstract: The method of implementation of security and privacy in low cost tags is a key technique which needs to be solved in research field. Based on the use of partial ID, CRC checksum and dynamic update ID, this paper proposes a new RFID mutual authentication protocol which possesses forward security ability and can defeat location privacy attack, relay attack, eavesdropping attack and denial-of-service attack. The new scheme conforms to EPC Class1 Gen2 standards and effectively solves problems of RFID security and privacy with lower complexity of hardware, so it is useful for low cost RFID tags.

Key words: Radio Frequency IDentification (RFID); Security; Privacy; Mutual authentication; Partial ID

1 引言

在 20 世纪 60 年代，第一个电子物品监视反盗窃系统开始投入商业运营，今天无线射频识别技术(RFID)已被广泛应用在各种领域，从无钥匙的汽车开启、动物跟踪、高速公路收费到商业供应链的管理，随处可见 RFID 的身影[1]。随着 RFID 的大面积应用，安全与隐私方面暴露出的问题越发引起人们的关注，安全与隐私威胁主要表现在以下几个方面：数据安全威胁、个人隐私威胁和克隆威胁[2]。

数据安全威胁之一是可能出现竞争对手非法搜集企业的 RFID 数据，严重危及商业机密；威胁之二是 RFID 本身具有脆弱性，容易受到一系列安全攻击，如重写标签信息、欺骗攻击、窃听攻击和拒绝服务等。

对个人隐私的威胁：一方面，对标签信息未经授权的访问可能会泄露个人的私人信息；另一方面，RFID 的位置追踪能力，可能会危及到个人的“位置隐私”[2]。

2 RFID 安全隐私已有技术手段的简要介绍

RFID 目前在安全隐私方面存在的不足之处，在相当大程度上影响了它的推广和应用，例如美国德州等部分州政府已开始考虑制订限制电子标签使用的相关立法。一般来说，一个比较完善的 RFID 系统解决方案应当具备机密性、完整性、可用性、真实性和隐私性等基本特征。当前实现 RFID 安全机制所采用的方法大致分可为 3 种类型：基于物理方法、基于密码机制以及二者相结合的机制[3]。目前防止数据安全威胁的主要技术手段有：物理隔离、读取访问控制、主动干扰、kill 标签服务、双标签联合验证、智能标签、阻塞标签、Hash 加密、设置伪随机序列口令和重加密等[3−5]。近年来应用密码学方法解决 RFID 安全隐私问题日益受到人们的重视，迄今为止，已经有多种 RFID 安全协议被提出，如 Hash-Lock 协议、随机化 Hash-Lock 协议、Hash 链协议、基于杂凑的 ID 变化协议、David 的数字图书馆 RFID 协议、分布式 RFID 询问-响应认证协议、LCAP 协议和重加密机制等[3−5]。此外，还提出了基于 LPN 问题的 RFID 安全协议[5]：HB^{+}和 HB^{++}，虽然上述两种协议的复杂度较低，但 HB 类协议的安全模型受到限制，特别是在挑战矩阵完全随机的情况下，LPN 问题的困难性还没有被证明。近一段时期，在 RFID 安全领域取得的一个重要成果是：Dimitriou 提出的 RFID 安全协议[6]，该协议采用 Hash 技术，以标签的标识符(ID)作为共享秘密，只有在标签和阅读器完成相互认证后，

2007-12-07 收到，2008-04-28 改回
国家自然科学基金(60602055)资助课题

标签才改变它的计数器值和相应的输出值。该协议的缺点在于：存在数据库和标签更新不同步的问题，可能遭受拒绝服务攻击，此外，在同合法阅读器进行认证的期间，标签的输出值是静态的，在此期间易被跟踪，但从实际应用角度出发，对安全的影响不大[5]，但 Hash 硬件电路规模通常在 2~3 万门，不适于在低成本标签中采用。除以上方案外，Duc 等人使用随机数生成(PRNG)和循环冗余校验(CRC)方法，提出了一种低复杂度的安全协议[7]，但不能阻止拒绝服务攻击，不能检测非法标签，也不能提供前向安全功能。这里，具有前向安全功能，是指假设一个标签在某个阶段泄漏了标签信息，但该标签以前的通信信息仍然无法被跟踪。针对文献[7]的缺点，Chien 提出了改进协议[8]，但仍然会受到拒绝服务攻击[9]。解决 RFID 安全问题的另外一种途径是将标签的 ID 信息进行压缩。文献[10]采用标签部分 ID 的操作信息，提出一种新的安全协议，但由于 ID 直接参与运算，并且仅仅采用了简单的异或操作，安全方面还存在不足，此外，ID 标识也没有进行动态更新，可能遭受拒绝服务攻击，在安全和隐私方面还存在明显的缺陷。文献[11]采用部分 ID 和 Timestamp(时间标记)的方法，提出了一种新的解决途径，但采用 Timestamp 存在时钟同步问题，不适于多个阅读器的应用背景[6]。

综上所述，目前在电子标签领域还缺乏一个实用化、低成本的安全隐私协议，本文的研究目的就是解决该问题。

3 一种基于部分 ID 的新型 RFID 安全隐私认证协议

针对文献[8-11]的不足，本文采用部分 ID，CRC 校验以及 ID 动态更新的方法，提出了一种新型 RFID 相互认证协议，具体实施方案见图 1 所示。这是一种典型的询问-响应认证协议，该协议有效地解决了 RFID 的安全隐私问题，新协议符合 EPC Class1 Gen2 标准，并适用于低成本电子标签。由于采用 EPC Class1 Gen2 标准的标签计算资源非常有限，该标准只采用了硬件复杂度较低的 CRC 校验和 PRNG 函数，而加密函数和 Hash 函数在此类标签中难以实现，本文中符合 EPC Class1 Gen2 标准的安全协议，是泛指采用 CRC 校验，PRNG 函数和算术逻辑运算等简单操作类型的安全协议。

在本协议中，首先假设阅读器与后端数据库的通信是安全的，在有线连接的情况下，该假设条件通常是满足的。下面详细介绍文中提出的解决途径。

在初始化阶段，通过用户给标签编程，为每个标签分配各自的 ID 和 preID (预置 ID)， preID 相当于假名，与标签唯一对应。令 Index = CRC(preID)，通过查找 Index 值，能够快速找到标签对应的 ID 和 preID，减少了在后端数据库中的搜索时间， Index 类似一个数据指针，但又与指针不完全相同，因为本协议存在 ID 和 preID 的自动更新过程，

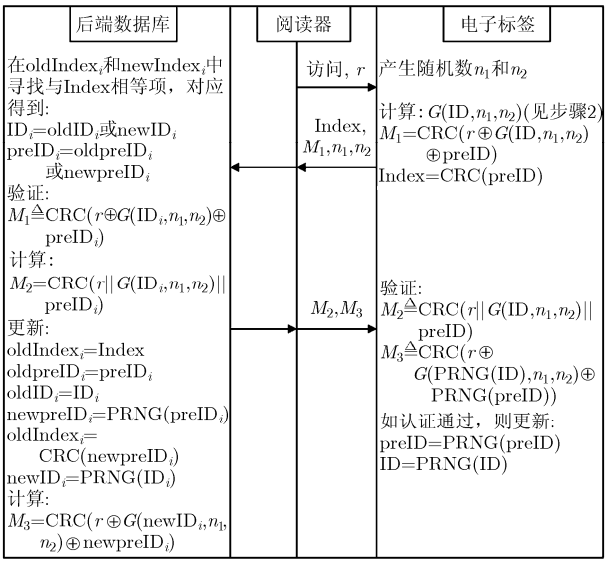

图 1 本文提出的 RFID 相互认证新协议

如果存在几十万个标签，在标签与阅读器进行多次相互认证和信息交换后，极少数标签的 Index 值在极端条件下可能会相等，这是由于 CRC 校验的内在特性决定的，即使 preID 不同，但经过 CRC 校验后，输出结果仍有可能相同。在这种特殊情况下，只要继续进行认证过程或重新开始新一轮认证过程就可解决该问题，这种特例情况在后面还会进一步解释，因此不能将 Index 完全当作指针对待。另外，为提高加密的安全性，CRC 校验本文采用 64 位或更高位数的校验函数。此外，在初始化阶段，为每一个标签在后端数据库存储一个数组 (oldIndex, oldpreID, oldID, newIndex, newpreID, newID)，在标签中存储一组数据(preID, ID)，为了防止在阻塞攻击下标签与数据库可能出现不同步的现象，在后端数据库中保留了认证通过前后的两组数据，其中 (oldIndex, oldpreID, oldID) 为标签上一组的 (Index, preID, ID)值，而(newIndex, newpreID, newID)为标签更新后的(Index, preID, ID)值。在首次执行安全协议时，每个电子标签在后端数据库的存储值对应为(Index, preID, ID, 0,0,0)，在随后协议的认证过程中(newIndex, newpreID, newID)值会被填充。

在图 1 中，符号≙表示“是否等于”的含义，‖为连接符号。本文提出的相互认证协议共包含 4 个步骤，具体认证过程如下：

步骤 1 阅读器产生随机数 r，并向该电子标签发出查询命令以及 r。

步骤 2 标签产生部分 ID，计算 M_1， Index，标签发送 Index， M_1， n_1 和 n_2 作为响应值。

(1)标签产生随机数 n_1 和 n_2，它们是下一阶段 RFID 相互认证协议中标签部分 ID 的随机长度，其中 $L/2 \le n_1 + n_2 \le 2L$， L 为标签 ID 的实际长度；

(2) 计算 $G(\mathrm{ID}, n_1, n_2) = \mathrm{PID}_{1L}(\mathrm{ID}, n_1) \oplus \mathrm{PID}_{2R}(\mathrm{ID}, n_2)$，其中 $\mathrm{PID}_{1L}(\mathrm{ID}, n_1)$ 表示在 ID 中选取从起始处到 n_1 位置的数

据，$\mathrm{PID}_{2R}(\mathrm{ID},n_2)$ 表示在 ID 中选取从 n_2 位置到结尾处的数据，$\oplus$ 为异或运算；

(3) 计算 $\mathrm{Index}=\mathrm{CRC}(\mathrm{preID})$，$M_1=\mathrm{CRC}(r\oplus G(\mathrm{ID},n_1,n_2)\oplus\mathrm{preID})$；

(4)标签向阅读器发送 Index，M_1，n_1 和 n_2 值，作为响应。

步骤 3　在数据库中寻找匹配标签，完成阅读器对该标签的认证。

(1)阅读器将 Index，M_1，n_1 和 n_2 发送给数据库；

(2)验证过程：

假设数据库中标签的数目为 N，后端数据库在 $\mathrm{oldIndex}_i$和$\mathrm{newIndex}_i$，$i=1,2,\cdots,N$ 中寻找与 Index 相等的所有项，然后对这些相等项进行查表，按照如下方式找到对应结果：

(a)如果数据库没有与 Index 相等项，则该标签是非法的，停止阅读器认证过程；

(b) 如果只有一个 $\mathrm{oldIndex}_i=\mathrm{Index}$，则 $\mathrm{preID}_i=\mathrm{oldpreID}_i$，$\mathrm{ID}_i=\mathrm{oldID}_i$；

(c) 如果只有一个 $\mathrm{newIndex}_i=\mathrm{Index}$，则 $\mathrm{preID}_i=\mathrm{newpreID}_i$，$\mathrm{ID}_i=\mathrm{newID}_i$；

(d)如果有两个或两个以上 $\mathrm{oldIndex}_i$ 或 $\mathrm{newIndex}_i$ 值与 Index 相等，假设有 X 组，类似地得到 X 组 $(\mathrm{preID}_i,\mathrm{ID}_i)$ 记录；

(e)将按照以上步骤得到的一组或 X 组 $(\mathrm{preID}_i,\mathrm{ID}_i)$ 进行如下验证：

(e_1) 如果没有记录满足 $M_1=\mathrm{CRC}(r\oplus G(\mathrm{ID}_i,n_1,n_2)\oplus\mathrm{preID}_i)$，则该标签是非法的，停止阅读器认证过程；

(e_2) 如果只有一组记录满足 $M_1=\mathrm{CRC}(r\oplus G(\mathrm{ID}_i,n_1,n_2)\oplus\mathrm{preID}_i)$，则该标签为合法标签，继续下一步(3)；

(e_3) 如果有两组或两组以上记录满足 $M_1=\mathrm{CRC}(r\oplus G(\mathrm{ID}_i,n_1,n_2)\oplus\mathrm{preID}_i)$，则返回步骤 1，重新开始认证过程，在新一轮认证过程中 r，n_1，n_2 均为随机数，再出现多组记录同时满足该条件的极端情况就会得到较好解决；

(3)计算 $M_2=\mathrm{CRC}(r||G(\mathrm{ID}_i,n_1,n_2)||\mathrm{preID}_i)$；

(4)更新数据库：

$\mathrm{oldIndex}_i=\mathrm{Index}$

$\mathrm{oldpreID}_i=\mathrm{preID}_i$

$\mathrm{oldID}_i=\mathrm{ID}_i$

$\mathrm{newpreID}_i=\mathrm{PRNG}(\mathrm{preID}_i)$

$\mathrm{newIndex}_i=\mathrm{CRC}(\mathrm{newpreID}_i)$

$\mathrm{newID}_i=\mathrm{PRNG}(\mathrm{ID}_i)$

其中 PRNG 为单向随机数发生器，具有不可逆性；

(5) 计算 $M_3=\mathrm{CRC}(r\oplus G(\mathrm{newID}_i,n_1,n_2)\oplus\mathrm{newpreID}_i)$；

(6)数据库将 M_2 和 M_3 发送给阅读器，由阅读器再发送给该标签。

步骤 4　标签对阅读器进行认证。

(1)验证过程：

如果同时满足下列条件：

$M_2=\mathrm{CRC}(r\,\|\,G(\mathrm{ID},n_1,n_2)\,\|\,\mathrm{preID})$

$M_3=\mathrm{CRC}(r\oplus G(\mathrm{PRNG}(\mathrm{ID}),n_1,n_2)\oplus\mathrm{PRNG}(\mathrm{preID}))$

则阅读器是合法的，阅读器通过安全认证，并继续下一阶段(2)；否则，阅读器是非法的，标签保留原来的 preID 和 ID 值，停止认证过程；

(2)如果阅读器通过安全认证，在标签中更新：

$\mathrm{preID}=\mathrm{PRNG}(\mathrm{preID})$

$\mathrm{ID}=\mathrm{PRNG}(\mathrm{ID})$

并在标签中删除旧的 preID，ID，n_1 和 n_2 值，这样可起到前向安全防护作用。

4　安全性分析

本文提出的协议是一种询问-响应认证协议，在标签与阅读器的相互认证中，双方都使用随机数，并且采用部分 ID 和 CRC 方法，在相互成功认证后，采用了单向随机数发生器自动更新数据库和标签的 ID 标识，因此即使当前标签的 ID 信息被泄漏出来，标签以前的通信信息仍然无法知道，使得该协议具有前向安全性。下面分析新协议对几种典型 RFID 攻击方式的防御能力。

(1)对位置隐私的攻击　隐私主要涉及的是标签位置信息和所有者信息的泄漏，当对手预先已经知道某一个标签的 ID 信息后，如果不采用 ID 动态更新措施，对于简单的异或和 CRC 运算，该标签的位置还是可以被估计出来。此外，如果采用固定 ID 标识，通过搜集处于不同固定位置的阅读器与标签的通信内容，假如标签中存在患者病理信息或者商品采购信息等，通过分析双方通信内容，标签的位置信息仍然会被跟踪，可见对于固定 ID 方式，不论采用何种高强度的加密措施，都会使标签暴露在位置隐私的攻击之下。在新协议的标签与阅读器相互认证过程中，每次发送和接收到的信息是不同的随机数，并且在标签与阅读器成功进行相互认证后，标签的 ID 就会自动更新，由于可被跟踪和固定的 ID 已不存在，因此位置隐私得到有效的保护。

(2)重传攻击(relay attack)　当对手扫描一个电子标签，并记录下该标签的响应数据，然后转播这个响应给合法的 RFID 阅读器，就会产生重传攻击，它是 RFID 面临的一个主要威胁。在本文提出的安全协议中，每次阅读器查询时采用不同的随机数 r，对手如果重放标签以前的响应数据，就会无法通过阅读器的认证，因此能够有效地防止重传攻击。

(3)窃听攻击　在标签和阅读器相互认证过程中，该协议的 ID 信息没有以显式格式发送，并且协议采用了 ID 自动更新以及 CRC 校验方法，对手很难解密出 ID 标识，因此就不会发生有用的信息被泄漏出来，窃听攻击就不会起到作用。

此外，如果将标签认证通过以后的具体通信内容进行加密，如与随机数进行异或运算等，就会更有效地防止泄密。

(4)拒绝服务攻击　本协议在后端数据库中保留了标签认证通过前后的两种数据，即 oldIndex，oldpreID，oldID，newIndex，newpreID 和 newID，如果攻击者阻塞住阅读器发送到标签的 M_2 和 M_3 信息，这时虽然会发生后端数据库信息已经更新，而标签信息仍没有更新的情况，但在下一次认证中，本协议使用 oldIndex，oldpreID 和 oldID 信息仍然能够完成对合法标签的认证，因而能够抵抗拒绝服务攻击。

(5)对标签发动攻击　当对手伪装成合法的阅读器对标签发出查询命令，这种攻击由于对手不知道标签的 ID 和 preID，非法阅读器发送到标签的 M_2 和 M_3 信息不正确，攻击就会被击败。

5 结束语

如何解决电子标签的安全隐私问题是 RFID 研究中的一个热点。本文采用部分 ID，动态 ID 更新以及 CRC 校验的途径，提出了一种新的 RFID 相互认证协议，该协议具有成本低、效率高、安全性和隐私性好等优点，并且可直接应用在 EPC 二代标准中，在工程实现上具有很强的实用性，在未来 RFID 市场中将具有一定的应用价值。但是，此方法还存在一些不足之处，如对手在解剖标签后再进行复制，然后用伪造的标签发动攻击，则该协议无法抵御这种攻击，这些尚需进一步研究改进。然而，这种攻击毕竟代价高昂，即使在此情况下，提出的协议仍具有前向安全性，标签以前交易的内容仍得到有效保护。相信随着这一领域研究的深入，将会产生更多实用、简捷的安全解决途径。

参 考 文 献

[1] Klaus F. RFID Handbook: Radio-Frequency Identification Fundamentals and Applications in Contactless Smart Cards and Identification[M]. Second Edition, West Sussex, England: John Wiley & Sons Ltd, 2003: 341–393.

[2] 广东电子工业研究院. RFID 研究动态. http://www. gdeii. com.cn /Technique/Technique7_content. jsp?id=38, 2005.

[3] 周永彬, 冯登国. RFID 安全协议的设计与分析[J]. 计算机学报, 2006, 29(4): 581–589.

[4] Garfinkel S L, Juels A, and Pappu R. RFID privacy: An overview of problems and proposed solutions[J]. *IEEE Security & Privacy Magazine*, 2005, 3(3): 34–44.

[5] Juels A. RFID security and privacy: A research survey[J]. *IEEE Journal on Selected Areas in Communications*, 2004, 24(2): 381–394.

[6] Dimitriou T. A lightweight RFID protocol to protect against traceability and cloning attacks[C]. First International Conference on Security and Privacy for Emerging Areas in Communications Networks, Athens, Greece, September 2005: 59–66.

[7] Duc D C, Park J, Lee H, and Kim K. Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning[C]. The 2006 Symposium on Cryptography and Information Security, Hiroshima, Japan, January 17-20, 2006: 269–277.

[8] Chien H Y and Chen C H. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards[J]. *Computer Standards & Interfaces*, 2006, 26(2): 254–259.

[9] 蔡庆玲, 詹宜巨, 史斌宁. 一种符合 EPC C1G2 标准的 RFID 随机化密钥双向认证协议[J]. 电信科学, 2007, 4: 70–74.

[10] Li Yong-Zhen, Jeong Yoon-Su, Sun Ning, and Lee Sang-Ho. Low-cost authentication protocol of the RFID system using partial ID[C]. Proceedings of 2006 International Conference on Computational Intelligence and Security. Guangzhou, China, November 3-6, 2006, 2: 1221–1224.

[11] Li Yong-Zhen, Cho Young-Bok, Um Nam-Kyoung, and Lee Sang-Ho. Security and privacy on authentication protocol for low-cost RFID[C]. Proceedings of 2006 International Conference on Computational Intelligence and Security. Guangzhou, China, November 3-6, 2006, 2: 1101–1104.

张　辉：男，1969 年生，博士后，研究方向为无线通信的安全协议以及 RFID 关键技术.

侯朝焕：男，1936 年生，研究员，中国科学院院士，研究方向为电路系统集成及水下制导系统.

王东辉：男，1973 年生，副研究员，研究方向为通信以及电路系统集成.