

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200610124662.5

[43] 公开日 2007 年 3 月 21 日

[51] Int. Cl.
G06K 7/00 (2006.01)
H04L 9/16 (2006.01)

[11] 公开号 CN 1932835A

[22] 申请日 2006.9.30

[21] 申请号 200610124662.5

[71] 申请人 华中科技大学

地址 430074 湖北省武汉市洪山区珞喻路
1037 号

[72] 发明人 邹雪城 刘冬生 刘政林 梁 浩

[74] 专利代理机构 华中科技大学专利中心

代理人 曹葆青

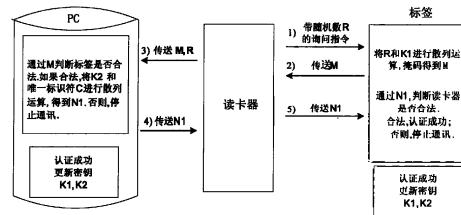
权利要求书 1 页 说明书 6 页 附图 2 页

[54] 发明名称

一种射频识别系统中的安全认证方法

[57] 摘要

本发明公开了一种射频识别系统中的安全认证方法，认证过程基于散列运算，并加入随机数掩码和密钥更新等方法。读卡器和电子标签双方均存有相同的密钥对 K1、K2。K1 和随机数 R 进行散列运算对电子标签进行认证，K2 和唯一标识符 C 进行散列运算对读卡器进行认证。本发明提供的安全认证方法对于射频识别系统中存在的几种安全和隐私问题的防护能够有效地解决，并能够满足电子标签芯片的低成本、低功耗的需求。本发明具有防止地点隐私泄露、防止标签信息被窃取、防止伪造标签和防止中间人攻击等特点，并且对于电子标签的低成本实现更具意义。



1、一种射频识别系统中的安全认证方法，其步骤包括：

(1) 读卡器向电子标签发送带伪随机数 R 的询问指令；

(2) 电子标签接收到询问指令后，从电子标签芯片内部 EEPROM 中读取密钥 k1，将密钥 k1 和伪随机数 R 进行散列运算，将加密后的结果 S1 与唯一标识符 C 用随机数 p 进行掩码，再将掩码得到的数据 M 传送给读卡器；

(3) 读卡器正确识别到上述掩码后的数据 M 后，将数据 M 和伪随机数 R 一起传送给终端；

(4) 终端对数据 M 和伪随机数 R 按下述步骤进行判断：

(4.1) 去掉数据 M 中的掩码，得到散列运算后的结果 S1 与唯一标识符 C；

(4.2) 根据唯一标识符 C 从终端的存储信息中获得对应的密钥 k1；

(4.3) 将密钥 k1 与伪随机数 R 按照步骤(2)中相同的算法进行散列运算，得到数据 S2；

(4.4) 将数据 S2 与 S1 进行比较，如果相等，则认为标签合法，否则认为标签是伪标签，终止通信；

(5) 如果标签为合法电子标签，终端从数据库中取出另一密钥 k2，将密钥 k2 与唯一标识符 C 进行散列运算，得到数据 N1，并发送给读卡器；

(6) 读卡器将数据 N1 传送给电子标签；

(7) 电子标签接收到数据 N1 后，从电子标签芯片内部 EEPROM 中读取另一密钥 k2，然后按照步骤(5)相同的算法将密钥 k2 与唯一标识符 C 进行散列运算，得到数据 N2；再比较数据 N1 与 N2，如果相等，则通过认证，交互认证完成；否则，认证失败，电子标签不对该读卡器的其他指令进行响应；

(8) 在完成认证后，读卡器和标签双方以相同的方式更新密钥 k1,k2。

2、根据权利要求 1 所述的方法，其特征在于：步骤(5)和步骤(2)采用相同的散列函数进行散列运算。

一种射频识别系统中的安全认证方法

技术领域

本发明属于射频识别技术领域，具体为一种射频识别系统中的安全认证方法，尤其适用于无源电子标签与读卡器之间的认证。

背景技术

射频识别（RFID）这一革命性的技术是 20 世纪 90 年代开始兴起的一种利用大规模集成电路与无线通信技术相结合的自动识别技术。但由于读卡器与 RFID 标签之间是无线通信，因此射频识别系统很容易受到攻击。在实际应用中，各应用领域已经对电子标签的应用安全提出了现实的需求。

在射频识别系统中，主要是针对信息安全和隐私防护两方面的考虑。由于标签携带有唯一标识符 UID，一旦被获得，也就获得了目标对象的数据信息。而且，攻击方也能根据这些特定的信息对特定目标进行地点跟踪。因此，射频识别系统中的安全认证显得意义重大。

目前，国际上还没有将具有交互（标签芯片和读写器及后端系统之间）安全认证协议用于 RFID 系统中。但相关的研究工作较多，主要是针对信息安全和隐私防护。S. Weis[见 S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in 1st Intern. Conference on Security in Pervasive Computing (SPC), 2003.]等提出了一种基于散列函数锁存的认证方法，在这个认证方法中，每个电子标签分配了不同的认证密钥 k，电子标签存储密钥 k 的 hash 值 mentalID ($mentalID = hash(k)$)。当读卡器询问电子标签时，电子标签将 mentalID 值发送给读写器，读卡器将 mentalID 值传给后端数据库，同时在后端的数据库中查找相应的认证密钥 k。数据库通过读写器将认证密钥 k 发送给电子标签，标签将得到的认证密钥 k 通过散列函数运算得到一个散列值，将该值与本身储存的 mentalID 值进行比较，如果两个值相等的话，电子标签将通过认证并向周围的阅读器提供

所有的存储信息。这是一种较直接和经济的方法，但是电子标签对读写器的响应的信息是可预测的，所以地点隐私被泄露。此外，认证密钥 k 和电子标签的存储信息容易被窃取。S. Weis 在这种锁存方法的基础上做了一些改进，改进后的方案虽然可以保护地点隐私，但是无法对抗中间人攻击。

Jeongkyu Yang[见 Jeongkyu Yang, Jaemin Park, Hyunrok Lee and Kui Ren, “Mutual Authentication Protocol for Low-cost RFID,” ECRYPT Workshop on RFID and Lightweight Crypto, Graz University of Technology, Austria, 2005]等在此基础上提出了一种交互认证的方案，此方案运用密钥对 (k_1, k_2) 来认证读卡器和电子标签，能较好的防止上述攻击，但是存在两个缺点；第一，在每次认证后，密钥 (k_1, k_2) 才会更新。在密钥更新之前，攻击方每次用相同的询问指令询问电子标签时，电子标签的响应是相同的。这样，地点隐私也会被泄露，第二，在这种认证方案中，数据库的计算量很大，不适合同时处理大量标签，例如共有 N 个标签的 ID，那么就需要进行 N 次搜索和 N 次散列 (hash) 函数计算。Tassos Dimitriou[见 Tassos Dimitriou, “A Lightweight RFID Protocol to protect against Traceability and Cloning attacks”, ECRYPT Workshop on RFID and Lightweight Crypto, Graz University of Technology, Austria, 2005]等给出一种防地点隐私和防伪造的安全认证机制，它的原理是在标签和后端数据库共享的秘密 ID 被不断刷新，不公布的秘密 ID 可以防伪造，秘密 ID 的刷新可以防跟踪。但是这种方案需要标签处理的信息很多，需要产生两个散列函数值发送给读写器，并在接收读写器的散列值的同时，产生相应的值进行比较，使得标签安全认证电路的实现成本较高。

国内相关的研究产品中，只有一些加密产品的推出，对于包含认证机制的系统推出，还没有相关报道。

发明内容

本发明的主要目的是实现一种射频识别系统中的安全认证方法，该方法可以保护地点隐私，防止标签信息被窃取，防止伪造标签的攻击以及防止中间人攻击。

本发明提供的一种射频识别系统中的安全认证方法，其步骤包括：

- (1) 读卡器向电子标签发送带伪随机数 R 的询问指令；
- (2) 电子标签接收到询问指令后，从电子标签芯片内部 EEPROM 中读取密钥 k1，将密钥 k1 和伪随机数 R 进行散列运算，将散列运算后的结果 S1 与唯一标识符 C 用随机数 p 进行掩码，再将掩码得到的数据 M 传送给读卡器；
- (3) 读卡器正确识别到上述掩码后的数据 M 后，将数据 M 和伪随机数 R 一起传送给终端；
- (4) 终端对数据 M 和伪随机数 R 按下述步骤进行判断：
 - (4.1) 去掉数据 M 中的掩码，得到散列运算后的结果 S1 与唯一标识符 C；
 - (4.2) 根据唯一标识符 C 从终端的存储信息中获得对应的密钥 k1；
 - (4.3) 将密钥 k1 与伪随机数 R 按照步骤(2)中相同的算法进行散列运算，得到数据 S2；
 - (4.4) 将数据 S2 与 S1 进行比较，如果相等，则认为标签合法，否则认为标签是伪标签，终止通信；
- (5) 如果标签为合法电子标签，终端从数据库中取出另一密钥 k2，将密钥 k2 与唯一标识符 C 进行散列运算，得到数据 N1，并发送给读卡器；
- (6) 读卡器将数据 N1 传送给电子标签；
- (7) 电子标签接收到数据 N1 后，从电子标签芯片内部 EEPROM 中读取另一密钥 k2，然后按照步骤(5)相同的算法将密钥 k2 与唯一标识符 C 进行散列运算，得到数据 N2；再比较数据 N1 与 N2，如果相等，则通过认证，交互认证完成；否则，认证失败，电子标签不对该读卡器的其他指令进行响应；
- (8) 在完成认证后，读卡器和标签双方以相同的方式更新密钥 k1, k2。

本发明在理论上是一种安全的认证方案，对于射频识别系统中存在的几种安全隐患和隐私问题都能较好的防护，而且实际中也已经成功实现，特别是针对采用无源标签的射频识别系统，这种认证方式优势更为明显。具体而言，本发明具有以下技术效果：

- (1) 防止地点隐私泄露：即防止攻击方根据标签上所携带的特定信息

而得到标签使用者的某些私人信息或者跟踪标签。即使攻击方每次带相同的 R 询问标签，由于步骤（2）中存在随机数掩码的过程，使标签每次的响应是不同的，能够保障地点隐私，防止跟踪；而且每次通过认证后， k_1 的更新也能防止地点隐私泄露。

（2）防止标签信息被窃取：即没有通过认证的读卡器（非法读卡器）是不能获得电子标签内部存储的有效信息的。

（3）防止伪造标签：即没有通过认证的电子标签（非法标签），读卡器是不会读取其内部存储的信息的。

（4）防止中间人攻击：即利用电子标签的认证信息来攻击读卡器或者利用读卡器的认证信息来攻击电子标签。由于每次交互认证完成后，读卡器和电子标签之间都会更新密钥，攻击方监听得到的认证信息不再有效。即使攻击方监听了多次认证过程，获得多组数据，但由于每次传送与密钥 k_1 , k_2 相关的信息时，都经过了散列运算，攻击方很难分析出 k_1 , k_2 。

（5）此安全认证方法的电路实现成本低、功耗小，能够满足标签芯片的低成本、低功耗的需求。

附图说明

图 1 为发明内容示意图。

图 2 为射频识别系统示意图。

图 3 为本发明实例的认证过程示意图。

具体实施方式

如图 2 所示，一个基本的射频识别系统由三部分组成：电子标签 102、读卡器 101 和天线 103、104。读卡器 101 和电子标签 102 之间通过天线 103、104 来传输信号，而读卡器 101 端，因为设计需要来决定是否与以数据处理终端 105 相连。电子标签 102 由耦合元件及芯片组成，每个标签具有唯一的电子编码，附着在物体上标识目标对象。读卡器 101 是读取（或写入）标签信息的设备，可设计为手持式或固定式。天线 103、104 是用来在标签和读卡器间传递射频信号。读卡器 101 可以被设计为手持式或固定式，其

中，手持式的读卡器应具有相应的存储功能和数据运算功能，以确保能顺利的完成认证功能，而固定式的读卡器则可与终端 PC 相连，存储功能和数据运算功能可由终端承担。电子标签也被设计成具有相应运算和控制功能。读卡器或者终端存有所有合法电子标签的唯一标识符 UID (C) 和相应的认证密钥 (k1,k2)。电子标签内部的存储器空间被划分为三部分，分别用来存储唯一标识符 UID (C)，认证密钥 (k1,k2) 和用户信息。

在认证过程中，伪标签攻击方因为不知道合法的 c 和 k1，计算不出正确的认证码，无法冒充成合法标签。对于标签的攻击，因为 k2 的存在，也可以避免。而且，标签每次的响应经过了随机数 P 的掩码以及 k1 的更新，地点隐私得到了较好的保护。同时，散列函数的使用，也使攻击方企图分析数据以获得密钥变成不可能。

下面举例对本发明方法作进一步详细的说明。

实例：

结合图 3 来说明本认证方式的具体实施方式：手持式设备中读卡器具备存储功能和数据运算功能，而固定式设备可将读卡器 101 与终端 PC105 相连。在本例中，读卡器设定为固定式设备，认证过程如下：

(1)首先，读卡器发送带伪随机数 R 的询问指令。

(2)电子标签接收到询问指令后，从标签芯片内部 EEPROM 中读取密钥 k1，进行运算 $S1 = \text{hash}(R, k1)$ ，并返回 $M = f(s1 \| c, p)$ 。其中 $f = (x, p)$ 表示将 x 用随机数 p 进行掩码，符号 “ $\|$ ” 表示位串。

(3)读卡器通过防冲突机制正确识别到电子标签响应的信息 M 后，将 M 和随机数 R 一起传送给终端 PC。

(4)终端对响应 M 进行判断，即认证电子标签。认证过程为：首先运行 $f^{-1}(s1 \| c, p)$ ，得到响应电子标签的 UID 信息 C，然后根据 C 从存储的信息中取得相应的 k1，计算 $S2 = \text{hash}(R, k1)$ ，判断 S2 是否等于 S1。不等，则认为标签是伪标签，终止通信；相等，则认为标签合法，继续下一步操作。

(5)如果电子标签为合法电子标签，终端从数据库取出另一密钥 k2，运算 $N1 = \text{hash}(k2, c)$ ，并发送给读卡器。

(6)读卡器将 N1 传送给电子标签。

(7)电子标签正确接收到 N1 后，从电子标签芯片内部 EEPROM 中读取另一密钥 k2，然后进行运算 $N2 = \text{hash}(k2, c)$ ，再比较 N2 与 N1。相等，则通过认证，此时，交互认证完成，读卡器可以对电子标签进行一系列需要的操作。不等，则认证失败，电子标签不会对读卡器的其他指令进行响应。

(8)在完成认证后，读卡器和标签双方以相同的方式更新密钥 k1,k2。

本实例步骤(2)和步骤(5)均采用相同的散列函数如安全 hash 算法 (SHA) 或者 hash 算法 MD5 等进行散列运算，这样对于标签的低成本实现更具意义。

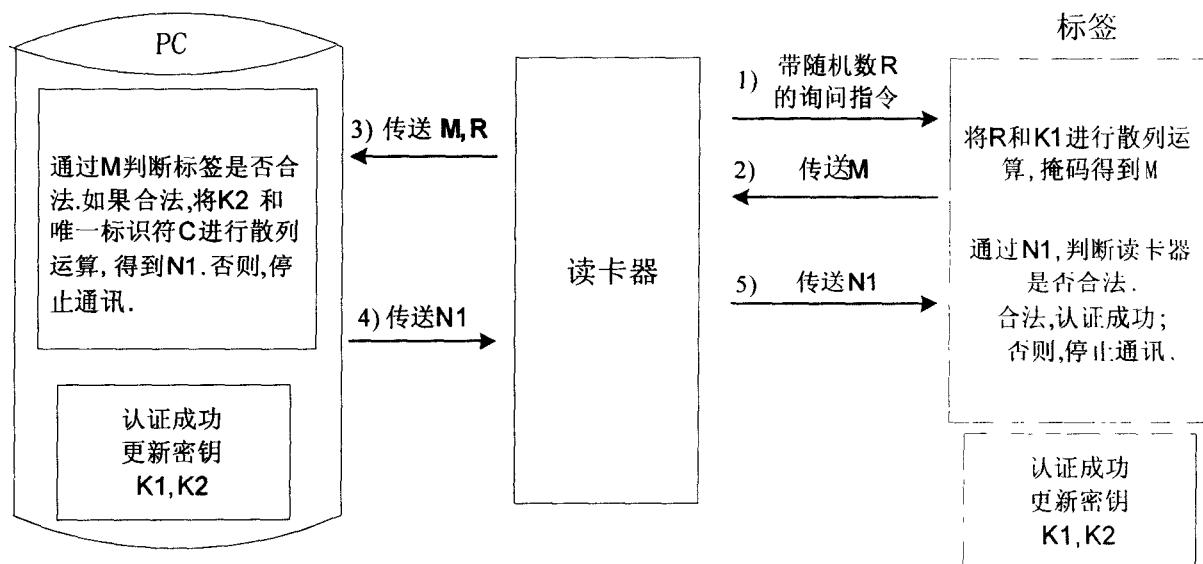


图 1

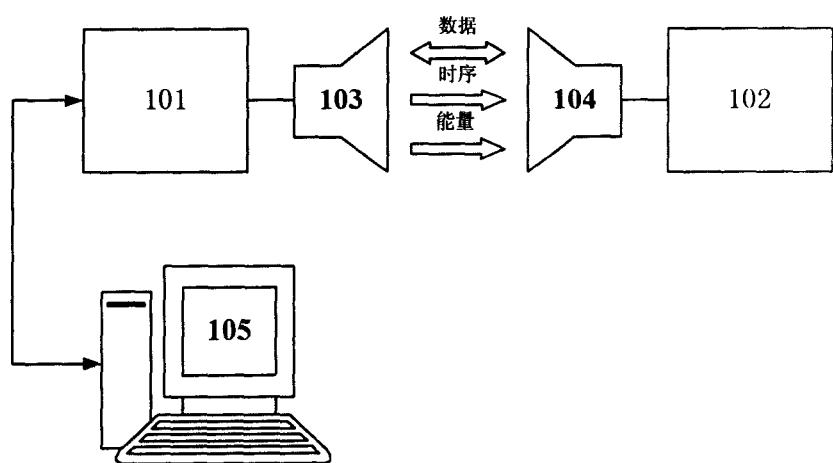


图 2

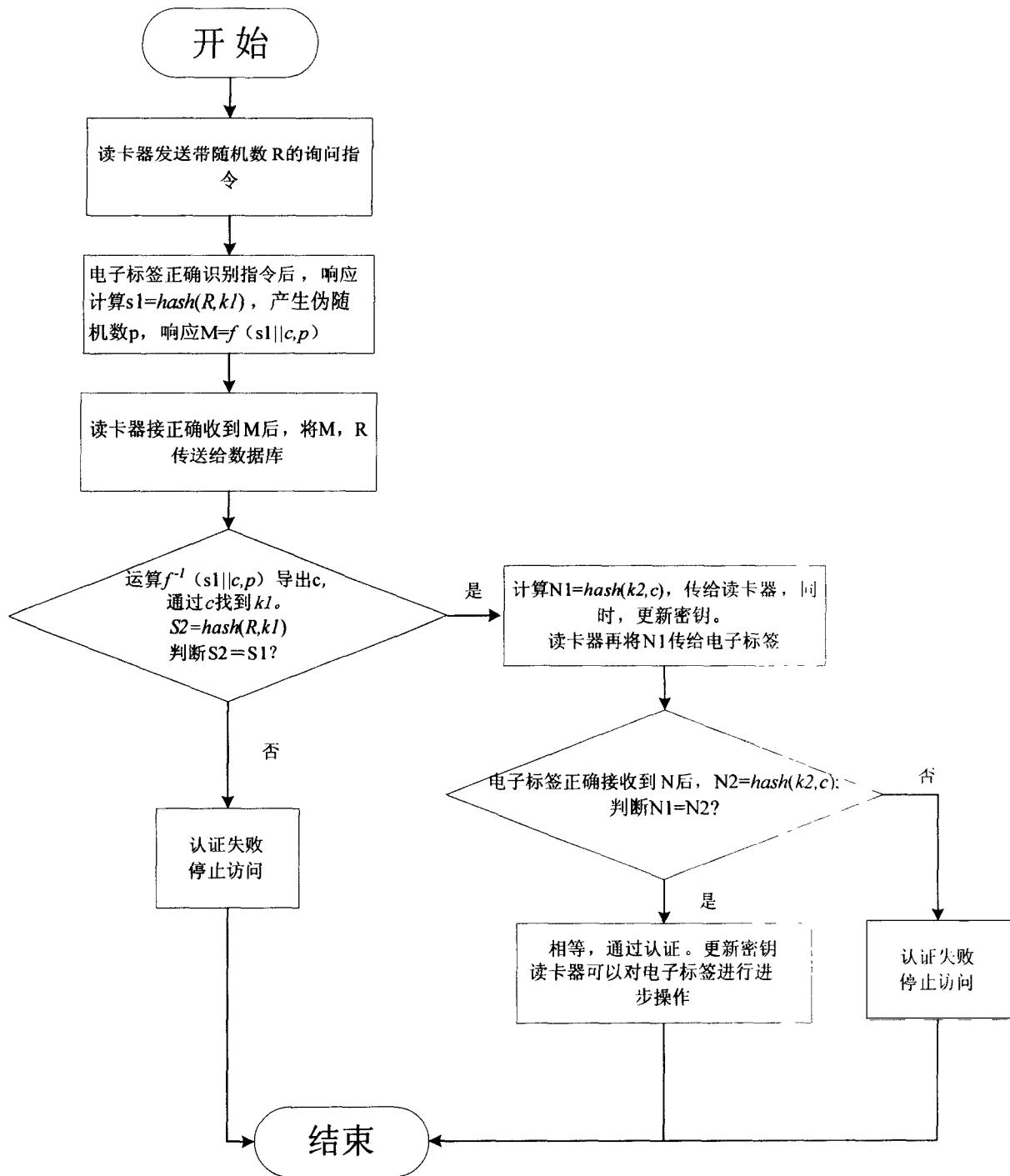


图 3