(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101488854 B
(45)授权公告日 2011.11.09

(21)申请号 200810001408.5

(22)申请日 2008.01.18

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 张向东 刘培 张振宇

(74)专利代理机构 北京挺立专利事务所 11265
代理人 皋吉甫

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/18(2006.01)
H04L 9/08(2006.01)
G06K 7/00(2006.01)
G06K 9/00(2006.01)

(56)对比文件
CN 1588386 A,2005.03.02, 全文.
WO 2006019854 A1,2006.02.23, 全文.
CN 101053199 A,2007.10.10, 全文.
WO 2006015617 A1,2006.02.16, 全文.
CN 1897016 A,2007.01.17, 全文.

审查员 沈敏洁

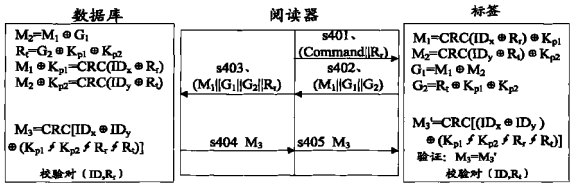
权利要求书 5 页 说明书 10 页 附图 3 页

(54)发明名称

一种无线射频识别系统认证方法和设备

(57)摘要

本发明的实施例公开了一种无线射频识别RFID中的认证方法，用于标签、阅读器、数据库之间的双向认证。本发明的实施例还公开了一种用于RFID中认证的系统和设备。通过使用本发明实施例提供的方法和设备，在标签ID的传递方式上将ID进行分割，并分别进行加密和传输，这种方式使ID信息不以明文的形式传输。以匿名的方式，把信息通过标签传给阅读器，保护了标签ID的信息。另外，本发明的实施例还提出了一种标签询问式的通信方式，通过在网络侧增加存储临时密钥、以及数据库在更新密钥前向标签发送更新密钥请求以确认是否更新密钥的方法，提高了标签与网络侧之间密钥更新同步的可靠性。



CN 101488854 B

1. 一种无线射频识别 RFID 中的认证方法，其特征在于，包括以下步骤：

将标签的标识 ID 的至少两个部分分别加密后作为加密内容向阅读器发送；

接收所述阅读器根据所述加密内容对标签认证通过时发送的认证消息，利用所述标签的标识 ID 的至少两个部分对所述认证消息进行认证；

所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；

所述将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理。

2. 如权利要求 1 所述 RFID 中的认证方法，其特征在于，所述随机数包括标签产生的随机数或从所述阅读器接收的随机数。

3. 如权利要求 1 所述 RFID 中的认证方法，其特征在于，接收所述阅读器发送的认证消息，利用所述分割而成的部分认证所述认证消息具体为：

利用与所述阅读器共享的密钥、所述至少一个随机数、所述分割而成的部分中的一个或多个生成认证信息，将所述生成的认证信息与从阅读器发送的认证信息进行比较，比较结果为相同时，对所述阅读器发送的认证消息的认证通过。

4. 如权利要求 1 所述 RFID 中的认证方法，其特征在于，利用所述分割而成的部分认证所述认证消息后，还包括：

对所述认证消息的认证成功时，根据所述认证消息中携带的内容，按照预设的规则更新与所述阅读器共享的密钥。

5. 如权利要求 1 所述 RFID 中的认证方法，其特征在于，接收到的所述阅读器发送的认证消息中包括更新询问请求时，利用所述分割而成的部分认证所述认证消息后，还包括：

对所述认证消息的认证成功时，根据所述认证消息中携带的内容，按照预设的规则更新与所述阅读器共享的密钥，并向所述阅读器发送更新响应。

6. 一种 RFID 中的认证方法，其特征在于，包括以下步骤：

阅读器接收标签发送的内容，所述内容中包括所述标签对其标识 ID 分割成至少两个部分后分别进行的加密；

所述阅读器将所述标签发送的内容向数据库转发；

所述阅读器接收所述数据库发送的认证消息，并转发给所述标签；

所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；

将所述标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理。

7. 如权利要求 6 所述 RFID 中的认证方法，其特征在于，所述将所述标签发送的内容向数据库转发时，同时将认证所述标签发送的内容所需的随机数向所述数据库发送。

8. 如权利要求 6 所述 RFID 中的认证方法，其特征在于，所述阅读器接收并转发给所述标签所述数据库发送的认证消息中，包括更新询问请求。

9. 一种 RFID 中的认证方法，其特征在于，包括以下步骤：

数据库接收阅读器转发的由标签发送的内容，所述内容中包括所述标签对其标识 ID 中至少两个部分分别进行的加密后得到的加密内容；

所述数据库对所述标签发送的加密内容进行认证；

所述认证通过时，所述数据库通过所述阅读器向所述标签发送认证消息，用于所述标签对所述阅读器的认证；

所述标签的标识ID的至少两个部分具体为：将标签的标识ID按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；

将所述标签的标识ID的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识ID的至少两个部分分别进行加密处理。

10. 如权利要求9所述RFID中的认证方法，其特征在于，所述对标签发送的加密内容进行认证具体为：

根据所述标签发送的内容、从所述阅读器获取的认证所述内容所需的随机数、以及本地存储的所有标签的标识ID，生成认证信息并与所述标签发送的加密内容进行比较；

生成的认证信息中存在与所述标签发送的加密内容相同的信息时，对所述内容进行认证。

11. 如权利要求9或10所述RFID中的认证方法，其特征在于，所述认证通过时，所述数据库通过所述阅读器向所述标签发送认证消息具体为：

根据所述阅读器与所述标签共享的密钥、至少一个随机数、所述分割而成的部分中的一个或多个，按照预定的规则生成认证消息并向所述标签发送。

12. 如权利要求9所述RFID中的认证方法，其特征在于，所述数据库对所述标签发送的内容进行认证后，还包括：

所述认证通过时，所述数据库更新所述阅读器与所述标签共享的密钥。

13. 如权利要求9所述RFID中的认证方法，其特征在于，所述认证通过时，所述数据库通过所述阅读器向所述标签发送的认证消息中，包括更新询问请求；

所述数据库接收到所述阅读器转发的标签的更新响应时，更新所述阅读器与所述标签共享的密钥。

14. 如权利要求9所述RFID中的认证方法，其特征在于，所述阅读器上存储有标签的共享密钥，以及与所述共享密钥对应的临时密钥，

所述数据库对所述标签发送的加密内容进行认证的步骤具体为：

所述临时密钥为空时，根据所述标签发送的内容、从所述阅读器获取的验证所述内容所需的随机数、本地存储的所有标签的标识ID以及共享密钥，生成认证信息并与所述标签发送的加密内容进行比较；

生成的认证信息中存在与所述标签发送的加密内容相同的信息时，对所述标签发送的加密内容进行的认证通过。

15. 如权利要求9所述RFID中的认证方法，其特征在于，所述阅读器上存储有标签的共享密钥，以及与所述共享密钥对应的临时密钥，

所述数据库对所述标签发送的加密内容进行认证的步骤具体为：

所述临时密钥为非空时，根据所述标签发送的内容、从所述阅读器获取 的验证所述内容所需的随机数、本地存储的所有标签的标识ID以及共享密钥，生成认证信息并与所述标签发送的加密内容进行比较；

生成的认证信息中存在与所述标签发送的加密内容相同的信息时，对所述标签发送的

加密内容进行的认证通过，并将所述临时密钥置为空；否则根据所述标签发送的内容、从所述阅读器获取的验证所述内容所需的随机数、本地存储的所有标签的标识 ID 以及临时密钥，生成认证信息并与所述标签发送的加密内容进行比较；

生成的认证信息中存在与所述标签发送的加密内容相同的信息时，对所述标签发送的加密内容进行的认证通过，并使用所述临时密钥替换所述共享密钥后，将所述临时密钥置空。

16. 如权利要求 14 或 15 所述 RFID 中的认证方法，其特征在于，所述数据库对所述标签发送的内容进行认证后，还包括：

所述认证通过时，所述数据库更新所述阅读器与所述标签共享的密钥，并将更新后的密钥存储在所述临时密钥中；

所述数据库接收到所述阅读器转发的标签的更新响应时，使用所述临时密钥替换所述共享密钥，并将所述临时密钥置空；否则保留所述临时密钥和共享密钥。

17. 一种 RFID 中的认证方法，其特征在于，包括以下步骤：

阅读器侧接收标签发送的内容，所述内容中包括所述标签对其标识 ID 中至少两个部分分别进行的加密后得到的加密内容；

阅读器侧对所述标签发送的加密内容进行认证；

所述认证通过时，所述阅读器侧向所述标签发送认证消息，用于所述标签对所述阅读器侧的认证；

所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；

所述将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理。

18. 一种标签，用于 RFID 系统中的认证，其特征在于，包括：

标识分割单元，用于将标签的标识 ID 分割成至少两个部分用于生成加密内容；所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理；

标识加密单元，用于将所述标识分割单元分割后的部分分别加密后作为加密内容，并向所述阅读器发送；

认证消息验证单元，用于接收所述阅读器根据所述加密内容对标签认证通过时发送的认证消息，利用所述标识分割单元得到的标签的标识 ID 的至少两个部分对所述认证消息进行认证。

19. 如权利要求 18 所述标签，其特征在于，所述标识加密单元具体包括：

共享密钥获取子单元，用于获取与所述阅读器共享的密钥；

随机数获取子单元，用于获取标签产生的随机数、和 / 或从所述阅读器接收的随机数用于加密；

加密子单元，用于利用所述共享密钥获取子单元获取的密钥、和 / 或所述随机数获取子单元获取的随机数，对所述标识分割单元分割后的部分分别进行加密处理。

20. 如权利要求 18 所述标签，其特征在于，所述认证消息验证单元具体包括：

共享密钥获取子单元，用于获取与所述阅读器共享的密钥；

随机数获取子单元，用于获取标签产生的随机数、和 / 或从所述阅读器接收的随机数用于对所述阅读器发送的认证消息进行认证；

验证子单元，用于利用所述共享密钥获取子单元获取的密钥、所述随机数获取子单元获取的随机数、所述标识分割单元分割后的部分中的一种或多种，对所述阅读器发送的认证消息进行认证。

21. 如权利要求 18 所述标签，其特征在于，还包括：

密钥更新单元，用于当所述认证消息验证单元对所述认证消息的认证成 功时，根据所述认证消息中携带的内容更新与所述阅读器共享的密钥。

22. 如权利要求 21 所述标签，其特征在于，还包括：

更新请求接收单元，用于接收所述阅读器发送的认证消息中包括的更新询问请求；

更新响应发送单元，用于当所述认证消息验证单元对所述认证消息的认证成功时，根据所述阅读器发送的更新询问请求向所述阅读器发送更新响应。

23. 一种阅读器，用于 RFID 系统中的认证，其特征在于，包括：

第一转发单元，用于接收标签发送的内容，所述内容中包括所述标签对其标识 ID 中至少两个部分分别进行的加密后得到的加密内容；所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；所述将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理；并将所述标签发送的内容向数据库转发；

第二转发单元，用于接收所述数据库发送的认证消息，并转发给所述标签。

24. 如权利要求 23 所述阅读器，其特征在于，还包括：

随机数生成单元，用于当所述将所述标签发送的内容向数据库转发时，同时将验证所述标签发送的内容所需的随机数向所述数据库发送。

25. 一种数据库，用于 RFID 系统中的认证，其特征在于，包括：

接收单元，用于接收阅读器转发的由标签发送的内容，所述内容中包括所述标签对其标识 ID 中至少两个部分分别进行的加密后得到的加密内容；标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理；

验证单元，用于对所述接收单元接收的标签发送的加密内容进行验证；

认证消息发送单元，用于当所述验证单元验证通过时，通过所述阅读器 向所述标签发送认证消息，用于所述标签对所述阅读器的认证。

26. 如权利要求 25 所述数据库，其特征在于，所述验证单元进一步包括：

随机数获取子单元，用于获取验证所述内容所需的随机数；

标签标识获取子单元，用于获取本地存储的所有标签的标识 ID；

验证子单元，用于根据所述随机数获取子单元获取的随机数、以及所述标签标识获取子单元获取的本地存储的所有标签的 ID，对所述标签发送的内容进行验证。

27. 如权利要求 25 所述数据库，其特征在于，所述认证消息发送单元进一步包括：

共享密钥获取子单元，用于获取所述阅读器与所述标签共享的密钥；

随机数获取子单元，用于获取生成认证消息所需的随机数；

认证消息生成子单元，用于利用所述共享密钥获取子单元获取的密钥、所述随机数获取子单元获取的随机数、所述分割后的部分中的一种或多种，生成认证消息并向所述标签发送。

28. 如权利要求 25 所述数据库，其特征在于，还包括：

密钥更新单元，用于当所述验证单元对所述认证消息的认证成功时，更新所述阅读器与所述标签共享的密钥。

29. 如权利要求 28 所述数据库，其特征在于，还包括：

更新请求发送单元，用于所述验证单元的验证通过时，在向所述标签发送的认证消息中携带更新询问请求；

更新响应接收单元，用于接收到所述阅读器转发的标签的更新响应时，通知所述密钥更新单元更新所述阅读器与所述标签共享的密钥。

一种无线射频识别系统认证方法和设备

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种RFID(Radio Frequency Identification,无线射频识别）中的认证方法和设备。

背景技术

[0002] RFID技术是从上世纪六、七十年代兴起的一项非接触式自动识别技术。由于RFID技术具有多目标识别和非接触识别等特点，目前已广泛应用于制造业、商业、军事、日常生活等领域，并显示出巨大的发展潜力与应用空间，被认为是21世纪最有发展前途的技术之一。

[0003] RFID系统的结构如图1所示，一般由三大部分构成：标签、阅读器以及数据库。

[0004] RFID系统中，数据库可以是运行于任意硬件平台的数据库系统，可由用户根据实际需要自行选择，通常假设其计算和存储能力强大，它保存所有标签的信息。阅读器实际是一个带有天线的无线发射与接收设备，它的处理能力强，存储空间比较大。标签是带有天线的微型电路，通常没有微处理器，仅由数千个逻辑门电路组成。

[0005] 虽然RFID技术有着广泛的应用前景，但是RFID通信系统缺乏有效的安全机制，已经成为制约其大规模部署和运用的重要因素。RFID系统中最主要的安全问题是保密性。没有安全机制的标签会向邻近的阅读器泄漏标签内容和敏感信息。一旦攻击者获得标签标识(ID)，也就获得了目标对象的数据信息。由于缺乏有效的安全保护机制，在RFID系统应用过程中，攻击者可以监听数据通信、交易分析，实施业务欺骗或业务抵赖。如果没有有效的访问控制机制，未授权的阅读器可以随时访问附近的标签从而获得机密数据；黑客可以使用软/硬件等手段读取、篡改甚至删除标签上的信息等。

[0006] RFID系统中另一个安全问题是可跟踪性。在物流领域，不仅要防止商业 间谍窃取标签内货物的信息，也要防止他们通过跟踪标签来获得货物的流向和通过对标签进行计数来估计货物的数量。

[0007] 通常情况，假设阅读器和数据库之间的通信信道是安全的，而阅读器与标签之间的通信信道是不安全的。由于无线射频识别系统的阅读器与标签之间是无线通信，系统没有点对点的安全信道，而且标签的低成本要求和标签的计算能力及存储空间有限，使得现有成熟的加密机制无法使用，所以RFID系统的安全防护能力极其薄弱。如何在标签计算速度、通信能力和存储空间非常有限的情况下，设计较好的安全机制，提供安全性和隐私性保护，防止各种恶意攻击，为RFID系统创造一个相对安全的工作环境，关系到RFID系统能否真正走向实用。

[0008] 现有技术中提出了一种RFID系统中的认证方案，为基于随机化Hash-Lock协议的方法。其原理如图2所示，其中，ID_k为标签的标识符；Getall ID_S为阅读器向数据库提出获得所有标签标识符的请求；

[0009] 随机化Hash-Lock协议的执行过程如下：

[0010] 步骤s201、阅读器向标签发送Query认证请求；

[0011] 步骤 s202、标签生成一个随机数 R，计算 $H(ID_k \| R)$。其中 H( ) 为 HASH 函数。标签将 $(R, H(ID_k \| R))$ 发送给阅读器；

[0012] 步骤 s203、阅读器向数据库发出获取所有标签标识符的请求；

[0013] 步骤 s204、数据库将自己数据库中的所有标签标识符 (ID1，ID2，...，IDs) 发送给阅读器；

[0014] 步骤 s205、阅读器检查是否有某个 ID_j，使得 $H(ID_j \| R) = (ID_k \| R)$ 成立；如果有，则认证通过，并将 ID_j 发送给标签；

[0015] 标签验证 ID_j 与 ID_k 是否相同，如相同，则认证通过，如不同，则停止认证。

[0016] 发明人在实现本发明的过程中，发现现有的随机化 Hash-Lock 协议技术至少存在以下缺点：

[0017] (1) 明文传输，泄漏 ID

[0018] 在随机化 Hash-Lock 协议中，认证通过后的标签标识符 ID_k 仍以明文的形 式通过不安全信道传送，因此攻击者可以对标签进行有效的追踪。同时，一旦获得了标签的标识符 ID_k，攻击者就可以对标签进行假冒。因此该协议也无法抵抗重传攻击。

[0019] (2) 标签计算负荷过大

[0020] 标签是一个带有天线的无线发射与接收设备，标签通常没有微处理器，仅由数千个逻辑门电路组成。它的处理能力、存储空间都比较小，致使现有成熟的加密机制无法使用。所以随机化 Hash-Lock 协议中的 Hash 函数是很难在标签中实现的。

[0021] 现有技术中还提出另一种 RFID 系统中的认证方法，为基于杂凑的 ID 变化协议的方法。

[0022] 在基于杂凑的 ID 变化协议中，系统使用了一个随机数 R 对标签标识符不断进行动态刷新，同时还对 TID（最后一次回话号）和 LST（最后一次成功的回话号）信息进行更新。因此每一次回话中的 ID 交换信息都不相同，可以抗重传攻击，其协议流程如图 3 所示，包括如下步骤：

[0023] 步骤 s301、阅读器向标签发送 Query 认证请求；

[0024] 步骤 s302、标签将当前回话号加 1，并将 H(ID)，H(TID*ID)，ΔTID 发送给阅读器；其中，H(ID) 可以使得数据库恢复出标签的标识符，ΔTID 则可以使得数据库计算出 TID（最后一次回话号），进而计算出 H(TID*ID)；

[0025] 步骤 s303、阅读器将 H(ID)，H(TID*ID)，ΔTID 转发给数据库；

[0026] 步骤 s304、依据所存储的标签信息，数据库检查接收到数据的有效性。如果所有数据全部有效，则产生一个随机数 R，并将 (R，H(R*TID*ID)) 发送给阅读器。然后，数据库更新该标签 ID 为 $ID \oplus R$，并相应地更新 TID 和 LST。

[0027] 步骤 s305、阅读器将 R，H(R*TID*ID) 转发给标签；标签验证所接收的信息的有效性；如果有效，则认证通过，使用认证过程中的 TID 更新本地的 LST。

[0028] 发明人在实现本发明的过程中，发现现有的基于杂凑的 ID 变化协议技术方案存在以下缺点：

[0029] (1) 数据不同步问题

[0030] 由上述可知，标签是在接收到 s305 中的消息且验证通过之后才更新其 ID 和 LST 信息的，而在此之前，数据库已经成功地完成相关信息的更新。因此，如果此时攻击者进行

攻击（例如，攻击者可以伪造一个假消息，或者干脆实施干扰使标签无法接收到该消息），则就会在数据库和标签之间出现数据不同步问题。这就意味着合法的标签在以后的回话中将无法通过认证。也就是说，存在数据库同步的潜在安全隐患。

[0031] (2) 标签计算负荷过大

[0032] 与随机化 Hash-Lock 协议技术方案中存在的问题相同，由标签的处理能力有限造成，在这里不再赘述。

[0033] 发明内容

[0034] 本发明的实施例提供一种 RFID 系统中的认证方法和设备，用于完善现有技术中 RFID 系统中的认证方法，进一步提高 RFID 系统的安全性能。

[0035] 为达到上述目的，本发明的实施例提供一种无线射频识别 RFID 中的认证方法，包括以下步骤：

[0036] 将标签的标识 ID 的至少两个部分分别加密后作为加密内容向阅读器发送；

[0037] 接收所述阅读器根据所述加密内容对标签认证通过时发送的认证消息，利用所述标签的标识 ID 的至少两个部分对所述认证消息进行认证；

[0038] 所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；

[0039] 所述将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理。

[0040] 本发明的实施例还提供一种 RFID 中的认证方法，包括以下步骤：

[0041] 阅读器接收标签发送的内容，所述内容中包括所述标签对其标识 ID 分割成至少两个部分后分别进行的加密；

[0042] 所述阅读器将所述标签发送的内容向数据库转发；

[0043] 所述阅读器接收所述数据库发送的认证消息，并转发给所述标签；

[0044] 所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；

[0045] 所述将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理。

[0046] 本发明的实施例还提供一种 RFID 中的认证方法，包括以下步骤：

[0047] 数据库接收阅读器转发的由标签发送的内容，所述内容中包括所述标签对其标识 ID 中至少两个部分分别进行的加密后得到的加密内容；

[0048] 所述数据库对所述标签发送的加密内容进行认证；

[0049] 所述验证通过时，所述数据库通过所述阅读器向所述标签发送认证消息，用于所述标签对所述阅读器的认证；

[0050] 所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；

[0051] 所述将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处

理。

[0052] 本发明的实施例还提供一种 RFID 中的认证方法，包括以下步骤：

[0053] 阅读器侧接收标签发送的内容，所述内容中包括所述标签对其标识 ID 中至少两个部分分别进行的加密后得到的加密内容；

[0054] 阅读器侧对所述标签发送的加密内容进行认证；

[0055] 所述验证通过时，所述阅读器侧向所述标签发送认证消息，用于所述标签对所述阅读器侧的认证；

[0056] 所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；

[0057] 所述将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理。

[0058] 本发明的实施例还提供一种标签，用于 RFID 系统中的认证，包括：

[0059] 标识分割单元，用于将标签的标识 ID 分割成至少两个部分用于生成加密内容；所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理；

[0060] 标识加密单元，用于将所述标识分割单元分割后的部分分别加密后作为加密内容，并向所述阅读器发送；

[0061] 认证消息验证单元，用于接收所述阅读器根据所述加密内容对标签认证通过时发送的认证消息，利用所述标识分割单元得到的标签的标识 ID 的至少两个部分对所述认证消息进行认证。

[0062] 本发明的实施例还提供一种阅读器，用于 RFID 系统中的认证，包括：

[0063] 第一转发单元，用于接收标签发送的内容，所述内容中包括所述标签对其标识 ID 中至少两个部分分别进行的加密后得到的加密内容；并将所述标签发送的内容向数据库转发；所述标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；所述将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理；

[0064] 第二转发单元，用于接收所述数据库发送的认证消息，并转发给所述标签。

[0065] 本发明的实施例还提供一种数据库，用于 RFID 系统中的认证，包括：

[0066] 接收单元，用于接收阅读器转发的由标签发送的内容，所述内容中包括所述标签对其标识 ID 中至少两个部分分别进行的加密后得到的加密内容；标签的标识 ID 的至少两个部分具体为：将标签的标识 ID 按照高位到低位、或低位到高位的顺序分割而成的至少两个部分；将标签的标识 ID 的至少两个部分分别加密的步骤具体为：利用与所述阅读器共享的密钥或至少一个随机数，对所述标签的标识 ID 的至少两个部分分别进行加密处理；

[0067] 验证单元，用于对所述接收单元接收的标签发送的加密内容进行验证；

[0068] 认证消息发送单元，用于当所述验证单元验证通过时，通过所述阅读器向所述标

签发送认证消息，用于所述标签对所述阅读器的认证。

[0069] 与现有技术相比，本发明的实施例具有以下优点：

[0070] 本发明的实施例在标签的标识 ID 的传递方式上将 ID 进行分割，并分别进行加密和传输，这种方式使 ID 信息不以明文的形式传输。以匿名的方式，把信息通过标签传给阅读器，保护了标签的标识 ID 的信息。

附图说明

[0071] 图 1 是现有技术中 RFID 系统组成示意图；

[0072] 图 2 是现有技术中随机化 Hash-Lock 协议流程图；

[0073] 图 3 是现有技术中基于杂凑的 ID 变化协议流程图；

[0074] 图 4 是本发明的实施例一中 RFID 系统中的认证方法流程图；

[0075] 图 5 是本发明的实施例二中 RFID 系统中的认证方法流程图；

[0076] 图 6 是本发明的实施例三中 RFID 系统中的认证方法流程图。

具体实施方式

[0077] 本发明的实施例提供一种 RFID 系统中的认证方法，在标签的标识 ID 的匿名方式上将 ID 分割为若干部分，并分别进行加密和传输，这种方式使 ID 信息不以明文的形式传输，而以匿名的方式把信息通过标签传给阅读器，保护了标签的标识 ID 的信息。另外，本发明的实施例在数据同步的问题上提出标签询问式的通信方式，通过在网络侧增加存储临时密钥、以及数据库在得到标签对更新密钥请求的响应后再更新密钥的方法，提高了标签与网络侧之间密钥同步的可靠性。

[0078] 以下结合附图和实施例，描述本发明的具体实施方式。

[0079] 本发明实施例一中，一种 RFID 系统中的认证方法如图 4 所示，为一种低成本标签双向认证方法，在本实施例中没有进行任何的数据更新，可用在低成本只读标签中。其中，Command 是阅读器向标签发送的命令；K_{p1}，K_{p2} 是标签和阅读器共享的密钥；R_t 是标签生成的随机数，R_r 是阅读器生成的随机数；ID_x（M 位）是以二进制形式表示的 ID（N 位）字符串的高 M 位（$M < N$）；ID_y（N-M 位）是以二进制形式表示的 ID（N 位）字符串的低（N-M）位；CRC 是循环校验函数；$\oplus$ 是异或运算符，$\|$ 是字符串关联符，$\$$ 是字符串连接符。

[0080] 为描述清楚起见，本实施例中使用的 R_t 为 48 位随机数，ID_x 和 ID_y 分别为 ID（96 位）的高 48 位和低 48 位。这些数字以及 ID_x 与 ID_y 的分配方法并不用于限定本发明实施例的保护范围，任何在数字上的对本发明的修改，也应在本发明保护范围内。

[0081] 在进行双向认证之前，标签和后端数据库要共享密钥 K_{p1}，K_{p2}，在后端数据库存放标签簇的 ID 码。认证的具体流程如图 4 所示，包括：

[0082] 步骤 s401、阅读器对标签发送命令（Command $\|$ R_r）。

[0083] 该步骤中，阅读器向标签发送 Command 和随机数 R_r 给标签，等待标签的回应。

[0084] 步骤 s402、标签回应阅读器的请求（$M_1 \| G_1 \| G_2$）。

[0085] 该步骤中，标签在收到阅读器的请求后，将进行以下运算：

[0086] $M_1 = CRC(ID_x \oplus R_r) \oplus K_{p1}$，$M_2 = CRC(ID_y \oplus R_t) \oplus K_{p2}$，

[0087] $G_1 = M_1 \oplus M_2$，$G_2 = R_t \oplus K_{p1} \oplus K_{p2}$，

[0088] 然后标签将 $(M_1 \| G_1 \| G_2)$ 传给阅读器，等待阅读器的认证。

[0089] 步骤 s403、阅读器将待认证标签发送给数据库 $(M_1 \| G_1 \| G_2 \| R_r)$，由数据库进行认证。

[0090] 该步骤中，当阅读器收到 $(M_1 \| G_1 \| G_2)$ 后，它将自己生成的随机数 R_r 连同 $(M_1 \| G_1 \| G_2)$ 发给数据库。由数据库进行以下运算：

[0091] 运算 $M_2 = M_1 \oplus G_1$，$R_t = G_2 \oplus K_{p1} \oplus K_{p2}$，得出 M_2 和 R_t；然后分别用 R_r，R_t 与数据库中所有的 ID 进行计算：$CRC(ID_x \oplus R_r)$ 和 $CRC(ID_y \oplus R_t)$，将计算结果分别与 $M_1 \oplus K_{p1}$ 和 $M_2 \oplus K_{p2}$ 做比较，如果某个标签的 ID 计算结果经过上述比较相等，则该标签通过认证，转向步骤 404，否则停止认证操作。

[0092] 步骤 s404、数据库将加密信息 M_3 向阅读器发送。

[0093] 该步骤中，对于通过认证的标签，数据库会将 $(K_{p1}, K_{p2}, R_r, R_t)$ 二进制码连接到一起，并与 ID_x 和 ID_y 进行异或运算，对其最后结果再进行 CRC 运算，生成加密信息 M_3，即：$M_3 = CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \oint K_{p2} \oint R_r \oint R_t)]$，

[0094] 并将最后的结果 M_3 传给阅读器；

[0095] 步骤 s405、标签对阅读器进行认证。

[0096] 该步骤中，标签收到 M_3 后，标签用本身的 K_{p1}，K_{p2}，R_r，R_t，ID_x，ID_y，进行计算：$CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \oint K_{p2} \oint R_r \oint R_t)]$，将计算值与 M_3 进行比较，检测是否为合法阅读器，如果相等，则为合法标签，如果不等，则停止认证。

[0097] 通过使用本发明的上述实施例一提供的方法，可以实现以下有益效果：

[0098] (1) 降低标签因安全而增加的成本和计算复杂度。

[0099] 本发明实施例对标签所做运算包括：异或、CRC 和二进制码连接，这些运算比对称和非对称加密算法中包含的运算简单得多。本发明的实施例通过简单的运算使标签信息在一定程度上得到保护，这可以在很大程度上降低标签因安全而增加的成本和计算复杂度。

[0100] (2) 标签 ID 的匿名性。

[0101] 以实施例一为例，匿名性是体现在交互流程的步骤 s402 中，本发明实施例把 ID 一分为二（也可以分割成更多的部分），传输给阅读器，分解后的 ID 进行匿名传输，保护了用户的隐私，这给篡改者增加了难度，匿名的 ID 在被传给数据库后进行了比较，即：分别用 R_r，R_t 与数据库中的所有 ID 进行异或和 CRC 运算，验证是否有 (ID_x, R_r) 和 (ID_y, R_t) 满足 $CRC(ID_x \oplus R_r)$ 和 $CRC(ID_y \oplus R_t)$。只有满足上述条件的标签 ID 才能通过，否则将被禁止。

[0102] 本发明的实施例对标签的 ID 进行了很好的保护，这相对现有一些解决方案中 ID 暴露的现象是很大的改善。本发明实施例使中间的攻击者很难获得 ID 信息，这使标签的信息和用户的隐私得到了保障。

[0103] (3) 双向认证

[0104] 以实施例一为例，标有校验对 (R_t, ID_y) 和 (ID_x, R_r)。在标签端，它将做校验 (R_t, ID) 与标签存有的数据是否相同。R_t 是标签所发的随机数，R_t 经过加密，传给阅读器和数据库，再传回给标签本身，加上它自己的 ID 进行对比认证，确定是否认证了阅读器。另一方面，阅读器也是这样认证标签 的。

[0105] (4) 抗重放性

[0106] 抗重放性体现在对随机数的保护，以实施例一为例，攻击者想在步骤 s402 进行截

获攻击，并想伪造数据进行简单的重传是不可能实现的，由于每次交互过程中标签使用不同的随机数，所以攻击者伪造数据后进行重传攻击不可行。攻击者试图获得随机数也不是那么容易的，因为在实施例一的步骤 s402 中攻击者只能得到 M_2，不能获得 K_{p1}，K_{p2} 和随机数 R_t。

[0107] (5) 抗中间人攻击

[0108] 中间人位于标签和阅读器之间，其通过对交互数据的截获，来分析标签的信息，在这种攻击中，本发明实施例采用隐藏关键数据的方法来抵御中间人攻击。如在步骤 s402 中 $G_2 = R_t \oplus K_{p1} \oplus K_{p2}$ 隐藏 R_t，$M_1 = CRC(ID_x \oplus R_r) \oplus K_{p1}$，$M_2 = CRC(ID_y \oplus R_t) \oplus K_{p2}$ 隐藏 ID_x，ID_y，使攻击者不能从所截获数据中获得重要信息。

[0109] 本发明实施例二中，一种 RFID 系统中的认证方法如图 5 所示，为基于密钥更新的低成本标签双向认证协方法，此方法是在实施例一的基础上进行的改进。

[0110] 其中，Command 是阅读器向标签发送的命令；K_{p1}，K_{p2} 是标签和阅读器共享的密钥；R_t（以 48 位为例）是标签生成的随机数，R_r 是阅读器生成的随机数；ID_x（以 48 位为例）是以二进制形式表示的 ID（以 96 位为例）字符串的高 48 位；ID_y（以 48 位为例）是以二进制形式表示的 ID 字符串的低 48 位；CRC 是循环校验函数；$\oplus$ 是异或运算符，$\|$ 是字符串关联符，$\oint$ 是字符串连接符。K_{pt1}，K_{pt2} 是更新以后的共享密钥，RTEMP 是数据库生成的随机数，M_3' 是标签校验字符串。需要说明的是，本实施例中的数字信息以及 ID_x 与 ID_y 的分配方法，只是为说明方便而做为实施例的一种表达，并不用于限定本发明实施例的保护范围，任何在数字上的对本发明的修改，也应在本发明保护范围内。

[0111] 具体流程如图 5 所示，其中的步骤 s501 ～步骤 s503 与实施例一中步骤 s401 ～步骤 s403 相同，因此不进行重复描述。步骤 s504、步骤 s505 步是共享 密钥更新的过程。

[0112] 步骤 501、阅读器向标签发送命令。

[0113] 步骤 502、标签回应阅读器的请求。

[0114] 步骤 503、数据库认证标签。

[0115] 步骤 504、数据库共享密钥更新。

[0116] 该步骤中，数据库生成随机数 R_{TEMP}，并计算 $M_4 = R_{TEMP} \oplus K_{p1} \oplus K_{p2}$；更新密钥 $K_{p1} = R_{TEMP} \oplus K_{p1}$，$K_{p2} = R_{TEMP} \oplus K_{p2}$，计算 $M_3 = CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \oint K_{p2} \oint R_r \oint R_t)]$，然后将 (M_3, M_4) 发给阅读器，阅读器将 (M_3, M_4) 转发给标签。

[0117] 步骤 505、标签认证阅读器并更新共享密钥

[0118] 该步骤中，当标签收到 (M_3, M_4) 以后，计算 $R_{TEMP} = M_4 \oplus K_{p1} \oplus K_{p2}$，得到 R_{TEMP}。再利用标签自身的 K_{p1}，K_{p2} 计算 $K_{pt1} = R_{TEMP} \oplus K_{p1}$，$K_{pt2} = R_{TEMP} \oplus K_{p2}$，由此得出校验串：

[0119] $M_3' = CRC[(ID_x \oplus ID_y) \oplus (K_{pt1} \oint K_{pt2} \oint R_r \oint R_t)]$

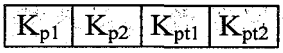
[0120] 标签进行校验计算，验证阅读器传来的 M_3 是否满足 $M_3 = M_3'$，如果相等则验证成功，进行更新 $K_{p1} = K_{pt1}$，$K_{p2} = K_{pt2}$，否则将被阻止。

[0121] 本发明实施例三中，一种 RFID 系统中的认证方法如图 6 所示，为基于询问式密钥更新的低成本标签双向认证方法，此方法是在实施例一的基础上进行的改进。

[0122] 其中，K_{p1}，K_{p2} 是标签和阅读器共享的密钥；R_t（以 48 位为例）是标签生成的随机数，R_r 是阅读器生成的随机数；ID_x（以 48 位为例）是以二进制形式表示的 ID（以 96 位为例）字符串的高 48 位；ID_y（以 48 位为例）是以二进制形式表示的 ID（以 96 位为例）字符

串的低 48 位；CRC 是循环校验函数。K_{pt1} 和 K_{pt2} 是更新以后的共享密钥，RTEMP 是数据库生成的随机数，M_3' 是标签校验字符串，OK 是标签的更新回应，Q_new(Query_new 的简写）是密钥更新询问请求。需要说明的是，本实施例中的数字信息以及 ID_x 与 ID_y 的分配方法，只是为说明方便而做为实施例的一种表达，并不用于限定本发明 实施例的保护范围，任何在数字上的对本发明的修改，也应在本发明保护范围内。

[0123] 具体流程如图 6 所示，步骤 s604 ～步骤 s607 步是共享密钥更新的过程。

[0124] 初始化：在数据库中，初始化一个存储表  。在初始时：K_{p1}，K_{p2} 是初始共享密钥，K_{pt1}，K_{pt2} 为空。

[0125] 步骤 601、阅读器对标签发送命令。

[0126] 阅读器发送询问请求 Command，和随机数 R_r 给标签，等待标签的回应；

[0127] 步骤 602、标签回应阅读器的请求。

[0128] 标签在收到询问请求后，进行以下运算：$M_1 = CRC(ID_x \oplus R_r) \oplus K_{p1}$，$M_2 = CRC(ID_y \oplus R_r) \oplus K_{p2}$，$G_1 = M_1 \oplus M_2$ 和 $G_2 = R_t \oplus K_{p1} \oplus K_{p2}$ 然后将 (M_1, G_1, G_2) 传给阅读器；

[0129] 步骤 603、数据库认证标签。

[0130] 当阅读器收到 (M_1, G_1, G_2) 后，它将自己生成的随机数 R_r 连同 (M_1, G_1, G_2) 发给数据库。数据库首先进行判断：(K_{pt1}, K_{pt2}) 是否为空，如果 (K_{pt1}, K_{pt2}) 为空，则进行 A 方案，否则进行 B 方案。

[0131] A 方案：数据库运算 $M_2 = M_1 \oplus G_1$，$R_t = G_2 \oplus K_{p1} \oplus K_{p2}$，得出 M_2 和 R_t；然后分别用 R_r，R_t 与数据库中所有的 ID 进行计算：$CRC(ID_x \oplus R_r)$ 和 $CRC(ID_y \oplus R_t)$，将计算结果分别与 $M_1 \oplus K_{p1}$ 和 $M_2 \oplus K_{p2}$ 做比较，如果某个标签的 ID 计算结果经过上述比较相等，则该标签通过认证，转向步骤 604，否则停止认证操作。

[0132] B 方案：进行以下两组运算：

[0133] 第一组：数据库运算 $M_2 = M_1 \oplus G_1$，$R_t = G_2 \oplus K_{p1} \oplus K_{p2}$，得出 M_2 和 R_t；然后分别用 R_r，R_t 与数据库中所有的 ID 进行计算：$CRC(ID_x \oplus R_r)$ 和 $CRC(ID_y \oplus R_t)$，将计算结果分别与 $M_1 \oplus K_{p1}$ 和 $M_2 \oplus K_{p2}$ 做比较，如果这组标签 ID 计算结果经过上述比较相等，则该标签通过认证，并摒弃密钥 (K_{pt1}, K_{pt2})，即把 (K_{pt1}, K_{pt2}) 置空，转向步骤 604，如果这组标签 ID 计算结果经过上述比较不相等，进行第二组运算；

[0134] 第二组：数据库运算 $M_2 = M_1 \oplus G_1$，$R_t = G_2 \oplus K_{pt1} \oplus K_{pt2}$，得出 M_2 和 R_t；然 后分别用 R_r，R_t 与数据库中所有的 ID 进行计算：$CRC(ID_x \oplus R_r)$ 和 $CRC(ID_y \oplus R_t)$，将计算结果分别与 $M_1 \oplus K_{pt1}$ 和 $M_2 \oplus K_{pt2}$ 做比较。如果这组标签 ID 计算结果经过上述比较相等，则该标签通过认证，并用 (K_{pt1}, K_{pt2}) 替换 (K_{p1}, K_{p2})，然后把 (K_{pt1}, K_{pt2}) 置为空；如果这组标签 ID 计算结果经过上述比较不相等，则停止认证操作。

[0135] 步骤 604、数据库发起更新询问

[0136] 该步骤中，数据库生成随机数 R_{TEMP}，进行如下计算：

[0137] $M_4 = R_{TEMP} \oplus K_{p1} \oplus K_{p2}$，

[0138] $M_3 = CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \oplus K_{p2} \oplus R_r \oplus R_t)]$，$K_{pt1} = R_{TEMP} \oplus K_{p1}$，$K_{pt2} = R_{TEMP} \oplus K_{p2}$，然后将 (M_3, M_4) 和密钥更新询问请求 Q_new 一起发给阅读器。

[0139] 步骤 605、标签对阅读器进行认证

[0140] 该步骤中，标签收到阅读器的更新询问请求 Q_new 和 (M_3, M_4) 之后，标签利用自身

的 ID_x，ID_y，R_t，K_{p1}，K_{p2}，计算 $M_3' = CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \oplus K_{p2} \oplus Rr \oplus Rt)]$，并验证 M_3 是否满足：$M_3 = M_3'$，如果相等则进行步骤 s606，否则将停止验证。

[0141] 步骤 606、标签更新共享密钥并回应。

[0142] 该步骤中，标签对阅读器认证之后，标签进行如下计算：$R_{TEMP} = M_4 K_{p1} \oplus K_{p2}$，得到 R_{TEMP}。并更新共享密钥 $K_{pt1} = R_{TEMP} \oplus K_{p1}$，$K_{pt2} = R_{TEMP} \oplus K_{p2}$，并向阅读器发出更新回应 OK。

[0143] 步骤 607、数据库完成更新

[0144] 该步骤中，阅读器收到更新回应 OK 之后通知数据库，数据库分别将密钥 K_{p1}、K_{p2} 替换为 K_{pt1}，K_{pt2}，并把 K_{pt1}，K_{pt2} 置为空；如果未收到更新回应 OK，则数据库存储两组密钥 (K_{p1}，K_{p2}) 和 (K_{pt1}，K_{pt2})。

[0145] 通过使用上述实施例提供的方法，在上述实施例一的基础上，进一步实现了以下有益效果：实施例二中，阅读器与标签完成双向认证后，对与标签侧共享的密钥进行动态更新，并在下次认证过程中使用新更新的密钥，提高了对于认证过程的保护性。实施例三中，采用在网络侧同时存储共享密钥临 时密钥的方法，阅读器与标签完成双向认证后，首先对临时密钥进行更新并向阅读器发送更新询问请求，当接收到标签的更新响应后对共享密钥进行更新，否则同时保留原有的共享密钥和临时密钥。在下次认证过程中，同时使用共享密钥和临时密钥对标签进行认证，提高了标签与网络侧之间密钥更新同步的可靠性，避免了因标签与网络侧认证过程不同步引起的认证失败问题。

[0146] 需要说明的是，上述各个实施例中分别对数据库、阅读器以及标签的操作流程进行了描述。在实际的应用中，数据库与阅读器作为网络侧设备，只需共同完成上述流程中网络侧的功能即可，不需要对数据库的功能以及阅读器的功能进行明确划分。

[0147] 本发明的实施例还提供一种 RFID 系统中的认证系统，包括标签 10、阅读器 20 和数据库 30。

[0148] 其中，标签 10 具体包括：

[0149] 标识分割单元 11，用于将本标签的标识 ID 分割成至少两个部分；

[0150] 标识加密单元 12，用于将标识分割单元 11 分割后的部分分别加密后作为加密内容，并向阅读器 20 发送。

[0151] 该单元进一步包括：共享密钥获取子单元 121，用于获取与阅读器 20 共享的密钥；随机数获取子单元 122，用于获取本设备产生的随机数、和 / 或从阅读器 20 接收的随机数用于加密；加密子单元 123，用于利用共享密钥获取子单元 121 获取的密钥、和 / 或随机数获取子单元 122 获取的随机数，对标识分割单元 11 分割后的部分分别进行加密处理。

[0152] 认证消息验证单元 13，用于接收阅读器 20 发送的认证消息，利用标识分割单元 11 分割后的部分验证该认证消息。

[0153] 该单元进一步包括：共享密钥获取子单元 131，用于获取与所述阅读器 20 共享的密钥；随机数获取子单元 132，用于获取本设备产生的随机数、和 / 或从阅读器 20 接收的随机数；验证子单元 133，用于利用共享密钥获取子单元 131 获取的密钥、随机数获取子单元 132 获取的随机数、标识分割单元 10 分割后的部分中的一种或多种，对阅读器发送的认证消息进行认证。

[0154] 密钥更新单元 14，用于当认证消息验证单元 13 对所述认证消息的认证成 功时，根据所述认证消息中携带的内容更新与所述阅读器共享的密钥。

[0155] 更新请求接收单元 15，用于接收所述阅读器发送的认证消息中包括的更新询问请求；

[0156] 更新响应发送单元 16，用于当所述认证消息验证单元 13 对认证消息的认证成功时，根据阅读器 20 发送的更新询问请求，向阅读器 20 发送更新响应。

[0157] 阅读器 20 具体包括：

[0158] 第一转发单元 21，用于接收标签 10 发送的内容，该内容中包括标签 10 对其 ID 分割成至少两个部分后分别进行加密后得到的加密内容；并将标签 10 发送的内容向数据库 30 转发；

[0159] 第二转发单元 22，用于接收数据库 30 发送的认证消息，并转发给所述标签。

[0160] 随机数生成单元 22，用于当所述将标签 10 发送的内容向数据库 30 转发时，同时将验证该标签 10 发送的内容所需的随机数向数据库 30 发送。

[0161] 数据库 30 具体包括：

[0162] 接收单元 31，用于接收阅读器 20 转发的由标签发送的内容，该内容中包括所述标签对其 ID 中至少两个部分后分别进行的加密后得到的加密内容；

[0163] 验证单元 32，用于对接收单元 31 接收的标签 10 发送的内容进行验证；

[0164] 该单元具体包括：随机数获取子单元 321，用于获取验证所述内容所需的随机数；标签标识获取子单元 322，用于获取本地存储的所有标签的 ID；验证子单元 323，用于根据随机数获取子单元 321 获取的随机数、以及标签标识获取子单元 322 获取的本地存储的所有标签的 ID，对标签 10 发送的内容进行验证。

[0165] 认证消息发送单元 33，用于当验证单元 32 验证通过时，向阅读器 20 发送认证消息。

[0166] 该单元具体包括：共享密钥获取子单元 331，用于获取阅读器 20 与标签 10 共享的密钥；随机数获取子单元 332，用于获取生成认证消息所需的随机 数；认证消息生成子单元 333，用于利用共享密钥获取子单元 331 获取的密钥、随机数获取子单元 332 获取的随机数、所述分割后的部分中的一种或多种，生成认证消息并向标签 10 发送。

[0167] 密钥更新单元 34，用于当验证单元 32 对认证消息的认证成功时，更新阅读器 20 与标签 10 共享的密钥。

[0168] 更新请求发送单元 35，用于验证单元 32 的验证通过时，在向标签 10 发送的认证消息中携带更新询问请求。

[0169] 更新响应接收单元 36，用于接收到阅读器 20 转发的标签 10 的更新响应时，通知密钥更新单元 34 更新阅读器 20 与标签 10 共享的密钥。

[0170] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台设备执行本发明各个实施例所述的方法。

[0171] 以上公开的仅为本发明的几个具体实施例，但是，本发明并非局限于此，任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

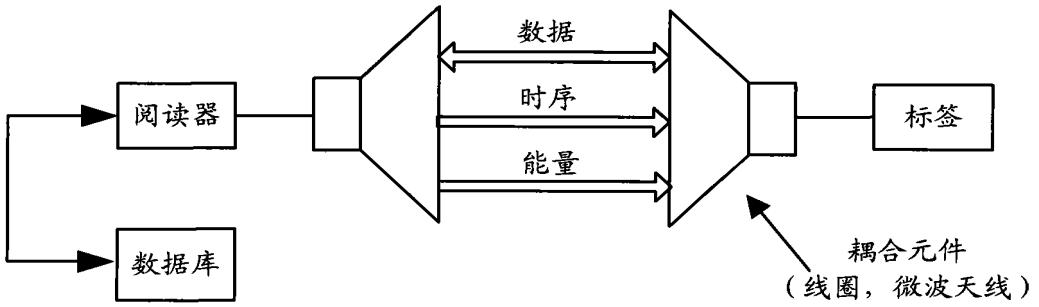

数据
时序
能量
阅读器
标签
数据库
耦合元件
（线圈，微波天线）

图 1

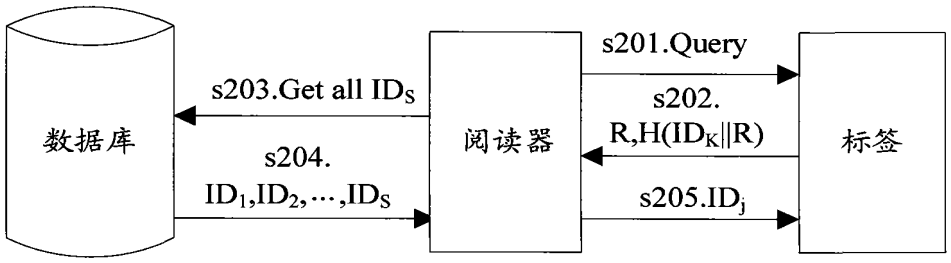

数据库
s203.Get all IDs
s204.
ID1,ID2,…,IDS
阅读器
s201.Query
s202.
R,H(IDK||R)
s205.IDj
标签

图 2

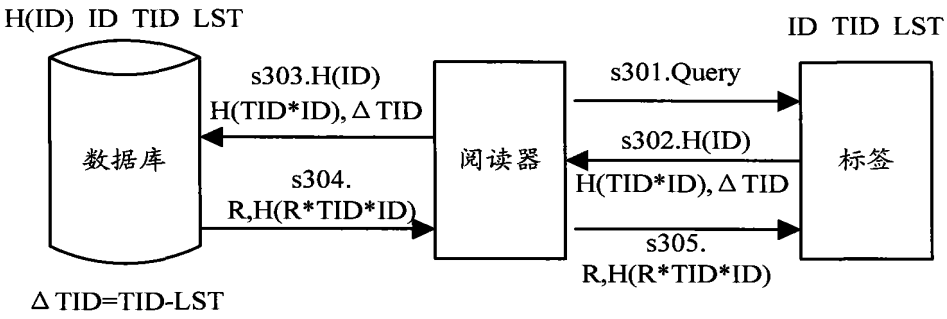

H(ID) ID TID LST
ID TID LST
数据库
s303.H(ID)
H(TID*ID),Δ TID
s304.
R,H(R*TID*ID)
阅读器
s301.Query
s302.H(ID)
H(TID*ID),Δ TID
s305.
R,H(R*TID*ID)
标签
Δ TID=TID-LST

图 3

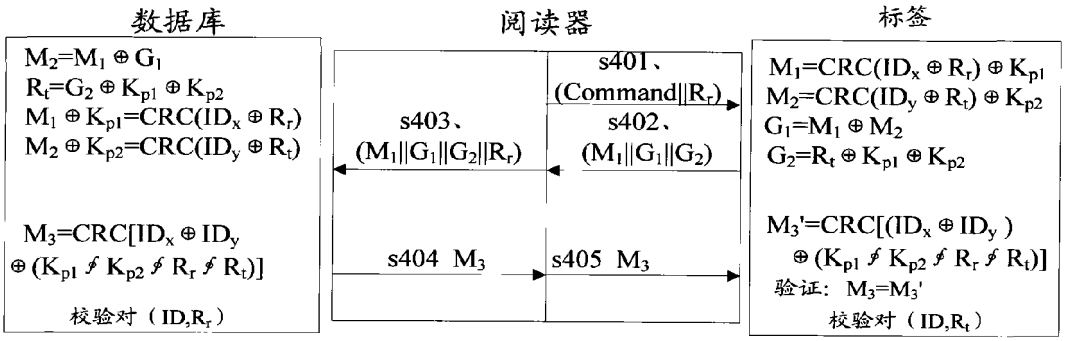

数据库
阅读器
标签
$M_2=M_1 \oplus G_1$
$R_t=G_2 \oplus K_{p1} \oplus K_{p2}$
$M_1 \oplus K_{p1}=CRC(ID_x \oplus R_r)$
$M_2 \oplus K_{p2}=CRC(ID_y \oplus R_t)$
$M_3=CRC[ID_x \oplus ID_y \oplus (K_{p1} \lambda K_{p2} \lambda R_r \lambda R_t)]$
校验对（ID,R_r）
s401、$(Command||R_r)$
s402、$(M_1||G_1||G_2)$
s403、$(M_1||G_1||G_2||R_r)$
s404 M_3
s405 M_3
$M_1=CRC(ID_x \oplus R_r) \oplus K_{p1}$
$M_2=CRC(ID_y \oplus R_t) \oplus K_{p2}$
$G_1=M_1 \oplus M_2$
$G_2=R_t \oplus K_{p1} \oplus K_{p2}$
$M_3'=CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \lambda K_{p2} \lambda R_r \lambda R_t)]$
验证：$M_3=M_3'$
校验对（ID,R_t）

图 4

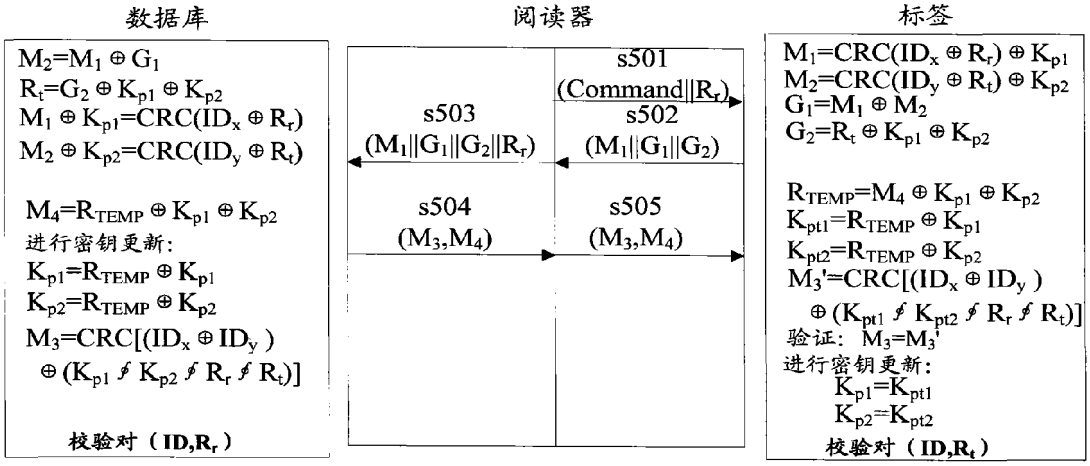

数据库
阅读器
标签
$M_2=M_1 \oplus G_1$
$R_t=G_2 \oplus K_{p1} \oplus K_{p2}$
$M_1 \oplus K_{p1}=CRC(ID_x \oplus R_r)$
$M_2 \oplus K_{p2}=CRC(ID_y \oplus R_t)$
$M_4=R_{TEMP} \oplus K_{p1} \oplus K_{p2}$
进行密钥更新：
$K_{p1}=R_{TEMP} \oplus K_{p1}$
$K_{p2}=R_{TEMP} \oplus K_{p2}$
$M_3=CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \lambda K_{p2} \lambda R_r \lambda R_t)]$
校验对（ID,R_r）
s501 $(Command||R_r)$
s502 $(M_1||G_1||G_2)$
s503 $(M_1||G_1||G_2||R_r)$
s504 (M_3,M_4)
s505 (M_3,M_4)
$M_1=CRC(ID_x \oplus R_r) \oplus K_{p1}$
$M_2=CRC(ID_y \oplus R_t) \oplus K_{p2}$
$G_1=M_1 \oplus M_2$
$G_2=R_t \oplus K_{p1} \oplus K_{p2}$
$R_{TEMP}=M_4 \oplus K_{p1} \oplus K_{p2}$
$K_{pt1}=R_{TEMP} \oplus K_{p1}$
$K_{pt2}=R_{TEMP} \oplus K_{p2}$
$M_3'=CRC[(ID_x \oplus ID_y) \oplus (K_{pt1} \lambda K_{pt2} \lambda R_r \lambda R_t)]$
验证：$M_3=M_3'$
进行密钥更新：
$K_{p1}=K_{pt1}$
$K_{p2}=K_{pt2}$
校验对（ID,R_t）

图 5

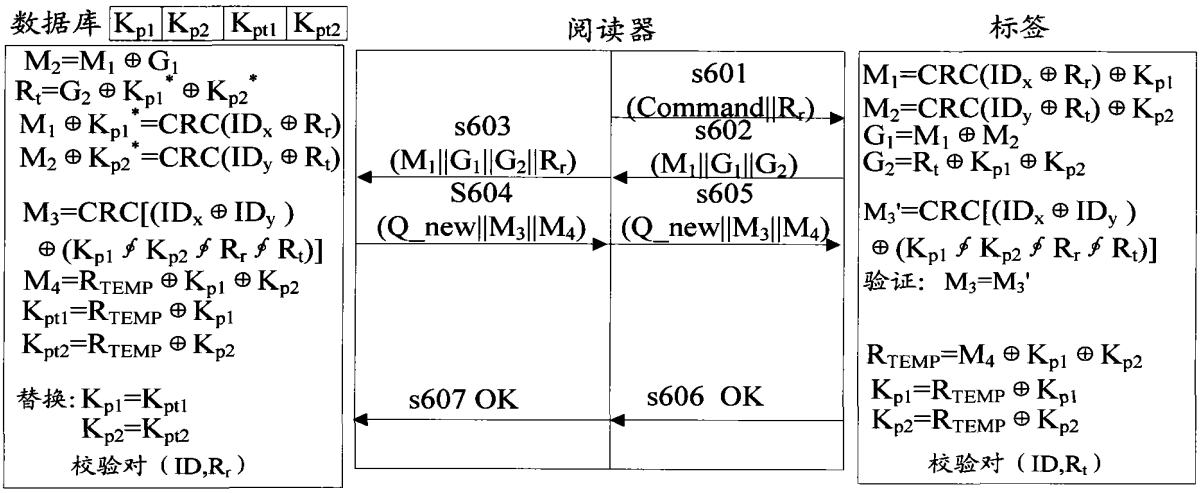

数据库
K_{p1} K_{p2} K_{pt1} K_{pt2}
$M_2=M_1 \oplus G_1$
$R_t=G_2 \oplus K_{p1}^* \oplus K_{p2}^*$
$M_1 \oplus K_{p1}^*=CRC(ID_x \oplus R_r)$
$M_2 \oplus K_{p2}^*=CRC(ID_y \oplus R_t)$
$M_3=CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \lll K_{p2} \lll R_r \lll R_t)]$
$M_4=R_{TEMP} \oplus K_{p1} \oplus K_{p2}$
$K_{pt1}=R_{TEMP} \oplus K_{p1}$
$K_{pt2}=R_{TEMP} \oplus K_{p2}$
替换: $K_{p1}=K_{pt1}$
$K_{p2}=K_{pt2}$
校验对（ID,R_r）
阅读器
s601
(Command||R_r)
s603
(M_1||G_1||G_2||R_r)
s602
(M_1||G_1||G_2)
S604
(Q_new||M_3||M_4)
s605
(Q_new||M_3||M_4)
s607 OK
s606 OK
标签
$M_1=CRC(ID_x \oplus R_r) \oplus K_{p1}$
$M_2=CRC(ID_y \oplus R_t) \oplus K_{p2}$
$G_1=M_1 \oplus M_2$
$G_2=R_t \oplus K_{p1} \oplus K_{p2}$
$M_3'=CRC[(ID_x \oplus ID_y) \oplus (K_{p1} \lll K_{p2} \lll R_r \lll R_t)]$
验证: $M_3=M_3'$
$R_{TEMP}=M_4 \oplus K_{p1} \oplus K_{p2}$
$K_{p1}=R_{TEMP} \oplus K_{p1}$
$K_{p2}=R_{TEMP} \oplus K_{p2}$
校验对（ID,R_t）

图 6