(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 101350060 B
(45)授权公告日 2011.06.01

(21)申请号 200810150433.X

(22)申请日 2008.07.23

(73)专利权人 西安西电捷通无线网络通信股份有限公司
地址 710075 陕西省西安市高新区科技二路68号西安软件园秦风阁A201

(72)发明人 庞辽军 曹军 铁满霞

(74)专利代理机构 西安智邦专利商标代理有限公司 61211
代理人 商宇科

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

审查员 李晴晖

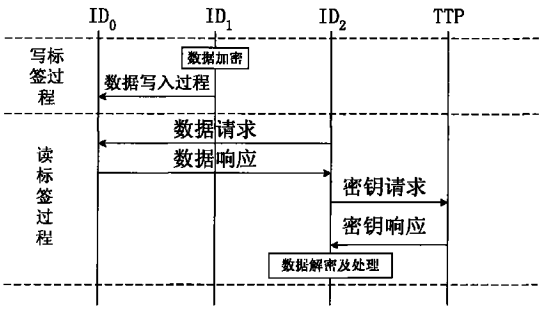
权利要求书 2 页 说明书 6 页 附图 1 页

(54)发明名称

一种适合电子标签的数据安全存取方法

(57)摘要

本发明涉及一种适合于电子标签的数据安全存取方法。该方法包括以下步骤：1)数据写入过程：由第一读写器将消息MSG加密后写入电子标签；2)数据读取过程：2.1)第二读写器发送数据请求分组给电子标签；2.2)电子标签根据数据请求分组向第二读写器发送数据响应分组；2.3)第二读写器向可信第三方发送密钥请求分组；2.4)可信第三方根据密钥请求分组向第二读写器发送密钥响应分组；3)第二读写器根据密钥响应分组得到电子标签消息MSG的明文。本发明可实现低性能电子标签的数据的安全存取。



CN 101350060 B

1. 一种适合于电子标签的数据安全存取方法，其特征在于：该方法包括以下步骤：

0) 通过可信第三方建立系统参数，所述系统参数包括：两个 q 阶的循环群 $(G_1, +)$ 和 $(G_2, \cdot)$；P 为 G_1 的生成元；令 e 为 G_1 和 G_2 上的双线性变换，即 $e: G_1 \times G_1 \rightarrow G_2$；可信第三方随机选取自己的私钥 $S_{TTP} \in Z_q^*$，其对应公钥为 $Q_{TTP} = S_{TTP} \cdot P \in G_1$；$E_K(m)$ 表示使用对称加密算法对消息 m 加密，加密密钥为 K；h(x) 表示一个单向 hash 函数；

1) 数据写入过程：由第一读写器将消息 MSG 加密后写入电子标签，所述第一读写器将消息 MSG 加密的具体过程是：首先，第一读写器随机选取一个密钥标识 PKeyID，并将该密钥标识作为一个公钥；接着，第一读写器选取一个秘密随机整数 r，计算 $K = r \cdot Q_{TTP} \cdot PKeyID$；然后，使用 K 加密 MSG 获得相应密文 CMSG，即计算 $CMSG = E_K(MSG)$；同时，计算 $CP = r \cdot P$ 和消息完整性校验值 $MIC = h(ID_1||S_1||TTP||PKeyID||CMSG||CP)$，最后，将 ID_1、TTP、CP、PKeyID、CMSG 及 MIC 一起写入电子标签；

2) 数据读取过程：

2.1) 第二读写器发送数据请求分组给电子标签；

2.2) 电子标签根据数据请求分组向第二读写器发送数据响应分组；

2.3) 第二读写器向可信第三方发送密钥请求分组；

2.4) 可信第三方根据密钥请求分组向第二读写器发送密钥响应分组；

3) 第二读写器根据密钥响应分组得到电子标签消息 MSG 的明文。

2. 根据权利要求 1 所述的适合于电子标签的数据安全存取方法，其特征在于：所述步骤 2.2) 中数据响应分组内容包括：

ID_1	TTP	PKeyID	CP	CMSG	MIC

其中：

ID_1 字段：写入数据信息的第一读写器 ID_1 的身份；

TTP 字段：可信第三方的身份；

PKeyID 字段：为第一读写器所选取并写入电子标签的 PKeyID 值；

CP 字段：为第一读写器所计算的并写入电子标签的 CP 值，其值等于 r·P；

CMSG 字段：为第一读写器所写入电子标签信息 MSG 的密文；

MIC 字段：为第一读写器所计算的并写入电子标签的 MIC 值，其值等于 $h(ID_1||S_1||PKeyID||CMSG||CP)$。

3. 根据权利要求 2 所述的适合于电子标签的数据安全存取方法，其特征在于：所述步骤 2.3) 中密钥请求分组内容包括：

ID_2	TTP	Nonce	ID_1	PKeyID	CP	CMSG	MIC	MIC_1

其中：

ID2 字段：读取数据信息的第二读写器 ID_2 的身份；

TTP 字段：可信第三方的身份；

Nonce 字段：第二读写器选取的一次性随机数；

ID_1 字段：写入数据信息的第一读写器 ID_1 的身份；

PKeyID 字段：为 ID_1 第一读写器所选取并写入电子标签的 PKeyID 值；

CP 字段：为第一读写器所计算的并写入电子标签的 CP 值；

CMSG 字段：为第一读写器所写入电子标签信息 MSG 的密文；

MIC 字段：为第一读写器所计算的并写入电子标签的 MIC 值；

MIC_1 字段：为第二读写器所计算的消息完整性校验值，其值计算方法为 $h(ID_2||S_2||TTP||Nonce||MIC)$。

4. 根据权利要求 3 所述的适合于电子标签的数据安全存取方法，其特征在于：所述步骤 2.3) 中当可信第三方收到第二读写器的密钥请求分组后，可以对第二读写器的身份有效性进行验证，如果其身份无效，协议结束，否则，计算第二读写器的私钥 S_2，同时，重新计算 MIC_1 值，并与接收到的 MIC_1 值进行比较，如果 MIC_1 值不相等，协议结束，否则，对第一读写器的身份有效性进行验证，如果第一读写器的身份无效，协议结束，否则，计算第一读写器的私钥 S_1，同时，重新计算 MIC 值，并与接收到的 MIC 值进行比较，如果 MIC 值不相等，协议结束，否则，构造密钥响应分组并发送给第二读写器。

5. 根据权利要求 4 所述的适合于电子标签的数据安全存取方法，其特征在于：所述步骤 2.4) 中密钥响应分组内容包括

ID_2	TTP	CSKeyID	CP_1	Nonce	MIC

其中：

ID_2 字段：读取数据信息的第二读写器 ID_2 的身份；

TTP 字段：可信第三方的身份；

CSkeyID 字段：所请求的密钥 SKeyID 的密文，计算过程为：首先可信第三方计算 $SKeyID = S_{TTP} \cdot PKeyID$，接着，可信第三方选取一个秘密随机整数 r_1，计算 $K_1 = r_1 \cdot Q_{TTP} \cdot ID_2$，并由 K_1 导出一个加密密钥 EK 和一个完整校验密钥 IK；然后，使用 EK 加密 SKeyID 获得相应密文 CSKeyID，即计算 $CSKeyID = E_{EK}(SKeyID)$；

CP_1 字段：$CP_1 = r_1 \cdot P$；

Nonce 字段：第二读写器所选取的一次性随机数；

MIC 字段：使用由 K_1 导出的完整性校验密钥 IK 对该字段之前所以字段求取完整性校验值。

6. 根据权利要求 5 所述的适合于电子标签的数据安全存取方法，其特征在于：所述步骤 2.4) 中当第二读写器收到密钥响应分组后，验证 Nonce 是否第二读写器所选随机数，如果不是，协议出错停止，否则，重新计算 $K_1 = CP_1 \cdot S_2$ 并由其导出加密密钥 EK 和完整校验密钥 IK，利用 IK 可以重新计算 MIC 值并与接收的 MIC 进行比较来验证该分组的有效性，如果验证有效，则利用 EK 解密 CSKeyID 得到 SKeyID 明文，在得到 SKeyID 后，根据数据响应分组的内容，计算 $K = CP \cdot SKeyID$，最后，利用 K 作为密钥解密 CMSG 即可得到 MSG 明文。

一种适合电子标签的数据安全存取方法

[0001] 发明领域

[0002] 本发明涉及一种适合电子标签的数据安全存取方法。

背景技术

[0003] 对于无线网络来说，如无线局域网或无线城域网等，其安全问题远比有线以太网严重的多。射频识别标签 (RFID) 同样面临安全问题，在进行安全通信之前，同样必须有效地解决 RFID 中读写器和电子标签之间的权限鉴别问题。如果电子标签的性能较高，具有一定的计算和处理能力，那么，我们可以使用或借鉴现有无线网络的安全接入协议来实现电子标签和读写器之间的认证和权限鉴别问题。但是，如果电子标签只提供存储数据的功能，本身不具备任何数据处理能力，则传统的安全协议很难保证所存储数据的安全性。

[0004] 根据电子标签的使用场合和应用环境，电子标签大概可以分为三种 :1) 高级的电子标签，具有可读可写功能，并具有一定的内存空间和计算能力 ;2) 中档次的电子标签，跟高级标签相比，性能稍差一些，功能类似 ;3) 低档次的电子标签，只用来记录一些数据信息，保证信息能够被读写器读出或写入，一般来说没有数据处理功能和计算能力，这种标签如充值计费卡等。

[0005] 对于前两种电子标签，我们可以通过认证协议来保证电子标签和读写器之间的信道安全，而对于第三种电子标签，由于电子标签本身没有计算和用于计算的内存能力，也没有身份等信息，只是一个存放了信息的介质。尽管性能比较低，但其所存储的数据信息的安全性要求可能较高，需要保证所存储的信息只能被意定的、合法的读写器读取并解密 ;同样，只有意定的、合法的读写器写入的信息能够被其他读写器所认可。通过现有的认证方案来实现该安全需求显然是不可行的。

[0006] 现有的无线网络的安全方案，如 :无线局域网 IEEE802.11i、无线城域网 IEEE802.16e、无线局域网中国国家标准 WAPI 等安全方案，对协议各方都有计算、数据处理等基本性能要求，或多或少地可以用于前两种电子标签，而对于第三种标签是根本无法应用的。

[0007] 因此，必须设计新的安全方案来实现对读写器身份和权限的鉴别功能，保证这一类电子标签数据信息的安全性。

发明内容

[0008] 本发明为解决背景技术中的低性能电子标签存在的信息无法安全写入和安全读取的技术问题，而提供一种适合于低性能电子标签的数据安全存取方法。

[0009] 本发明的技术解决方案是 :本发明为一种适合于低性能电子标签的数据安全存取方法，其特殊之处在于 :该方法包括以下步骤 :

[0010] 1) 数据写入过程 :由第一读写器将消息 MSG 加密后写入电子标签 ;

[0011] 2) 数据读取过程 :

[0012] 2.1) 第二读写器发送数据请求分组给电子标签 ;

[0013] 2.2) 电子标签根据数据请求分组向第二读写器发送数据响应分组；

[0014] 2.3) 第二读写器向可信第三方发送密钥请求分组；

[0015] 2.4) 可信第三方根据密钥请求分组向第二读写器发送密钥响应分组；

[0016] 3) 第二读写器根据密钥响应分组得到电子标签消息 MSG 的明文。

[0017] 上述步骤 1) 之前还包括有通过可信第三方建立系统参数的步骤。

[0018] 上述系统参数包括：两个 q 阶的循环群 $(G_1, +)$ 和 $(G_2, \cdot)$；P 为 G_1 的生成元；令 e 为 G_1 和 G_2 上的双线性变换，即 $e: G_1 \times G_1 \rightarrow G_2$；可信第三方随机选取自己的私钥 $S_{TTP} \in Z_q^*$，其对应公钥为 $Q_{TTP} = S_{TTP} \cdot P \in G_1$；$E_K(m)$ 表示使用对称加密算法对消息 m 加密，加密密钥为 K；h(x) 表示一个单向 hash 函数。

[0019] 上述第一读写器将消息 MSG 加密的具体过程如下：首先，第一读写器随机选取一个密钥标识 PKeyID，并将该密钥标识作为一个公钥；接着，第一读写器选取一个秘密随机数 r，计算 $K = r \cdot Q_{TTP} \cdot PKeyID$；然后，使用 K 加密 MSG 获得相应密文 CMSG，即计算 $CMSG = E_K(MSG)$；同时，计算 $CP = r \cdot P$ 和消息完整性校验值 $MIC = h(ID_1||S_1||TTP||PKeyID||CMSG||CP)$，最后，将 ID_1、TTP、CP、PKeyID、CMSG 及 MIC 一起写入电子标签。

[0020] 上述步骤 2.2) 中数据响应分组内容包括：

[0021]

ID_1	TTP	PKeyID	CP	CMSG	MIC

[0022] 其中：

[0023] ID_1 字段：写入数据信息的第一读写器 ID_1 的身份；

[0024] TTP 字段：可信第三方的身份；

[0025] PKeyID 字段：为第一读写器所选取并写入电子标签的 PKeyID 值；

[0026] CP 字段：为第一读写器所计算的并写入电子标签的 CP 值，其值等于 $r \cdot P$；

[0027] CMSG 字段：为第一读写器所写入电子标签信息 MSG 的密文；

[0028] MIC 字段：为第一读写器所计算的并写入电子标签的 MIC 值，其值等于 $h(ID_1||S_1||PKeyID||CMSG||CP)$。

[0029] 上述步骤 2.3) 中密钥请求分组内容包括：

[0030]

ID_2	TTP	Nonce	ID_1	PKeyID	CP	CMSG	MIC	MIC_1

[0031] 其中：

[0032] ID2 字段：读取数据信息的第二读写器 ID_2 的身份；

[0033] TTP 字段：可信第三方的身份；

[0034] Nonce 字段：第二读写器选取的一次性随机数；

[0035] ID_1 字段：写入数据信息的第一读写器 ID_1 的身份；

[0036] PKeyID 字段：为 ID_1 第一读写器所选取并写入电子标签的 PKeyID 值；

[0037] CP 字段：为第一读写器所计算的并写入电子标签的 CP 值；

[0038] CMSG 字段：为第一读写器所写入电子标签信息 MSG 的密文；

[0039] MIC 字段：为第一读写器所计算的并写入电子标签的 MIC 值；

[0040] MIC_1 字段：为第二读写器所计算的消息完整性校验值，其值计算方法为 $h(ID_2||S_2||TTP||Nonce||MIC)$。

[0041] 上述步骤 2.3) 中当可信第三方收到第二读写器的密钥请求分组后，可以对第二读写器的身份有效性进行验证，如果其身份无效，协议结束，否则，计算第二读写器的私钥 S_2，同时，重新计算 MIC_1 值，并与接收到的 MIC_1 值进行比较，如果 MIC_1 值不相等，协议结束，否则，对第一读写器的身份有效性进行验证，如果第一读写器 $_1$ 的身份无效，协议结束，否则，计算第一读写器的私钥 S_1，同时，重新计算 MIC 值，并与接收到的 MIC 值进行比较，如果 MIC 值不相等，协议结束，否则，构造密钥响应分组并发送给第二读写器。

[0042] 上述步骤 2.4) 中密钥响应分组内容包括

[0043]

ID_2	TTP	CSKeyID	CP_1	Nonce	MIC

[0044] 其中：

[0045] ID_2 字段：读取数据信息的第二读写器 ID_2 的身份；

[0046] TTP 字段：可信第三方的身份；

[0047] CSkeyID 字段：所请求的密钥 SKeyID 的密文，计算过程为：首先可信第三方计算 $SKeyID = S_{TTP} \cdot PKeyID$，接着，可信第三方选取一个秘密随机数 r_1，计算 $K_1 = r_1 \cdot Q_{TTP} \cdot ID_2$，并由 K_1 导出一个加密密钥 EK 和一个完整校验密钥 IK；然后，使用 EK 加密 SKeyID 获得相应密文 CSKeyID，即计算 $CSKeyID = E_{EK}(SKeyID)$；

[0048] CP_1 字段：$CP_1 = r_1 \cdot P$；

[0049] Nonce 字段：第二读写器所选取的一次性随机数；

[0050] MIC 字段：使用由 K_1 导出的完整性校验密钥 IK 对该字段之前所以字段求取完整性校验值。

[0051] 上述步骤 2.4) 中当第二读写器收到密钥响应分组后，验证 Nonce 是否第二读写器所选随机数，如果不是，协议出错停止，否则，重新计算 $K_1 = CP_1 \cdot S_2$ 并由其导出加密密钥 EK 和完整校验密钥 IK，利用 IK 可以重新计算 MIC 值并与接收的 MIC 进行比较来验证该分组的有效性，如果验证有效，则利用 EK 解密 CSKeyID 得到 SKeyID 明文，在得到 SKeyID 后，根据数据响应分组的内容，计算 $K = CP \cdot SKeyID$，最后，利用 K 作为密钥解密 CMSG 即可得到 MSG 明文。

[0052] 本发明具有以下优点：

[0053] 1、基于身份公钥机制，不需要像传统公钥那样维护 PKI。

[0054] 2、在认证过程中无须传送数字证书，节约通信开销。

[0055] 3、增加了身份鉴别功能，能够避免基于身份公钥机制中难以进行身份有效性验证的缺点。

[0056] 4、实现了各读写器之间的身份认证和权限鉴别，只有合法的读写器存储的数据能够得到其他读写器的认可，同样，只有合法的读写器才有权读取和解密其他读写器存储的数据信息。

[0057] 5、采用椭圆曲线上的双线性对，能够在不降低安全性的基础上，缩短安全数据的长度，从而大大地提高计算和通信性能。

附图说明

[0058] 图 1 为本发明的方法流程示意图。

具体实施方式

[0059] 本发明的方法是通过一个可信第三方 (TTP) 来实现，该可信第三方可以是认证服务器或其它可实现认证的设备，可信第三方负责用户实体身份的物理鉴别、系统参数生成以及用户参数建立过程。

[0060] 参照图 1，本发明的具体实现方法如下：

[0061] 1) 首先由可信第三方建立系统参数，该系统参数包括：两个 q 阶的循环群 $(G_1, +)$ 和 $(G_2, \cdot)$；P 为 G_1 的生成元；令 e 为 G_1 和 G_2 上的双线性变换，即 $e: G_1 \times G_1 \rightarrow G_2$；可信第三方随机选取自己的私钥 $S_{TTP} \in Z_q^*$，其对应公钥为 $Q_{TTP} = A_{TTP} \cdot P \in G_1$；$E_K(m)$ 表示使用对称加密算法对消息 m 加密，加密密钥为 K；h(x) 表示一个单向 hash 函数；

[0062] 第一读写器和第二读写器的身份 ID_1 和 ID_2 分别为其公钥，其私钥分别为 $S_1 = S_{TTP} \cdot ID_1$ 和 $S_2 = S_{TTP} \cdot ID_2$。电子标签 ID_0 无须计算公、私钥对。

[0063] 该步骤只是在首次应用时来建立系统参数，建立好后，在以后的重复应用中则无须该步骤；

[0064] 2) 数据写入过程：该过程由任意一个读写器，如第一读写器，将消息 MSG 加密后写入电子标签；加密过程如下：

[0065] 首先，第一读写器随机选取一个密钥标识 PKeyID，并将该密钥标识作为一个公钥；接着，第一读写器选取一个秘密随机数 r，计算 $K = r \cdot Q_{TTP} \cdot PKeyID$；然后，使用 K 加密 MSG 获得相应密文 CMSG，即计算 $CMSG = E_K(MSG)$；同时，计算 $CP = r \cdot P$ 和消息完整性校验值 $MIC = h(ID_1||S_1||TTP||PKeyID||CMSG||CP)$，最后，将 ID_1、TTP、CP、PKeyID、CMSG 及 MIC 一起写入电子标签；

[0066] 这样，就完成了第一读写器 ID_1 把信息 MSG 安全写入电子标签的过程；

[0067] 3) 数据读取过程：包括两个子过程：数据获取和密钥获取过程。其中数据获取包括数据请求和数据响应两个分组；密钥获取包括密钥请求和密钥响应两个分组。分别描述如下：

[0068] 3.1) 第二读写器发送数据请求分组给电子标签；本分组内容为空；

[0069] 3.2) 电子标签根据数据请求分组向第二读写器发送数据响应分组；

[0070] 其中数据响应分组内容包括：

[0071]

ID_1	TTP	PKeyID	CP	CMSG	MIC

[0072] 其中：

[0073] ID_1 字段：写入数据信息的第一读写器 ID_1 的身份；

[0074] TTP 字段：可信第三方的身份；

[0075] PKeyID 字段：为第一读写器 ID_1 所选取并写入电子标签的 PKeyID 值；

[0076] CP 字段：为第一读写器 ID_1 所计算的并写入电子标签的 CP 值，其值等于 $r \cdot P$；

[0077] CMSG 字段：为第一读写器 ID_1 所写入电子标签信息 MSG 的密文；

[0078] MIC 字段：为第一读写器 ID_1 所计算的并写入电子标签的 MIC 值，其值等于 $h(ID_1||S_1||PKeyID||CMSG||CP)$。

[0079] 2.3) 第二读写器向可信第三方发送密钥请求分组；

[0080] 其中密钥请求分组内容包括：

[0081]

ID_2	TTP	Nonce	ID_1	PKeyID	CP	CMSG	MIC	MIC_1

[0082] 其中：

[0083] ID2 字段：读取数据信息的第二读写器 ID_2 的身份；

[0084] TTP 字段：可信第三方的身份；

[0085] Nonce 字段：第二读写器 ID_2 选取的一次性随机数；

[0086] ID_1 字段：写入数据信息的第一读写器 ID_1 的身份；

[0087] PKeyID 字段：为第一读写器 ID_1 所选取并写入电子标签的 PKeyID 值；

[0088] CP 字段：为第一读写器 ID_1 所计算的并写入电子标签的 CP 值；

[0089] CMSG 字段：为第一读写器 ID_1 所写入电子标签信息 MSG 的密文；

[0090] MIC 字段：为第一读写器 ID_1 所计算的并写入电子标签的 MIC 值；

[0091] MIC_1 字段：为第二读写器 ID_2 所计算的消息完整性校验值，其值计算方法为 $h(ID_2||S_2||TTP||Nonce||MIC)$；

[0092] 当可信第三方收到二读写器的密钥请求分组后，可以对二读写器的身份有效性进行验证，如果其身份无效，协议结束，否则，计算二读写器的私钥 S_2，同时，重新计算 MIC_1 值，并与接收到的 MIC_1 值进行比较，如果 MIC_1 值不相等，协议结束，否则，对第一读写器的身份有效性进行验证，如果第一读写器的身份无效，协议结束，否则，计算第一读写器的私钥 S_1，同时，重新计算 MIC 值，并与接收到的 MIC 值进行比较。如果 MIC 值不相等，协议结束，否则，构造密钥响应分组并发送给第二读写器；

[0093] 2.4) 可信第三方根据密钥请求分组向第二读写器发送密钥响应分组；

[0094] 其中密钥响应分组内容包括：

[0095]

ID_2	TTP	CSKeyID	CP_1	Nonce	MIC

[0096] 其中：

[0097] ID_2 字段：读取数据信息的第二读写器 ID_2 的身份；

[0098] TTP 字段：可信第三方的身份；

[0099] CSkeyID 字段：所请求的密钥 SKeyID 的密文，计算过程为：首先可信第三方计算 $SKeyID = S_{TTP} \cdot PKeyID$，接着，可信第三方选取一个秘密随机数 r_1，计算 $K_1 = r_1 \cdot Q_{TTP} \cdot ID_2$，并由 K_1 导出一个加密密钥 EK 和一个完整校验密钥 IK；然后，使用 EK 加密 SKeyID 获得相应密文 CSKeyID，即计算 $CSKeyID = E_{EK}(SKeyID)$；

[0100] CP_1 字段：$CP_1 = r_1 \cdot P$；

[0101] Nonce 字段：第二读写器所选取的一次性随机数；

[0102] MIC字段：使用由K_1导出的完整性校验密钥IK对该字段之前所以字段求取完整性校验值；

[0103] 当第二读写器收到密钥响应分组后，验证Nonce是否自己所选随机数。如果不是，协议出错停止，否则，重新计算$K_1 = CP_1 \cdot S_2$并由其导出加密密钥EK和完整校验密钥IK，利用IK可以重新计算MIC值并与接收的MIC进行比较来验证该分组的有效性，如果验证有效，则利用EK解密CSKeyID得到SKeyID明文，在得到SKeyID后，根据数据响应分组的内容，计算K = CP·SKeyID，最后，利用K作为密钥解密CMSG即可得到MSG明文。

[0104] 通过以上协议，利用步骤2）可以实现读写器对电子标签的安全写入功能；利用步骤3）可以完成读写器对电子标签的安全读取功能。同时，通过可信第三方的验证功能，实现了对读写器身份有效性和权限验证功能。

[0105] 如果第二读写器获取了电子标签数据信息中的明文信息并进行了相关处理后，需要重新把处理后的数据信息写入电子标签，则可以采用步骤2）来实现。

[0106] 名词解释：

[0107] ID_0：电子标签的身份信息；

[0108] ID_1：第一读写器的身份信息；

[0109] ID_2：第二读写器的身份信息；

[0110] Nonce：一次性随机数；

[0111] PKeyID：密钥标识，作为公钥使用；

[0112] SKeyID：与PKeyID对应的私钥；

[0113] MSG：写入电子标签的信息。

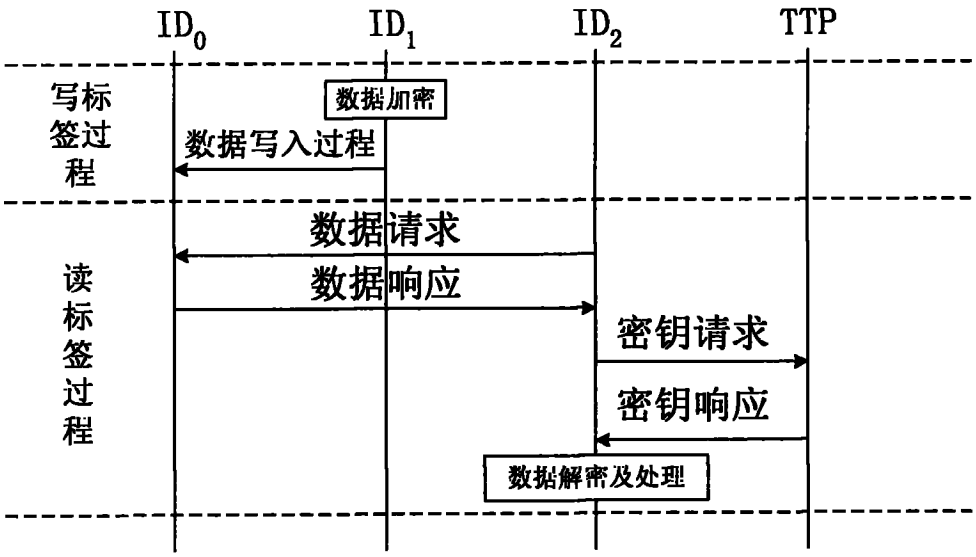

ID0
ID1
ID2
TTP
写标签过程
数据加密
数据写入过程
读标签过程
数据请求
数据响应
密钥请求
密钥响应
数据解密及处理

图 1