(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104618109 A
(43)申请公布日 2015.05.13

(21)申请号 201410854215.X

(22)申请日 2014.12.31

(71)申请人 国家电网公司
地址 100031 北京市西城区西长安街86号
申请人 中国电力科学研究院
江苏省电力公司
江苏省电力公司信息通信分公司

(72)发明人 邵志鹏 楚杰 张涛 马媛媛
周诚 汪晨 李伟伟 时坚 张波
戴造建 王玉雯 费稼轩 孙知兴
夏云浩 陈华智

(74)专利代理机构 北京安博达知识产权代理有限公司 11271
代理人 徐国文

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

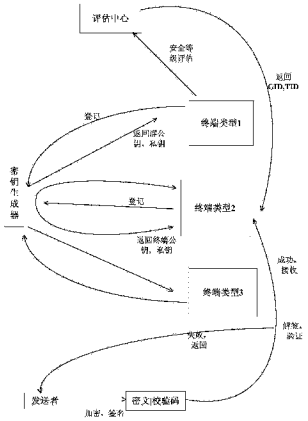
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于数字签名的电力终端数据安全传输方法

(57)摘要

本发明提供一种基于数字签名的电力终端数据安全传输方法，包括以下步骤：对电力终端进行安全评估和注册；密钥生成器生成密钥，并将密钥分发给电力终端；电力终端之间数据传输。本发明提供的基于数字签名的电力终端数据安全传输方法，解决了电力终端数据安全校验问题，且可以实现电力终端数据加密传输及身份验证，提高了电力终端的数据安全性。



CN 104618109 A

1. 一种基于数字签名的电力终端数据安全传输方法，其特征在于：所述方法包括以下步骤：

步骤 1：对电力终端进行安全评估和注册；

步骤 2：密钥生成器生成密钥，并将密钥分发给电力终端；

步骤 3：电力终端之间数据传输。

2. 根据权利要求 1 所述的基于数字签名的电力终端数据安全传输方法，其特征在于：所述步骤 1 具体包括以下步骤：

步骤 1-1：电力终端将自身的信息反馈给评估中心，评估中心根据收集到的业务功能、物理位置、使用网络信息将各个电力终端进行安全分级；

步骤 1-2：具有相同安全级别的电力终端获得相同的组编号，用于密钥的分发；与此同时，评估中心为每个电力终端分配全局唯一的终端编号 TID，用于数据的点到点加密传输。

3. 根据权利要求 1 所述的基于数字签名的电力终端数据安全传输方法，其特征在于：所述步骤 2 包括以下步骤：

步骤 2-1：并定义 p 和 q 均为大素数，且 q 是 p-1 的质因子，设 G_1 为以 p 为特征的有限域上的加法群，G_2 为以 p 为特征的有限域上的乘法群，记 P 为 G_1 的生成元，$\hat{e}$ 为 $G_1 \times G_1 \rightarrow G_2$ 的双线性映射；密钥生成器随机选择 q 以内的正整数 s，认定 s 为系统主私钥，同时认定系统主公钥 $PK = sP$，选取单向哈希函数 H_1 为公钥提取函数，该公钥提取函数满足将任意长度的字符串映射到加法群 G_1 中，即 $\{0,1\}^* \rightarrow G_1$；选取单向哈希函数 H_2 为明文摘要函数，满足将任意明文消息 m 映射到任意长度的字符串中，即 $H_2(m) \rightarrow \{0,1\}^*$；选取单向哈希函数 H_3 为对称密钥提取函数；选取单向哈希函数 H_4，满足将 G_2 中的元素映射到长度为 n 的字母串中，即 $G_2 \rightarrow \{0,1\}^n$，系统公开 $\{P, PK, H_1, H_2, H_3, H_4, G_1, G_2, \hat{e}\}$；

步骤 2-2：各个电力终端将自身的所在组的组编号发送给密钥生成器，密钥生成器为每个相同安全级别的电力终端组颁发组公钥 PK_{GID} 和组私钥 SK_{GID}，有：

$$PK_{GID} = H_1(GID)$$

$$SK_{GID} = sH_1(GID)$$

其中，GID 表示各个电力终端将自身的所在组的组编号，$H_1(GID)$ 表示 GID 作为输入的单向哈希函数运算结果；

发送者的标志号记为 SID，密钥生成器为发送者颁发的公钥 PK_{SID} 和私钥 SK_{SID}，分别表示为：

$$PK_{SID} = H_1(SID)$$

$$SK_{SID} = sH_1(SID)$$

其中，$H_1(SID)$ 表示 SID 作为输入的单向哈希函数运算结果；

步骤 2-3：密钥生成器通过安全信道和协议将产生的私钥分发给发送者及各个组。

4. 根据权利要求 1 所述的基于数字签名的电力终端数据安全传输方法，其特征在于：所述步骤 3 具体包括以下步骤：

步骤 3-1：电力终端间开始传输数据时，由发送者计算明文消息 m 的校验码 h，$h = H_2(m)$，之后确定含校验码的明文消息 M，即 $M = m||h$，其中校验码的打开方式设置为只读；

步骤 3-2：发送者对含校验码的明文消息 M 加密，获得密文消息 C；选择随机正整数 r，

计算发送者的明文消息校验值 T、发送者的密钥向量 V、发送者的对称密钥 K 和密文消息 C，有：

$$T = \hat{e}(PK_{GID},\ PK)^{r}$$

$V = H_4(T)$

$K = H_3(V)$

$C = E_K(M)$

其中，E_K表示对称密钥 K 的对称加密算法，令签名 $S = rPK\text{-}sH_1(SID)$；

步骤 3-3：发送者将 {V，C，S} 作为消息 -- 签名组合发送至数据中心；

步骤 3-4：接收者从数据中心下载消息 -- 签名组合 {V，C，S}，并验证签名；具体有：

先计算发送者的公钥 PK_{SID}，接着用自身所在组的组私钥计算接收者的明文消息校验值 T_1、接收者的密钥向量 V_1和接受者的对称密钥 K_1，有：

$$T_1 = \hat{e}(PK_{GID}, S)\hat{e}(SK_{GID}, PK_{SID})$$

$V_1 = H_4(T_1)$

$K_1 = H_3(V_1)$

判断是否满足 $T_1 = T$，若满足表验证签名成功；若不满足表明验证签名失败，接收者丢弃网络数据包并将校验失败结果反馈给发送者；

步骤 3-5：接受者对接收的密文消息 C 进行解密；具体有：

1) 还原含校验码的明文消息 M，之后分离出明文消息 m 与校验码 h；含校验码的明文消息 M 由下式获得：

$$M = D_{K_1}(C)$$

其中，$D_{K_1}(C)$为密文消息解密算法；

2) 接收者计算 $H_2(m)$ 并且与校验码 h 比对，若 $H_2(m) = h$，则表明数据完整，接收作进一步处理；若 $H_2(m) \neq h$，则表明数据完整性遭到破坏，丢弃数据包并将结果反馈给发送者；

步骤 3-6：若发送者希望与某电力终端点到点通信，则由密钥生成器为每个电力终端的终端编号 TID 生成终端私钥 SK_{TID}，具体有：

$SK_{TID} = sH_1(TID)$

其中，$H_1(TID)$ 表示 TID 作为输入的单向哈希函数运算结果；

电力终端得到 DK_{TID}之后，发送者与其进行通信。

一种基于数字签名的电力终端数据安全传输方法

技术领域

[0001] 本发明涉及一种传输方法，具体涉及一种基于数字签名的电力终端数据安全传输方法。

背景技术

[0002] 随着智能电网的发展和网络通信的复杂化，各种终端在电网业务系统中的使用越来越多样化，这对智能电网数据的安全产生了极大的威胁。终端数据的完整性、保密性以及可用性直接关系到各个电力业务系统的正常使用，其安全性越来越受到重视。面对日渐突出的终端数据泄露问题，对于终端敏感数据进行保护，提高其安全性也愈发重要。嵌入式终端的数据传输过程进行安全强化，主要的安全增强步骤是利用数字签名对传输数据进行完整性校验。校验的步骤包括，首先基于可信的 CA 对公钥进行有效性验证，其次利用公钥对签名数据解密，之后对传输数据进行摘要对比。

[0003] 目前数据传输安全的主要依据是通过计算明文的摘要并与文件的验证码进行比对，但该方法具有明显的局限性。具体而言，现有方法存在以下两点不足 :1) 电力终端数量大，分布广，与每一个终端进行加密数据传输会消耗系统的大量的密钥分配和加密算法资源 ;2) 若敌手在传输过程中截了明文，并重新计算校验码，则电力终端无法分辨，缺少发送者有效身份的验证。签密技术结合了数字签名和数据加密，能有效的解决数据传输过程中加密和认证的问题，在相同安全强度下，签密方案的效率远远大于“先签名后加密”的流程。

发明内容

[0004] 为了克服上述现有技术的不足，本发明提供一种基于数字签名的电力终端数据安全传输方法，解决了电力终端数据安全校验问题，且可以实现电力终端数据加密传输及身份验证，提高了电力终端的数据安全性。

[0005] 为了实现上述发明目的，本发明采取如下技术方案 :

[0006] 本发明提供一种基于数字签名的电力终端数据安全传输方法，所述方法包括以下步骤 :

[0007] 步骤 1 :对电力终端进行安全评估和注册 ;

[0008] 步骤 2 :密钥生成器生成密钥，并将密钥分发给电力终端 ;

[0009] 步骤 3 :电力终端之间数据传输。

[0010] 所述步骤 1 具体包括以下步骤 :

[0011] 步骤 1-1 :电力终端将自身的信息反馈给评估中心，评估中心根据收集到的业务功能、物理位置、使用网络信息将各个电力终端进行安全分级 ;

[0012] 步骤 1-2 :具有相同安全级别的电力终端获得相同的组编号，用于密钥的分发 ;与此同时，评估中心为每个电力终端分配全局唯一的终端编号 TID，用于数据的点到点加密传输。

[0013] 所述步骤 2 包括以下步骤 :

[0014] 步骤 2-1：并定义 p 和 q 均为大素数，且 q 是 p-1 的质因子，设 G_1 为以 p 为特征的有限域上的加法群，G_2 为以 p 为特征的有限域上的乘法群，记 P 为 G_1 的生成元，$\hat{e}$ 为 $G_1 \times G_1 \rightarrow G_2$ 的双线性映射；密钥生成器随机选择 q 以内的正整数 s，认定 s 为系统主私钥，同时认定系统主公钥 PK = sP，选取单向哈希函数 H_1 为公钥提取函数，该公钥提取函数满足将任意长度的字符串映射到加法群 G_1 中，即 $\{0,1\}^* \rightarrow G_1$；选取单向哈希函数 H_2 为明文摘要函数，满足将任意明文消息 m 映射到任意长度的字符串中，即 $H_2(m) \rightarrow \{0,1\}^*$；选取单向哈希函数 H_3 为对称密钥提取函数；选取单向哈希函数 H_4，满足将 G_2 中的元素映射到长度为 n 的字母串中，即 $G_2 \rightarrow \{0,1\}^n$，系统公开 $\{P, PK, H_1, H_2, H_3, H_4, G_1, G_2, \hat{e}\}$；

[0015] 步骤 2-2：各个电力终端将自身的所在组的组编号发送给密钥生成器，密钥生成器为每个相同安全级别的电力终端组颁发组公钥 PK_{GID} 和组私钥 SK_{GID}，有：

[0016] $PK_{GID} = H_1(GID)$

[0017] $SK_{GID} = sH_1(GID)$

[0018] 其中，GID 表示各个电力终端将自身的所在组的组编号，$H_1(GID)$ 表示 GID 作为输入的单向哈希函数运算结果；

[0019] 发送者的标志号记为 SID，密钥生成器为发送者颁发的公钥 PK_{SID} 和私钥 SK_{SID}，分别表示为：

[0020] $PK_{SID} = H_1(SID)$

[0021] $SK_{SID} = sH_1(SID)$

[0022] 其中，$H_1(SID)$ 表示 SID 作为输入的单向哈希函数运算结果；

[0023] 步骤 2-3：密钥生成器通过安全信道和协议将产生的私钥分发给发送者及各个组。

[0024] 所述步骤 3 具体包括以下步骤：

[0025] 步骤 3-1：电力终端间开始传输数据时，由发送者计算明文消息 m 的校验码 h，$h = H_2(m)$，之后确定含校验码的明文消息 M，即 M = m||h，其中校验码的打开方式设置为只读；

[0026] 步骤 3-2：发送者对含校验码的明文消息 M 加密，获得密文消息 C；选择随机正整数 r，计算发送者的明文消息校验值 T、发送者的密钥向量 V、发送者的对称密钥 K 和密文消息 C，有：

[0027] $$T = \hat{e}(PK_{GID},\ PK)^r$$

[0028] $V = H_4(T)$

[0029] $K = H_3(V)$

[0030] $C = E_K(M)$

[0031] 其中，E_K 表示对称密钥 K 的对称加密算法，令签名 $S = rPK - sH_1(SID)$；

[0032] 步骤 3-3：发送者将 {V，C，S} 作为消息 -- 签名组合发送至数据中心；

[0033] 步骤 3-4：接收者从数据中心下载消息 -- 签名组合 {V，C，S}，并验证签名；具体有：

[0034] 先计算发送者的公钥 PK_{SID}，接着用自身所在组的组私钥计算接收者的明文消息校验值 T_1、接收者的密钥向量 V_1 和接受者的对称密钥 K_1，有：

[0035] $$T_1 = \hat{e}(PK_{GID}, S)\hat{e}(SK_{GID}, PK_{SID})$$

[0036] $V_1 = H_4(T_1)$

[0037] $K_1 = H_3(V_1)$

[0038] 判断是否满足 $T_1 = T$，若满足表验证签名成功；若不满足表明验证签名失败，接收者丢弃网络数据包并将校验失败结果反馈给发送者；

[0039] 步骤 3-5：接受者对接收的密文消息 C 进行解密；具体有：

[0040] 1) 还原含校验码的明文消息 M，之后分离出明文消息 m 与校验码 h；含校验码的明文消息 M 由下式获得：

[0041] $$M = D_{K_1}(C)$$

[0042] 其中，$D_{K_1}(C)$为密文消息解密算法；

[0043] 2) 接收者计算 $H_2(m)$ 并且与校验码 h 比对，若 $H_2(m) = h$，则表明数据完整，接收作进一步处理；若 $H_2(m) \neq h$，则表明数据完整性遭到破坏，丢弃数据包并将结果反馈给发送者；

[0044] 步骤 3-6：若发送者希望与某电力终端点到点通信，则由密钥生成器为每个电力终端的终端编号 TID 生成终端私钥 SK_{TID}，具体有：

[0045] $SK_{TID} = sH_1(TID)$

[0046] 其中，$H_1(TID)$ 表示 TID 作为输入的单向哈希函数运算结果；

[0047] 电力终端得到 SK_{TID} 之后，发送者与其进行通信。

[0048] 与现有技术相比，本发明的有益效果在于：

[0049] (1) 主要的安全增强步骤是利用数字签名对升级文件进行完整性校验，首先基于可信的 PKG 发放各个电力终端的公钥私钥，数据发送者利用自身的私钥签名和接收者的公钥加密，数据接收者解签成果之后对升级数据进行摘要对比，适合普适的数据远程校验环境。

[0050] (2) 针对电力终端数量多分布广的特点，为相同安全级别的电力终端分配相同的 GID 号，减少了多接收者过程中对明文的重复加密。此外，以每个智能终端标识符的哈希值作公钥，大大减少了 PKG 的公、私钥生成的工作量，提高了系统运行效率。

[0051] (3) 在对明文处理的过程中，将校验码设置为只读模式并且与明文一起加密传输，适用于数据远程完整性校验。此外将数字签名与数据加密技术相结合，相比于传统“先签名后加密”，明文的加密和签名的计算量大大降低。

附图说明

[0052] 图 1 是本发明实施例中基于数字签名的电力终端数据安全传输方法流程图；

[0053] 图 2 是本发明实施例中电力终端远程数据校验流程图。

具体实施方式

[0054] 下面结合附图对本发明作进一步详细说明。

[0055] 本发明提供一种基于数字签名的电力终端数据安全传输方法，可以准确地对电力远程数据进行完整性验证和签名验证，为每个电力终端分配了全局唯一识别号并结合了签密技术，有效的减少了密钥分发以及传输加密签名过程中的计算量，同时增加了电力终端

的数据安全性。

[0056] 如图 1，基于数字签名的电力终端数据安全传输方法包括以下步骤：

[0057] 步骤 1：对电力终端进行安全评估和注册；

[0058] 步骤 2：密钥生成器生成密钥，并将密钥分发给电力终端；

[0059] 步骤 3：电力终端之间数据传输。

[0060] 所述步骤 1 具体包括以下步骤：

[0061] 步骤 1-1：电力终端将自身的信息反馈给评估中心，评估中心根据收集到的业务功能、物理位置、使用网络信息将各个电力终端进行安全分级；

[0062] 步骤 1-2：具有相同安全级别的电力终端获得相同的组编号，用于密钥的分发；与此同时，评估中心为每个电力终端分配全局唯一的终端编号 TID，用于数据的点到点加密传输。

[0063] 所述步骤 2 包括以下步骤：

[0064] 步骤 2-1：并定义 p 和 q 均为大素数，且 q 是 p-1 的质因子，设 G_1 为以 p 为特征的有限域上的加法群，G_2 为以 p 为特征的有限域上的乘法群，记 P 为 G_1 的生成元，$\hat{e}$ 为 $G_1 \times G_1 \rightarrow G_2$ 的双线性映射；密钥生成器随机选择 q 以内的正整数 s，认定 s 为系统主私钥，同时认定系统主公钥 PK = sP，选取单向哈希函数 H_1 为公钥提取函数，该公钥提取函数满足将任意长度的字符串映射到加法群 G_1 中，即 $\{0,1\}^* \rightarrow G_1$；选取单向哈希函数 H_2 为明文摘要函数，满足将任意明文消息 m 映射到任意长度的字符串中，即 $H_2(m) \rightarrow \{0,1\}^*$；选取单向哈希函数 H_3 为对称密钥提取函数；选取单向哈希函数 H_4，满足将 G_2 中的元素映射到长度为 n 的字母串中，即 $G_2 \rightarrow \{0,1\}^n$，系统公开 $\{P, PK, H_1, H_2, H_3, H_4, G_1, G_2, \hat{e}\}$；

[0065] 步骤 2-2：各个电力终端将自身的所在组的组编号发送给密钥生成器，密钥生成器为每个相同安全级别的电力终端组颁发组公钥 PK_{GID} 和组私钥 SK_{GID}，有：

[0066] $PK_{GID} = H_1(GID)$

[0067] $SKGID = sH_1(GID)$

[0068] 其中，GID 表示各个电力终端将自身的所在组的组编号，$H_1(GID)$ 表示 GID 作为输入的单向哈希函数运算结果；

[0069] 发送者的标志号记为 SID，密钥生成器为发送者颁发的公钥 PK_{SID} 和私钥 SK_{SID}，分别表示为：

[0070] $PK_{SID} = H_1(SID)$

[0071] $SK_{SID} = sH_1(SID)$

[0072] 其中，$H_1(SID)$ 表示 SID 作为输入的单向哈希函数运算结果；

[0073] 步骤 2-3：密钥生成器通过安全信道和协议将产生的私钥分发给发送者及各个组。

[0074] 如图 2，所述步骤 3 具体包括以下步骤：

[0075] 步骤 3-1：电力终端间开始传输数据时，由发送者计算明文消息 m 的校验码 h，$h = H_2(m)$，之后确定含校验码的明文消息 M，即 $M = m||h$，其中校验码的打开方式设置为只读；

[0076] 步骤 3-2：发送者对含校验码的明文消息 M 加密，获得密文消息 C；选择随机正整数 r，计算发送者的明文消息校验值 T、发送者的密钥向量 V、发送者的对称密钥 K 和密文消息 C，有：

[0077] $T = \hat{e}(PK_{GID},\ PK)^{r}$

[0078] $V = H_4(T)$

[0079] $K = H_3(V)$

[0080] $C=E_K(M)$

[0081] 其中，E_K表示对称密钥 K 的对称加密算法，令签名 $S=rPK-sH_1(SID)$；

[0082] 步骤 3-3：发送者将 {V，C，S} 作为消息 -- 签名组合发送至数据中心；

[0083] 步骤 3-4：接收者从数据中心下载消息 -- 签名组合 {V，C，S}，并验证签名；具体有：

[0084] 先计算发送者的公钥 PK_{SID}，接着用自身所在组的组私钥计算接收者的明文消息校验值 T_1、接收者的密钥向量 V_1和接受者的对称密钥 K_1，有：

[0085] $T_1 = \hat{e}(PK_{GID},S)\hat{e}(SK_{GID},PK_{SID})$

[0086] $V_1 = H_4(T_1)$

[0087] $K_1 = H_3(V_1)$

[0088] 判断是否满足 $T_1 = T$，若满足表验证签名成功；若不满足表明验证签名失败，接收者丢弃网络数据包并将校验失败结果反馈给发送者；结论正确性的证明如下：

[0089]

$$\begin{aligned} T_1 = \hat{e}(PK_{GID},S)\hat{e}(SK_{GID},PK_{SID}) &= \hat{e}(PK_{GID},rPK - sPK_{SID})\hat{e}(sPK_{GID},PK_{SID}) \\ &= \hat{e}(PK_{GID},rPK)\hat{e}(PK_{GID},-sPK_{SID})\hat{e}(sPK_{GID},PK_{SID}) \\ &= \hat{e}(PK_{GID},PK)^{r}\hat{e}(PK_{GID},PK_{SID})^{-S}\hat{e}(PK_{GID},PK_{SID})^{S} = \hat{e}(PK_{GID},PK)^{r} = T \end{aligned}$$

[0090] 步骤 3-5：接受者对接收的密文消息 C 进行解密；具体有：

[0091] 1) 还原含校验码的明文消息 M，之后分离出明文消息 m 与校验码 h；含校验码的明文消息 M 由下式获得：

[0092] $M = D_{K_1}(C)$

[0093] 其中，$D_{K_1}(C)$为密文消息解密算法；

[0094] 2) 接收者计算 $H_2(m)$ 并且与校验码 h 比对，若 $H_2(m) = h$，则表明数据完整，接收作进一步处理；若 $H_2(m) \neq h$，则表明数据完整性遭到破坏，丢弃数据包并将结果反馈给发送者；

[0095] 步骤 3-6：若发送者希望与某电力终端点到点通信，则由密钥生成器为每个电力终端的终端编号 TID 生成终端私钥 SK_{TID}，具体有：

[0096] $SK_{TID} = sH_1(TID)$

[0097] 其中，$H_1(TID)$ 表示 TID 作为输入的单向哈希函数运算结果，

[0098] 电力终端得到 SK_{TID}之后，发送者与其进行通信。

[0099] 最后应当说明的是：以上实施例仅用以说明本发明的技术方案而非对其限制，所属领域的普通技术人员参照上述实施例依然可以对本发明的具体实施方式进行修改或者等同替换，这些未脱离本发明精神和范围的任何修改或者等同替换，均在申请待批的本发明的权利要求保护范围之内。

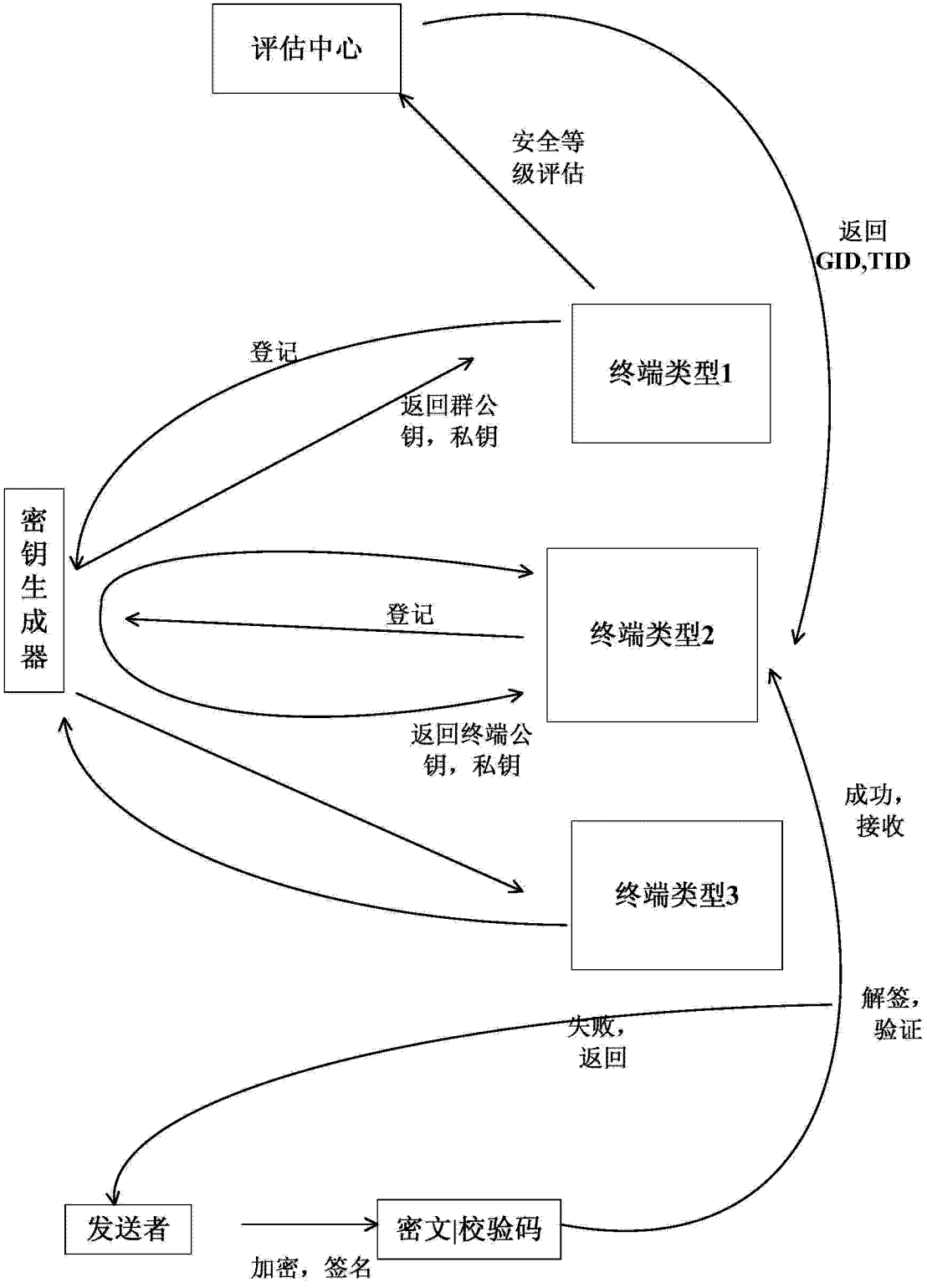

评估中心
安全等级评估
返回GID,TID
登记
返回群公钥，私钥
终端类型1
密钥生成器
登记
终端类型2
返回终端公钥，私钥
成功，接收
终端类型3
解签，验证
失败，返回
发送者
密文|校验码
加密，签名

图 1

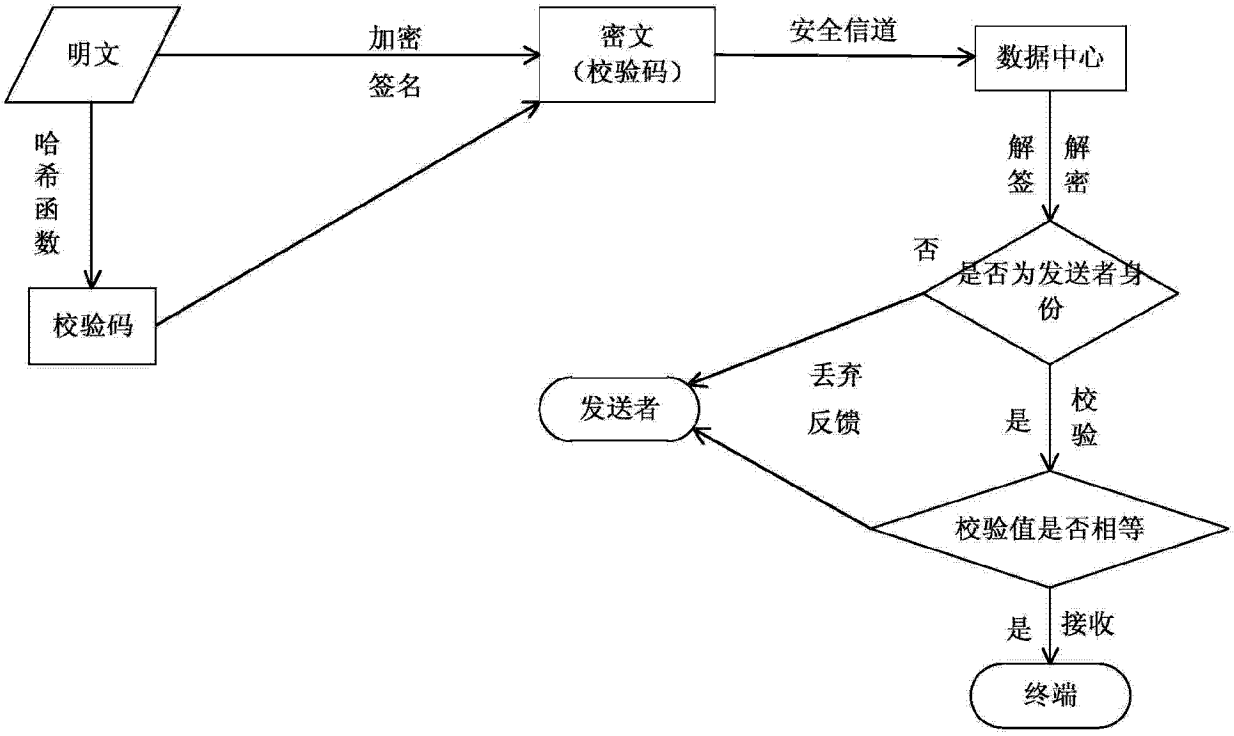

明文
加密
签名
密文
（校验码）
安全信道
数据中心
哈希函数
校验码
解签
解密
否
是否为发送者身份
丢弃
反馈
发送者
是
校验
校验值是否相等
是
接收
终端

图 2