(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 114422588 A
(43)申请公布日 2022.04.29

(21)申请号 202210060167.1

(22)申请日 2022.01.19

(71)申请人 南京南瑞信息通信科技有限公司
地址 210003 江苏省南京市南瑞路8号
申请人 国网江苏省电力有限公司信息通信分公司

(72)发明人 何迎利 梁伟 缪巍巍 王佳 赵华 马涛 曾锃 葛红舞 王元强 张翔 陈民 张明轩 曹光耀 卢岸 龚雯雯 翁春华 左浩然

(74)专利代理机构 南京纵横知识产权代理有限公司 32224
代理人 史俊军

(51)Int.Cl.
H04L 67/56(2022.01)
H04L 9/40(2022.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 67/10(2022.01)
H04L 67/12(2022.01)

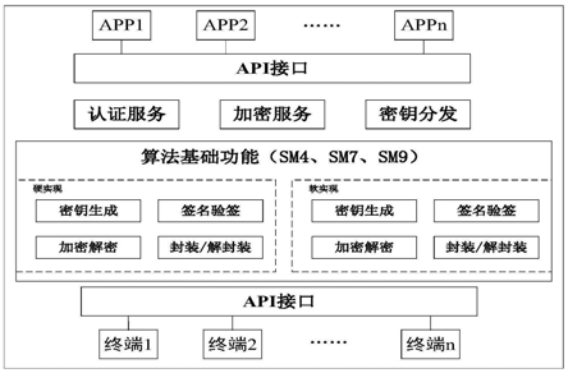
权利要求书2页 说明书5页 附图3页

(54)发明名称

安全自治实现系统及边缘物联代理对终端接入认证的方法

(57)摘要

本发明公开了一种安全自治实现系统及边缘物联代理对终端接入认证的方法，本发明将云端密钥管理中心的密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能下沉至边缘物联代理中，终端的数据通信行为中止于边缘物联代理，降低了对云端的安全攻击的可能，并且降低了云端的负荷。



CN 114422588 A

1.安全自治实现系统,包括边缘物联代理、连接边缘物联代理的云端以及接入边缘物联代理的终端,其特征在于,云端密钥管理中心的密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能下沉至边缘物联代理中,边缘物联代理用以对接入的终端进行接入认证和保密通信。

2.根据权利要求1所述的安全自治实现系统,其特征在于,密钥生成功能、签名验签功能、加密解密功能和密钥/解封装封装功能采用加密芯片实现,加密芯片通过硬件API接口连接终端和云端。

3.根据权利要求1所述的安全自治实现系统,其特征在于,密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能采用软件实现,通过软件API接口连接终端和云端。

4.边缘物联代理对终端接入认证的方法,其特征在于,所述边缘物联代理为权利要求1~3任意一项系统中的边缘物联代理,所述接入认证方法包括:

接收终端发送的ID;

调用密钥生成功能,生成ID对应的主公钥对和私钥对;其中,主公钥对包括加密主公钥和签名主公钥,私钥对包括加密私钥和签名私钥;

接收终端发送的加密临时密钥;

调用加密解密功能,采用加密私钥,对加密临时密钥进行解密,获得临时密钥;

调用加密解密功能,采用临时密钥对私钥对进行加密,并将加密的私钥对发送给终端;

接收终端发送的加密签名的消息;

调用加密解密功能,对加密签名的消息进行解密,获得签名的消息;

调用签名验签功能,对签名的消息进行验签;

响应于验签通过,调用密钥封装/解封装功能,生成封装的会话密钥;

调用加密解密功能,对封装的会话密钥进行加密,并将加密的封装会话密钥发送给终端。

5.根据权利要求4所述的边缘物联代理对终端接入认证的方法,其特征在于,在生成主公钥对和私钥对之前,对ID进行合法性验证。

6.边缘物联代理对终端接入认证的方法,其特征在于,所述终端为权利要求1~3任意一项系统中的边缘物联代理,所述接入认证方法包括:

将自身ID发送给边缘物联代理;

接收边缘物联代理发送的主公钥;其中,主公钥对包括加密主公钥和签名主公钥;

生成临时密钥;

调用加密解密功能,采用加密主公钥加密临时密钥,并将加密的临时密钥发送给边缘物联代理;

接收边缘物联代理发送的加密的私钥对;

调用加密解密功能,对加密的私钥对进行解密,获得私钥对;其中,私钥对包括加密私钥和签名私钥;

调用签名验签功能,对消息进行签名;

调用加密解密功能,对签名的消息进行加密,并将加密签名的消息发送给边缘物联代理;

接收边缘物联代理发送的加密的封装会话密钥；

调用加密解密功能，对加密的封装会话密钥进行解密，获得封装的会话密钥；

调用密钥封装/解封装功能，对封装的会话密钥进行解封装，获得会话密钥。

安全自治实现系统及边缘物联代理对终端接入认证的方法

技术领域

[0001] 本发明涉及一种安全自治实现系统及边缘物联代理对终端接入认证的方法，属于安全加密认证技术领域。

背景技术

[0002] 电力物联网是工业互联网的重要组成部分，建设高效、安全、可信的感知层就成为电力行业重要的建设工作。目前，边缘计算为数据共享及区域自治提供了重要技术手段，主要着力于是对业务数据的预处理，并在安全防护方面仍然沿用传统的身份认证机制。但是随着语音、视频、图像等多元数据的接入，随着高频次数据采集及异构数据存储，边缘物联代理装置仍需解决安全性及可靠性等关键问题。

[0003] 传统身份认证机制中，由于云端安全防护措施高、计算资源多，在密钥管理的性能和安全性方面具备优势，因此将密钥管理中心设置在云端。但在该机制中，由于终端(即业务终端)直接与云端密钥管理中心进行交互，则非法终端可直接恶意攻击云端，使得云系统被攻击的风险较高，且云端密钥管理中心需要为海量的终端提供密钥管理服务，负荷较大。

发明内容

[0004] 本发明提供了一种安全自治实现系统及边缘物联代理对终端接入认证的方法，解决了背景技术中披露的问题。

[0005] 为了解决上述技术问题，本发明所采用的技术方案是：

安全自治实现系统，包括边缘物联代理、连接边缘物联代理的云端以及接入边缘物联代理的终端，云端密钥管理中心的密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能下沉至边缘物联代理中，边缘物联代理用以对接入的终端进行接入认证和保密通信。

[0006] 密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能采用加密芯片实现，加密芯片通过硬件API接口连接终端和云端。

[0007] 密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能采用软件实现，通过软件API接口连接终端和云端。

[0008] 边缘物联代理对终端接入认证的方法，所述边缘物联代理为安全自治实现系统中的边缘物联代理，所述接入认证方法包括：

接收终端发送的ID；

调用密钥生成功能，生成ID对应的主公钥对和私钥对；其中，主公钥对包括加密主公钥和签名主公钥，私钥对包括加密私钥和签名私钥；

接收终端发送的加密临时密钥；

调用加密解密功能，采用加密私钥，对加密临时密钥进行解密，获得临时密钥；

调用加密解密功能，采用临时密钥对私钥对进行加密，并将加密的私钥对发送给终端；

接收终端发送的加密签名的消息；

调用加密解密功能，对加密签名的消息进行解密，获得签名的消息；

调用签名验签功能，对签名的消息进行验签；

响应于验签通过，调用密钥封装/解封装功能，生成封装的会话密钥；

调用加密解密功能，对封装的会话密钥进行加密，并将加密的封装会话密钥发送给终端。

[0009] 在生成主公钥对和私钥对之前，对ID进行合法性验证。

[0010] 边缘物联代理对终端接入认证的方法，所述终端为安全自治实现系统中的边缘物联代理，所述接入认证方法包括：

将自身ID发送给边缘物联代理；

接收边缘物联代理发送的主公钥；其中，主公钥对包括加密主公钥和签名主公钥；

生成临时密钥；

调用加密解密功能，采用加密主公钥加密临时密钥，并将加密的临时密钥发送给边缘物联代理；

接收边缘物联代理发送的加密的私钥对；

调用加密解密功能，对加密的私钥对进行解密，获得私钥对；其中，私钥对包括加密私钥和签名私钥；

调用签名验签功能，对消息进行签名；

调用加密解密功能，对签名的消息进行加密，并将加密签名的消息发送给边缘物联代理；

接收边缘物联代理发送的加密的封装会话密钥；

调用加密解密功能，对加密的封装会话密钥进行解密，获得封装的会话密钥；

调用密钥封装/解封装功能，对封装的会话密钥进行解封装，获得会话密钥。

[0011] 本发明所达到的有益效果：本发明将云端密钥管理中心的密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能下沉至边缘物联代理中，终端的数据通信行为中止于边缘物联代理，降低了对云端的安全攻击的可能，并且降低了云端的负荷。

附图说明

[0012] 图1为本发明系统的结构框图；

图2为基于硬件加密芯片设计的功能；

图3为基于软件设计的功能；

图4为功能集成示意图；

图5为接入认证方法的流程图。

具体实施方式

[0013] 下面结合附图对本发明作进一步描述。以下实施例仅用于更加清楚地说明本发明的技术方案，而不能以此来限制本发明的保护范围。

[0014] 如图1所示，安全自治实现系统，包括边缘物联代理、云端和终端，其中云端依此通过安全接入装置、4G/5G/有线连接边缘物联代理，终端接入边缘物联代理。

[0015] 在云端仍部署密钥管理中心，负责与边缘物联代理根证书等安全认证、保密通信所需要的参量等分发与认证，但不直接为终端提供身份认证服务；在边缘物联代理上部署原先密钥管理中心的部分功能，主要包括密钥生成功能、签名验签功能、加密解密功能和密钥封装功能，即云端密钥管理中心的密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能下沉至边缘物联代理中，边缘物联代理为小区域中心节点，包含具备生成根证书、审核边缘物联代理的认证接入等功能，并负责对接入的终端进行接入认证和保密通信。

[0016] 边缘物联代理与终端设备间的认证接入和保密通信以轻量级加密算法SM7和SM9为主，考虑到SM7算法需要硬件实现，而部分终端设备、边缘物联代理硬件资源难以满足要求的情况，可以用SM4算法替代SM7算法。

[0017] 也就是说上述功能根据不同的情况可以存在以下两种情况实现，一种是采用加密芯片实现，加密芯片通过硬件API接口连接终端和云端；一种是采用软件实现，通过软件API接口连接终端和云端。

[0018] 如图2所示，采用硬件加密芯片实现，主要包括硬件API接口、指令函数和cos程序，其中cos程序在加密芯片里加载运行。

[0019] 硬件API接口包含SM4、SM7加密解密、SM9签名验签、SM9加密解密、SM9封装解封装等API接口，以动态库或者静态库的方式提供给终端使用；指令函数中，定义了SM4、SM7、SM9轻量级加密算法加密解密等各个功能的命令，并与cos程序的指令一一对应；cos程序针对芯片侧SM4、SM7、SM9轻量级加密算法指令集的封装与集成，即轻量级加密算法的具体实现过程。终端调用API接口，通过功能函数向加密芯片发送指令，cos程序接到相应指令后，查找相应的指令集封装函数，执行相应功能，并返回结果。

[0020] 终端通过调用硬件API接口，可以实现轻量级加密算法SM4、SM7加密解密、SM9签名验签、SM9加密解密、SM9封装解封装等功能，降低了用户对加密芯片依赖性，提高了轻量级加密算法的可维护性和可扩展性，提高了用户的工作效率。

[0021] 如图3所示，采用软件实现，主要包含两个部分：软件API接口、功能函数。同硬件API接口相同，软件API接口包含SM4、SM7加密解密、SM9签名验签、SM9加密解密、SM9封装解封装等API接口，以动态库或者静态库的方式提供给用户使用；功能函数中，与硬件加密的指令函数不同，软加密功能函数直接实现了SM4、SM7、SM9轻量级加密算法加密解密等各个功能。用户调用API接口，通过功能函数，执行相应功能，并返回结果。

[0022] 如图4所示，边缘物联代理可以开放的支撑多种轻量级加密认证算法集成(目前支持SM4、SM7和SM9)。对下通过一组统一的API接口实现对不同软、硬件实现的算法的差异性屏蔽，并采用动态库或静态库方式实现不同加密算法的软件定义；对上同样提供一种相对固定的API接口，为其它应用提供安全认证、保密通信、密钥分发等服务。对于不同认证过程以及不同加密算法带来的过程性差异，通过功能性封装成统一的API接口提供给其他APP调用。

[0023] 一般情况下，混合加密方案使用非对称密码算法传输某密钥，而之后使用对称密码算法、用此密钥保密传输消息。这种混合使用模式适用于消息显著长于密钥的情形。上述系统采用SM4、SM7、SM9混合加密方案，提升安全性。

[0024] 上述系统中，边缘物联代理对终端接入认证的方法，如图5所示，具体包括边缘物

联代理侧方法和终端侧方法。

[0025] 边缘物联代理侧方法,包括:

1)接收终端发送的ID;

2)对ID进行合法性验证(在已有设备列表中查找,若存在则合法,否则不合法),若验证通过,转至3),否则拒绝访问;

3)调用密钥生成功能,生成ID对应的主公钥对和私钥对;其中,主公钥对包括SM9加密主公钥和签名主公钥,对于公钥来说,是透传的,无需加密,私钥对包括SM9加密私钥和签名私钥;

4)接收终端发送的加密SM4/SM7临时密钥;

5)调用加密解密功能,采用SM9加密私钥,对加密临时密钥进行解密,获得SM4/SM7临时密钥;

6)调用加密解密功能,采用SM4/SM7临时密钥对私钥对进行SM9加密,并将加密的私钥对发送给终端;

7)接收终端发送的加密签名的消息;

8)调用加密解密功能,对加密签名的消息进行SM9解密,获得签名的消息;

9)调用签名验签功能,对签名的消息进行验签;

10)响应于验签通过,调用密钥封装/解封装功能,生成封装的会话密钥;

11)调用加密解密功能,对封装的会话密钥进行SM9加密,并将加密的封装会话密钥发送给终端。

[0026] 终端侧方法,包括:

21)将自身ID发送给边缘物联代理;

22)接收边缘物联代理发送的主公钥对;其中,主公钥对包括加密主公钥和签名主公钥;

终端获得主公钥对后,可以本地安全保存,在有效期内重新上电掉电后无需再重新申请;

23)生成SM4/SM7临时密钥;

24)调用加密解密功能,采用SM9加密主公钥加密SM4/SM7临时密钥,并将加密的SM4/SM7临时密钥发送给边缘物联代理;

25)接收边缘物联代理发送的加密的私钥对;

26)调用加密解密功能,对加密的私钥对进行SM4/SM7解密,获得私钥对;

终端获取到私钥对后可以本地安全保存,在私钥有效期内重新上电掉电后无需再重新申请;终端申请主公钥对和私钥对完成;

27)调用签名验签功能,对消息进行签名;

28)调用加密解密功能,对签名的消息进行SM9加密,并将加密签名的消息发送给边缘物联代理;

29)接收边缘物联代理发送的加密的封装会话密钥;

210)调用加密解密功能,对加密的封装会话密钥进行SM9解密,获得封装的会话密钥;

211)调用密钥封装功能,对封装的会话密钥进行解封装,获得会话密钥;此会话密

钥是后续业务数据加密通信的对称密钥,实现终端与边缘物联代理之间的安全通信。

[0027] 结合上述步骤,边缘物联代理与终端设备之间的认证流程,主要采用了SM9轻量级加密算法,有效降低了系统资源的消耗;只有认证通过的终端才能被接入,减少了非法终端入侵的可能性,提高了安全性;兼容软/硬两种实现方式,支持API接口调用,方便使用,对于弱智能终端则可采用软件实现,对于智能终端则两种方法均可采用。

[0028] 本发明以边缘物联代理为核心,实现一套“边-端”小区域级的局部认证机制,将部署在云端的密钥生成功能、签名验签功能、加密解密功能和密钥封装/解封装功能下沉到边缘物联代理中,边缘物联代理作为小区域中心节点,负责其物理接入的终端设备的认证接入,实现与终端设备的保密通信,将终端的数据通信行为中止于边缘物联代理,降低了对云端的安全攻击的可能,并且大量减少了云端密钥管理中心的身份认证服务对象,使得云端的计算负荷得到释放,降低了云端的负荷。

[0029] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明技术原理的前提下,还可以做出若干改进和变形,这些改进和变形也应视为本发明的保护范围。

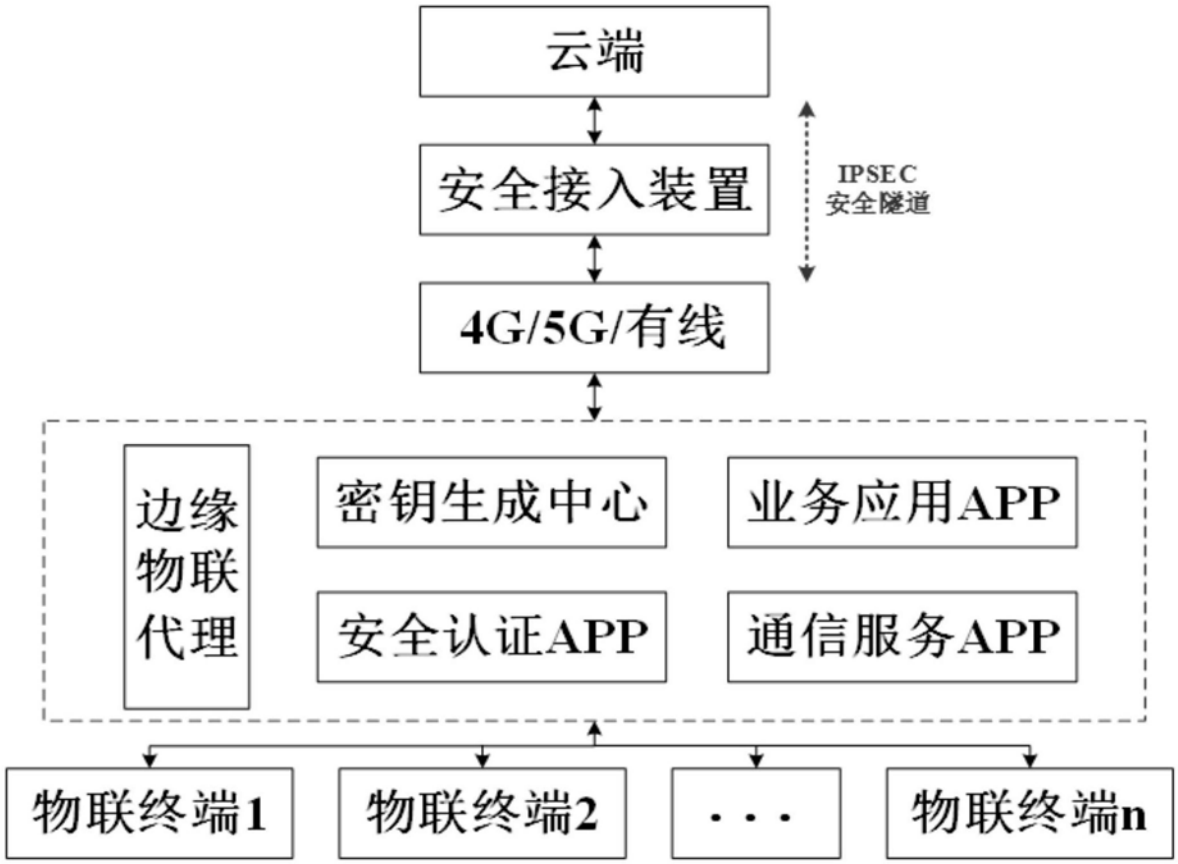

云端
安全接入装置
IPSEC
安全隧道
4G/5G/有线
边缘
物联
代理
密钥生成中心
业务应用APP
安全认证APP
通信服务APP
物联终端1
物联终端2
· · ·
物联终端n

图1

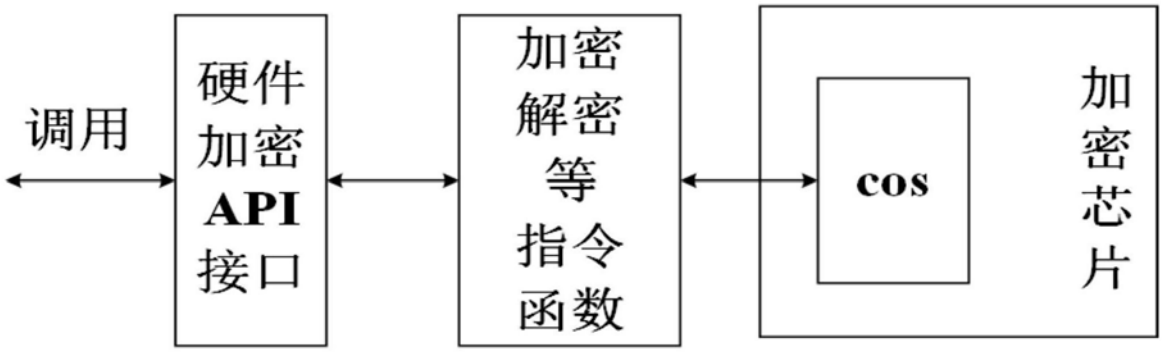

调用
硬件
加密
API
接口
加密
解密
等
指令
函数
cos
加
密
芯
片

图2

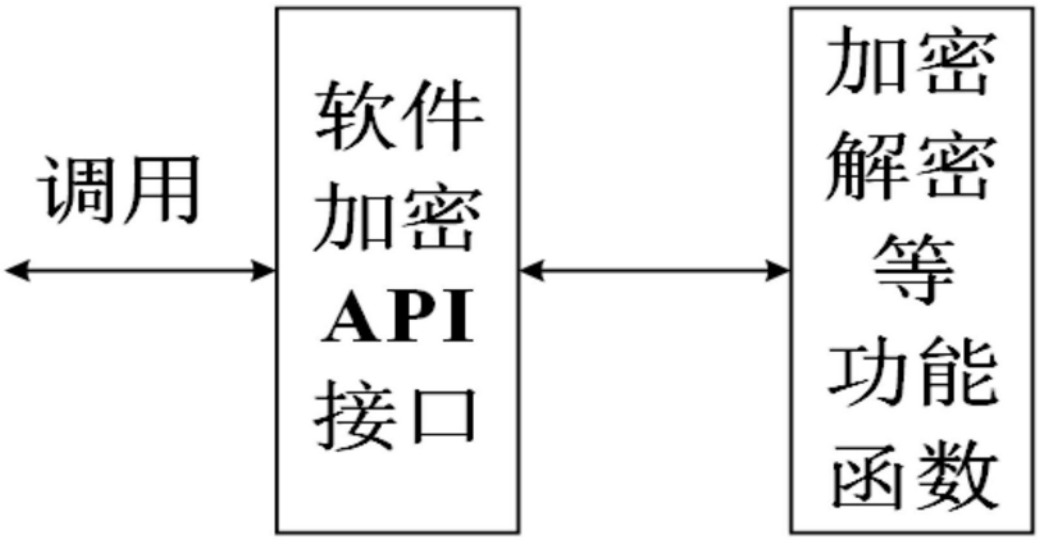

调用
软件加密API接口
加密解密等功能函数

图3

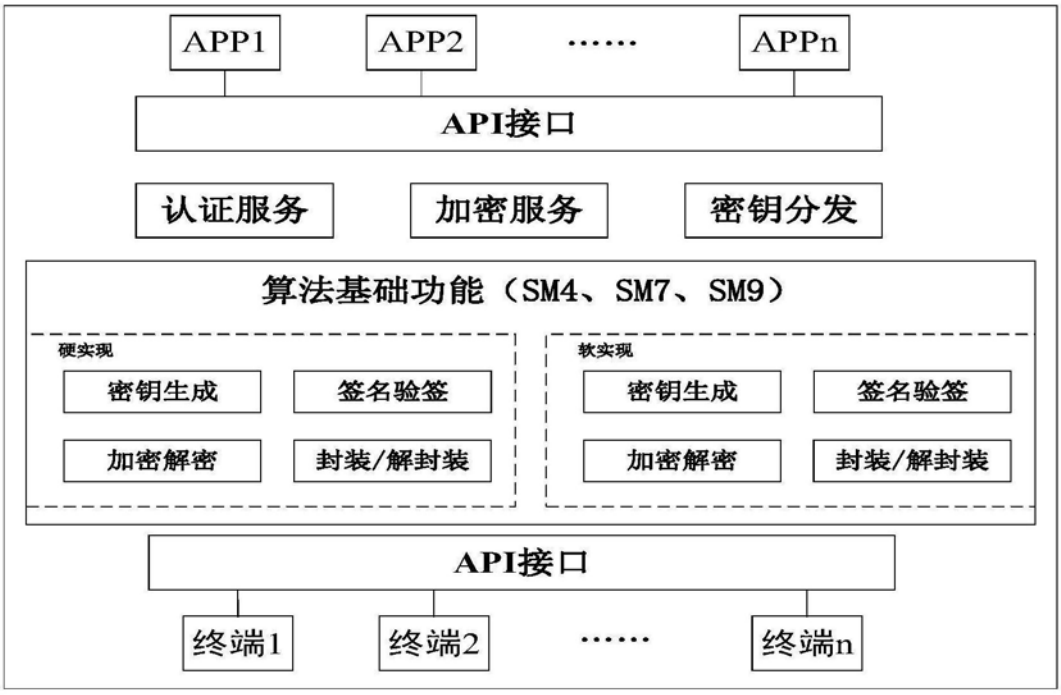

APP1
APP2
……
APPn
API接口
认证服务
加密服务
密钥分发
算法基础功能（SM4、SM7、SM9）
硬实现
密钥生成
签名验签
加密解密
封装/解封装
软实现
密钥生成
签名验签
加密解密
封装/解封装
API接口
终端1
终端2
……
终端n

图4

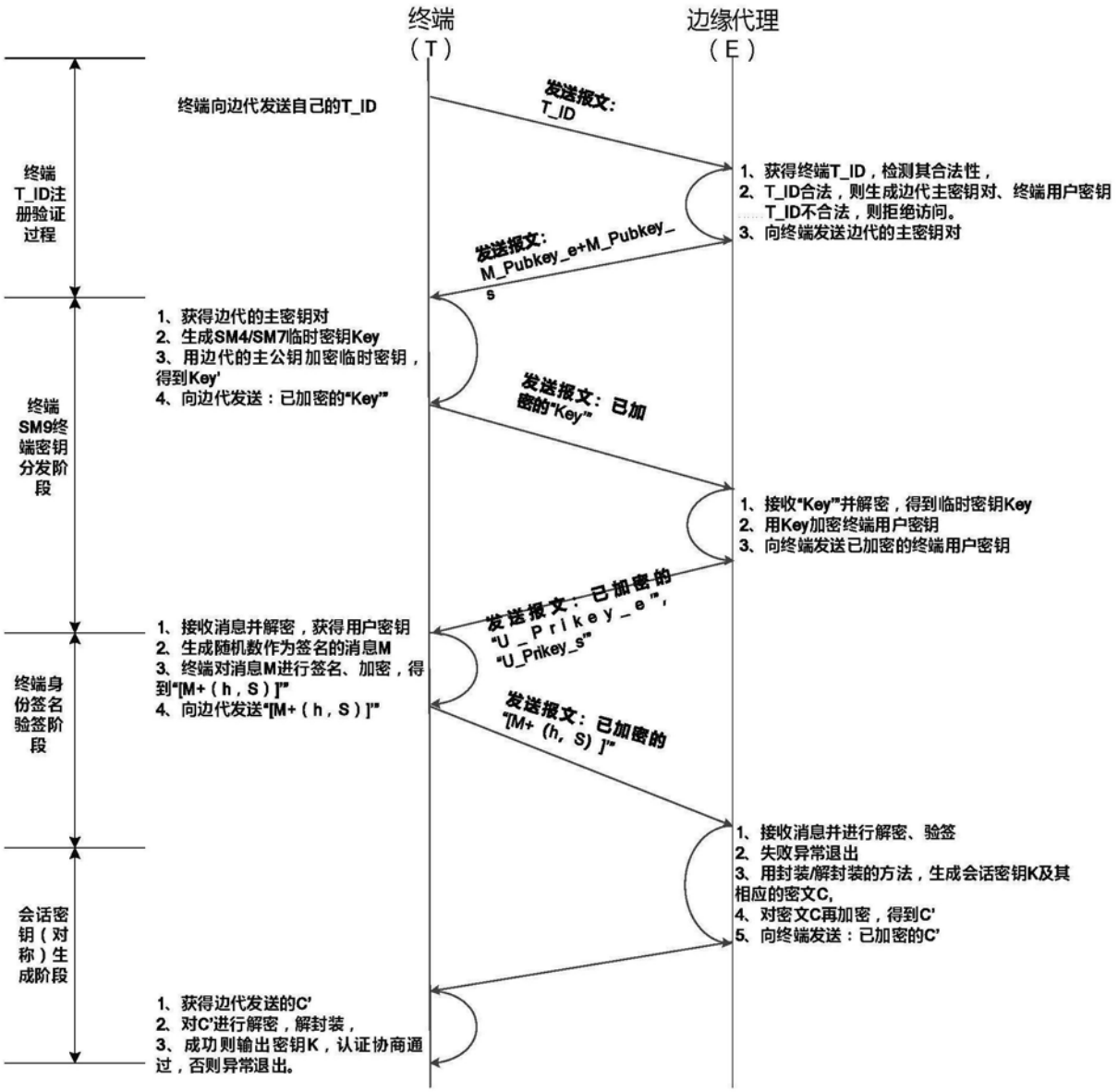

终端
（T）
边缘代理
（E）
终端向边代发送自己的T_ID
发送报文:
T_ID
1、获得终端T_ID，检测其合法性，
2、T_ID合法，则生成边代主密钥对、终端用户密钥
T_ID不合法，则拒绝访问。
3、向终端发送边代的主密钥对
发送报文:
M_Pubkey_e+M_Pubkey_s
终端T_ID注册验证过程
1、获得边代的主密钥对
2、生成SM4/SM7临时密钥Key
3、用边代的主公钥加密临时密钥，得到Key'
4、向边代发送：已加密的"Key'"
发送报文：已加密的"Key'"
1、接收"Key'"并解密，得到临时密钥Key
2、用Key加密终端用户密钥
3、向终端发送已加密的终端用户密钥
终端SM9终端密钥分发阶段
1、接收消息并解密，获得用户密钥
2、生成随机数作为签名的消息M
3、终端对消息M进行签名、加密，得到"[M+（h，S）]"
4、向边代发送"[M+（h，S）]"
发送报文：已加密的"U_Prikey_e'"，"U_Prikey_s'"
发送报文：已加密的"[M+（h，S）]"
终端身份签名验签阶段
1、接收消息并进行解密、验签
2、失败异常退出
3、用封装/解封装的方法，生成会话密钥K及其相应的密文C,
4、对密文C再加密，得到C'
5、向终端发送：已加密的C'
会话密钥（对称）生成阶段
1、获得边代发送的C'
2、对C'进行解密，解封装，
3、成功则输出密钥K，认证协商通过，否则异常退出。

图5