

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 11 月 30 日 (30.11.2017)



(10) 国际公布号
WO 2017/201809 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/087576

(22) 国际申请日: 2016 年 6 月 29 日 (29.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610368125.9 2016 年 5 月 27 日 (27.05.2016) CN

(71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(72) 发明人: 汤镇辉 (TANG, Zhenhui); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(74) 代理人: 北京友联知识产权代理事务所(普通合伙) (YOU LINK INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区学清路8号科技财富中心A座506室尚志峰, Beijing 100192 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,

(54) Title: COMMUNICATION METHOD AND SYSTEM FOR TERMINAL

(54) 发明名称: 终端通信方法及系统

向注册服务器发送入网注册请求, 以执行在注册服务器中的注册

向所述注册服务器发送会话密钥产生请求, 并根据所述服务器传送过来的数据产生会话私钥

向所述注册服务器发送与第二终端通信的请求, 接收所述注册服务器发送的会话公钥, 并根据所述终端的会话私钥以及所述会话公钥获取第二终端的会话私钥, 从而与第二终端进行安全通信

图 1

- S1 Send to a registration server a networking registration request to register at the registration server
- S2 Send to the registration server a session key generation request, and generate a session private key according to data transmitted by the server
- S3 Send to the registration server a request for communicating with a second terminal, receive a session public key sent by the registration server, and acquire, according to the session private key of the terminal and the session public key, a session private key of the second terminal to perform secure communication with the second terminal

(57) Abstract: A communication method for a terminal, used to enable secure communication between terminals. The method comprises: sending to a server a networking registration request, and receiving a registration code generated and sent by the server; sending to the server a session key generation request, receiving a temporary identifier code generated and sent by the server according to an identifier code of the terminal, and generating a session private key according to the registration code, the temporary identifier code, and a random number generated by the terminal; and sending to the server a request for communicating with a second terminal, receiving a session public key sent by the server, and acquiring, according to the session private key of the terminal and the session public key, a session private key of the second terminal to perform secure communication with the second terminal. Also provided in the present invention is a communication system for a terminal. The present invention ensures identity privacy, location privacy, and untraceability during the communication process, thus ensuring communication security of users.

(57) 摘要: 一种终端通信方法, 用于实现终端之间的安全通信, 包括: 向服务器发送入网注册请求, 并接收所述服务器产生并传送的注册码; 向服务器发送会话密钥产生请求, 接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码, 并根据所述注册码、临时识别码以及所述终端产生的随机数产生会话私钥; 及向服务器发送与第二终端通信的请求, 接收所述服务器发送的会话公钥, 并根据所述终端的会话私钥以及所述会话公钥获取第二终端的会话私钥, 从而与第二终端进行安全通信。本发明还提供一种终端通信系统。本发明可以确保通信过程中的身份机密性、位置机密性以及不可跟踪性, 从而保证用户的通信安全。

RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

终端通信方法及系统

技术领域

本发明涉及网络安全技术领域，具体地，涉及一种终端通信的方法及系统。

背景技术

随着科技水平的不断提升，手机已成为人们随身携带的生活必需品，逐渐地改变了人们的工作和生活方式。人们在利用手机获得了移动通信便利的同时，对通信中的信息安全也有了更高的要求。

目前，在移动通信系统中，为了确保用户间信息的安全保密性，保密通信的实现是非常重要的，这就需要对所传输的数据进行加密保护。对数据进行加密保护就是在通信双方采用加密算法，发送方将要传输的数据按选定的加密算法加密后传输，接收方收到数据后再按选定的解密算法解密后分析使用。通常，传统移动通信系统中大多数采用对称加密算法。

所述对称加密（也叫私钥加密）算法指加密和解密使用相同密钥的加密算法，有时也叫传统密码算法。在对称加密算法中，加密密钥能够从解密密钥中推算出来，同时解密密钥也可以从加密密钥中推算出来。而在大多数的对称加密算法中，加密密钥和解密密钥是相同的，所以也称这种加密算法为

秘密密钥算法或单密钥算法。对称加密算法要求发送方和接收方在安全通信之前，商定一个密钥，因此，对称加密算法的安全性依赖于密钥，泄漏密钥就意味着任何人都可以对他们发送或接收的消息解密，所以密钥的保密性对通信的安全性至关重要。

因此，传统的对称加密方式存在管理密钥困难，可扩展性差，无法提供防止抵赖功能等问题。

发明内容

鉴于以上内容，有必要提出一种终端通信方法，其可以确保通信过程中的身份机密性、位置机密性以及不可跟踪性，从而保证用户的通信安全。

一种终端通信方法，应用于终端中，所述通信方法包括：

向服务器发送入网注册请求，以执行终端在所述服务器中的注册，并接收所述服务器产生并传送的注册码；

向所述服务器发送会话密钥产生请求，接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码，并根据所述注册码、所述临时识别码以及所述终端产生的随机数产生会话私钥；及

向所述服务器发送与第二终端通信的请求，接收所述服务器发送的会话公钥，并根据所述终端的会话私钥以及所述会话公钥获取所述第二终端的会话私钥，从而与所述第二终端进行安全通信。

本发明较佳实施例中，所述执行终端在所述服务器中的注册包括：

接收所述服务器的数字证书；及

当验证所述服务器的数字证书合法时，存储所述注册码。

本发明较佳实施例中，所述向所述服务器发送会话密钥产生请求之前还包括：

通过加密函数，对所述终端的识别码以及代表所述终端身份的数据进行加密运算，其中，所述终端的识别码为所述终端的国际移动用户识别码，以及所述代表终端身份的数据包括所述终端的数字证书以及所述注册码。

本发明较佳实施例中，所述对所述终端的识别码以及代表所述终端身份的数据进行加密运算包括：

产生随机数，所述随机数包括随机验证码及随机私钥，根据所述注册码以及随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名私钥；

根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，利用所述服务器的公钥以及非对称加密函数计算加密密钥包；

将所述服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中。

本发明较佳实施例中，所述接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码，并根据所述注册码、临时识别码以及所述终端产生的随机数产生会话私钥包括：

将所述终端计算出来的加密信息包以及加密密钥包传送给所述服务器；

接收所述服务器根据所述终端的加密信息包以及加密密钥包产生的所述服

务器的签名私钥以及所述服务器的加密信息包；

使用所述终端的随机私钥和对称解密函数解密所述服务器的加密信息包，得到识别码以及临时识别码；

使用验名函数和所述服务器的公钥，对所述服务器的签名私钥进行解密，得到注册码及随机验证码；

在解密得到的识别码与所述终端的识别码相同以及解密得到的随机验证码与所述终端产生的随机验证码相同时，根据所述注册码、随机验证码、随机私钥以及临时识别码生成所述终端的会话私钥。

本发明较佳实施例中，所述服务器的签名私钥以及服务器的加密信息包通过下述方法得到：

所述服务器在收到所述终端的加密信息包及加密密钥包后，使用非对称加密函数和所述服务器的私钥，对所述加密密钥包进行解密，以得到所述终端的随机私钥；

所述服务器使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书；

所述服务器利用认证中心的公钥，验证所述终端的数字证书；

若所述终端的数字证书验证成功，则所述服务器使用验名函数和所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码；

所述服务器根据所述终端的注册码判断所述终端是否合法；

在所述终端合法时，所述服务器根据所述终端的识别码生成终端的临时识

别码，并将所述终端的识别码与临时识别码相关联；

所述服务器根据所述注册码及随机验证码，利用所述服务器的私钥以及签名函数，计算所述服务器的签名私钥，以及根据所述服务器的签名私钥、所述终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述服务器的加密信息包。

本发明较佳实施例中，所述服务器发送的会话公钥是将所述终端的会话私钥以及所述第二终端的会话私钥进行异或运算得到。

本发明较佳实施例中，根据所述终端的会话私钥以及所述会话公钥获取第二终端的会话私钥包括：

利用所述终端的会话私钥与所述会话公钥执行异或运算，得到所述第二终端的会话私钥。

一种终端通信方法，应用于服务器中，所述终端通信方法包括：

接收终端发送的入网注册请求，根据所述入网注册请求生成随机的注册码，并将所述注册码发送给所述终端；

接收所述终端发送的会话密钥产生请求，向所述终端发送根据所述终端的识别码产生的临时识别码，以及根据所述注册码，所述终端产生并传送的随机数以及所述临时识别码生成所述终端的会话私钥；及

接收所述终端发送的与第二终端通信的请求，向所述终端发送会话公钥，其中，所述会话公钥为根据所述终端以及所述第二终端的会话私钥通过异或运算得到。

本发明较佳实施例中，所述通信方法还包括产生所述临时识别码的步骤：

接收所述终端的加密信息包及加密密钥包；

使用非对称加密函数和所述服务器的私钥，对所述加密密钥包进行解密，以得到所述终端的随机私钥；

使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书；

利用认证中心的公钥，验证所述终端的数字证书；

若所述终端的数字证书验证成功，则所述服务器使用签名函数和所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码；

根据所述终端的注册码判断所述终端的合法性；

在所述终端合法时，根据所述终端的识别码生成所述终端的临时识别码，并将所述终端的识别码与临时识别码相关联；

根据所述注册码及随机验证码，利用所述服务器的私钥以及签名函数，计算所述服务器的签名私钥，以及根据所述服务器的签名私钥、所述终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述服务器的加密信息包；及

传送所述加密信息包给所述终端。

本发明较佳实施例中，所述终端的加密信息包及加密密钥包通过下述方法得到：

产生随机数，所述随机数包括随机验证码及随机私钥，根据所述注册码以及随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名

私钥；

根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，利用所述服务器的公钥以及非对称加密函数计算加密密钥包；

将所述服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中。

鉴于以上内容，还有必要提出一种终端通信系统，其可以确保通信过程中的身份机密性、位置机密性以及不可跟踪性，从而保证用户的通信安全。

一种终端通信系统，应用于终端中，所述通信系统包括：

注册模块，用于向服务器发送入网注册请求，以执行终端在所述服务器中的注册，并接收所述服务器产生并传送的注册码；

会话密钥生成模块，用于向服务器发送会话密钥产生请求，接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码，并根据所述注册码、所述临时识别码以及所述终端产生的随机数产生会话私钥；及

通信模块，用于向所述服务器发送与第二终端通信的请求，接收所述服务器发送的会话公钥，并根据所述终端的会话私钥以及所述会话公钥获取所述第二终端的会话私钥，从而与所述第二终端进行安全通信。

本发明较佳实施例中，所述注册模块还用于：

接收所述服务器的数字证书；及

当验证所述服务器的数字证书合法时，存储所述注册码。

本发明较佳实施例中，所述的注册模块还用于：

通过加密函数，对所述终端的识别码以及代表所述终端身份的数据进行加密运算，其中，所述终端的识别码为所述终端的国际移动用户识别码，以及所述代表终端身份的数据包括所述终端的数字证书以及所述注册码。

本发明较佳实施例中，所述对所述终端的识别码以及代表所述终端身份的数据进行加密运算包括：

产生随机数，所述随机数包括随机验证码及随机私钥，根据所述注册码以及随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名私钥；

根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，利用所述服务器的公钥以及非对称加密函数计算加密密钥包；

将所述服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中。

本发明较佳实施例中，所述接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码，并根据所述注册码、临时识别码以及所述终端产生的随机数产生会话私钥包括：

将所述终端计算出来的加密信息包以及加密密钥包传送给所述服务器；

接收所述服务器根据所述终端的加密信息包以及加密密钥包产生的所述服务器的签名私钥以及所述服务器的加密信息包；

使用所述终端的随机私钥和对称解密函数解密所述服务器的加密信息包，得到识别码以及临时识别码；

使用验名函数和所述服务器的公钥，对所述服务器的签名私钥进行解密，得到所述注册码及随机验证码；

在解密得到的识别码与所述终端的识别码相同以及解密得到的随机验证码与所述终端产生的随机验证码相同时，根据所述注册码、随机验证码、随机私钥以及临时识别码生成所述终端的会话私钥。

本发明较佳实施例中，所述服务器的签名私钥以及服务器的加密信息包通过下述方法得到：

所述服务器在收到所述终端的加密信息包及加密密钥包后，使用非对称加密函数和所述服务器的私钥，对所述加密密钥包进行解密，以得到所述终端的随机私钥；

所述服务器使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书；

所述服务器利用所述认证中心的公钥，对所述终端的数字证书进行验证；

若所述终端的数字证书验证成功，则所述服务器使用验名函数和所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码；

所述服务器根据所述终端的注册码判断所述终端是否合法；

在所述终端合法时，所述服务器根据所述终端的识别码生成终端的临时识别码，并将所述终端的识别码与临时识别码相关联；

所述服务器根据所述注册码及随机验证码，利用所述服务器的私钥以及签名函数，计算所述服务器的签名私钥，以及根据所述服务器的签名私钥、所述

终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述服务器的加密信息包。

本发明较佳实施例中，所述服务器发送的会话公钥是将所述终端的会话私钥以及所述第二终端的会话私钥进行异或运算得到。

本发明较佳实施例中，所述根据所述终端的会话私钥以及所述会话公钥获取第二终端的会话私钥包括：

利用所述终端的会话私钥与所述会话公钥执行异或运算，得到所述第二终端的会话私钥。

一种终端通信系统，应用于服务器中，所述通信系统包括：

注册模块，用于接收终端发送的入网注册请求，根据所述入网注册请求生成随机的注册码，并将所述注册码发送给终端；

会话密钥生成模块，用于接收所述终端发送的会话密钥产生请求，向所述终端发送根据所述终端的识别码产生的临时识别码，以及根据所述注册码，所述终端产生并传送过来的随机数以及所述临时识别码生成所述终端的会话私钥；及

通信模块，用于接收终端发送的与第二终端通信的请求，向所述终端发送会话公钥，其中，所述会话公钥为所述终端以及所述第二终端的会话私钥通过异或运算得到。

本发明较佳实施例中，所述会话密钥生成模块还用于：

接收所述终端的加密信息包及加密密钥包；

使用非对称加密函数和所述服务器的私钥，对所述加密密钥包进行解密，

以得到所述终端的随机私钥；

使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书；

利用所述认证中心的公钥，对所述终端的数字证书进行验证；

若所述终端的数字证书验证成功，则所述服务器使用验名函数和所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码；

根据所述终端的注册码判断所述终端的合法性；

在所述终端合法时，根据所述终端的识别码生成所述终端的临时识别码，并将所述终端的识别码与临时识别码相关联；

根据所述注册码及随机验证码，利用所述服务器的私钥以及签名函数，计算所述服务器的签名私钥，以及根据所述服务器的签名私钥、所述终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述服务器的加密信息包；及

传送所述加密信息包给所述终端。

本发明较佳实施例中，所述终端的加密信息包及加密密钥包通过下述方法得到：

产生随机数，所述随机数包括随机验证码及随机私钥，根据所述注册码以及随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名私钥；

根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所

述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，利用所述服务器的公钥以及非对称加密函数计算加密密钥包；

将所述服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中。

相较于现有技术，在本发明中，每次的会话私钥都是由随机数所生成，窃听者无法通过多次比较获得任何通信的内容，保证了用户的不可跟踪性。即使某一次的会话私钥被窃取了，也无法继续获得以后的会话私钥，并可以有效防范重放攻击。

附图说明

图 1 所示是本发明终端通信方法较佳实施例的方法流程图。

图 2 所示是本发明终端通信方法较佳实施例的注册阶段的方法流程图。

图 3 所示是本发明所述终端通信方法较佳实施例的注册阶段的数据交互示例图。

图 4 及图 5 所示是本发明终端通信方法较佳实施例的会话私钥生成阶段的方法流程图。

图 6 所示是本发明所述终端通信方法较佳实施例的会话私钥生成阶段的数据交互示例图。

图 7 所示是本发明终端通信方法较佳实施例的安全通信阶段的方法流程图。

图 8 所示是本发明所述终端通信方法较佳实施例的安全通信阶段的示例

图。

图 9 所示是本发明终端通信系统较佳实施例的应用环境示意图。

图 10 所示是本发明终端的硬件架构图。

图 11 所示是本发明终端通信系统较佳实施例的功能模块图。

主要元件符号说明

终端	1
注册服务器	2
认证中心服务器	3
通信系统	10
通信单元	11
存储器	12
处理器	13
eSIM 卡	14
注册模块	100
会话密钥生成模块	101
通信模块	102

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明的一部分实施例，

而不是全部的实施例。

基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

下面首先对本发明所使用的一些函数和符号进行说明：

签名函数 SIGN-enc (message, key)，其表示为使用私钥 key 对消息 message 进行签名操作函数；

验名函数 SIGN-dec (message, key)，其表示为使用公钥 key 对消息 message 进行验名操作函数；

非对称加密函数 RSA-enc (message, key)，其表示为使用公钥 key 对消息 message 进行非对称加密操作函数；

非对称解密函数 RSA-dec (message, key)，其表示为使用私钥 key 对消息 message 进行非对称解密操作函数；

对称加密函数 AES-enc (message, key)，其表示为使用私钥 key 对消息 message 进行对称加密操作函数；

对称解密函数 AES-dec (message, key)，其表示为使用私钥 key 对消息 message 进行对称解密操作函数；

※符号表示和的意思，如 SIGN-enc (A ※ B, key)表示使用私钥 key 对 A 和 B 进行签名；

$\oplus$ 是数学运算符号，代表异或算法，如 $a \oplus b = (\neg a \wedge b) \vee (a \wedge \neg b)$ 中，如果 a、b 两个值不相同，则异或结果为 1；如果 a、b 两个值相同，异或结果为 0。

下面，请参考图 1，是本发明终端通信方法较佳实施例的方法流程图。根据不同的需求，本图所示流程中的执行顺序可以改变，某些可以省略。

本发明较佳实施例中，所述终端可以为移动通信设备，如手机等。所述终端安装有客户识别模块（Subscriber Identity Module，SIM）卡。本发明较佳实施例中，所述 SIM 卡为嵌入式用户身份模块（Embedded Subscriber Identity Module，eSIM）卡。

所述 eSIM 卡是将传统 SIM 卡直接嵌入到终端设备的芯片上，而不是作为独立的可移除零部件加入终端设备中，从而，允许用户以更加灵活的方式选择运营商套餐，或者在无需解锁终端设备、购买新终端设备的前提下随时更换运营商。

所述 eSIM 卡中存储有国际移动用户识别码（International Mobile Subscriber Identification Number，IMSI）。所述 IMSI 是为了在无线路径和整个全球移动通信系统（Global System for Mobile Communications，GSM）移动通信网络上正确地识别某个移动客户，而给移动客户分配的一个特定的识别码。

S1，终端向注册服务器发送入网注册请求，以执行在所述注册服务器中的注册。

在本发明较佳实施例中，所述注册服务器收到所述终端发送的入网注册请求后，根据所述入网注册请求会生成随机的注册码，并将所述注册码连同所述注册服务器的数字证书 CertRS 发送给所述终端。

在本发明较佳实施例中，所述 S1 还可包括：所述终端根据所述注册服

务器的数字证书 CertRS 验证所述注册服务器是否合法。

应该了解，所述数字证书就是互联网通信中标志通信各方身份信息的一串数字，提供了一种在 Internet 上验证通信实体身份的方式，由权威机构——认证（Certificate Authority，CA）中心发行的，可以在网上识别通信对方的身份。

在本发明较佳实施例中，所述终端通过利用所述认证中心的公钥，验证所述注册服务器的数字证书 CertRS 的真实性，来验证所述注册服务器是否合法。

在其他实施例中，所述 S1 还可包括：在验证所述注册服务器合法之后，所述终端进一步通过加密函数，对所述终端的识别码以及代表所述终端身份的数据进行加密运算。

在本实施例中，所述终端的识别码可以为所述终端的 IMSI，以及所述代表终端身份的数据可以为所述终端的数字证书以及所述注册服务器分配给所述终端的注册码。

所述 S1 的详细实施流程图可以参阅图 2 以及图 3 以及下述对图 2 以及图 3 的描述。

S2，所述终端向所述注册服务器发送会话密钥产生请求，并根据所述注册服务器传送过来的数据产生会话私钥，其中，所述会话私钥是根据所述注册服务器以及所述终端产生的随机数以及根据所述终端的识别码产生的临时识别码而生成的。

在本发明较佳实施例中，所述 S2 还包括：所述终端向所述注册服务器

发送会话密钥产生请求的同时，进一步将所述经过加密运算的终端的识别码以及代表所述终端身份的数据传送给所述注册服务器。

所述注册服务器通过对应的解密算法对所述终端的识别码以及所述代表终端身份的数据进行解密后，首先进行终端的身份认证操作，当根据所述代表终端身份的数据确定终端的用户身份合法后，会根据所述终端的识别码生成临时识别码，如临时移动用户识别码（Temporary Mobile Subscriber Identity, TMSI），其中，所述生成的 TMSI 与所述终端的 IMSI 是相关联的，并根据所述 TMSI 生成终端的会话私钥，并经过加密运算后，将所述会话私钥传送给所述终端。

所述 S2 的详细流程图可以参阅图 4 至图 6 以及下述对图 4 至图 6 的描述。

S3，所述终端向所述注册服务器发送与第二终端通信的请求，接收所述注册服务器发送的会话公钥，并根据所述终端的会话私钥以及所述会话公钥获取第二终端的会话私钥，从而与第二终端进行安全通信。

本发明较佳实施例中，当终端 A 与终端 B 进行通信时，所述终端 A 利用自己的会话私钥 TKA 从所述注册服务器获得终端 B 的会话私钥 TKB。同理，终端 B 用自己的会话私钥 TKB 可以获得终端 A 的会话私钥 TKA。于是，终端 A 与终端 B 就可以利用对方的会话私钥进行安全通信。

所述 S3 的详细流程图可以参阅图 7 以及图 8 以及下述对图 7 以及图 8 的描述。

参阅图 2 所示，是本发明终端的通信方法较佳实施例中的注册阶段的方

法流程图。根据不同的需求，本图所示流程图中的执行顺序可以改变，某些可以省略。

在图 1 所示的 S1 中，所述终端向所述注册服务器发送入网注册请求，以执行在所述注册服务器中的注册之后，S10，所述终端接收所述注册服务器传送过来的获取终端识别码的请求，以及接收所述注册服务器的数字证书以及随机的注册码。

S11，所述终端利用认证中心的公钥，验证所接收到的所述注册服务器的数字证书的真实性，并在 S12 中，判断所述注册服务器的数字证书是否验证成功。当所述注册服务器的数字证书验证不成功时，直接结束流程。

当所述注册服务器的数字证书验证成功时，执行 S13，所述终端产生随机验证码及随机私钥，并在 S14 中，根据所述注册码以及随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名私钥。

S15，所述终端根据所述终端的签名私钥、终端的识别码以及所述终端的数字证书，利用所述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，利用所述注册服务器的公钥以及非对称加密函数计算加密密钥包。

S16，所述终端将所述注册服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中，如所述终端的 eSIM 卡的安全区域中。

所述注册阶段的示例，请参阅如图 3 所示的示意图。

所述终端的注册过程，分为以下几个阶段：

- 1: 用户使用所述终端向所述注册服务器发送入网注册请求;
- 2: 所述注册服务器接收到入网注册请求后, 产生随机的注册码 RN1;
- 3: 服务器向终端发送请求获取终端 IMSI 的请求, 并将所述随机的注册码 RN1 和所述注册服务器的证书 CertRS 发送到所述终端中;
- 4: 所述终端使用认证中心的公钥验证所述注册服务器证书 CertRS 的真实性, 如果验证成功, 则产生随机验证码 RN2 和随机私钥 KRN; 否则, 若注册服务器证书 CertRS 验证不成功, 则结束此次流程;
- 5: 在所述注册服务器证书 CertRS 验证成功的前提下, 所述终端使用签名函数 $\text{SIGN-enc}(\text{message}, \text{key})$ 和终端私钥 SKsim 计算终端的签名函数 $\text{SignKsim} = \text{SIGN-enc}((\text{RN1} \times \text{RN2}), \text{SKsim})$; 使用对称加密函数 $\text{AES-enc}(\text{message}, \text{key})$ 和终端产生的随机私钥 KRN 计算终端的加密信息包 $\text{AKsim} = \text{AES-enc}((\text{SignKsim} \times \text{IMSI} \times \text{CertSIM}), \text{KRN})$; 以及使用非对称加密函数 $\text{RSA-enc}(\text{message}, \text{key})$ 和服务公钥 PKrs 计算终端的加密密钥包的 $\text{RKrs} = \text{RSA-enc}(\text{KRN}, \text{PKrs})$;
- 6: 所述终端将注册码 RN1、随机验证码 RN2、随机私钥 KRN 和所述注册服务器证书 CertRS 存储于所述终端的 eSIM 卡的安全区域中。

至此, 完成一个终端的注册过程。应该可以理解, 其他终端的注册过程与上述描述过程相同。

参阅图 4 及图 5 所示, 是本发明终端通信方法较佳实施例中会话私钥生成阶段的方法流程图。根据不同的需求, 本图所示流程图中的执行顺序可以改变, 某些可以省略。

参阅图 4 所示：

S20，所述终端向所述注册服务器发送会话密钥产生请求，并将所述终端的加密信息包以及加密密钥包发送给所述注册服务器。

S21，所述注册服务器使用非对称加密函数和服务器的私钥，对所述加密密钥包进行解密，以得到所述终端的随机私钥。

S22，所述注册服务器使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书。

S23，所述注册服务器利用所述认证中心的公钥，验证所述终端的数字证书是否真实，并在 S24 中，判断所述终端的数字证书是否验证成功。若终端的数字证书验证不成功，则直接结束流程。

若所述终端的数字证书验证成功，则执行 S25，所述注册服务器向所述认证中心获取所述终端的公钥。

S26，所述注册服务器使用签名函数和所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码。

S27，所述注册服务器进一步根据所述终端的注册码判断所述终端的合法性，并于 S28 中，判断所述终端是否合法。

若所述注册码并不是所述注册服务器发送的，则所述终端不合法，此时直接结束流程。

若所述注册码是所述注册服务器发送的，则所述终端合法，执行下述的图 5 中的 S29。

参阅图 5 所示：

S29，所述注册服务器根据所述终端的识别码生成终端的临时识别码，并将所述终端识别码与临时识别码相关联，并将所述临时识别码及所述随机验证码存储于所述注册服务器中。

S30，所述注册服务器根据所述注册码及随机验证码，利用所述注册服务器私钥以及签名函数，计算所述注册服务器的签名私钥，根据所述所述注册服务器的签名私钥、所述终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述注册服务器的加密信息包。

S31，所述注册服务器将所述注册服务器的签名私钥以及所述注册服务器的加密信息包传送给所述终端，并根据所述注册码、随机验证码、随机私钥以及临时识别码生成所述终端的会话私钥。

S32，所述终端使用终端的随机私钥和对称解密函数解密所述注册服务器的加密信息包，得到所述注册服务器的签名私钥、所述终端的识别码以及临时识别码。

S33，所述终端使用验名函数和所述注册服务器的公钥，对所述注册服务器的签名私钥进行解密，得到所述注册码及随机验证码。

S34，所述终端根据所述解密得到的识别码以及随机验证码判断所述注册服务器的合法性，并于 S35 中，判断所述注册服务器是否合法。当解密得到的识别码以及随机验证码与所述终端的识别码以及随机验证码不匹配时，所述注册服务器不合法，直接结束流程。

当解密得到的识别码以及随机验证码与所述终端的识别码以及随机验

证码都匹配时，所述注册服务器合法，执行 S36，所述终端根据所述注册码、随机验证码、随机私钥以及临时识别码生成会话私钥。

至此，完成一个终端的会话私钥生成操作。应该理解，其他终端的会话私钥生成操作采用上述描述的相同流程执行。

所述会话私钥生成阶段的示例，请参阅图 6 所示的示意图。

如图 6 所示，生成会话私钥的过程可以分为以下几个阶段：

1：所述终端向所述注册服务器发送生成会话密钥请求，并将 AKsim 和 RKrs 发送给所述注册服务器；

2：所述注册服务器使用非对称解密函数 RSA-dec (message , key)和所述注册服务器私钥 SKrs 计算终端的随机私钥 $KRN = \text{RSA-dec}(\text{RKrs}, \text{SKrs})$ ；使用对称解密函数 AES-dec (message, key)和终端生成的随机私钥 KRN 计算终端的密钥包 $\text{SignKsim} \times \text{IMSI} \times \text{CertSIM} = \text{AES-dec}(\text{AKsim}, \text{KRN})$ ；

3：所述注册服务器使用认证中心 CA 的公钥验证所述终端的数字证书 CertSIM 的真实性，如果验证成功，向认证中心 CA 获取所述终端的公钥 PKsim，否则，若验证不成功，则结束此次流程；

4：在所述终端的数字证书 CertSIM 验证成功后，所述注册服务器使用验名函数 SIGN-dec (message, key)和终端公钥 PKsim 计算注册码 RN1 和随机验证码 RN2： $\text{RN1} \times \text{RN2} = \text{SIGN-dec}(\text{SignKsim}, \text{PKsim})$ ；

5：所述注册服务器判断上述解密出来的注册码 RN1 的真实性，如果验证成功，所述注册服务器就根据所述终端的国际移动用户识别码 IMSI 产生临时移动用户识别码 TMSI,且将所述 TMSI 与 IMSI 相关联,进一步,将 TMSI

和随机验证码 RN2 存储于所述注册服务器中；如果 RN1 的真实性验证失败，就结束此次流程；

6：在解密出来的注册码 RN1 验证成功后，所述注册服务器使用签名函数 SIGN-enc (message, key)和所述注册服务器私钥 SKrs 计算 SignKrs = SIGN-enc (RN1 ※ RN2 , SKrs)；使用对称加密函数 AES-enc (message, key)和所述终端生成的随机私钥 KRN 计算 AKrs = AES-enc ((SignKrs ※ IMSI ※ TMSI), KRN)。

7：所述注册服务器将 SignKrs 和 AKrs 发送给所述终端，并且所述注册服务器生成所述终端的会话私钥 $TK = RN1 \oplus RN2 \oplus KRN \oplus TMSI$ 。

8：所述终端使用对称解密函数 AES-dec (message, key)和所述终端生成的随机私钥 KRN 计算密钥包：SignKrs ※ IMSI ※ TMSI = AES-dec (AKrs, KRN)；使用验名函数 SIGN-dec (message, key)和所述注册服务器公钥 PKrs 计算 $RN1 \times RN2 = SIGN-dec (SignKrs, PKrs)$ 。

9：所述终端判断上述解密出来的 RN2 和 IMSI 的真实性，如果 RN2 和 IMSI 验证成功，则产生会话私钥 $TK = RN1 \oplus RN2 \oplus KRN \oplus TMSI$ ，否则，若 RN2 和 IMSI 验证不成功，则结束此次流程。

参阅图 7 所示，是本发明终端通信方法较佳实施例中安全通信阶段的方法流程图。根据不同的需求，本图所示流程图中的执行顺序可以改变，某些可以省略。

S40，第一终端向注册服务器发送与第二终端通话的请求。

S41，接收所述注册服务器传送的会话公钥，并根据所述第一终端的会

话私钥以及所述会话公钥获取所述第二终端的会话私钥。

S42, 所述第一终端通过所述第二终端的会话私钥与所述第二终端进行安全通信。

所述安全通信阶段的示例, 请参阅图 8 所示的示意图。

所述安全通信过程可以分为以下几个阶段:

1: 在所述第一终端与所述第二终端通话时, 所述注册服务器生成会话公钥 $TKC = TKA \oplus TKB$;

2: 所述第一终端用自己的私钥 TKA 可以获得所述第二终端的会话私钥 $TKB = TKC \oplus TKA$;

3: 所述第二终端用自己的私钥 TKB 可以获得所述第一终端的会话私钥 $TKA = TKC \oplus TKB$;

4: 所述第一终端与所述第二终端利用对方的会话私钥执行安全通信。

根据上述描述的方法流程图以及示例图可以看出, 本发明可包括用户注册、生成会话私钥和安全通信三个阶段。首先, 用户使用包括有 eSIM 卡的终端对注册服务器发送入网注册请求, 所述注册服务器会生成随机数, 并发送给 eSIM 卡终端, eSIM 卡终端会验证所述注册服务器证书的真实性, 当验证成功时, 会随机生成相关的密钥并存储在自己的安全区域中。然后 eSIM 卡终端再向所述注册服务器发送生成会话密钥产生请求, 所述注册服务器在经过复杂的加解密和身份认证操作后, 当确定用户身份合法后, 会生成临时移动用户识别码 TMSI 和根据所述 TMSI 生成会话私钥 TK, 其中所述 TMSI 与 eSIM 卡终端的国际移动用户识别码 IMSI 是相关联的, 每次临时移动用户

识别码 TMSI 和会话私钥 TK 都是变化的。最后，当一个第一终端与一个第二终端进行通信时，所述注册服务器会生成所述第一终端和第二终端的会话公钥 TKC，所述第一终端用自己的私钥 TKA 可以获得所述第二终端的会话私钥。同理，所述第二终端用自己的私钥 TKB 可以获得所述第一终端的会话私钥。这样所述第一终端与所述第二终端就可以利用对方的会话私钥进行安全通信。

对本发明方法的安全性进行分析：

在本发明的方法中，对 eSIM 卡终端的 IMSI 进行了加密，用户身份是以密文方式在网络中传输。当用户在获取了 TMSI 之后，通过保存在所述注册服务器中的 IMSI 与 TMSI 的关联对用户身份进行识别，因此窃听者无法获知用户的身份，保证用户身份的机密性。

在本发明的方法中，每次的会话私钥都是根据随机数 RN1、RN2、KRN 和临时移动用户识别码 TMSI 所生成，窃听者无法通过多次比较获得任何通信的内容，这样就保证了用户的不可跟踪性。即使某一次的会话私钥被窃取了，也无法继续获得以后的会话私钥，因为每次随机数 RN1、RN2、KRN 和临时移动用户识别码 TMSI 都重新生成。

使用本发明的方法，即使攻击者事先获得 CertSIM，RN1，RN2 和 SignKsim，但是对于新的随机数 RN1 无法生成对应的新的 SignKsim，因此本方法可以有效抗重放攻击。

以上所述，仅是本发明的具体实施方式，但本发明的保护范围并不局限于此，对于本领域的普通技术人员来说，在不脱离本发明创造构思的前提下，

还可以做出改进，但这些均属于本发明的保护范围。

上述图 1 至图 8 详细介绍了本发明的终端的注册方法、会话密钥生成方法以及安全通信方法，下面结合第 9~11 图，分别对实现上述终端的通信方法的硬件系统架构以及实现所述终端的通信方法的软件系统的功能模块进行介绍。

应该了解，所述实施例仅为说明之用，在专利申请范围上并不受此结构的限制。

如图 9 所示，为本发明实现所述终端的通信方法较佳实施例的硬件系统架构图。

在本发明的其中一个较佳实施例中，所述终端的通信方法的实现由两大部分构成：

一、多台终端

终端 1 可以为移动通信设备，如手机等。所述终端 1 安装有客户识别模块（Subscriber Identity Module，SIM）卡。本发明较佳实施例中，所述 SIM 卡为 eSIM 卡 14。

所述 eSIM 卡 14 是将传统 SIM 卡直接嵌入到终端 1 的芯片上，而不是作为独立的可移除零部件加入终端 1 中，从而，允许用户以更加灵活的方式选择运营商套餐，或者在无需解锁终端 1、购买新终端 1 的前提下随时更换运营商。

所述 eSIM 卡 14 中存储有国际移动用户识别码（International Mobile Subscriber Identification Number，IMSI）。所述 IMSI 是为了在无线路径和整

个全球移动通信系统（Global System for Mobile Communications, GSM）移动通信网络上正确地识别某个移动客户，而给移动客户分配的一个特定的识别码。所述 IMSI 的总长度不超过 15 位，同样使用 0~9 的数字，其中 MCC 是移动用户所属国家代号，占 3 位数字，中国的 MCC 规定为 460；MNC 是移动网号码，由两位或者三位数字组成，中国移动的移动网络编码（MNC）为 00；用于识别移动用户所归属的移动通信网；MSIN 是移动用户识别码，用以识别某一移动通信网中的移动用户。

如图 10 所示，所述终端 1 还包括通信系统 10、通信单元 11、存储器 12 以及处理器 13。应该了解，所述终端 1 也可以包括其他硬件或者软件，例如，显示屏幕、摄像头、控制电路等，而并不限制于上述列举的部件。

所述通信单元 11 用于所述终端 1 与其他设备，如其他终端 1 或者服务器之间的信息交换。

所述通信单元 11 可以是无线通信模块，包括 Wi-Fi 模块，WiMax（World Interoperability for Microwave Access，即全球微波接入互操作性）模块，GSM（Global System for Mobile Communication，全球移动通信系统）模块，CDMA（Code Division Multiple Access，码分多址）模块，包括 CDMA2000，CDMA，CDMA2000 1x evdo，WCDMA，TD-SCDMA 等等），LTE（Long Term Evolution，长期演进）模块，HiperLAN（high-performance radio local area network，高性能无线局域网）模块、以及短距离无线传输模块，如蓝牙、Zigbee、RF 等等。

所述存储器 12 用于存储程序和各种数据，并在所述终端 1 运行过程中

实现高速、自动地完成程序或数据的存取。所述存储器 12 可以是终端 1 的外部存储器和/或内部存储器。进一步地，所述存储器 12 可以是集成电路中没有实物形式的具有存储功能的电路，如 RAM（Random-Access Memory，随机存取存储器）、FIFO（First In First Out，）等。或者，所述存储器 12 也可以是具有实物形式的存储设备，如内存条、TF 卡（Trans-flash Card）等等。

所述处理器 13 又称中央处理器（CPU，Central Processing Unit），是一块超大规模的集成电路，是终端 1 的运算核心（Core）和控制核心（Control Unit）。处理器 11 的功能主要是解释程序指令以及处理软件中的数据。

所述通信系统 10 可以包括多个由程序段所组成的功能模块（详见图 11）。所述通信系统 10 中的各个程序段的程序代码可以存储于所述存储器 12 中，并由所述处理器 13 所执行，以执行与其他终端 1 的安全通信等操作（详见图 11 中描述）。

二、服务器

本发明较佳实施例中，所述服务器可以包括注册服务器 2 以及认证（Certificate Authority，CA）服务器 3。

其中，所述 CA 服务器 3 是权威机构——CA 中心的服务器，用于执行数字证书的发放、管理、取消等操作。所述 CA 服务器 3 可以检查终端 1 以及注册服务器 2 的身份合法性，并签发数字证书（用数学方法在证书上签字）给终端 1 以及注册服务器 2，并可以鉴定所述终端 1 以及注册服务器 2 的数字证书的合法性。

在本发明较佳实施例中，所述注册服务器 2 也包括所述通信系统 10，用于接受各个终端 1 的注册，并实现各个终端 1 之间的安全通信。详细地，所述注册服务器 2 接受终端 1 的入网注册请求，随机地生成所述终端 1 的注册码，并根据终端 1 及注册服务器 2 产生的注册码等随机数为终端 1 生成并分配会话私钥，并在两个终端 1 之间进行通信时，生成两个终端 1 的会话公钥，以便每个终端 1 可以根据所述会话公钥获取对方的会话私钥，以利用对方的会话私钥执行两个终端 1 之间的安全通信。

参阅图 10 所示，为本发明终端通信较佳实施例的功能模块图。本实施例中，所述通信系统 10 根据其所执行的功能，可以被划分为多个功能模块。本实施例中，所述功能模块包括：注册模块 100、会话密钥生成模块 101 及通信模块 102。

所述注册模块 100 用于向注册服务器（下称：服务器）2 发送入网注册请求，并接收所述服务器传送的注册码，并在验证所述服务器合法之后，存储所述注册码。

本发明较佳实施例中，所述注册模块 100 向注册服务器 2 发送入网注册请求后，会接收到所述注册服务器 2 传送过来的获取终端 1 的识别码的请求，以及接收到所述注册服务器 2 的数字证书以及注册码；进一步，所述注册模块 100 利用认证中心的公钥，验证所接收到的注册服务器 2 的数字证书的真实性，当所述注册服务器 2 的数字证书验证成功时，所述注册模块 100 产生随机验证码及随机私钥，并根据所述注册码、所述随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名私钥；进一步地，所述注册模

块 100 根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，利用所述注册服务器 2 的公钥以及非对称加密函数计算加密密钥包，并存储所述注册服务器 2 的数字证书、注册码、随机验证码及随机私钥于终端 1 的安全存储区域中，如所述终端 1 的 eSIM 卡 14 的安全区域中。

所述会话密钥生成模块 101 用于向注册服务器 2 发送会话密钥产生请求，并接收所述注册服务器 2 传送过来的会话私钥。

详细地，所述会话密钥生成模块 101 将所述终端 1 的加密信息包及加密密钥包发送给注册服务器 2，并接收所述注册服务器 2 的签名私钥以及注册服务器 2 的加密信息包，使用终端 1 的随机私钥和对称解密函数解密所述注册服务器 2 的加密信息包，得到终端识别码以及临时识别码，使用验名函数和所述注册服务器 2 的公钥，对所述注册服务器 2 的签名私钥进行解密，得到所述注册码及随机验证码，根据所述解密得到的识别码以及随机验证码判断所述注册服务器 2 的合法性，并在解密得到的识别码以及随机验证码与所述终端 1 的识别码以及随机验证码都匹配时，根据所述注册码、随机验证码、随机私钥以及临时识别码生成所述终端 1 的会话私钥。

本发明较佳实施例中，所述注册服务器 2 在收到终端 1 的加密信息包及加密密钥包后，使用非对称加密函数和注册服务器 2 的私钥，对所述加密密钥包进行解密，以得到所述终端 1 的随机私钥，使用对称加密函数和所述终端 1 的随机私钥，对所述加密信息包进行解密，以得到所述终端 1 的签名私钥、终端 1 的识别码以及终端 1 的数字证书，并利用所述认证服务器 3 的公

钥，验证所述终端 1 的数字证书是否真实；若所述终端 1 的数字证书验证成功，则使用验名函数和所述终端 1 的公钥，对所述终端 1 的签名私钥进行解密，得到所述终端 1 的注册码及随机验证码，进一步根据所述终端 1 的注册码判断所述终端 1 是否合法，在所述终端 1 合法时，根据所述终端 1 的识别码生成终端 1 的临时识别码，将所述终端 1 的识别码与临时识别码相关联，并根据所述注册码及随机验证码，利用服务器私钥以及签名函数，计算服务器的签名私钥，以及根据所述注册服务器 2 的签名私钥、所述终端 1 的识别码以及临时识别码，利用所述终端 1 的随机私钥以及对称加密函数，计算所述注册服务器 2 的加密信息包。

进一步地，所述注册服务器 2 还会根据所述注册码、随机验证码、随机私钥以及临时识别码生成所述终端 1 的会话私钥。

所述通信模块 102 用于向注册服务器 2 发送与第二终端通信的请求，接收所述注册服务器 2 发送的会话公钥，并根据所述会话公钥获取第二终端的会话私钥，从而与第二终端进行安全通信。

详细地，在第一终端 1 与第二终端 1 通话时，注册服务器 2 生成会话公钥 $TKC = TKA \oplus TKB$ ；第一终端 1 用自己的私钥 TKA 可以获得第二终端 1 的会话私钥 $TKB = TKC \oplus TKA$ ，以及第二终端 1 用自己的私钥 TKB 也可以获得第一终端 1 的会话私钥 $TKA = TKC \oplus TKB$ ，于是第一终端 1 与第二终端 1 就可以利用对方的会话私钥执行安全通信。

在本发明所提供的几个实施例中，应该理解到，所揭露的系统，终端和

方法，可以通过其它的方式实现。例如，以上所描述的终端实施例仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

另外，在本发明各个实施例中的各功能模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能模块的形式实现。

上述以软件功能模块的形式实现的集成的单元，可以存储在计算机可读取存储介质中。上述软件功能模块存储在存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明各个实施例所述方法的部分。

对于本领域技术人员而言，显然本发明不限于上述示范性实施例的细节，而且在不背离本发明的精神或基本特征的情况下，能够以其他的具体形式实现本发明。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本发明的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本发明内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。此外，显然“包括”一词不排除其他单元或，单数不排除复数。系统权利要求中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

最后应说明的是，以上实施例仅用以说明本发明的技术方案而非限制，

尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或等同替换，而不脱离本发明技术方案的精神和范围。

权 利 要 求 书

1. 一种终端通信方法，应用于终端中，其特征在于，所述终端通信方法包括：

向服务器发送入网注册请求，以执行终端在所述服务器中的注册，并接收所述服务器产生并传送的注册码；

向所述服务器发送会话密钥产生请求，接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码，并根据所述注册码、所述临时识别码以及所述终端产生的随机数产生会话私钥；及

向所述服务器发送与第二终端通信的请求，接收所述服务器发送的会话公钥，并根据所述终端的会话私钥以及所述会话公钥获取所述第二终端的会话私钥，从而与所述第二终端进行安全通信。

2. 如权利要求 1 所述的终端通信方法，其特征在于，所述执行终端在所述服务器中的注册包括：

接收所述服务器的数字证书；及

当验证所述服务器的数字证书合法时，存储所述注册码。

3. 如权利要求 2 所述的终端通信方法，其特征在于，所述向所述服务器发送会话密钥产生请求之前还包括：

通过加密函数，对所述终端的识别码以及代表所述终端身份的数据进行加密运算，其中，所述终端的识别码为所述终端的国际移动用户识别码，以及所述代表终端身份的数据包括所述终端的数字证书以及所述注册码。

4. 如权利要求 3 所述的终端通信方法，其特征在于，所述对所述终端的识别码以及代表所述终端身份的数据进行加密运算包括：

产生随机数，所述随机数包括随机验证码及随机私钥，根据所述注册码以及所述随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名私钥；

根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，利用所述服务器的公钥以及非对称加密函数计算加密密钥包；

将所述服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中。

5. 如权利要求 4 所述的终端通信方法，其特征在于，所述接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码，并根据所述注册码、临时识别码以及所述终端产生的随机数产生会话私钥包括：

将所述终端计算出来的加密信息包以及加密密钥包传送给所述服务器；

接收所述服务器根据所述终端的加密信息包以及加密密钥包产生的所述服务器的签名私钥以及所述服务器的加密信息包；

使用所述终端的随机私钥和对称解密函数解密所述服务器的加密信息包，得到识别码以及临时识别码；

使用验名函数和所述服务器的公钥，对所述服务器的签名私钥进行解密，得到注册码及随机验证码；

在解密得到的识别码与所述终端的识别码相同以及解密得到的随机验证

码与所述终端产生的随机验证码相同时，根据所述注册码、随机验证码、随机私钥以及临时识别码生成所述终端的会话私钥。

6. 如权利要求 5 所述的终端通信方法，其特征在于，所述服务器的签名私钥以及服务器的加密信息包通过下述方法得到：

所述服务器在收到所述终端的加密信息包及加密密钥包后，使用非对称加密函数和所述服务器的私钥，对所述加密密钥包进行解密，以得到所述终端的随机私钥；

所述服务器使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书；

所述服务器利用认证中心的公钥，验证所述终端的数字证书；

若所述终端的数字证书验证成功，则所述服务器使用签名函数及所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码；

所述服务器根据所述终端的注册码判断所述终端是否合法；

在所述终端合法时，所述服务器根据所述终端的识别码生成终端的临时识别码，并将所述终端的识别码与临时识别码相关联；

所述服务器根据所述注册码及随机验证码，利用所述服务器的私钥以及签名函数，计算所述服务器的签名私钥，以及根据所述服务器的签名私钥、所述终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述服务器的加密信息包。

7. 如权利要求 1 所述的终端通信方法，其特征在于，所述服务器发送的会

话公钥是将所述终端的会话私钥以及所述第二终端的会话私钥进行异或运算得到。

8. 如权利要求 7 所述的终端通信方法, 其特征在于, 所述根据所述终端的会话私钥以及所述会话公钥获取第二终端的会话私钥包括:

利用所述终端的会话私钥与所述会话公钥执行异或运算, 得到所述第二终端的会话私钥。

9. 一种终端通信系统, 应用于终端中, 其特征在于, 所述终端通信系统包括:

注册模块, 用于向服务器发送入网注册请求, 以执行终端在所述服务器中的注册, 并接收所述服务器产生并传送的注册码;

会话密钥生成模块, 用于向服务器发送会话密钥产生请求, 接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码, 并根据所述注册码、所述临时识别码以及所述终端产生的随机数产生会话私钥; 及

通信模块, 用于向所述服务器发送与第二终端通信的请求, 接收所述服务器发送的会话公钥, 并根据所述终端的会话私钥以及所述会话公钥获取所述第二终端的会话私钥, 从而与所述第二终端进行安全通信。

10. 如权利要求 9 所述的终端通信系统, 其特征在于, 所述注册模块还用于: 接收所述服务器的数字证书; 及

当验证所述服务器的数字证书合法时, 存储所述注册码。

11. 如权利要求 10 所述的终端通信系统, 其特征在于, 所述的注册模块还用于:

通过加密函数，对所述终端的识别码以及代表所述终端身份的数据进行加密运算，其中，所述终端的识别码为所述终端的国际移动用户识别码，以及所述代表终端身份的数据包括所述终端的数字证书以及所述注册码。

12.如权利要求 11 所述的终端通信系统，其特征在于，所述对所述终端的识别码以及代表所述终端身份的数据进行加密运算包括：

产生随机数，所述随机数包括随机验证码及随机私钥，根据所述注册码以及所述随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名私钥；

根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所述随机私钥以及对称加密函数，计算出加密信息包，以及根据所述随机私钥，利用所述服务器的公钥以及非对称加密函数计算加密密钥包；

将所述服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中。

13.如权利要求 12 所述的终端通信系统，其特征在于，所述接收所述服务器产生并传送的根据所述终端的识别码生成的临时识别码，并根据所述注册码、临时识别码以及所述终端产生的随机数产生会话私钥包括：

将所述终端计算出来的加密信息包以及加密密钥包传送给所述服务器；

接收所述服务器根据所述终端的加密信息包以及加密密钥包产生的所述服务器的签名私钥以及所述服务器的加密信息包；

使用所述终端的随机私钥和对称解密函数解密所述服务器的加密信息包，得到识别码以及临时识别码；

使用验名函数和所述服务器的公钥，对所述服务器的签名私钥进行解密，得到注册码及随机验证码；

在解密得到的识别码与所述终端的识别码相同以及解密得到的随机验证码与所述终端产生的随机验证码相同时，根据所述注册码、随机验证码、随机私钥以及临时识别码生成所述终端的会话私钥。

14.如权利要求 13 所述的终端通信系统，其特征在于，所述服务器的签名私钥以及服务器的加密信息包通过下述方法得到：

所述服务器在收到所述终端的加密信息包及加密密钥包后，使用非对称加密函数和所述服务器的私钥，对所述加密密钥包进行解密，以得到所述终端的随机私钥；

所述服务器使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书；

所述服务器利用所述认证中心的公钥，对所述终端的数字证书进行验证；

若所述终端的数字证书验证成功，则所述服务器使用验名函数和所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码；

所述服务器根据所述终端的注册码判断所述终端是否合法；

在所述终端合法时，所述服务器根据所述终端的识别码生成终端的临时识别码，并将所述终端的识别码与临时识别码相关联；

所述服务器根据所述注册码及随机验证码，利用所述服务器的私钥以及签名函数，计算所述服务器的签名私钥，以及根据所述服务器的签名私钥、所述

终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述服务器的加密信息包。

15.如权利要求 9 所述的终端通信系统，其特征在于，所述服务器发送的会话公钥是将所述终端的会话私钥以及所述第二终端的会话私钥进行异或运算得到。

16.如权利要求 15 所述的终端通信系统，其特征在于，所述根据所述终端的会话私钥以及所述会话公钥获取第二终端的会话私钥包括：

利用所述终端的会话私钥与所述会话公钥执行异或运算，得到所述第二终端的会话私钥。

17.一种终端通信方法，应用于服务器中，其特征在于，所述终端通信方法包括：

接收终端发送的入网注册请求，根据所述入网注册请求生成随机的注册码，并将所述注册码发送给所述终端；

接收所述终端发送的会话密钥产生请求，向所述终端发送根据所述终端的识别码产生的临时识别码，以及根据所述注册码，所述终端产生并传送的随机数以及所述临时识别码生成所述终端的会话私钥；及

接收所述终端发送的与第二终端通信的请求，向所述终端发送会话公钥，其中，所述会话公钥为根据所述终端以及所述第二终端的会话私钥通过异或运算得到。

18. 如权利要求 17 所述的终端通信方法，其特征在于，所述终端通信方法还包括产生所述临时识别码的步骤：

接收所述终端的加密信息包及加密密钥包；

使用非对称加密函数和所述服务器的私钥，对所述加密密钥包进行解密，以得到所述终端的随机私钥；

使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书；

利用认证中心的公钥，验证所述终端的数字证书；

若所述终端的数字证书验证成功，则所述服务器使用签名函数和所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码；

根据所述终端的注册码判断所述终端的合法性；

在所述终端合法时，根据所述终端的识别码生成所述终端的临时识别码，并将所述终端的识别码与临时识别码相关联；

根据所述注册码及随机验证码，利用所述服务器的私钥以及签名函数，计算所述服务器的签名私钥，以及根据所述服务器的签名私钥、所述终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述服务器的加密信息包；及

传送所述加密信息包给所述终端。

19.如权利要求 18 所述的终端通信方法，其特征在于，所述终端的加密信息包及加密密钥包通过下述方法得到：

产生随机数，所述随机数包括随机验证码及随机私钥，根据所述注册码以及随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名

私钥；

根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，利用所述服务器的公钥以及非对称加密函数计算加密密钥包；

将所述服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中。

20.一种终端通信系统，应用于服务器中，其特征在于，所述通信系统包括：

注册模块，用于接收终端发送的入网注册请求，根据所述入网注册请求生成随机的注册码，并将所述注册码发送给终端；

会话密钥生成模块，用于接收所述终端发送的会话密钥产生请求，向所述终端发送根据所述终端的识别码产生的临时识别码，以及根据所述注册码，所述终端产生并传送过来的随机数以及所述临时识别码生成所述终端的会话私钥；及

通信模块，用于接收终端发送的与第二终端通信的请求，向所述终端发送会话公钥，其中，所述会话公钥为所述终端以及所述第二终端的会话私钥通过异或运算得到。

21. 如权利要求 20 所述的终端通信系统，其特征在于，所述会话密钥生成模块还用于：

接收所述终端的加密信息包及加密密钥包；

使用非对称加密函数和所述服务器的私钥，对所述加密密钥包进行解密，以得到所述终端的随机私钥；

使用对称加密函数和所述终端的随机私钥，对所述加密信息包进行解密，以得到所述终端的签名私钥、终端的识别码以及终端的数字证书；

利用所述认证中心的公钥，对所述终端的数字证书进行验证；

若所述终端的数字证书验证成功，则所述服务器使用签名函数和所述终端的公钥，对所述终端的签名私钥进行解密，得到所述终端的注册码及随机验证码；

根据所述终端的注册码判断所述终端的合法性；

在所述终端合法时，根据所述终端的识别码生成所述终端的临时识别码，并将所述终端的识别码与临时识别码相关联；

根据所述注册码及随机验证码，利用所述服务器的私钥以及签名函数，计算所述服务器的签名私钥，以及根据所述服务器的签名私钥、所述终端的识别码以及临时识别码，利用所述终端的随机私钥以及对称加密函数，计算所述服务器的加密信息包；及

传送所述加密信息包给所述终端。

22.如权利要求 21 所述的终端通信方法，其特征在于，所述终端的加密信息包及加密密钥包通过下述方法得到：

产生随机数，所述随机数包括随机验证码及随机私钥，根据所述注册码以及随机验证码，利用所述终端的私钥以及签名函数，生成所述终端的签名私钥；

根据所述终端的签名私钥、终端的识别码以及终端的数字证书，利用所述随机私钥以及对称加密函数，计算加密信息包，以及根据所述随机私钥，

利用所述服务器的公钥以及非对称加密函数计算加密密钥包；

将所述服务器的数字证书、注册码、随机验证码及随机私钥存储于所述终端的安全存储区域中。

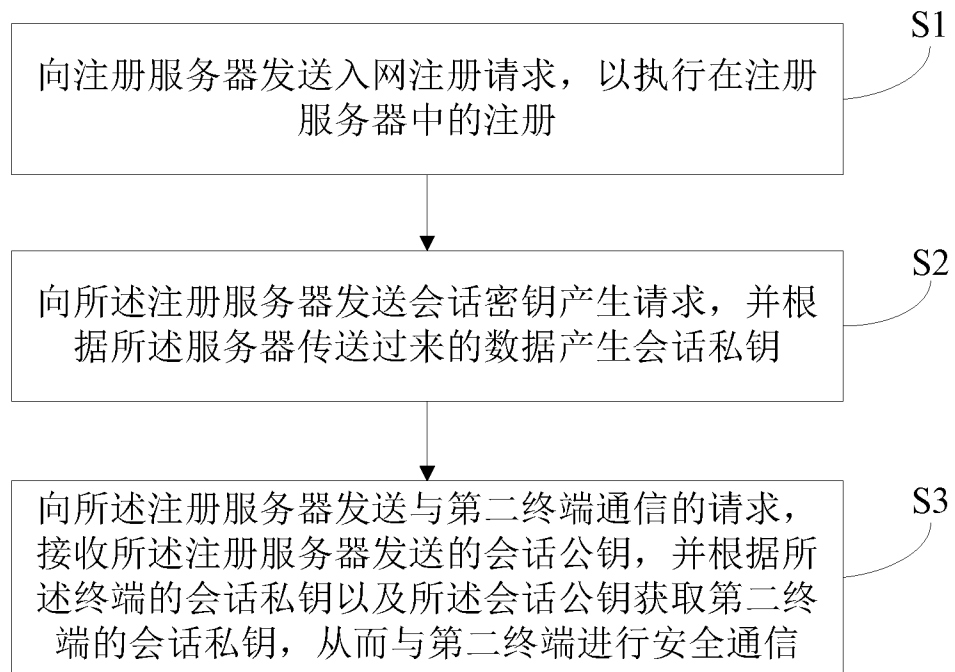


图 1

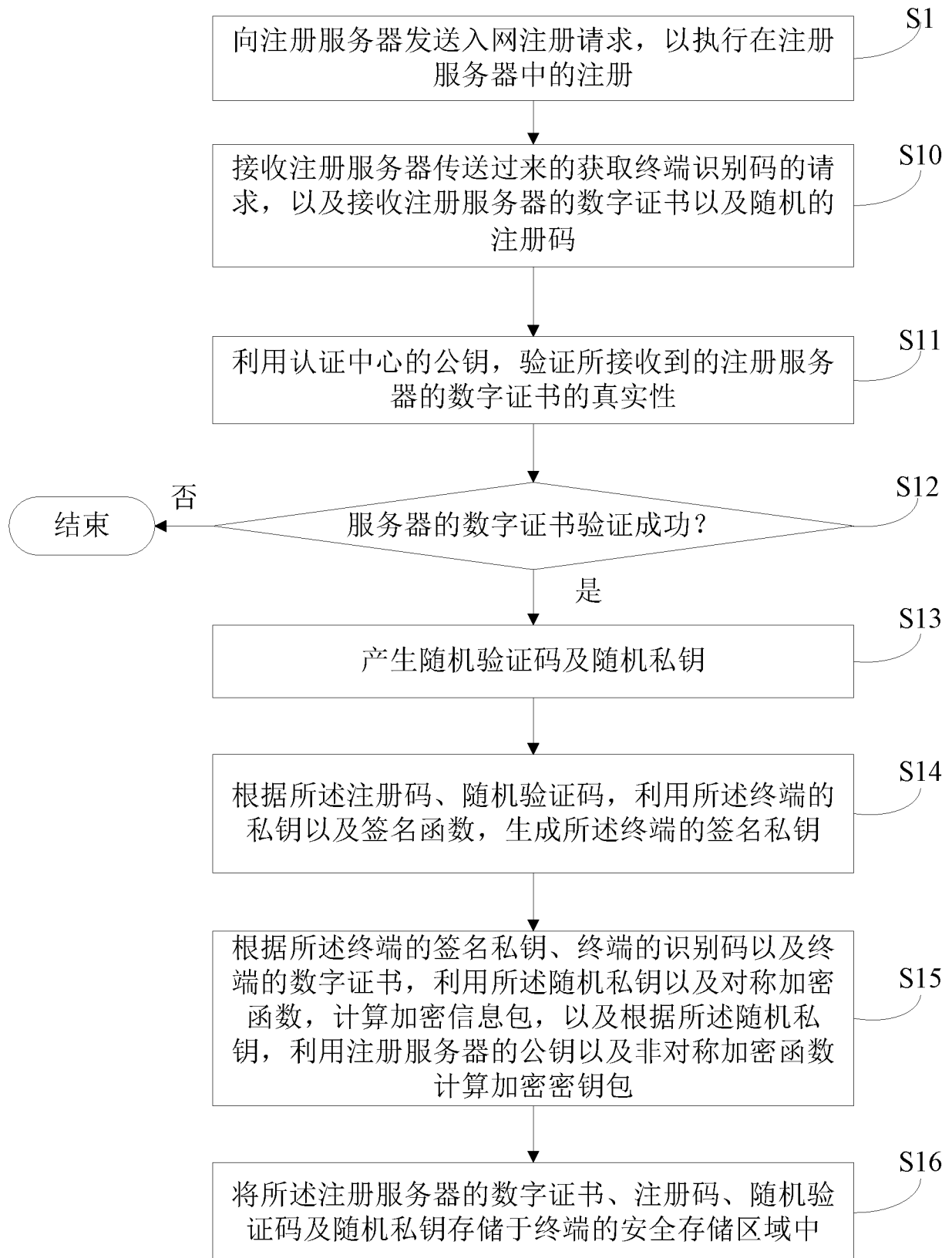


图 2

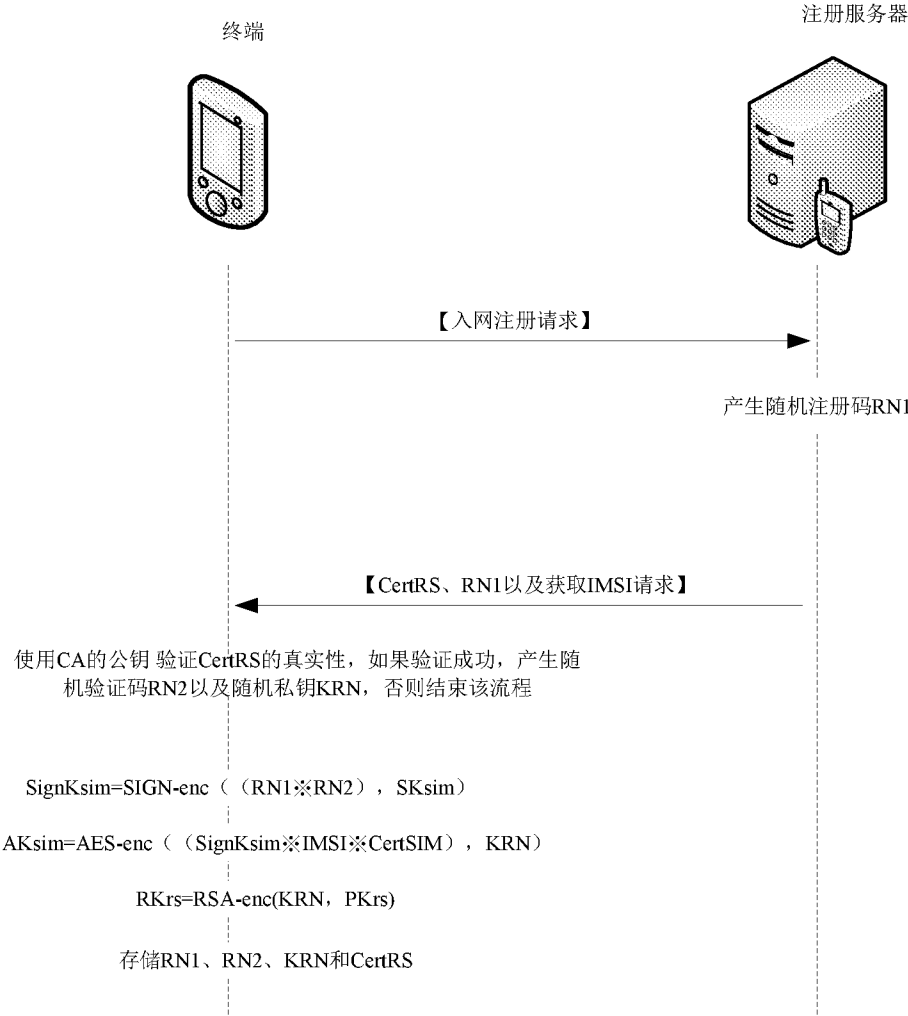


图 3

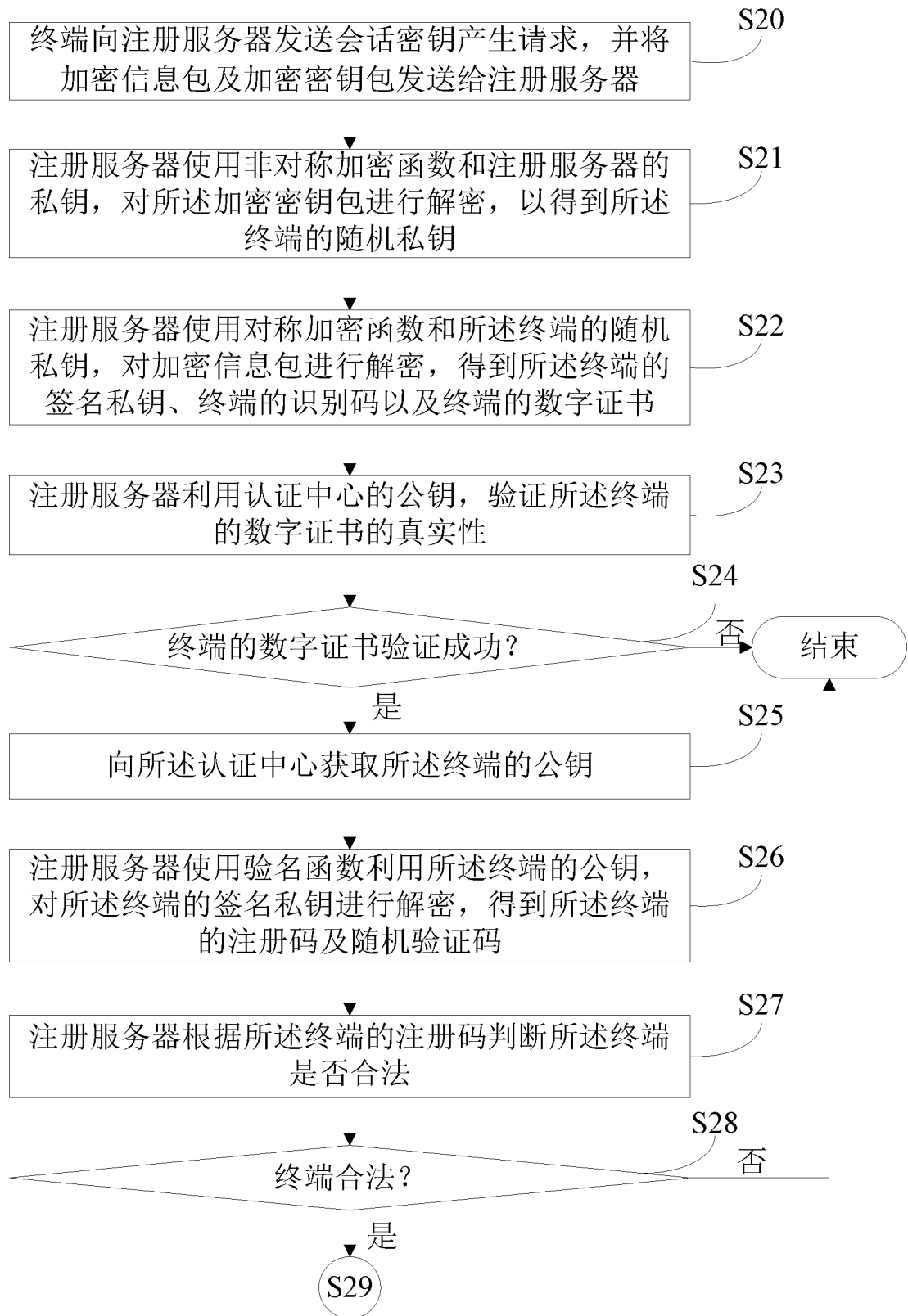


图 4

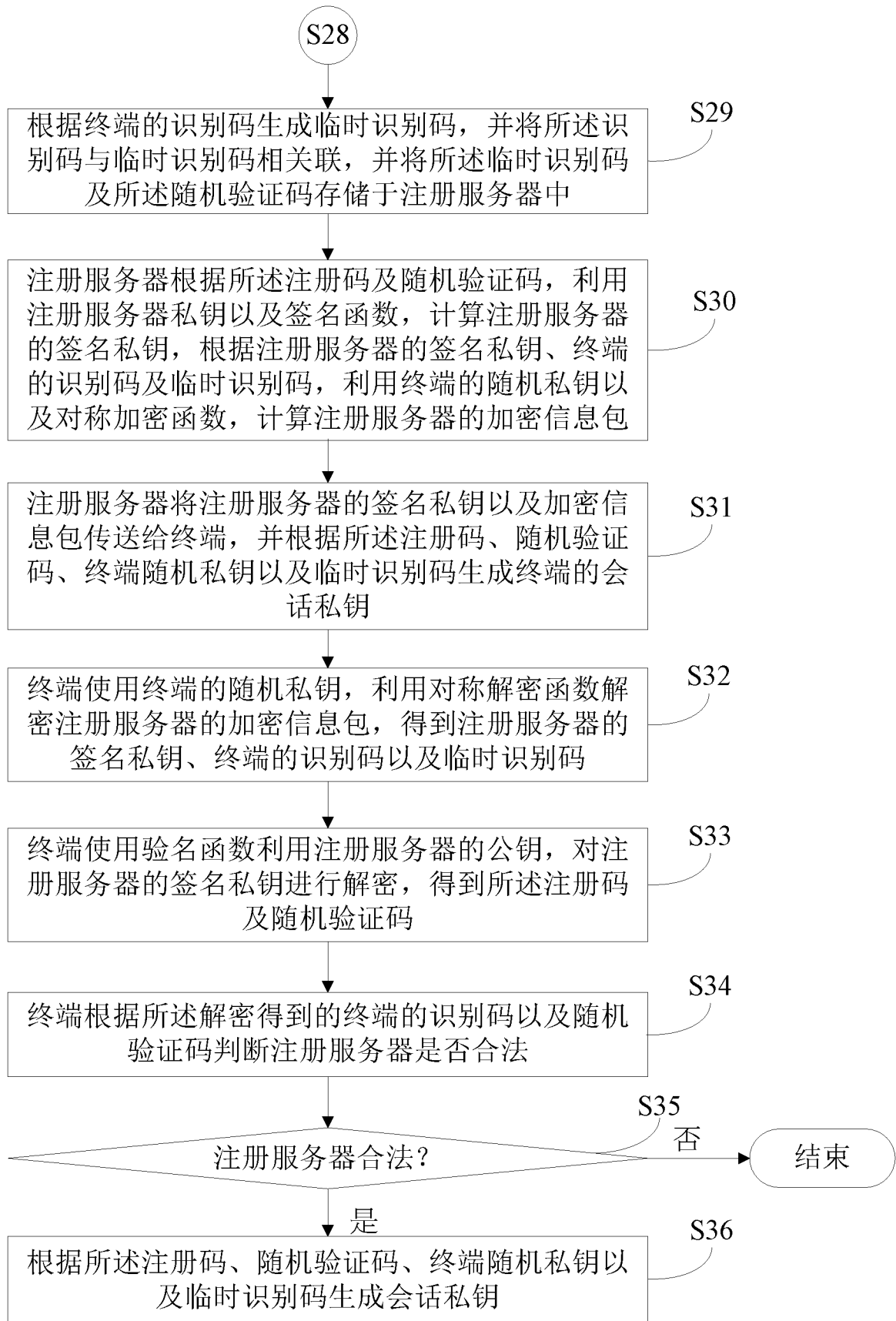


图 5

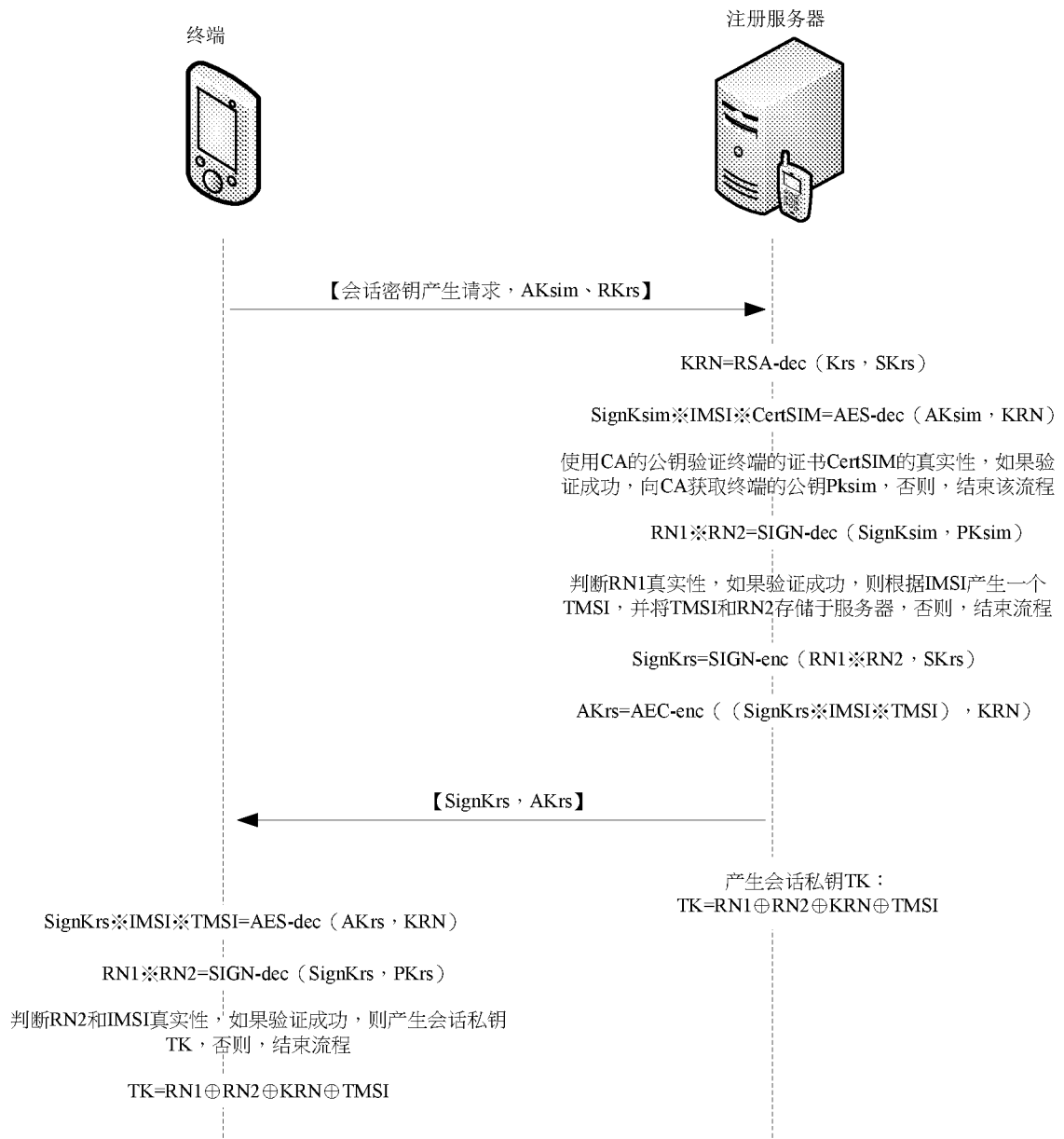


图 6

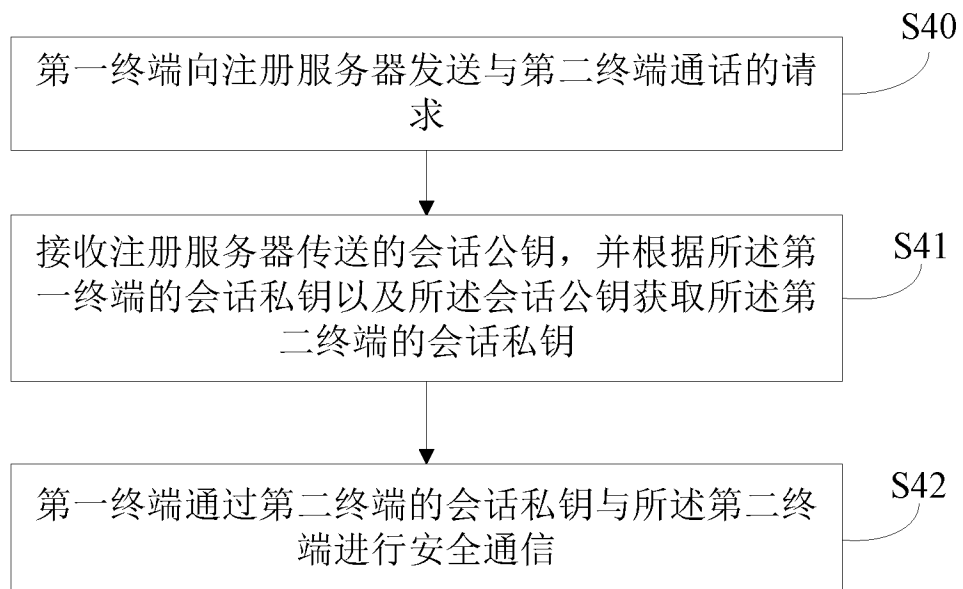


图 7

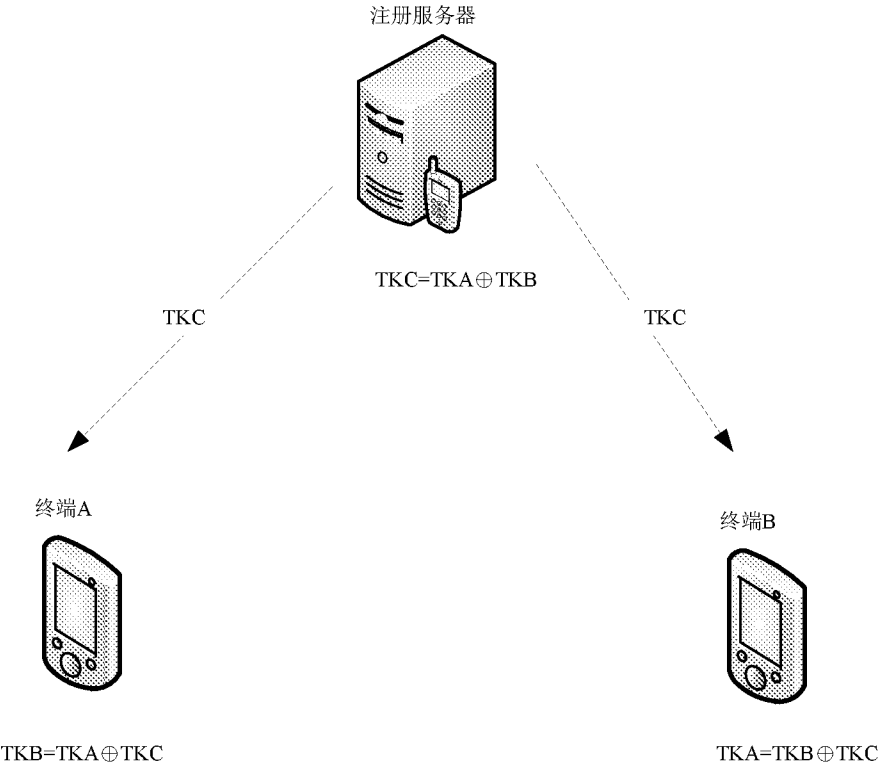


图 8

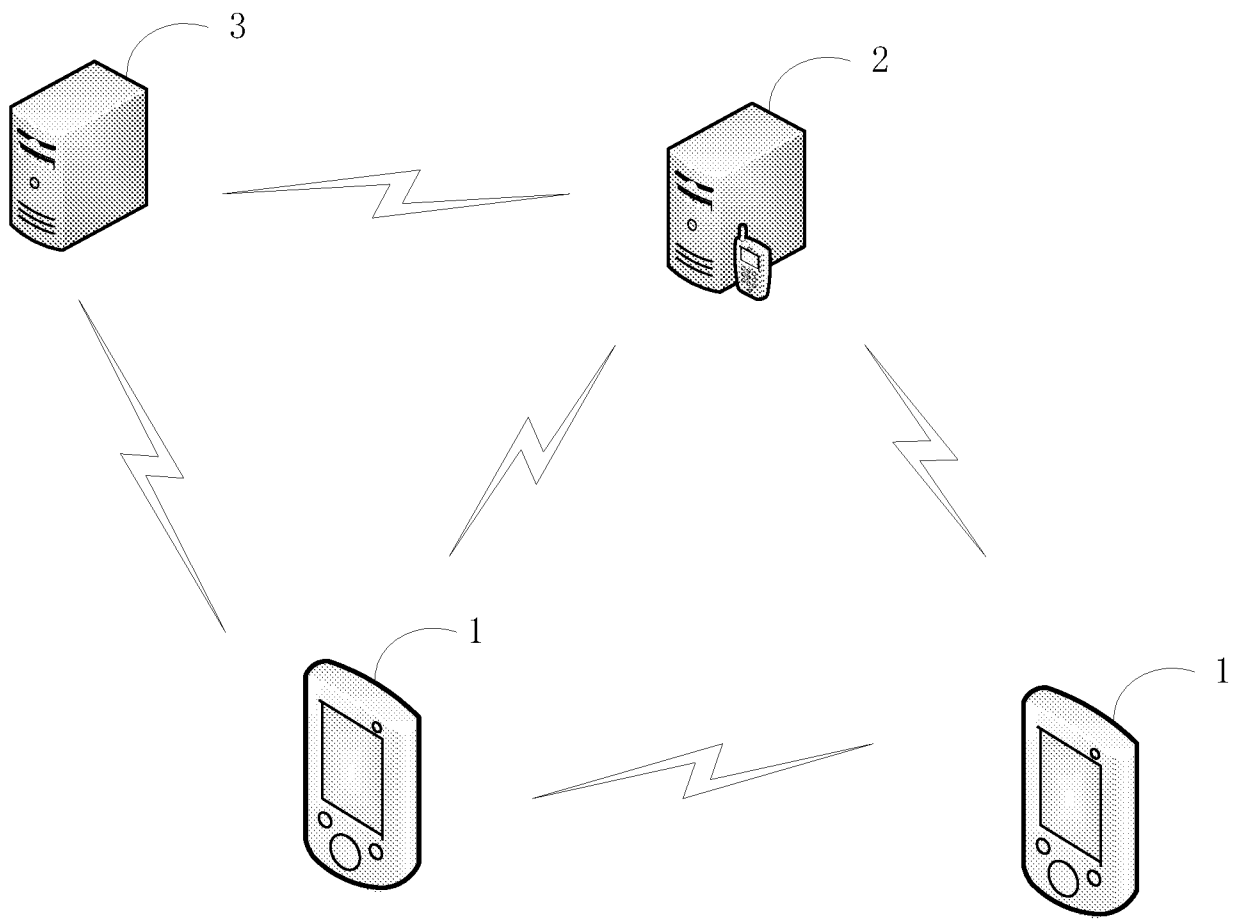


图 9

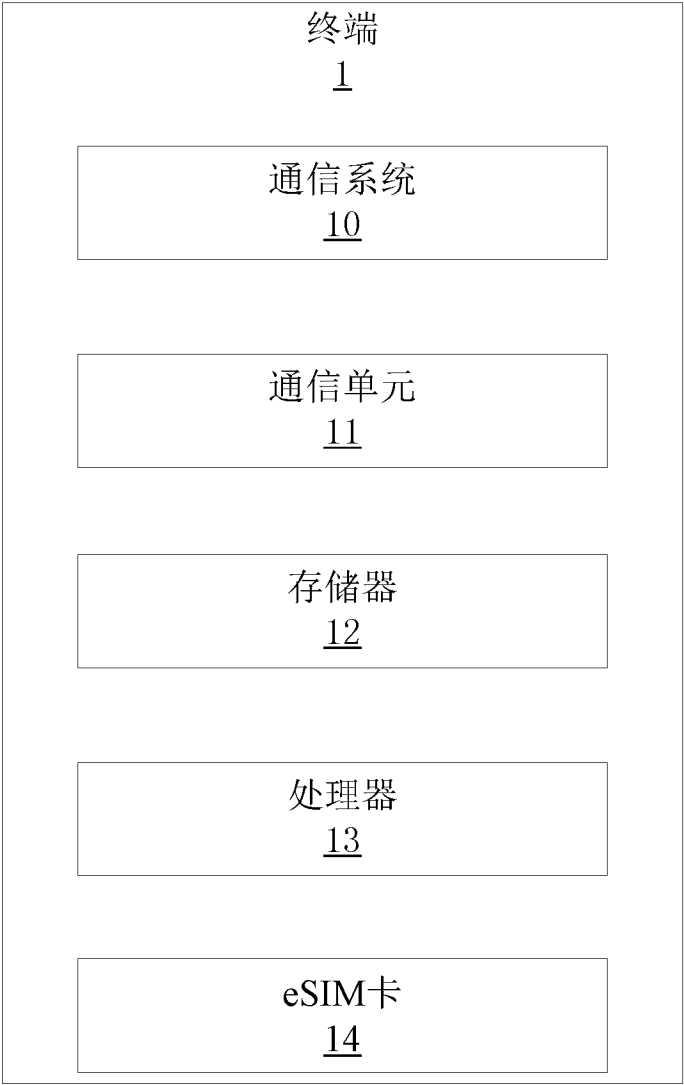


图 10



图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/087576

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: secret key, private key, public key, server, terminal, key, public, private, security, first, second, conversation

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 105337969 A (ZHU, Jianlong) 17 February 2016 (17.02.2016) description, paragraphs [0024]-[0036], and figures 1-5	1-22
A	CN 105450406 A (HUAWEI TECHNOLOGIES CO., LTD.) 30 March 2016 (30.03.2016) the whole document	1-22
A	CN 102474509 A (ALCATEL LUCENT USA INC.) 23 May 2012 (23.05.2012) the whole document	1-22
A	CN 105577377 A (AISINO CORPORATION INC.) 11 May 2016 (11.05.2016) the whole document	1-22
A	CN 105491076 A (Xidian university) 13 April 2016 (13.04.2016) the whole document	1-22

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 22 January 2017	Date of mailing of the international search report 09 February 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LI, Ting Telephone No. (86-10) 62414115

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/087576

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016080327 A1 (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 17 March 2016 (17.03.2016) the whole document	1-22

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/087576

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105337969 A	17 February 2016	None	
CN 105450406 A	30 March 2016	US 2016028701 A1	28 January 2016
		WO 2016011778 A1	28 January 2016
		EP 2991268 A1	02 March 2016
CN 102474509 A	23 May 2012	EP 2452477 A2	16 May 2012
		JP 2012533218 A	20 December 2012
		US 2011010549 A1	13 January 2011
		KR 20120027485 A	21 March 2012
		WO 2011005569 A2	13 January 2011
CN 105577377 A	11 May 2016	None	
CN 105491076 A	13 April 2016	None	
US 2016080327 A1	17 March 2016	JP 2016059022 A	21 April 2016

A. 主题的分类 H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L; H04W; H04Q 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNPAT, CNKI, WPI, EPDOC: 服务器, 终端, 密钥, 私钥, 公钥, 安全, 会话, 第一, 第二, server, terminal, key, public, private, security, first, second, conversation		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 105337969 A (朱建龙) 2016年 2月 17日 (2016 - 02 - 17) 说明书第[0024]-[0036]段, 附图1-5	1-22
A	CN 105450406 A (华为技术有限公司) 2016年 3月 30日 (2016 - 03 - 30) 全文	1-22
A	CN 102474509 A (阿尔卡特朗讯公司) 2012年 5月 23日 (2012 - 05 - 23) 全文	1-22
A	CN 105577377 A (航天信息股份有限公司) 2016年 5月 11日 (2016 - 05 - 11) 全文	1-22
A	CN 105491076 A (西安电子科技大学) 2016年 4月 13日 (2016 - 04 - 13) 全文	1-22
A	US 2016080327 A1 (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 2016年 3月 17日 (2016 - 03 - 17) 全文	1-22
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2017年 1月 22日		国际检索报告邮寄日期 2017年 2月 9日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 李亭 电话号码 (86-10)62414115

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/087576

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	105337969	A	2016年 2月 17日	无			
CN	105450406	A	2016年 3月 30日	US	2016028701	A1	2016年 1月 28日
				WO	2016011778	A1	2016年 1月 28日
				EP	2991268	A1	2016年 3月 2日
CN	102474509	A	2012年 5月 23日	EP	2452477	A2	2012年 5月 16日
				JP	2012533218	A	2012年 12月 20日
				US	2011010549	A1	2011年 1月 13日
				KR	20120027485	A	2012年 3月 21日
				WO	2011005569	A2	2011年 1月 13日
CN	105577377	A	2016年 5月 11日	无			
CN	105491076	A	2016年 4月 13日	无			
US	2016080327	A1	2016年 3月 17日	JP	2016059022	A	2016年 4月 21日