(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
2012 年 3 月 1 日 (01.03.2012)

PCT

(10) 国际公布号
WO 2012/024905 A1

(51) 国际专利分类号:
H04L 9/14 (2006.01)

(21) 国际申请号: PCT/CN2011/070337

(22) 国际申请日: 2011 年 1 月 17 日 (17.01.2011)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201010265297.6 2010 年 8 月 25 日 (25.08.2010) CN

(71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **张蓬勃 (ZHANG, Pengbo)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **曹耀斌 (CAO, Yaobin)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **薛宝林 (XUE, Baolin)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **薛涛 (XUE, Tao)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **于松 (YU, Song)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **邓方民 (DENG, Fangmin)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **孙君生 (SUN, Junsheng)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。 **杨玉林 (YANG, Yulin)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: **北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE)**; 中国北京市海淀区学清路 8 号 B 座 1601A, 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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

[见续页]

(54) Title: METHOD, TERMINAL AND GGSN FOR ENCRYPTING AND DECRYPTING DATA IN MOBILE COMMUNICATION NETWORK

(54) 发明名称 : 一种移动通讯网中数据加解密方法、终端和 GGSN

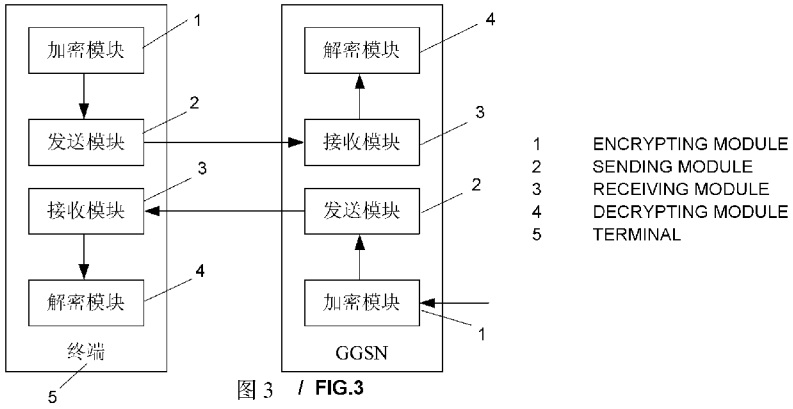

图 3 / FIG.3

(57) Abstract: A method for encrypting and decrypting data in a mobile communication network is disclosed, which includes: before transmitting packet data, a sender sends original packet data message to an encrypting module(1), and the encrypting module(1) encrypts the original packet data reporting using an cipher key (CK), and the sender sends it to a receiver after performing the protocol encapsulation to the encrypted packet data report; after receiving the encrypted packet data report, the receiver sends it to a decrypting module(4), and the decrypting module(4) decrypts the packet data report using the CK which is the same to the CK used to encrypt the packet report in the sender, and sends the decrypted packet data report to the next target. A terminal and Gateway GPRS Support Node (GGSN) in the mobile communication network are also disclosed. The present invention can ensure that transmitting user information by plain text is prevented.

[见续页]

WO 2012/024905 A1

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

— 发明人资格(细则 4.17(iv))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(57) 摘要:

本发明公开了一种移动通讯网中数据加解密方法,该方法包括：在分组数据传输之前，发送端将原始分组数据报文送入加密模块（1），由加密模块（1）采用加密密钥(CK)对原始分组数据报文进行加密，对加密后的分组数据报文进行协议封装后发送至接收端；以及接收端收到加密的分组数据报文后，将其送入解密模块（4），由解密模块（4）使用与发送端加密分组数据报文所采用的 CK 相同的 CK 对分组数据报文进行解密，将解密后的分组数据报文发往下一目的地。本发明还公开了一种移动通讯网中的终端和 GGSN。本发明可以保证用户信息不通过明文传输。

一种移动通讯网中数据加解密方法、终端和 GGSN

技术领域

本发明涉及移动通信领域，尤其涉及一种移动通信网中数据加解密方法、终端和网关通用分组无线业务支持节点。

背景技术

数据业务是第三代移动通讯技术发展的重点，也最受用户和运营商的关注，很多传统的业务（比如语音通话）也已经通过分组交互实现（网络电话（Voice over IP，VOIP）），因此数据业务的保密性和安全性也越来越受到关注。

移动网络本身有自身的通讯加密方法，在第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）（包括通用移动通讯系统（Universal Mobile Telecommunications System，UMTS）和全球移动通讯系统（Global System for Mobile Communications，GSM））系统中，用户的用户识别模块（Subscriber Identity Module，SIM）卡和归属网络的归属位置存储器/鉴权中心（Home Location Register/Authentication Center，HLR/AuC），通用表示方式，表示集成了 AUC 的 HLR）共享一个安全密钥 Ki（128bit），基于该安全密钥 Ki，核心网和用户之间可以进行双向鉴权，同时基站和手机间也利用 Ki 对无线链路进行加密和完整性保护。

3GPP 中定义的加密方法只是加密无线环境，在移动终端和节点 B（Node B）之间对传输的数据进行加/解密，数据在网络中都是通过明文传输的，很容易被监听，现有的网络监听技术大都在网络侧实现。图 1 为分组数据网络示意图，移动终端 A 和 B 分别通过各自的无线网络系统(Radio Network System，RNS)、服务通用分组无线业务（General Packet Radio Service，GPRS）支持节点（Serving GPRS Support Node，SGSN）、网关 GPRS 支持节点 GGSN（Gateway GPRS Support Node，）接入分组数据网络（Packet Data Network，PDN）。如图 1，通常在 SGSN 和 GGSN 中进行监听。

目前已有相关专利或者方案都是端到端的加密，这样的加密参数不能动态变化，很容易被破解。支持加密的用户和不支持加密的用户之间数据输出方式很难协调。

发明内容

本发明要解决的技术问题是提供一种移动通讯网中数据加解密方法、终端和网关通用分组无线业务支持节点，保证用户信息不通过明文传输，防止用户信息被非法监听，提高数据传输的安全性和保密性。

为解决上述技术问题，本发明提供了一种移动通讯网中数据加解密方法，该方法包括：

在分组数据传输之前，发送端将原始分组数据报文送入加密模块，由加密模块采用加密密钥（CK）对原始分组数据报文进行加密，对加密后的分组数据报文进行协议封装后发送至接收端；以及

接收端收到加密的分组数据报文后，将其送入解密模块，由解密模块使用与发送端加密分组数据报文所采用的 CK 相同的 CK 对分组数据报文进行解密，将解密后的分组数据报文发送到下一目的地。

发送端将原始分组数据报文送入加密模块的步骤之前，所述方法还包括：判断在分组数据通道建立时是否接收到加密标识，如果接收到，则将原始分组数据报文送入加密模块进行加密。

所述发送端为终端，所述接收端为网关通用分组无线业务支持节点（GGSN）；或者，所述发送端为 GGSN，所述接收端为终端。

所述发送端为终端，所述接收端为 GGSN 时，

发送端将原始分组数据报文送入加密模块，由加密模块对原始分组数据报文进行加密，对加密后的分组数据报文进行协议封装后发送至接收端的步骤包括：终端在发送分组数据报文前，先通过终端中的加密模块使用 CK 对所述分组数据报文进行加密，终端对加密后的分组数据报文进行协议封装后发送至网络；

接收端将加密的分组数据报文送入解密模块，由解密模块对分组数据报文进行解密，将解密后的分组数据报文发送到下一目的地的步骤包括：所述GGSN收到终端发送的分组数据报文后，GGSN中的解密模块使用与所述终端加密分组数据报文所采用的CK相同的CK对所述分组数据报文进行解密，所述GGSN将解密后的分组数据报文发送至所述报文的目的地址。

所述发送端为GGSN，所述接收端为终端时，

发送端将原始分组数据报文送入加密模块，由加密模块对原始分组数据报文进行加密，对加密后的分组数据报文进行协议封装后发送至接收端的步骤包括：所述GGSN在接收到发送至终端的分组数据报文后，GGSN中的加密模块使用CK对所述分组数据报文进行加密，GGSN对加密后的分组数据报文进行协议封装后发送，通过网络发送至终端；

接收端将加密的分组数据报文送入解密模块，由解密模块对分组数据报文进行解密，将解密后的分组数据报文发送到下一目的地的步骤包括：所述终端接收到加密的分组数据报文后，由终端中的解密模块使用与所述GGSN加密分组数据报文所采用的CK相同的CK对所述分组数据报文进行解密，获取解密后的分组数据报文。

GGSN中的解密模块使用与所述终端相同的CK对所述分组数据报文进行解密的步骤包括：所述GGSN收到终端发送的分组数据报文后，将所述终端的CK和所述分组数据报文发送给解密模块，由所述解密模块使用所述CK对所述分组数据报文进行解密；

所述GGSN在数据传输链路建立时，从归属位置存储器/鉴权中心（HLR/AUC）中获取所述终端的CK。

GGSN中的加密模块使用CK对所述分组数据报文进行加密的步骤包括：所述GGSN收到发送至终端的分组数据报文后，将所述终端的CK和所述分组数据报文发送给加密模块，由所述加密模块使用所述CK对所述分组数据报文进行加密；

所述GGSN在数据传输链路建立时，从归属位置存储器/鉴权中心（HLR/AUC）中获取所述终端的CK。

为解决上述技术问题，本发明还提供了一种移动通讯网中的终端，所述终端包括加密模块、发送模块、接收模块和解密模块，其中：

所述加密模块设置为：使用加密密钥（CK）对所述分组数据报文进行加密；

所述发送模块设置为：对加密后的分组数据报文进行协议封装后发送至网络侧；

所述接收模块设置为：接收网络侧发送的加密的分组数据报文；

所述解密模块设置为：使用与网络侧加密分组数据报文所采用的 CK 相同的 CK 对所述分组数据报文进行解密，获取解密后的分组数据报文。

所述终端还包括判断模块，所述判断模块设置为：在发送分组数据报文前，判断是否有加密标识，如果有，则触发加密模块，如果没有触发发送模块；以及在接收到分组数据报文后，如果判断有加密标识，则触发解密模块。

为解决上述技术问题，本发明还提供了一种网关通用分组无线业务支持节点（GGSN），所述 GGSN 包括接收模块、解密模块、加密模块和发送模块，其中：

所述接收模块设置为：接收终端发送的加密的分组数据报文，以及用于接收发送至终端的分组数据报文；

所述解密模块设置为：使用与终端加密分组数据报文所采用的加密密钥（CK）相同的 CK 对所述接收的加密的分组数据报文进行解密；

所述发送模块设置为：将解密后的分组数据报文发送至所述报文的目的地址，以及将加密后的分组数据报文进行协议封装后通过网络发送至终端；

所述加密模块设置为：使用 CK 对所述接收的发送至终端的分组数据报文进行加密。

所述 GGSN 还包括：

密钥获取模块，其设置为：在数据传输链路建立时，从归属位置存储器/鉴权中心（HLR/AUC）中获取的所述终端的 CK；以及：

在收到终端发送的分组数据报文后，将获取的所述终端的 CK 和所述分组数据报文发送给解密模块，由所述解密模块使用所述 CK 对所述分组数据报文进行解密；

在收到发送至终端的分组数据报文后，将获取的所述终端的 CK 和所述分组数据报文发送给加密模块，由所述加密模块使用所述 CK 对所述分组数据报文进行加密。

所述 GGSN 还包括判断模块，所述判断模块设置为：在发送分组数据报文前，判断是否有加密标识，如果有，则触发加密模块，如果没有触发发送模块；以及在接收到分组数据报文后，如果判断有加密标识，则触发解密模块。

本发明通过在移动终端和 GGSN 中分别配置硬件加解密模块，硬件加解密模块通过加密密钥（Cipher Key，CK）对上下行分组数据报文进行加解密，可以保证用户信息不通过明文传输。加密后的数据在网络侧无法监听，而且在无线环境传输还会进行加密，相当于双加密的，更加保密和安全。即使窃听方获得了被窃听方得安全密钥 Ki，也无法在无线传输环境中进行窃听，提高数据传输的安全性和保密性。

本发明适用于政府敏感部门，情报机关，等等非常重视安全和保密的组织和个人。

附图概述

图 1 为分组数据网络示意图；

图 2 为加密后的分组网络及数据传输示意图；

图 3 为终端和 GGSN 的具体结构示意图。

本发明的较佳实施方式

目前技术中端到端的加密由于没有传输网络参与，这样的加密参数不能动态变化，很容易被破解。为了解决这一问题，本发明的发明构思是：

在分组数据传输之前，发送端（用户终端或者 GGSN）将原始分组数据报文送入加密模块，由加密模块采用加密密钥（CK）作为加密运算因子对原始分组数据报文进行加密，得到加密后的分组数据报文，对加密后的分组数据报文进行协议封装后发送至接收端；

接收端（发送端为用户终端时，接收端为 GGSN；发送端为 GGSN 时，接收端为用户终端）收到加密的分组数据报文后，将其送入解密模块，由解密模块使用与发送端加密模块相同的 CK 对分组数据报文进行解密，之后将解密后的分组数据报文发送到下一目的地。

其中：

●对于上行分组数据，终端在发送分组数据报文前，先通过终端中的加密模块使用加密密钥（CK）对所述分组数据报文进行加密，终端对加密后的分组数据报文进行协议封装后发送至网络；GGSN 收到终端发送的分组数据报文后，GGSN 中的解密模块使用与所述终端相同的 CK 对所述分组数据报文进行解密，所述 GGSN 将解密后的分组数据报文发送至所述报文的目的地址。

所述 GGSN 收到终端发送的分组数据报文后，GGSN 中的解密模块使用与所述终端相同的CK对所述分组数据报文进行解密的步骤包括：所述GGSN收到终端发送的分组数据报文后，将所述终端的 CK 和所述分组数据报文发送给解密模块，由所述解密模块使用所述 CK 对所述分组数据报文进行解密。

所述 GGSN 中的终端的 CK 是在数据传输链路建立时，从归属位置存储器/鉴权中心（HLR/AUC）中获取的。

●对于下行分组数据，GGSN 在接收到发送至终端的分组数据报文后，GGSN 中的加密模块使用 CK 对所述分组数据报文进行加密，GGSN 对加密后的分组数据报文进行协议封装后发送，通过网络发送至终端；所述终端接收到加密的分组数据报文后，由终端中的解密模块使用与所述 GGSN 相同的 CK 对所述分组数据报文进行解密，获取解密后的分组数据报文。

所述 GGSN 在接收到发送至终端的分组数据报文后，GGSN 中的加密模块使用 CK 对所述分组数据报文进行加密的步骤包括：所述 GGSN 收到发送

至终端的分组数据报文后，将所述终端的 CK 和所述分组数据报文发送给加密模块，由所述加密模块使用所述 CK 对所述分组数据报文进行加密。

本文的实现与移动网络自身加密无关，直接对需要传输的原始数据进行加密和解密，数据加密后在网络中传输，以保证数据的保密性和安全性。

硬件加密、解密模块使用 CK 作为加密因子对分组数据进行加解密。该 CK 是通过加密算法（A3）、RAND（随机数）和 Ki（根密钥）计算出来的，如 CK= A3（RAND，Ki）。Ki 由网络(如网络单元 HLR/AUC)与终端共享，在终端（如全球用户识别模块（Universal Subscriber Identity Module，USIM）卡中）和 HLR/AUC 中存储，不在网络中传输，很难窃取。而 RAND 是随机序列，在每次连接建立中都会变化，具有很强的随机性。因此在本方案中加密因子每次都不同，只在本次会话中有效，所以又称为实时加密，此举更加大了无线传输环境中对 CK 进行破解的难度，从而保证数据传输私密性。

另一方面，本发明中使用数据业务的双方（包括终端和 GGSN 服务器）不需要知道对方的 CK。对终该而言，网络侧负责在每次认证时将 RAND 传给终端，终端可根据算法自己生成 CK；对于 GGSN 而言，GGSN 可从 HLR/AUC 中获取 HLR/AUC 计算出的 CK。不会增加额外的损耗。

上述硬件加密模块和解密模块可以由第三方提供，嵌入终端及网络设备中，负责对分组数据进行加解密运算。这样即使网络设备商、终端设备商和运营商都无法对加密分组数据进行窃听。

分组数据都是基于 IP 传输，本申请中，对原始的数据进行加密，密文作为 IP 包的原始数据，通过 IP 相关协议封装，不影响网关对分组数据的处理及路由选择。

实现上述方法的系统如图 2 和图 3 所示，主要包括终端和 GGSN，其中：

所述终端包括加密模块、发送模块、接收模块和解密模块，其中：

所述加密模块设置为：使用 CK 对所述分组数据报文进行加密；

所述发送模块设置为：对加密后的分组数据报文进行协议封装后发送至

网络侧;

所述接收模块设置为：于接收网络侧发送的加密的分组数据报文;

所述解密模块设置为：使用与网络侧加密分组数据报文是所采用的 CK 相同的 CK 对所述分组数据报文进行解密，获取解密后的分组数据报文。

所述 GGSN 包括接收模块、解密模块、加密模块和发送模块，其中：

所述接收模块设置为：接收终端发送的加密的分组数据报文，以及接收发送至终端的分组数据报文;

所述解密模块设置为：使用与终端加密分组数据报文时所采用的 CK 相同的 CK 对所述接收的加密的分组数据报文进行解密;

所述发送模块设置为：将解密后的分组数据报文发送至所述报文的目的地址，以及将加密后的分组数据报文进行协议封装后通过网络发送至终端;

所述加密模块设置为：使用 CK 对所述接收的发送至终端的分组数据报文进行加密。

上述终端中的加密模块和解密模块可以合一设置为加解密模块;同样地，所述 GGSN 中的加密模块和解密模块也可合一设置。发送模块和接收模块也可合一设置为收发模块。终端中如何设置与 GGSN 中如何设置无关，GGSN 中如何设置也与终端中如何设置无关。但 GGSN 和终端中加解密模块的运算规则相同，具体采用哪种加解密算法本发明不作限定。

优选地，所述 GGSN 还设置为：在数据传输链路建立时，从 HLR/AUC 中获取的所述终端的 CK; 以及，在收到终端发送的分组数据报文后，将获取的所述终端的 CK 和所述分组数据报文发送给解密模块，由所述解密模块使用所述 CK 对所述分组数据报文进行解密; 以及，在收到发送至终端的分组数据报文后，将获取的所述终端的 CK 和所述分组数据报文发送给加密模块，由所述加密模块使用所述 CK 对所述分组数据报文进行加密。

优选地，所述终端还包括判断模块，该判断模块设置为：在发送分组数据报文前，判断是否有加密标识，如果有，则触发加密模块，如果没有，触发发送模块; 以及在接收到分组数据报文后，如果判断有加密标识，则触发

解密模块。

优选地，所述 GGSN 还包括判断模块，该判断模块设置为：在发送分组数据报文前，判断是否有加密标识，如果有，则触发加密模块，如果没有触发发送模块；以及在接收到分组数据报文后，如果判断有加密标识，则触发解密模块。

下面结合附图对本发明的实施例作进一步的详细描述，需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互任意组合。

本发明所提出的实现方法需要网络参与，因此需要在终端和 GGSN 中嵌入硬件加密模块。选择把 GGSN 作为加密/解密的另一端，有几个好处：

1）分组业务包括很多种类，客户端/服务器（Client/Server，C/S）类的业务占了绝大多数，同时还有部分会话类业务，在 GGSN 中加密/解密，可以实现对各种类型的分组业务的加密。

2）GGSN 是第三代移动通讯分组域网络的网关节点，是移动网络和公用 PDN 的分界点，用户数据在外部 PDN 传输时用户的 IP 地址都是动态分配的，根据 IP 很难获取到用户信息，而用户的标识信息（比如国际移动用户识别码（International Mobile Subscriber Identity，IMSI）等）只在移动网络中传输，因此在 GGSN 中加密能够保证用户数据不被非法监听，所以在 GGSN 中加密能够保证用户信息的安全性和私密性。

终端和 GGSN 中的中的硬件加密模块作用稍有差异，而运算规则完全相同。

在本实施例中，可在分组数据通道建立过程中，通过参数控制终端和 GGSN 是否需要对分组数据报文进行加密。下面分三个部分对具体实现流程进行介绍：

第一部分：加密判断及加密密钥（CK）的获得

加密标识：

在处理数据之前，移动终端和 GGSN 需要知道是否需要对用户数据进行

加密解密。参照 3GPP 协议，在分组数据通道建立时，在终端和 GGSN 之间会共享传输相关的参数信息，如 IP 配置信息以及域名系统（Domain Name System，DNS）配置信息等，终端通过在该参数中增加加密标识，通知 GGSN 是否需要进行加解密操作。

终端和 GGSN 在数据发送之前，判断是否有该加密标识，如果有，则触发加密模块进行加密，如果没有，则按正常流程，对分组数据封装后发送。

CK 的获得:

终端中:

根据 3GPP 协议规定，在建立分组数据传输通道建立之前，首先要建立信令连接，在信令连接建立过程中需要对用户进行认证，在认证过程中网络侧将 RAND 发给终端，终端按照获得的 RAND，结合自身 Ki，通过 A3 算法，产生当前有效 CK ，将 CK 传递给终端硬件加解密模块。

GGSN 中:

按照 3GPP 的协议流程，GGSN 不参与信令链路的建立，因此在 GGSN 中无法根据现有流程获得 CK 值，因此需要增加额外的信令流程来实现。利用现有的 GGSN 和 HLR/AUC 之间的接口（Gc）口，在数据传输链路建立时，判断如果需要对数据进行加解密操作，从 HLR/Auc 中获取 CK，存储在 GGSN 中，在对应的用户终端需要传输数据时，发给硬件加解密模块。

第二部分：终端中的加密解密处理

加密:

终端在发送数据前，现把分组数据报文发给硬件加解密模块，硬件加解密模块使用在链路建立时获得的 CK 对分组数据报文进行加密，终端加密后的分组数据报文进行相关的协议封装后发送给网络。

解密:

终端从网络收到分组数据报文后，把分组数据报文传给硬件加解密模块进行解密，硬件加解密模块使用 CK 对分组数据报文进行解密，终端把解密后明文数据报文传给对应的应用模块。

第三部分：GGSN 中的加密解密处理

GGSN 从终端收到分组数据报文后，先进行解密，把分组数据报文以明文的形式发给外部 PDN；GGSN 从外部 PDN 或者其他 GGSN 收到分组数据报文后，进行加密后，以密文形式发给终端。

加密：

GGSN 从外部 PDN 或者其他 GGSN 收到分组数据报文后，根据目的地址获得用户信息，判断是否需要对当前用户的数据进行加密，需要加密时，获取当前用户的 CK，和原始分组数据报文一起传给硬件加解密模块，硬件加解密模块使用收到的 CK 对分组数据报文进行加密生成密文。GGSN 把密文按照 3GPP 规定的协议（和 SGSN 之间通过 GPRS 隧道协议（GPRS Tunneling Protocol，GTP）封装））封装后，发送终端。

解密：

GGSN 根据从终端收到数据获得用户标识（按照 3GPP 协议规定，SGSN 和 GGSN 之间采用 GTP 进行数据传输，根据 GTP 的标识可以获得用户标识信息），根据获得的用户标识，从保存的 CK 中查出该 UE 的 CK，把分组数据报文和 CK 一起送给硬件加解密模块进行解密，解密后获得明文形式的分组数据报文，按照报文中指定的目的地址发送报文。

本领域普通技术人员可以理解上述方法中的全部或部分步骤可通过程序来指令相关硬件完成，所述程序可以存储于计算机可读存储介质中，如只读存储器、磁盘或光盘等。可选地，上述实施例的全部或部分步骤也可以使用一个或多个集成电路来实现。相应地，上述实施例中的各模块可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。本发明不限制于任何特定形式的硬件和软件的结合。

当然，本发明还可有其他多种实施例，在不背离本发明精神及其实质的情况下，熟悉本领域的技术人员当可根据本发明作出各种相应的改变和变形，但这些相应的改变和变形都应属于本发明所附的权利要求的保护范围。

工业实用性

本发明可以保证用户信息不通过明文传输。加密后的数据在网络侧无法监听，而且在无线环境传输还会进行加密，相当于双加密的，更加保密和安全。即使窃听方获得了被窃听方得安全密钥 Ki，也无法在无线传输环境中进行窃听，提高数据传输的安全性和保密性。

本发明适用于政府敏感部门，情报机关，等等非常重视安全和保密的组织和个人。

权 利 要 求 书

1、一种移动通讯网中数据加解密方法，该方法包括:

在分组数据传输之前，发送端将原始分组数据报文送入加密模块，由加密模块采用加密密钥（CK）对原始分组数据报文进行加密，对加密后的分组数据报文进行协议封装后发送至接收端；以及

接收端收到加密的分组数据报文后，将其送入解密模块，由解密模块使用与发送端加密分组数据报文所采用的 CK 相同的 CK 对分组数据报文进行解密，将解密后的分组数据报文发送到下一目的地。

2、如权利要求 1 所述的方法，其中:

发送端将原始分组数据报文送入加密模块的步骤之前,所述方法还包括:判断在分组数据通道建立时是否接收到加密标识，如果接收到，则将原始分组数据报文送入加密模块进行加密。

3、如权利要求 1 或 2 所述的方法，其中:

所述发送端为终端，所述接收端为网关通用分组无线业务支持节点（GGSN）；或者，所述发送端为 GGSN，所述接收端为终端。

4、如权利要求 3 所述的方法，其中:

所述发送端为终端，所述接收端为 GGSN 时，

发送端将原始分组数据报文送入加密模块，由加密模块对原始分组数据报文进行加密，对加密后的分组数据报文进行协议封装后发送至接收端的步骤包括：终端在发送分组数据报文前，先通过终端中的加密模块使用 CK 对所述分组数据报文进行加密，终端对加密后的分组数据报文进行协议封装后发送至网络;

接收端将加密的分组数据报文送入解密模块，由解密模块对分组数据报文进行解密，将解密后的分组数据报文发送到下一目的地的步骤包括：所述

GGSN 收到终端发送的分组数据报文后，GGSN 中的解密模块使用与所述终端加密分组数据报文所采用的 CK 相同的 CK 对所述分组数据报文进行解密，所述 GGSN 将解密后的分组数据报文发送至所述报文的目的地址。

5、如权利要求 3 所述的方法，其中：

所述发送端为 GGSN，所述接收端为终端时，

发送端将原始分组数据报文送入加密模块，由加密模块对原始分组数据报文进行加密，对加密后的分组数据报文进行协议封装后发送至接收端的步骤包括：所述 GGSN 在接收到发送至终端的分组数据报文后，GGSN 中的加密模块使用 CK 对所述分组数据报文进行加密，GGSN 对加密后的分组数据报文进行协议封装后发送，通过网络发送至终端；

接收端将加密的分组数据报文送入解密模块，由解密模块对分组数据报文进行解密，将解密后的分组数据报文发送到下一目的地的步骤包括：所述终端接收到加密的分组数据报文后，由终端中的解密模块使用与所述 GGSN 加密分组数据报文所采用的 CK 相同的 CK 对所述分组数据报文进行解密，获取解密后的分组数据报文。

6、如权利要求 4 所述的方法，其中：

GGSN 中的解密模块使用与所述终端相同的 CK 对所述分组数据报文进行解密的步骤包括：所述 GGSN 收到终端发送的分组数据报文后，将所述终端的 CK 和所述分组数据报文发送给解密模块，由所述解密模块使用所述 CK 对所述分组数据报文进行解密；

所述 GGSN 在数据传输链路建立时，从归属位置存储器/鉴权中心（HLR/AUC）中获取所述终端的 CK。

7、如权利要求 5 所述的方法，其中：

GGSN 中的加密模块使用 CK 对所述分组数据报文进行加密的步骤包括：所述 GGSN 收到发送至终端的分组数据报文后，将所述终端的 CK 和所述分组数据报文发送给加密模块，由所述加密模块使用所述 CK 对所述分组数据

报文进行加密;

所述 GGSN 在数据传输链路建立时，从归属位置存储器/鉴权中心（HLR/AUC）中获取所述终端的 CK。

8、一种移动通讯网中的终端，所述终端包括加密模块、发送模块、接收模块和解密模块，其中:

所述加密模块设置为: 使用加密密钥（CK）对所述分组数据报文进行加密;

所述发送模块设置为: 对加密后的分组数据报文进行协议封装后发送至网络侧;

所述接收模块设置为: 接收网络侧发送的加密的分组数据报文;

所述解密模块设置为: 使用与网络侧加密分组数据报文所采用的 CK 相同的 CK 对所述分组数据报文进行解密，获取解密后的分组数据报文。

9、如权利要求 8 所述的终端，其中:

所述终端还包括判断模块，所述判断模块设置为: 在发送分组数据报文前，判断是否有加密标识，如果有，则触发加密模块，如果没有触发发送模块; 以及在接收到分组数据报文后，如果判断有加密标识，则触发解密模块。

10、一种网关通用分组无线业务支持节点（GGSN），所述 GGSN 包括接收模块、解密模块、加密模块和发送模块，其中:

所述接收模块设置为: 接收终端发送的加密的分组数据报文，以及用于接收发送至终端的分组数据报文;

所述解密模块设置为: 使用与终端加密分组数据报文所采用的加密密钥（CK）相同的 CK 对所述接收的加密的分组数据报文进行解密;

所述发送模块设置为: 将解密后的分组数据报文发送至所述报文的目的地址，以及将加密后的分组数据报文进行协议封装后通过网络发送至终端;

所述加密模块设置为：使用 CK 对所述接收的发送至终端的分组数据报文进行加密。

11、如权利要求 10 所述的 GGSN，其还包括：

密钥获取模块，其设置为：在数据传输链路建立时，从归属位置存储器/鉴权中心（HLR/AUC）中获取的所述终端的 CK；以及：

在收到终端发送的分组数据报文后，将获取的所述终端的 CK 和所述分组数据报文发送给解密模块，由所述解密模块使用所述 CK 对所述分组数据报文进行解密；

在收到发送至终端的分组数据报文后，将获取的所述终端的 CK 和所述分组数据报文发送给加密模块，由所述加密模块使用所述 CK 对所述分组数据报文进行加密。

12、如权利要求 10 所述的 GGSN，其中：

所述 GGSN 还包括判断模块，所述判断模块设置为：在发送分组数据报文前，判断是否有加密标识，如果有，则触发加密模块，如果没有触发发送模块；以及在接收到分组数据报文后，如果判断有加密标识，则触发解密模块。

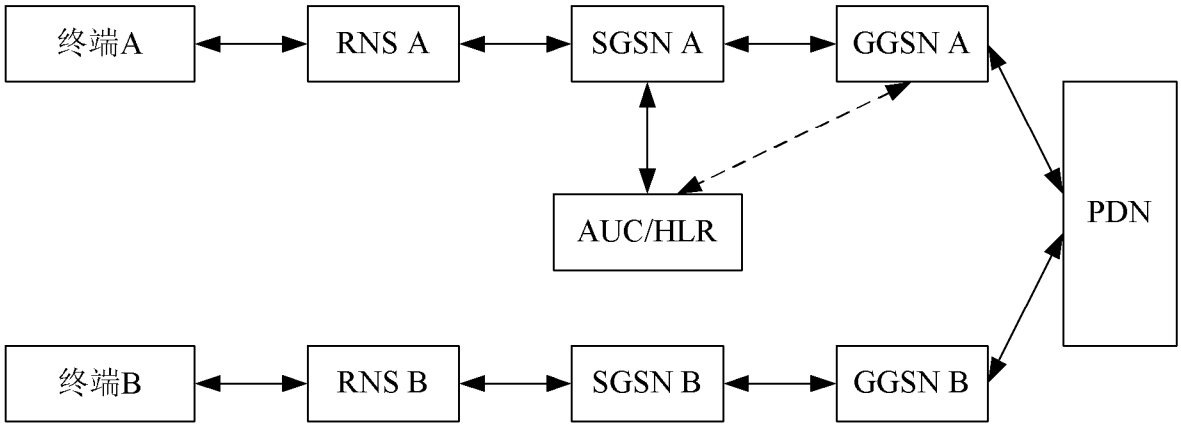
终端A
RNS A
SGSN A
GGSN A
PDN
AUC/HLR
终端B
RNS B
SGSN B
GGSN B

图 1

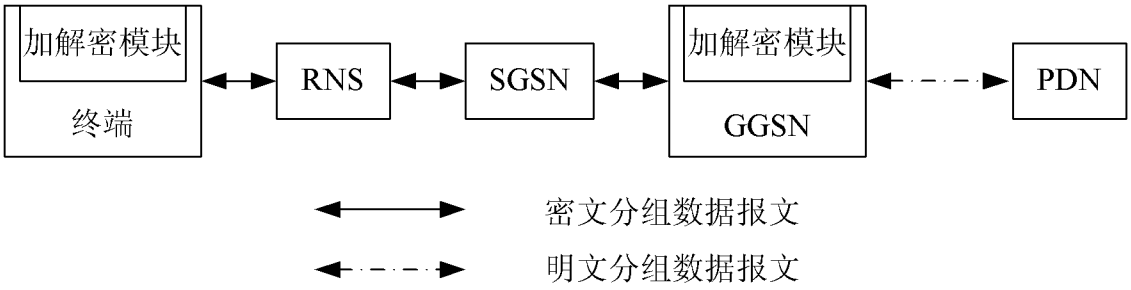
加解密模块
终端
RNS
SGSN
加解密模块
GGSN
PDN
密文分组数据报文
明文分组数据报文

图 2

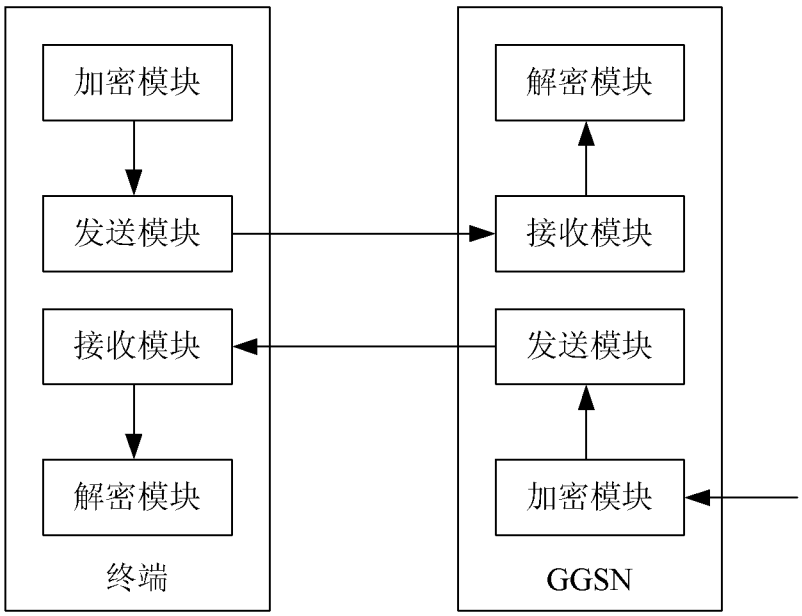
加密模块
发送模块
接收模块
解密模块
终端
解密模块
接收模块
发送模块
加密模块
GGSN

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2011/070337

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/14(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)

IPC: H04L

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)

CPRSABS, CNABS, CNTXT,CNKI, VEN: Mobile, telecommunication, cell phone, encrypt, decrypt, decipher, protocol package, CK, key, similar, same

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1784899A (SAMSUNG ELECTRONICS CO LTD) , 07 June 2006 (07.06.2006) description page 6 line 14 to page 7 line 17	1-12
PX	CN101917712A (ZTE CORP) 15 Dec. 2010 (15.12.2010), description paragraph [0065] to [0090]	1-12
A	CN101483865A (ZTE CORP) 15 July 2009 (15.07.2009), the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 May 2011(10.05.2011)	**02 Jun. 2011 (02.06.2011)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer SUN, Di Telephone No. (86-10)62411246

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2011/070337

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1784899A	07.06.2006	EP1478138A2	17.11.2004
		US2004228360A1	18.11.2004
		WO2004102966A1	25.11.2004
		KR20040099084A	26.11.2004
		JP2006526355T	16.11.2006
CN101917712A	15.12.2010	NONE	
CN101483865A	15.07.2009	NONE	

国际检索报告

国际申请号
PCT/CN2011/070337

A. 主题的分类

H04L9/14(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)

IPC: H04L

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）)

CPRSABS, CNABS, CNTXT,CNKI, VEN: 移动通讯，移动通信，加密，解密，协议封装，CK，密钥，相同

Mobile, telecommunication, cell phone, encrypt, decrypt, decipher, protocol package, CK, key, similar, same

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
X	CN1784899A (三星电子株式会社) 07. 6 月 2006 (07.06.2006)，说明书第 6 页第 14 行至第 7 页第 17 行	1-12
PX	CN101917712A(中兴通讯股份有限公司) 15. 12 月 2010 (15.12.2010)，说明书[0065]至[0090]段	1-12
A	CN101483865A (中兴通讯股份有限公司) 15.7 月 2009 (15.07.2009)，全文	1-12

☐ 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	国际检索报告邮寄日期
10.5 月 2011 (10.05.2011)	**02.6 月 2011 (02.06.2011)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 **孙迪** 电话号码：(86-10) **62411246**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2011/070337

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1784899A	07.06.2006	EP1478138A2	17.11.2004
		US2004228360A1	18.11.2004
		WO2004102966A1	25.11.2004
		KR20040099084A	26.11.2004
		JP2006526355T	16.11.2006
CN101917712A	15.12.2010	无	
CN101483865A	15.07.2009	无	