(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
2014 年 11 月 20 日 (20.11.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/183535 A1

(51) 国际专利分类号:
H04W 12/04 (2009.01)

(21) 国际申请号: PCT/CN2014/075724

(22) 国际申请日: 2014 年 4 月 18 日 (18.04.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310604096.8 2013 年 11 月 25 日 (25.11.2013) CN

(71) 申请人: **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: **余万涛 (YU, Wantao)**; 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)。

(74) 代理人: **北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE)**; 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (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, LT, 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, 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, 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))。
— 在修改权利要求的期限届满之前进行，在收到该修改后将重新公布(细则 48.2(h))。

[见续页]

(54) Title: METHOD AND SYSTEM FOR SECURE TRANSMISSION OF SMALL DATA OF MTC DEVICE GROUP

(54) 发明名称 : 一种用于 MTC 设备组的小数据安全传输方法和系统

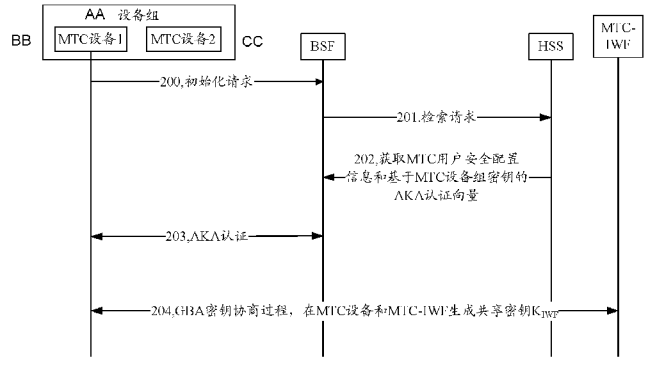

图 2 / Fig. 2

200 INITIALIZATION REQUEST
201 SEARCH REQUEST
202 OBTAIN MTC USER SECURITY SETTINGS INFORMATION AND MTC GROUP KEY-BASED AKA AUTHENTICATION VECTOR
203 AKA AUTHENTICATION
204 GBA KEY AGREEMENT PROCEDURE, THEN MTC DEVICE AND MTC-IWF GENERATE SHARED KEY KIWF ON BASIS OF SAID PROCEDURE
AA DEVICE GROUP
BB MTC DEVICE 1
CC MTC DEVICE 2

(57) **Abstract**: Disclosed is a method for secure transmission of small data of a machine type communication (MTC) device group, comprising a process wherein an MTC device and an MTC-Interworking Function (MTC-IWF) generate a shared key K_{IWF} on the basis of a GBA procedure, the MTC device and a bootstrapping server (BSF) performing AKA authentication: a home subscriber server (HSS) determines whether the MTC device belongs to the MTC device group and whether said device has small data transmission and reception capabilities; if said device belongs to said group and has said capabilities, an AKA authentication vector generated on the basis of the MTC device group key is sent to said BSF; the BSF carries out AKA authentication with the MTC device on the basis of the received AKA authentication vector. Also disclosed is a system for secure transmission of small data of an MTC device group.

(57) **摘要**: 本发明公开了一种用于 MTC 设备组的小数据安全传输方法，包括机器类通讯（MTC）设备与外部接口功能实体（MTC-IWF）基于 GBA 过程生成共享密钥 K_{IWF} 的过程，在 MTC 设备与引导服务器（BSF）进行 AKA 认证中：用户归属服务器（HSS）判断 MTC 设备是否属于 MTC 设备组以及是否具有小数据发送和接收能力，若是，则向所述 BSF 发送基于 MTC 设备组密钥生成的 AKA 认证向量；所述 BSF 根据接收的所述 AKA 认证向量与所述 MTC 设备进行 AKA 认证。本发明还公开了一种用于 MTC 设备组的小数据安全传输系统。

WO 2014/183535 A1

— 根据申请人的请求，在条约第 21 条(2)(a)所规定的期限届满之前进行。

一种用于 MTC 设备组的小数据安全传输方法和系统

技术领域

本发明涉及一种 GBA 密钥协商技术，具体地，涉及一种用于 MTC 设备组的小数据安全传输方法和系统。

背景技术

机器类通信（Machine Type Communication，简称为 MTC）是指应用无线通信技术，实现机器与机器、机器与人之间的数据通信和交流的一系列技术及其组合的总称。MTC 包含两层含义：第一层是机器本身，在嵌入式领域称为智能设备；第二层意思是机器和机器之间的连接，通过网络把机器连接在一起。机器类通信的应用范围非常广泛，例如智能测量、远程监控等，使人类生活更加智能化。与传统的人与人之间的通信相比，MTC 设备（MTC Device）数量巨大，应用领域广泛，具有巨大的市场前景。

在现有 MTC 通信系统中，MTC 设备通过 3GPP（the 3rd Generation Partnership Project，第三代合作伙伴项目）网络和外部接口功能实体（MTC InterWorking Function，MTC-IWF）与业务服务器如 MTC 服务器进行通信。

GBA 是指通用引导架构（Generic Bootstrapping Architecture），GBA 体系架构定义了一种在终端和服务器之间的通用的密钥协商机制。

在移动通信系统中，引入 MTC 设备后，由于 MTC 设备数量众多，为了降低网络负载节省网络资源，需要对 MTC 设备以组的方式进行管理优化。并且这些 MTC 设备可能经常发送小数据，从而导致移动通信系统效率降低。为了高效使用网络资源，需要根据小数据传输对移动通信系统进行增强和优化，以提高移动通信系统传输小数据的效率。通过信令在 MTC 设备与 MTC-IWF 和业务服务器之间传输小数据是一种非常有效的方式，不仅可以

避免用户面资源的分配，还可以降低无线资源的使用。同时，针对 MTC 设备组的情况，在进行小数据传输时，需要按组的方式对 MTC 设备进行安全控制和管理。

目前，通过信令在 MTC 设备与 IWF 和业务服务器之间传输小数据的方法中引入了小数据传输协议（SDT，Small Data Transmission protocol），部署在 MTC 设备和 MTC-IWF。MTC 设备和业务服务器之间的任何数据交换都需要经过 MTC-IWF。在上述方法中，要保证 MTC 设备和 MTC-IWF 之间数据传输的安全性，需要在 MTC 设备与 MTC-IWF 之间建立共享密钥。现有解决方案是，附着阶段通过认证与密钥协商（AKA，Authentication and Key Agreement）过程在 MTC-IWF 建立用于保护小数据安全传输的密钥。这样，在同一附着过程中，MTC 设备可以采用相同的小数据传输保护密钥进行多次小数据安全传输。由于多次小数据传输过程都使用相同的小数据传输保护密钥，这增加了小数据传输保护密钥被攻击的风险。另外，在实际的 M2M 应用中，MTC 设备在一次附着过程中，可能需要针对不同的目的服务器发起小数据传输，为安全起见，这些针对不同目的服务器的小数据传输需要不同的密钥进行保护。因此，当 MTC 设备进行小数据传输时，需要针对每一次小数据传输过程，在 MTC 设备与 MTC-IWF 之间建立用于保护小数据安全传输的共享密钥。针对 MTC 设备组的情况，则需要在 MTC 设备组进行每一次小数据传输时，在一组 MTC 设备与 MTC-IWF 之间建立共享密钥。如何针对每一次小数据传输的情况，在一组 MTC 设备与 MTC-IWF 之间建立用于保护小数据安全传输的共享密钥是亟待解决的技术问题。

发明内容

为了解决现有存在的技术问题，本发明实施例提供了一种用于 MTC 设备组的小数据安全传输方法和系统。

本发明实施例提供的一种用于MTC设备组的小数据安全传输方法，包括机器类通讯MTC设备与外部接口功能实体MTC-IWF基于GBA过程生成共享密钥K_{IWF}的过程，在MTC设备与引导服务器BSF进行AKA认证中：

用户归属服务器HSS判断MTC设备是否属于MTC设备组以及是否具有小数据发送和接收能力，若是，则向所述BSF发送基于MTC设备组密钥生成的AKA认证向量；

所述BSF根据接收的所述AKA认证向量与所述MTC设备进行AKA认证。

较佳地，所述BSF与所述MTC设备进行AKA认证通过后，还包括：

所述MTC设备和BSF生成根密钥Ks；

所述MTC设备、BSF以及MTC-IWF在GBA密钥协商过程中，在所述根密钥Ks基础上生成所述K_{IWF}。

较佳地，所述MTC设备与所述BSF进行AKA认证之前，还包括：

所述MTC设备向所述BSF发送初始化请求，并携带MTC设备标识信息与MTC设备组标识信息，所述MTC设备组标识信息包括所述MTC设备组密钥信息；

所述BSF收到所述MTC设备发送的初始化请求后，向所述HSS发送检索请求，并携带所述MTC设备标识信息与MTC设备组标识信息；

所述HSS根据所述MTC设备标识信息与MTC设备组标识信息判断MTC设备是否属于MTC设备组。

较佳地，所述生成K_{IWF}之后还包括：

所述MTC设备与外部接口功能实体MTC-IWF之间根据所述K_{IWF}进行数据的传输。

较佳地，所述MTC设备信息包括MTC设备的标识信息，所述MTC设备组信息还包括MTC设备组的标识信息；

HSS 根据所述 MTC 设备信息与 MTC 设备组信息判断 MTC 设备是否属于 MTC 设备组具体包括:

HSS 根据所述 MTC 设备的标识信息与 MTC 设备组的标识信息判断 MTC 设备是否属于 MTC 设备组。

较佳地，MTC 设备信息还包括 MTC 设备的小数据传输能力信息;

所述 HSS 判断 MTC 设备是否具有小数据发送和接收能力具体包括:

所述 HSS 根据所述 MTC 设备的小数据传输能力信息判断 MTC 设备是否具有小数据发送和接收能力。

较佳地，所述 HSS 判断 MTC 设备是否具有小数据发送和接收能力具体包括:

所述 HSS 根据保存的签约信息判断 MTC 设备是否具有小数据发送和接收能力，所述签约信息中包括 MTC 设备的小数据传输能力信息。

较佳地，所述在根密钥 Ks 基础上生成所述 K_{IWF} 之后，还包括:

所述 MTC 设备与所述 BSF 在所述 K_{IWF} 基础上生成数据加密密钥和/或数据完整性保护密钥，并发送至所述 MTC-IWF。

较佳地，HSS 根据所述 MTC 设备的标识信息与 MTC 设备组的标识信息确认 MTC 设备属于 MTC 设备组之后，还包括:

HSS 根据所述 MTC 设备的标识信息与 MTC 设备组的标识信息生成用户安全配置信息。

本发明实施例提供的一种用于 MTC 设备组的小数据安全传输方法，包括:

所述 MTC 设备组中至少一个 MTC 设备根据本发明实施例的方法建立共享密钥 K_{IWF} 后，另一 MTC 设备与所述 MTC-IWF 密钥协商过程中:

所述 BSF 根据 MTC 设备组标识信息和用户安全配置信息确认有正在使用的 K_{IWF} 后，根据最近使用的 MTC 设备组标识对应的认证向量与所述另一 MTC 设备进行 AKA 向量认证，认证通过后，所述另一 MTC 设备和

BSF 生成根密钥 Ks;

所述另一 MTC 设备、BSF 以及 MTC-IWF 在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成所述 K_{IWF}。

本发明实施例提供的一种用于 MTC 设备组的小数据安全传输方法，包括:

所述 MTC 设备组中至少一个 MTC 设备根据本发明实施例的方法建立共享密钥 K_{IWF} 以及根据本发明实施例的方法生成用户安全配置信息后，另一 MTC 设备与所述 MTC-IWF 密钥协商过程中:

所述 BSF 根据 MTC 设备组标识信息和用户安全配置信息确认有正在使用的数据加密密钥和/或数据完整性保护密钥后，根据最近使用的 MTC 设备组标识对应的认证向量与所述另一 MTC 设备进行 AKA 向量认证，认证通过后，所述另一 MTC 设备和 BSF 生成根密钥 Ks;

所述另一 MTC 设备、BSF 以及 MTC-IWF 在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成所述 K_{IWF}。

本发明实施例提供的一种用于 MTC 设备组的小数据安全传输系统，应用于 MTC 设备组中的 MTC 设备与引导服务器 BSF 进行 AKA 认证中，包括 MTC 设备、引导服务器 BSF 和用户归属服务器 HSS，其中:

HSS，配置为在确认 MTC 设备属于 MTC 设备组以及具有小数据发送和接收能力后，向所述 BSF 发送基于 MTC 设备组密钥生成的 AKA 认证向量;

BSF，配置为根据接收的所述 AKA 认证向量与所述 MTC 设备进行 AKA 认证。

较佳地，所述 MTC 设备和 BSF 还配置为，在所述 BSF 与 MTC 设备进行 AKA 认证通过后，生成根密钥 Ks;

所述 MTC 设备、BSF 以及外部接口功能实体 MTC-IWF 在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成共享密钥 K_{IWF}。

较佳地，所述 MTC 设备与所述 BSF 进行 AKA 认证之前:

所述 MTC 设备还配置为，向所述 BSF 发送初始化请求，并携带 MTC 设备信息与 MTC 设备组信息，所述 MTC 设备组信息包括所述 MTC 设备组密钥信息;

所述 BSF 还配置为，收到所述 MTC 设备发送的初始化请求后，向所述 HSS 发送检索请求，并携带所述 MTC 设备信息与 MTC 设备组信息;

所述 HSS 还配置为，根据所述 MTC 设备信息与 MTC 设备组信息判断 MTC 设备是否属于 MTC 设备组。

较佳地，所述在根密钥 Ks 基础上生成所述 K_{IWF} 之后:

所述 MTC 设备与所述 BSF 还配置为，在所述 K_{IWF} 基础上生成数据加密密钥和数据完整性保护密钥，并发送至所述 MTC-IWF。

较佳地，所述 MTC 设备信息包括 MTC 设备的标识信息，所述 MTC 设备组信息还包括 MTC 设备组的标识信息;

所述 HSS 还配置为，根据所述 MTC 设备的标识信息与 MTC 设备组的标识信息生成用户安全配置信息。

较佳地，所述在根密钥 Ks 基础上生成所述 K_{IWF} 之后:

所述 MTC 设备与所述 BSF 还配置为，在所述 K_{IWF} 基础上生成数据加密密钥和/或数据完整性保护密钥，并发送至所述 MTC-IWF。

本发明实施例提供的一种用于 MTC 设备组的小数据安全传输系统，应用于 MTC 设备组中至少一个 MTC 设备根据本发明实施例所述的系统建立共享密钥 K_{IWF} 后，另一 MTC 设备与所述 MTC-IWF 密钥协商过程中，包括 MTC 设备、BSF 以及 MTC-IWF，其中:

所述 BSF 配置为，根据 MTC 设备组标识信息和用户安全配置信息确认有正在使用的数据加密密钥和数据完整性保护密钥后，根据最近使用的 MTC 设备组标识对应的认证向量与所述 MTC 设备进行 AKA 向量认证，认证通过后，所述 MTC 设备和 BSF 生成根密钥 Ks;

所述 MTC 设备、BSF 以及 MTC-IWF 配置为，在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成所述 K_{IWF}。

本发明实施例提供的一种用于 MTC 设备组的小数据安全传输系统，应用于 MTC 设备组中至少一个 MTC 设备根据本发明实施例所述的系统建立共享密钥 K_{IWF} 后，另一 MTC 设备与所述 MTC-IWF 密钥协商过程中，包括 MTC 设备、BSF 以及 MTC-IWF，其中：

所述 BSF 配置为，根据 MTC 设备组标识信息和用户安全配置信息确认有正在使用的数据加密密钥和/或数据完整性保护密钥后，根据最近使用的 MTC 设备组标识对应的认证向量与所述另一 MTC 设备进行 AKA 向量认证，认证通过后，所述另一 MTC 设备和 BSF 生成根密钥 Ks;

所述 MTC 设备、BSF 以及 MTC-IWF 配置为，在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成所述 K_{IWF}。

本发明实施例提供的一种机器类通讯 MTC 设备组，包括：

存储模块，配置为存储 MTC 设备标识信息和 MTC 设备组标识信息，所述 MTC 设备组标识信息包括 MTC 设备组密钥信息;

初始化请求发送模块，配置为向所述 BSF 发送初始化请求，并携带所述 MTC 设备信息与 MTC 设备组信息;

第一 AKA 认证模块，配置为在根据 AKA 认证向量与 BSF 进行 AKA 认证，所述 AKA 认证向量由 HSS 基于 MTC 设备组密钥生成;

第一根密钥生成模块，配置为在所述 BSF 进行 AKA 认证通过后，与所述 BSF 生成根密钥 Ks;

第一密钥协商模块，配置为与所述 BSF 以及 MTC-IWF 进行 GBA 密钥协商。

本发明实施例提供的一种引导服务器 BSF，包括：

第一接收模块，配置为接收 MTC 设备发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息，所述 MTC 设备

组标识信息包括 MTC 设备组密钥信息;

检索请求发送模块，配置为接收到所述 MTC 设备发送的初始化请求后，向 HSS 发送检索请求，并携带所述 MTC 设备信息与 MTC 设备组信息;

第二 AKA 认证模块，配置为根据 AKA 认证向量与 MTC 设备进行 AKA 认证，所述 AKA 认证向量由 HSS 基于 MTC 设备组密钥生成;

第二根密钥生成模块，配置为在与所述 MTC 设备进行 AKA 认证通过后，与所述 MTC 设备生成根密钥 Ks;

第二密钥协商模块，配置为与所述 MTC 设备以及 MTC-IWF 进行 GBA 密钥协商。

本发明实施例提供的一种用户归属服务器 HSS，包括:

第二接收模块，配置为接收 BSF 发送的检索请求，所述检索请求中携带上午 MTC 设备信息与 MTC 设备组信息;

判断模块，配置为判断 MTC 设备是否属于 MTC 设备组以及是否具有小数据发送和接收能力;

认证向量生成模块，配置为在所述判断模块确认 MTC 设备属于 MTC 设备组以及具有小数据发送和接收能力后，基于 MTC 设备组密钥生成 AKA 认证向量;

认证向量发送模块，配置为将所述生成的 AKA 认证向量发送给 BSF。

本发明实施例提供的一种引导服务器 BSF，包括:

第一接收模块，配置为接收 MTC 设备发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息;

第一判断模块，配置为根据 MTC 设备组标识信息和用户安全配置信息确认是否有正在使用的共享密钥 K_{IWF};

第二 AKA 认证模块，配置为根据最近使用的 MTC 设备组标识对应的认证向量与 MTC 设备进行 AKA 向量认证;

第二根密钥生成模块，配置为在与所述 MTC 设备进行 AKA 认证通过

后，与所述 MTC 设备生成根密钥 Ks;

第二密钥协商模块，配置为与所述 MTC 设备以及 MTC-IWF 进行 GBA 密钥协商。

本发明实施例提供的一种引导服务器 BSF，包括:

第一接收模块，配置为接收 MTC 设备发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息;

第二判断模块，配置为根据 MTC 设备组标识信息和用户安全配置信息确认是否有正在使用的数据加密密钥和/或数据完整性保护密钥;

第二 AKA 认证模块，配置为根据最近使用的 MTC 设备组标识对应的认证向量与 MTC 设备进行 AKA 向量认证;

第二根密钥生成模块，配置为在与所述 MTC 设备进行 AKA 认证通过后，与所述 MTC 设备生成根密钥 Ks;

第二密钥协商模块，配置为与所述 MTC 设备以及 MTC-IWF 进行 GBA 密钥协商。

相较于现有技术，本发明实施例的方法和系统，解决了 MTC 设备组中的 MTC 设备与 MTC-IWF 之间进行小数据安全传输的技术问题。这样，在每一次进行小数据传输时，MTC 设备组中的任何 MTC 设备都可以根据 MTC 设备组信息与 MTC-IWF 之间建立安全的小数据安全传输通道。

附图说明

图 1 是本发明实施例的基于 MTC 设备组的小数据安全传输系统示意图;

图 2 是本发明实施例一中基于 MTC 设备组的小数据安全传输共享密钥建立方法流程图;

图 3 是本发明实施例二中基于 MTC 设备组的小数据安全传输共享密钥建立方法流程图;

图 4 是本发明实施例三中基于 MTC 设备组的小数据安全传输共享密钥

建立方法流程图;

图 5 是本发明实施例四中基于 MTC 设备组的小数据安全传输共享密钥建立方法流程图;

图 6 是本发明实施例五中基于 MTC 设备组的小数据安全传输系统的结构框图;

图 7 为本发明实施例六中 BSF 的结构框图;

图 8 为本发明实施例七中 BSF 的结构框图。

具体实施方式

下文中将参考附图并结合实施例来详细说明本发明。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组合。

如图 1 所示，本发明用于 MTC 设备组的小数据安全传输系统包括: MTC 设备组及 MTC 设备组中的设备，MTC 设备用于存储 MTC 设备组信息和小数据传输共享密钥信息；引导服务功能实体（BSF，Bootstrapping Server Function），用于 GBA 过程，并保存维护 MTC 用户安全配置信息；归属用户服务器（HSS，Home Subscriber Server），用于管理维护 MTC 设备及 MTC 设备组信息，并生成 MTC 用户安全配置信息，同时用于基于 MTC 设备组密钥生成 AKA 认证向量; MTC-IWF 用于实现网络附属存储（NAF，Network Attached Storage）服务器功能，并存储 MTC 用户安全配置信息和小数据传输共享密钥信息。

实施例一

该实施例一中，MTC 设备需要进行小数据传输时与 MTC-IWF 建立共享密钥 K_{IWF}，具体地，如图 2 所示，包括以下步骤:

步骤 200，MTC 设备（如图 2 所示的 MTC 设备组内的 MTC 设备 1）向 BSF 发送初始化请求信息，初始化请求信息中包含 MTC 设备标识信息，如 IMSI，还包括 MTC 设备组标识信息和 MTC 设备发送/接收小数据能力

信息;

步骤 201，BSF 向 HSS 发送检索请求信息，检索请求信息包含 MTC 设备标识信息和 MTC 设备组标识信息；还可以进一步包括 MTC 设备发送/接收小数据能力信息;

步骤 202，BSF 根据 MTC 设备组标识信息从 HSS 取回 MTC 用户安全配置信息和基于 MTC 设备组密钥生成的 AKA 认证向量，即 HSS 向 BSF 发送 MTC 用户安全配置信息和基于 MTC 设备组密钥生成的 AKA 认证向量。

HSS 首先根据保存的 MTC 设备信息与 MTC 设备组信息，检查检索请求信息中的 MTC 设备标识信息与 MTC 设备组标识信息，当确定 MTC 设备属于 MTC 设备组时，HSS 向 BSF 发送 MTC 用户安全配置信息和基于 MTC 设备组密钥生成的 AKA 认证向量；另外，当 HSS 检查检索请求信息中的 MTC 设备标识信息与 MTC 设备组标识信息，并确定 MTC 设备属于 MTC 设备组后，HSS 可以进一步检查 MTC 设备的小数据传输能力，如根据 MTC 设备的签约信息检查 MTC 设备的小数据发送/接收能力，以确定是否向 BSF 发送 MTC 用户安全配置信息和基于 MTC 设备组密钥生成的 AKA 认证向量。

步骤 203，BSF 保存收到的 MTC 用户安全配置信息和 AKA 认证向量。并根据接收到的 AKA 认证向量，与 MTC 设备进行 AKA 认证过程。AKA 认证过程结束后，MTC 设备和 BSF 生成 GBA 根密钥 Ks。

步骤 204，MTC 设备、MTC-IWF 与 BSF 之间进行 GBA 密钥协商过程，并在 MTC 设备与 MTC-IWF 之间，在 GBA 根密钥 Ks 的基础上生成用于保护小数据传输的共享密钥 K_{IWF}；另外，在 GBA 密钥协商过程中，BSF 将 MTC 用户安全配置信息发送到 MTC-IWF 并进行保存。

实施例二

该实施例二中，MTC 设备与 MTC-IWF 在建立共享密钥 K_{IWF} 的基础上，

进一步生成小数据加密密钥和小数据完整性保护密钥，具体地，如图 3 所示，包括以下步骤:

步骤 300，MTC 设备（如图 3 所示的 MTC 设备组内的 MTC 设备 1）向 BSF 发送初始化请求信息，初始化请求信息中包含 MTC 设备标识信息，如 IMSI，还包括 MTC 设备组标识信息和 MTC 设备发送/接收小数据能力信息。

步骤 301，BSF 向 HSS 发送检索请求信息，检索请求信息包含 MTC 设备标识信息和 MTC 设备组标识信息；还可以进一步包括 MTC 设备发送/接收小数据能力信息。

步骤 302，BSF 根据 MTC 设备组标识信息从 HSS 取回 MTC 用户安全配置信息和基于 MTC 设备组密钥生成的 AKA 认证向量，即 HSS 向 BSF 发送 MTC 用户安全配置信息和基于 MTC 设备组密钥生成的 AKA 认证向量。

HSS 首先根据保存的 MTC 设备信息与 MTC 设备组信息，检查检索请求信息中的 MTC 设备标识信息与 MTC 设备组标识信息，当确定 MTC 设备属于 MTC 设备组时，HSS 向 BSF 发送 MTC 用户安全配置信息和基于 MTC 设备组密钥生成的 AKA 认证向量；另外，当 HSS 检查检索请求信息中的 MTC 设备标识信息与 MTC 设备组标识信息，并确定 MTC 设备属于 MTC 设备组后，HSS 可以进一步检查 MTC 设备的小数据传输能力，如根据 MTC 设备的签约信息检查 MTC 设备的小数据发送/接收能力，以确定是否向 BSF 发送 MTC 用户安全配置信息和基于 MTC 设备组密钥生成的 AKA 认证向量。

步骤 303，BSF 保存收到的 MTC 用户安全配置信息和 AKA 认证向量。根据接收到的 AKA 认证向量，与 MTC 设备进行 AKA 认证过程。AKA 认证过程结束后，MTC 设备和 BSF 生成 GBA 根密钥 Ks。

步骤 304，MTC 设备、MTC-IWF 与 BSF 之间进行 GBA 密钥协商过程，

并在 MTC 设备与 MTC-IWF 之间，在 GBA 根密钥 Ks 的基础上生成用于保护小数据传输的共享密钥 K_{IWF}。BSF 在生成 K_{IWF} 时，可以进一步根据系统需要或根据小数据传输安全保护需要，通过 K_{IWF} 生成用于保护小数据安全传输的下一级密钥，如加密密钥和完整性保护密钥，然后将生成的密钥信息发送给 MTC-IWF 进行保存。另外，在 GBA 密钥协商过程中，BSF 将 MTC 用户安全配置信息发送到 MTC-IWF 并进行保存。MTC 设备在生成 K_{IWF} 时，可以进一步根据系统需要或根据小数据传输安全保护需要，通过 K_{IWF} 生成用于保护小数据安全传输的下一级密钥，如加密密钥和完整性保护密钥。

实施例三

该实施例三中，MTC 设备组中的其他 MTC 设备需要进行小数据传输时与 MTC-IWF 建立共享密钥 K_{IWF}，具体地，如图 4 所示，包括以下步骤：

步骤 400，MTC 设备（如图 4 所示的 MTC 设备组内的 MTC 设备 2）向 BSF 发送初始化请求信息，初始化请求信息中包含 MTC 设备标识信息，如 IMSI，还包括 MTC 设备组标识信息和 MTC 设备发送/接收小数据能力信息；

步骤 401，BSF 根据 MTC 设备的初始化请求信息中 MTC 设备组标识信息、以及 BSF 保存的 MTC 用户安全配置信息，判断是否有正在使用的 K_{IWF} 密钥；

步骤 402，如果判定有正在使用的 K_{IWF} 密钥，则 BSF 直接根据最近使用的 MTC 设备组标识对应的 AKA 认证向量与 MTC 设备进行 AKA 认证过程。AKA 认证过程结束后，MTC 设备和 BSF 生成 GBA 根密钥 Ks；

步骤 403，MTC 设备进一步在 GBA 根密钥 Ks 的基础上生成用于保护小数据传输的共享密钥 K_{IWF}。

实施例四

该实施例四中，MTC 设备组中的其他 MTC 设备需要进行小数据传输

时，MTC 设备在密钥 K_{IWF} 的基础上，进一步生成与 MTC-IWF 共享的小数据加密密钥和小数据完整性保护密钥，具体地，如图 5 所示，包括以下步骤:

步骤 500，MTC 设备（如图 5 所示的 MTC 设备组内的 MTC 设备 2）向 BSF 发送初始化请求信息，初始化请求信息中包含 MTC 设备标识信息，如 IMSI，还包括 MTC 设备组标识信息和 MTC 设备发送/接收小数据能力信息;

步骤 501，BSF 根据 MTC 设备的初始化请求信息中 MTC 设备组标识信息、以及 BSF 保存的 MTC 用户安全配置信息，判断是否有正在使用的加密密钥和完整性密钥;

步骤 502，如果判定有正在使用的加密密钥和完整性密钥，则 BSF 直接根据最近使用的 MTC 设备组标识对应的 AKA 认证向量与 MTC 设备进行 AKA 认证过程。AKA 认证过程结束后，MTC 设备和 BSF 生成 GBA 根密钥 Ks;

步骤 503，MTC 设备进一步在 GBA 根密钥 Ks 的基础上生成 K_{IWF}。

步骤 504，MTC 设备进一步在密钥 K_{IWF} 的基础上生成用于保护小数据传输的加密密钥和完整性密钥。

实施例五

本实施例公开了一种用于 MTC 设备组的小数据安全传输系统，如图 6 所示，包括 MTC 设备 10、BSF 20、MTC-IWF 30 和 HSS 40，其中:

MTC 设备 10 包括:

存储模块 11，配置为存储 MTC 设备标识信息和 MTC 设备组标识信息，所述 MTC 设备组标识信息包括 MTC 设备组密钥信息;

初始化请求发送模块 12，配置为向 BSF 20 发送初始化请求，并携带所述 MTC 设备标识信息与 MTC 设备组标识信息;

第一 AKA 认证模块 13，配置为根据 AKA 认证向量与 BSF 20 进行 AKA

认证，所述 AKA 认证向量由 HSS 40 基于 MTC 设备组密钥生成;

第一根密钥生成模块 14，配置为在 BSF 20 进行 AKA 认证通过后，与 BSF 20 生成根密钥 Ks;

第一密钥协商模块 15，配置为与 BSF 20 以及 MTC-IWF 30 进行 GBA 密钥协商。

BSF 20 包括:

第一接收模块 21，配置为接收 MTC 设备 10 发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息，所述 MTC 设备组标识信息包括 MTC 设备组密钥信息;

检索请求发送模块 22，配置为接收到所述 MTC 设备 10 发送的初始化请求后，向 HSS 40 发送检索请求，检索请求中携带所述 MTC 设备标识信息与 MTC 设备组标识信息;

第二 AKA 认证模块 23，配置为根据 AKA 认证向量与 MTC 设备 10 进行 AKA 认证，所述 AKA 认证向量由 HSS 40 基于 MTC 设备组密钥生成;

第二根密钥生成模块 24，配置为在与所述 MTC 设备 10 进行 AKA 认证通过后，与 MTC 设备 10 生成根密钥 Ks;

第二密钥协商模块 25，配置为与 MTC 设备 10 以及 MTC-IWF 30 进行 GBA 密钥协商。

HSS 40 包括:

第二接收模块 41，配置为接收 BSF 20 发送的检索请求，所述检索请求中携带上述 MTC 设备标识信息与 MTC 设备组标识信息;

判断模块 42，配置为判断 MTC 设备 10 是否属于 MTC 设备组以及是否具有小数据发送和接收能力;

认证向量生成模块 43，配置为在判断模块 42 确认 MTC 设备 10 属于 MTC 设备组以及具有小数据发送和接收能力后，基于 MTC 设备组密钥生成 AKA 认证向量;

认证向量发送模块 44，配置为将所述生成的 AKA 认证向量发送给 BSF 20。

实施例六

本实施例公开了一种引导服务器 BSF，如图 7 所示，包括：

第一接收模块 21，配置为接收 MTC 设备发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息；

判断模块 26，配置为根据 MTC 设备组标识信息和用户安全配置信息确认是否有正在使用的共享密钥 K_{IWF}；

第二 AKA 认证模块 23，配置为根据最近使用的 MTC 设备组标识对应的认证向量与 MTC 设备进行 AKA 向量认证；

第二根密钥生成模块 24，配置为在与所述 MTC 设备进行 AKA 认证通过后，与所述 MTC 设备生成根密钥 Ks；

第二密钥协商模块 25，配置为与所述 MTC 设备以及 MTC-IWF 进行 GBA 密钥协商。

实施例七

本实施例公开了一种引导服务器 BSF，如图 8 所示，包括：

第一接收模块 21，配置为接收 MTC 设备发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息；

第二判断模块 27，配置为根据 MTC 设备组标识信息和用户安全配置信息确认是否有正在使用的数据加密密钥和/或数据完整性保护密钥；

第二 AKA 认证模块 23，配置为根据最近使用的 MTC 设备组标识对应的认证向量与 MTC 设备进行 AKA 向量认证；

第二根密钥生成模块 24，配置为在与所述 MTC 设备进行 AKA 认证通过后，与所述 MTC 设备生成根密钥 Ks；

第二密钥协商模块 25，配置为与所述 MTC 设备以及 MTC-IWF 进行 GBA 密钥协商。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

权利要求书

1、一种用于MTC设备组的小数据安全传输方法，包括机器类通讯MTC设备与外部接口功能实体MTC-IWF基于通用引导架构GBA过程生成共享密钥K_{IWF}的过程，在MTC设备与引导服务器BSF进行认证与密钥协商AKA认证中：

用户归属服务器HSS判断MTC设备是否属于MTC设备组以及是否具有小数据发送和接收能力，若是，则向所述BSF发送基于MTC设备组密钥生成的AKA认证向量；

所述BSF根据接收的所述AKA认证向量与所述MTC设备进行AKA认证。

2、如权利要求1所述的方法，其中，

所述BSF与所述MTC设备进行AKA认证通过后，还包括：

所述MTC设备和BSF生成根密钥Ks；

所述MTC设备、BSF以及MTC-IWF在GBA密钥协商过程中，在所述根密钥Ks基础上生成所述K_{IWF}。

3、如权利要求1或2所述的方法，其中，

所述MTC设备与所述BSF进行AKA认证之前，还包括：

所述MTC设备向所述BSF发送初始化请求，并携带MTC设备标识信息与MTC设备组标识信息，所述MTC设备组标识信息包括所述MTC设备组密钥信息；

所述BSF收到所述MTC设备发送的初始化请求后，向所述HSS发送检索请求，并携带所述MTC设备标识信息与MTC设备组标识信息；

所述HSS根据所述MTC设备标识信息与MTC设备组标识信息判断MTC设备是否属于MTC设备组。

4、如权利要求2所述的方法，其中，

所述生成 K_{IWF} 之后还包括:

所述 MTC 设备与外部接口功能实体 MTC-IWF 之间根据所述 K_{IWF} 进行数据的传输。

5、如权利要求 4 所述的方法，其中，

所述 MTC 设备信息包括 MTC 设备的标识信息，所述 MTC 设备组信息还包括 MTC 设备组的标识信息;

HSS 根据所述 MTC 设备信息与 MTC 设备组信息判断 MTC 设备是否属于 MTC 设备组具体包括:

HSS 根据所述 MTC 设备的标识信息与 MTC 设备组的标识信息判断 MTC 设备是否属于 MTC 设备组。

6、如权利要求 4 所述的方法，其中，

MTC 设备信息还包括 MTC 设备的小数据传输能力信息;

所述 HSS 判断 MTC 设备是否具有小数据发送和接收能力具体包括:

所述 HSS 根据所述 MTC 设备的小数据传输能力信息判断 MTC 设备是否具有小数据发送和接收能力。

7、如权利要求 4 所述的方法，其中，

所述 HSS 判断 MTC 设备是否具有小数据发送和接收能力具体包括:

所述 HSS 根据保存的签约信息判断 MTC 设备是否具有小数据发送和接收能力，所述签约信息中包括 MTC 设备的小数据传输能力信息。

8、如权利要求 2 所述的方法，其中，

所述在根密钥 Ks 基础上生成所述 K_{IWF} 之后，还包括:

所述 MTC 设备与所述 BSF 在所述 K_{IWF} 基础上生成数据加密密钥和/或数据完整性保护密钥，并发送至所述 MTC-IWF。

9、如权利要求 5 所述的方法，其中，

HSS 根据所述 MTC 设备的标识信息与 MTC 设备组的标识信息确认 MTC 设备属于 MTC 设备组之后，还包括:

HSS 根据所述 MTC 设备的标识信息与 MTC 设备组的标识信息生成用户安全配置信息。

10、一种用于 MTC 设备组的小数据安全传输方法，包括:

所述 MTC 设备组中至少一个 MTC 设备根据所述权利要求 9 所述的方法建立共享密钥 K_{IWF} 后，另一 MTC 设备与所述 MTC-IWF 密钥协商过程中:

所述 BSF 根据 MTC 设备组标识信息和用户安全配置信息确认有正在使用的 K_{IWF} 后，根据最近使用的 MTC 设备组标识对应的认证向量与所述另一 MTC 设备进行 AKA 向量认证，认证通过后，所述另一 MTC 设备和 BSF 生成根密钥 Ks;

所述另一 MTC 设备、BSF 以及 MTC-IWF 在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成所述 K_{IWF}。

11、一种用于 MTC 设备组的小数据安全传输方法，包括:

所述 MTC 设备组中至少一个 MTC 设备根据所述权利要求 8 所述的方法建立共享密钥 K_{IWF} 以及根据权利要求 9 所述的方法生成用户安全配置信息后，另一 MTC 设备与所述 MTC-IWF 密钥协商过程中:

所述 BSF 根据 MTC 设备组标识信息和用户安全配置信息确认有正在使用的数据加密密钥和/或数据完整性保护密钥后，根据最近使用的 MTC 设备组标识对应的认证向量与所述另一 MTC 设备进行 AKA 向量认证，认证通过后，所述另一 MTC 设备和 BSF 生成根密钥 Ks;

所述另一 MTC 设备、BSF 以及 MTC-IWF 在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成所述 K_{IWF}。

12、一种用于 MTC 设备组的小数据安全传输系统，应用于 MTC 设备组中的 MTC 设备与引导服务器 BSF 进行 AKA 认证中，包括 MTC 设备、引导服务器 BSF 和用户归属服务器 HSS，其中:

HSS，配置为在确认 MTC 设备属于 MTC 设备组以及具有小数据发送

和接收能力后，向所述 BSF 发送基于 MTC 设备组密钥生成的 AKA 认证向量;

BSF，配置为根据接收的所述 AKA 认证向量与所述 MTC 设备进行 AKA 认证。

13、如权利要求 12 所述的系统，其中，

所述 MTC 设备和 BSF 还配置为，在所述 BSF 与 MTC 设备进行 AKA 认证通过后，生成根密钥 Ks;

所述 MTC 设备、BSF 以及外部接口功能实体 MTC-IWF 在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成共享密钥 K_{IWF}。

14、如权利要求 12 或 13 所述的系统，其中，

所述 MTC 设备与所述 BSF 进行 AKA 认证之前:

所述 MTC 设备还配置为，向所述 BSF 发送初始化请求，并携带 MTC 设备信息与 MTC 设备组信息，所述 MTC 设备组信息包括所述 MTC 设备组密钥信息;

所述 BSF 还配置为，收到所述 MTC 设备发送的初始化请求后，向所述 HSS 发送检索请求，并携带所述 MTC 设备信息与 MTC 设备组信息;

所述 HSS 还配置为，根据所述 MTC 设备信息与 MTC 设备组信息判断 MTC 设备是否属于 MTC 设备组。

15、如权利要求 14 所述的系统，其中，

所述在根密钥 Ks 基础上生成所述 K_{IWF} 之后:

所述 MTC 设备与所述 BSF 还配置为，在所述 K_{IWF} 基础上生成数据加密密钥和数据完整性保护密钥，并发送至所述 MTC-IWF。

16、如权利要求 15 所述的系统，其中，

所述 MTC 设备信息包括 MTC 设备的标识信息，所述 MTC 设备组信息还包括 MTC 设备组的标识信息;

所述 HSS 还配置为，根据所述 MTC 设备的标识信息与 MTC 设备组的

标识信息生成用户安全配置信息。

17、如权利要求 15 所述的系统，其中，

所述在根密钥 Ks 基础上生成所述 K_{IWF} 之后:

所述 MTC 设备与所述 BSF 还配置为，在所述 K_{IWF} 基础上生成数据加密密钥和/或数据完整性保护密钥，并发送至所述 MTC-IWF。

18、一种用于 MTC 设备组的小数据安全传输系统，应用于 MTC 设备组中至少一个 MTC 设备根据所述权利要求 16 所述的系统建立共享密钥 K_{IWF} 后，另一 MTC 设备与所述 MTC-IWF 密钥协商过程中，包括 MTC 设备、BSF 以及 MTC-IWF，其中:

所述 BSF 配置为，根据 MTC 设备组标识信息和用户安全配置信息确认有正在使用的数据加密密钥和数据完整性保护密钥后，根据最近使用的 MTC 设备组标识对应的认证向量与所述 MTC 设备进行 AKA 向量认证，认证通过后，所述 MTC 设备和 BSF 生成根密钥 Ks;

所述 MTC 设备、BSF 以及 MTC-IWF 配置为，在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成所述 K_{IWF}。

19、一种用于 MTC 设备组的小数据安全传输系统，应用于 MTC 设备组中至少一个 MTC 设备根据所述权利要求 17 所述的系统建立共享密钥 K_{IWF} 后，另一 MTC 设备与所述 MTC-IWF 密钥协商过程中，包括 MTC 设备、BSF 以及 MTC-IWF，其中:

所述 BSF 配置为，根据 MTC 设备组标识信息和用户安全配置信息确认有正在使用的数据加密密钥和/或数据完整性保护密钥后，根据最近使用的 MTC 设备组标识对应的认证向量与所述另一 MTC 设备进行 AKA 向量认证，认证通过后，所述另一 MTC 设备和 BSF 生成根密钥 Ks;

所述 MTC 设备、BSF 以及 MTC-IWF 配置为，在 GBA 密钥协商过程中，在所述根密钥 Ks 基础上生成所述 K_{IWF}。

20、一种机器类通讯 MTC 设备，包括:

存储模块，配置为存储 MTC 设备标识信息和 MTC 设备组标识信息，所述 MTC 设备组标识信息包括 MTC 设备组密钥信息；

初始化请求发送模块，配置为向所述 BSF 发送初始化请求，并携带所述 MTC 设备信息与 MTC 设备组信息；

第一 AKA 认证模块，配置为在根据 AKA 认证向量与 BSF 进行 AKA 认证，所述 AKA 认证向量由 HSS 基于 MTC 设备组密钥生成；

第一根密钥生成模块，配置为在所述 BSF 进行 AKA 认证通过后，与所述 BSF 生成根密钥 Ks；

第一密钥协商模块，配置为与所述 BSF 以及 MTC-IWF 进行 GBA 密钥协商。

21、一种引导服务器 BSF，包括：

第一接收模块，配置为接收 MTC 设备发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息，所述 MTC 设备组标识信息包括 MTC 设备组密钥信息；

检索请求发送模块，配置为接收到所述 MTC 设备发送的初始化请求后，向 HSS 发送检索请求，并携带所述 MTC 设备信息与 MTC 设备组信息；

第二 AKA 认证模块，配置为根据 AKA 认证向量与 MTC 设备进行 AKA 认证，所述 AKA 认证向量由 HSS 基于 MTC 设备组密钥生成；

第二根密钥生成模块，配置为在与所述 MTC 设备进行 AKA 认证通过后，与所述 MTC 设备生成根密钥 Ks；

第二密钥协商模块，配置为与所述 MTC 设备以及 MTC-IWF 进行 GBA 密钥协商。

22、一种用户归属服务器 HSS，包括：

第二接收模块，配置为接收 BSF 发送的检索请求，所述检索请求中携带上午 MTC 设备信息与 MTC 设备组信息；

判断模块，配置为判断 MTC 设备是否属于 MTC 设备组以及是否具有

小数据发送和接收能力;

认证向量生成模块，配置为在所述判断模块确认 MTC 设备属于 MTC 设备组以及具有小数据发送和接收能力后，基于 MTC 设备组密钥生成 AKA 认证向量;

认证向量发送模块，配置为将所述生成的 AKA 认证向量发送给 BSF。

23、一种引导服务器 BSF，包括:

第一接收模块，配置为接收 MTC 设备发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息;

第一判断模块，配置为根据 MTC 设备组标识信息和用户安全配置信息确认是否有正在使用的共享密钥 K_{IWF};

第二 AKA 认证模块，配置为根据最近使用的 MTC 设备组标识对应的认证向量与 MTC 设备进行 AKA 向量认证;

第二根密钥生成模块，配置为在与所述 MTC 设备进行 AKA 认证通过后，与所述 MTC 设备生成根密钥 Ks;

第二密钥协商模块，配置为与所述 MTC 设备以及 MTC-IWF 进行 GBA 密钥协商。

24、一种引导服务器 BSF，包括:

第一接收模块，配置为接收 MTC 设备发送的初始化请求，所述初始化请求中携带 MTC 设备标识信息和 MTC 设备组标识信息;

第二判断模块，配置为根据 MTC 设备组标识信息和用户安全配置信息确认是否有正在使用的数据加密密钥和/或数据完整性保护密钥;

第二 AKA 认证模块，配置为根据最近使用的 MTC 设备组标识对应的认证向量与 MTC 设备进行 AKA 向量认证;

第二根密钥生成模块，配置为在与所述 MTC 设备进行 AKA 认证通过后，与所述 MTC 设备生成根密钥 Ks;

第二密钥协商模块，配置为与所述 MTC 设备以及 MTC-IWF 进行

GBA 密钥协商。

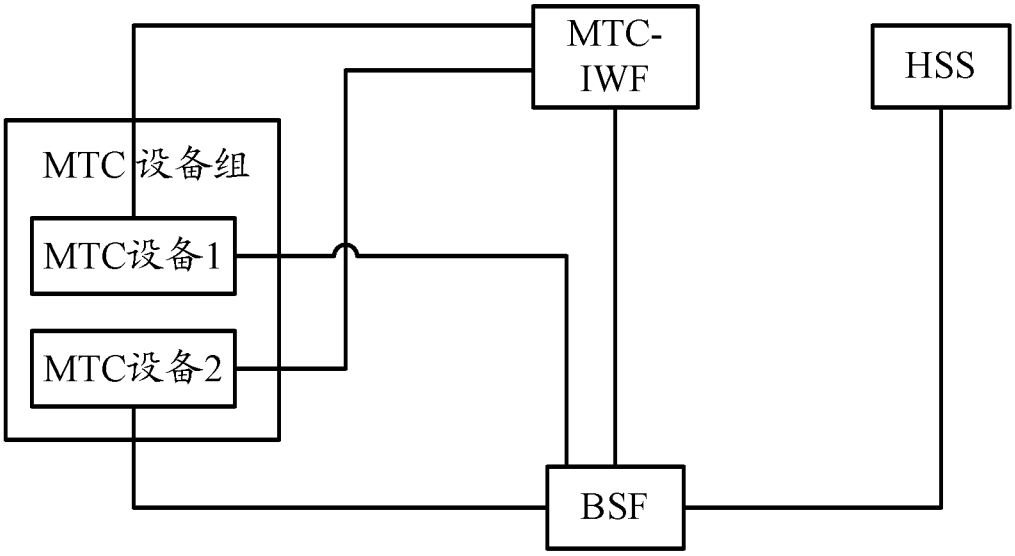
MTC-
IWF
HSS
MTC 设备组
MTC设备1
MTC设备2
BSF

图 1

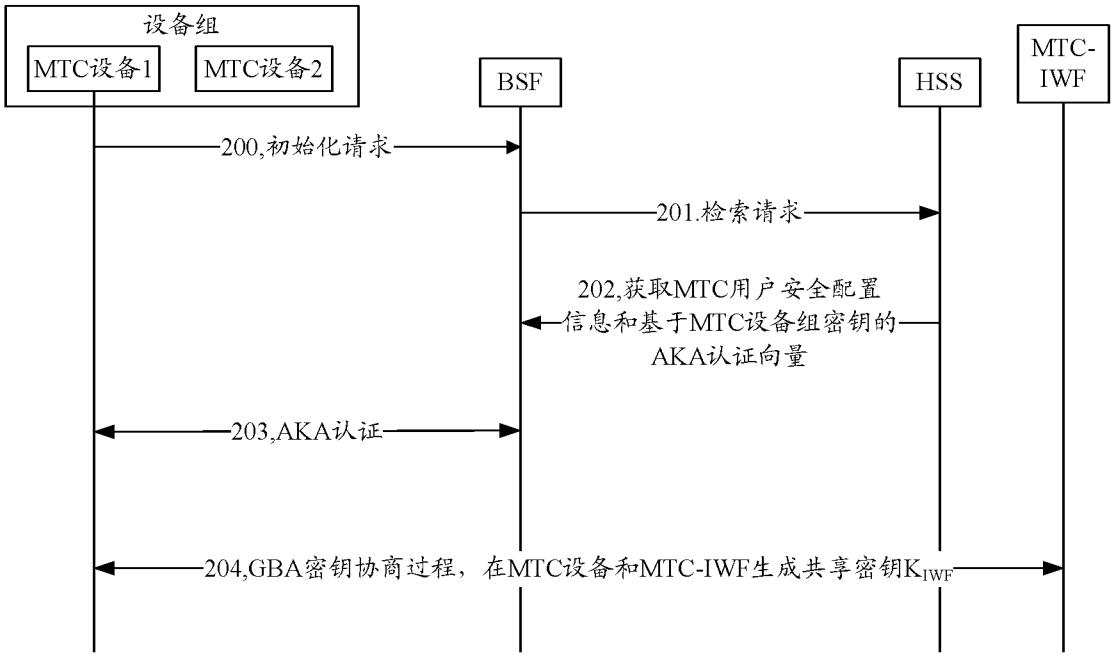
设备组
MTC设备1
MTC设备2
BSF
HSS
MTC-
IWF
200,初始化请求
201.检索请求
202,获取MTC用户安全配置
信息和基于MTC设备组密钥的
AKA认证向量
203,AKA认证
204,GBA密钥协商过程，在MTC设备和MTC-IWF生成共享密钥K_IWF

图 2

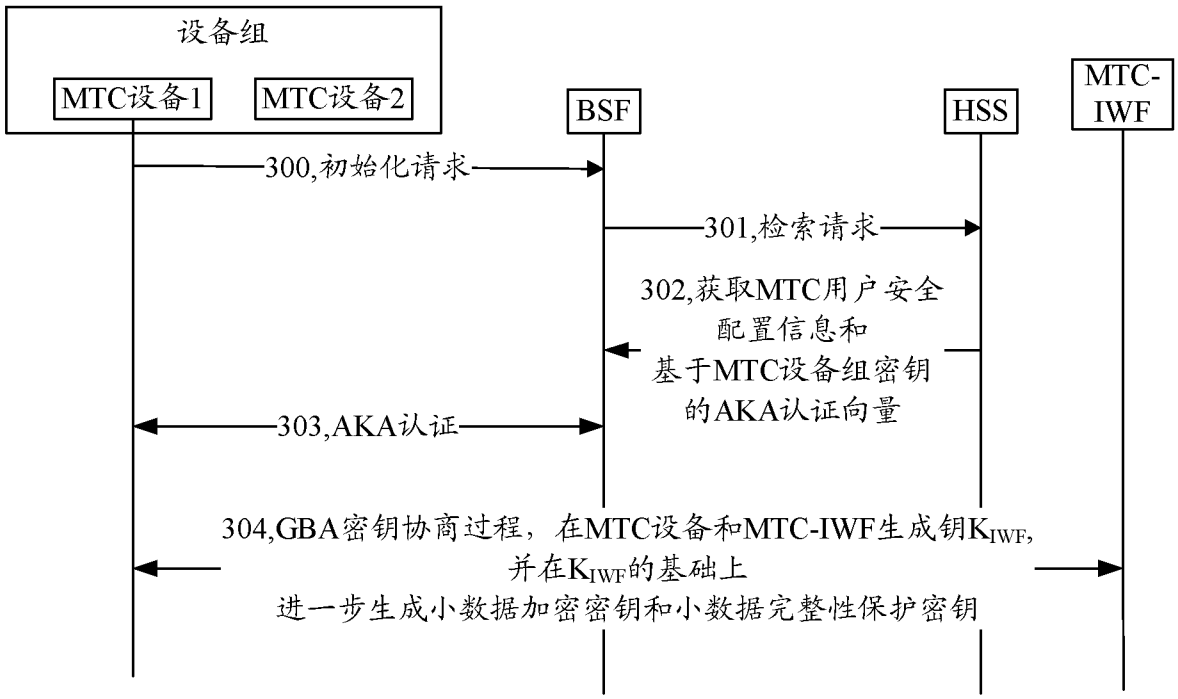
设备组
MTC设备1
MTC设备2
BSF
HSS
MTC-IWF
300,初始化请求
301,检索请求
302,获取MTC用户安全配置信息和基于MTC设备组密钥的AKA认证向量
303,AKA认证
304,GBA密钥协商过程，在MTC设备和MTC-IWF生成钥K_{IWF},并在K_{IWF}的基础上进一步生成小数据加密密钥和小数据完整性保护密钥

图 3

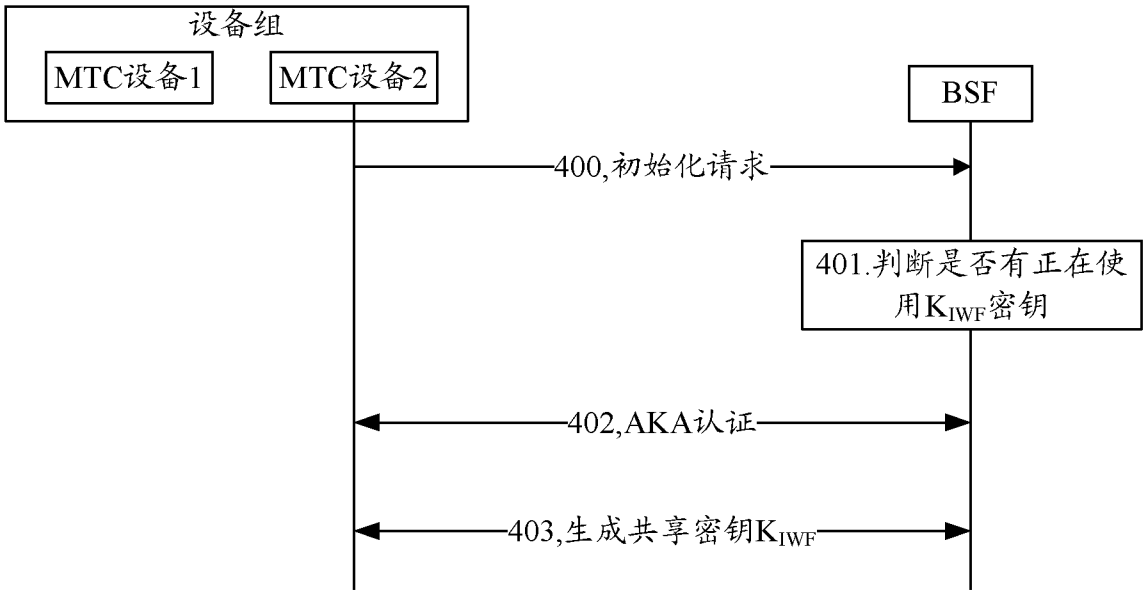
设备组
MTC设备1
MTC设备2
BSF
400,初始化请求
401.判断是否有正在使用K_{IWF}密钥
402,AKA认证
403,生成共享密钥K_{IWF}

图 4

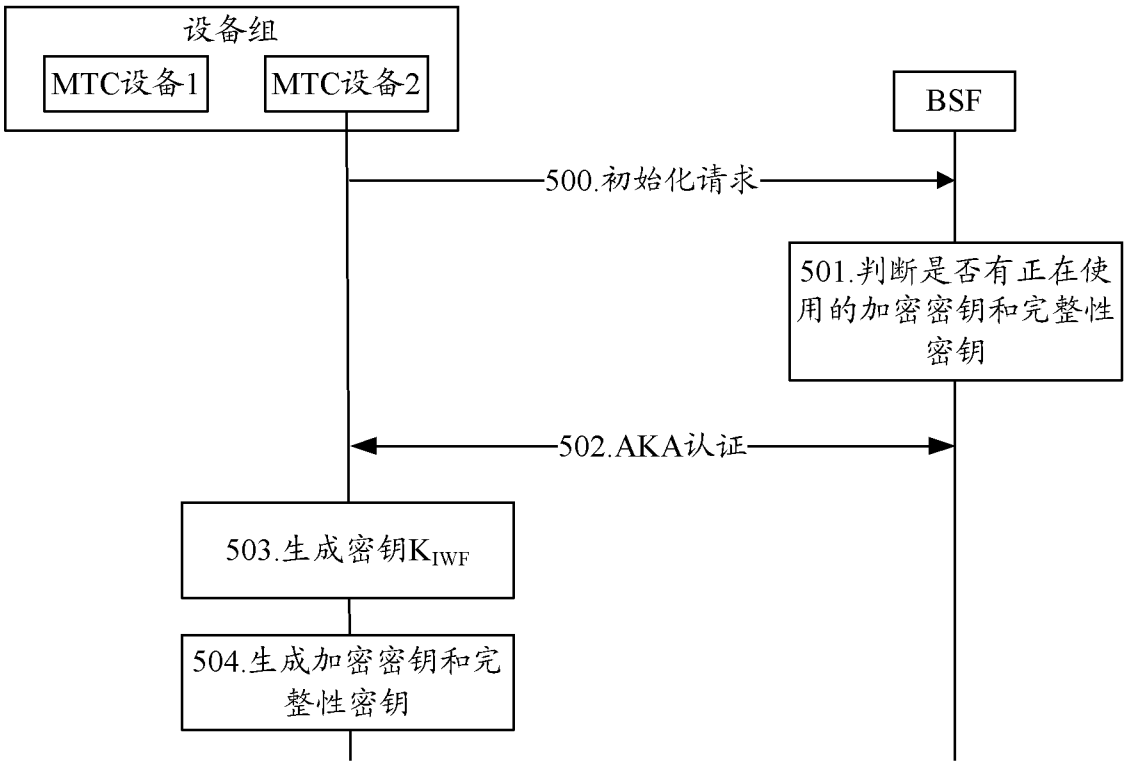
设备组
MTC设备1
MTC设备2
BSF
500.初始化请求
501.判断是否有正在使用的加密密钥和完整性密钥
502.AKA认证
503.生成密钥K_{IWF}
504.生成加密密钥和完整性密钥

图 5

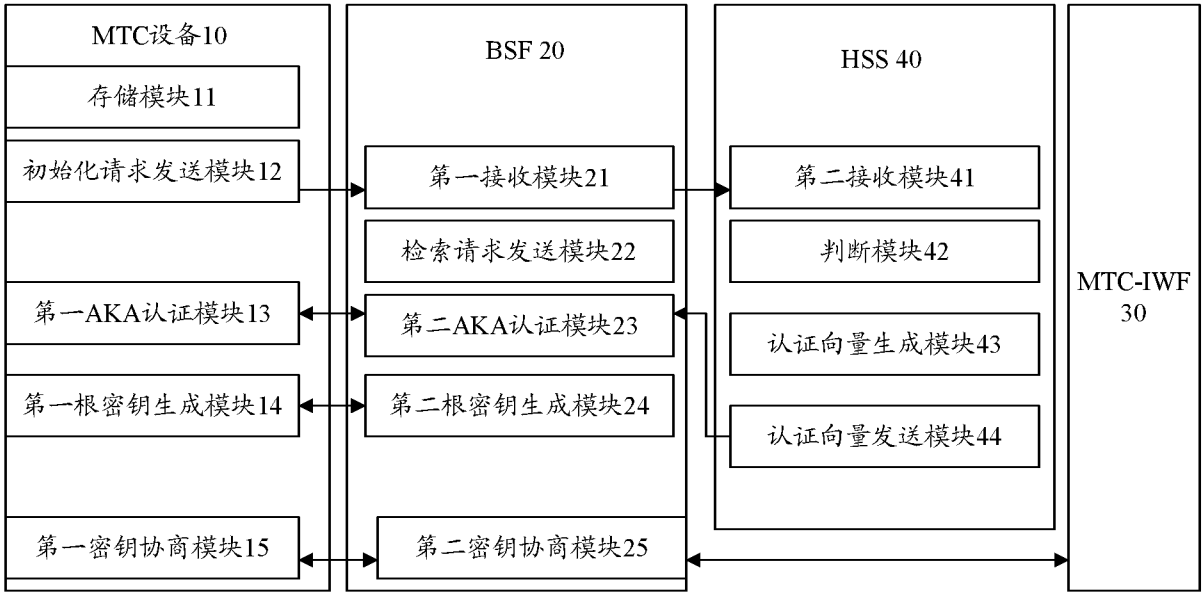
MTC设备10
存储模块11
初始化请求发送模块12
第一AKA认证模块13
第一根密钥生成模块14
第一密钥协商模块15
BSF 20
第一接收模块21
检索请求发送模块22
第二AKA认证模块23
第二根密钥生成模块24
第二密钥协商模块25
HSS 40
第二接收模块41
判断模块42
认证向量生成模块43
认证向量发送模块44
MTC-IWF 30

图 6

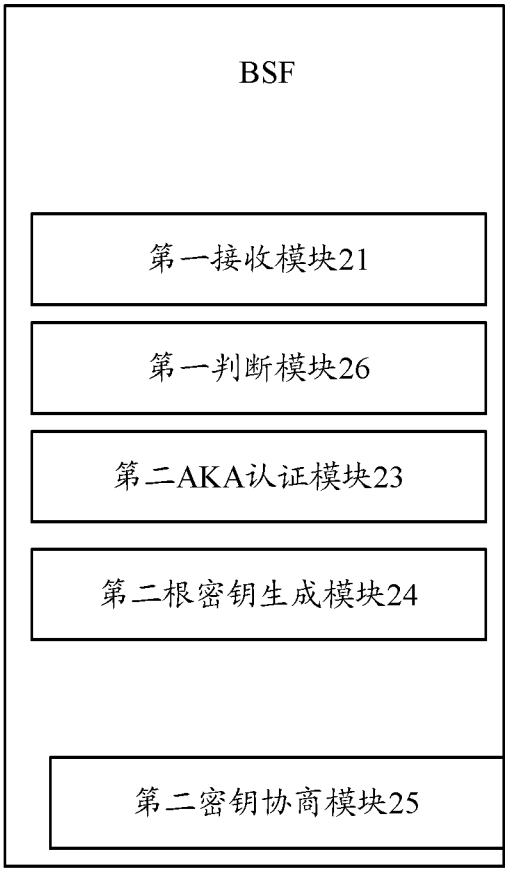
BSF
第一接收模块21
第一判断模块26
第二AKA认证模块23
第二根密钥生成模块24
第二密钥协商模块25

图 7

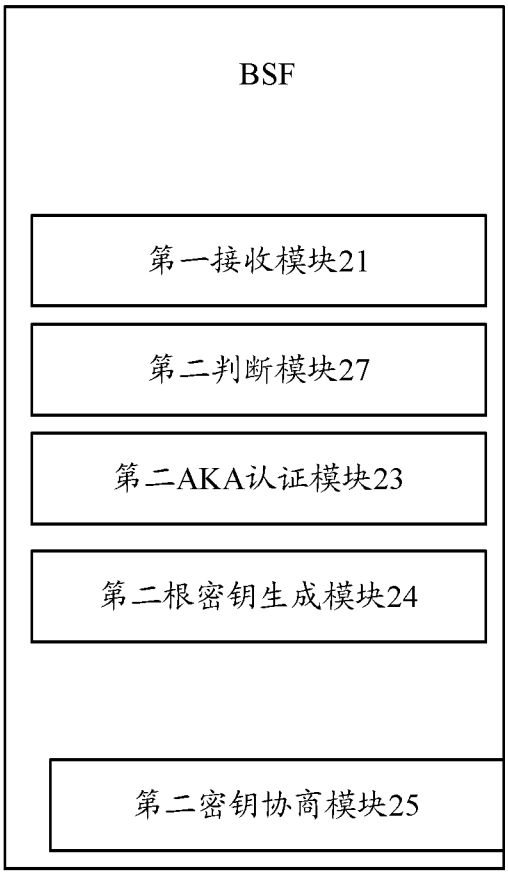
BSF
第一接收模块21
第二判断模块27
第二AKA认证模块23
第二根密钥生成模块24
第二密钥协商模块25

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/075724

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) 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)

H04W; H04Q; H04B; 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, SIPOABS, DWPI, WOTXT, EPTXT, USTXT, 3GPP: MTC, HSS, BSF, GBA, AKA, AV, G-ID, authentication, group, small data, key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 1878169 A (HUAWEI TECHNOLOGIES CO., LTD.), 13 December 2006 (13.12.2006), description, page 9, paragraph 1 to page 11, paragraph 3	1-24
A	CN 102572818 A (ZTE CORP.), 11 July 2012 (11.07.2012), description, paragraphs [0064]-[0077]	10, 11, 18, 19, 23, 24
A	CN 102469455 A (ZTE CORP.), 23 May 2012 (23.05.2012), the whole document	1-24

☐ 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
19 August 2014 (19.08.2014)	**03 September 2014 (03.09.2014)**
Name and mailing address of the ISA/CN: 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 **LU, Shan** Telephone No.: (86-10) **62089551**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/075724

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1878169 A	13 December 2006	None	
CN 10257281 A	11 July 2012	WO 2012075814 A1	14 June 2012
CN 102469455 A	23 May 2012	WO 2012062077 A1	18 May 2012

国际检索报告

国际申请号
PCT/CN2014/075724

A. 主题的分类

H04W 12/04(2009.01)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)

H04W; H04Q; H04B; 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, SIPOABS, DWPI, WOTXT, EPTXT, USTXT, 3GPP: MTC, HSS, BSF, GBA, AKA, AV, G-ID, 组，小数据，密钥，认证，group, small data, key

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 1878169 A (华为技术有限公司) 2006年 12月 13日 (2006-12-13) 说明书第9页第1段至第11页第3段	1-24
A	CN 102572818 A (中兴通讯股份有限公司) 2012年 7月 11日 (2012-07-11) 说明书第[0064]-[0077]段	10, 11, 18, 19, 23, 24
A	CN 102469455 A (中兴通讯股份有限公司) 2012年 5月 23日 (2012-05-23) 全文	1-24

☐ 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
2014年 8月 19日	2014年 9月 03日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国 传真号 (86-10)62019451	卢杉 电话号码 (86-10)62089551

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/075724

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 1878169 A	2006年 12月 13日	无	
CN 102572818 A	2012年 7月 11日	WO 2012075814 A1	2012年 6月 14日
CN 102469455 A	2012年 5月 23日	WO 2012062077 A1	2012年 5月 18日