

(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:

2005年2月10日(10.02.2005)

PCT

(10) 国际公布号:

WO 2005/013558 A1

- (51) 国际分类号⁷: H04L 12/26
- (21) 国际申请号: PCT/CN2003/001069
- (22) 国际申请日: 2003年12月16日(16.12.2003)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
03149767.5 2003年8月5日(05.08.2003) CN
- (71) 申请人(对除美国以外的所有指定国): 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)。

(81) 指定国(国家): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(84) 指定国(地区): ARIPO专利(BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

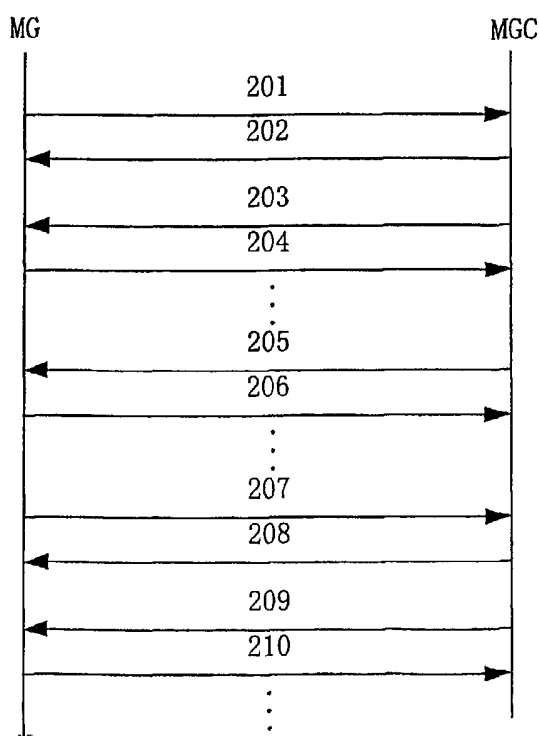
- (72) 发明人: 及
- (75) 发明人/申请人(仅对美国): 乔克智(QIAO, Kezhi) [CN/CN]; 倪明(NI, Ming) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

- (74) 代理人: 北京市中咨律师事务所(ZHONGZI LAW OFFICE); 中国北京市西城区阜成门北大街6号-9国际投资大厦C座17层, Beijing 100034 (CN)。

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号, 请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

- (54) Title: AUTHENTICATION METHOD FOR MEDIC GATEWAY
- (54) 发明名称: 媒体网关鉴权的方法



(57) Abstract: The present invention relates to an authentication method for Media Gateway, including the following step: Set up an initial key between the Media Gateway and Media Gateway Controller, for validate the both sides initial digital signature; performs signaling communication between the said Media Gateway and the said Media Gateway Controller by use of the said initial key, to generates a new shared key which have a special lifetime. The said Media Gateway and the said Media Gateway Controller authenticate the call and response using the said new shared key. If the lifetime of the said shared key is finished, then the said Media Gateway and the said Media Gateway Controller updates the said shared key. The invention authenticate each call, update the shared key periodic, prevent calling out illegally effectively.

[见续页]

WO 2005/013558 A1



(57) 摘要

本发明涉及媒体网关鉴权的方法，包括以下步骤：为媒体网关和媒体网关控制器之间设定一个用于验证双方初始数字签名的初始密钥；所述媒体网关和所述媒体网关控制器用所述初始密钥进行信令通信，以生成新的具有特定生存期的共享密钥；所述媒体网关和所述媒体网关控制器用所述新的共享密钥对呼叫和应答进行鉴权；若所述新的共享密钥的生存期结束，则所述媒体网关和所述媒体网关控制器更新所述共享密钥。本发明能对每个呼叫都进行鉴权，定期更换共享密钥，有效防止不合法呼叫。

媒体网关鉴权的方法

技术领域

- 5 本发明涉及通信技术领域，尤其涉及用 MEGACO/MGCP 协议实现媒体网关鉴权方法。

背景技术

- 10 媒体网关控制(Media Gateway Control, MEGACO) 协议是因特网工程业务组(The Internet Engineering Task Force, 简称 IETF)的 RFC3015 协议。

- 15 如图 1 所示为实现 MEGACO 协议的系统组网图。MEGACO 协议采用了分离网关思想，将原来信令和媒体集中处理的网关分解为两部分：媒体网关(Media Gateway, 简称 MG)和媒体网关控制器(Media Gateway Controller, 简称 MGC)。MGC 通过 MEGACO 协议控制 MG 的动作：MGC 向 MG 发出要执行的命令，MG 执行并将结果返回，媒体网关控制器 MGC 也要处理媒体网关 MG 主动上报所发生的事件请求。MEGACO 协议中的逻辑关系是通过连接模型来表示，连接模型中两个最基本的构件就是关联和终结点，关联表示了终结点之间的连接和拓扑关系。

- 20 媒体网关控制器 MGC 和媒体网关 MG 之间的主要命令包括 SERVICECHANGE(注册)，ADD(增加)，MODIFY(修改)，SUBTRACT(删除)，NOTIFY(通知)等等。

- 25 传统的媒体网关鉴权方法，当媒体网关 MG 注册完成后，通过一个不变的密钥定期对媒体网关 MG 进行鉴权：一方面用同一密钥长时间进行鉴权，易于被第三者破解；另一方面定期鉴权的方法，第三者易于通过只把鉴权消息过滤给真正 MG，使媒体网关控制器 MGC 和媒体网关 MG 之间成功鉴权，而伪造其它的 MG 消息发起呼叫；第三，原有的方法中只有媒体

网关控制器 MGC 对媒体网关 MG 鉴权，因此媒体网关 MG 有可能被不合法的媒体网关控制器 MGC 伪造消息对其呼叫。

发明内容

5 本发明的目的在于提供一种更加完备的对媒体网关鉴权机制，解决传统 MG 鉴权方法中第三者易于伪造媒体网关 MG 发起呼叫、易于伪造媒体网关控制器 MGC 呼叫媒体网关 MG 以及密钥长时间不变可能被人破解的问题，能对每个呼叫都进行鉴权，能定期更换共享密钥，有效防止不合法的伪造消息对其呼叫。

10 本发明是这样实现的：

 本发明公开了一种媒体网关鉴权的方法，包括：为媒体网关和媒体网关控制器之间设定一个用于验证双方初始数字签名的初始密钥；所述媒体网关和所述媒体网关控制器用所述初始密钥进行信令通信，以生成新的具有特定生存期的共享密钥；所述媒体网关和所述媒体网关控制器用所述新的共享密钥对呼叫和应答进行鉴权；若所述新的共享密钥的生存期结束，则所述媒体网关和所述媒体网关控制器更新所述共享密钥。

 优选地，所述生成共享密钥的步骤进一步包括：所述媒体网关向所述媒体网关控制器发起注册信令进行注册，所述注册信令中带有用于生成共享密钥的参数及由所述初始密钥生成的数字签名；所述媒体网关控制器用所述初始密钥验证所述媒体网关合法后，生成共享密钥并设定所述共享密钥的生存期；所述媒体网关控制器对所述媒体网关发起修改命令，所述修改命令中带有用于生成共享密钥的参数、由所述初始密钥生成的数字签名及共享密钥的生存期；所述媒体网关用所述初始密钥验证所述媒体网关控制器合法后，生成共享密钥并设定所述共享密钥的生存期。

 优选地，所述鉴权步骤进一步包括：所述媒体网关控制器用所述共享密钥在每次对媒体网关的呼叫消息中进行数字签名；所述媒体网关用所述共享密钥对所述呼叫消息中的所述数字签名进行验证，若合法，则

返回给所述媒体网关控制器带有用所述共享密钥数字签名的应答消息；所述媒体网关控制器用所述共享密钥对所述应答消息中的所述数字签名进行验证，若合法，则建立呼叫，否则，拒绝此次呼叫。

优选地，所述更新共享密钥的步骤进一步包括：所述媒体网关向所述媒体网关控制器发送通知命令，请求所述媒体网关控制器生成新的共享密钥，所述通知命令中带有用于生成共享密钥的参数和由所述初始密钥生成的数字签名；所述媒体网关控制器用所述初始密钥验证所述媒体网关合法后，生成新的共享密钥并设定所述共享密钥的生存期；所述媒体网关控制器对所述媒体网关发起修改命令，所述修改命令中带有用于生成共享密钥的参数、由所述初始密钥生成的数字签名及共享密钥的生存期；所述媒体网关用所述初始密钥验证所述媒体网关控制器合法后，生成共享密钥并设定所述共享密钥的生存期。

优选地，所述媒体网关控制器和所述媒体网关生成共享密钥采用的算法与所述媒体网关控制器和所述媒体网关生成数字签名的算法为不同的算法。

优选地，所述生成共享密钥的参数和数字签名的传送可以通过扩展协议的字段或包来实现。

优选地，所述共享密钥的生存期可以是时间，也可以是新的共享密钥可用于鉴权的次数。

采用本发明技术方案的有益效果，不仅能够定期更换密钥，防止长时间用同一密钥鉴权易于被破解；能够对媒体网关 MG 发起的每一个呼叫进行鉴权，解决了第三者通过过滤消息发起非法呼叫的问题；还能够防止媒体网关 MG 被不合法的媒体网关控制器 MGC 控制完成呼叫。

附图说明

图 1 示出了 MEGACO 协议系统的原理图；

图 2 示出了本发明实现媒体网关鉴权的流程示意图。

具体实施方式

本发明公开了一种媒体网关鉴权的方法，包括以下步骤：

设定媒体网关 MG 和媒体网关控制器 MGC 之间生成共享密钥采用的算法为 $y=f_1(x)$ ，设定 MG 和 MGC 之间生成数字签名采用的算法为 $y=f_2(x)$ ；

- 5 所述媒体网关控制器和所述媒体网关生成共享密钥的算法，以及所述媒体网关控制器和所述媒体网关生成数字签名的算法，可以根据安全级别的需要而采用合适算法，本发明对具体所用的算法不做限定。

- 媒体网关 MG 和媒体网关控制器 MGC 之间初始配有一个用于验证双方初始数字签名的密钥 S，媒体网关 MG 和媒体网关控制器 MGC 的密钥 S 可以不同，只要能验证对方的数字签名即可；密钥及参数的传送可以通过扩展 MEGACO 字段或包来实现。

- 媒体网关 MG 首先向媒体网关控制器 MGC 发起注册信令注册，并带有生成共享密钥的参数及数字签名。媒体网关控制器 MGC 验证合法后生成共享密钥，用修改命令发送给媒体网关 MG 生成共享密钥的参数、数字签名及设定共享密钥生存期，媒体网关 MG 收到后验证数字签名合法将生成共享密钥。

在后续的媒体网关控制器 MGC 和媒体网关 MG 之间的每一个呼叫建立及应答的消息中，媒体网关控制器 MGC 和媒体网关 MG 用共享密钥进行签名，相互验证合法后进行呼叫，否则拒绝呼叫。

- 20 当共享密钥生存期结束以后，媒体网关控制器 MGC 使原有的密钥无效；媒体网关 MG 需立刻用通知命令请求媒体网关控制器 MGC 生成新的共享密钥及获取新密钥的生存期。

如此不断变化密钥并用新的密钥对呼叫鉴权。

下面将结合附图，举例说明本发明的一个实施的方式。

- 25 图 2 所示的一种实现 MG 鉴权的详细过程。设定 MG 和 MGC 之间的初始密钥为 S。

201) 媒体网关 MG 向媒体网关控制器 MGC 发起注册消息，消息中带有用于媒体网关控制器 MGC 生成共享密钥的信息 M，并带有用密钥 S 对共

享密钥的信息 M 或注册消息生成的数字签名;

202) 媒体网关控制器 MGC 收到该消息后用密钥 S 验证数字签名, 如果成功则用共享密钥的信息 M 生成共享密钥 S', 并给媒体网关 MG 应答成功;

5 203) 媒体网关控制器 MGC 给媒体网关 MG 发修改 (MODIFY) 消息, 消息中带有用于媒体网关 MG 生成共享密钥的信息 N, 并带有用密钥 S 对共享密钥的信息 N 或整个消息生成的数字签名, 同时还带有新的共享密钥生存期: 生存期可以是一个时间, 也可以是新的共享密钥可用于鉴权的次数;

10 204) 媒体网关 MG 收到该消息后用密钥 S 验证数字签名, 如果成功则用共享密钥的信息 N 生成共享密钥 S', 并给媒体网关控制器 MGC 应答成功;

205) 在以后的每次呼叫建立的某个消息 (比如 ADD) 中, 媒体网关控制器 MGC 用新的共享密钥 S' 进行数字签名;

15 206) 媒体网关 MG 收到该消息后用新的共享密钥 S' 验证数字签名, 如果成功证明是合法的媒体网关控制器 MGC, 对媒体网关控制器 MGC 的应答也用新的共享密钥 S' 进行数字签名, 媒体网关控制器 MGC 收到后用新的共享密钥 S' 验证成功后建立呼叫, 否则为非法的媒体网关 MG, 拒绝该呼叫; 在媒体网关控制器 MGC 对媒体网关 MG 的定期鉴权中也用同样的方
20 法;

207) 当媒体网关控制器 MGC 设定的共享密钥生存期结束后, 媒体网关 MG 向媒体网关控制器 MGC 上报通知 (NOTIFY) 消息, 消息中带有用于媒体网关控制器 MGC 生成共享密钥的信息 M', 并带有用密钥 S 对共享密钥的信息 M' 或整个消息生成的数字签名;

25 208) 媒体网关控制器 MGC 收该消息后用密钥 S 验证数字签名, 如果成功则用共享密钥的信息 M' 生成共享密钥 S'', 并给媒体网关 MG 应答成功;

209) 媒体网关控制器 MGC 给媒体网关 MG 发修改 (MODIFY) 消息,

消息中带有用于媒体网关 MG 生成共享密钥的信息 N'，并带有用密钥 S 对共享密钥的信息 N' 或整个消息生成的数字签名，同时还带有新的共享密钥生存期；媒体网关 MG 用共享密钥的信息 N' 生成新的共享密钥 S''，并用新的共享密钥 S'' 对后续呼叫鉴权及定期鉴权；

5 210) 媒体网关 MG 给媒体网关控制器 MGC 成功的应答。

新的共享密钥 S'' 生存期到后再重复 207) -- 210) 步骤生成新的共享密钥 S'''，依次类推。

10 尽管参照实施例对所公开的涉及使用 MEGACO 协议实现对媒体网关鉴权的方法进行了特别描述，本领域技术人员将能理解，在不偏离本发明的范围和精神的条件下，可以对它进行形式和细节的种种显而易见的修改。例如，由于 MEGACO 协议和 MGCP 协议的相似性，本法的技术方案的实质内同对于使用 MGCP 协议实现媒体网关鉴权同样适用。因此，以上描述的实施例是说明性的而不是限制性的，在不脱离本发明的精神和范围的情况下，所有的变化和修改都在本发明的范围之内。

15

权利要求

1. 一种媒体网关鉴权的方法，其特征在于，该方法包括：
为媒体网关和媒体网关控制器之间设定一个用于验证双方初始数字签名的初始密钥；
5 所述媒体网关和所述媒体网关控制器用所述初始密钥进行信令通信，以生成新的具有特定生存期的共享密钥；
 所述媒体网关和所述媒体网关控制器用所述新的共享密钥对呼叫和应答进行鉴权；
 若所述新的共享密钥的生存期结束，则所述媒体网关和所述媒体网关控制器更新所述共享密钥。
10 2. 如权利要求1所述的方法，其特征在于，所述生成共享密钥的步骤进一步包括：
 所述媒体网关向所述媒体网关控制器发起注册信令进行注册，所述注册信令中带有用于生成共享密钥的参数及由所述初始密钥生成的数字
15 签名；
 所述媒体网关控制器用所述初始密钥验证所述媒体网关合法后，生成共享密钥并设定所述共享密钥的生存期；
 所述媒体网关控制器对所述媒体网关发起修改命令，所述修改命令中带有用于生成共享密钥的参数、由所述初始密钥生成的数字签名及共
20 享密钥的生存期；
 所述媒体网关用所述初始密钥验证所述媒体网关控制器合法后，生成共享密钥并设定所述共享密钥的生存期。
 3. 如权利要求1所述的方法，其特征在于，所述鉴权步骤进一步包括：
25 所述媒体网关控制器用所述共享密钥在每次对媒体网关的呼叫消息中进行数字签名；
 所述媒体网关用所述共享密钥对所述呼叫消息中的所述数字签名进行验证，若合法，则返回给所述媒体网关控制器带有所述共享密钥数

字签名的应答消息;

所述媒体网关控制器用所述共享密钥对所述应答消息中的所述数字签名进行验证, 若合法, 则建立呼叫, 否则, 拒绝此次呼叫。

4. 如权利要求 1 所述的方法, 其特征在于, 所述更新共享密钥的步骤进一步包括:

所述媒体网关向所述媒体网关控制器发送通知命令, 请求所述媒体网关控制器生成新的共享密钥, 所述通知命令中带有用于生成共享密钥的参数和由所述初始密钥生成的数字签名;

- 所述媒体网关控制器用所述初始密钥验证所述媒体网关合法后, 生成新的共享密钥并设定所述共享密钥的生存期;

所述媒体网关控制器对所述媒体网关发起修改命令, 所述修改命令中带有用于生成共享密钥的参数、由所述初始密钥生成的数字签名及共享密钥的生存期;

- 所述媒体网关用所述初始密钥验证所述媒体网关控制器合法后, 生成共享密钥并设定所述共享密钥的生存期。

5. 如权利要求 2、3 或 4 所述的方法, 其特征在于, 所述媒体网关控制器和所述媒体网关生成共享密钥采用的算法与所述媒体网关控制器和所述媒体网关生成数字签名的算法为不同的算法。

6. 如权利要求 2、3 或 4 所述的方法, 其特征在于, 所述生成共享密钥的参数和数字签名的传送可以通过扩展协议的字段或包来实现。

7. 如权利要求 1 所述的方法, 其特征在于, 所述共享密钥的生存期可以是时间, 也可以是新的共享密钥可用于鉴权的次数。

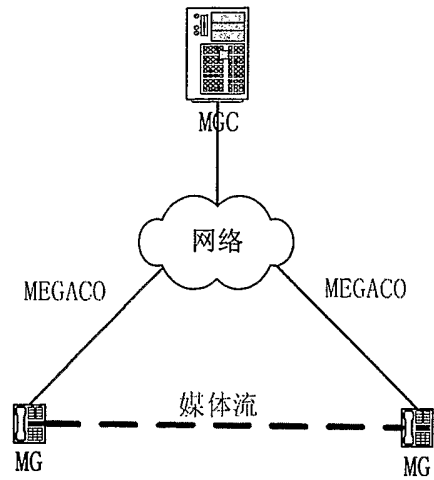


图 1

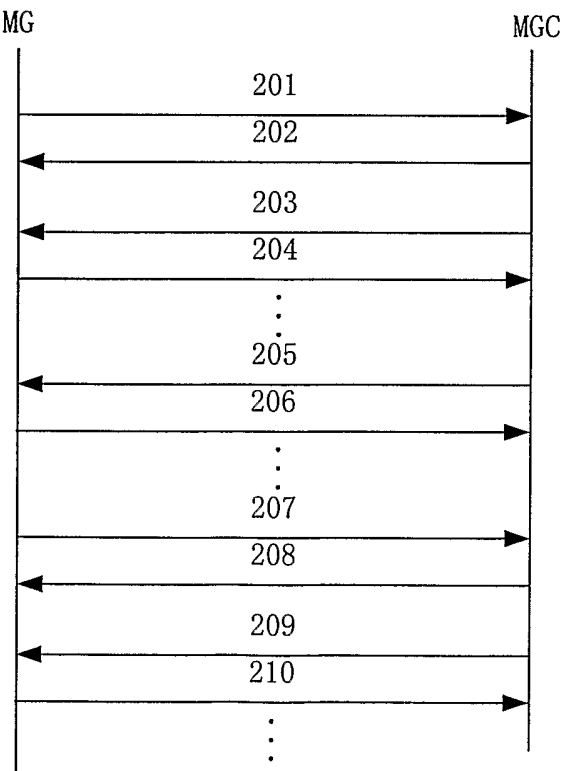


图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN03/01069

A. CLASSIFICATION OF SUBJECT MATTER

IPC7:H04L12/26

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)

IPC7: H04L12/00

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)

WPI, EPODOC, PAJ, CNPAT: media gateway controller key authenticity initial signaling life time share

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO A2 02054201, (INTEL CORP) 11.July.2002(11.07.2002) Whole document	1—7
A	CN A 1411224, (HUAWEI TECH CO LTD) ,16.April.2003(16.04.2003)Whole document	1—7
A	CN A 1308472, (LUCENT TECHNOLOGIES INC) ,15.August.2001(15.08.2001) Whole document	1,4

☐ 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	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“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
“O” document referring to an oral disclosure, use, exhibition or other means	“&” document member of the same patent family
“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.June.2004(22.06.2004)

Date of mailing of the international search report
08 . JUL 2004 (08 . 07 . 2004)

Name and mailing address of the ISA/CN
6 Xitucheng Rd., Jimen Bridge, Haidian District,
100088 Beijing, China
Facsimile No. 86-10-62019451

Authorized officer 华李
LI Zhen Hua
Telephone No. 86-10-62084559

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN03/01069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO A2 02054201	11.July.2002	US A1 2002087858	04.July.2002
CN A 1411224	16.April.2003	WO,A1,03030464	10.April.2003
CN A 1308472	15.August.2001	EP A2 1124401	16.August.2001
		AU,A 1828001	16.August.2001
		JP A 2001251292	14.September.2001

国际检索报告

国际申请号
PCT/CN03/01069

A. 主题的分类

IPC7:H04L12/26

按照国际专利分类表(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(标明分类体系和分类号)

IPC7: H04L12/00

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, 如果实际可行的, 使用的检索词)

WPI, EPODOC, PAJ, CNPAT: media gateway controller key authenticity initial signaling life time share
媒体网关 控制器 密钥 鉴权 初始 信令 生存期 共享

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求编号
A	WO A2 02054201, (因特尔有限公司), 11.7 月.2002(11.07.2002) 全文	1—7
A	CN A 1411224, (华为技术有限公司), 16.4 月.2003(16.04.2003) 全文	1—7
A	CN A 1308472, (朗讯科技有限公司), 15.8 月.2001(15.08.2001) 全文	1,4

☐ 其余文件在 C 栏的续页中列出。☒ 见同族专利附件。

* 引用文件的专用类型:

“A” 明确叙述了被认为不是特别相关的一般现有技术的文件

“E” 在国际申请日的当天或之后公布的在先的申请或专利

“L” 可能引起对优先权要求的怀疑的文件, 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

“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的在后文件, 它与申请不相抵触, 但是引用它是为了理解构成发明基础的理论或原理

“X” 特别相关的文件, 仅仅考虑该文件, 权利要求所记载的发明就不能认为是新颖的或不能认为是有创造性

“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, 权利要求记载的发明不具有创造性

“&” 同族专利成员的文件

国际检索实际完成的日期

22.6 月.2004 年(22.06.2004)

国际检索报告邮寄日期

08 · 7 月 2004 (08 · 07 · 2004)

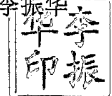
国际检索单位名称和邮寄地址

ISA/CN

中国北京市海淀区西土城路 6 号(100088)

传真号: 86-10-62019451

受权官员 李振华



电话号码: 86-10-62084559

国际检索报告
关于同族专利成员的情报

国际申请号
PCT/CN03/01069

检索报告中引用的 专利文件	公布日期	同族专利成员	公布日期
WO A2 02054201	11.7 月.2002	US A1 2002087858	04.7 月.2002
CN A 1411224	16.4 月.2003	WO,A1,03030464	10.4 月.2003
CN A 1308472	15.8 月.2001	EP A2 1124401	16.8 月.2001
		AU,A 1828001	16.8 月.2001
		JP A 2001251292	14.9 月.2001