

(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 2 月 27 日 (27.02.2014)



(10) 国际公布号
WO 2014/029169 A1

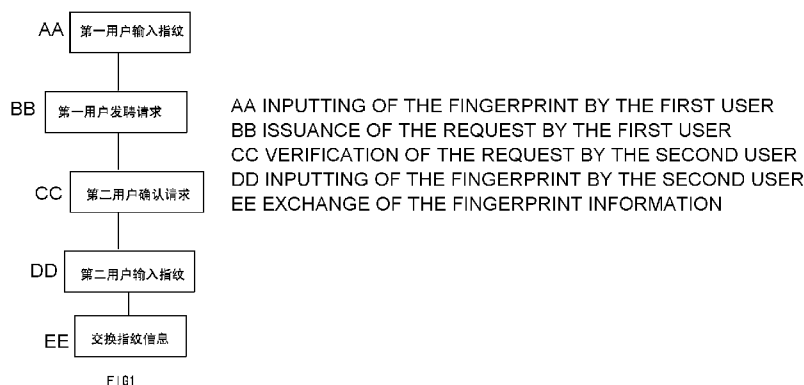
- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2012/084427
- (22) 国际申请日: 2012 年 11 月 10 日 (10.11.2012)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201210297631.5 2012 年 8 月 21 日 (21.08.2012) CN
- (71) 申请人 (对除美国外的所有指定国): **鹤山世达光电科技有限公司 (WTT TECHNOLOGY CHINA)** [CN/CN]; 中国广东省江门市鹤山市共和镇新材料基地 (鹤山市世逸电子科技有限公司 H 座), Guangdong 529728 (CN)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): **王国芳 (WONG, Kwok Fong)** [CN/CN]; 中国广东省江门市鹤山市共和镇新材料基地 (鹤山市世逸电子科技有限公司 H 座), Guangdong 529728 (CN)。
程佩仪 (CHING, Pui Yi) [CN/CN]; 中国广东省江门市鹤山市共和镇新材料基地 (鹤山市世逸电子科技有限公司 H 座), Guangdong 529728 (CN)。

- (74) 代理人: 佛山东平知识产权事务所 (普通合伙) (FOSHAN DONG PING INTELLECTUAL PROPERTY FIRM (GENERAL PARTNERSHIP)); 中国广东省佛山市禅城区岭南大道北 123 号一座 1508 室, Guangdong 528000 (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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: COMMUNICATION METHOD UTILIZING FINGERPRINT INFORMATION FOR AUTHENTICATION

(54) 发明名称: 利用指纹信息认证的通信方法



(57) Abstract: Disclosed is a communication method utilizing fingerprint information for authentication. The method comprises the following steps: a fingerprint information exchange stage, when a request instruction is received, a second user verifies a request and extracts the fingerprint information thereof via a collection and identification device of a fingerprint sensing device, the second user stores the fingerprint information thereof to an information exchange platform and performs an exchange with a first user to verify the identities of both parties; an encryption and transmission stage, the identity of the first user is authenticated, after passing the authentication, the first user inputs in an encryption unit information that needs to be transmitted, performs encryption via the encryption unit to acquire encrypted information that needs to be transmitted, and introduces into a communication application unit the encrypted information that needs to be transmitted and forwards same to the second user, while the second user receives the encrypted information via the communication application unit; and, a decryption and reading stage, the identity of the second user is authenticated, after passing the authentication, the second user performs decryption via a decryption unit.

(57) 摘要:

[见续页]



WO 2014/029169 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开一种利用指纹信息认证的通信方法，它包括以下步骤：交换指纹信息阶段，第二用户收到请求指令后确认请求并通过指纹传感装置的采集识别装置提取其指纹信息，第二用户将其指纹信息存储至信息交换平台并与第一用户进行交换以确认双方的身份；加密发送阶段，认证第一用户的身份，当通过认证后第一用户在加密单元中输入需要发送的信息，并通过加密单元进行加密得到需要发送的加密信息，将需要发送的加密信息导入通信应用单元中并发送给第二用户，所述第二用户通过通信应用单元接收到加密信息；解密读取阶段，认证第二用户的身份，当通过认证后第二用户通过解密单元进行解密。

发明名称: 利用指纹信息认证的通信方法

技术领域

- [1] 本发明涉及一种利用指纹信息认证的通信方法。

背景技术

- [2] 目前, 人们无论在使用各种各样的聊天软件或者其他发布即时消息的软件进行聊天的时候, 总有些信息是不想别人看到的。例如, 双方聊天的时候, 第三方在旁边经过, 总是不经意就会看到聊天的内容; 又或者群聊的时候, 我只喜欢某人见到信息, 但是又不想单独的发起私聊, 目前的聊天软件是不能解决这个问题, 那么我们需要一种能只让特定的人收看到特定的信息, 确保聊天内容或者发布信息的秘密性的解决方法。

对发明的公开

技术问题

- [3] 本发明的目的是提供一种利用指纹信息认证的通信方法, 在利用指纹认证以及不改变原有的通信应用单元的基础下, 增加聊天的秘密性和安全性。

问题的解决方案

技术解决方案

- [4] 发明所采用的技术方案是一种利用指纹信息认证的通信方法, 它包括以下步骤:
- [5] A) 交换指纹信息阶段:
- [6] 第一用户通过指纹传感装置的采集识别装置提取其指纹信息并上传至信息交换平台, 第一用户通过其指纹信息在信息交换平台中向第二用户发出请求指令, 第二用户收到请求指令后确认请求并通过指纹传感装置的采集识别装置提取其指纹信息, 第二用户将其指纹信息存储至信息交换平台并与第一用户进行交换以确认双方的身份;
- [7] B) 加密发送阶段:
- [8] 指纹传感装置的采集识别装置提取第一用户的指纹信息, 并认证第一用户的身

份，当通过认证后，第一用户在加密单元中输入需要发送的信息，并通过加密单元进行加密得到需要发送的加密信息，将需要发送的加密信息导入通信应用单元中并发送给第二用户，所述第二用户通过通信应用单元接收到加密信息；

[9] C) 解密读取阶段：

[10] 指纹传感装置的采集识别装置提取第二用户的指纹信息，并认证第二用户的身份，当通过认证后，第二用户通过解密单元进行解密。

[11] 优选地，在步骤A) 交换指纹信息阶段，通过指纹传感装置的采集识别装置提取第一用户的指纹信息，并生成相对应的第一公匙和第一私匙，将第一私匙保存在指纹传感装置的存储器中，将第一公匙存储至信息交换平台，第一用户通过第一公匙向第二用户发出请求指令，第二用户收到请求指令后确认请求并通过指纹传感装置的采集识别装置提取自己的指纹信息，生成第二公匙和第二私匙，第二私匙保存在指纹传感装置的存储器中，将第二公匙存储至信息交换平台并与第一用户的第一公匙进行交换；

[12] 在步骤B) 加密发送阶段：指纹传感装置的采集识别装置提取其指纹信息，并将该指纹信息与在步骤A) 中存储至指纹传感装置的存储器中的第一私匙进行比对，当一致时，第一用户通过认证；

[13] 在步骤C) 解密读取阶段：指纹传感装置的采集识别装置提取其指纹信息，并将该指纹信息生成的私匙与在步骤A) 中存储至指纹传感装置的存储器中的第二私匙进行比对，当一致时，第二用户通过认证。

[14] 优选地，所述信息交换平台为主机或服务器。

[15] 优选地，所述通信应用单元可以是微博、QQ、MSN、SKYPE中的一种或几种。

[16] 优选地，第一用户与第二用户之间通过通信应用单元的信息传输可通过网络、红外、蓝牙中的一种或几种。

发明的有益效果

有益效果

[17] 本发明采用以上方法能够使人们可以利用指纹对信息进行加解密管理，从而使任何非指纹所有人均不能查看加密信息，在原有的基础上增强了用户信息及隐

私的保密性、安全性。

对附图的简要说明

附图说明

[18] 附图1为本发明中交换指纹信息阶段的流程示意图。

[19] 附图2为本发明中加密发送阶段的流程示意图。

[20] 附图3为本发明中解密读取阶段的流程示意图。

[21] 附图4为本发明交换指纹信息阶段结构原理框图。

实施该发明的最佳实施例

本发明的最佳实施方式

[22] 下面结合附图对本发明的较佳实施例进行详细阐述，以使本发明的优点和特征能更易于被本领域技术人员理解，从而对本发明的保护范围做出更为清楚明确的界定。

[23] 如附图1-4所示，一种利用指纹信息认证的通信方法，它包括以下步骤：

[24] A) 交换指纹信息阶段：

[25] 如图1和4所示，第一用户通过指纹传感装置的采集识别装置提取其指纹信息并上传至信息交换平台，第一用户通过其指纹信息在信息交换平台中向第二用户发出请求指令，第二用户收到请求指令后确认请求并通过指纹传感装置的采集识别装置提取其指纹信息，第二用户将其指纹信息存储至信息交换平台并与第一用户进行交换以确认双方的身份。

[26] B) 加密发送阶段：

[27] 如图2所示，第一用户通过指纹传感装置的采集识别装置提取其指纹信息，并认证第一用户的身份，当通过认证后第一用户在加密单元中输入需要发送的信息，并通过加密单元进行加密，将完成加密的需要发送的信息导入通信应用单元中并发送给第二用户，所述第二用户通过通信应用单元接收到加密的信息；

[28] C) 解密读取阶段：

[29] 如图3所示，第二用户通过指纹传感装置的采集识别装置提取其指纹信息，并认证第二用户的身份，当通过认证后第二用户通过解密单元进行解密。

[30] 在本实施例中，指纹传感装置包括采集识别装置以及存储器。采集识别装置能

够对指纹进行提取操作，并且还能够对指纹信息与存储在存储器中的指纹信息进行识别比对和认证操作。存储器主要存储指纹认证信息和用户交换的以及进行信息加解密的私匙。

[31] 信息交换平台与指纹传感装置相交互连接。信息交换平台可以是一台主机，也可以是一个网络服务器，其主要用于在用户间进行指纹信息的交换，达到交换公匙的目的，并最终完成用户之间的身份确认。

[32] 如图1和4所示，指纹传感装置的采集识别装置提取第一用户的指纹信息，并生成一对相对应的第一公匙和第一私匙，将第一私匙保存在指纹传感装置的存储器中，将第一公匙存储至信息交换平台，第一用户通过第一公匙在信息交换平台中向第二用户发出请求指令，第二用户收到请求指令后确认请求并通过指纹传感装置的采集识别装置提取自己的指纹信息，生成第二公匙和第二私匙，第二私匙保存在指纹传感装置的存储器中，将第二公匙存储至信息交换平台并与第一用户的第一公匙进行交换。

[33] 如图2所示，加密单元可以是设置在指纹传感装置上，也可以采用各种其他的加密工具。该加密单元利用了指纹信息，对于将要发送的信息进行了加密。加密后的信息在未解密前，该信息变成乱码、代码、图形等与正常阅读时不同的各种形式。因此该信息在未解密前无法被他人阅读。

[34] 指纹传感装置的采集识别装置提取第一用户的指纹信息，并将该指纹信息与在步骤A)中存储至指纹传感装置的存储器中的第一私匙进行识别比对。如果不同时，第一用户没有通过认证不能进行接下的操作。

[35] 如果一致时，第一用户通过认证后可在加密单元中输入需要发送的信息，加密单元对将要发送的信息进行加密得到需要发送的加密信息。将需要发送的加密信息导入通信应用单元中发送给第二用户，第二用户通过通信应用单元接收到加密信息。

[36] 通信应用单元可以是目前互联网流行的各种聊天应用软件或其他各种即时信息的应用，如微博，QQ，MSN，skype等等。

[37] 如图3所示，指纹传感装置的采集识别装置提取第二用户的指纹信息，并将该指纹信息生成的私匙与在步骤A)中存储至指纹传感装置的存储器中的第二私匙

进行识别比对。当不同时，第二用户没有通过认证，不能进行下一步的操作。当一致时，第二用户通过认证。此时，第二用户可利用解密单元对接受到的加密信息进行解密。该解密软件应该与加密软件相对应，能够逆向识别出信息。

[38] 解密后，原始乱码的文字或图形可自动重组形成正常字体的文字，也可以是鼠标处于乱码文字中的任意处位置，任意处位置的乱码文字变成正常字体或放大的文字。这样，其他用户即使在第二用户操作，但是由于他不具有第二用户的指纹信息，无法对聊天内容进行解密。因此，本方法较之以往具有更好的安全性。

[39] 以上对本发明的特定实施例结合图示进行了说明，很明显，在不离开本发明的范围和精神的基礎上，可以对现有技术和工艺进行很多修改。在本发明的所属技术领域，只要掌握通常知识，就可以在本发明的技术要旨范围内，进行多种多样的变更。

权利要求书

[权利要求 1]

一种利用指纹信息认证的通信方法，其特征在于，它包括以下步骤：

A) 交换指纹信息阶段：

第一用户通过指纹传感装置的采集识别装置提取其指纹信息并上传至信息交换平台，第一用户通过其指纹信息在信息交换平台中向第二用户发出请求指令，第二用户收到请求指令后确认请求并通过指纹传感装置的采集识别装置提取其指纹信息，第二用户将其指纹信息存储至信息交换平台并与第一用户进行交换以确认双方的身份；

B) 加密发送阶段：

指纹传感装置的采集识别装置提取第一用户的指纹信息，并认证第一用户的身份，当通过认证后，第一用户在加密单元中输入需要发送的信息，并通过加密单元进行加密得到需要发送的加密信息，将需要发送的加密信息导入通信应用单元中并发送给第二用户，所述第二用户通过通信应用单元接收到加密信息；

C) 解密读取阶段：

指纹传感装置的采集识别装置提取第二用户的指纹信息，并认证第二用户的身份，当通过认证后，第二用户通过解密单元进行解密，第二用户对解密后的信息进行读取。

[权利要求 2]

根据权利要求1所述的利用指纹信息认证的通信方法，其特征在于：

在步骤A)交换指纹信息阶段，通过指纹传感装置的采集识别装置提取第一用户的指纹信息,并生成相对应的第一公匙和第一私匙，将第一私匙保存在指纹传感装置的存储器中,将第一公匙存储至信息交换平台，第一用户通过第一公匙向第二用户发出请求指令,第二用户收到请求指令后确认请求并通过指纹传感装置的采集识别装置提取自己的指纹信息，生成第二公匙和第二私匙，第二私匙

保存在指纹传感装置的存储器中，将第二公匙存储至信息交换平台并与第一用户的第一公匙进行交换；

在步骤B) 加密发送阶段：指纹传感装置的采集识别装置提取其指纹信息，并将该指纹信息与在步骤A) 中存储至指纹传感装置的存储器中的第一私匙进行比对，当一致时，第一用户通过认证；

在步骤C) 解密读取阶段：指纹传感装置的采集识别装置提取其指纹信息，并将该指纹信息生成的私匙与在步骤A) 中存储至指纹传感装置的存储器中的第二私匙进行比对，当一致时，第二用户通过认证。

[权利要求 3] 根据权利要求1所述的利用指纹信息认证的通信方法，其特征在于：
所述信息交换平台为主机或服务器。

[权利要求 4] 根据权利要求1所述的利用指纹信息认证的通信方法，其特征在于：
所述通信应用单元可以是微博、QQ、MSN、SKYPE中的一种或几种。

[权利要求 5] 根据权利要求1所述的利用指纹信息认证的通信方法，其特征在于：
第一用户与第二用户之间通过通信应用单元的信息传输可通过网络、红外、蓝牙中的一种或几种。

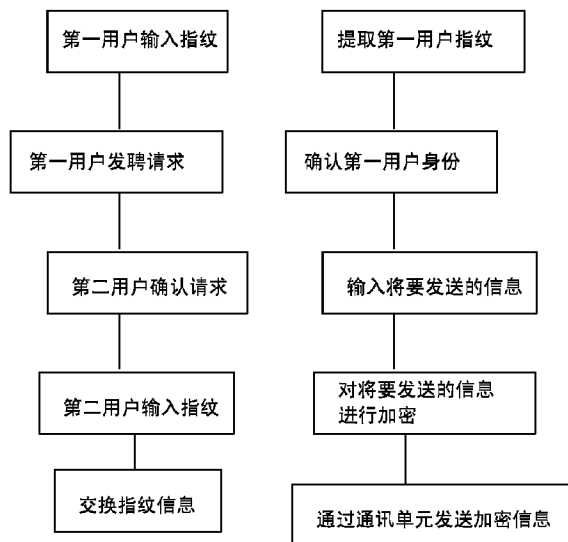


FIG1

FIG2

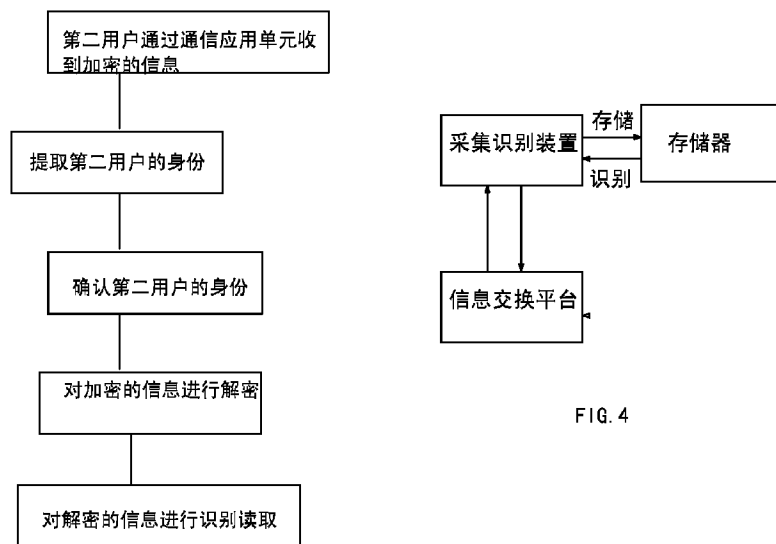


FIG. 3

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/084427

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)

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)

CNKI, CNABS, VEN: dactylogram, fingerprint, authentication, distill, distinguish, identify, public 1w key, private 1w key, encrypt, information, message, transmit+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102638459 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 15 August 2012 (15.08.2012) see claims 1 to 5	1-5
Y	CN 101340285 A (HANGZHOU ZHONGZHENG BIOLOGICAL IDENTIFIC) 07 January 2009 (07.01.2009) see claims 1 and 5	1-5
A	CN 1859092 A (LIU R) 08 November 2006 (08.11.2006) see the whole document	1-5

☐ 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 05 May 2013 (05.05.2013)	Date of mailing of the international search report 30 May 2013 (30.05.2013)
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 PAN, Bin Telephone No. (86-10) 62412162

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/084427

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102638459 A	15.08.2012	None	
CN 101340285 A	07.01.2009	None	
CN 1859092 A	08.11.2006	None	

国际检索报告

国际申请号
PCT/CN2012/084427

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)

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))

CNKI,CNABS,VEN: 指纹, 认证, 提取, 识别, 公匙, 私匙, 公钥, 私钥, 加密, 信息, 发送, dactylogram, fingerprint, authentication, distill, distinguish, identify, public 1w key, private 1w key, encrypt, information, message, transmit+

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
Y	CN102638459A (腾讯科技(深圳)有限公司) 15.8 月 2012 (15.08.2012)	1-5
	权利要求 1-5	
Y	CN101340285A (杭州中正生物认证技术有限公司) 07.1 月 2009 (07.01.2009) 权利要求 1, 5	1-5
A	CN1859092A (刘瑞祯) 08.11 月 2006 (08.11.2006) 全文	1-5

☐ 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
05.5 月 2013 (05.05.2013)

国际检索报告邮寄日期
30.5 月 2013 (30.05.2013)

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

授权官员

潘斌
电话号码: (86-10) **62412162**

国际申请号
PCT/CN2012/084427

PCT/ISA/210 表(同族专利附件) (2009 年 7 月)