

# (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 7 月 27 日 (27.07.2017)



(10) 国际公布号  
WO 2017/124954 A1

- (51) 国际专利分类号:  
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2017/070907
- (22) 国际申请日: 2017 年 1 月 11 日 (11.01.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201610041698.0 2016 年 1 月 21 日 (21.01.2016) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 范鑫 (FAN, Xin) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。李华明 (LI, Huaming) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。汤鑫 (TANG, Xin) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。吴

大瑞 (WU, Darui) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

- (74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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, DJ, 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, KH, KN, KP, KR, KW, 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, 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,

[见续页]

(54) Title: METHOD AND SYSTEM FOR LOCATING MALICIOUS ACCOUNT THROUGH MISSING ACCOUNT

(54) 发明名称: 一种通过丢失账号定位恶意账号的方法和系统

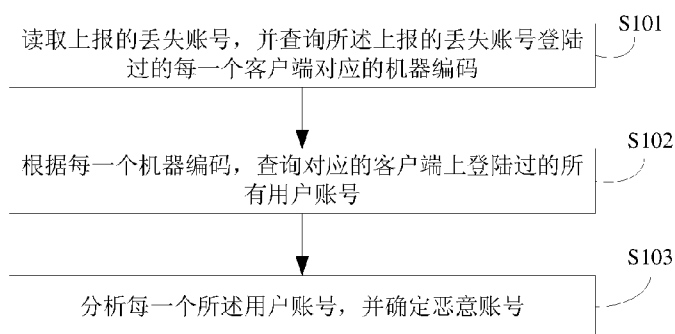


图1

- S101 READING A REPORTED MISSING ACCOUNT, AND QUERYING MACHINE CODES CORRESPONDING TO EACH CLIENT LOGGED IN BY THE REPORTED MISSING ACCOUNT
- S102 ACCORDING TO EACH MACHINE CODE, QUERYING ALL USER ACCOUNTS LOGGED IN ON THE CORRESPONDING CLIENT
- S103 ANALYZING EACH OF THE USER ACCOUNTS TO DETERMINE THE MALICIOUS ACCOUNT

(57) Abstract: Disclosed in the present application is a method and a system for locating a malicious account through a missing account, the method comprising: reading a reported missing account, and querying machine codes corresponding to each client logged in by the reported missing account; according to each of the machine codes, querying all user accounts logged in on the corresponding client; and analyzing each of the user accounts to determine the malicious account and other missing accounts. According to the method and the system for locating the malicious account through a missing account proposed by the embodiment of the present application, the malicious account can be analyzed through the correspondence between the machine code and the user account, so as to crack down on hackers or criminals from the source, and to solve the problem in the prior art that hackers or criminals cannot be tracked.

(57) 摘要: 本申请公开一种通过丢失账号定位恶意账号的方法和系统, 该方法包括: 读取上报的丢失账号, 并查询该上报的丢失账号登陆过的每一个客户端对应的机器编码; 根据每一个机器编码, 查询对应的客户端上登陆过的所有用户账号; 分析每一个所述用户账号, 确定恶意账号和其他丢失账号。本申请实施例提出的通过丢失账号定位恶意账号的定位方法和系统, 从源头上打击黑客或不法分子, 解决了现有技术

中, 能够通过机器编码和用户账号的对应关系分析恶意账号, 中无法跟踪黑客或不法分子的问题。



WO 2017/124954 A1



RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, **本国际公布:**

CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, — 包括国际检索报告(条约第 21 条(3))。  
TG)。

## 一种通过丢失账号定位恶意账号的方法和系统

### 技术领域

本申请涉及互联网领域，尤其涉及一种通过丢失账号定位恶意账号的方法和系统。

### 5 背景技术

随着互联网的发展，黑客盗用正常用户账号、不法分子通过黑色产业大量购买垃圾账号到目标网站实施破坏行为的事情屡见不鲜。

由于目前自然人实名认证的成本比较高，网站上注册的相当数量的账号均没有经过实名认证。一旦这些没有经过实名认证的账户被盗，或者被  
10 购买以作为攻击网站之用，只能基于某一账号从事的攻击网站的行为将该账号查封，并不能定位到该账号背后真正盗号的黑客或攻击网站的不法分子。因此不法分子即使攻击网站的行为被追踪到，也只损失一个或数个账号，基本不存在违法成本，这样变相助长了不法分子的恶意行为。

现有技术可以采用追踪 IP 的方式追踪账户背后的黑客或不法分子的  
15 身份。然而 IP 定位不准确，无法真实反映用户的环境信息；并且越来越多的黑客或不法分子使用代理 IP，为使用 IP 定位增加了难度。

因此，需要提出一种能够对恶意账号进行定位和追踪的方案，对潜在风险进行预判和预警，从源头上打击黑客或不法分子。

### 20 发明内容

鉴于上述问题，提出了本申请实施例以便提供一种克服上述问题或者至少部分地解决上述问题的通过丢失账号定位恶意账号的方法和系统。

为解决上述问题，本申请公开一种通过丢失账号定位恶意账号的定位方法，包括：

25 读取上报的丢失账号，并查询所述上报的丢失账号登陆过的每一个客

户端对应的机器编码;

根据每一个机器编码, 查询对应的客户端上登陆过的所有用户账号;

分析每一个所述用户账号, 并确定恶意账号。

本申请实施例还公开一种通过丢失账号定位恶意账号的定位系统, 包括:

机器编码查询模块, 用于读取上报的丢失账号, 并查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码;

用户账号查询模块, 用于根据每一个机器编码, 查询对应的客户端上登陆过的所有用户账号;

10 账号分析模块, 用于分析每一个所述用户账号, 并确定恶意账号。

本申请实施例至少具有以下优点:

本申请实施例提出的通过丢失账号定位恶意账号的定位方法和定位系统中, 能够通过丢失账号查询到机器编码, 再通过机器编码查询到登陆对应于机器编码的客户端的每一个用户账号, 通过机器编码和用户账号的  
15 对应关系分析和定位恶意账号, 从源头上定位黑客或不法分子, 解决了现有技术中无法跟踪黑客或不法分子的问题。

## 附图说明

图 1 是本申请第一实施例的通过丢失账号定位恶意账号的定位方法的  
20 流程图。

图 2 是本申请第二实施例的通过丢失账号定位恶意账号的定位方法的流程图。

图 3 是对应于本申请第一实施例的定位方法的通过丢失账号定位恶意账号的定位系统的方框图。

25 图 4 是对应于本申请第二实施例的定位方法的通过丢失账号定位恶意

账号的定位系统的方框图。

## 具体实施方式

下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员所获得的所有其他实施例，都属于本申请保护的范围。

本申请的核心思想之一在于，读取丢失账号登陆过的每一台客户端的机器编码，根据每一个机器编码查找对应的每一个客户端上登陆过的所有用户账号，分析每一个用户账号，进而从所有的用户账号里确定恶意账号。

### 第一实施例

本申请第一实施例提出一种通过丢失账号定位恶意账号的定位方法，值得说明的是，本申请所述的恶意账号包括黑客账号，以及不法分子用来攻击网站的垃圾账号等，是相对用户正常使用的账号而言，并不特别限定为某一类账号。

如图1所示为本申请第一实施例的通过丢失账号定位恶意账号的定位方法的流程图。本申请第一实施例提出的通过丢失账号定位恶意账号的定位方法包括如下步骤：

S101，读取上报的丢失账号，并查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码；

在这一步骤中，若某一用户发觉账号丢失，例如输入用户名或密码后账户无法开启，或者发觉账户有被其他人使用的痕迹，该用户可以从网页的申诉通道上报丢失的账号。服务器读取用户上报的丢失账号，并从例如数据库中查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码。

举例来说，服务器从数据库中查询到用户上报的丢失账号分别关联五个机器编码，则可以判断该丢失账号分别在 5 个客户端上登陆过。机器编码是每一个客户端区别于其他客户端的唯一编码，例如可以为客户端的 Mac 地址。

5 S102，根据每一个机器编码，查询对应的客户端上登陆过的所有用户账号；

在这一步骤中，服务器根据步骤 S101 中查询到的每一个机器编码查询每一个机器编码对应的客户端上登陆过的所有用户账号。例如在步骤 S101 中查询到 5 个关联的机器编码，再根据每一个关联的机器编码查询每  
10 一个客户端上登陆过的用户账号。举例来说，5 个关联的机器编码对应的客户端上分别有 1 个、2 个、3 个、4 个、5 个用户账号登陆过，即在 5 个客户端上共有 15 个用户账号登陆过。

S103，分析每一个所述用户账号，并确定恶意账号；

在这一步骤中，以上述 15 个用户账号为例，服务器可以逐一分析上  
15 述的 15 个用户账号，通过特定的规则确定哪一个或多个账号为恶意账号。

由上述可知，本申请第一实施例提出的通过丢失账号定位恶意账号的定位方法中，能够通过丢失账号查询到机器编码，再通过机器编码查询到登陆对应于机器编码的客户端的每一个用户账号，通过机器编码和用户账号的对应关系分析和定位恶意账号，从源头上定位黑客或不法分子，解决  
20 了现有技术中无法跟踪黑客或不法分子的问题。

## 第二实施例

本申请第二实施例提出一种通过丢失账号定位恶意账号的定位方法，如图 2 所示为本申请第二实施例的通过丢失账号定位恶意账号的方法的流程图。本申请第二实施例提出的通过丢失账号定位恶意账号的定位方法包  
25 括如下步骤：

S201，将用以提取客户端的机器编码的信息采集工具加载至网页端；

在这一步骤中，信息采集工具例如为脚本或插件，脚本可以为 JavaScript 脚本。服务器例如将 JavaScript 代码加载在网页端，当通过客户端的浏览器访问该网页时，该 JavaScript 代码随着网页的其他脚本一起加载在浏览器中，用以提取客户端的机器编码。当然，该信息采集工具可以  
5 不限于 JavaScript 代码或插件，任何能够实现将客户端的机器编码上传至服务器的网页代码均是可行的。

S202，当通过所述客户端登陆所述网页端时，获取所述客户端的机器编码，并将该机器编码传送至服务器；

在这一步骤中，当用户通过客户端登陆所述网页端时，步骤 S201 中的  
10 的信息采集工具可以获取该客户端的机器编码，并传送至服务器。优选地，该服务器设置有数据库，该机器编码可以被上传至数据库中。

S203，从服务器中对应所述客户端的用户访问日志中提取用户信息；

在这一步骤中，服务器中记录有每一次该客户端访问该网页端的历史记录，这一记录例如为用户访问日志，记载有每次登录时间、下线时间、  
15 用户账号、用户 IP、登陆地点等内容，服务器从用户访问日志中提取相关的用户信息，从用户访问日志中提取相关的用户信息例如可以为“清洗日志”。

S204，提取所述用户信息中的所有用户账号，并将所有用户账号分别与  
所述客户端的机器编码关联；

20 用户信息中包括该客户端登录过的一个或多个用户账号，如果有多个用户用同一个客户端登陆，则该用户访问日志中记录的用户信息中包含多个用户账号。在这一步骤中，服务器从用户信息中提取所有的用户账号，并将所有用户账号分别与该客户端的机器编码对应。即，在同一客户端上提取到的每一个用户账号均与该客户端的机器编码对应匹配，以利于后续  
25 通过该用户账号能够查询到该机器编码，或者通过机器编码能够查询到该用户账号。

用户信息中例如还可以包括用户 IP、登录地点、用户预留的联系方式

中的至少一项。在这一步骤中，将用户账号与机器编码关联，例如可以为将用户信息中包含的每一项与机器编码关联，即，可以将用户 IP、登陆地点等与机器编码关联，以利于通过机器编码能够查询到用户信息中的任一项，并且通过用户信息中的任一项能够查询到机器编码。

- 5        在这一步骤之后，服务器中可以形成一个为多对多的映射，每一个用户账号可以对应多个机器编码，每一个机器编码也可以对应多个用户账号。

S205，读取上报的丢失账号，并查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码；

- 10       在这一步骤中，通过数据库中的机器编码和用户账号的匹配，可以通过该上报的丢失账号（即用户账号）查询到对应的至少一个机器编码。这一步骤与第一实施例中的步骤 S101 相同或相似，在此不再赘述。

S206，根据每一个机器编码，查询对应的客户端上登陆过的所有用户账号；

- 15       在这一步骤中，根据服务器中记录的用户账号和机器编码的多对多的对应关系，查找所有的登陆过该客户端的所有用户账号。这一步骤与第一实施例中的步骤 S102 相同或相似，在此不再赘述。

S207，分析每一个所述用户账号，并确定恶意账号。

这一步骤与第一实施例中的步骤 S103 相同或相似，在此不再赘述。

- 20       在一优选实施例中，步骤 S207 即所述分析每一个所述用户账号，确定恶意账号的步骤包括：

当其中一个用户账号分别与多个丢失账号对应相同的机器编码，确定该用户账号为恶意账号。

- 25       在这一步骤中，假设某一个用户账号总是与其他已上报为丢失账号的账号先后登陆同一机器编码对应的客户端，则该用户账号将与这些丢失账号对应相同的机器编码。在这一情况下，如果该用户账号与丢失账号对应

同一机器编码的次数超过特定数目，例如 100 次，可以确定此用户账号为恶意账号。

或者，所述分析每一个所述用户账号，确定恶意账号的步骤还包括：

5 当其中一个用户账号的操作频度超过了阈值，则确定该用户账号为恶意账号。

由于恶意账号通常是很活跃的，假设某一用户账号有频繁的操作，例如已经超过了某一阈值，该阈值可以为一个真实用户在固定时间内的最大操作频度，例如检测到该用户账号的操作频度为每一小时内操作 100 次，这个次数超过了真实用户可能进行的最大操作频度（例如 60 次），则可以  
10 确定该用户账号为恶意账号。该真实用户的最大操作频度可以通过统计获得，在此不再赘述。

在一优选实施例中，所述分析每一个所述用户账号，并确定恶意账号之后，所述定位方法还包括：

分析每一个所述用户账号，确定未上报的其他丢失账号。

15 在这一步骤中，由于已经可以确定哪一个或哪一些账号为恶意账号，则可以同时确定哪一个或哪些账号为其他未上报的丢失账号。

例如，当其中一个用户账号与所确定出的恶意账号对应同一个机器编码，且该用户账号所对应的登录地点不是过去特定时间内的固定登录地点，确定所述用户账号为未上报的丢失账号。举例来说，某一个用户账号  
20 在 2015 年间 90%的时间内的固定登陆地点为杭州，则可以判定该用户账号的固定登陆地点为杭州，当在此步骤中检测到该用户账号与恶意账号对应同一个登陆地点，同时该用户账号最近一次登陆地点为北京，则可以判定该用户账号为丢失账号。

再例如，当其中一个用户账号与所确定出的恶意账号对应同一个机器  
25 编码，并且该用户账号在与该恶意账号对应同一个机器编码所在的时间节点之后的特定时间段内只登陆过一次，可以判定该账号为丢失账号。举例来说，某一用户账号与恶意账号同在一个客户端上登陆之后，该用户账号

被盗，通常恶意账号只会使用一次该用户账号就不会再使用了，因此这种情况下可以判断该用户账号为丢失账号。

正如本领域技术人员可知，本领域有多种判断是否为恶意账号和丢失账号的方法，以上仅为举例说明，并非对本申请的限制。

- 5        在一优选实施例中，分析每一个所述用户账号，并确定未上报的其他丢失账号之后，所述方法还包括：

注销所述恶意账号；和/或

通过用户预留的联系方式通知该丢失账号的用户。

- 10        上述两个步骤可以认为对恶意账号打、对丢失账号预警的步骤，通过上述步骤可以控制风险的蔓延。本领域还有其他多种对恶意账号进行打击、对丢失账号进行预警和通知的方法，在此并不特别说明。

- 15        由上述可知，本申请第二实施例提出的通过丢失账号定位恶意账号的定位方法中，能够通过丢失账号查询到机器编码，再通过机器编码查询到登陆对应于机器编码的客户端的每一个用户账号，通过机器编码和用户账号的对应关系分析和定位恶意账号，从源头上定位黑客或不法分子，并能够对黑客进行打击，对丢失账号的用户进行预警，解决了现有技术中无法跟踪黑客或不法分子的问题，控制了风险蔓延。

### 第三实施例

- 20        本申请实施例还提出一种通过丢失账号定位恶意账号的定位系统，如图3所示为对应于本申请第一实施例的定位恶意账号的方法的定位恶意账号的定位系统的方框图。该定位系统300包括：

机器编码查询模块301，用于读取上报的丢失账号，并查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码；

- 25        用户账号查询模块302，用于根据每一个机器编码，查询对应的客户端上登陆过的所有用户账号；

账号分析模块 303，用于分析每一个所述用户账号，确定恶意账号。

本申请第三实施例提出的通过丢失账号定位恶意账号的定位系统中，能够通过机器编码和用户账号的对应关系分析恶意账号，从源头上定位黑客或不法分子，解决了现有技术中无法跟踪黑客或不法分子的问题。

5

#### 第四实施例

本申请实施例还提出一种通过丢失账号定位恶意账号的定位系统，如图 4 所示为对应于本申请第二实施例的定位恶意账号的方法的定位恶意账号的定位系统的方框图。该定位系统包括：

10 加载模块 401，用于将用以提取客户端的机器编码的信息采集工具加载至网页端；

机器编码传送模块 402，用于当通过所述客户端登陆所述网页端时，获取所述客户端的机器编码，并将该客户端的机器编码传送至服务器；

15 用户信息提取模块 403，用于从服务器中对应所述客户端的用户访问日志中提取用户信息；

信息匹配模块 404，用于提取所述用户信息中的所有用户账号，并将所述所有用户账号分别与所述客户端的机器编码关联。

机器编码查询模块 405，用于读取上报的丢失账号，并查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码；

20 用户账号查询模块 406，用于根据每一个机器编码，查询对应的客户端上登陆过的所有用户账号；

账号分析模块 407，用于分析每一个所述用户账号，确定恶意账号。

在一实施例中，所述账号分析模块 407 包括：

25 恶意账号确定子模块，用于当其中一个用户账号分别与多个丢失账号对应相同的机器编码，确定该用户账号为恶意账号。

在一实施例中，所述用户信息还包括用户 IP、登陆地点、用户预留的联系方式中的至少一者。

所述账号分析模块还用于分析每一个所述用户账号，确定未上报的其他丢失账号。

5 在一优选实施例中，所述账号分析模块还包括：

未上报丢失账号确定子模块，用于当其中一个用户账号与所述恶意账号对应同一个机器编码，且所述用户账号所对应的登录地点不是过去特定时间内的固定登录地点，确定所述用户账号为未上报的丢失账号。

在一优选实施例中，所述系统进一步包括：

10 恶意账号打击模块，用于注销所述恶意账号，和/或

丢失账号预警模块，用于通过用户预留的联系方式通知该丢失账号的用户。

在一优选实施例中，所述机器编码为所述客户端的 Mac 地址。

15 本申请第四实施例提出的通过丢失账号定位恶意账号的定位系统中，能够通过机器编码和用户账号的对应关系分析恶意账号，从源头上定位黑客或不法分子，并能够对黑客进行打击，对丢失账号的用户进行预警，解决了现有技术中无法跟踪黑客或不法分子的问题。

20 对于装置实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

25 本领域内的技术人员应明白，本申请实施例的实施例可提供为方法、装置、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、

完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

5        在一个典型的配置中，所述计算机设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM) 和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。计算机可读介质包括永久性和非永久性、可移动和非可移动媒  
10        体可以由任何方法或技术来实现信号存储。信号可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他  
15        其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信号。按照本文中的界定，计算机可读介质不包括非持续性的电脑可读媒体(transitory media)，如调制的数据信号和载波。

20        本申请实施例是参照根据本申请实施例的方法、终端设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理终端设备的处  
25        理器以产生一个机器，使得通过计算机或其他可编程数据处理终端设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理终端设备以特定方式工作的计算机可读存储器中，使得存储在该计算机

可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理终端设备上，使得在计算机或其他可编程终端设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程终端设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本申请实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请实施例范围的所有变更和修改。

最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

以上对本申请所提供的一种通过丢失账号定位恶意账号的定位方法和系统，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

## 权 利 要 求 书

1. 一种通过丢失账号定位恶意账号的定位方法，其特征在于，包括：

读取上报的丢失账号，并查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码；

5        根据每一个所述机器编码，查询对应的所述客户端上登陆过的所有用户账号；

分析每一个所述用户账号，并确定恶意账号。

2. 如权利要求 1 所述的定位方法，其特征在于，所述分析每一个所述用户账号，并确定恶意账号的步骤包括：

10       当其中一个用户账号分别与多个丢失账号对应相同的机器编码，确定该用户账号为恶意账号；或

当其中一个用户账号的操作频度超过了阈值，确定该用户账号为恶意账号。

15       3. 如权利要求 1 所述的定位方法，其特征在于，在读取上报的丢失账号，并查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码之前，所述方法还包括：

将用以提取客户端的机器编码的信息采集工具加载至网页端；

当通过所述客户端登陆所述网页端时，获取所述客户端的机器编码，并将该客户端的机器编码传送至服务器；

20       从服务器中对应所述客户端的用户访问日志中提取用户信息；

提取所述用户信息中的所有用户账号，并将所述所有用户账号分别与所述客户端的机器编码关联。

4. 如权利要求 3 所述的定位方法，其特征在于，所述用户信息还包括用户 IP、登录地点、用户预留的联系方式中的至少一者。

25       5. 如权利要求 4 所述的定位方法，其特征在于，所述分析每一个所述

用户账号，并确定恶意账号之后，所述定位方法还包括：

分析每一个所述用户账号，确定未上报的其他丢失账号。

6. 如权利要求 5 所述的定位方法，其特征在于，所述分析每一个所述用户账号，确定未上报的其他丢失账号的步骤包括：

- 5 当其中一个用户账号与所述恶意账号对应同一个机器编码，且所述用户账号所对应的登录地点不是特定时间内的固定登录地点，确定所述用户账号为未上报的丢失账号。

7. 如权利要求 6 所述的定位方法，其特征在于，分析每一个所述用户账号，确定未上报的其他丢失账号之后，所述方法还包括：

- 10 注销所述恶意账号；和/或

通过用户预留的联系方式通知该丢失账号的用户。

8. 如权利要求 1 所述的定位方法，其特征在于，所述机器编码为所述客户端的 Mac 地址。

9. 一种通过丢失账号定位恶意账号的定位系统，其特征在于，包括：

- 15 机器编码查询模块，用于读取上报的丢失账号，并查询所述上报的丢失账号登陆过的每一个客户端对应的机器编码；

用户账号查询模块，用于根据每一个机器编码，查询对应的客户端上登陆过的所有用户账号；

账号分析模块，用于分析每一个所述用户账号，并确定恶意账号。

- 20 10. 如权利要求 9 所述的定位系统，所述账号分析模块包括恶意账号确定子模块，所述恶意账号确定子模块用于：

当其中一个用户账号分别与多个丢失账号对应相同的机器编码，确定该用户账号为恶意账号；或

- 25 当其中一个用户账号的操作频度超过了阈值，确定该用户账号为恶意账号。

11. 如权利要求 9 所述的定位系统，所述系统还包括：

加载模块，用于将用以提取客户端的机器编码的信息采集工具加载至网页端；

5 机器编码传送模块，用于当通过所述客户端登陆所述网页端时，获取所述客户端的机器编码，并将该客户端的机器编码传送至服务器；

用户信息提取模块，从服务器中对应所述客户端的用户访问日志中提取用户信息；

信息匹配模块，用于提取所述用户信息中的所有用户账号，并将所述所有用户账号分别与所述客户端的机器编码关联。

10 12. 如权利要求 11 所述的定位系统，其特征在于，所述用户信息还包括用户 IP、登陆地点、用户预留的联系方式中的至少一者。

13. 如权利要求 12 所述的定位系统，其特征在于，所述账号分析模块还用于分析每一个所述用户账号，确定未上报的其他丢失账号。

15 14. 如权利要求 13 所述的定位系统，其特征在于，所述账号分析模块还包括：

未上报丢失账号确定子模块，用于当其中一个用户账号与所述恶意账号对应同一个机器编码，且所述用户账号所对应的登录地点不是过去特定时间内的固定登录地点，确定所述用户账号为未上报的丢失账号。

15. 如权利要求 14 所述的定位系统，其特征在于，所述系统还包括：

20 恶意账号打击模块，用于注销所述恶意账号，和/或

丢失账号预警模块，用于通过用户预留的联系方式通知该丢失账号的用户。

16. 如权利要求 9 所述的定位系统，其特征在于，所述机器编码为所述客户端的 Mac 地址。

25

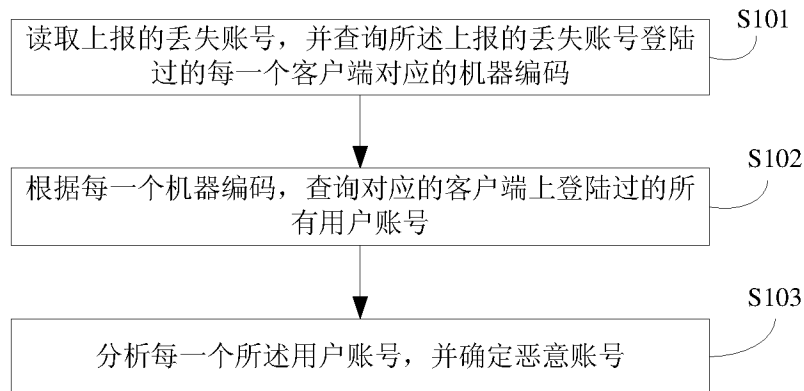


图1

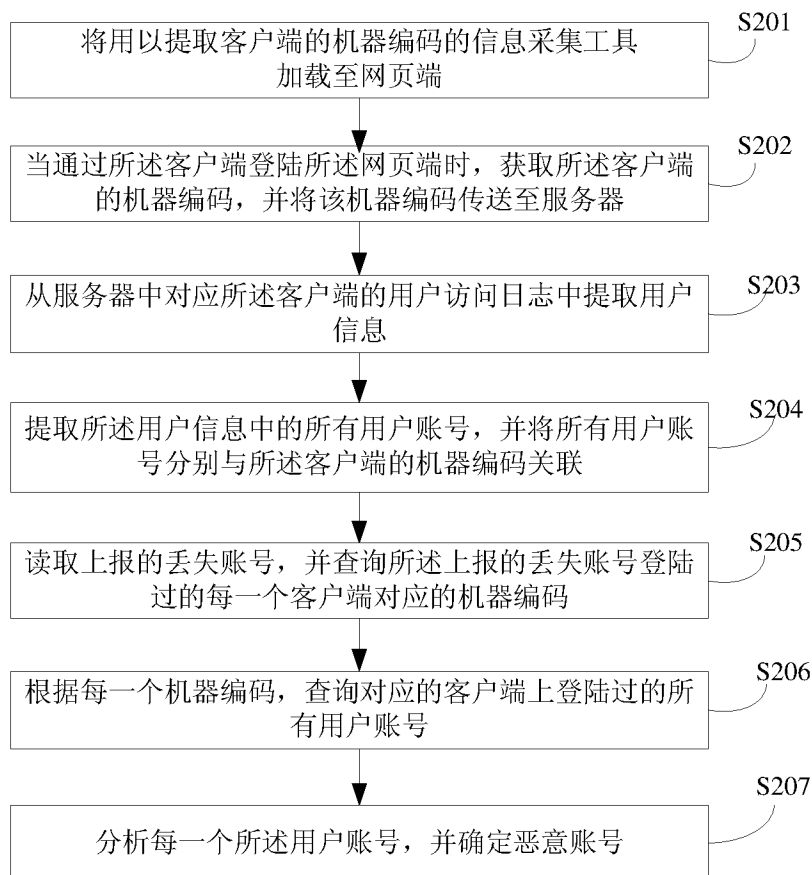


图2

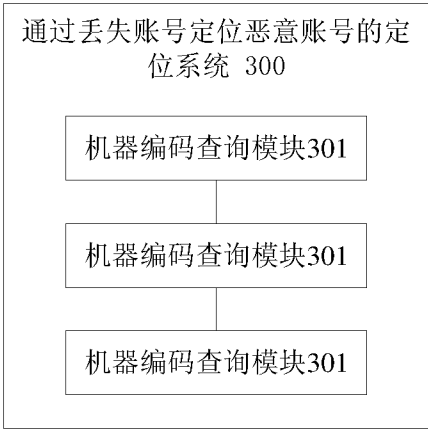


图3

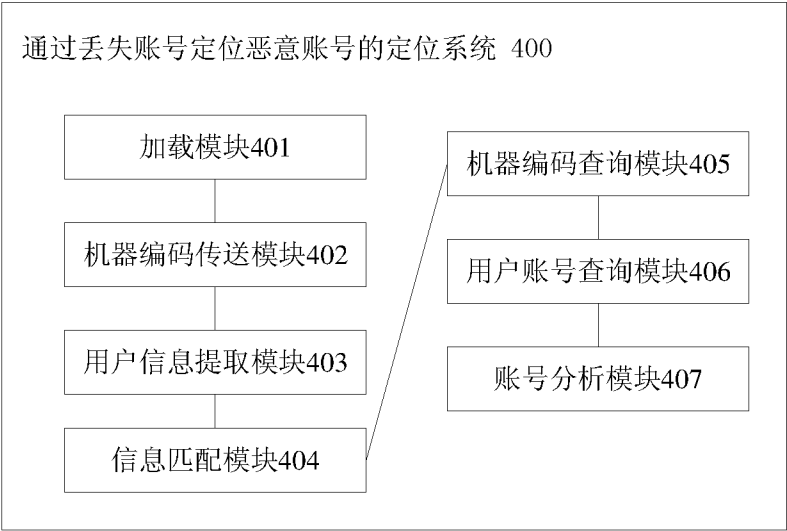


图4

# INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CN2017/070907**

## 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)

CNKI, CNPAT, WPI, EPODOC: abandon, loss reporting, reveal, hacker, account number, client, machine coding, lost, steal, rob, abnormal, stolen, malicious, account, terminal, customer, address, position, location, IP, mac

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                         | Relevant to claim No. |
|-----------|----------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y         | CN 104426885 A (TENCENT INC.), 18 March 2015 (18.03.2015), description, paragraphs [0035]-[0053]                           | 1-16                  |
| Y         | CN 104852886 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.), 19 August 2015 (19.08.2015), description, paragraphs [0029]-[0040] | 1-16                  |
| A         | CN 104917643 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.), 16 September 2015 (16.09.2015), the whole document                 | 1-16                  |
| A         | CN 105227532 A (ALIBABA GROUP HOLDING LIMITED), 06 January 2016 (06.01.2016), the whole document                           | 1-16                  |
| A         | WO 2015043491 A1 (TENCENT TECHNOLOGY SHENZHEN CO., LTD.), 02 April 2015 (02.04.2015), the whole document                   | 1-16                  |

☐ 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<br>16 March 2017 (16.03.2017)                                                                                                                            | Date of mailing of the international search report<br><b>06 April 2017 (06.04.2017)</b> |
| Name and mailing address of the ISA/CN:<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No.: (86-10) 62019451 | Authorized officer<br><b>CHEN, Wenjing</b><br>Telephone No.: (86-10) <b>61648264</b>    |

International application No.  
**PCT/CN2017/070907**

Form PCT/ISA/210 (patent family annex) (July 2009)

| <b>A. 主题的分类</b><br>H04L 29/06 (2006.01) i<br><br>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>B. 检索领域</b><br>检索的最低限度文献 (标明分类系统和分类号)<br>H04L, H04W, H04Q<br><br>包含在检索领域中的除最低限度文献以外的检索文献<br><br>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))<br>CNKI, CNPAT, WPI, EPDOC: 丢失, 被盗, 废弃, 丢弃, 异常, 挂失, 泄露, 黑客, 恶意, 账号, 账户, 客户端, 终端, 地址, 机器编码, lost, steal, rob, abnormal, stolen, malicious, account, terminal, customer, address, position, location, IP, mac                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                     |                                             |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| <b>C. 相关文件</b> <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>CN 104426885 A (深圳市腾讯计算机系统有限公司) 2015年 3月 18日 (2015 - 03 - 18)<br/>说明书第[0035]-[0053]段</td> <td>1-16</td> </tr> <tr> <td>Y</td> <td>CN 104852886 A (腾讯科技深圳有限公司) 2015年 8月 19日 (2015 - 08 - 19)<br/>说明书第[0029]-[0040]段</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>CN 104917643 A (腾讯科技深圳有限公司) 2015年 9月 16日 (2015 - 09 - 16)<br/>全文</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>CN 105227532 A (阿里巴巴集团控股有限公司) 2016年 1月 6日 (2016 - 01 - 06)<br/>全文</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>WO 2015043491 A1 (腾讯科技深圳有限公司) 2015年 4月 2日 (2015 - 04 - 02)<br/>全文</td> <td>1-16</td> </tr> </tbody> </table> |                                                                                     |                                             | 类 型* | 引用文件, 必要时, 指明相关段落 | 相关的权利要求 | Y | CN 104426885 A (深圳市腾讯计算机系统有限公司) 2015年 3月 18日 (2015 - 03 - 18)<br>说明书第[0035]-[0053]段 | 1-16 | Y | CN 104852886 A (腾讯科技深圳有限公司) 2015年 8月 19日 (2015 - 08 - 19)<br>说明书第[0029]-[0040]段 | 1-16 | A | CN 104917643 A (腾讯科技深圳有限公司) 2015年 9月 16日 (2015 - 09 - 16)<br>全文 | 1-16 | A | CN 105227532 A (阿里巴巴集团控股有限公司) 2016年 1月 6日 (2016 - 01 - 06)<br>全文 | 1-16 | A | WO 2015043491 A1 (腾讯科技深圳有限公司) 2015年 4月 2日 (2015 - 04 - 02)<br>全文 | 1-16 |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 引用文件, 必要时, 指明相关段落                                                                   | 相关的权利要求                                     |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CN 104426885 A (深圳市腾讯计算机系统有限公司) 2015年 3月 18日 (2015 - 03 - 18)<br>说明书第[0035]-[0053]段 | 1-16                                        |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CN 104852886 A (腾讯科技深圳有限公司) 2015年 8月 19日 (2015 - 08 - 19)<br>说明书第[0029]-[0040]段     | 1-16                                        |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CN 104917643 A (腾讯科技深圳有限公司) 2015年 9月 16日 (2015 - 09 - 16)<br>全文                     | 1-16                                        |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CN 105227532 A (阿里巴巴集团控股有限公司) 2016年 1月 6日 (2016 - 01 - 06)<br>全文                    | 1-16                                        |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | WO 2015043491 A1 (腾讯科技深圳有限公司) 2015年 4月 2日 (2015 - 04 - 02)<br>全文                    | 1-16                                        |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                     |                                             |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“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)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“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<br>“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<br>“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<br>“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<br>“&” 同族专利的文件                                                                                                                                                                                                                                                                                                                                                             |                                                                                     |                                             |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| 国际检索实际完成的日期<br><br>2017年 3月 16日                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                     | 国际检索报告邮寄日期<br><br>2017年 4月 6日               |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |
| ISA/CN的名称和邮寄地址<br><br>中华人民共和国国家知识产权局 (ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                     | 授权官员<br><br>陈文静<br><br>电话号码 (86-10)61648264 |      |                   |         |   |                                                                                     |      |   |                                                                                 |      |   |                                                                 |      |   |                                                                  |      |   |                                                                  |      |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2017/070907

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利 |            |    | 公布日<br>(年/月/日) |
|-------------|------------|----|----------------|------|------------|----|----------------|
| CN          | 104426885  | A  | 2015年 3月 18日   | WO   | 2015032318 | A1 | 2015年 3月 12日   |
| CN          | 104852886  | A  | 2015年 8月 19日   | 无    |            |    |                |
| CN          | 104917643  | A  | 2015年 9月 16日   | 无    |            |    |                |
| CN          | 105227532  | A  | 2016年 1月 6日    | HK   | 1215902    | A1 | 2016年 9月 23日   |
| WO          | 2015043491 | A1 | 2015年 4月 2日    | CN   | 104519032  | A  | 2015年 4月 15日   |