

(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3月2日 (02.03.2017)



(10) 国际公布号
WO 2017/032192 A1

- (51) 国际专利分类号:
H04L 12/26 (2006.01) H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/090715
- (22) 国际申请日: 2016年7月20日 (20.07.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510531804.9 2015年8月26日 (26.08.2015) CN
- (71) 申请人: 广州视睿电子科技有限公司 (GUANG-ZHOU SHIRUI ELECTRONICS CO., LTD.) [CN/CN]; 中国广东省广州市广州经济技术开发区科学城科珠路 192 号, Guangdong 510663 (CN)。
- (72) 发明人: 李彬 (LI, Bin); 中国广东省广州市广州经济技术开发区科学城科珠路 192 号, Guangdong 510663 (CN)。 林强生 (LIN, Qiangsheng); 中国广东省广州市广州经济技术开发区科学城科珠路 192 号, Guangdong 510663 (CN)。 张龙华 (ZHANG, Longhua); 中国广东省广州市广州经济技术开发区科学城科珠路 192 号, Guangdong 510663 (CN)。 向建中 (XIANG, Jianzhong); 中国广东省广州市广州经济技术开发区科学城科珠路 192 号, Guangdong

510663 (CN)。 薄景仁 (BO, Jingren); 中国广东省广州市广州经济技术开发区科学城科珠路 192 号, Guangdong 510663 (CN)。

- (74) 代理人: 广州华进联合专利商标代理有限公司 (ADVANCE CHINA IP LAW OFFICE); 中国广东省广州市天河区花城大道 85 号 3901 房, Guangdong 510623 (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, 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,

[见续页]

(54) Title: ENCRYPTION STATE DETECTION METHOD AND SYSTEM

(54) 发明名称: 加密状态检测方法和系统

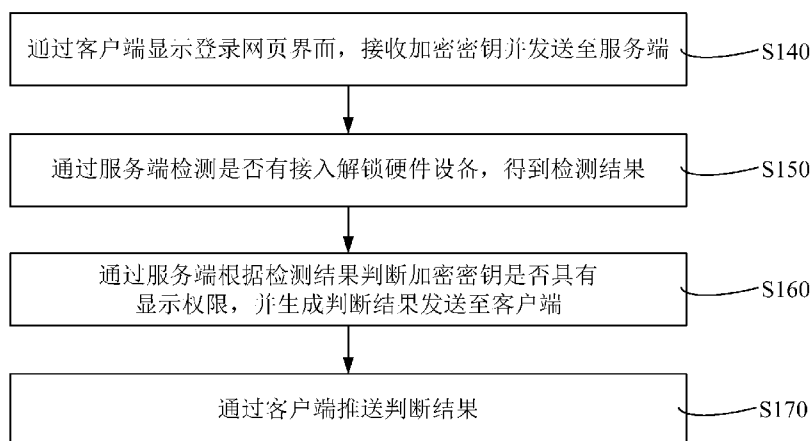


图 1

- S140 DISPLAYING A LOGIN WEBPAGE INTERFACE VIA A CLIENT, AND RECEIVING AN ENCRYPTION KEY AND SENDING SAME TO A SERVER
- S150 DETECTING WHETHER THERE IS AN ACCESSED HARDWARE UNLOCK DEVICE VIA THE SERVER TO OBTAIN A DETECTION RESULT
- S160 JUDGING WHETHER THE ENCRYPTION KEY HAS A DISPLAY RIGHT VIA THE SERVER ACCORDING TO THE DETECTION RESULT, AND GENERATING A JUDGEMENT RESULT AND SENDING SAME TO THE CLIENT
- S170 PUSHING THE JUDGEMENT RESULT VIA THE CLIENT

(57) Abstract: The present invention relates to an encryption state detection method and system. The method comprises: displaying a login webpage interface via a client, and receiving an encryption key and sending same to a server; detecting whether there is an accessed hardware unlock device via the server to obtain a detection result; judging whether the encryption key has a display right via the server according to the detection result, and generating a judgement result and sending same to the client; and pushing the judgement result via the client. Whether an encryption key has a display right is judged by combining software with hardware, and a judgement result is pushed to inform a user whether restricted access exists to restrict a login person, thereby avoiding leakage of access contents and improving encryption security.

(57) 摘要: 本发明涉及一种加密状态检测方法和系统, 通过客户端显示登录网页界面, 接收加密密钥并发送至服务端; 通过服务端检测是否有接入解锁硬件设备, 得到检测结果。通过服

务端根据检测结果判断加密密钥是否具有显示权限, 并生成判断结果发送至客户端; 通过客户端推送判断结果。通过软件结合硬件判断加密密钥是否具有显示权限, 并推送判断结果以告知用户是否有限制访问, 对登陆人员进行限制, 避免访问内容泄露, 提高了加密安全性。



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))。

加密状态检测方法和系统

技术领域

本发明涉及网络信息安全技术领域，特别是涉及一种加密状态检测方法
5 和系统。

背景技术

目前随着互联网技术应用的越来越广泛，人们很多的日常工作和娱乐都
在网络上进行。人们通过网页浏览器浏览网页，获取有用的信息和数据，进
10 行在线联系和交流。

传统的网页加密只限于单一的软件加密方式，加密方式也主要是保护密
码之类的信息，WEB 后台中的内容容易被爬虫、恶意软件、搜索引擎等攻击
和抓取，导致信息不安全。

15 发明内容

基于此，有必要针对上述问题，提供一种提高加密安全性的加密状态检
测方法和系统。

一种加密状态检测方法，包括以下步骤：

通过客户端显示登录网页界面，接收加密密钥并发送至服务端；

20 通过所述服务端检测是否有接入解锁硬件设备，得到检测结果；

通过所述服务端根据所述检测结果判断所述加密密钥是否具有显示权
限，并生成判断结果发送至所述客户端；

通过所述客户端推送所述判断结果。

一种加密状态检测系统，包括：

25 登录模块，用于通过客户端显示登录网页界面，接收加密密钥并发送至
服务端；

检测模块，用于通过所述服务端检测是否有接入解锁硬件设备，得到检
测结果；

判断模块，用于通过所述服务端根据所述检测结果判断所述加密密钥是否具有显示权限，并生成判断结果发送至所述客户端；

推送模块，用于通过所述客户端推送所述判断结果。

上述加密状态检测方法和系统，通过客户端显示登录网页界面，接收加密密钥并发送至服务端；通过服务端检测是否有接入解锁硬件设备，得到检测结果。通过服务端根据检测结果判断加密密钥是否具有显示权限，并生成判断结果发送至客户端；通过客户端推送判断结果。通过软件结合硬件判断加密密钥是否具有显示权限，并推送判断结果以告知用户是否有限制访问，对登陆人员进行限制，避免访问内容泄露，提高了加密安全性。

10

附图说明

图 1 为一实施例中加密状态检测方法的流程图；

图 2 为另一实施例中加密状态检测方法的流程图；

图 3 为一实施例中加密状态检测系统的结构图；

15 图 4 为另一实施例中加密状态检测系统的结构图。

具体实施方式

一种加密状态检测方法，可应用于网页内容访问，或其他应用程序的内容访问等场景。如图 1 所示，加密状态检测方法包括以下步骤：

20 步骤 S140：通过客户端显示登录网页界面，接收加密密钥并发送至服务端。

客户端具体可以是台式电脑或笔记本电脑等终端设备，服务端具体可以是后台服务器等设备。通过客户端显示登录网页界面，用户可在登录网页界面的对话框中输入加密密钥，客户端接收加密密钥后发送至服务端。进一步地，当用户输入加密密钥的时候，还可通过客户端向广域网服务端查询对应的限制信息，同时自动把限制信息发送到后台的服务端中。

25

步骤 S150：通过服务端检测是否有接入解锁硬件设备，得到检测结果。

用户登陆到某个后台服务器的网页中，同时可使用相应的解锁硬件设备。

可以得知，检测结果包括两种：服务端接入有解锁硬件设备，或服务端未接入解锁硬件设备。如果服务端有相应的解锁硬件设备，则说明限制信息可以解开；否则不能解开，用户只能进行有限的操作。

- 步骤 S160：通过服务端根据检测结果判断加密密钥是否具有显示权限，
5 并生成判断结果发送至客户端。

根据解锁硬件设备的检测结果，软件结合硬件判断加密密钥的权限得到判断结果。在其中一个实施例中，步骤 S160 中通过服务端根据检测结果判断加密密钥是否具有显示权限，具体包括步骤 162 至步骤 168。

- 步骤 162：若服务端有接入解锁硬件设备，则获取解锁硬件设备预存的解
10 锁数据。如果检测到解锁硬件设备，则提取其中存储的解锁数据。

- 步骤 164：根据解锁数据判断加密密钥是否具有显示权限，得到判断结果。解锁数据具体可以包括用户数量和管理终端数量等，用户数量用于限制用户登入的数量，管理终端数量用于限制登录同一用户的客户端的数量。客户端在发送加密密钥时也可同时将查询得到的限制信息一并发送至服务端，服务端将解锁数据与限制信息进行比较，并以解锁数据为准确定加密密钥的权限。
15 比如解锁硬件设备中的用户登陆数量为 1 的话，则只可以让一个用户登陆。服务端后台记录同一个帐户有多少个登陆数，如果同一用户再次登陆的话则把它踢下线，即不具备显示权限。管理终端数量也是类似，不仅如此，解锁硬件设备还可以存储其它数据来做更多的限制。

- 进一步地，步骤 164 可包括以下步骤：检测加密密钥的登录次数是否大于解锁数据限定的权限次数。若是，则加密密钥不具备显示权限；若否，则加密密钥具备显示权限，得到判断结果。通过比较加密密钥的登录次数和解锁数据限定的权限次数，确定此次登入加密密钥是否具备显示权限，得到判断结果。
20

- 步骤 166：若服务端未接入解锁硬件设备，则获取加密密钥对应的限制信息。如果服务器没有接入解锁硬件设备，获取加密密钥初始对应的限制信息。
25

步骤 168：根据限制信息判断加密密钥是否具有显示权限，得到判断结果。类似的，限制信息同样可以包括用户数量和管理终端数量等。步骤 168 同样

可包括以下步骤：检测加密密钥的登录次数是否大于限制信息限定的权限次数；若是，则加密密钥不具备显示权限；若否，则加密密钥具备显示权限，得到判断结果。通过比较加密密钥的登录次数和限制信息限定的权限次数，确定此次登入加密密钥是否具备显示权限，得到判断结果。

5 进一步地，步骤 168 之后，步骤 S160 还包括将判断结果发送至客户端的步骤。将得到的判断结果发送至客户端以便进行推送。

本实施例中根据服务端是否接入解锁硬件设备的实际情况，分别利用解锁数据和限制信息来判断加密密钥是否有显示权限。由于在广域网中存储有客户端唯一的硬件标识信息与加密密钥进行匹配。用户在登陆中，服务端后台通过查询广域网服务器中的信息，可知道加密密钥已登入的用户数量和管理终端数量等信息，可实现对登陆人员的访问限制。

步骤 S170：通过客户端推送判断结果。利用客户端推送判断结果，告知用户是否有限制显示访问。以网页内容访问为例，推送判断结果具体可以通过客户页面显示相关信息，如显示“具备页面显示权限”或“不具备页面显示权限”等信息；也可以是通过语音播报或其他方式告知用户判断结果。

上述加密状态检测方法，通过软件结合硬件判断加密密钥是否具有显示权限，并推送判断结果以告知用户是否有限制访问，对登陆人员进行限制，避免访问内容泄露，提高了加密安全性。

20 在其中一个实施例中，步骤 S150 之后，加密状态检测方法还包括以下步骤：

通过服务端根据预设的密钥列表对加密密钥进行认证，得到认证结果。步骤 S160 中通过服务端根据检测结果判断加密密钥是否具有显示权限具体为，通过服务端根据检测结果和认证结果判断加密密钥是否具有显示权限。在服务端接收加密密钥后，可启动解密应用程序并传入加密密钥，通过解密应用程序来检测解锁硬件设备是否插入，以及检测加密密钥是否有效。

进一步地，通过服务端根据预设的密钥列表对加密密钥进行认证，得到认证结果的步骤，具体包括：判断加密密钥是否存储于密钥列表中；若是，则加密密钥为正确密钥；若否，则加密密钥为错误密钥，得到认证结果。在

得到检测结果后，还对加密密钥进行认证，确认加密密钥的有效性。例如服务端可将注册成功的加密密钥存入密钥列表，接收到客户端发送的加密密钥后，判断是否存储在密钥列表中，若是，则说明加密密钥有效，若否，则说明加密密钥无效。

5 通过服务端根据检测结果和认证结果判断加密密钥是否具有显示权限，具体可以是先将加密密钥与解锁数据或限制信息进行比较，详见步骤 162 至步骤 168。例如若加密密钥的登录次数不大于解锁数据或限制信息限定的权限次数，可认为加密密钥具备初步权限，此时若检测到加密密钥有效，则最终确认加密密钥具备显示权限。

10 本实施例中在得到检测结果后，还对加密密钥进行认证，确认加密密钥的有效性。结合检测结果和认证结果来确认加密密钥的权限，即是以上两种条件均满足时确认加密密钥具备权限，只要有一种条件不满足则认为加密密钥不具备权限，可进一步提高加密安全性。

15 在其中一个实施例中，如图 2 所示，步骤 S140 之前，加密状态检测方法还包括步骤 S110 至步骤 S130。

 步骤 S110：通过客户端显示注册页面，接收用户名信息。具体可以在用户第一次开启客户端时，通过 service 进程自动调出注册界面，将用户输入的注册名作为用户名信息。

20 步骤 S120：通过客户端读取硬件标识信息，并将用户名信息和硬件标识信息发送至服务端。同样通过 service 进程读取客户端的硬件标识信息，并将用户名信息和硬件标识信息发送至服务端，此外也可将客户端的硬件标识信息发送至广域网服务器存储，以便后续再次调用。

25 步骤 S130：通过服务端对用户名信息和硬件标识信息进行匹配，并将用户名信息作为加密密钥进行存储。服务端对用户名信息和硬件标识信息进行匹配，如果匹配成功，则用户注册成功并能用于其它地方登陆，把用户名作为加密密钥进行存储。

 步骤 S110 至步骤 S130 即是提供了用户注册功能，便于登录人员的管理。各注册用户对应设置有限制，比如最多可以同时打开多少软件，最多可以几

人同时使用等，通过在服务端接入解锁硬件设备可以解锁这些限制。

在其中一个实施例中，步骤 S170 之后，加密状态检测方法还包括以下步骤：

5 若判断结果为加密密钥具有显示权限，通过客户端在接收显示指令后显示访问内容。

如果用户登入的加密密钥具有显示权限，在客户端推送判断结果后，用户可通过客户端输入显示指令，控制客户端显示访问内容以使用户查看，提高操作便利性。

10 本发明还提供了一种加密状态检测系统，可应用于网页内容访问，或其他应用程序的内容访问等场景。如图 3 所示，加密状态检测系统包括登录模块 140、检测模块 150、判断模块 160 和推送模块 170。

登录模块 140 用于通过客户端显示登录网页界面，接收加密密钥并发送至服务端。

15 客户端具体可以是台式电脑或笔记本电脑等终端设备，服务端具体可以是后台服务器等设备。通过客户端显示登录网页界面，用户可在登录网页界面的对话框中输入加密密钥，客户端接收加密密钥后发送至服务端。进一步地，当用户输入加密密钥的时候，还可通过客户端向广域网服务端查询对应的限制信息，同时自动把限制信息发送到后台的服务端中。

20 检测模块 150 用于通过服务端检测是否有接入解锁硬件设备，得到检测结果。

用户登陆到某个后台服务器的网页中，同时可使用相应的解锁硬件设备。可以得知，检测结果包括两种：服务端接入有解锁硬件设备，或服务端未接入解锁硬件设备。如果服务端有相应的解锁硬件设备，则说明限制信息可以
25 解开；否则不能解开，用户只能进行有限的操作。

判断模块 160 用于通过服务端根据检测结果判断加密密钥是否具有显示权限，并生成判断结果发送至客户端。

根据解锁硬件设备的检测结果，软件结合硬件判断加密密钥的权限得到

判断结果。在其中一个实施例中，判断模块 160 包括第一处理单元、第一判断单元、第二处理单元、第二判断单元和发送单元。

第一处理单元用于在服务端有接入解锁硬件设备时，获取解锁硬件设备预存的解锁数据。如果检测到解锁硬件设备，则提取其中存储的解锁数据。

5 第一判断单元用于根据解锁数据判断加密密钥是否具有显示权限，得到判断结果。解锁数据具体可以包括用户数量和管理终端数量等，用户数量用于限制用户登入的数量，管理终端数量用于限制登录同一用户的客户端的数量。客户端在发送加密密钥时也可同时将查询得到的限制信息一并发送至服务端，服务端将解锁数据与限制信息进行比较，并以解锁数据为准确定加密
10 密钥的权限。比如解锁硬件设备中的用户登陆数量为 1 的话，则只可以让一个用户登陆。服务端后台会记录同一个帐户有多少个登陆数，如果同一用户再次登陆的话则把它踢下线，即不具备显示权限。管理终端数量也是类似，不仅如此，解锁硬件设备还可以存储其它数据来做更多的限制。

进一步地，第一判断单元根据解锁数据判断加密密钥是否具有显示权限，
15 得到判断结果具体包括：检测加密密钥的登录次数是否大于解锁数据限定的权限次数。若是，则加密密钥不具备显示权限；若否，则加密密钥具备显示权限，得到判断结果。通过比较加密密钥的登录次数和解锁数据限定的权限次数，确定此次登入加密密钥是否具备显示权限，得到判断结果。

第二处理单元用于在服务端未接入解锁硬件设备时，获取加密密钥对应的限制信息。如果服务器没有接入解锁硬件设备，获取加密密钥初始对应的限制信息。
20 限制信息。

第二判断单元用于根据限制信息判断加密密钥是否具有显示权限，得到判断结果。类似的，限制信息同样可以包括用户数量和管理终端数量等。第二判断单元根据限制信息判断加密密钥是否具有显示权限，得到判断结果具体可包括：检测加密密钥的登录次数是否大于限制信息限定的权限次数；若是，则加密密钥不具备显示权限；若否，则加密密钥具备显示权限，得到判断结果。通过比较加密密钥的登录次数和限制信息限定的权限次数，确定此次登入加密密钥是否具备显示权限，得到判断结果。
25 限制信息。

发送单元用于将判断结果发送至客户端。

本实施例中根据服务端是否接入解锁硬件设备的实际情况，分别利用解锁数据和限制信息来判断加密密钥是否有显示权限。由于在广域网中存储有客户端唯一的硬件标识信息与加密密钥进行匹配。用户在登陆中，服务端后台通过查询广域网服务器中的信息，可知道加密密钥已登入的用户数量和管理终端数量等信息，可实现对登陆人员的访问限制。

推送模块 170 用于通过客户端推送判断结果。利用客户端推送判断结果，告知用户是否有限制访问。以网页内容访问为例，推送判断结果具体可以通过客户页面显示相关信息，如显示“具备页面显示权限”或“不具备页面显示权限”等信息；也可以是通过语音播报或其他方式告知用户判断结果。

上述加密状态检测系统，通过软件结合硬件判断加密密钥是否具有显示权限，并推送判断结果以告知用户是否有限制访问，对登陆人员进行限制，避免访问内容泄露，提高了加密安全性。

在其中一个实施例中，加密状态检测系统还包括密钥认证模块，密钥认证模块用于在检测模块 150 通过服务端检测是否有接入解锁硬件设备，得到检测结果后，通过服务端根据预设的密钥列表对加密密钥进行认证，得到认证结果。判断模块 160 通过服务端根据检测结果判断加密密钥是否具有显示权限具体为，通过服务端根据检测结果和认证结果判断加密密钥是否具有显示权限。在服务端接收加密密钥后，可启动解密应用程序并传入加密密钥，通过解密应用程序来检测解锁硬件设备是否插入，以及检测加密密钥是否有效。

进一步地，密钥认证模块通过服务端根据预设的密钥列表对加密密钥进行认证，得到认证结果具体包括：判断加密密钥是否存储于密钥列表中；若是，则加密密钥为正确密钥；若否，则加密密钥为错误密钥，得到认证结果。在得到检测结果后，还对加密密钥进行认证，确认加密密钥的有效性。例如服务端可将注册成功的加密密钥存入密钥列表，接收到客户端发送的加密密钥后，判断是否存储在密钥列表中，若是，则说明加密密钥有效，若否，则说明加密密钥无效。

通过服务端根据检测结果和认证结果判断加密密钥是否具有显示权限，具体可以是先将加密密钥与解锁数据或限制信息进行比较。例如若加密密钥的登录次数不大于解锁数据或限制信息限定的权限次数，可认为加密密钥具备初步权限，此时若检测到加密密钥有效，则最终确认加密密钥具备显示权限。

本实施例中在得到检测结果后，还对加密密钥进行认证，确认加密密钥的有效性。结合检测结果和认证结果来确认加密密钥的权限，即是以上两种条件均满足时确认加密密钥具备权限，只要有一种条件不满足则认为加密密钥不具备权限，可进一步提高加密安全性。

在其中一个实施例中，如图 4 所示，加密状态检测系统还包括注册页面显示模块 110、标识信息读取模块 120 和信息匹配存储模块 130。

注册页面显示模块 110 用于在登录模块 140 通过客户端显示登录网页界面，接收加密密钥并发送至服务端之前，通过客户端显示注册页面，接收用户名信息。具体可以在用户第一次开启客户端时，通过 service 进程自动调出注册界面，将用户输入自己的注册名作为用户名信息。

标识信息读取模块 120 用于通过客户端读取硬件标识信息，并将用户名信息和硬件标识信息发送至服务端。同样通过 service 进程读取客户端的硬件标识信息，并将用户名信息和硬件标识信息发送至服务端，此外也可将客户端的硬件标识信息发送至广域网服务器存储，以便后续再次调用。

信息匹配存储模块 130 用于通过服务端对用户名信息和硬件标识信息进行匹配，并将用户名信息作为加密密钥进行存储。服务端对用户名信息和硬件标识信息进行匹配，如果匹配成功，则用户注册成功并能用于其它地方登陆，把用户名作为加密密钥进行存储。

本实施例中即是提供了用户注册功能，便于登录人员的管理。各注册用户对应设置有限制，比如最多可以同时打开多少软件，最多可以几人同时使用等，通过在服务端接入解锁硬件设备可以解锁这些限制。

在其中一个实施例中，加密状态检测系统还包括页面显示模块，页面显示模块用于在推送模块 170 通过客户端推送判断结果后，若判断结果为加密

密钥具有显示权限，通过客户端在接收显示指令后显示访问内容。

如果用户登入的加密密钥具有显示权限，在客户端推送判断结果后，用户可通过客户端输入显示指令，控制客户端显示访问内容以使用户查看，提高操作便利性。

5

以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

10 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明的保护范围应以所附权利要求为准。

权利要求书

1、一种加密状态检测方法，其特征在于，包括以下步骤：

通过客户端显示登录网页界面，接收加密密钥并发送至服务端；

通过所述服务端检测是否有接入解锁硬件设备，得到检测结果；

5 通过所述服务端根据所述检测结果判断所述加密密钥是否具有显示权限，并生成判断结果发送至所述客户端；

通过所述客户端推送所述判断结果。

2、根据权利要求1所述的加密状态检测方法，其特征在于，通过所述服务端根据所述检测结果判断所述加密密钥是否具有显示权限，包括以下步骤：

10 若所述服务端有接入解锁硬件设备，则获取所述解锁硬件设备预存的解锁数据；

根据所述解锁数据判断所述加密密钥是否具有显示权限，得到所述判断结果；

15 若所述服务端未接入解锁硬件设备，则获取所述加密密钥对应的限制信息；

根据所述限制信息判断所述加密密钥是否具有显示权限，得到所述判断结果。

3、根据权利要求2所述的加密状态检测方法，其特征在于，根据所述解锁数据判断所述加密密钥是否具有显示权限，得到所述判断结果的步骤，包括以下步骤：

检测所述加密密钥的登录次数是否大于所述解锁数据限定的权限次数；

若是，则所述加密密钥不具备显示权限；

若否，则所述加密密钥具备显示权限，得到所述判断结果。

4、根据权利要求1所述的加密状态检测方法，其特征在于，通过所述服务端检测是否有接入解锁硬件设备，得到检测结果之后，还包括以下步骤：

25 通过所述服务端根据预设的密钥列表对所述加密密钥进行认证，得到认证结果；

所述通过所述服务端根据所述检测结果判断所述加密密钥是否具有显示

权限为，通过所述服务端根据所述检测结果和认证结果判断所述加密密钥是否具有显示权限。

5、根据权利要求4所述的加密状态检测方法，其特征在于，所述服务端根据预设的密钥列表判断对所述加密密钥进行认证，得到认证结果的步骤，

5 包括以下步骤：

判断所述加密密钥是否存储于所述密钥列表中；

若是，则所述加密密钥为正确密钥；

若否，则所述加密密钥为错误密钥，得到所述认证结果。

6、根据权利要求1所述的加密状态检测方法，其特征在于，通过客户端
10 显示登录网页界面，接收加密密钥并发送至服务端的步骤之前，还包括以下步骤：

通过所述客户端显示注册页面，接收用户名信息；

通过所述客户端读取硬件标识信息，并将所述用户名信息和硬件标识信息发送至所述服务端；

15 通过所述服务端对所述用户名信息和硬件标识信息进行匹配，并将所述用户名信息作为加密密钥进行存储。

7、根据权利要求1所述的加密状态检测方法，其特征在于，所述通过所述客户端推送所述判断结果的步骤之后，还包括以下步骤：

20 若所述判断结果为加密密钥具有显示权限，通过所述客户端在接收显示指令后显示访问内容。

8、一种加密状态检测系统，其特征在于，包括：

登录模块，用于通过客户端显示登录网页界面，接收加密密钥并发送至服务端；

25 检测模块，用于通过所述服务端检测是否有接入解锁硬件设备，得到检测结果；

判断模块，用于通过所述服务端根据所述检测结果判断所述加密密钥是否具有显示权限，并生成判断结果发送至所述客户端；

推送模块，用于通过所述客户端推送所述判断结果。

9、根据权利要求 8 所述的加密状态检测系统，其特征在于，还包括：

注册页面显示模块，用于在登录模块通过客户端显示登录网页界面，接收加密密钥并发送至服务端之前，通过所述客户端显示注册页面，接收用户名信息；

5 标识信息读取模块，用于通过所述客户端读取硬件标识信息，并将所述用户名信息和硬件标识信息发送至所述服务端；

信息匹配存储模块，用于通过所述服务端对所述用户名信息和硬件标识信息进行匹配，并将所述用户名信息作为加密密钥进行存储。

10 10、根据权利要求 8 所述的加密状态检测系统，其特征在于，还包括页面显示模块，所述页面显示模块用于在推送模块通过所述客户端推送所述判断结果后，若所述判断结果为加密密钥具有显示权限，通过所述客户端在接收显示指令后显示访问内容。

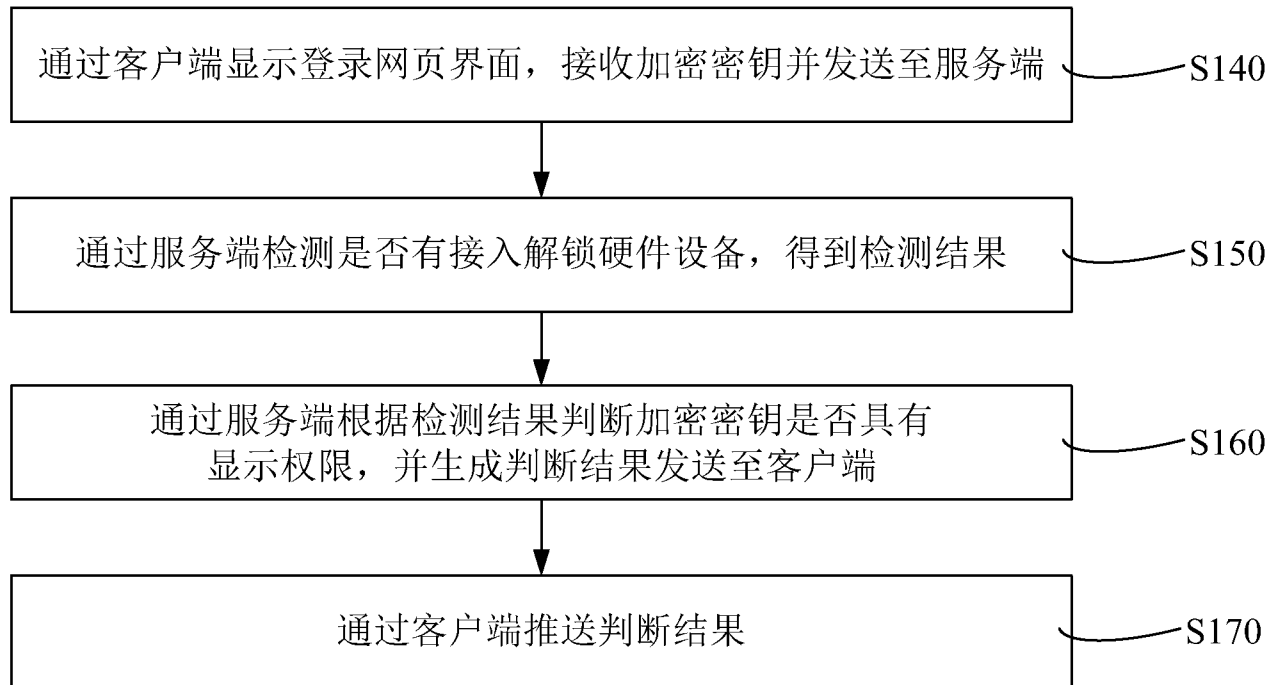


图 1

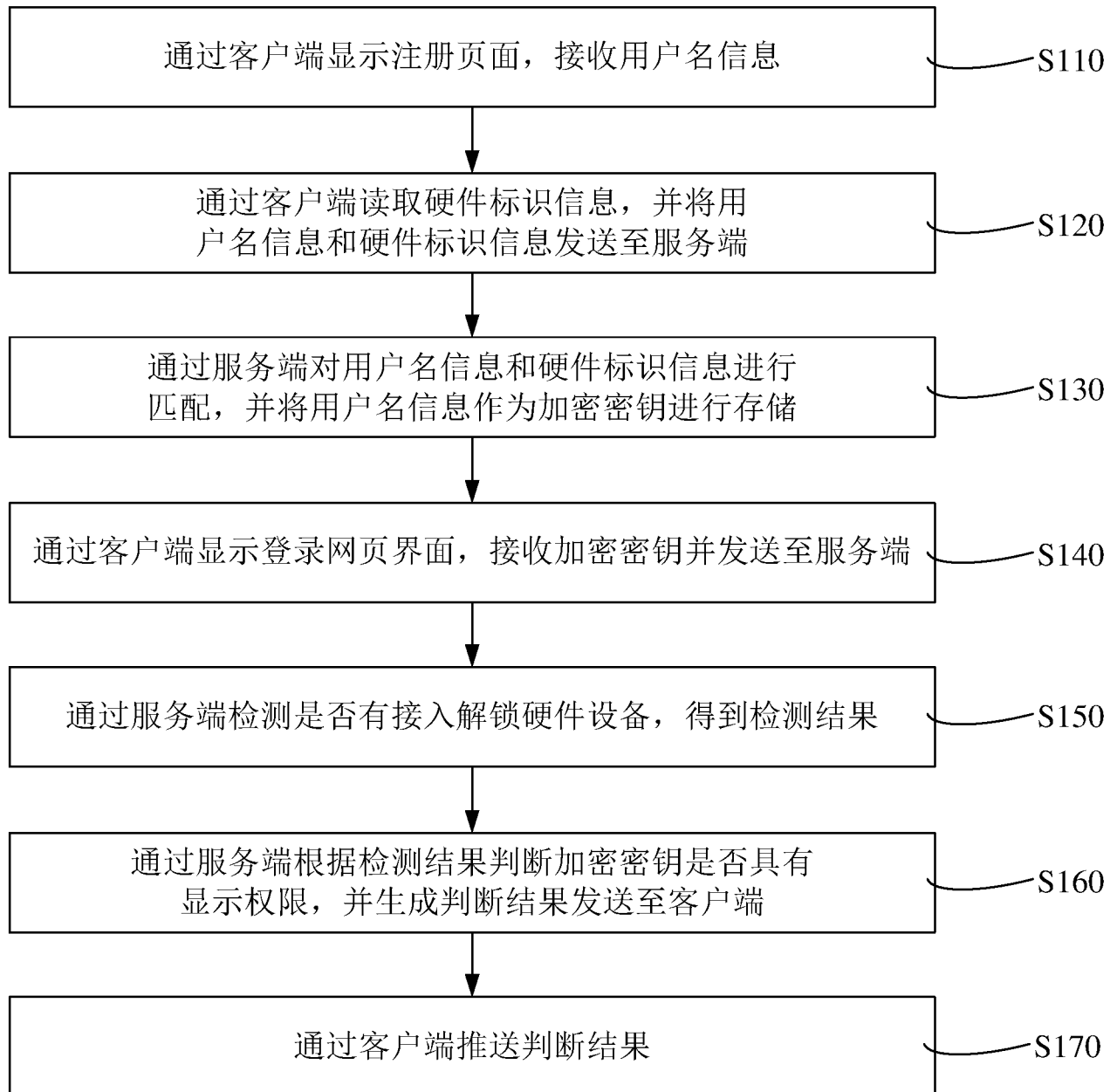


图 2

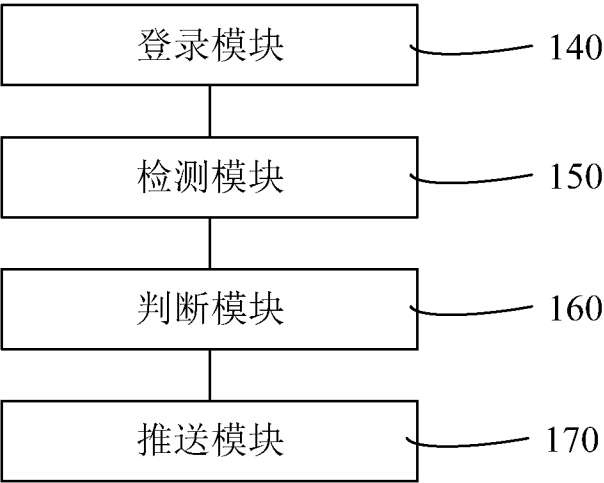


图 3

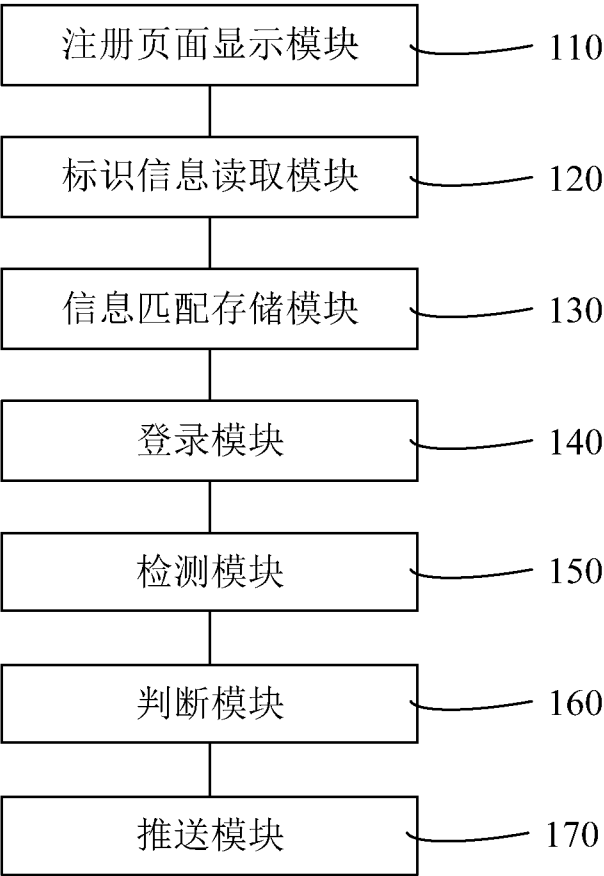


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/090715

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/26 (2006.01) i; 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; G06F; H04W

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: encrypt, authentication, client, server, hardware

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103825738 A (BEIJING HUAHONG INTEGRATED CIRCUIT DESIGN CO., LTD.) 28 May 2014 (28.05.2014) description, paragraphs [0090]-[0102]	1-10
PX	CN 105071993 A (GUANGZHOU SHIRUI ELECTRICAL TECHNOLOGY CO., LTD.) 18 November 2015 (18.11.2015) claims 1-10, description, paragraphs [0020]-[0075]	1-10
A	EP 2445242 A1 (HUAWEI DEVICE CO., LTD.) 25 April 2012 (25.04.2012) the whole document	1-10
A	CN 104378334 A (PEKING UNIVERSITY et al.) 25 February 2015 (25.02.2015) the whole document	1-10

☐ 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 21 September 2016	Date of mailing of the international search report 18 October 2016
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 HUANG, Fei Telephone No. (86-10) 61648275

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/090715

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103825738 A	28 May 2014	None	
CN 105071993 A	18 November 2015	None	
EP 2445242 A1	25 April 2012	WO 2011017924 A1	17 February 2011
		CN 101621801 A	06 January 2010
		US 2012144189 A1	07 June 2012
CN 104378334 A	25 February 2015	None	

国际检索报告

国际申请号

PCT/CN2016/090715

A. 主题的分类

H04L 12/26(2006.01)i; 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)

H04L; G06F; H04W

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, CNPAT, WPI, EPDOC: 加密, 认证, 客户端, 服务端, 服务器, 硬件, encrypt, authentication, client, server, hardware

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 103825738 A (北京华虹集成电路设计有限责任公司) 2014年 5月 28日 (2014 - 05 - 28) 说明书第[0090]-[0102]段	1-10
PX	CN 105071993 A (广州视睿电子科技有限公司) 2015年 11月 18日 (2015 - 11 - 18) 权利要求1-10, 说明书第[0020]-[0075]段	1-10
A	EP 2445242 A1 (HUAWEI DEVICE CO., LTD.) 2012年 4月 25日 (2012 - 04 - 25) 全文	1-10
A	CN 104378334 A (北京大学等) 2015年 2月 25日 (2015 - 02 - 25) 全文	1-10

☐ 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

2016年 9月 21日

国际检索报告邮寄日期

2016年 10月 18日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

黄菲

传真号 (86-10)62019451

电话号码 (86-10)61648275

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/090715

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	103825738	A	2014年 5月 28日	无			
CN	105071993	A	2015年 11月 18日	无			
EP	2445242	A1	2012年 4月 25日	WO	2011017924	A1	2011年 2月 17日
				CN	101621801	A	2010年 1月 6日
				US	2012144189	A1	2012年 6月 7日
CN	104378334	A	2015年 2月 25日	无			