(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
2015 年 8 月 20 日 (20.08.2015)

WIPO | PCT

(10) 国际公布号
WO 2015/120769 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2015/071726

(22) 国际申请日: 2015 年 1 月 28 日 (28.01.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201410048642.9 2014 年 2 月 12 日 (12.02.2014) CN

(71) 申请人: **中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.)** [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: **柴洪峰 (CHAI, Hongfeng)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **鲁志军 (LU, Zhijun)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **李卷孺 (LI, Juanru)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **束骏亮 (SHU, Junliang)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **华锦芝 (HUA, Jinzhi)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **徐泽伟 (XU, Zewei)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。 **刘发章 (LIU, Fazhang)**; 中国上海市浦东新区含笑路 36 号银联大厦 7 楼, Shanghai 200135 (CN)。

(74) 代理人: **中国专利代理（香港）有限公司 (CHINA PATENT AGENT (HK)LTD.)**; 中国香港特别行政区香港湾仔港湾道 23 号鹰君中心 22 字楼, Hong Kong (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,

[见续页]

(54) **Title**: PASSWORD MANAGEMENT METHOD AND SYSTEM

(54) **发明名称** : 密码管理方法及系统

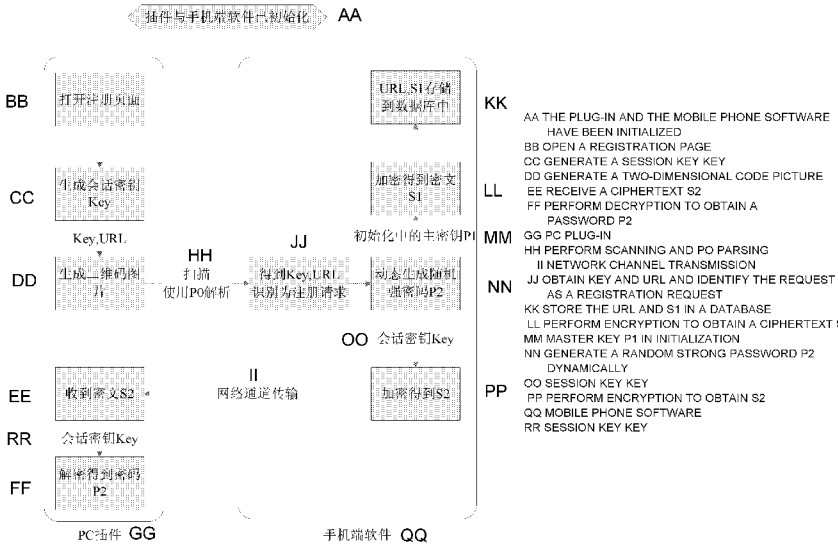


图2 / Fig.2

(57) **Abstract**: Disclosed is a password management method. The method comprises: transferring a session key from a first device to a second device in a first communication mode, wherein the session key is generated by the first device; and returning a first ciphertext from the second device to the first device in a second communication mode, wherein the first ciphertext is obtained through the second device by encrypting a protection password with the session key, and the protection password is generated by the second device dynamically and randomly. Also disclosed is a password management system.

(57) **摘要**: 本发明公开了一种密码管理方法，包括利用第一通信方式从第一装置向第二装置传送会话密钥，其中所述会话密钥由所述第一装置生成；以及利用第二通信方式从所述第二装置向所述第一装置返回第一密文，所述第一密文是所述第二装置利用所述会话密钥对保护密码进行加密所得，所述保护密码由所述第二装置动态随机生成。本发明还公开了一种密码管理系统。

WO 2015/120769 A1

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, 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))。

密码管理方法及系统

技术领域

本发明涉及密码管理领域，特别是涉及一种密码管理方法及系统。

背景技术

随着近年来电子商务的盛行，网络上的交易买卖已成为当今流行的一种交易方法，也随之带来一些交易上的风险。为了提高交易的安全性，人们不得不通过一些安全措施来保证交易的安全，密码的输入便是其中的一种，但是这并非就是一堵密不透风的墙。

由于密码往往是用户自设的，故而所设的密码不可避免地会带有个人的痕迹。另外，用户可能会用同一密码来登录不同的账号，如果某一个账号的密码发生泄漏，其它账号的密码也会有被破解的风险。这些都给密码的安全性带来了隐患。

为了解决这个问题，申请号为 201210225542.X、发明名称为“一种密码管理方法和系统”的发明专利申请提出一种密码管理方法。该方法包括当接收到用户请求某一账号的密码时，为该账号随机生成一密码；保存该账号与密码的对应关系；以及当检测到登录该账号的事件时，发起输出该密码的操作。该方案通过随机生成密码，实现密码的多元化，从而提高了信息安全性。另外，在检测到用户需要输入密码时，发起输出该密码的操作，使得用户无需记忆密码，方便了用户的密码管理。但是，该方案仅保存了密码与账号的对应关系，并没有考虑对密码传输过程进行保护。

申请号为 201110000718.7、发明名称为“一种密码管理系统及方法”的发明专利申请提出了一种密码管理系统，但该密码管理系统对通信信道无保护，一旦出现监听程序，密码将会泄漏，且对于个人用户而言，远程服务器并不一定安全。

可见，在现有密码管理系统中，一方面使用互联网服务器作为存储介质，个人密码隐私不能得到有效的安全保障，另一方面使用传统的网络通信传输，一旦传输通道被监听窃取，用户密码会泄漏。

发明内容

本发明提出一种通信信道分离的密码管理方法及系统。在本发明的方案中，PC 与智能终端（例如手机）的通信分为两条通信通道，分别为二维码与网络通道，通过通信信道的分离，可防止单一通道上的信息泄漏，保障了密码的传输的安全性。

根据本发明的一个方面，提供了一种密码管理方法，包括：利用第一通信方式从第一装置向第二装置传送会话密钥，其中所述会话密钥由所述第一装置生成；利用第二通信方式从所述第二装置向所述第一装置返回第一密文，所述第一密文是所述第二装置利用所述会话密钥对保护密码进行加密所得，所述保护密码由所述第二装置动态随机生成。

在上述密码管理方法中，所述第一装置为计算机插件，而所述第二装置为手机端软件。

在上述密码管理方法中，利用第一通信方式从第一装置向第二装置传送会话密钥包括：所述第一装置将待传送会话密钥以二维码图片的形式显示在计算机屏幕上，以及所述第二装置利用二维码密钥解析图片数据，从而取得所述会话密钥，其中，所述二维码密钥由所述第一装置和所述第二装置共享。

在上述密码管理方法中，利用第二通信方式从所述第二装置向所述第一装置返回第一密文包括：所述第二装置动态随机生成保护密码，并利用所得到的会话密钥将所述保护密码进行加密，从而生成第一密文；以及所述第二装置通过局域网将所述第一密文传送给所述第一装置。

上述密码管理方法还可包括：所述第一装置利用所述会话密钥对所述第一密文进行解密，以便得到所述保护密码。

上述密码管理方法还可包括：所述第二装置利用主密钥来对所述保护密码进行加密以便得到第二密文并将其进行存储，其中所述主密钥由所述第二装置在初始化流程中随机生成。

在上述密码管理方法中，所述第二密文与特定网站的 URL 对应，使得所述第二装置可通过所要访问网站的 URL 来检索与该网站对应的第二密文，并进而获得保护密码。

根据本发明的另一个方面，提供了一种密码管理系统。所述密码管理系统包括第一装置和第二装置，其中，所述第一装置配置成生成会话密钥并利用第一通信方式将所述会话密钥发送给所述第二装置；所述第二装置配置成动态随机生成保护密码，利用所述会话密钥对所述保护密码进行加密从而得到第一密文，并利用第二通信方式向所述第一装置返回所述第一密文。

在上述密码管理系统中，所述第一装置为计算机插件，而所述第二装置为手机端软件。

在上述密码管理系统中，所述第一装置配置成：将待传送会话密钥以二维码图片的形式显示在计算机屏幕上，以及利用二维码密钥解析图片数据，从而取得所述会话密钥，其中，所述二维码密钥由所述第一装置和所述第二装置共享。

在上述密码管理系统中，所述第二装置配置成：通过局域网将所述第一密文传送给所述第一装置。

在上述密码管理系统中，所述第一装置还配置成：利用所述会话密钥对所接收到的第一密文进行解密，以便得到所述保护密码。

在上述密码管理系统中，所述第二装置还配置成：利用主密钥来对所述保护密码进行加密以便得到第二密文并将所述第二密文进行存储，其中所述主密钥由所述第二装置在初始化流程中随机生成。

在上述密码管理方法中，所述第二密文与特定网站的 URL 对应，使得所述第二装置可通过所要访问网站的 URL 来检索与该网站对应的第二密文，并进而获得保护密码。

通过采用本发明的技术方案，用户 PC 端不再保存密码，仅在需要使用密码时向手机端获取，保障了密码存储的安全性。另外，由于 PC 端到手机端的密钥传输使用二维码图片，不使用传统的网络通信，保护了会话密钥不被窃取。再者，生成的二维码图片经过加密处理，且密钥动态可变，保障了传输通道的安全性。本发明技术方案中的密码保护基于用户指定的手机终端，其中的数据通信均在本地完成，无远程服务器，可保证了密码不外泄，保障了密码安全。通过使用本方案，用户可在指定的手机终端中方便快捷的保存个人密码，个人手机随身携带，使用时很方便。

附图说明

在参照附图阅读了本发明的具体实施方式以后，本领域技术人员将会更清楚地了解本发明的各个方面。本领域技术人员应当理解的是：这些附图仅仅用于配合具体实施方式说明本发明的技术方案，而并非意在对本发明的保护范围构成限制。

图 1 是根据本发明的一个实施例、密码管理的初始化流程示意图；

图 2 是根据本发明的一个实施例、密码生成流程示意图；

图 3 是根据本发明的一个实施例、密码使用流程示意图。

具体实施方式

下面介绍的是本发明的多个可能实施例中的一些，旨在提供对本发明的基本了解，并不旨在确认本发明的关键或决定性的要素或限定所要保护的范围。容易理解，根据本发明的技术方案，在不变更本发明的实质精神下，本领域的一般技术人员可以提出可相互替换的其它实现方式。因此，以下具体实施方式以及附图仅是对本发明的技术方案的示例性说明，而不应当视为本发明的全部或者视为对本发明技术方案的限定或限制。

根据本发明的一个实施例，密码管理系统可包括第一装置和第二装置。第一装置可配置成生成会话密钥并利用第一通信方式将该会话密钥发送给第二装置。第二装置配置成动态随机生成保护密码，利用会话密钥对该保护密码进行加密从而得到第一密文，并利用第二通信方式向第一装置返回第一密文。

由于采用两种不同的通信方式来传送密钥和密文，即使其中的一个传输通道（例如网络）被监听，用户所要保护的密码也不会外泄，因为这时被监听到的仅是经会话密钥加密的第一密文。

为了提供网络的安全性，第一装置与第二装置可位于同一局域网中。并且，第一装置可以某种方式与第二装置共享二维码密钥，来用于对二维码图片进行加密及解密，从而即使二维码图片被恶意程序所截屏分析，二维码图片中的内容也不会泄漏。

在一个具体的实施例中，第一装置可以是计算机插件，例如 PC 浏览器中

的插件。第二装置可以是智能终端软件，例如手机端的密码管理软件。

图 1 示意示出了根据本发明的一个实施例的密码初始化流程。首先，确保 PC 与手机处于同一局域网中，使得 PC 通过本地网络可连接手机软件。接着，PC 插件向手机端软件发送二维码密钥，作为探测请求。手机端软件在检测到探测请求后，发送回复。随后，手机端软件随机生成强密码 P1，用作密码加密存储的主密钥。最后，手机端软件保存二维码密钥。至此，该初始化流程完成。

图 2 示意示出了根据本发明的一个实施例的密码生成流程。如图 2 所示，此时 PC 插件与手机端软件已初始化，可正常工作。用户在浏览器中打开网站注册页面。当浏览器插件检测到注册页面时，浏览器插件根据 URL 生成随机会话密钥 Key，插件根据 Key、URL 生成自定义二维码图片，显示在屏幕上。接着，手机端软件扫描二维码，使用二维码密钥解析图片数据，取得会话在密钥 Key，URL 等信息，识别到此次是注册请求，检测提取 Key，URL 等信息。然后，手机端软件动态生成随机强密码 P2，使用初始化流程中生成的主密钥 P1 加密 P2 得到密文 S1，并将 URL、S1 存储到手机端数据库中。再后，手机端软件使用会话密钥 Key 加密 P2 得到密文 S2，并将 S2 发送到插件。最后，插件使用会话密钥 Key 解密 S2，得到 P2 并将密码填入页面密码框中。

图 3 示意示出了根据本发明的一个实施例的密码使用流程。用户在浏览器中打开网站登录页面。当浏览器插件检测到登录页面时，其生成随机会话密钥 Key，根据 Key、URL 生成二维码图片，并将二维码图片显示在屏幕上。接着，手机端软件扫描二维码，使用二维码密钥解析图片数据，取得会话在密钥 Key，URL 等信息，识别到此次是登录请求，检测提取请求中的 Key，URL。手机端软件可根据 URL 从数据库取得密码对应的密文 S1，使用主密钥 P1 将 S1 解密为明文，并将明文使用会话密钥 Key 加密生成密文 S2。然后，手机端软件将 S2 传输到浏览器插件中，插件收到 S2，使用会话密钥解密得到密码。最后，插件将密码填入页面密码框中。

通过采用本发明的技术方案，用户 PC 端不再保存密码，仅在需要使用密码时向手机端获取，保障了密码存储的安全性。另外，由于 PC 端到手机端的密钥传输使用二维码图片，不使用传统的网络通信，保护了会话密钥不被窃取。

再者，生成的二维码图片经过加密处理，且密钥动态可变，保障了传输通道的安全性。本发明技术方案中的密码保护基于用户指定的手机终端，其中的数据通信均在本地完成，无远程服务器，可保证了密码不外泄，保障了密码安全。通过使用本方案，用户可在指定的手机终端中方便快捷的保存个人密码，个人手机随身携带，使用时很方便。

上文中，参照附图描述了本发明的具体实施方式。但是，本领域中的普通技术人员能够理解，在不偏离本发明的精神和范围的情况下，还可以对本发明的具体实施方式作各种变更和替换。这些变更和替换都落在本发明权利要求书所限定的范围内。

权利要求

1. 一种密码管理方法，包括:

利用第一通信方式从第一装置向第二装置传送会话密钥，其中所述会话密钥由所述第一装置生成;

利用第二通信方式从所述第二装置向所述第一装置返回第一密文，所述第一密文是所述第二装置利用所述会话密钥对保护密码进行加密所得，所述保护密码由所述第二装置动态随机生成。

2. 如权利要求 1 所述的密码管理方法，其中，所述第一装置为计算机插件，而所述第二装置为智能终端软件。

3. 如权利要求 2 所述的密码管理方法，其中，利用第一通信方式从第一装置向第二装置传送会话密钥包括:

所述第一装置将待传送会话密钥以二维码图片的形式显示在计算机屏幕上，以及

所述第二装置利用二维码密钥解析图片数据，从而取得所述会话密钥，

其中，所述二维码密钥由所述第一装置和所述第二装置共享。

4. 如权利要求 2 所述的密码管理方法，其中，利用第二通信方式从所述第二装置向所述第一装置返回第一密文包括:

所述第二装置动态随机生成保护密码，并利用所得到的会话密钥将所述保护密码进行加密，从而生成第一密文; 以及

所述第二装置通过局域网将所述第一密文传送给所述第一装置。

5. 如权利要求 1 所述的密码管理方法，还包括:

所述第一装置利用所述会话密钥对所述第一密文进行解密，以便得到所述保护密码。

6. 如权利要求 1 所述的密码管理方法，还包括:

所述第二装置利用主密钥来对所述保护密码进行加密以便得到第二密文并将其进行存储，其中所述主密钥由所述第二装置在初始化流程中随机生成。

7. 如权利要求 6 所述的密码管理方法，其中，所述第二密文与特定网站的 URL 对应，使得所述第二装置可通过所要访问网站的 URL 来检索与该网站

对应的第二密文，并进而获得保护密码。

8. 一种密码管理系统，其特征在于，包括：第一装置和第二装置，

其中，所述第一装置配置成生成会话密钥并利用第一通信方式将所述会话密钥发送给所述第二装置；

其中，所述第二装置配置成动态随机生成保护密码，利用所述会话密钥对所述保护密码进行加密从而得到第一密文，并利用第二通信方式向所述第一装置返回所述第一密文。

9. 如权利要求 8 所述的密码管理系统，其中，所述第一装置为计算机插件，而所述第二装置为智能终端软件。

10. 如权利要求 9 所述的密码管理系统，其中，所述第一装置配置成：

将待传送会话密钥以二维码图片的形式显示在计算机屏幕上，以及

利用二维码密钥解析图片数据，从而取得所述会话密钥，其中，所述二维码密钥由所述第一装置和所述第二装置共享。

11. 如权利要求 9 所述的密码管理系统，其中，所述第二装置配置成：

通过局域网将所述第一密文传送给所述第一装置。

12. 如权利要求 8 所述的密码管理系统，其中，所述第一装置还配置成：

利用所述会话密钥对所接收到的第一密文进行解密，以便得到所述保护密码。

13. 如权利要求 8 所述的密码管理系统，其中，所述第二装置还配置成：

利用主密钥来对所述保护密码进行加密以便得到第二密文并将所述第二密文进行存储，其中所述主密钥由所述第二装置在初始化流程中随机生成。

14. 如权利要求 13 所述的密码管理方法，其中，所述第二密文与特定网站的 URL 对应，使得所述第二装置可通过所要访问网站的 URL 来检索与该网站对应的第二密文，并进而获得保护密码。

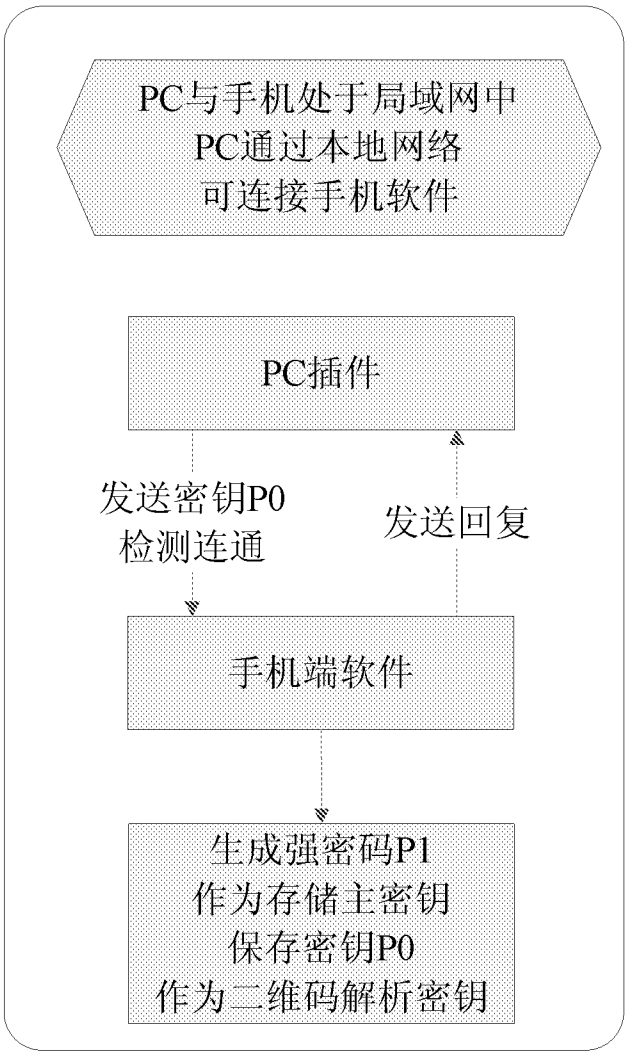

PC与手机处于局域网中
PC通过本地网络
可连接手机软件
PC插件
发送密钥P0
检测连通
发送回复
手机端软件
生成强密码P1
作为存储主密钥
保存密钥P0
作为二维码解析密钥

图 1

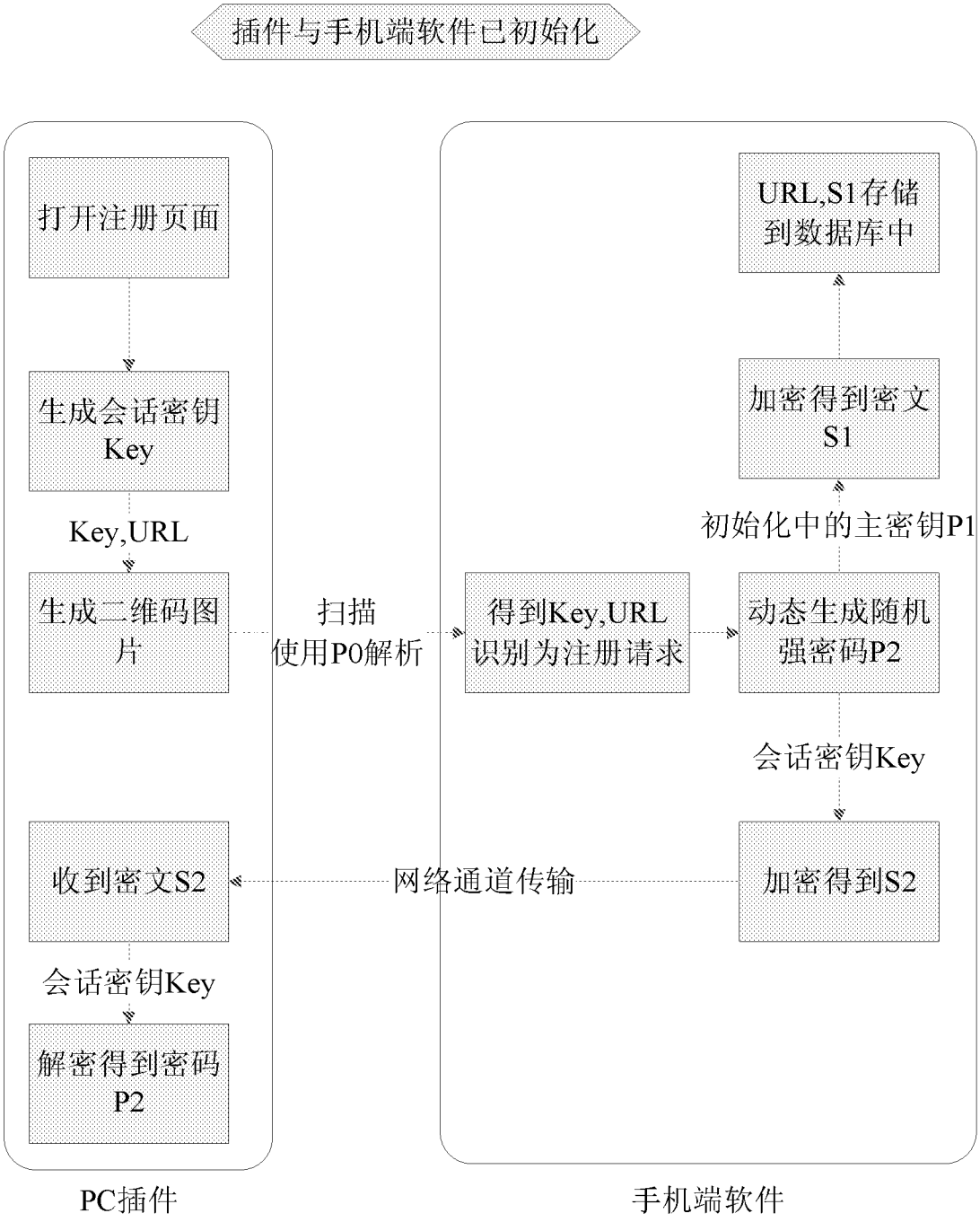

插件与手机端软件已初始化
打开注册页面
生成会话密钥Key
Key,URL
生成二维码图片
扫描
使用P0解析
得到Key,URL识别为注册请求
动态生成随机强密码P2
URL,S1存储到数据库中
加密得到密文S1
初始化中的主密钥P1
会话密钥Key
加密得到S2
网络通道传输
收到密文S2
会话密钥Key
解密得到密码P2
PC插件
手机端软件

图 2


插件与手机端软件已初始化
打开登录页面
生成会话密钥Key
Key,URL
生成二维码图片
扫描
使用P0解析
得到Key,URL识别为登录请求
根据URL读数据库
取得密码对应的密文S1
使用主密钥P1解密
解密为明文
使用会话密钥Key加密
加密为S2
网络通道传输
收到密文S2
会话密钥Key
解密得到密码P2
PC插件
手机端软件

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/071726

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08 (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; G06Q

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; CNTXT; CNKI; VEN: encrypt, session, scan, web page, random, pay+, mobile, mobilephone, two dimension barcode, key, URL, password, encryp+, "2D", input, transmi+, mobile terminal, log on

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103327485 A (NVIDIA CORPORATION), 25 September 2013 (25.09.2013), description, paragraphs [0054]-[0082], and figure 1	1-14
PX	CN 104079404 A (SENSELOCK TECHNOLOGY CO., LTD.), 01 October 2014 (01.10.2014), description, paragraphs [0049]-[0055]	1-5, 8-12
A	CN 103178964 A (CHINA UNIVERSITY OF GEOSCIENCES, WUHAN), 26 June 2013 (26.06.2013), the whole document	1-14

☐ 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
16 April 2015 (16.04.2015)	**06 May 2015 (06.05.2015)**
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 **MA, Yingying** Telephone No.: (86-10) **62411362**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/071726

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103327485 A	25 September 2013	US 8787577 B2	22 July 2014
		US 2013251149 A1	26 September 2013
CN 104079404 A	01 October 2014	None	
CN 103178964 A	26 June 2013	None	

国际检索报告

国际申请号
PCT/CN2015/071726

A. 主题的分类

H04L 9/08(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; G06Q

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;CNTXT;CNKI;VEN:会话，扫描，网页，支付，随机，移动，手机，二维码，密钥，输入，传输，移动终端，登录，密码，加密，session，scan，web page，random，pay+，mobile，mobilephone，two dimension barcode，key，URL，password，encryp+，"2D"，input，transmi+，mobile terminal，log on

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 103327485 A (辉达公司) 2013年 9月 25日 (2013 - 09 - 25) 说明书第[0054]段至第[0082]段，附图1	1-14
PX	CN 104079404 A (北京深思数盾科技有限公司) 2014年 10月 1日 (2014 - 10 - 01) 说明书第[0049]-[0055]段	1-5，8-12
A	CN 103178964 A (中国地质大学武汉) 2013年 6月 26日 (2013 - 06 - 26) 全文	1-14

☐ 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
2015年 4月 16日	2015年 5月 6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	马莹莹 电话号码 (86-10)62411362

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/CN2015/071726

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	103327485	A	2013年 9月 25日	US	8787577	B2	2014年 7月 22日
				US	2013251149	A1	2013年 9月 26日
CN	104079404	A	2014年 10月 1日		无		
CN	103178964	A	2013年 6月 26日		无		