(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
2009 年 12 月 30 日 (30.12.2009)

PCT

(10) 国际公布号
WO 2009/155813 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2009/071883

(22) 国际申请日: 2009 年 5 月 20 日 (20.05.2009)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200810127553.8 2008 年 6 月 27 日 (27.06.2008) CN

(71) 申请人 (对除美国外的所有指定国): **腾讯科技（深圳）有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED)** [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): **陈启祥 (CHEN, Qixiang)** [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。 **陈定佳 (CHEN, Dingjia)** [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。 **傅建兵 (FU, Jianbing)** [CN/CN]; 中国广东省深圳市福田区振兴路赛格科技园 2 栋东 4 楼, Guangdong 518044 (CN)。

(74) 代理人: **北京德琦知识产权代理有限公司 (DEQI INTELLECTUAL PROPERTY LAW CORPORATION)**; 中国北京市海淀区知春路 1 号学院国际大厦 7 层, Beijing 100083 (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, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) **Title**: METHOD FOR STORING ENCRYPTED DATA IN CLIENT AND SYSTEM THEREOF

(54) **发明名称**: 一种在客户端保存加密数据的方法及系统

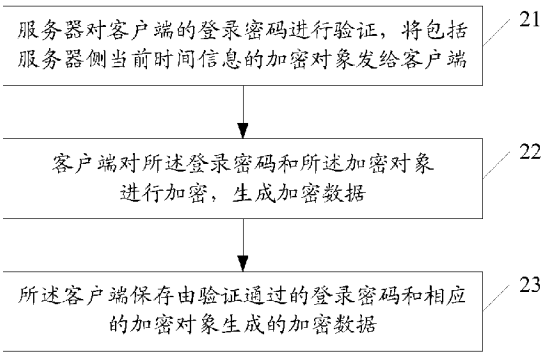

图 2 / Fig. 2

21 A SERVER AUTHENTICATES A LOGIN PASSWORD FROM A CLIENT, AND TRANSMITS AN ENCRYPTION OBJECT WITH THE CURRENT TIME OF THE SERVER SIDE TO THE CLIENT

22 THE CLIENT ENCRYPTS THE LOGIN PASSWORD AND THE ENCRYPTION OBJECT TO GENERATE ENCRYPTED DATA

23 THE CLIENT STORES THE ENCRYPTED DATA GENERATED BY THE VALIDATED LOGIN PASSWORD AND THE CORRESPONDING ENCRYPTION OBJECT

(57) **Abstract**: A method for storing encrypted data in client is provided by the present invention. The following steps are included in the method: a server authenticates a login password from a client, and transmits an encryption object with the current time of the server side to the client; the client encrypts the login password and the encryption object to generate encrypted data; the client stores the encrypted data generated by the validated login password and the corresponding encryption object. A system for storing encrypted data in client is also provided by the present invention. The method and system for storing encrypted data in client provided by the present invention enhance the security of storing encrypted data in client.

[见续页]

WO 2009/155813 A1

(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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))。

(57) **摘要**:

本发明具体公开了一种在客户端保存加密数据的方法，所述方法包括：服务器对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端；客户端对所述登录密码和所述加密对象进行加密，生成加密数据；所述客户端保存由验证通过的登录密码和相应的加密对象生成的加密数据。本发明还公开了一种在客户端保存加密数据的系统。本发明所述在客户端保存加密数据的方法及系统，增强了在客户端保存加密数据的安全性。

一种在客户端保存加密数据的方法及系统

技术领域

本发明涉及通讯网络领域，特别是涉及一种在客户端保存加密数据的方法及系统。

发明背景

一般情况下，用户在客户端使用服务器提供的有权限要求的软件或应用程序时，通常会要求用户输入相应的登录账号和登录密码，以防止非法用户使用。为方便用户登录，客户端提供登录账号的“记住密码”功能。用户在第一次登录时使用“记住密码”功能，与登录账号和登录密码相对应的记住密码票据保存在客户端。当用户在同一客户端再次登录时，只需提供登录账号，该客户端就会依据该登录账号直接读出相应的记住密码票据，登陆账户。

参见图 1，为现有技术中在客户端保存加密数据的方法流程图。所述方法包括以下步骤:

步骤 101：用户在某客户端登录界面输入登录账号和登录密码，并选择“记住密码”功能;

步骤 102：客户端根据用户提供的登录账号和登录密码，将所述登录密码的明文或是由所述登录密码的明文散列得到的密码散列作为记住密码票据，并保存。

当用户再次在所述客户端登录时，输入登录账号，客户端根据用户提供的登录账号，提取出该登录账号对应的记住密码票据，传递给服务器。

服务器校验接收到的记住密码票据与自身保存的登录密码信息是否

相符，如果是，认为登录密码正确，允许用户直接登录；如果否，返回登录密码错误信息，客户端提示用户重新输入登录密码。

服务器保存的登录密码信息可以是登录密码的明文，也可以是与登录密码明文相对应的密码散列。若服务器保存的是登录密码明文，则首先根据登录密码明文计算出相应的密码散列，再校验计算得到的密码散列与接收到的密码散列是否相同；若服务器保存的是密码散列，则直接校验自身保存的密码散列与接收到的密码散列是否相同。

上述在客户端保存记住密码票据的方法，直接将登录密码明文或密码散列作为记住密码票据保存在本地客户端。

很显然，这种做法是非常不安全的。如果用户在公共场合的客户端上使用“记住密码”功能后忘记取消所述功能，生成的记住密码票据将保存在客户端，很容易被他人获取。当所述记住密码票据是登录密码明文时，直接导致登录密码被盗；当所述记住密码票据是密码散列时，只要知道密码散列的计算方法，就可以根据密码散列由散列结果数据库反查出登录密码的明文，导致登录密码被盗。

发明内容

本发明所要解决的技术问题是提供一种在客户端保存加密数据的方法及系统，以增强在客户端保存加密数据的安全性。

为解决上述技术问题，本发明提供了一种在客户端保存加密数据的方法，所述方法包括：服务器对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端；客户端对所述登录密码和所述加密对象进行加密，生成加密数据；所述客户端保存由验证通过的登录密码和相应的加密对象生成的加密数据。

本发明还提供了一种在客户端保存加密数据的系统，包括客户端和

服务器，所述客户端，对登录密码和服务器发来的加密对象进行加密，生成加密数据，保存由服务器验证通过的登录密码和相应的加密对象生成的加密数据；所述服务器，对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端。

与现有技术相比，本发明具有以下优点：

采用本发明实施例所述方法，保存在客户端的加密数据，是采用对登录密码散列得到的散列数据作为密钥，对服务器返回的包括当前时间的加密对象加密得到的。当所述加密数据被获取，即使知道采用的加密算法，由于很难获得关于被加密对象的信息，因此，仅仅根据所述加密数据来获得作为密钥的与登录密码相关的散列数据的可能性非常小，保障保存加密数据的安全性。相较于现有技术中仅仅使用密码散列作为记住密码票据，大大增强了在客户端保存加密数据的安全性。

同时，本发明实施例所述方法中，所述服务器返回的包括当前时间的加密对象，所述当前时间即为在所述客户端首次进行密码保存的时间。即使他人能够根据保存在客户端的加密数据登录成功，服务器会将加密对象中的首次进行密码保存的时间与此次的登录时间进行比较，当首次进行密码保存的时间与此次登录时间之间的间隔过大时，服务器会通知客户端拒绝对所述账号进行自动登录，提示用户重新输入登录密码。因此，即使他人能够根据保存在客户端的加密数据登录成功，也无法长期使用所述账号，在一定期限内，所述账号的自动登录功能将自动取消。

附图简要说明

图 1 为现有技术中在客户端保存加密数据的方法流程图；

图 2 是本发明提供的在客户端保存加密数据的方法流程图；

图 3 是本发明提供的在客户端保存加密数据方法的第一方案流程图;

图 4 是本发明提供的在客户端保存加密数据方法的第二方案流程图;

图 5 是本发明提供的在客户端保存加密数据方法的第三方案流程图;

图 6 为本发明实施例所述在客户端保存加密数据的方法流程图;

图 7 为本发明第一实施例所述在客户端保存加密数据的方法流程图;

图 8 为采用本发明第一实施例所述在客户端保存加密数据的方法实现自动登录的流程图;

图 9 为本发明第二实施例所述在客户端保存加密数据的方法流程图;

图 10 为采用本发明第二实施例所述在客户端保存加密数据的方法实现自动登录的流程图;

图 11 为本发明第一实施例所述在客户端保存加密数据的系统图;

图 12 为本发明第二实施例所述在客户端保存加密数据的系统图。

实施本发明的方式

为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

图 2 是本发明提供的在客户端保存加密数据的方法流程图，如图 2 所示，该方法包括:

步骤 21，服务器对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端。

步骤 22，客户端对所述登录密码和所述加密对象进行加密，生成加密数据。

步骤 23，所述客户端保存由验证通过的登录密码和相应的加密对象生成的加密数据。

由于本发明中客户端保存的加密数据是由验证通过的登录密码和相应的加密对象生成的，其中，登录密码验证通过保证了当前客户端的合法性，包括服务器侧时间信息的加密对象很难被第三方获得，保证了加密数据难以被破解或篡改，因此，应用本发明能够增强在客户端保存加密数据的安全性。

至于具体如何验证客户端登录密码、所述加密对象除了包括服务器侧当前时间信息外还包括哪些信息、验证客户端登录密码和返回加密对象的具体顺序这些具体的技术细节，可以采用多种方案实现，任何一种方案并不构成对本发明的限制，下面对相应的技术方案分别举例说明:

参见图 3，图 3 是本发明提供的在客户端保存加密数据方法的第一方案流程图，如图 3 所示，该流程包括:

步骤 310: 服务器根据客户端的请求，将包括服务器侧当前时间信息的加密对象发给客户端。

步骤 320: 客户端对登录密码和所述加密对象进行加密，生成加密数据，将生成的加密数据发给服务器。

步骤 330: 服务器对所述加密数据进行验证，如果验证通过，则向客户端发送登录密码验证通过的指示，所述客户端保存由验证通过的登录密码和相应的加密对象生成的加密数据。

参见图 4，图 4 是本发明提供的在客户端保存加密数据方法的第二方案流程图，如图 4 所示，该流程包括:

步骤 410: 服务器根据客户端的请求，将包括服务器侧当前时间信

息的加密对象发给客户端。

步骤 420：客户端发送登录密码信息给服务器，接收所述服务器返回的验证结果。

本步骤中的登录密码信息可以就是登录密码，也可以是登录密码的函数等相关信息。

步骤 430：客户端对验证通过的登录密码和所述加密对象进行加密，生成加密数据并保存。

参见图 5，图 5 是本发明提供的在客户端保存加密数据方法的第三方案流程图，如图 5 所示，该流程包括：

步骤 510：客户端发送登录密码信息给服务器。

本步骤中的登录密码信息同步骤 420 中的登录密码信息。

步骤 520：服务器向客户端返回验证结果和包括服务器侧当前时间的加密对象。

步骤 530：客户端对验证通过的登录密码和相应的加密对象进行加密，生成加密数据并保存。

下面以方案三为例，对本发明各种可能的技术细节进行详细介绍：

参见图 6，为本发明实施例所述在客户端保存加密数据的方法流程图。

步骤 1111：客户端发送登录密码给服务器，接收所述服务器返回的包括当前时间的加密对象；

步骤 1112：所述客户端对所述登录密码进行至少一次散列，生成与登录密码对应的散列数据，作为密钥，对所述包括当前时间的加密对象加密，生成加密数据；

步骤 1113：所述客户端保存加密数据。

参见图 7，为本发明第一实施例所述在客户端保存加密数据的方法

流程图。

步骤 201：用户在客户端登录界面输入登录账号和登录密码，并选择“记住密码”功能；

步骤 202：客户端发送包括用户登录账号和登录密码的登录请求给服务器，接收服务器返回的含有当前时间信息的加密对象；

所述当前时间，即为用户在所述客户端第一次保存所述用户登录密码时服务器侧的时间。对同一客户端，所述时间是唯一的。

步骤 203：客户端选择散列算法，对用户提供的登录密码进行至少一次散列，得到与登录密码对应的散列数据，作为密钥；

所述散列算法是单向函数，接收密码的明文，将表述密码明文的字符串，转换成一段无法用来重建原始明文的散列数据，即密码散列。

本发明实施例所述方法中，可以直接对用户提供的登录密码进行散列，生成密码散列，作为密钥。

为了增强登录密码保存的安全性，本发明还可以采用预先设定的运算函数 f 对密码散列进行计算，得到与密码散列相关的散列数据，作为密钥。

所述与密码散列相关的散列数据 = f（密码散列）

f 为预先设定的运算函数，可以根据需要具体设定。f 可以是对所述密码散列再进行 N（N 为不小于 1 的整数）次散列，一般选择 N 为 2、3 或 4，得到散列数据，作为密钥；也可以是先对所述密码散列进行 N 次散列，然后在得到的散列数据中按预先设定的规则加入相应的混淆数据，得到新的散列数据，作为密钥；也可以是先在所述密码散列中按预先设定的规则加入相应的混淆数据，再进行 N 次散列，得到新的散列数据，作为密钥。

在函数 f 中，为了进一步加强安全性，对 N 次散列，每次散列可以

采用相同的散列算法，也可以采用不同的散列算法，以增强作为密钥的散列数据的复杂度，加强被破译的难度。

步骤 204：客户端采用预先设定的加密算法，用所述散列数据作为密钥，对所述加密对象进行加密，生成加密数据，作为记住密码票据，保存在客户端。

所述加密算法是一些特定的公式和法则，用于规定明文和密文之间的变换方法。以常用的数据加密标准数据加密算法（DES：Data Encryption Standard）为例来说明采用加密算法进行加密的过程。

所述 DES 是一种对二进制数据进行加密的算法，包括三个参数：密钥（Key）、数据明文（Data）和模式选择（Mode）。其中所述 Key 为 8 个字节共 64 位，是 DES 算法的工作密钥；Data 也为 8 个字节 64 位，是要被加密或被解密的数据明文；Mode 位 DES 的工作模式，包括加密或解密。

当所述 Mode 为加密时，用 Key 对 Data 进行加密，要加密的数据明文经过 16 轮的叠代、乘积变换、压缩变换等编码过程，生成 Data 的加密数据（64 位）作为 DES 的输出结果。在解密过程中，采用同样的 Key 对密码数据进行解密，再现明码形式的数据明文。

本发明实施例所述方法中，所述加密对象即为要加密的 Data，用所述散列数据作为 Key，Mode 为加密。采用 DES 算法对所述加密对象进行加密运算，生成的加密数据作为记住密码票据保存在客户端。

采用本发明实施例所述方法，保存在客户端的记住密码票据，即加密数据，是采用对登录密码散列得到的散列数据作为密钥，对服务器返回的包括当前时间的加密对象加密得到的。当所述记住密码票据被获取，即使知道采用的加密算法，由于很难获得关于被加密对象的信息，因此，仅仅根据所述记住密码票据来获得作为密钥的与登录密码相关的

散列数据信息的可能性非常小，保障在客户端保存记住密码票据的安全性。相较于现有技术中仅仅使用密码散列作为记住密码票据，大大增强了在客户端保存记住密码票据安全性。

本发明实施例所述方法中，所述作为密钥的散列数据可以通过预先设定的函数 f 对密码散列进行计算得到，即使所述记住密码票据被破译，得到加密对象，但是由于无法获悉函数 f 的具体定义方式，也很难通过反查散列数据获得密码明文。

本发明实施例中所述客户端可以是客户端的软件、万维网（web）触发的网页应用、移动终端类的无线应用等。本发明实施例所述方法适用于即时通信、邮件以及游戏等领域。

参见图 8，为采用本发明第一实施例所述在客户端保存加密数据的方法实现自动登录的流程图。

步骤 301：用户再次在所述客户端登录，客户端根据用户提供的登录账号，从本地提取出对应的记住密码票据，即加密数据，发送含有所述记住密码票据和登录账号的自动登录请求给服务器；

步骤 302：服务器接收到所述自动登录请求信息，从数据库中提取出与所述登录账号对应的密码散列数据，作为解密的密钥；

如果步骤 202 中是由密码散列根据函数 f 运算得到的散列数据作为密钥的，则相应地，步骤 302 中，对所述密码散列按照步骤 202 中所述预先设定的运算函数 f 进行运算，生成散列数据，作为解密的密钥；

步骤 303：服务器用所述散列数据对接收自客户端的记住密码票据进行解密，如果解密成功，证明客户端密码正确，得到加密对象，进入步骤 304；如果解密失败，进入步骤 306；

服务器采用与步骤 204 中相同的加密算法对所述记住密码票据进行解密。

步骤 304: 服务器对解密后得到的所述加密对象进行检查，判断所述记住密码票据是否有效,如果所述记住密码票据有效，进入步骤 305; 否则，进入步骤 306;

所述加密对象为在所述客户端第一次保存所述用户登录密码相关信息时服务器侧的时间，简称为密码保存时间。

所述判断记住密码票据是否有效具体包括以下步骤。

步骤 304a: 判断所述密码保存时间是否晚于服务器当前时间，如果是，说明所述记住密码票据无效，进入步骤 306; 否则，进入步骤 304b;

步骤 304b: 判断所述密码保存时间与所述服务器当前时间之间的时间间隔是否超过预设的最大允许时间间隔，如果是，说明所述记住密码票据已经在本地客户端保存了很久没有登录，所述记住密码票据已经失效，进入步骤 306，否则进入步骤 305;

所述最大允许时间间隔的长度可以根据需要具体设定，一般为一个月。

步骤 305: 服务器通知所述客户端允许用户自动登录，自动登录流程结束。

步骤 306: 服务器通知所述客户端提示用户再次输入密码，自动登录流程结束。

由上述自动登录过程可知，本发明实施例所述在客户端保存加密数据的方法，采用所述密码保存时间作为加密对象，即使他人能够解密成功或是根据保存在客户端的加密数据登录成功，服务器会将加密对象中的密码保存时间与服务器当前时间进行比较，当密码保存时间与服务器当前时间之间的时间间隔过大时，说明所述记住密码票据已经在客户端保存了很久没有登录，服务器会通知客户端拒绝对所述账号进行自动登录，提示用户重新输入登录密码。因此，即使他人能够解密成功或是根

据保存在客户端的加密数据登录成功，也无法长期使用所述账号，在一定期限内，所述账号的自动登录功能将自动取消。

为了进一步增强密码保存的安全性，本发明第一实施例中所述加密对象还可以进一步包括服务器接收密码保存续期请求时间和服务器接收密码保存续期请求次数，分别简称为续期时间和续期次数。

在步骤 201 中，当用户选择“记住密码”功能时，进一步包括：设置“记住密码”功能的有效期。

一般在客户端保存密码的时间是有一定期限的，即有效期，比如一周、一个月、四个月或一年。在用户选择“记住密码”功能时，客户端提示用户选择“记住密码”的有效期或是自动生成默认的有效期。所述有效期即为当前记住密码票据的有效期。

在所述记住密码票据的有效期内，当用户在本地客户端登录时，客户端会自动进行“记住密码”功能续期操作，客户端发出含有当前记住密码票据的密码保存续期请求给所述服务器，服务器对所述记住密码票据解密成功得到所述加密对象后，会自动更新所述加密对象中的续期时间为当前时间，并将所述续期次数加 1，然后对新生成的加密对象进行加密，返回一个新的记住密码票据给所述客户端，客户端保存新的记住密码票据，并为所述新的记住密码票据设置新的有效期。

一般情况下，当客户在所述记住密码票据有效期到期前三天或是一周内登录所述客户端时，客户端会自动为所述用户进行“记住密码”功能的续期操作。如果在此期间，用户一直没有在所述客户端登录，当超过所述有效期后，所述记住密码票据失效，客户端不再保存所述用户的记住密码票据。用户下次登录时，需要再次输入登录账号和登录密码。

当用户在所述客户端第一次选择“记住密码”时，所述续期时间为 0，所述续期次数也为 0。每次所述客户端进行续期操作时，服务器更新

所述加密对象中的续期时间为本次续期时间，并对所述续期次数加 1。

例如：某用户在 2008 年 1 月 1 日 13:33:45 在某客户端登录 MSN 账号时，选择使用“记住密码”功能，假定记住密码票据的有效期默认为一个月，则此时，所述加密对象为：生成时间 = 2008/01/01 13:33:45；续期时间 = 0；续期次数 = 0。假设提前续期时间为到期前一周，则在 2008 年 1 月 24 日后某时间，假设为 2008 年 1 月 25 日 14:34:36，用户在所述客户端登录，客户端自动为用户进行续期操作，更新所述加密对象为：生成时间 = 2008/01/01 13:33:45；续期时间 = 2008/01/25 14:34:36；续期次数 = 1。如果用户在 2008 年 2 月 1 日 13:33:45 前没有在所述客户端登录，则 2008 年 2 月 1 日 13:33:45 起，所述客户端不再保存所述用户的记住密码票据。

对于采用密码保存时间、续期时间和续期次数作为加密对象的在客户端保存加密数据的方法，当用户在客户端自动登录时，所述步骤 304 中，所述判断记住密码票据是否有效具体包括以下步骤：

步骤 304A：判断所述密码保存时间是否晚于服务器当前时间，如果是，说明所述记住密码票据无效，进入步骤 306；否则，进入步骤 304B；

步骤 304B：判断所述密码保存时间与所述服务器当前时间之间的时间间隔是否超过预设的最大允许时间间隔，如果是，说明所述记住密码票据已经在本地客户端保存了很久没有登录，进入步骤 304C，否则进入步骤 305；

所述最大允许时间间隔的长度可以根据需要具体设定，一般为一个月。

步骤 304C：当所述续期时间为 0 或所述续期时间与当前时间之间的时间间隔在预设的最大允许时间间隔内，通知客户端进行续期操作；否则，不允许进行续期操作，认为所述记住密码票据失效，进入步骤 306；

步骤 305：服务器通知所述客户端允许用户自动登录，自动登录流程结束。

步骤 306：服务器通知所述客户端提示用户再次输入密码，自动登录流程结束。

步骤 304C 中所述服务器通知客户端进行续期操作时，客户端发送含有当前记住密码票据的密码保存续期请求给所述服务器，服务器对所述记住密码票据解密成功得到所述加密对象后，会自动更新所述加密对象中的续期时间为当前时间信息，并对所述续期次数加 1，然后对新生成的加密对象进行加密，返回一个新的记住密码票据给所述客户端，所述客户端对所述新的记住密码票据进行保存。因此，对于每次更新后的所述记住密码票据，其续期时间是不相同的，均为最近一次续期操作的时间。

在步骤 304C 中，所述服务器通知客户端进行续期操作前，还可以进一步判断所述续期次数是否已经超过预设的最大允许续期次数，如果是，不再进行续期操作，服务器直接通知客户端提示用户再次输入密码。

在步骤 304C 中，服务器还可以进一步判断所述续期时间与所述生成时间之间的时间间隔，如果所述时间间隔超过预设的最大允许时间间隔，不再进行续期操作，服务器直接通知客户端提示用户再次输入密码。

由上述自动登录过程可知，当所述加密对象为密码保存时间、续期时间和续期次数时，将进一步加强服务器进行验证的强度，增强密码的安全性。在实际运用中，即使所述记住密码票据被破译了，而且实现了登录，如果不续期的话，也不能使用太长时间，降低了密码被盗的损失。

为了增强加密数据保存的可靠性，所述服务器信息还可以进一步包括：格式版本号、混淆数据以及其他数据，以进一步增加加密对象的复杂度，增强加密数据保存的安全性。

本发明实施例所述方法中，加密对象的设定可以根据具体需要灵活设置。当服务器对记住密码票据进行验证，判断所述记住密码票据是否有效时，只要所述加密对象中任一项不满足验证条件，服务器都会通知客户端拒绝用户自动登录，提示用户再次输入登录密码。通过所述方法，大大加强服务器验证的可靠性和灵活性，增强客户端保存加密数据的安全性。

本发明第二实施例与第一实施例的区别在于：用所述散列数据对加密对象进行加密后，再用客户端本地信息对第一次加密后得到的密码数据进行二次加密，从而生成记住密码票据，保存在客户端，进一步增加记住密码票据的复杂度，提高在客户端保存加密数据的安全性。

参照图 9，为本发明第二实施例所述在客户端保存加密数据的方法流程图。

步骤 401：用户在客户端登录界面输入登录账号和登录密码，并选择“记住密码”功能；

步骤 402：客户端发送含有用户登录账号和登录密码的登录请求给服务器，接收服务器返回的包括当前时间的加密对象；

步骤 403：客户端选择散列算法，对用户提供的登录密码进行散列，得到与登录密码对应的散列数据，作为密钥；

步骤 404：客户端采用预先设定的加密算法，用所述散列数据作为密钥，对所述加密对象进行一次加密，得到一次加密数据，再采用客户端本地信息作为密钥，对所述一次加密数据进行二次加密，得到二次加密数据，作为记住密码票据，保存在客户端。

所述客户端本地信息可以是本地客户端自身固有的机器信息，也可以是本地网络相关信息或是本地随机生成数据等。

所述客户端自身固有的机器信息可以是客户端网卡的物理（MAC）

地址、客户端首个硬盘的序列号等。所述本地网络相关信息可以是客户端的 IP 地址、网关地址、子网掩码等。所述本地随机生成数据可以是在本地客户端随机生成的数据，按照预先设定的规则，与客户端自身固有的机器信息或本地网络相关信息一起使用，起混淆作用，用以增强密钥的复杂度，加强被破译的难度。

采用所述客户端本地信息作为密钥是为了增强密钥被破译的难度。根据需要，客户端随机选择这些相关信息，按照一定的规则组成密钥，对加密对象进行加密，别人很难通过技术手段得到上述密钥，因此，即使加密算法被获知，仍很难破译得到加密对象，盗取密码。

一般多采用客户端自身固有的机器信息作为客户端本地信息，因为这部分信息是固定不变的，而且可以通过管理员锁定让外人无法获知，进一步增强密码保存的安全性。相应地，所述本地网络相关信息可能是固定不变的，也可能是随意变动的，例如本地网络采用自动获取 IP 地址的方式，则所述客户端的 IP 地址可能每次都不相同。这样可以进一步增强了密码保存的安全性。

本发明实施例所述方法中，可以采用相同的加密算法对所述加密对象进行一次加密和二次加密，也可以对两次加密分别采用不同的加密算法，以进一步增强密码保存的安全性。

本发明第二实施例所述在客户端保存加密数据的方法，采用客户端本地信息作为密钥，对加密对象进行二次加密，将生成加密数据作为记住密码票据，保存在客户端。

本发明实施例所述方法中，所述作为二次加密密钥的客户端本地信息可以根据客户端的需要由本地客户端自身固有的机器信息、本地网络相关信息和本地随机生成数据按照预先设定的规则随意组合生成，增强了密钥的保密性，即使有人获知了加密算法，但是由于无法获悉密钥的

组成部分和定义方式，很难得到密钥以破译密码，因此，所述在客户端保存加密数据的方法具有很高的安全性。

参见图 10，为采用本发明第二实施例所述在客户端保存加密数据的方法实现自动登录的流程图。

步骤 501：用户再次在所述客户端登录，客户端根据用户提供的登录账号，从本地提取出对应的记住密码票据，根据客户端本地信息对所述记住密码票据进行解密，得到所述一次加密数据，将含有所述一次加密数据和登录账号的自动登录请求信息传递给服务器；

服务器采用与步骤 404 中二次加密算法相应算法对所述记住密码票据进行解密。

步骤 502：服务器接收到所述自动登录请求信息，从数据库中提取出与所述登录账号对应的密码散列数据，作为密钥；

如果步骤 402 中是由密码散列根据函数 f 运算得到的散列数据作为密钥的，则相应地，步骤 502 中，对所述密码散列数据按照步骤 402 中所述预先设定的运算函数 f 进行运算，生成散列数据，作为解密的密钥；

步骤 503：服务器用所述散列数据对接收自客户端的一次加密数据进行解密，如果解密成功，证明客户端密码正确，得到加密对象，进入步骤 504；如果解密失败，进入步骤 506；

服务器采用与步骤 404 中一次加密算法相应算法对所述记住密码票据进行解密。

步骤 504：服务器对解密后得到的所述加密对象进行检查，判断所述记住密码票据是否有效,如果所述记住密码票据有效，进入步骤 505；否则，进入步骤 506；

所述加密对象为在所述客户端第一次保存所述用户登录密码时服务器侧的时间，简称为密码保存时间。

所述判断记住密码票据是否有效的具体过程与本发明实施例一所述步骤 304 相同。

步骤 505：服务器通知所述客户端允许用户自动登录，自动登录流程结束。

步骤 506：服务器通知所述客户端提示用户再次输入密码，自动登录流程结束。

为了增强密码保存的可靠性，本发明第二实施例中所述加密对象也可以进一步包括续期时间和续期次数，所述服务器对续期时间和续期次数的验证过程与第一实施例所述验证过程相同。

为了增强加密数据保存的可靠性，所述服务器信息还可以进一步包括：格式版本号、混淆数据以及其他数据，以增加生成记住密码票据的复杂度。

基于上述在客户端保存加密数据的方法，本发明还提供一种在客户端保存加密数据的系统。

参见图 11，为本发明第一实施例所述在客户端保存加密数据的系统图。

所述系统包括客户端 61 和服务器 62，其中，客户端 61 包括：

加密对象接收模块 610，用于接收所述服务器返回的包括当前时间的加密对象。

登录密码散列模块 611，用于对所述登录密码至少一次散列，生成散列数据。

散列数据加密模块 612，用于按照预先设定的加密算法，利用所述登录密码散列模块 611 生成的散列数据作为密钥，对所述加密对象生成模块 610 生成的加密对象加密，将生成的加密数据作为记住密码票据发送到存储模块 613。

存储模块 613，用于保存所述散列数据加密模块 612 发送的记住密码票据，即加密数据。

为了增强密码保存的可靠性，本发明实施例所述登录密码散列模块 611，可以直接对用户提供的登录密码进行散列，生成密码散列，作为密钥，也可以采用预先设定的运算函数 f 对密码散列进行计算，得到与密码散列相关的散列数据，作为密钥。即使有人获知了散列算法，但是由于无法获悉函数 f 的定义方式，很难得到密钥以破译密码。

采用本发明实施例所述系统，存储模块 613 保存的记住密码票据，即加密数据，是采用对登录密码散列得到的散列数据作为密钥，对服务器返回的含有当前时间的加密对象加密得到的。当所述记住密码票据被获取，即使知道采用的加密算法，由于很难获得关于被加密对象的信息，因此，仅仅根据所述记住密码票据来获得作为密钥的与登录密码相关的散列数据信息的可能性非常小，保障保存密码的安全性。相较于现有技术中仅仅使用密码散列作为记住密码票据，大大增强了在客户端保存加密数据的安全性。

参见图 12，为本发明第二实施例所述在客户端保存加密数据的系统图。

本发明第一实施例和第二实施例所述在客户端保存加密数据的系统的区别在于：第二实施例所述客户端进一步包括本地信息加密模块 614。

所述本地信息加密模块 614，用于采用预先设定的加密算法，利用客户端本地信息作为密钥，对所述散列数据加密模块 612 输出的加密数据加密，生成记住密码票据，发送到存储模块 613。

相应地，所述存储模块 613，用于保存所述本地信息加密模块发送的记住密码票据。

所述客户端本地信息可以是本地客户端自身固有的机器信息，也可

以是本地网络相关信息或是本地随机生成数据等。

本发明实施例所述系统中，所述客户端本地信息加密模块 614 采用客户端本地信息作为密钥，所述客户端本地信息可以根据客户端的需要由本地客户端自身固有的机器信息、本地网络相关信息和本地随机生成数据按照预先设定的规则随意组合生成，增强了密钥的保密性，即使有人获知了加密算法，但是由于无法获悉密钥的组成部分和定义方式，很难得到密钥以破译密码，因此，所述在客户端保存加密数据的系统具有很高的安全性。

以上对本发明所提供的一种在客户端保存加密数据的方法及系统，进行了详细介绍，本文中应用了具体个例对本发明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发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，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发明的限制。

权利要求书

1、一种在客户端保存加密数据的方法，其特征在于，所述方法包括:

服务器对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端;

客户端对所述登录密码和所述加密对象进行加密，生成加密数据;

所述客户端保存由验证通过的登录密码和相应的加密对象生成的加密数据。

2、如权利要求 1 所述的方法，其特征在于，

所述服务器对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端，客户端对所述登录密码和所述加密对象进行加密，生成加密数据包括:

服务器根据客户端的请求将包括服务器侧当前时间信息的加密对象发给客户端;

客户端对登录密码和所述加密对象进行加密，生成加密数据，将生成的加密数据发给服务器;

服务器对所述加密数据进行验证，如果验证通过，则向客户端发送登录密码验证通过的指示。

3、如权利要求 1 所述的方法，其特征在于，

所述服务器对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端，客户端对所述登录密码和所述加密对象进行加密，生成加密数据包括:

服务器根据客户端的请求将包括服务器侧当前时间信息的加密对象发给客户端;

客户端发送登录密码信息给服务器，接收所述服务器返回的验证结果;

客户端对验证通过的登录密码和所述加密对象进行加密，生成加密数据。

4、如权利要求 1 所述的方法，其特征在于，

所述服务器对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端包括:

客户端发送登录密码信息给服务器，接收所述服务器返回的验证结果和包括当前时间的加密对象。

5、如权利要求 1 至 4 任一权项所述的方法，其特征在于，

所述客户端对所述登录密码和所述加密对象进行加密包括:

所述客户端对所述登录密码至少一次散列，生成散列数据，利用所述散列数据对所述加密对象加密。

6、根据权利要求 5 所述的方法，其特征在于，利用所述散列数据对所述加密对象加密具体为:

在所述散列数据中加入混淆数据，利用加入混淆数据后的散列数据对所述加密对象加密。

7、根据权利要求 5 所述的方法，其特征在于，利用所述散列数据对所述加密对象加密后进一步包括:

利用客户端本地信息对所述加密对象二次加密。

8、根据权利要求 7 所述的方法，其特征在于，所述客户端本地信息为客户端网卡物理地址、客户端硬盘序列号、和/或客户端随机生成的数据。

9、根据权利要求 5 所述的方法，其特征在于，进一步包括:

客户端发送含有加密数据的自动登录请求给所述服务器;

所述服务器解密所述加密数据，确定所述加密对象中的当前时间未超过预设的最大允许时间间隔，返回允许自动登录信息给所述客户端。

10、根据权利要求 5 所述的方法，其特征在于，客户端发送登录密码信息给服务器之后，进一步包括：设置密码的保存有效期。

11、根据权利要求 10 所述的方法，其特征在于，进一步包括：

客户端发送含有加密数据的密码保存续期请求给所述服务器；

所述服务器解密所述加密数据，更新解密后得到的加密对象，再对更新后的加密对象加密，返回更新后加密数据给所述客户端；

所述服务器延长密码保存有效期。

12、根据权利要求 11 所述的方法，其特征在于，所述服务器延长密码保存有效期之前，进一步包括：

所述服务器确定接收密码保存续期请求次数未超过预设的最大允许续期次数。

13、根据权利要求 11 所述的方法，其特征在于，所述服务器延长密码保存有效期之前，进一步包括：

所述服务器确定接收密码保存续期请求时间未超过预设的最大允许时间间隔。

14、根据权利要求 11 所述的方法，其特征在于，更新解密后得到的加密对象包括：

服务器在所述加密对象中加设接收密码保存续期请求时间。

15、根据权利要求 14 所述的方法，其特征在于，接收密码保存续期请求时间为最近接收密码保存续期请求的时间。

16、根据权利要求 11 所述的方法，其特征在于，更新解密后得到的加密对象包括：

服务器在所述加密对象中加设接收密码保存续期请求次数。

17、根据权利要求 16 所述的方法，其特征在于，更新解密后得到的加密对象包括：

服务器在所述加密对象中加设格式版本号和混淆数据。

18、一种在客户端保存加密数据的系统，包括客户端和服务器，其特征在于，

所述客户端，对登录密码和服务器发来的加密对象进行加密，生成加密数据，保存由服务器验证通过的登录密码和相应的加密对象生成的加密数据；

所述服务器，对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端。

19、如权利要求 18 所述的系统，其特征在于，

所述客户端，向服务器请求包括服务器侧当前时间信息的加密对象，对登录密码和所述加密对象进行加密，生成加密数据，将生成的加密数据发给服务器，接收服务器发来的登录密码验证通过的指示后，保存所述加密数据；

所述服务器，根据客户端的请求返回包括服务器侧当前时间信息的加密对象，对客户端发来的加密数据进行验证，如果验证通过，则向客户端发送登录密码验证通过的指示。

20、如权利要求 18 所述的系统，其特征在于，

所述客户端，向服务器请求包括服务器侧当前时间信息的加密对象，发送登录密码信息给服务器，接收所述服务器返回的验证结果，对验证通过的登录密码和所述加密对象进行加密，生成加密数据并保存；

所述服务器，根据客户端的请求返回包括服务器侧当前时间信息的加密对象，对客户端发来的登录密码信息进行验证，如果验证通过，则向客户端发送登录密码验证通过的指示。

21、如权利要求 18 所述的系统，其特征在于，

所述客户端，发送登录密码信息给服务器，接收所述服务器返回的

验证结果和包括当前时间的加密对象，对验证通过的登录密码和所述加密对象进行加密，生成加密数据并保存;

所述服务器，接收客户端发来的登录密码信息，对所述登录密码信息进行验证，并将验证结果连同包括服务器侧当前时间信息的加密对象一起发给所述客户端。

22、如权利要求 18 至 21 任一权项所述的系统，其特征在于，

所述客户端包括:

加密对象接收模块，用于发送登录密码信息给服务器，接收所述服务器返回的验证结果和包括当前时间的加密对象;

登录密码散列模块，用于对通过验证的所述登录密码至少一次散列，生成散列数据;

散列数据加密模块，用于利用所述散列数据对所述加密对象加密，生成加密数据;

存储模块，用于保存所述散列数据加密模块发送的加密数据。

23、根据权利要求 22 所述的系统，其特征在于，所述客户端进一步包括:

本地信息加密模块，用于利用客户端本地信息对所述散列数据加密模块输出的加密数据加密;

所述存储模块，用于保存所述本地信息加密模块发送的加密数据。

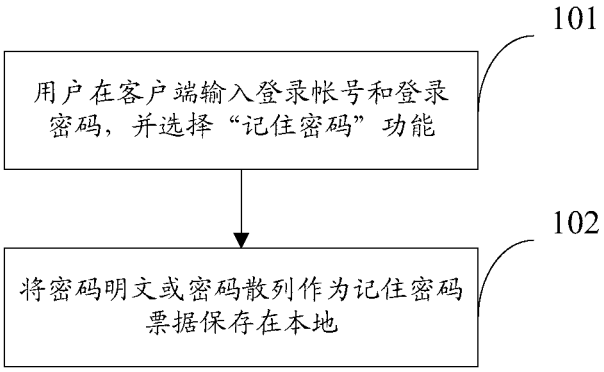
101
用户在客户端输入登录帐号和登录密码，并选择“记住密码”功能
102
将密码明文或密码散列作为记住密码票据保存在本地

图 1

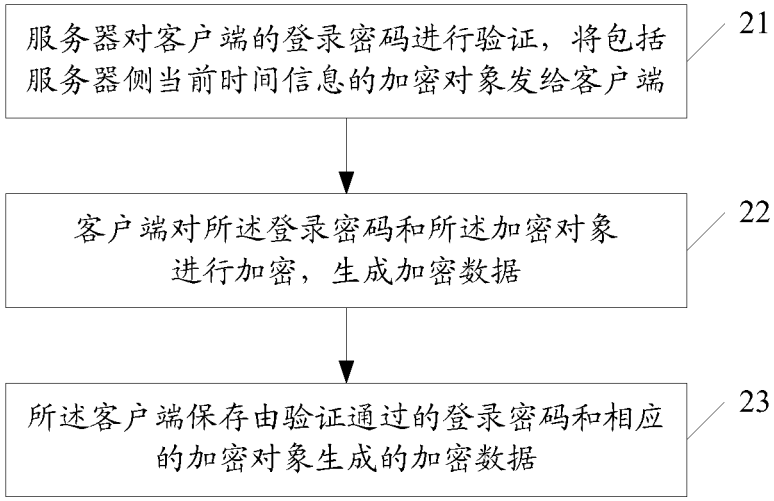
服务器对客户端的登录密码进行验证，将包括服务器侧当前时间信息的加密对象发给客户端
21
客户端对所述登录密码和所述加密对象进行加密，生成加密数据
22
所述客户端保存由验证通过的登录密码和相应的加密对象生成的加密数据
23

图 2

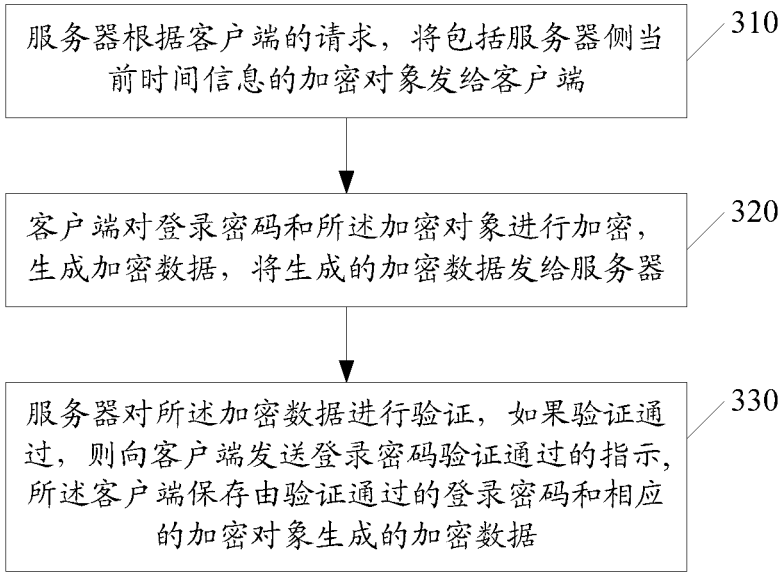
服务器根据客户端的请求，将包括服务器侧当前时间信息的加密对象发给客户端
310
客户端对登录密码和所述加密对象进行加密，生成加密数据，将生成的加密数据发给服务器
320
服务器对所述加密数据进行验证，如果验证通过，则向客户端发送登录密码验证通过的指示，所述客户端保存由验证通过的登录密码和相应的加密对象生成的加密数据
330

图 3

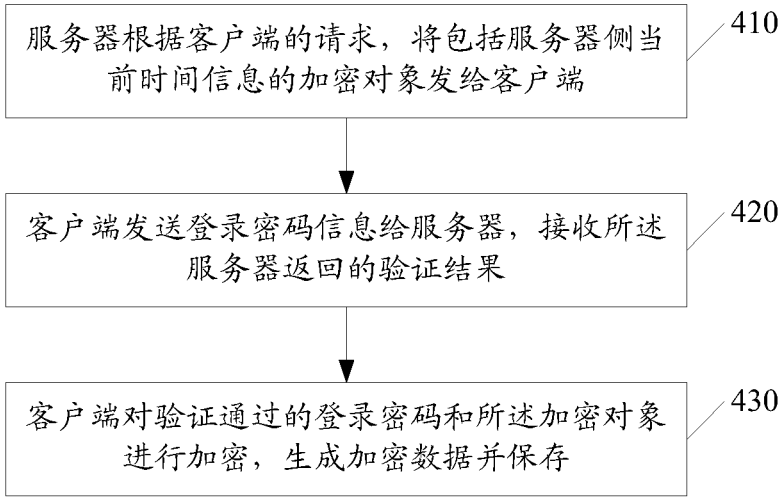
服务器根据客户端的请求，将包括服务器侧当前时间信息的加密对象发给客户端
410
客户端发送登录密码信息给服务器，接收所述服务器返回的验证结果
420
客户端对验证通过的登录密码和所述加密对象进行加密，生成加密数据并保存
430

图 4

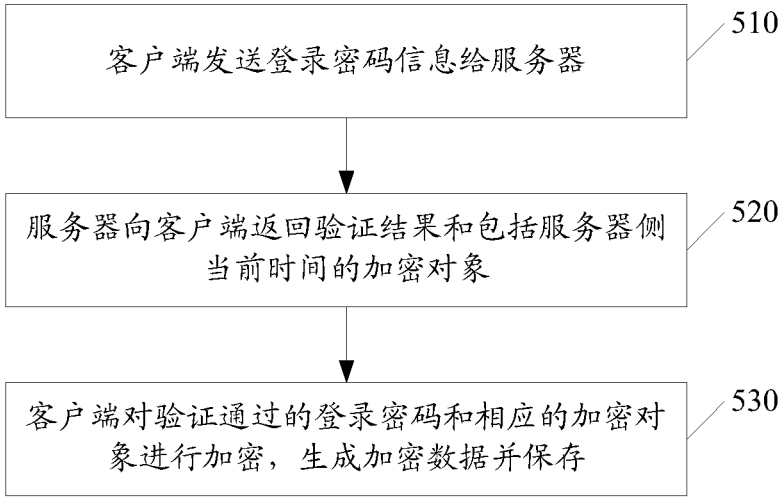
客户端发送登录密码信息给服务器
510
服务器向客户端返回验证结果和包括服务器侧当前时间的加密对象
520
客户端对验证通过的登录密码和相应的加密对象进行加密，生成加密数据并保存
530

图 5

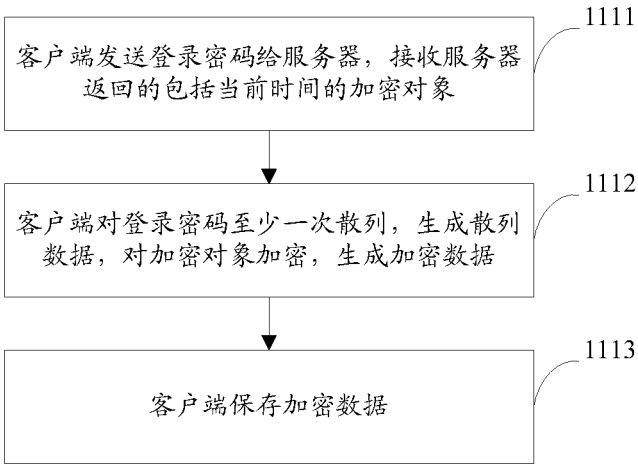
客户端发送登录密码给服务器，接收服务器返回的包括当前时间的加密对象
1111
客户端对登录密码至少一次散列，生成散列数据，对加密对象加密，生成加密数据
1112
客户端保存加密数据
1113

图 6

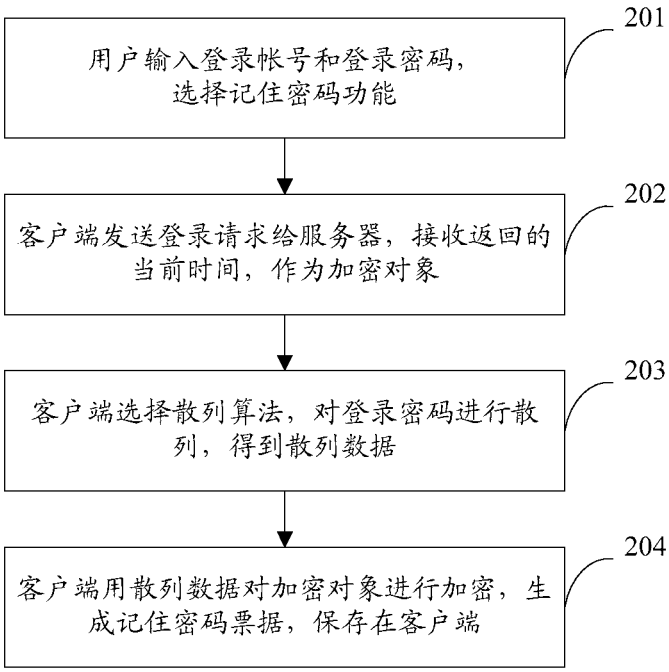
用户输入登录帐号和登录密码，选择记住密码功能
201
客户端发送登录请求给服务器，接收返回的当前时间，作为加密对象
202
客户端选择散列算法，对登录密码进行散列，得到散列数据
203
客户端用散列数据对加密对象进行加密，生成记住密码票据，保存在客户端
204

图 7

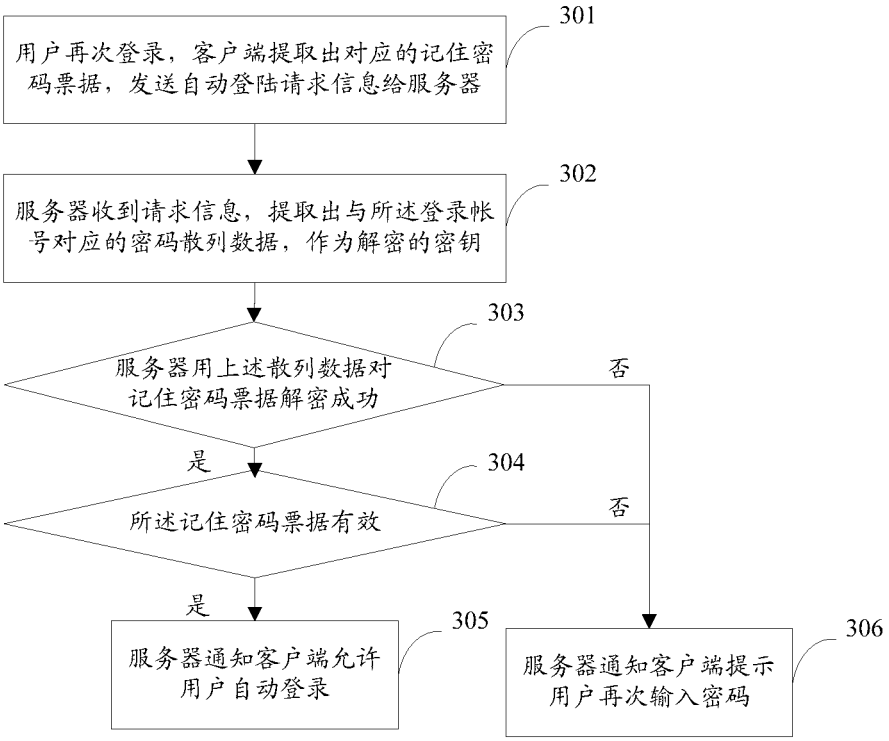
用户再次登录，客户端提取出对应的记住密码票据，发送自动登陆请求信息给服务器
301
服务器收到请求信息，提取出与所述登录帐号对应的密码散列数据，作为解密的密钥
302
服务器用上述散列数据对记住密码票据解密成功
303
否
是
所述记住密码票据有效
304
否
是
服务器通知客户端允许用户自动登录
305
服务器通知客户端提示用户再次输入密码
306

图 8

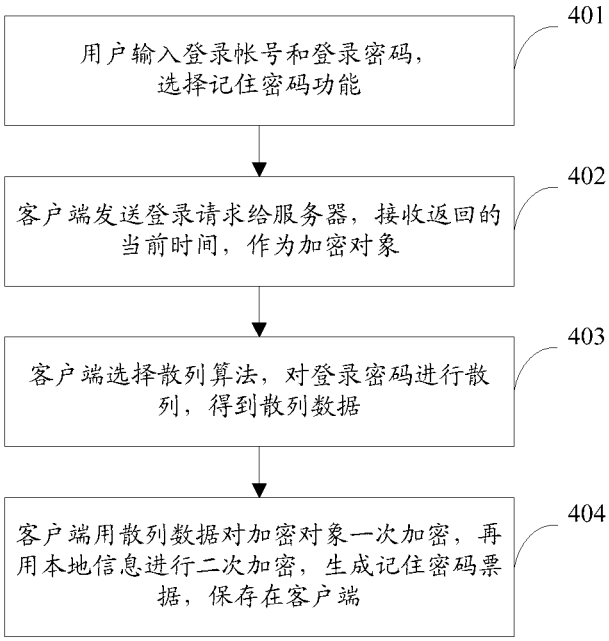
用户输入登录帐号和登录密码，选择记住密码功能
401
客户端发送登录请求给服务器，接收返回的当前时间，作为加密对象
402
客户端选择散列算法，对登录密码进行散列，得到散列数据
403
客户端用散列数据对加密对象一次加密，再用本地信息进行二次加密，生成记住密码票据，保存在客户端
404

图 9

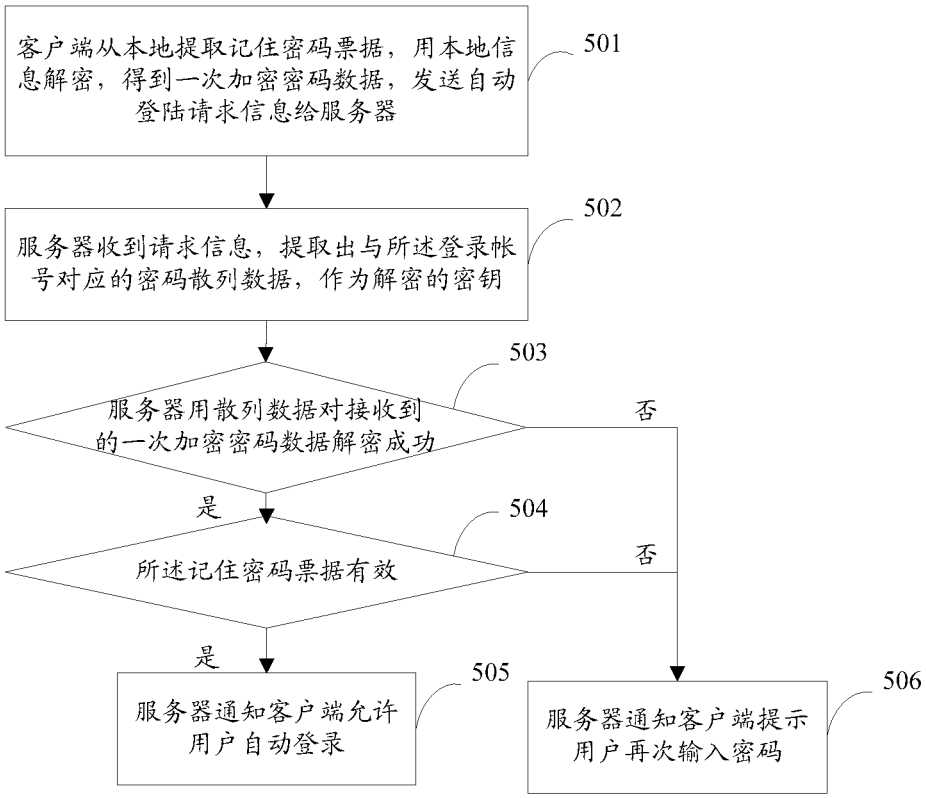
客户端从本地提取记住密码票据，用本地信息解密，得到一次加密密码数据，发送自动登陆请求信息给服务器
501
服务器收到请求信息，提取出与所述登录帐号对应的密码散列数据，作为解密的密钥
502
服务器用散列数据对接收到的一次加密密码数据解密成功
503
否
是
所述记住密码票据有效
504
否
是
服务器通知客户端允许用户自动登录
505
服务器通知客户端提示用户再次输入密码
506

图 10

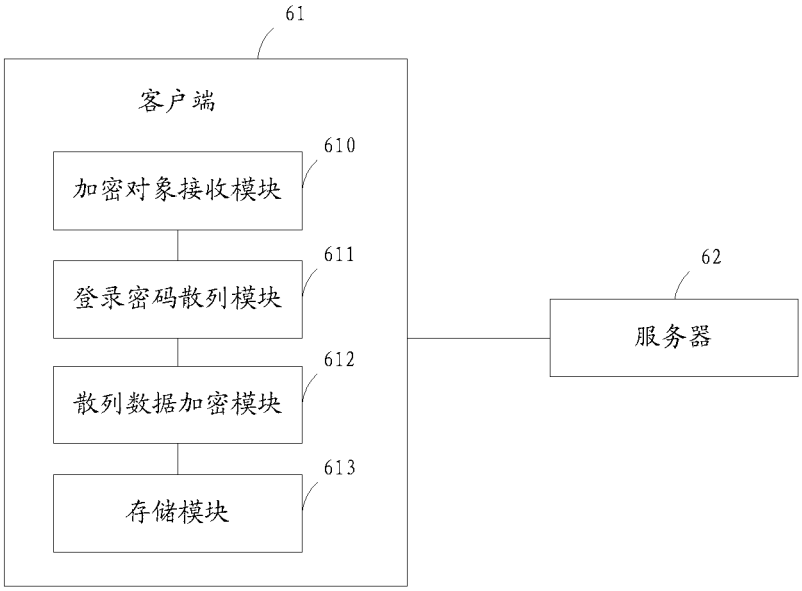
61
客户端
610
加密对象接收模块
611
登录密码散列模块
612
散列数据加密模块
613
存储模块
62
服务器

图 11

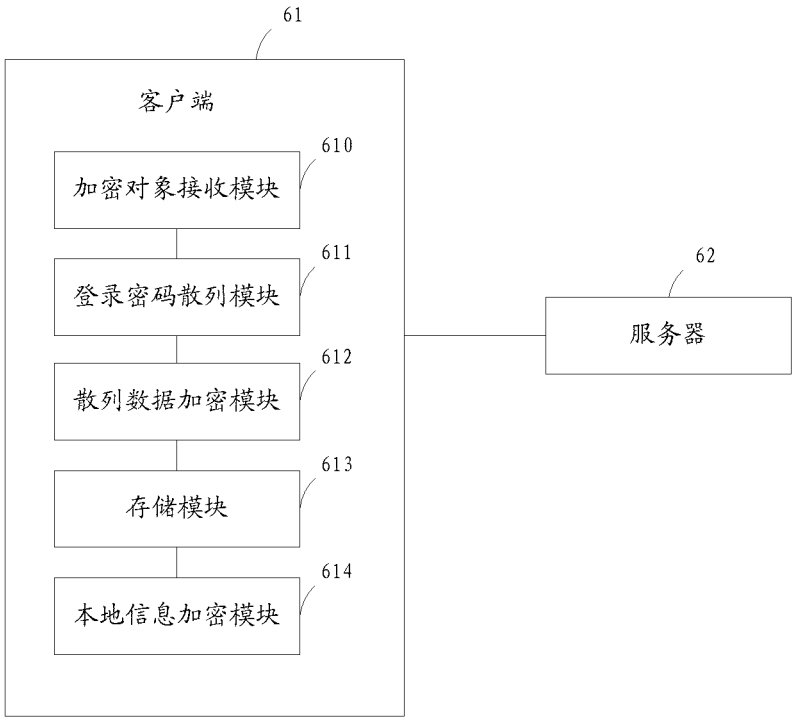
61
客户端
610
加密对象接收模块
611
登录密码散列模块
612
散列数据加密模块
613
存储模块
614
本地信息加密模块
62
服务器

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/071883

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (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: H04L9/-; H04L12/-; H04L29/-;G06F9/-

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, IEEE, CKNI, CNPAT: client, user, terminal, server, login, validat+, authenticat+, authoriz+, verify, time stamp, password, certificat+, store, save

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX PY	CN 101309278 A (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) 19 Nov. 2008 (19.11.2008) Page 4 line 23 to page 14 line 16 in the description, claims 1-15, figures 2-8	1,3-18,20-23 2,19
Y	CN 1567294 A (HUAWEI TECHNOLOGIES CO., LTD.) 19 Jan. 2005 (19.01.2005) Page 3 lines 2 to 24 in the description, figures 2,3	2,19
X Y	CN 1505309 A (MICROSOFT CORPORATION) 16 June 2004 (16.06.2004) Page 19 paragraph 2 to page 22 paragraph 2 in the description, figures 2A,3,5,6	1,18 2,19
A	US 2006/0037064 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 16 Feb. 2006 (16.02.2006) the whole document	1-23

☐ 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
25 July 2009(25.07.2009)	**20 Aug. 2009 (20.08.2009)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer LU, Yanping Telephone No. (86-10)62413782

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/071883

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101309278 A	19.11.2008	None	
CN 1567294 A	19.01.2005	None	
CN 1505309 A	16.06.2004	US 2004098609 A1	20.05.2004
		CA 2450056 A1	20.05.2004
		EP 1422907 A2	26.05.2004
		KR 20040044375 A	28.05.2004
		AU 2003257894 A1	10.06.2004
		JP 2004173285 A	17.06.2004
		BRPI 0305140 A	31.08.2004
		MXPA 03010477 A	15.10.2004
		INDEL 200301357 A	25.11.2005
		RU 2003133768 A	10.05.2005
US 2006/0037064 A1	16.02.2006	None	

国际检索报告

国际申请号
PCT/CN2009/071883

A. 主题的分类

H04L 9/32（2006.01）i

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(标明分类系统和分类号)

IPC：H04L9/-; H04L12/-; H04L29/-;G06F9/-

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）)

CNPAT，CNKI：客户、用户、终端、服务、登陆、认证、鉴权、验证、密码、证书、加密、时间、时间戳、保存；WPI，EPODOC，PAJ，IEEE：client、user、terminal、server、login、validat+、authenticat+、authoriz+、verify、time stamp、password、certificat+、store、save

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
PX	CN 101309278 A（腾讯科技（深圳）有限公司）19.11 月 2008（19.11.2008）	1，3-18，20-23
PY	说明书第 4 页第 23 行至第 14 页第 16 行，权利要求 1-15，图 2-8	2，19
Y	CN 1567294 A（华为技术有限公司）19.1 月 2005（19.01.2005）说明书第 3 页第 2 行至第 24 行，图 2、3	2，19
X	CN 1505309 A（微软公司）16.6 月 2004（16.06.2004）说明书第 19 页第 2	1，18
Y	段至第 22 页第 2 段，图 2A、3、5、6	2，19
A	US 2006/0037064 A1（INTERNATIONAL BUSINESS MACHINES CORPORATION）16.2 月 2006（16.02.2006）全文	1-23

☐ 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

"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
25.7 月 2009（25.07.2009）	**20.8 月 2009 (20.08.2009)**

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 传真号： (86-10)62019451	受权官员 鲁艳萍 电话号码：(86-10) **62413782**

国际检索报告

关于同族专利的信息

国际申请号
PCT/CN2009/071883

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN 101309278 A	19.11.2008	无	
CN 1567294 A	19.01.2005	无	
CN 1505309 A	16.06.2004	US 2004098609 A1	20.05.2004
		CA 2450056 A1	20.05.2004
		EP 1422907 A2	26.05.2004
		KR 20040044375 A	28.05.2004
		AU 2003257894 A1	10.06.2004
		JP 2004173285 A	17.06.2004
		BRPI 0305140 A	31.08.2004
		MXPA 03010477 A	15.10.2004
		INDEL 200301357 A	25.11.2005
		RU 2003133768 A	10.05.2005
US 2006/0037064 A1	16.02.2006	无	