(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
2020 年 8 月 6 日 (06.08.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/155779 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2019/118800

(22) 国际申请日: 2019 年 11 月 15 日 (15.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910100467.6 2019年1月31日 (31.01.2019) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 易杉峰 (YI, Shanfeng); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳市明日今典知识产权代理事务所（普通合伙） (SHENZHEN MINGRIJINDIAN INTELLECTUAL PROPERTY AGENCY FIRM (GENERAL)); 中国广东省深圳市南山区南头街道安乐社区关口二路15号智恒产业园30栋4层406室, Guangdong 518000 (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, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

WO 2020/155779 A1

(54) **Title:** METHOD AND APPARATUS FOR AUTHENTICATING DIGITAL SIGNATURE, COMPUTER DEVICE AND STORAGE MEDIUM

(54) 发明名称: 数字签名的认证方法、装置、计算机设备和存储介质

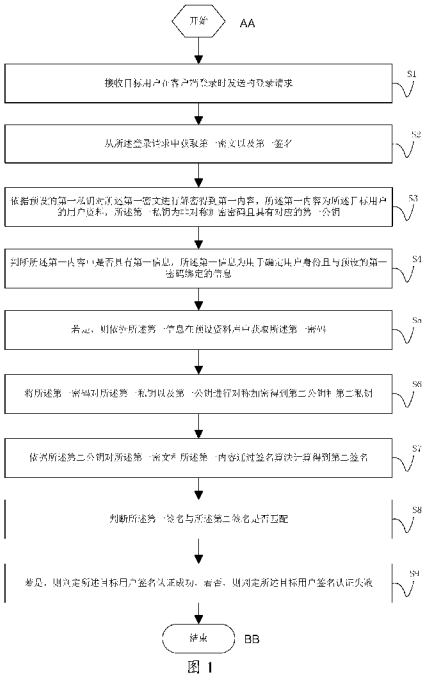

图 1

S1 Receive a login request sent by a target user when the target user logs in to a client
S2 Acquire, from the login request, first ciphertext and a first signature
S3 Decrypt the first ciphertext according to a first private key to obtain a first content, the first content being user information of the target user, and the first private key being an asymmetric encryption password and having a corresponding first public key
S4 Determine whether the first content has first information, the first information being the information used for determining the identity of a user and being bonded to a preset first password
S5 If so, acquire the first password from a preset database according to the first information
S6 Encrypt the first private key and a first public key by using the first password to obtain a second public key and a second private key
S7 Calculate, according to the second public key, the first ciphertext and the first content by means of a signature algorithm to obtain a second signature
S8 Determine whether the first signature matches the second signature
S9 If so, determine that the signature authentication succeeds, and otherwise, determine that the signature authentication fails
AA Start
BB End

(57) **Abstract:** The present application provides a method and an apparatus for authenticating a digital signature, a computer device and a storage medium. Said method comprises: receiving a login request sent by a target user when the target user logs in to a client; acquiring, from the login request, first ciphertext and a first signature; decrypting the first ciphertext according to a first private key to obtain first content; determining whether the first content has first information bonded to a preset first password; if so, acquiring the first password according to the first information; encrypting the first private key and a first public key by using the first password, so

[见续页]

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, 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))。

as to obtain a second public key and a second private key; calculating, according to the second public key, the first ciphertext and the first content by means of a signature algorithm to obtain a second signature; determining whether the first signature matches the second signature; if so, determining that the signature authentication succeeds; and otherwise, determining that the signature authentication fails. The method above improves the security of authentication of secret-free login, and also verifies the consistency of the signatures on the basis of preliminary verification of the first content, thereby providing high security by means of double verification.

(57) 摘要：本申请提出的数字签名的认证方法、装置、计算机设备和存储介质，其中方法包括：接收目标用户在客户端登录时发送的登录请求；从登录请求中获取第一密文和第一签名；依据第一私钥对第一密文解密得到第一内容；判断第一内容中是否具有与预设的第一密码绑定的第一信息；若是，则依据第一信息获取第一密码；将第一密码对第一私钥和第一公钥加密得到第二公钥和第二私钥；依据第二公钥对第一密文和第一内容通过签名算法计算得到第二签名；判断第一签名与第二签名是否匹配；若是，则判定签名认证成功，否则判定签名认证失败，通过上述方法大大地提高了免密登录认证的安全性，且在初步验证第一内容的基础上，还验证签名是否一致，双重验证，安全性更高。

说明书

发明名称: 数字签名的认证方法、装置、计算机设备和存储介质

[0001] 本申请要求于2019年1月31日提交中国专利局、申请号为201910100467.6，申请名称为“数字签名的认证方法、装置、计算机设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[0002] 本申请涉及到数字签名的技术领域，特别是涉及到一种数字签名的认证方法、装置、计算机设备和存储介质。

背景技术

[0003] 随着人们生活与互联网的联系越来越密切，各种移动终端及其上应用程序也逐渐普及，在互联网上确定一个用户身份极其重要，其中如登录手机、平板、各种支付软件等等，都涉及互联网中用户身份确认问题。

[0004] 目前一般是通过静态密码、动态密码以及PKI（Public Key Infrastructure）进行确认用户身份，例如静态密码结合动态验证码等，但是容易泄露，安全性不高，且不够便利。另一方面现有的免密登录技术中程序相对简单，容易被破解，无法满足用户身份认证的高度安全性以及方便性的需求。

发明概述

技术问题

[0005] 本申请的主要目的为提供一种数字签名的认证方法、装置、计算机设备和存储介质，旨在解决现有数字签名认证安全性较低的技术问题。

问题的解决方案

技术解决方案

[0006] 基于上述发明目的，本申请提出一种数字签名的认证方法，包括：

[0007] 接收目标用户在客户端登录时发送的登录请求；

[0008] 从所述登录请求中获取第一密文以及第一签名；

[0009] 依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一

公钥；

[0010] 判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；

[0011] 若是，则依据所述第一信息在预设资料库中获取所述第一密码；

[0012] 将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；

[0013] 依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；

[0014] 判断所述第一签名与所述第二签名是否匹配；

[0015] 若是，则判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[0016] 本申请还提供一种数字签名的认证装置，包括：

[0017] 接收请求单元，用于接收目标用户在客户端登录时发送的登录请求；

[0018] 获取签名单元，用于从所述登录请求中获取第一密文以及第一签名；

[0019] 解密内容单元，用于依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；

[0020] 判断信息单元，用于判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；

[0021] 获取密码单元，用于判定所述第一内容中具有第一信息时，依据所述第一信息在预设资料库中获取所述第一密码；

[0022] 对称加密单元，用于将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；

[0023] 签名计算单元，用于依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；

[0024] 判断匹配单元，用于判断所述第一签名与所述第二签名是否匹配；

[0025] 判定认证单元，用于判定所述第一签名与所述第二签名匹配时，判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[0026] 本申请还提供一种计算机设备，包括存储器和处理器，所述存储器存储有计算机可读指令，所述处理器执行所述计算机可读指令时实现上述方法的步骤。

[0027] 本申请还提供了一种计算机可读存储介质，其上存储有计算机可读指令，所述计算机可读指令被处理器执行时实现上述方法的步骤。

发明的有益效果

有益效果

[0028] 通过多次加密解密过程，大大地提高了认证的安全性，用户可以安全地免密登录，简单方便，且在获得第一内容之后初步验证的基础上，还通过验证签名是否一致，双重验证，安全性更高。

对附图的简要说明

附图说明

[0029] 图1 为本申请一实施例中数字签名的认证方法的步骤示意图；

[0030] 图2 为本申请一实施例中数字签名的认证装置的结构示意框图；

[0031] 图3 为本申请一实施例的计算机设备的结构示意框图。

[0032] 本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

实施该发明的最佳实施例

本发明的最佳实施方式

[0033] 应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0034] 参照图1，本实施例中的数字签名的认证方法，包括：

[0035] 步骤S1：接收目标用户在客户端登录时发送的登录请求；

[0036] 步骤S2：从所述登录请求中获取第一密文以及第一签名；

[0037] 步骤S3：依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；

[0038] 步骤S4：判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；

[0039] 步骤S5：若是，则依据所述第一信息在预设资料库中获取所述第一密码；

[0040] 步骤S6：将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；

[0041] 步骤S7：依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；

[0042] 步骤S8：判断所述第一签名与所述第二签名是否匹配；

[0043] 步骤S9：若是，则判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[0044] 本实施例中，目标用户在客户端进行登录时，如登录手机或登录某个应用软件（Application，简称APP），可采用本申请提供的方法进行免密认证登录，安全快捷，具体而言，如上述步骤S1及S2所述，当目标用户在客户端进行登录，这时会发送登录请求到服务端，登录请求中携带有密文以及签名信息，服务端接收到该登录请求之后，可从该登录请求中获取到第一密文以及第一签名，第一密文为事先对预设的明文进行加密得到的密文，第一签名为字母数字的字符组合。需要注意的是，该第一密文以及第一签名可能是恶意破解登录认证的信息，这时预设的明文可为恶意破解登录认证之前获取的各种虚假信息，如虚假的用户资料，包括姓名、性别、手机号码等等，此时可通过上述认证方法可判定其认证不成功。但第一密文以及第一签名也有可能是已进行注册并绑定信息的用户，而对于这种情况该第一密文以及第一签名均唯一地对应上述目标用户，其中产生该第一签名的方法与在认证过程中生成第二签名的方法一致。

[0045] 如上述步骤S3所述，由于第一密文为通过第一公钥对预设的明文进行加密得到，故而可通过第一私钥对第一密文进行解密得到上述预设的明文，为了便于描述，此处预设的明文命名为第一内容，上述加密以及解密均可通过非对称加密算法（Rivest-Shamir-Adleman，简称RSA）进行计算，其公式如下：密文＝明文E mod N，则公钥＝(E,N)；明文＝密文D mod N，其私钥＝(D,N)，本实施例中，上述第一内容可为目标用户用于注册时使用的用户资料，如姓名、性别、证件号码以及手机号码等等。

[0046] 需要注意的是，本实施例中的第一公私钥对（即上述第一公钥和第一私钥）由

系统统一生成，对于不同的用户均可采用该第一公私钥对，即在上述步骤S1之前，可依据上述RSA算法产生所有用户统一使用的第一私钥以及第一公钥，所有用户当中包括上述目标用户，以及在服务端已注册并绑定信息的用户。

[0047] 如上述步骤S4-S5所述，上述第一信息可为上述用户资料内容中的任意一个属性，且事先和第一密码绑定，本实施例中，第一信息为姓名，则这时可判断解密出来的第一内容中是否包含有已经被绑定的姓名，若有，则说明当前请求登录的目标用户可能为上述客户端或者当前登录网站的真实用户，由于第一信息已与第一密码绑定，这时可依据第一信息在预设的资料库中获取第一密码。与现有技术中在此处获得第一信息即判定目标用户通过认证相比，本方案提供的身份认证还包括步骤S6-S9进一步验证，更加安全可靠。

[0048] 但是，若判断第一内容中不具有第一信息，则可直接判定目标用户未通过身份认证。具体的说，上述步骤S4之后，包括：

[0049] 步骤S40：若判定所述第一内容中不具有所述第一信息，则生成结束认证指令，并发送认证失败的警示信息至所述客户端。

[0050] 本实施例中，当判定第一内容不具有第一信息，即表明上述目标用户可能不是上述客户端或者当前登录的网站的用户，或者可能该目标用户没有事先认证绑定，所以无法进行免密登录，这时系统会生成结束认证的指令，依据该指令停止执行接下来的认证流程，同时发送认证失败的警示信息给用户。

[0051] 如上述步骤S6所述，上述对称加密可以通过对称加密算法（Advanced Encryption Standard，简称AES）进行计算，相对于加密算法（Des encryption algorithm，简称DES）而言，AES算法安全性更高，具体可使用第一密码对上述第一公钥以及第一私钥通过AES算法进行对称加密得到一对公私钥对，此处为了区别分别命名为第二公钥和第二私钥，由于AES算法为现有算法，此处不再赘述。

[0052] 如上述步骤S7所述，当获得第二公钥，这时可采用第二公钥对上述第一密文和第一内容通过签名算法计算，得到上述第二签名。上述签名算法可以为HMAC-SHA1签名算法，该算法为对一段信息进行生成签名摘要的算法，亦为现有算法，此处不再赘述。

[0053] 如上述步骤S8-S9所述，当得到第二签名，则可以将第二签名和第一签名进行比较，判断两者是否匹配，若是，则说明当前请求登录的目标用户已事先进行了绑定认证，为该当前登录的真实用户，即用于生成第一签名以及第二签名的信息一致且生成步骤也一致，这时可判定目标用户签名认证成功，若第一签名和第二签名不匹配，则说明获得到用户资料与预存的不匹配，该目标用户事先并没有绑定认证，这时可判定目标用户签名认证失败。

[0054] 在一个实施例中，上述步骤S1之前，包括：

[0055] 步骤S01：获取所述目标用户在客户端注册时输入的用户资料；

[0056] 步骤S02：将所述用户资料中的第一信息与所述第一密码进行绑定；

[0057] 步骤S03：将所述第一密码对所述第一公钥以及第一私钥进行对称加密得到第二公钥和第二私钥；

[0058] 步骤S04：将所述第一公钥和第二公钥发送至目标用户的客户端，以便于所述客户端依据所述第二公钥对所述第一密文以及所述第一内容通过签名算法计算得到所述第一签名，其中，所述第一密文为所述客户端获取所述第一内容后，依据所述第一公钥对所述第一内容进行非对称加密得到的密文。

[0059] 本实施例中，若目标用户认证成功，即表明该目标用户在进行免密登录之前，目标用户已通过客户端与服务端进行绑定确认身份，而这一过程可通过上述步骤S01-S04来实现，首先服务端获取到客户端发送过的用户资料信息，其中包括第一信息，这时服务端可通过通用唯一识别码（Universally Unique Identifier，简称UUID）生成器对应用户资料信息生成第一密码，并将第一密码与第一信息绑定，然后使用第一密码对上述第一公钥以及第一私钥进行对称加密得到第二公钥和第二私钥，实现的方式可参照上述步骤S6，同样可采用AES算法进行计算。然后服务端将第一公钥和第二公钥发送至客户端，客户端接收到第一公钥和第二公钥之后，获取上述第一内容，包括用户的资料，如姓名、性别、证件号码、手机号码等等，然后在客户端中使用第一公钥对第一内容通过RSA算法进行非对称加密得到第一密文，再使用第二公钥对第一密文和第二内容通过为HMAC-SHA1签名算法计算得到第一签名，完成上述步骤之后，这时可对目标用户进一步验证，将第一密文和第一签名发送至服务端按上述步骤S1-S9进行验证，即可绑

定确认用户身份，当该用户再次免密登陆时，直接发送登陆请求到服务端，然后通过服务端经过上述步骤S1-S9处理即可。

[0060] 在一个实施例中，上述步骤SS02，包括：

[0061] 步骤S021：通过通用唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串；

[0062] 步骤S022：将所述字符串记作所述第一密码，并将所述第一密码与所述目标用户的第一信息进行绑定。

[0063] 本实施例中，可以理解的是，在用户进行免密登录之前，需要目标用户的客户端与服务端进行绑定确认身份，当目标用户进行注册以确认身份的时候，目标用户会通过客户端输入上述用户资料，这时服务端获取这些用户资料，并会通过UUID生成器随机生成一串对应上述用户资料的字符串，该字符串可预设位数，该串字符串即为上述第一密码，然后将用户用于确认身份的第一信息与该第一密码进行绑定，对于不同的用户，对应生成的第一密码也不一样，每一个用户都对应唯一的第一密码。

[0064] 进一步地，上述步骤S021，包括：

[0065] 步骤S0211：通过通用唯一识别码生成器生成指定位数的初始字符串；

[0066] 步骤S0212：在所述初始字符串的指定位置添加时间戳以得到所述预设位数的字符串。

[0067] 本实施例中，为了进一步提高安全性，可以在UUID生成器生成字符串的基础上进一步复杂化，如上述步骤 S0211- S0212所述，先通过UUID生成器生成指定位数的初始字符串，然后在该初始字符串的指定位置添加时间戳，例如在初始字符串的起始位置或结束位置加上时间戳，得到上述预设位数的字符串。

[0068] 在一个具体实施例中，服务端通过UUID生成器随机生成为32位字符串的第一密码（vfcqkkHIzMuIxQ9mszaLAY61WpRWR6mx），将该第一密码与用户的第一信息（name=张三）绑定，使用第一密码对预设的第一公钥以及第一私钥通过AES算法对称加密得到第二公钥以及第二私钥，然后将第一公钥和第二公钥发送到客户端存储。

[0069] 客户端接收到第一公钥和第二公钥之后，获取用户的第一内容（name=张三&s

ex=性别&age=年龄&address=家庭地址&idNo=证件号码&phone=手机号码&其他），使用第一公钥对第一内容通过RSA算法进行非对称加密得到第一密文（U2FsdGVkX19z1299htPGOqzL4hfiHKPSqAMPtajMTUBEj7lSbEX4ayfvjGFjeo2Z7mfslOTjBc8ZCPB72AexfQeYocwZfZLpdIdOXyr5iXak+gWUDQ4ciPVpHiHAuQ0hF2iP5bzEhEdejb2iS1VWNQ==），然后使用第二公钥对第一密文和第一内容通过HMAC-SHA1签名算法计算得到第一签名（86aa7900076b8925866c3208170c5a79099b6121），登录认证时，客户端将第一密文和第一签名发送至服务端。

[0070] 服务端接收到上述第一密文以及第一签名后，使用第一私钥对第一密文通过RSA算法进行解密得到第一内容（name=张三&sex=性别&age=年龄&address=家庭地址&idNo=证件号码&phone=手机号码&其他），通过第一内容中的第一信息（name=张三）在预设的资料库中找到第一密码（vfcqkkHIzMuIxQ9mszaLAY61WpRWR6mx），使用第一密码对第一公钥以及第一私钥通过AES算法对称加密得到第二公钥以及第二私钥,使用第二公钥对第一密文和第一内容通过HMAC-SHA1签名算法计算得到第二签名（86aa7900076b8925866c3208170c5a79099b6121），将第一签名和第二签名进行对比，判断一致，则通过免密认证。

[0071] 在一个实施例中，上述步骤S3，包括：

[0072] 步骤S31：依据预设的第一私钥对所述第一密文进行解密得到解密内容，所述解密内容为多个预设格式的英文单词加汉字的组合,每个所述组合均为一个英文单词以及对应的汉字；

[0073] 步骤S32：将所述解密内容中各个所述组合按所述组合的英文单词起始字母的自然顺序进行排序，若所述起始字母一致，则按所述英文单词的第二个字母的自然顺序进行排序，以此类推，以得到所述第一内容。

[0074] 本实施例中，为了方便用户，使用更简化，在依据第一私钥对第一密文进行解密之后，将得到的解密内容按各个英文单词起始字母的自然顺序进行排序，在一个实施例中，上述步骤S32包括：判断所述解密内容中各所述组合的英文单词起始字母是否均一致；若不一致，则将各所述组合按所述组合的英文单词起始字母的自然顺序进行排序，若均一致，则将各所述组合按英文单词的第二个字母的自然顺序进行排序，若各所述组合的第二个字母一致，则按各所述组合的

英文单词的第三个字母的自然顺序进行排序，以此类推，得到所述第一内容。

[0075] 在另一实施例中，首先判断上述解密内容中各组合的英文单词起始字母是否一致，若部分组合的英文单词的起始字母一致，则将各组合先按英文单词的起始字母自然顺序排序，其中起始字母一致的组合置于同一位置，然后将起始字母一致的组合按其英文单词的第二个字母的自然顺序进行排序，若该部分组合的英文单词的第二个字母也一致，则将起始字母以及第二个字母均一致的组合按其英文单词的第三个字母的自然顺序进行排序，以此类推，得到上述第一内容。

[0076] 具体而言，解密内容为多个预设格式的英文单词加汉字的组合，且每个均为一个英文单词以及对应的汉字，如上述例子中的解密内容为：name=张三&sex=性别&age=年龄&address=家庭地址&idNo=证件号码&phone=手机号码&其他，其中，“name=张三”、“sex=性别”等均分别为一个组合，上述解密内容排序之后则得到的为address=家庭地址&age=年龄&phone=手机号码&name=张三&sex=性别&其他，这样最后通过签名算法计算得到的签名也会按字母的自然顺序自动排序。为了保证第一签名和第二签名正常匹配，在步骤S31之前，客户端获取第一内容时，先将第一内容按起始字母的自然顺序排序，这样每个用户的签名设定规则，则可统一按字母的自然顺序排序，用户使用更方便。

[0077] 参照图2，本实施例中数字签名的认证装置，包括：

[0078] 接收请求单元100，用于接收目标用户在客户端登录时发送的登录请求；

[0079] 获取签名单元200，用于从所述登录请求中获取第一密文以及第一签名；

[0080] 解密内容单元300，用于依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；

[0081] 判断信息单元400，用于判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；

[0082] 获取密码单元500，用于判定所述第一内容中具有第一信息时，依据所述第一信息在预设资料库中获取所述第一密码；

[0083] 对称加密单元600，用于将所述第一密码对所述第一私钥以及第一公钥进行对

称加密得到第二公钥和第二私钥；

[0084] 签名计算单元700，用于依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；

[0085] 判断匹配单元800，用于判断所述第一签名与所述第二签名是否匹配；

[0086] 判定认证单元900，用于判定所述第一签名与所述第二签名匹配时，判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[0087] 本实施例中，目标用户在客户端进行登录时，如登录手机或登录某个APP，可采用本方案提供的方法进行免密认证登录，安全快捷，具体而言，如上述接收请求单元100及获取签名单元200所述，当目标用户在客户端进行登录，这时会发送登录请求到服务端，登录请求中携带有密文以及签名信息，服务端接收到该登录请求之后，可从该登录请求中获取到第一密文以及第一签名，第一密文为事先对预设的明文进行加密得到的密文，第一签名为字母数字的字符组合。需要注意的是，该第一密文以及第一签名可能恶意破解登录认证的信息，这时预设的明文可为恶意破解登录认证之前获取的各种虚假信息，如虚假的用户资料，包括姓名、性别、手机号码等等，此时可通过上述认证装置判定其认证不成功。但第一密文以及第一签名也有可能是已进行注册并绑定信息的用户，而对于这种情况该第一密文以及第一签名均唯一地对应上述目标用户，其中产生该第一签名的方法与在认证过程中生成第二签名的过程一致。

[0088] 如上述解密内容单元300所述，由于第一密文为通过第一公钥对预设的明文进行加密得到，故而可通过第一私钥对第一密文进行解密得到上述预设的明文，为了便于描述，此处预设的明文命名为第一内容，上述加密以及解密均可通过RSA算法进行计算，其公式如下：密文＝明文E mod N，则公钥＝(E,N)；明文＝密文D mod N，其私钥＝(D,N)，本实施例中，上述第一内容可为目标用户用于注册时使用的用户资料，如姓名、性别、证件号码以及手机号码等等。

[0089] 需要注意的是，本实施例中的第一公私钥对（即上述第一公钥和第一私钥）由系统统一生成，对于不同的用户均可采用该第一公私钥对，如可依据上述RSA算法产生所有用户统一使用的第一私钥以及第一公钥。

[0090] 如上述判断信息单元400以及获取密码单元500所述，上述第一信息可为上述用

户资料内容中的任意一个属性，且事先和第一密码绑定，本实施例中，第一信息为姓名，则这时可判断解密出来的第一内容中是否包含有已经被绑定的姓名，若有，则说明当前请求登录的目标用户可能为上述客户端或者当前登录网站的真实用户，由于第一信息已与第一密码绑定，这时可依据第一信息在预设的资料库中获取第一密码。与现有技术中在此处获得第一信息即判定目标用户通过认证相比，本申请提供的认证装置还包括进一步验证签名，更加安全可靠。

[0091] 但是，若判断第一内容中不具有第一信息，则可直接判定目标用户未通过身份认证。具体的说，上述数字签名的认证装置，还包括：

[0092] 结束警示单元，用于判定所述第一内容中不具有所述第一信息时，生成结束认证指令，并发送认证失败的警示信息至所述客户端。

[0093] 本实施例中，当判定第一内容不具有第一信息，即表明上述目标用户可能不是上述客户端或者当前登录的网站的用户，或者可能是该目标用户没有事先认证绑定，所以无法进行免密登录，这时系统会生成结束认证的指令，依据该指令停止执行接下来的认证流程，同时发送认证失败的警示信息给用户。

[0094] 如上述对称加密单元600所述，上述对称加密可以通过AES算法进行计算，相对于DES算法而言，AES算法安全性更高，具体可使用第一密码对上述第一公钥以及第一私钥通过AES算法进行对称加密得到一对公私钥对，此处为了区别分别命名为第二公钥和第二私钥，由于AES算法为现有算法，此处不再赘述。

[0095] 如上述签名计算单元700所述，当获得第二公钥，这时可采用第二公钥对上述第一密文和第一内容通过签名算法计算，得到上述第二签名。上述签名算法可以为HMAC-SHA1签名算法，该算法为对一段信息进行生成签名摘要的算法，亦为现有算法，此处不再赘述。

[0096] 如上述判断匹配单元800以及判定认证单元900所述，当得到第二签名，则可以将第二签名和第一签名进行比较，判断两者是否匹配，若是，则说明当前请求登录的目标用户已事先进行了绑定认证，为该当前登录的真实用户，即用于生成第一签名以及第二签名的信息一致且生成方法也一致，这时可判定目标用户签名认证成功，若第一签名和第二签名不匹配，则说明获得到用户资料与预存的不匹配，该目标用户事先并没有绑定认证，这时可判定目标用户签名认证失

败。

[0097] 在一个实施例中，上述数字签名的认证装置，包括：

[0098] 获取资料单元，用于获取所述目标用户在客户端注册时输入的用户资料；

[0099] 绑定密码单元，用于将所述用户资料中的第一信息与所述第一密码进行绑定；

[0100] 加密密码单元，用于将所述第一密码对所述第一公钥以及第一私钥进行对称加密得到第二公钥和第二私钥；

[0101] 发送公钥单元，用于将所述第一公钥和第二公钥发送至目标用户的客户端，以便于所述客户端依据所述第二公钥对所述第一密文以及所述第一内容通过签名算法计算得到所述第一签名，其中，所述第一密文为所述客户端获取所述第一内容后，依据所述第一公钥对所述第一内容进行非对称加密得到的密文。

[0102] 在一个实施例中，上述绑定密码单元，包括：

[0103] 生成字符子单元，用于通过UUID生成器生成一串对应所述用户资料的预设位数的字符串；

[0104] 绑定信息子单元，用于将所述字符串记作所述第一密码，并将所述第一密码与所述目标用户的第一信息绑定。

[0105] 进一步地，上述生成字符子单元，包括：

[0106] 生成初符模块，用于通过UUID生成器生成指定位数的初始字符串；

[0107] 添加时间模块，用于在所述初始字符串的指定位置添加时间戳以得到所述预设位数的字符串。

[0108] 本实施例中，为了进一步提高安全性，可以在UUID生成器生成字符串的基础上进一步复杂化，先通过UUID生成器生成指定位数的初始字符串，然后在该初始字符串的指定位置添加时间戳，例如在初始字符串的起始位置或结束位置加上时间戳，得到上述预设位数的字符串。

[0109] 在一个实施例中，上述解密内容单元300，包括：

[0110] 解密密文单元，用于依据预设的第一私钥对所述第一密文进行解密得到解密内容，所述解密内容为多个预设格式的英文单词加汉字的组合,每个所述组合均为一个英文单词以及对应的汉字；

[0111] 字母排序单元，用于将所述解密内容中各个所述组合按所述组合的英文单词起

始字母的自然顺序进行排序，若所述起始字母一致，则按所述英文单词的第二个字母的自然顺序进行排序，以此类推，以得到所述第一内容。

[0112] 参照图3，本申请实施例中还提供一种计算机设备，该计算机设备可以是服务器，其内部结构可以如图3所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中，该计算机设计的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统、计算机可读指令和数据库。该内存器为非易失性存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机设备的数据库用于存储数字签名认证过程中所需的所有数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机可读指令被处理器执行时以实现一种数字签名的认证方法。

[0113] 上述处理器执行上述数字签名的认证方法的步骤：接收目标用户在客户端登录时发送的登录请求；从所述登录请求中获取第一密文以及第一签名；依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；若是，则依据所述第一信息在预设资料库中获取所述第一密码；将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；判断所述第一签名与所述第二签名是否匹配；若是，则判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[0114] 上述计算机设备，上述接收目标用户在客户端登录时发送的登录请求的步骤之前，包括：获取所述目标用户在客户端注册时输入的用户资料；将所述用户资料中的第一信息与所述第一密码进行绑定；将所述第一密码对所述第一公钥以及第一私钥进行对称加密得到所述第二公钥和所述第二私钥；将所述第一公钥和第二公钥发送至目标用户的客户端，以便于所述客户端依据所述第二公钥对所述第一密文以及所述第一内容通过签名算法计算得到所述第一签名，其中，

所述第一密文为所述客户端获取所述第一内容后，依据所述第一公钥对所述第一内容进行非对称加密得到的密文。

[0115] 在一个实施例中，上述将所述用户资料中的第一信息与所述第一密码进行绑定的步骤，包括：通过通用唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串；将所述字符串记作所述第一密码，并将所述第一密码与所述目标用户的第一信息进行绑定。

[0116] 在一个实施例中，上述通过通用唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串的步骤，包括：通过通用唯一识别码生成器生成指定位数的初始字符串；在所述初始字符串的指定位置添加时间戳以得到所述预设位数的字符串。

[0117] 在一个实施例中，上述依据预设的第一私钥对所述第一密文进行解密得到第一内容的步骤，包括：依据预设的第一私钥对所述第一密文进行解密得到解密内容，所述解密内容为多个预设格式的英文单词加汉字的组合,每个所述组合均为一个英文单词以及对应的汉字；将所述解密内容中各个所述组合按所述组合的英文单词起始字母的自然顺序进行排序，以得到所述第一内容。

[0118] 在一个实施例中，上述接收目标用户在客户端登录时发送的登录请求的步骤之前，包括：依据非对称加密算法算法产生所有用户统一使用的所述第一私钥以及所述第一公钥。

[0119] 在一个实施例中，上述判断所述第一内容中是否具有第一信息的步骤之后，包括：若判定所述第一内容中不具有所述第一信息，则生成结束认证指令，并发送认证失败的警示信息至所述客户端。

[0120] 本领域技术人员可以理解，图3中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定。

[0121] 本申请一实施例还提供一种计算机可读存储介质，所述计算机可读存储介质，例如为非易失性的计算机可读存储介质，或者为易失性的计算机可读存储介质，其上存储有计算机可读指令，计算机可读指令被处理器执行时实现一种数字签名的认证方法，具体为：接收目标用户在客户端登录时发送的登录请求；从所述登录请求中获取第一密文以及第一签名；依据预设的第一私钥对所述第一

密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；若是，则依据所述第一信息在预设资料库中获取所述第一密码；将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；判断所述第一签名与所述第二签名是否匹配；若是，则判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[0122] 上述计算机可读存储介质，上述接收目标用户在客户端登录时发送的登录请求的步骤之前，包括：获取所述目标用户在客户端注册时输入的用户资料；将所述用户资料中的第一信息与所述第一密码进行绑定；将所述第一密码对所述第一公钥以及第一私钥进行对称加密得到所述第二公钥和所述第二私钥；将所述第一公钥和第二公钥发送至目标用户的客户端，以便于所述客户端依据所述第二公钥对所述第一密文以及所述第一内容通过签名算法计算得到所述第一签名，其中，所述第一密文为所述客户端获取所述第一内容后，依据所述第一公钥对所述第一内容进行非对称加密得到的密文。

[0123] 在一个实施例中，上述将所述用户资料中的第一信息与所述第一密码进行绑定的步骤，包括：通过通用唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串；将所述字符串记作所述第一密码，并将所述第一密码与所述目标用户的第一信息进行绑定。

[0124] 在一个实施例中，上述通过通用唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串的步骤，包括：通过通用唯一识别码生成器生成指定位数的初始字符串；在所述初始字符串的指定位置添加时间戳以得到所述预设位数的字符串。

[0125] 在一个实施例中，上述依据预设的第一私钥对所述第一密文进行解密得到第一内容的步骤，包括：依据预设的第一私钥对所述第一密文进行解密得到解密内容，所述解密内容为多个预设格式的英文单词加汉字的组合,每个所述组合均为一个英文单词以及对应的汉字；将所述解密内容中各个所述组合按所述组合的

英文单词起始字母的自然顺序进行排序，以得到所述第一内容。

[0126] 在一个实施例中，上述接收目标用户在客户端登录时发送的登录请求的步骤之前，包括：依据非对称加密算法算法产生所有用户统一使用的所述第一私钥以及所述第一公钥。

[0127] 在一个实施例中，上述判断所述第一内容中是否具有第一信息的步骤之后，包括：若判定所述第一内容中不具有所述第一信息，则生成结束认证指令，并发送认证失败的警示信息至所述客户端。

[0128] 以上所述仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

权利要求书

[权利要求 1] 一种数字签名的认证方法，其特征在于，包括：

接收目标用户在客户端登录时发送的登录请求；

从所述登录请求中获取第一密文以及第一签名；

依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；

判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；

若是，则依据所述第一信息在预设资料库中获取所述第一密码；

将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；

依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；

判断所述第一签名与所述第二签名是否匹配；

若是，则判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[权利要求 2] 根据权利要求1所述的数字签名的认证方法，其特征在于，所述接收目标用户在客户端登录时发送的登录请求的步骤之前，包括：

获取所述目标用户在客户端注册时输入的用户资料；

将所述用户资料中的第一信息与所述第一密码进行绑定；

将所述第一密码对所述第一公钥以及第一私钥进行对称加密得到所述第二公钥和所述第二私钥；

将所述第一公钥和第二公钥发送至目标用户的客户端，以便于所述客户端依据所述第二公钥对所述第一密文以及所述第一内容通过签名算法计算得到所述第一签名，其中，所述第一密文为所述客户端获取所述第一内容后，依据所述第一公钥对所述第一内容进行非对称加密得到的密文。

[权利要求 3] 根据权利要求2所述的数字签名的认证方法，其特征在于，所述将所述用户资料中的第一信息与所述第一密码进行绑定的步骤，包括：

通过通用唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串；

将所述字符串记作所述第一密码，并将所述第一密码与所述目标用户的第一信息进行绑定。

[权利要求 4] 根据权利要求3所述的数字签名的认证方法，其特征在于，所述通过通用唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串的步骤，包括：

通过通用唯一识别码生成器生成指定位数的初始字符串；

在所述初始字符串的指定位置添加时间戳以得到所述预设位数的字符串。

[权利要求 5] 根据权利要求1所述的数字签名的认证方法，其特征在于，所述依据预设的第一私钥对所述第一密文进行解密得到第一内容的步骤，包括：

依据预设的第一私钥对所述第一密文进行解密得到解密内容，所述解密内容为多个预设格式的英文单词加汉字的组合,每个所述组合均为一个英文单词以及对应的汉字；

将所述解密内容中各个所述组合按所述组合的英文单词起始字母的自然顺序进行排序，以得到所述第一内容。

[权利要求 6] 根据权利要求5所述的数字签名的认证方法，其特征在于，所述将所述解密内容中各个所述组合按所述组合的英文单词起始字母的自然顺序进行排序，以得到所述第一内容的步骤，包括：

判断所述解密内容中各所述组合的英文单词起始字母是否均一致；

若不一致，则将各所述组合按所述组合的英文单词起始字母的自然顺序进行排序，若均一致，则将各所述组合按英文单词的第二个字母的自然顺序进行排序，若各所述组合的第二个字母一致，则按各所述组合的英文单词的第三个字母的自然顺序进行排序，以此类推，得到所

述第一内容。

[权利要求 7] 根据权利要求1所述的数字签名的认证方法，其特征在于，所述接收目标用户在客户端登录时发送的登录请求的步骤之前，包括：

依据非对称加密算法产生所有用户统一使用的所述第一私钥以及所述第一公钥。

[权利要求 8] 根据权利要求1所述的数字签名的认证方法，其特征在于，所述判断所述第一内容中是否具有第一信息的步骤之后，包括：

若判定所述第一内容中不具有所述第一信息，则生成结束认证指令，并发送认证失败的警示信息至所述客户端。

[权利要求 9] 一种数字签名的认证装置，其特征在于，包括：

接收请求单元，用于接收目标用户在客户端登录时发送的登录请求；

获取签名单元，用于从所述登录请求中获取第一密文以及第一签名；

解密内容单元，用于依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；

判断信息单元，用于判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；

获取密码单元，用于判定所述第一内容中具有第一信息时，依据所述第一信息在预设资料库中获取所述第一密码；

对称加密单元，用于将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；

签名计算单元，用于依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；

判断匹配单元，用于判断所述第一签名与所述第二签名是否匹配；

判定认证单元，用于判定所述第一签名与所述第二签名匹配时，判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[权利要求 10] 根据权利要求9所述的数字签名的认证装置，其特征在于，还包括：

获取资料单元，用于获取所述目标用户在客户端注册时输入的用户资料；

绑定密码单元，用于将所述用户资料中的第一信息与所述第一密码进行绑定；

加密密码单元，用于将所述第一密码对所述第一公钥以及第一私钥进行对称加密得到第二公钥和第二私钥；

发送公钥单元，用于将所述第一公钥和第二公钥发送至目标用户的客户端，以便于所述客户端依据所述第二公钥对所述第一密文以及所述第一内容通过签名算法计算得到所述第一签名，其中，所述第一密文为所述客户端获取所述第一内容后，依据所述第一公钥对所述第一内容进行非对称加密得到的密文。

[权利要求 11] 根据权利要求10所述的数字签名的认证装置，其特征在于，所述绑定密码单元包括：

生成字符子单元，用于通过唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串；

绑定信息子单元，用于将所述字符串记作所述第一密码，并将所述第一密码与所述目标用户的第一信息绑定。

[权利要求 12] 根据权利要求11所述的数字签名的认证装置，其特征在于，所述生成字符子单元包括：

生成初符模块，用于通过唯一识别码生成器生成指定位数的初始字符串；

添加时间模块，用于在所述初始字符串的指定位置添加时间戳以得到所述预设位数的字符串。

[权利要求 13] 根据权利要求9所述的数字签名的认证装置，其特征在于，所述解密内容单元，包括：

解密密文单元，用于依据预设的第一私钥对所述第一密文进行解密得到解密内容，所述解密内容为多个预设格式的英文单词加汉字的组合,每个所述组合均为一个英文单词以及对应的汉字；

字母排序单元，用于将所述解密内容中各个所述组合按所述组合的英文单词起始字母的自然顺序进行排序，若所述起始字母一致，则按所述英文单词的第二个字母的自然顺序进行排序，以此类推，以得到所述第一内容。

[权利要求 14] 一种计算机设备，包括存储器和处理器，所述存储器存储有计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现数字签名的认证方法，该数字签名的认证方法包括：

接收目标用户在客户端登录时发送的登录请求；

从所述登录请求中获取第一密文以及第一签名；

依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；

判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息；

若是，则依据所述第一信息在预设资料库中获取所述第一密码；

将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；

依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；

判断所述第一签名与所述第二签名是否匹配；

若是，则判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[权利要求 15] 根据权利要求14所述的数字签名的认证装置，其特征在于，所述接收目标用户在客户端登录时发送的登录请求的步骤之前，包括：

获取所述目标用户在客户端注册时输入的用户资料；

将所述用户资料中的第一信息与所述第一密码进行绑定；

将所述第一密码对所述第一公钥以及第一私钥进行对称加密得到所述第二公钥和所述第二私钥；

将所述第一公钥和第二公钥发送至目标用户的客户端，以便于所述客户端依据所述第二公钥对所述第一密文以及所述第一内容通过签名算法计算得到所述第一签名，其中，所述第一密文为所述客户端获取所述第一内容后，依据所述第一公钥对所述第一内容进行非对称加密得到的密文。

[权利要求 16] 根据权利要求15所述的数字签名的认证装置，其特征在于，所述将所述用户资料中的第一信息与所述第一密码进行绑定的步骤，包括：

通过通用唯一识别码生成器生成一串对应所述用户资料的预设位数的字符串；

将所述字符串记作所述第一密码，并将所述第一密码与所述目标用户的第一信息进行绑定。

[权利要求 17] 根据权利要求14所述的数字签名的认证装置，其特征在于，所述依据预设的第一私钥对所述第一密文进行解密得到第一内容的步骤，包括：

依据预设的第一私钥对所述第一密文进行解密得到解密内容，所述解密内容为多个预设格式的英文单词加汉字的组合,每个所述组合均为一个英文单词以及对应的汉字；

将所述解密内容中各个所述组合按所述组合的英文单词起始字母的自然顺序进行排序，以得到所述第一内容。

[权利要求 18] 一种计算机可读存储介质，其上存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现数字签名的认证方法，该数字签名的认证方法包括：

接收目标用户在客户端登录时发送的登录请求；

从所述登录请求中获取第一密文以及第一签名；

依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥；

判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用

户身份且与预设的第一密码绑定的信息；

若是，则依据所述第一信息在预设资料库中获取所述第一密码；

将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥；

依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名；

判断所述第一签名与所述第二签名是否匹配；

若是，则判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败。

[权利要求 19] 根据权利要求18所述的计算机可读存储介质，其特征在于，所述接收目标用户在客户端登录时发送的登录请求的步骤之前，包括：

获取所述目标用户在客户端注册时输入的用户资料；

将所述用户资料中的第一信息与所述第一密码进行绑定；

将所述第一密码对所述第一公钥以及第一私钥进行对称加密得到所述第二公钥和所述第二私钥；

将所述第一公钥和第二公钥发送至目标用户的客户端，以便于所述客户端依据所述第二公钥对所述第一密文以及所述第一内容通过签名算法计算得到所述第一签名，其中，所述第一密文为所述客户端获取所述第一内容后，依据所述第一公钥对所述第一内容进行非对称加密得到的密文。

[权利要求 20] 根据权利要求18所述的计算机可读存储介质，其特征在于，所述依据预设的第一私钥对所述第一密文进行解密得到第一内容的步骤，包括：

依据预设的第一私钥对所述第一密文进行解密得到解密内容，所述解密内容为多个预设格式的英文单词加汉字的组合,每个所述组合均为一个英文单词以及对应的汉字；

将所述解密内容中各个所述组合按所述组合的英文单词起始字母的自然顺序进行排序，以得到所述第一内容。

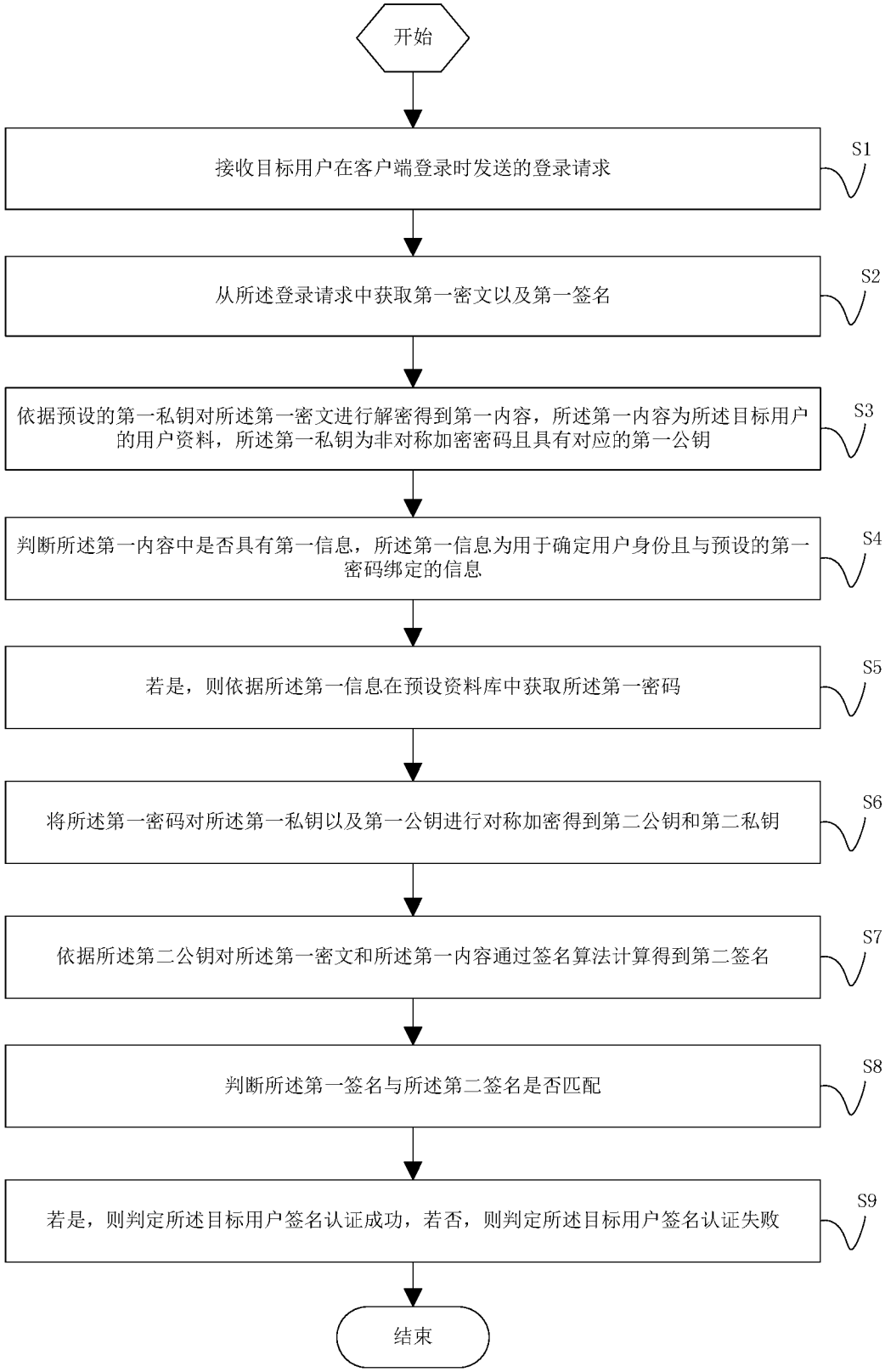
开始
接收目标用户在客户端登录时发送的登录请求
S1
从所述登录请求中获取第一密文以及第一签名
S2
依据预设的第一私钥对所述第一密文进行解密得到第一内容，所述第一内容为所述目标用户的用户资料，所述第一私钥为非对称加密密码且具有对应的第一公钥
S3
判断所述第一内容中是否具有第一信息，所述第一信息为用于确定用户身份且与预设的第一密码绑定的信息
S4
若是，则依据所述第一信息在预设资料库中获取所述第一密码
S5
将所述第一密码对所述第一私钥以及第一公钥进行对称加密得到第二公钥和第二私钥
S6
依据所述第二公钥对所述第一密文和所述第一内容通过签名算法计算得到第二签名
S7
判断所述第一签名与所述第二签名是否匹配
S8
若是，则判定所述目标用户签名认证成功，若否，则判定所述目标用户签名认证失败
S9
结束

图 1

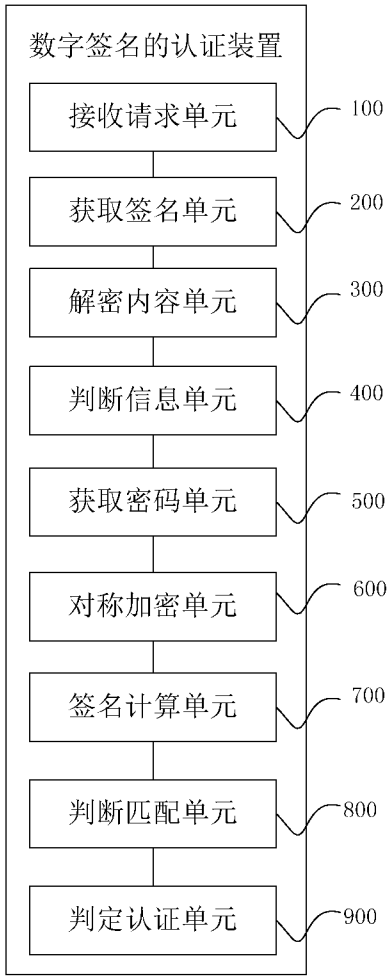
数字签名的认证装置
接收请求单元
100
获取签名单元
200
解密内容单元
300
判断信息单元
400
获取密码单元
500
对称加密单元
600
签名计算单元
700
判断匹配单元
800
判定认证单元
900

图 2

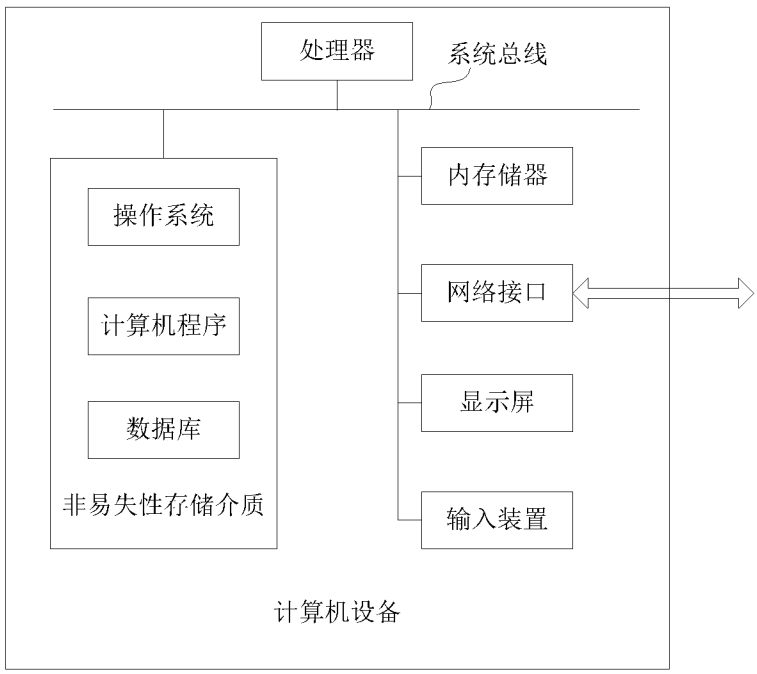
处理器
系统总线
内存储器
操作系统
网络接口
计算机程序
显示屏
数据库
输入装置
非易失性存储介质
计算机设备

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/118800

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)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: 签名, 登录, 请求, 加密, 解密, 密文, 用户, 信息, 内容, 密码, 公钥, 私钥, 比较, 匹配, 认证, 验证, sign, signature, login, request, encrypt, password, decrypt, user, information, content, public, private, match, compare, authenticate, identity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109756343 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 14 May 2019 (2019-05-14) claims 1-10, and description, paragraphs 51-150	1-20
Y	CN 107294937 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 24 October 2017 (2017-10-24) description, paragraphs 92-145	1-20
Y	CN 108650210 A (SHENZHEN VEB SAFETY CHIP TECHNOLOGY CO., LTD.) 12 October 2018 (2018-10-12) description, paragraphs 50-59	1-20
A	CN 101465735 A (PEKING UNIVERSITY et al.) 24 June 2009 (2009-06-24) entire document	1-20
A	CN 104394161 A (SHANGHAI ZHONGREN TECHNOLOGY CO., LTD.) 04 March 2015 (2015-03-04) entire document	1-20
A	WO 2018106063 A1 (SAMSUNG ELECTRONICS CO., LTD.) 14 June 2018 (2018-06-14) entire document	1-20

☐ 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
14 January 2020	**07 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/118800

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109756343 A	14 May 2019	None	
CN 107294937 A	24 October 2017	None	
CN 108650210 A	12 October 2018	None	
CN 101465735 A	24 June 2009	None	
CN 104394161 A	04 March 2015	None	
WO 2018106063 A1	14 June 2018	EP 3535920 A1	11 September 2019
		AU 2017373540 A1	18 July 2019
		CN 110063039 A	26 July 2019
		MX 2019006695 A	21 August 2019
		CA 3046451 A1	14 June 2018
		US 2018167931 A1	14 June 2018
		US 2018167932 A1	14 June 2018
		KR 20190095328 A	14 August 2019

国际检索报告

国际申请号
PCT/CN2019/118800

A. 主题的分类

H04L 9/32(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

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, EPODOC: 签名，登录，请求，加密，解密，密文，用户，信息，内容，密码，公钥，私钥，比较，匹配，认证，验证，sign, signature, login, request, encrypt, password, decrypt, user, information, content, public, private, match, compare, authenticate, identity

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 109756343 A (平安科技深圳有限公司) 2019年 5月 14日 (2019-05-14) 权利要求1-10，说明书第51-150段	1-20
Y	CN 107294937 A (平安科技深圳有限公司) 2017年 10月 24日 (2017-10-24) 说明书第92-145段	1-20
Y	CN 108650210 A (深圳市中易通安全芯科技有限公司) 2018年 10月 12日 (2018-10-12) 说明书第50-59段	1-20
A	CN 101465735 A (北京大学 等) 2009年 6月 24日 (2009-06-24) 全文	1-20
A	CN 104394161 A (上海众人科技有限公司) 2015年 3月 4日 (2015-03-04) 全文	1-20
A	WO 2018106063 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2018年 6月 14日 (2018-06-14) 全文	1-20

☐ 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
2020年 1月 14日	2020年 2月 7日
ISA/CN的名称和邮寄地址 中国国家知识产权局(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 李晓利 电话号码 86-(10)-53961772

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/118800

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	109756343	A	2019年 5月 14日	无			
CN	107294937	A	2017年 10月 24日	无			
CN	108650210	A	2018年 10月 12日	无			
CN	101465735	A	2009年 6月 24日	无			
CN	104394161	A	2015年 3月 4日	无			
WO	2018106063	A1	2018年 6月 14日	EP	3535920	A1	2019年 9月 11日
				AU	2017373540	A1	2019年 7月 18日
				CN	110063039	A	2019年 7月 26日
				MX	2019006695	A	2019年 8月 21日
				CA	3046451	A1	2018年 6月 14日
				US	2018167931	A1	2018年 6月 14日
				US	2018167932	A1	2018年 6月 14日
				KR	20190095328	A	2019年 8月 14日