

(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
2019 年 6 月 20 日 (20.06.2019)



(10) 国际公布号
WO 2019/114122 A1

(51) 国际专利分类号:
H04L 9/06 (2006.01) **H04L 29/06** (2006.01)
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2018/074868

(22) 国际申请日: 2018 年 1 月 31 日 (31.01.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201711339852.3 2017 年 12 月 14 日 (14.12.2017) 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八卦岭八卦三路平安大厦 6 楼, Guangdong 518000 (CN)。

(72) 发明人: 刘继超(LIU, Jichao); 中国广东省深圳市福田区八卦岭八卦三路平安大厦 6 楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳中一专利商标事务所(SHENZHEN ZHONGYI PATENT AND TRADEMARK OFFICE);
中国广东省深圳市福田区深南中路 1014 号老特区报社四楼 (5 号信箱), Guangdong 518028 (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, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) Title: ENCRYPTION METHOD FOR LOGIN INFORMATION, DEVICE, ELECTRONIC DEVICE, AND MEDIUM

(54) 发明名称: 登录信息的加密方法、装置、电子设备及介质

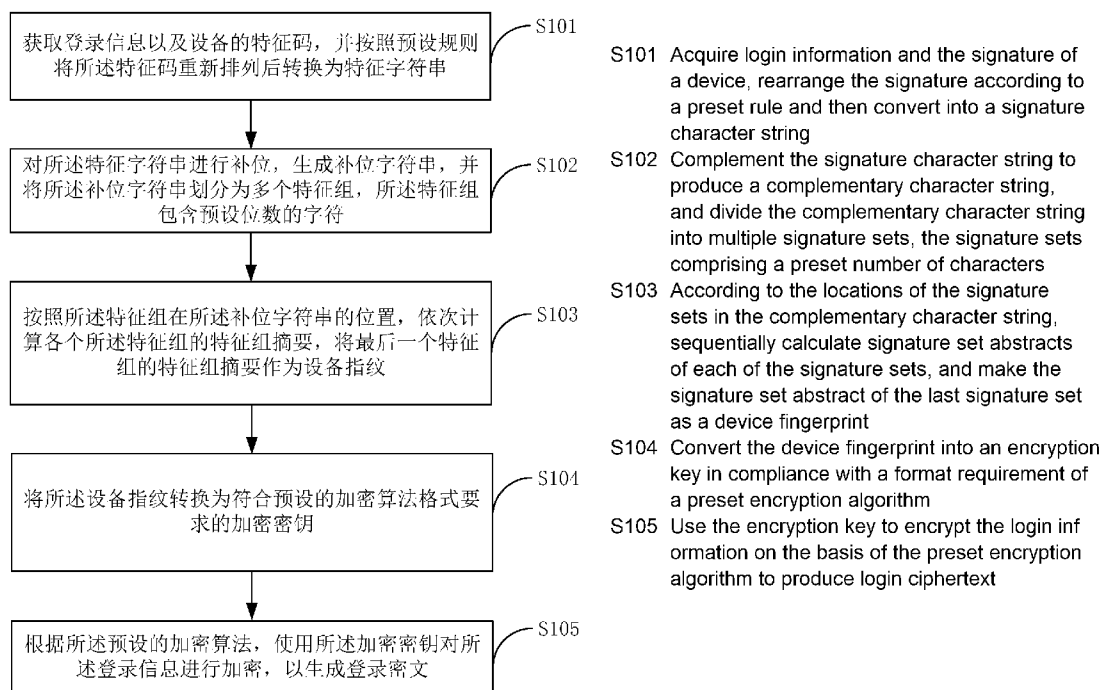


图 1

(57) Abstract: The present solution is applicable in the technical field of the internet. Provided are an encryption method for login information, a device, an electronic device, and a medium. The signature of a device is acquired, the signature is rearranged according to a preset rule and then converted into a signature character string, the signature character string is complemented to produce a complementary character string, according to the locations of signature sets in the complementary character string, signature set abstracts of the signature sets are sequentially calculated, the signature set abstract of the last signature set is made as a device fingerprint, the

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))。

device fingerprint is converted into an encryption key applicable in encryption, and the encryption key produced on the basis of the device fingerprint is used per a preset encryption algorithm in the encryption of login information, thus producing login ciphertext. This allows different devices to be provided with encryption keys different from that of other devices and prevents the login ciphertext from being decrypted even if the encryption algorithm and the login ciphertext are acquired by someone else, thus better ensuring that login information of a user is not fraudulently used by others.

(57) 摘要: 本方案适用于互联网技术领域, 提供了一种登录信息的加密方法、装置、电子设备及介质, 通过获取设备的特征码, 按照预设规则将所述特征码重新排列后转换为特征字符串, 对所述特征字符串进行补位, 生成补位字符串, 按照特征组在补位字符串的位置, 依次计算各个特征组的特征组摘要, 将最后一个特征组的特征组摘要作为设备指纹, 将所述设备指纹转换为可用于进行加密的加密密钥, 通过预设的加密算法使用根据设备指纹得到的加密密钥对登录信息进行加密, 生成登录密文, 使得不同的设备具有区别于其他设备的加密密钥, 他人即使获取了加密算法以及登录密文, 也无法对登录密文进行解密, 可以更好地保证用户的登录信息不被他人盗用。

登录信息的加密方法、装置、电子设备及介质

[0001] 本申请要求于2017年12月14日提交中国专利局、申请号为201711339852.3、发明名称为“登录信息的加密方法及终端设备”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] 本申请属于数据处理技术领域，尤其涉及一种登录信息的加密方法、装置、电子设备及介质。

背景技术

[0003] 目前，人们在使用互联网时经常需要输入登录信息，这些登录信息一般包括登录名和密码，当用户输入的登录信息与服务器中预先存储的数据相匹配时，用户就可以远程使用该登录信息对应的权限和数据。现有技术中，为了登录方便，用户往往会选择“下次自动登录”的方式，此时用户名和密码将作为登录信息被加密后保存在本地设备中，当用户下次再需要登录时，只需调用本地存储的登录信息就可以自动登录。

[0004] 但是当前用于为登录信息加密的加密密钥是硬编码的，通过EditPlus等文本编辑器打开软件就可以看到固定的加密密钥，而且由于加密密钥是硬编码的，因此与设备无关，当黑客截获了登录信息的密文之后，可以在其他设备直接使用登录信息的密文以被盗用户的身份登录，因此当前登录信息的加密方法安全性较低。

发明概述

技术问题

[0005] 本申请提供了一种登录信息的加密方法、装置、电子设备及介质，以解决现有技术在登录信息的加密和保存过程中存在的安全性差的问题。

问题的解决方案

技术解决方案

[0006] 本申请实施例的第一方面提供了一种登录信息的加密方法，包括：

[0007] 获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串；对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符；按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹；将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥；根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。

[0008] 本申请实施例的第二方面提供了一种登录信息的加密装置，包括：

[0009] 获取单元，用于获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串。分组单元，用于对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符。摘要计算单元，用于按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹。密钥生成单元，用于将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥。加密单元，用于根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。

[0010] 本申请实施例的第三方面提供了一种登录信息的加密电子设备，包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

[0011] 获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串；对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符；

[0012] 按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹；将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥；根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。

[0013] 本申请实施例的第四方面提供了一种计算机可读存储介质，所述计算机可读存储介质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至少一个

处理器执行时实现如下步骤:

- [0014] 获取登录信息以及设备的特征码, 并按照预设规则将所述特征码重新排列后转换为特征字符串; 对所述特征字符串进行补位, 生成补位字符串, 并将所述补位字符串划分为多个特征组, 所述特征组包含预设位数的字符; 按照所述特征组在所述补位字符串的位置, 依次计算各个所述特征组的特征组摘要, 将最后一个特征组的特征组摘要作为设备指纹; 将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥; 根据所述预设的加密算法, 使用所述加密密钥对所述登录信息进行加密, 以生成登录密文。

发明的有益效果

有益效果

- [0015] 本申请通过获取设备的特征码, 按照预设规则将所述特征码重新排列后转换为特征字符串, 对所述特征字符串进行补位, 生成补位字符串, 按照特征组在补位字符串的位置, 依次计算各个特征组的特征组摘要, 将最后一个特征组的特征组摘要作为设备指纹, 将所述设备指纹转换为可用于进行加密的加密密钥, 通过预设的加密算法使用根据设备指纹得到的加密密钥对登录信息进行加密, 生成登录密文, 使得不同的设备具有区别于其他设备的加密密钥, 他人即使获取了加密算法以及登录密文, 也无法对登录密文进行解密, 可以更好地保证用户的登录信息不被他人盗用。

对附图的简要说明

附图说明

- [0016] 为了更清楚地说明本申请实施例中的技术方案, 下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍, 显而易见地, 下面描述中的附图仅仅是本申请的一些实施例, 对于本领域普通技术人员来讲, 在不付出创造性劳动性的前提下, 还可以根据这些附图获得其他的附图。
- [0017] 图1是本申请提供的登录信息的加密方法的实现流程图;
- [0018] 图2是本申请提供的登录信息的加密方法S103的具体实现流程图;
- [0019] 图3是本申请提供的登录信息的加密方法S1034的具体实现流程图;
- [0020] 图4是本申请提供的登录信息的加密装置的结构框图;

[0021] 图5是本申请提供的终端设备的示意图。

发明实施例

本发明的实施方式

[0022] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0023] 为了说明本申请所述的技术方案，下面通过具体实施例来进行说明。

[0024] 图1示出了本申请提供的登录信息的加密方法的实现流程，该方法流程包括步骤S101至S105。各步骤的具体实现原理如下。

[0025] S101：获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串。

[0026] 在本申请中，当用户为了方便下次自动登录而选择将用户名和密码保存在设备后，登录信息的加密装置就获取了用户的登录信息，可以理解地，用户的登录信息包括用户名和密码。在本申请中，除了获取登录信息外还需要获取设备的特征码。可以理解地，目前人们使用的终端设备都有其唯一的特征码，例如，特征码可以为主板、CPU、硬盘或网卡等物理元器件的唯一识别码，也可以是操作系统的序列号。示例性地，在本申请中将CPU识别码作为设备的特征码，如果CPU识别码为BFEBFBFF000206A，则设备的特征码就是BFEBFBFF000206A。

[0027] 可选地，为了提高安全性，在获取了设备的特征码后还需要按照预设规则将特征码重新排列，例如：预设规则为：将特征码的第一位与第六位调换；第二位与第七位调换。可以理解地，上文示例中的特征码BFEBFBFF000206A在经过预设规则重新排列后变为BFEBFBFF6A02000。可以理解地，在本申请中对特征码进行重新排列组合的目的是让黑客无法直接通过截获CPU识别码，而推算出后续计算中的设备指纹。在本申请中，由于不同的设备的特征码的进制可能不同，因此在将特征码按照预设规则将所述特征码重新排列后转换为预设进制的特征字符串，可选地，特征字符串为二进制字符串。示例性地，上文示例中的特征

码BFEBFBFF000206A按照预设规则重新排列后转换为二进制的特征字符串10111111110101111111011111111101101010000000100000000000000。

[0028] 在本申请中，通过对设备的特征码的重新排列组合提高了整个加密算法的安全性，同时对特征码的转换使得特征码更适于后续的加密计算。

[0029] S102：对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符。

[0030] 在本申请中，由于为了满足安全性的需要，用于计算设备指纹的字符串要求比较长，通过特征码直接转换而来的特征码字符串的长度不能满足要求，所以需要特征字符串进行补位，生成满足后续计算要求的补位字符串。

[0031] 可选地，所述对所述字符串进行补位，包括：在所述特征字符串的末位增加字符1后继续增加一个以上的字符0，直至所述特征字符串在补位后的位数除以第一预设数字后的余数等于第二预设数字。

[0032] 示例性地，可以将所述第一预设数字设定为512，将所述第二预设数字设定为448，由于原特征字符串的长度可以通过64位字符串表示，所以经过补位后的补位字符串正好为第一预设数字的整数倍。

[0033] 在本申请中，将补位字符串划分为多个特征组，可以理解地，每个特征组包含的字符个数为第一预设数字。

[0034] S103：按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹。

[0035] 可以理解地，如果直接使用未经加密的补位字符串作为设备指纹以进行后续对登录信息的加密是有安全隐患的，因此本申请提出了一种算法以计算补位字符串的摘要，并将所述字符串的摘要作为设备指纹，使得黑客即使获取了设备的特征码，也难以确定设备指纹。

[0036] 作为本申请的一个实施例，如图2所示，上述S103包括：

[0037] S1031：按照所述特征组在所述补位字符串的位置，确定对所述特征组的计算顺序。

[0038] 可选地，如上文所述，一个补位字符串可以被划分为多个特征组，在本申请中，从补位字符串的最左侧开始，将每预设个数的字符作为一个特征组。在本申

请中，对所述特征组的计算顺序为：根据特征组在所述补位字符串的位置，从左至右依次计算各个特征组的特征组摘要，具体计算每一个特征组的特征组摘要的方法将在下文详述。

[0039] S1032：获取预设摘要，并将所述预设摘要作为首个特征组的初始摘要，所述首个特征组为根据所述计算顺序被第一个计算的特征组。

[0040] 在本申请中，算法的输入参数有两个，一个是特征组包含的字符串，另一个是特征组对应的初始摘要，其中，首个特征组的初始摘要为一个预设的摘要。

[0041] S1033：将所述首个特征组以及所述首个特征组的初始摘要作为输入值，计算出所述首个特征组的特征组摘要。

[0042] 具体计算特征组的特征组摘要的方法将在下文详述

[0043] S1034：根据所述计算顺序，将上一个特征组的特征组摘要作为下一个特征组的初始摘要；对各个特征组依次执行将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征组的特征组摘要的操作，直至计算出最后一个特征组的特征组摘要，并将所述最后一个特征组的特征组摘要作为设备指纹。

[0044] 在本申请中，通过对各个特征组依次执行预设的摘要计算，他人即使获取了设备的特征码，也难以破解设备指纹。

[0045] 作为本申请的一个实施例，图3示出了本申请提供的登录信息的加密方法S1034的具体实现流程，详述如下：

[0046] S10341：将所述特征组分成M个特征子组，根据预设的扩展规则将所述M个所述特征子组扩展为N个特征子组，并分别为所述N个特征子组编号。

[0047] 值得注意地，所述M为大于1的整数，所述N为大于M的整数。可以理解地，在本申请中，每个特征子组都是由若干个二进制的字符串组成的。可选地，将M个特征子组扩展为N个特征子组的扩展规则可以为：假设特征子组的编号为t，扩展前每个特征子组用 $X(t)$ 表示，扩展后的每个特征子组用 $Y(t)$ 表示，当t小于等于M时， $X(t) = Y(t)$ ；当t大于M时， $Y(t) = X(t-1) \oplus X(t-3) \oplus X(t-10) \oplus X(t-14)$ 。其中，“ $\oplus$ ”为“异或”运算符。

[0048] 值得注意地，上述扩展规则仅为一个示例，其他的基于原特征子组的扩展规则都可以用于扩展特征子组，由于本申请的一个目的是通过设备的特征码生成一

个动态的加密密钥，因此设备指纹也可以是动态的，所以N的值以及扩展规则都可以改变。

[0049] S10342: 将所述特征组的所述初始摘要按照排列顺序分为L个初始摘要组，并分别为所述初始摘要组编号。

[0050] 值得注意地，所述L为大于1的整数。可选地，在本申请中，将一个完整的初始摘要分为5个初始摘要组，并为各个初始摘要组编号，生成第一初始摘要组、第二初始摘要组、第三初始摘要组、第四初始摘要组以及第五初始摘要组。可以理解地，用户可以根据实际情况调整初始摘要组的数量。

[0051] S10343: 设置所述L个缓存组，并分别为所述缓存组编号。

[0052] 在本申请中，由于后续要进行赋值和移位计算，因此需要设置与初始摘要组数量相同的缓存组。示例性地，若初始摘要组的数量是5个，则设置5个缓存组，并为各个缓存组编号，生成第一缓存组、第二缓存组、第三缓存组、第四缓存组以及第五缓存组。

[0053] S10344: 判断移位赋值计算的轮次是否小于N。

[0054] 在本申请中，首先需要将L个初始摘要组分别存入编号相同的缓存组内，并通过移位赋值计算方法对缓存组中的数据反复计算N轮。值得注意的，在本申请中，对缓存组中的数据反复计算的轮次数等于扩展后的特征子组的数量，以保证在后续赋值计算过程中的相关步骤可以顺利进行。在本申请中，移位赋值计算的轮次的初始值为1，即进行第一次移位赋值计算时，移位赋值计算的轮次为1。

[0055] S10345: 若移位赋值计算的轮次小于N，则进行新一轮执行移位赋值计算，所述移位赋值计算包括：在将各个缓存组的数据移位存入后一个缓存组内后，将当前的首个缓存组的数据加上对应的特征子组的数据，作为新的所述首个缓存组的数据以更新所述首个缓存组，将所述移位赋值计算的轮次加1，并返回至S10344。

[0056] 示例性地，假设当前的各个缓存组内数据分别为：第一缓存组：1001010₁₀；第二缓存组：1000111；第三缓存组：1010101；第四缓存组：1000001；第五缓存组：1000000，其中第一缓存组就是本申请中的第二缓存组首个缓存组，缓存组

的排列顺序依次为第一缓存组、第二缓存组、第三缓存组、第四缓存组、第五缓存组。通过将各个缓存组的数据移位存入后一个缓存组内，可以得到更新后的各个缓存组内数据分别为：第二缓存组：1001010；第三缓存组：1001111；

[0057] 第四缓存组：1010101；第五缓存组：1000001。假设当前移位赋值计算的轮次为6，即移位赋值计算已经进行到第6轮，则需要将第一缓存组（首个缓存组）的数据与编号为6的特征子组相加求和，作为新的第一缓存组（首个缓存组）的数据。如果编号为6的特征子组为：1110，则更新后的第一缓存组（首个缓存组）的数据为：1001010+1110=0101100。在本申请中，当完成次轮移位赋值计算后，将所述移位赋值计算的轮次加1，并返回至S10344继续判断。

[0058] S10346：若移位赋值计算的轮次不小于N，则将各个缓存组内数据组合，作为所述特征组的特征组摘要。

[0059] 示例性地，假设经过N轮移位赋值计算后的各个缓存组内数据为：第一缓存组：1001011；第二缓存组：1010111；第三缓存组：1011101；第四缓存组：1000111；第五缓存组：1000100，则所述特征组的特征组摘要为将五个缓存组按排列顺序组合起来的数据，即：10010111010111101110110001111000100。

[0060] 在本申请中，通过循环执行多次移位赋值计算快速有效的计算出一个特征组的特征组摘要，再结合S1034所述，将上一个特征组的特征组摘要作为下一个特征组的初始摘要；对各个特征组依次执行移位赋值计算的操作，直至计算出最后一个特征组的特征组摘要，并将所述最后一个特征组的特征组摘要作为设备指纹。

[0061] S104：将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥。

[0062] 可以理解地，由于本申请提供的加密方法，从获取设备的特征码到生成登录信息的密文，存在一次计算摘要的过程和一个加密的过程。计算摘要的过程是根据设备的特征码生成设备指纹，加密的过程是根据加密密钥对登录信息进行加密生成登录信息的密文。由于计算摘要的过程与加密的过程使用的算法不同，因此设备指纹可能无法直接作为加密的加密密钥，因此需要对设备指纹进行转换。具体地，调取预设的对应关系，所述对应关系包括加密算法与加密密钥格式的对对应关系，并根据所述对应关系分析出在后续第二次加密过程中待使用的

加密算法对应的加密密钥格式。并将设备指纹通过补位以及数位进制转换等方式，将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥。本申请可以通过设备指纹转换出后续加密过程中的加密密钥，由于设备指纹是根据不同的设备的特征码而动态确定的，所以并不是一个固定的硬编码，所以他人难以破解出加密密钥。

[0063] S105：根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。

[0064] 在本申请中，由于加密密钥是根据预设的加密算法与加密密钥格式的对应关系从设备指纹转换而来的，所以根据上述步骤生成的加密密钥可以直接应用在预设的加密算法中，将登录信息作为预设的加密算法的输入值，通过预设的加密算法就可以计算出登录密文。具体地，将所述登录信息转换为明文矩阵。可选地，在本申请中，由于登录信息包括登录名和密码，所以登录信息可能包含十进制数字、字母以及汉字，其中，十进制数字可以直接转换成二进制字符串；字母可以根据ASCII码转换成二进制字符串；汉字可以根据UTF-8编码转换成二进制字符串。通过上述的转换方法，登录信息可以被转换为一组二进制字符串，随后将这组二进制字符串按顺序排列成一个预设列数的矩阵作为明文矩阵，并将所述明文矩阵最后一行补入若干个0以补齐明文矩阵的最后一行。

[0065] 具体地，将所述明文矩阵进行行移位操作、列混淆操作以及通过所述加密密钥进行轮密钥加操作，生成登录密文。可选地，可以根据AES加密算法对所述明文矩阵进行移位操作、列混淆操作以及轮密钥加操作，AES加密算法的输出结果就是登录密文。在本申请中，将登录密文存储在设备的存储器中，待下次用户需要登录时，对登录密文进行解密，以获取登录名和密码。

[0066] 在本申请中，通过获取设备的特征码，按照预设规则将所述特征码重新排列后转换为特征字符串，对所述特征字符串进行补位，生成补位字符串，按照特征组在补位字符串的位置，依次计算各个特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹，将所述设备指纹转换为可用于进行加密的加密密钥，通过预设的加密算法使用根据设备指纹得到的加密密钥对登录信息进行加密，生成登录密文，使得不同的设备具有区别于其他设备的加密密钥，他人

即使获取了加密算法以及登录密文，也无法对登录密文进行解密，可以更好地保证用户的登录信息不被他人盗用。

[0067] 对应于上文实施例所述的登录信息的加密方法，图4示出了本申请提供的登录信息的加密装置的结构框图，为了便于说明，仅示出了与本申请相关的部分。

[0068] 参照图4，该装置包括：

[0069] 获取单元401，用于获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串。分组单元402，用于对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符。摘要计算单元403，用于按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹。密钥生成单元404，用于将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥。加密单元405，用于根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。

[0070] 可选地，所述分组单元402包括：

[0071] 补位子单元，用于在所述特征字符串的末位增加字符1后继续增加一个以上的字符0，直至所述特征字符串在补位后的位数除以第一预设数字后的余数等于第二预设数字。

[0072] 可选地，所述摘要计算单元403包括：

[0073] 顺序确定子单元，用于按照所述特征组在所述补位字符串的位置，确定对所述特征组的计算顺序。摘要获取子单元，用于获取预设摘要，并将所述预设摘要作为首个特征组的初始摘要，所述首个特征组为根据所述计算顺序被第一个计算的特征组。第一摘要计算子单元，用于将所述首个特征组以及所述首个特征组的初始摘要作为输入值，计算出所述首个特征组的特征组摘要。第二摘要计算子单元，用于根据所述计算顺序，将上一个特征组的特征组摘要作为下一个特征组的初始摘要。对各个特征组依次执行将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征组的特征组摘要的操作，直至计算出最后一个特征组的特征组摘要，并将所述最后一个特征组的特征组摘要作为设备指纹。

[0074] 可选地，所述第二摘要计算子单元具体用于：

[0075] 将所述特征组分成M个特征子组，根据预设的扩展规则将所述M个特征子组扩展为N个特征子组，并分别为所述N个特征子组编号，所述M为大于1的整数，所述N为大于M的整数。将所述特征组的所述初始摘要按照排列顺序分为L个初始摘要组，并分别为所述初始摘要组编号，所述L为大于1的整数。设置所述L个缓存组，并分别为所述缓存组编号。将各个所述初始摘要组的数据分别存入编号相同的所述缓存组中，循环执行N轮移位赋值计算，所述移位赋值计算包括：在将各个缓存组的数据移位存入后一个缓存组内后，将当前的首个缓存组的数据加上对应的特征子组的数据，作为新的所述首个缓存组的数据以更新所述首个缓存组，所述对应的特征子组的编号与当前所述移位赋值计算的轮次相同。将经过N轮移位赋值计算后的各个缓存组内数据组合，作为所述特征组的特征组摘要。

[0076] 可选地，所述加密单元405包括：

[0077] 矩阵生成子单元，用于将所述登录信息转换为明文矩阵。加密操作子单元，用于将所述明文矩阵进行行移位操作、列混淆操作以及通过所述加密密钥进行轮密钥加操作，生成登录密文。在本申请中，通过获取设备的特征码，按照预设规则将所述特征码重新排列后转换为特征字符串，对所述特征字符串进行补位，生成补位字符串，按照特征组在补位字符串的位置，依次计算各个特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹，将所述设备指纹转换为可用于进行加密的加密密钥，通过预设的加密算法使用根据设备指纹得到的加密密钥对登录信息进行加密，生成登录密文，使得不同的设备具有区别于其他设备的加密密钥，他人即使获取了加密算法以及登录密文，也无法对登录密文进行解密，可以更好地保证用户的登录信息不被他人盗用。

[0078] 图5是本申请一实施例提供的电子设备的示意图。如图5所示，该实施例的电子设备5包括：处理器50、存储器51以及存储在所述存储器51中并可在所述处理器50上运行的计算机可读指令52，例如登录信息的加密程序。所述处理器50执行所述计算机可读指令52时实现上述各个登录信息的加密方法实施例中的步骤，例如图1所示的步骤101至105。或者，所述处理器50执行所述计算机可读指令52

时实现上述各装置实施例中各模块/单元的功能，例如图4所示单元401至405的功能。

[0079] 示例性的，所述计算机可读指令52可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器51中，并由所述处理器50执行，以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机可读指令指令段，该指令段用于描述所述计算机可读指令52在所述电子设备5中的执行过程。

[0080] 所述电子设备5可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述电子设备可包括，但不仅限于，处理器50、存储器51。本领域技术人员可以理解，图5仅仅是电子设备5的示例，并不构成对电子设备5的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述电子设备还可以包括输入输出设备、网络接入设备、总线等。

[0081] 以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权利要求书

- [权利要求 1] 一种登录信息的加密方法，其特征在于，包括：
- 获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串；
- 对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符；
- 按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹；
- 将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥；
- 根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。
- [权利要求 2] 如权利要求1所述的登录信息的加密方法，其特征在于，所述对所述字符串进行补位，包括：
- 在所述特征字符串的末位增加字符1后继续增加一个以上的字符0，直至所述特征字符串在补位后的位数除以第一预设数字后的余数等于第二预设数字。
- [权利要求 3] 如权利要求1所述的登录信息的加密方法，其特征在于，所述按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹，包括：
- 按照所述特征组在所述补位字符串的位置，确定对所述特征组的计算顺序；
- 获取预设摘要，并将所述预设摘要作为首个特征组的初始摘要，所述首个特征组为根据所述计算顺序被第一个计算的特征组；
- 将所述首个特征组以及所述首个特征组的初始摘要作为输入值，计算出所述首个特征组的特征组摘要；
- 根据所述计算顺序，将上一个特征组的特征组摘要作为下一个特征组的初始摘要；对各个特征组依次执行将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征组的特征组摘要的操作，直至

计算出最后一个特征组的特征组摘要，并将所述最后一个特征组的特征组摘要作为设备指纹。

[权利要求 4] 如权利要求3所述的登录信息的加密方法，其特征在于，所述将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征组的特征组摘要，包括：

将所述特征组分成M个特征子组，根据预设的扩展规则将所述M个特征子组扩展为N个特征子组，并分别为所述N个特征子组编号，所述M为大于1的整数，所述N为大于M的整数；

将所述特征组的所述初始摘要按照排列顺序分为L个初始摘要组，并分别为所述初始摘要组编号，所述L为大于1的整数；

设置所述L个缓存组，并分别为所述缓存组编号；

将各个所述初始摘要组的数据分别存入编号相同的所述缓存组中，循环执行N轮移位赋值计算，所述移位赋值计算包括：在将各个缓存组的数据移位存入后一个缓存组内后，将当前的首个缓存组的数据加上对应的特征子组的数据，作为新的所述首个缓存组的数据以更新所述首个缓存组，所述对应的特征子组的编号与当前所述移位赋值计算的轮次相同；

将经过N轮移位赋值计算后的各个缓存组内数据组合，作为所述特征组的特征组摘要。

[权利要求 5] 如权利要求1所述的登录信息的加密方法，其特征在于，所述根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文，包括：

将所述登录信息转换为明文矩阵；

将所述明文矩阵进行行移位操作、列混淆操作以及通过所述加密密钥进行轮密钥加操作，生成登录密文。

[权利要求 6] 一种登录信息的加密装置，其特征在于，包括：

获取单元，用于获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串。

分组单元，用于对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符。

摘要计算单元，用于按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹。

密钥生成单元，用于将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥。

加密单元，用于根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。

[权利要求 7] 如权利要求6所述的登录信息的加密装置，其特征在于，所述分组单元包括：

补位子单元，用于在所述特征字符串的末位增加字符1后继续增加一个以上的字符0，直至所述特征字符串在补位后的位数除以第一预设数字后的余数等于第二预设数字。

[权利要求 8] 如权利要求6所述的登录信息的加密装置，其特征在于，所述摘要计算单元包括：

顺序确定子单元，用于按照所述特征组在所述补位字符串的位置，确定对所述特征组的计算顺序。

摘要获取子单元，用于获取预设摘要，并将所述预设摘要作为首个特征组的初始摘要，所述首个特征组为根据所述计算顺序被第一个计算的特征组。

第一摘要计算子单元，用于将所述首个特征组以及所述首个特征组的初始摘要作为输入值，计算出所述首个特征组的特征组摘要。

第二摘要计算子单元，用于根据所述计算顺序，将上一个特征组的特征组摘要作为下一个特征组的初始摘要。对各个特征组依次执行将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征组的特征组摘要的操作，直至计算出最后一个特征组的特征组摘要，并

将所述最后一个特征组的特征组摘要作为设备指纹。

[权利要求 9]

如权利要求8所述的登录信息的加密装置，其特征在于，所述第二摘要计算子单元具体用于：

将所述特征组分成M个特征子组，根据预设的扩展规则将所述M个特征子组扩展为N个特征子组，并分别为所述N个特征子组编号，所述M为大于1的整数，所述N为大于M的整数。

将所述特征组的所述初始摘要按照排列顺序分为L个初始摘要组，并分别为所述初始摘要组编号，所述L为大于1的整数。

设置所述L个缓存组，并分别为所述缓存组编号。

将各个所述初始摘要组的数据分别存入编号相同的所述缓存组中，循环执行N轮移位赋值计算，所述移位赋值计算包括：在将各个缓存组的数据移位存入后一个缓存组内后，将当前的首个缓存组的数据加上对应的特征子组的数据，作为新的所述首个缓存组的数据以更新所述首个缓存组，所述对应的特征子组的编号与当前所述移位赋值计算的轮次相同。

将经过N轮移位赋值计算后的各个缓存组内数据组合，作为所述特征组的特征组摘要。

[权利要求 10]

如权利要求6所述的登录信息的加密装置，其特征在于，所述加密单元包括：

矩阵生成子单元，用于将所述登录信息转换为明文矩阵。

加密操作子单元，用于将所述明文矩阵进行行移位操作、列混淆操作以及通过所述加密密钥进行轮密钥加操作，生成登录密文。

[权利要求 11]

一种登录信息的加密电子设备，其特征在于，所述登录信息的加密处理电子设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串；

对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符；
按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹；
将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥；
根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。

[权利要求 12] 如权利要求11所述的登录信息的加密电子设备，其特征在于，所述对所述字符串进行补位，包括：

在所述特征字符串的末位增加字符1后继续增加一个以上的字符0，直至所述特征字符串在补位后的位数除以第一预设数字后的余数等于第二预设数字。

[权利要求 13] 如权利要求11所述的登录信息的加密电子设备，其特征在于，所述按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹，包括：
按照所述特征组在所述补位字符串的位置，确定对所述特征组的计算顺序；

获取预设摘要，并将所述预设摘要作为首个特征组的初始摘要，所述首个特征组为根据所述计算顺序被第一个计算的特征组；

将所述首个特征组以及所述首个特征组的初始摘要作为输入值，计算出所述首个特征组的特征组摘要；

根据所述计算顺序，将上一个特征组的特征组摘要作为下一个特征组的初始摘要；对各个特征组依次执行将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征组的特征组摘要的操作，直至计算出最后一个特征组的特征组摘要，并将所述最后一个特征组的特征组摘要作为设备指纹。

[权利要求 14] 如权利要求13所述的登录信息的加密电子设备，其特征在于，所述将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征

组的特征组摘要，包括：

将所述特征组分成M个特征子组，根据预设的扩展规则将所述M个特征子组扩展为N个特征子组，并分别为所述N个特征子组编号，所述M为大于1的整数，所述N为大于M的整数；

将所述特征组的所述初始摘要按照排列顺序分为L个初始摘要组，并分别为所述初始摘要组编号，所述L为大于1的整数；

设置所述L个缓存组，并分别为所述缓存组编号；

将各个所述初始摘要组的数据分别存入编号相同的所述缓存组中，循环执行N轮移位赋值计算，所述移位赋值计算包括：在将各个缓存组的数据移位存入后一个缓存组内后，将当前的首个缓存组的数据加上对应的特征子组的数据，作为新的所述首个缓存组的数据以更新所述首个缓存组，所述对应的特征子组的编号与当前所述移位赋值计算的轮次相同；

将经过N轮移位赋值计算后的各个缓存组内数据组合，作为所述特征组的特征组摘要。

[权利要求 15] 如权利要求11所述的登录信息的加密电子设备，其特征在于，所述根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文，包括：

将所述登录信息转换为明文矩阵；

将所述明文矩阵进行行移位操作、列混淆操作以及通过所述加密密钥进行轮密钥加操作，生成登录密文。

[权利要求 16] 一种计算机可读存储介质，所述计算机可读存储介质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至少一个处理器执行时实现如下步骤：

获取登录信息以及设备的特征码，并按照预设规则将所述特征码重新排列后转换为特征字符串；

对所述特征字符串进行补位，生成补位字符串，并将所述补位字符串划分为多个特征组，所述特征组包含预设位数的字符；

按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹；
将所述设备指纹转换为符合预设的加密算法格式要求的加密密钥；
根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文。

[权利要求 17] 根据权利要求16所述的计算机可读存储介质，其特征在于，所述对所述字符串进行补位，包括：

在所述特征字符串的末位增加字符1后继续增加一个以上的字符0，直至所述特征字符串在补位后的位数除以第一预设数字后的余数等于第二预设数字。

[权利要求 18] 根据权利要求16所述的计算机可读存储介质，其特征在于，所述按照所述特征组在所述补位字符串的位置，依次计算各个所述特征组的特征组摘要，将最后一个特征组的特征组摘要作为设备指纹，包括：

按照所述特征组在所述补位字符串的位置，确定对所述特征组的计算顺序；

获取预设摘要，并将所述预设摘要作为首个特征组的初始摘要，所述首个特征组为根据所述计算顺序被第一个计算的特征组；

将所述首个特征组以及所述首个特征组的初始摘要作为输入值，计算出所述首个特征组的特征组摘要；

根据所述计算顺序，将上一个特征组的特征组摘要作为下一个特征组的初始摘要；对各个特征组依次执行将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征组的特征组摘要的操作，直至计算出最后一个特征组的特征组摘要，并将所述最后一个特征组的特征组摘要作为设备指纹。

[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，所述将所述特征组以及所述特征组的初始摘要作为输入值，计算出所述特征组的特征组摘要，包括：

将所述特征组分成M个特征子组，根据预设的扩展规则将所述M个特

征子组扩展为N个特征子组，并分别为所述N个特征子组编号，所述M为大于1的整数，所述N为大于M的整数；

将所述特征组的所述初始摘要按照排列顺序分为L个初始摘要组，并分别为所述初始摘要组编号，所述L为大于1的整数；

设置所述L个缓存组，并分别为所述缓存组编号；

将各个所述初始摘要组的数据分别存入编号相同的所述缓存组中，循环执行N轮移位赋值计算，所述移位赋值计算包括：在将各个缓存组的数据移位存入后一个缓存组内后，将当前的首个缓存组的数据加上对应的特征子组的数据，作为新的所述首个缓存组的数据以更新所述首个缓存组，所述对应的特征子组的编号与当前所述移位赋值计算的轮次相同；

将经过N轮移位赋值计算后的各个缓存组内数据组合，作为所述特征组的特征组摘要。

[权利要求 20]

根据权利要求16所述的计算机可读存储介质，其特征在于，所述根据所述预设的加密算法，使用所述加密密钥对所述登录信息进行加密，以生成登录密文，包括：

将所述登录信息转换为明文矩阵；

将所述明文矩阵进行行移位操作、列混淆操作以及通过所述加密密钥进行轮密钥加操作，生成登录密文。

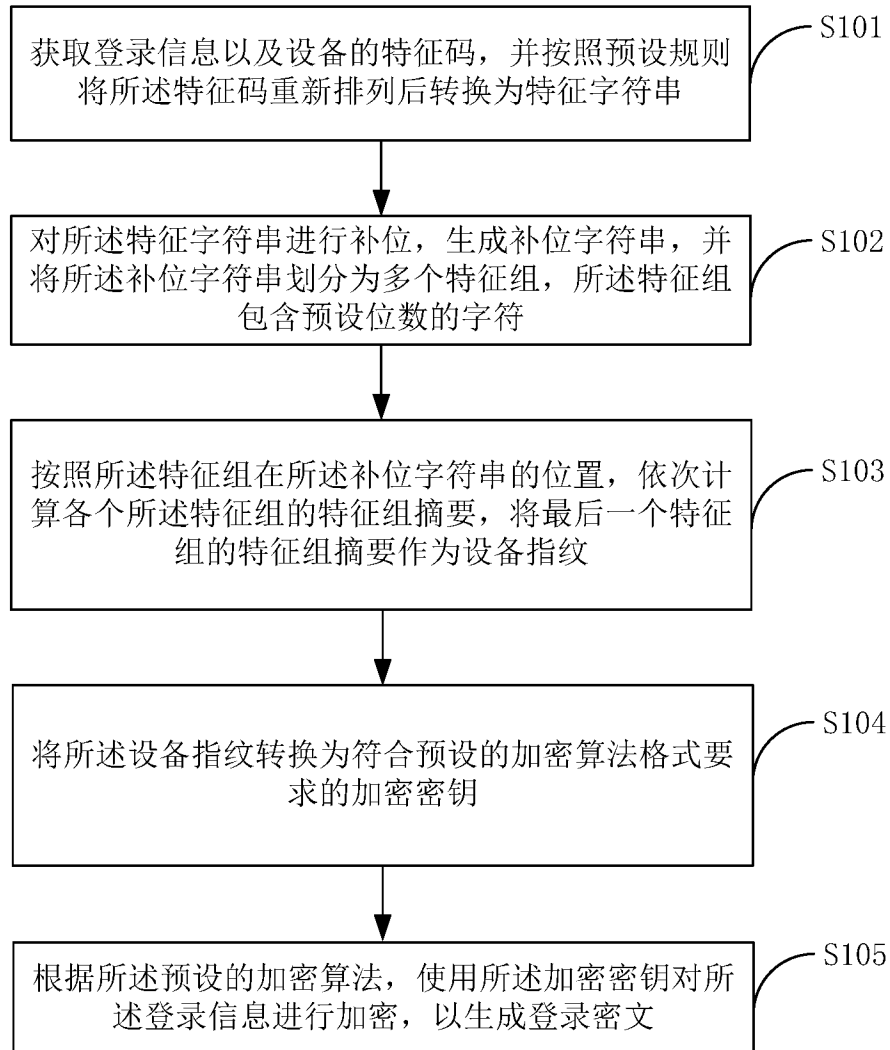


图 1

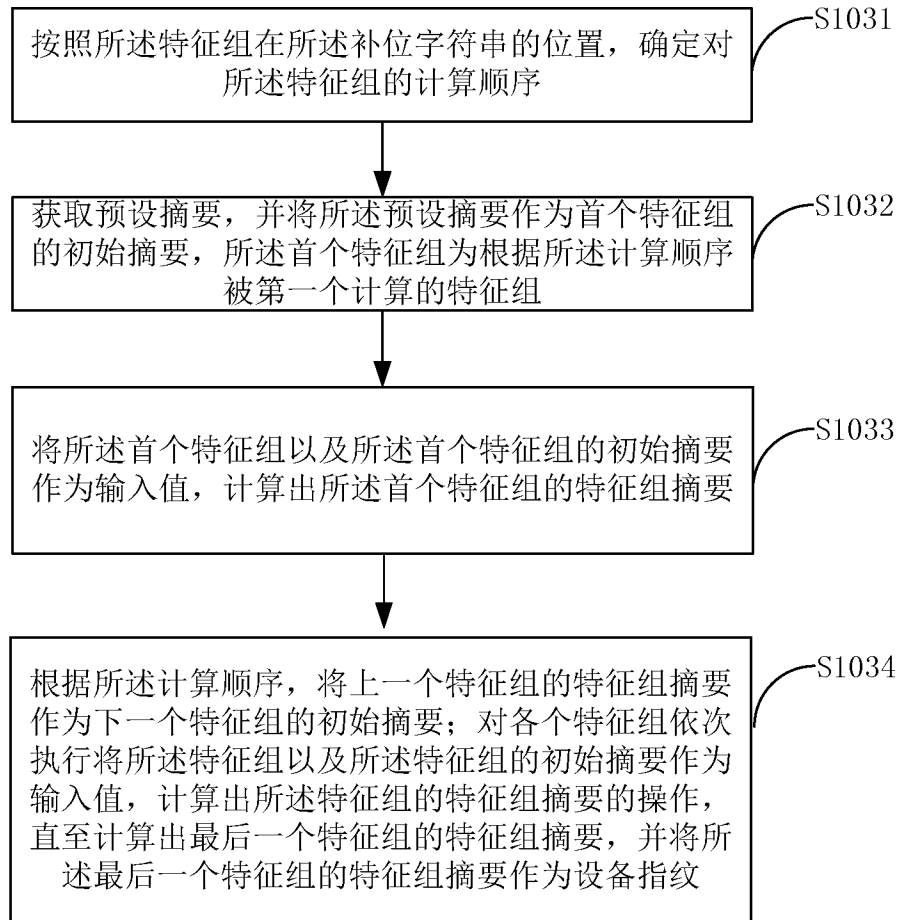


图 2

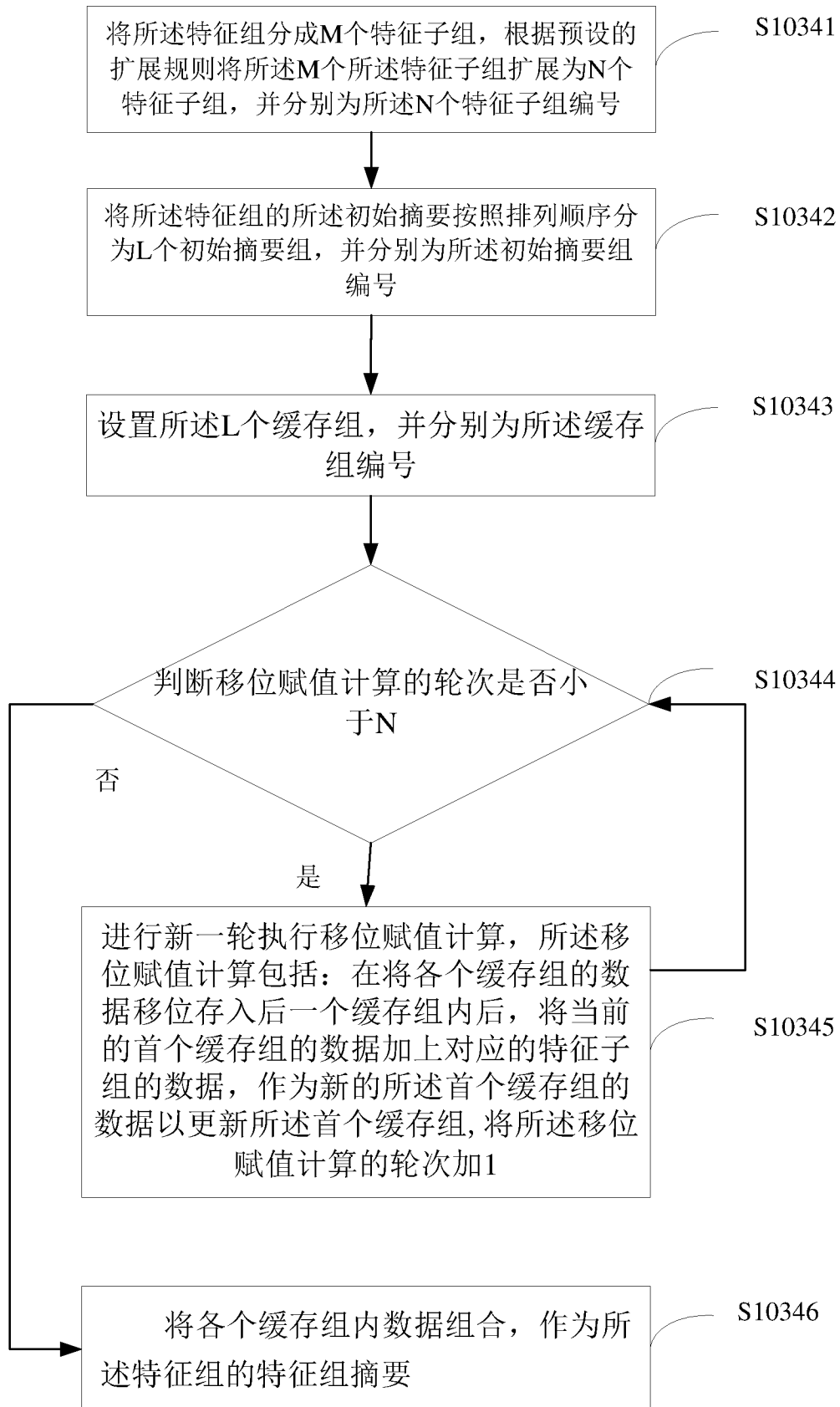


图 3

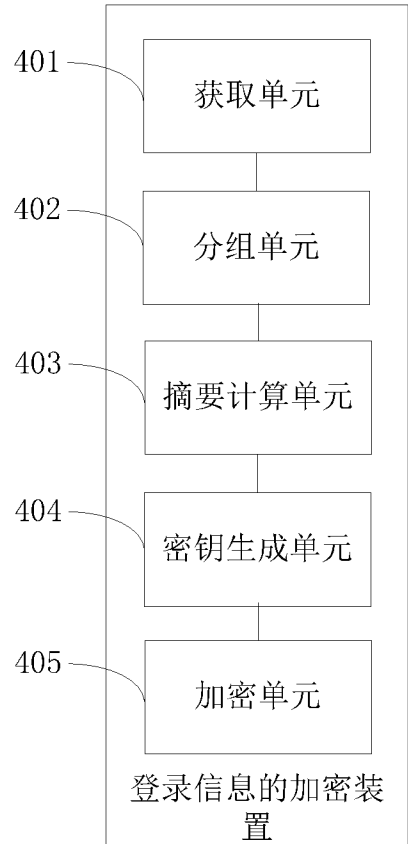


图 4

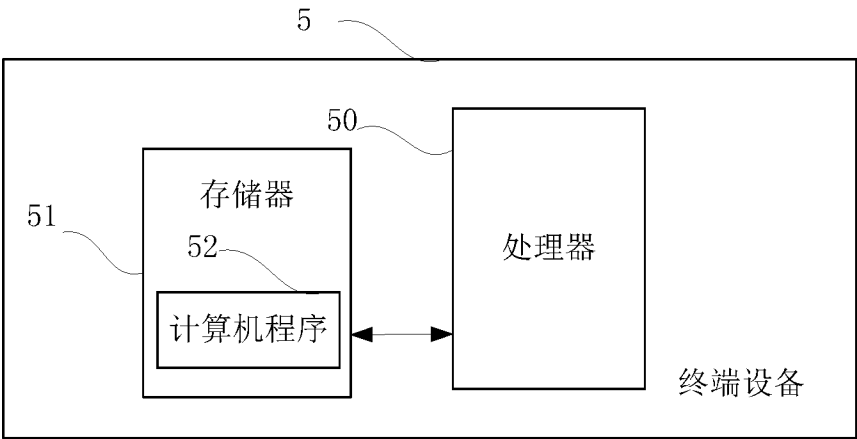


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/074868

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/06(2006.01)i; H04L 9/08(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

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)

CNABS; CNTXT; CNKI; VEN; DWPI; WOTXT; USTXT; EPTXT: 登录, 登陆, 加密, 设备, 终端, 装置, 特征码, 标识, 字符串, 排列, 补位, 填充, 填补, 划分, 拆分, 分组, 组合, 子组, 顺序, 摘要, 指纹, 密钥, 密文, login, encrypt+, device, terminal, apparatus, feature, code, identity, identifier, character string, alignment, filling, divide, group+, sub-group, order, sequence, abstract, fingerprint, key, ciphertext

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104253801 A (CHINA TELECOM CORPORATION LIMITED) 31 December 2014 (2014-12-31) see entire document	1-20
A	CN 104811298 A (CHINA UNITED NETWORK COMMUNICATIONS GROUP CO., LTD. ET AL.) 29 July 2015 (2015-07-29) see entire document	1-20
A	CN 104125055 A (XIAOMI TECHNOLOGY CO., LTD.) 29 October 2014 (2014-10-29) see entire document	1-20
A	CN 103780379 A (ALIBABA GROUP HOLDING LIMITED) 07 May 2014 (2014-05-07) see entire document	1-20
A	WO 2015052957 A1 (NEC CORP.) 16 April 2015 (2015-04-16) see 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

29 August 2018

Date of mailing of the international search report

05 September 2018

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

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/074868

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104253801	A	31 December 2014	CN	104253801	B	22 September 2017
CN	104811298	A	29 July 2015	CN	104811298	B	17 April 2018
CN	104125055	A	29 October 2014	CN	104125055	B	14 November 2017
CN	103780379	A	07 May 2014	CN	103780379	B	19 September 2017
				HK	1194564	A1	08 June 2018
				HK	1194564	A0	17 October 2014
WO	2015052957	A1	16 April 2015	US	2016240108	A1	18 August 2016
				JP	WO2015052957S	X	09 March 2017

国际检索报告

国际申请号

PCT/CN2018/074868

A. 主题的分类

H04L 9/06(2006.01)i; H04L 9/08(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

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))

CNABS;CNTXT;CNKI;VEN;DWPI;WOTXT;USTXT;EPTXT:登录, 登陆, 加密, 设备, 终端, 装置, 特征码, 标识, 字符串, 排列, 补位, 填充, 填补, 划分, 拆分, 分组, 组合, 子组, 顺序, 摘要, 指纹, 密钥, 密文, login, encrypt+, device, terminal, apparatus, feature, code, identity, identifier, character string, alignment, filing, divide, group+, sub-group, order, sequence, abstract, fingerprint, key, ciphertext

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
A	CN 104253801 A (中国电信股份有限公司) 2014年 12月 31日 (2014 - 12 - 31) 参见全文	1-20
A	CN 104811298 A (中国联合网络通信集团有限公司 等) 2015年 7月 29日 (2015 - 07 - 29) 参见全文	1-20
A	CN 104125055 A (小米科技有限责任公司) 2014年 10月 29日 (2014 - 10 - 29) 参见全文	1-20
A	CN 103780379 A (阿里巴巴集团控股有限公司) 2014年 5月 7日 (2014 - 05 - 07) 参见全文	1-20
A	WO 2015052957 A1 (NEC CORP) 2015年 4月 16日 (2015 - 04 - 16) 参见全文	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

2018年 8月 29日

国际检索报告邮寄日期

2018年 9月 5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

传真号 (86-10)62019451

受权官员

吴旭

电话号码 86-010-62089859

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/074868

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	104253801	A	2014年 12月 31日	CN	104253801	B	2017年 9月 22日
CN	104811298	A	2015年 7月 29日	CN	104811298	B	2018年 4月 17日
CN	104125055	A	2014年 10月 29日	CN	104125055	B	2017年 11月 14日
CN	103780379	A	2014年 5月 7日	CN	103780379	B	2017年 9月 19日
				HK	1194564	A1	2018年 6月 8日
				HK	1194564	A0	2014年 10月 17日
WO	2015052957	A1	2015年 4月 16日	US	2016240108	A1	2016年 8月 18日
				JP	W02015052957S	X	2017年 3月 9日

表 PCT/ISA/210 (同族专利附件) (2015年1月)