(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 9 月 26 日 (26.09.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/178981 A1

(51) 国际专利分类号:
G06F 21/46 (2013.01)

(21) 国际申请号: PCT/CN2018/094189

(22) 国际申请日: 2018 年 7 月 3 日 (03.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810242166.2 2018年3月22日 (22.03.2018) 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: 周泓宇 (ZHOU, Hongyu); 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)。

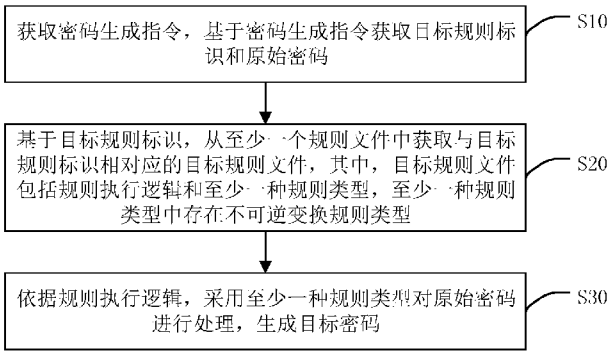
(74) 代理人: 深圳众鼎专利商标代理事务所（普通合伙) (SHENZHEN ZHONGDING INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市龙岗区龙城街道中心城清林路546号城投商务中心4层/B, Guangdong 518172 (CN)。

(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, 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,

(54) **Title:** PASSWORD MANAGEMENT METHOD AND DEVICE EMPLOYING CUSTOMIZED RULES, TERMINAL APPARATUS, AND STORAGE MEDIUM

(54) **发明名称:** 自定义规则密码管理方法、装置、终端设备及存储介质



S10 ACQUIRE A PASSWORD GENERATION INSTRUCTION, AND ACQUIRE, ON THE BASIS OF THE PASSWORD GENERATION INSTRUCTION, A TARGET RULE IDENTIFIER AND AN ORIGINAL PASSWORD

S20 ACQUIRE, FROM AT LEAST ONE RULE FILE ACCORDING TO THE TARGET RULE IDENTIFIER, A TARGET RULE FILE CORRESPONDING TO THE TARGET RULE IDENTIFIER, WHEREIN THE TARGET RULE FILE COMPRISES RULE EXECUTION LOGIC AND AT LEAST ONE RULE TYPE, AND THE AT LEAST ONE RULE TYPE COMPRISES AN IRREVERSIBLE TRANSFORMATION RULE TYPE

S30 USE THE AT LEAST ONE RULE TYPE TO PROCESS THE ORIGINAL PASSWORD ACCORDING TO THE RULE EXECUTION LOGIC, AND GENERATE A TARGET PASSWORD

图 1

(57) **Abstract:** The present application discloses a password management method and device employing customized rules, a terminal apparatus, and a storage medium. The password management method employing customized rules comprises: acquiring a password generation instruction, and acquiring, on the basis of the password generation instruction, a target rule identifier and an original password; acquiring, from at least one rule file according to the target rule identifier, a target rule file corresponding to the target rule identifier, wherein the target rule file comprises rule execution logic and at least one rule type, and the at least one rule type comprises an irreversible transformation rule type; and using the at least one rule type to process the original password according to the rule execution logic, and generating a target password. When the password management method employing customized rules is used to manage user passwords, a plurality of account passwords can be managed according to a unique original password of a user, thereby ensuring the security of password management.

WO 2019/178981 A1

[见续页]

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))。

(57) 摘要: 本申请公开了一种自定义规则密码管理方法、装置、终端设备及存储介质。该自定义规则密码管理方法，包括：获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。采用该自定义规则密码管理方法管理用户密码时，能够根据用户唯一的原始密码实现对多个账号密码的管理，并且保证密码管理的安全性。

自定义规则密码管理方法、装置、终端设备及存储介质

本申请以 2018 年 3 月 22 日提交的申请号为 201810242166.2，名称为“自定义规则密码管理方法、装置、终端设备及存储介质”的中国专利申请为基础，并要求其优先权。

技术领域

本申请涉及计算机领域，尤其涉及一种自定义规则密码管理方法、装置、终端设备及存储介质。

背景技术

当前各种支付方式，如支付宝、微信支付和银行卡等，一般都采用 6 位数字的验证方式作为支付密码。但是当用户全部使用一套相同的密码时，其风险太大，极易造成密码的泄露；若用户使用不同的密码时，又常常忘记密码，不能对用户密码进行有效的管理。

发明内容

本申请实施例提供一种自定义规则密码管理方法、装置、终端设备及存储介质，以解决当前用户密码容易泄露和被破译的问题。

第一方面，本申请实施例提供一种自定义规则密码管理方法，包括：

获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；

基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。

第二方面，本申请实施例提供一种自定义规则密码管理装置，包括：

标识密码获取模块，用于获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；

目标规则文件获取模块，用于基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和

至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

目标密码生成模块，用于依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。

第三方面，本申请实施例提供一种终端设备，包括存储器、处理器以及存储在所述存储器中并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：

获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；

基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。

第四方面，本申请实施例提供一个或多个存储有计算机可读指令的非易失性可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行如下步骤：

获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；

基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。

本申请的一个或多个实施例的细节在下面的附图和描述中提出，本申请的其他特征和优点将从说明书、附图以及权利要求变得明显。

附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例的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。

图 1 是本申请实施例 1 中自定义规则密码管理方法的一流程图。

图 2 是图 1 中步骤 S10 的一具体流程图。

图 3 是图 1 中步骤 S20 之前的一具体流程图。

图 4 是图 3 中步骤 S21 的一具体流程图。

图 5 是图 3 中步骤 S22 的一具体流程图。

图 6 是本申请实施例 2 中自定义规则密码管理装置的一原理框图。

图 7 是本申请实施例 4 中终端设备的一示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

实施例 1

图 1 示出本实施例中自定义规则密码管理方法的一流程图。该自定义规则密码管理方法可应用在应用程序中，能够根据用户唯一的原始密码和在数据库中保存的规则文件实时计算出与规则文件相对应的密码，有效实现用户的密码管理，该自定义规则密码管理方法具体可应用在安装在终端设备上的应用程序中。其中，该终端设备是可与用户进行人机交互的设备，包括但不限于电脑、智能手机和平板等设备。如图 1 所示，该自定义规则密码管理方法包括如下步骤：

S10：获取密码生成指令，基于密码生成指令获取目标规则标识和原始密码。

其中，密码生成指令是指用于获取目标规则标识和原始密码的指令。目标规则标识是指用于唯一识别目标规则文件的标识。目标规则文件是指用户想要获取的规则文件，规则文件是指保存规则设定的存储载体，具体可以是以文本格式的文件（.txt）形式保存，该文本格式的文件存储着按一定逻辑排序组合的（即规则执行逻辑）与规则类型相对应的函数，应用程序通过调用规则文件，执行规则文件中的函数，实现对原始密码的加密。原始密码是指是指用户唯一使用的密码，在该自定义规则密码管理方法中，用户只需要唯一记住原始密码就足够了。

本实施例中，在实现自定义规则密码管理的应用程序（以下简称应用程序）中，应用程序获取用户输入的密码生成指令，能够基于该密码生成指令快速、便捷地获取到目标规则标识和原始密码。

在一具体实施方式中，步骤S10中，如图2所示，获取密码生成指令，基于密码生成指令获取目标规则标识和原始密码，包括如下步骤：

S11：根据密码生成指令显示标识获取界面和原始密码获取界面。

其中，标识获取界面是指应用程序终端上显示的用于获取目标规则标识的界面，原始密码获取界面是指应用程序终端显示器上显示的用于获取原始密码的界面，标识获取界面和原始密码获取界面包括但不限于通过按键输入、语音输入等方式获取到相应的目标规则标识和原始密码。

本实施例中，应用程序获取用户输入的密码生成指令后在终端显示器上显示标识获取界面和原始密码获取界面，以提供获取用户输入信息的界面平台，顺利获取用户输入的目标规则标识和原始密码。

S12：通过标识获取界面和原始密码界面获取目标规则标识和原始密码。

本实施例中，应用程序可以提供按键输入、语音输入等录入信息的方式通过标识获取界面和原始密码界面获取用户输入的目标规则标识和原始密码。

S20：基于目标规则标识，从至少一个规则文件中获取与目标规则标识相对应的目标规则文件，其中，目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种规则类型中存在不可逆变换规则类型。

其中，规则执行逻辑是指规则类型对应的函数在规则设定中执行的顺序。规则类型是指对密码进行加密的运算规则的类型。从规则类型的概念可以自然、简易地理解规则设定的概念：规则设定是指由至少一种规则类型以自定义排序方式（也即规则执行逻辑）组合而成的规则类型的集合，从在开发平台创建规则设定的角度看，其实就是由至少一种规则类型对应的函数按自定义排序方式组合而成的运算程序。不可逆变换规则类型是指通过该规则类型加密后的值是不能反向推导、破译出加密前的值的规则类型。

本实施例中，基于目标规则标识，例如将规则文件 ID 作为目标规则标识，用户想要通过登录密码登录平安车险、平安寿险和平安产险的多个账号时，需要在应用程序通过规则文件ID（如平安车险、平安寿险和平安产险）查询获取已保存的目标规则文件（如平安车险.rule、平安寿险.rule 和平安产险.rule），以根据获取的目标规则文件获取规则文件ID为平安车险、平安寿险和平安产险的账号对应的登录密码。

在一具体实施方式中，步骤S20中，如图3所示，在基于目标规则标识，从至少一个规则文件中获取与目标规则标识相对应的目标规则文件的步骤之前，该自定义规则密码管理方法还包括：预先创建并保存至少一个规则文件。

该预先创建并保存至少一个规则文件的步骤包括：

S21：获取至少一种规则设定，每一规则设定包括相对应的规则执行逻辑和至少一种规则类型，至少一种规则类型中存在不可逆变换规则类型。

在创建规则设定的过程中，一种规则类型可以用相对应的函数来实现和表示，例如：用 add(pwd,num)函数表示其中的一种规则类型，该规则类型表示的是一种加法运算规则，其中，pwd 表示当前密码，num 表示该加法运算中增加的数值，当 num 取 123456 时，即函数表示为 add（pwd，123456）时，该加法运算规则的具体运算过程为 pwd+123456（即在当前密码的基础上加上 123456）。

可以理解地，当有三种规则类型 A（）、B（）和 C（）时，对这三种规则类型按照规则执行逻辑（自定义排序）进行组合可以得到 6 种不同的规则设定。当规则类型的运算更为复杂、规则类型的数量越多时，规则设定的种类就越多样，则根据规则设定计算获取的密码也越多样，加密的安全性就越高。

不可逆变换规则类型是指通过该规则类型加密后的值是不能反向推导、破译出加密前的值的规则类型，例如：采用基于 MD5 加密的截取法，首先对原始密码进行 MD5 加密，假设原始密码为 123456，则采用基于 MD5 加密的截取法加密后的值可表示为 32 位 16 进制数“E10ADC3949BA59ABBE56E057F20F883E”，截取前十位“E10ADC3949”，转化为 10 进制数“966549846345”，再截取后六位得到“846345”，由截取后的值 846345 是无法逆向还原为 123456 的。除基于 MD5 加密的截取法，采用其他不可逆变换规则类型也是可以的，如采用 SHA-1（安全散列算法中的一种）加密的截取法等不可逆变换规则类型。

本实施例中，获取至少一种规则设定，该规则设定包括相对应的规则执行逻辑和至少一种规则类型，每一规则设定的至少一种规则类型中存在至少一种不可逆变换规则类型，说明该规则设定的至少一种规则类型可以全部是不可逆变换规则类型，也可以同时包括至少一个不可逆变换规则类型和其他规则类型。通过相对应的规则执行逻辑（也即对规则类型的自定义排序组合）和至少一种规则类型获取的规则设定能够保证根据规则设定生成的密码具有多样性和高安全性的特点，能够有效防止密码泄露的问题。在至少一种规则类型中存在不可逆变换规则类型，可以保证根据规则设定生成的密码无法通过反向推导、破译的方式获取原始密码，极大提高原始密码的安全性。

在一具体实施方式中，步骤 S21 中，如图 4 所示，获取至少一种规则设定，每一规则设定包括相对应的规则执行逻辑和至少一种规则类型，至少一种规则类型中存在不可逆变换规则类型，包括如下步骤：

S211：获取预设的至少一种规则类型，规则类型中存在不可逆变换规则类型。

在实现自定义规则密码管理的应用程序中，会预先设置一些基础、常用的规则类型，例如在通常情况下，只是对以 6 位数字表示的原始密码进行加密转换，并且加密前和加密后的密码都是以 6 位数字的形式表示，则规则类型可以根据 6 位数字的特点预先设置相应的运算。不可逆变换规则类型是组成任何规则设定所不能缺少的一类规则类型，因此在预设规则类型时，也同样需要预设不可逆变换规则类型。

本实施例中，获取预先设置并保存在数据库中的至少一种规则类型，并且该至少一种规则类型中应存在不可逆变换规则类型，可以根据预设的规则类型判断该预设的规则类型是否满足组合规则设定的需求。

S212：若预设的至少一种规则类型存在组合规则设定所需的规则类型，则对组合规则设定所需的规则类型进行自定义排序组合，获取至少一种规则设定。

本实施例中，在获取预先设置的至少一种规则类型后，根据规则设定的实际需求，判断预设的至少一种规则类型是否存在组合规则设定所需的规则类型。若预设的至少一种规则类型存在组合规则设定所需的规则类型，则对组合规则设定所需的规则类型进行自定义排序组合，获取至少一种规则设定。例如：有规则类型 add(pwd,num)、invert（pwd）和 MD5(6)（pwd）三种规则类型（其中，invert（）指反转运算，该反转运算在这里具体运算规则为：如有数值 111111，则反转运算为 1000000-111111；MD5（6）表示基于 MD5 加密的截取法，最终截取的值为后 6 位）时，可以根据该三种规则类型进行自定义的排序并组合，由 $A_3^3 = \frac{3!}{(3-3)!}$（规定 0!为 1）能够得到 6 种不同的规则设定。具体地，如采用 invert（pwd）、add(pwd,num)和 MD5（pwd）的组合方式运算，当 pwd=888888，num=12344 时，得到的结果为“846345”，具体运算过程如下：

1）invert -> 1000000 - 888888 = 111112

2) add 12344 -> 111112 + 12344 = 123456

3) MD5(6) 123456 -> 846345

通过从预设的至少一种规则类型中对组合规则设定所需的规则类型进行自定义排序组合，能够得到多种规则设定，用户可以根据不同的规则类型进行自定义规则密码管理，能够实现对密码的有效管理，提高加密的安全性。

需要说明的是，规则类型是对用户公开的，用户能够知道规则类型具体是怎样进行加密运算的，能够减少用户对规则类型不透明的担忧，并且用户还可以根据公开的规则类型

进行运算和检验，而不需完全借助于应用程序本身，可以进一步提高密码管理的安全性和可靠性。

S213：若预设的至少一种规则类型缺少组合规则设定的规则类型，则创建组合规则设定所需的规则类型，并对所需的规则类型进行自定义排序组合，获取至少一种规则设定。

本实施例中，在获取预先设置的至少一种规则类型后，根据规则设定的实际需求，判断预设的至少一种规则类型是否存在组合规则设定所需的规则类型。若预设的至少一种规则类型缺少组合规则设定的规则类型，例如，规则设定要求能够对出现字母的原始密码进行处理，假设原始密码为 z1s123，则当预设的规则类型如 add（pwd，123456）对原始密码 z1s123 进行加密运算时，z1s123+123456 将无法对密码中的字母进行处理。因此，需要创建能够解决字母问题的组合规则设定所需的规则类型。对于原始密码为 z1s123，要求能够对字母进行处理的，可以直接创建新的规则类型，或者在原来 add（pwd，123456）等规则类型的基础上进行编辑修改后再另存为新的符合组合规则设定所需的规则类型。例如，在 add（pwd，123456）的基础上，再添加一种运算情况：令 a+1 = b, b+1=c，……，z+1 = a。则原始密码为 z1s123 时，采用该新的规则类型直接对原始密码 z1s123 进行运算能够得到 anv579，并再结合其他符合组成规则设定的规则类型（包括至少一种不可逆变换规则类型）进行自定义排序组合，能够得到相应的规则设定。本实施例中只是举了简单的例子，在实际应用中会采用更复杂、更多的规则类型对原始密码进行加密处理，以进一步地提高加密的安全性。

另外，在实际应用中，每次都创建新的规则类型是比较耗费时间的，因此除了用户通过自身创建规则类型的方式外，还可以在规则类型库中直接选取符合需求的规则类型，并将该规则类型下载到本地规则类型库中。该规则类型库保存大量的多种不同需求的规则类型，供用户使用。需要说明的是，由于组成规则设定的规则类型中存在至少一种不可逆变换规则类型，因此允许用户采用相同的规则设定，该做法不会造成用户原始密码的泄露，能够提高规则设定使用的灵活性。

需要说明的是，步骤 S211-S213 中“规则类型自定义排序组合”即“规则执行逻辑”，可以理解地，对规则类型自定义排序组合相当于规则设定中规则类型对应的函数在应用程序时执行的逻辑顺序。

S22：根据至少一种规则设定创建并保存相对应的至少一个规则文件，并给规则文件配置相应的规则标识。

本实施例中，根据至少一种规则设定创建相对应的至少一个规则文件，将规则文件保

存在数据库中，并给规则文件配置相应的规则标识，使得用户能够通过应用程序根据规则标识（用于唯一识别规则文件的标识）快速地调用规则文件，并根据规则文件执行加密运算。

在一具体实施方式中，步骤 S22 中，如图 5 所示，根据至少一种规则设定创建并保存相对应的至少一个规则文件，并给规则文件配置相应的规则标识，包括如下步骤：

S221：根据至少一种规则设定创建至少一个规则文件。

本实施例中，根据至少一种规则设定，创建相对应的至少一个规则文件，该规则文件以明文方式保存有按一定逻辑排序组合的与规则类型相对应的函数。

S222：对至少一个规则文件的内容进行加密，并将加密后的至少一个规则文件保存在数据库中。

本实施例中，虽然规则类型对用户是公开的，但是对于其他用户并不希望是公开的（除了在规则类型库中共享的），因此，规则文件中的内容，即规则类型对应的函数应当进行加密处理，具体的加密处理方式可以采用 base64 编码的方式实现。若存储规则文件的内容，base64 编码加密过程如下：

add （pwd，123456）

Invert（pwd）

MD5（pwd）

进行 base64 编码：

得到：

“YWRkIO+8iHB3ZO+8jDEyMzQ1Nu+8iQpJbnZlcnTvvIhwd2TvvIkKTUQ177yIcHdk77yJ”。

编码后将内容存入规则文件中即可，在后续使用该规则文件的时候，只要进行 base64 解码即可获取加密前规则文件保存的规则类型对应的函数的明文。本实施例中，将规则文件的内容进行加密，可以提高规则文件的安全性，保护保存在规则文件中规则类型对应的函数。

S30：依据规则执行逻辑，采用至少一种规则类型对原始密码进行处理，生成目标密码。

目标密码是指用户想要获取的密码。本实施例中，目标密码为用户唯一拥有的原始密码，依据目标规则文件中保存的至少一种规则类型，并根据该目标规则文件对应的规则执行逻辑对原始密码进行计算处理后获取。进一步地，该目标密码将限时地显示，即在一预设时间段后需要重新生成才可显示出来，以保证密码的安全性。通过用户只需记住原始密

码的方式，能够减轻用户的记忆负担，提高对于密码的高效管理。并且，生成的目标密码是无法通过破译从而获取用户的原始密码的，该基于用户唯一拥有的原始密码，并根据目标规则文件中规则执行逻辑和至少一种规则类型生成目标密码的方式保证了原始密码的安全性，用户不用担心原始密码泄露出去。

特别地，该自定义规则密码管理方法只保存规则文件而不保存用户的原始密码，即使规则文件泄露，规则设定被其他用户获知，也无法根据规则文件得到用户的原始密码，因此能够保证密码管理的安全性。

本实施例所提供的自定义规则密码管理方法中，目标规则标识从至少一个规则文件中获取与目标规则标识相对应的目标规则文件，其中，目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种规则类型中存在不可逆变换规则类型，基于规则执行逻辑和至少一种规则类型，能够保证根据目标规则文件生成的密码的多样性和高安全性，有效防止密码容易泄露的问题。在至少一种规则类型中加入不可逆变换规则类型，可以保证根据规则设定生成的密码将无法通过反向破译从而获取原始密码，极大提高规则设定生成密码的安全性。此外，还支持用户进行规则类型的自定义创建，能够实现对密码的有效管理，提高加密的安全性。根据至少一种规则设定创建并保存相对应的至少一个规则文件，对至少一个规则文件的内容进行加密，并将加密后的至少一个规则文件保存在数据库中，将至少一个规则文件的内容进行加密，可以提高规则文件的安全性，保护保存在规则文件中函数对应的规则类型。依据规则执行逻辑，采用至少一种规则类型对原始密码进行处理，生成目标密码，在获取目标规则文件（包括规则执行逻辑和至少一种规则类型）的基础下，只需获取唯一的原始密码即可根据目标规则文件实时生成目标密码，能够根据用户唯一拥有的原始密码创建所需账号的密码，并且通过只保存规则文件而不保存原始密码的方式，能够保证对密码进行管理时的安全性，实现有效的密码管理。

应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

实施例 2

图 6 示出与实施例 1 中自定义规则密码管理方法一一对应的自定义规则密码管理装置的原理框图。如图 6 所示，该自定义规则密码管理装置包括标识密码获取模块 10、目标规则文件获取模块 20 和目标密码生成模块 30。其中，标识密码获取模块 10、目标规则文件获取模块 20 和目标密码生成模块 30 的实现功能与实施例 1 中自定义规则密码管理方法对应的步骤一一对应，为避免赘述，本实施例不一一详述。

标识密码获取模块 10，用于获取密码生成指令，基于密码生成指令获取目标规则标识和原始密码。

目标规则文件获取模块 20，用于基于目标规则标识，从至少一个规则文件中获取与目标规则标识相对应的目标规则文件，其中，目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种规则类型中存在不可逆变换规则类型。

目标密码生成模块 30，用于依据规则执行逻辑，采用至少一种规则类型对原始密码进行处理，生成目标密码。

优选地，标识密码获取模块 10 包括界面生成单元 11 和标识密码获取单元 12。

界面生成单元 11，用于根据密码生成指令显示标识获取界面和原始密码获取界面。

标识密码获取单元 12，用于通过标识获取界面和原始密码界面获取目标规则标识和原始密码。

优选地，该自定义规则密码管理装置还包括规则文件创建保存模块 40，规则文件创建保存模块 40 包括规则设定获取单元 41 和规则文件创建保存单元 42。

规则设定获取单元 41，用于获取至少一种规则设定，每一规则设定包括相对应的规则执行逻辑和至少一种规则类型，至少一种规则类型中存在不可逆变换规则类型。

规则文件创建保存单元 42，用于根据至少一种规则设定创建并保存相对应的至少一个规则文件，并给规则文件配置相应的规则标识。

优选地，规则设定获取单元 41 包括规则类型获取子单元 411、第一规则设定获取子单元 412 和第二规则设定获取子单元 413。

规则类型获取子单元 411，用于获取预设的至少一种规则类型，规则类型中存在不可逆变换规则类型。

第一规则设定获取子单元 412，用于若预设的至少一种规则类型存在组合规则设定所需的规则类型，则对组合规则设定所需的规则类型进行自定义排序组合，获取至少一种规则设定。

第二规则设定获取子单元 413，用于若预设的至少一种规则类型缺少组合规则设定的规则类型，则创建组合规则设定所需的规则类型，并对所需的规则类型进行自定义排序组合，获取至少一种规则设定。

优选地，规则文件创建保存单元 42 包括规则文件创建子单元 421 和规则文件加密保存子单元 422。

规则文件创建子单元 421，用于根据至少一种规则设定创建至少一个规则文件。

规则文件加密保存子单元 422，用于对至少一个规则文件的内容进行加密，并将加密后的至少一个规则文件保存在数据库中。

实施例 3

本实施例提供一个或多个存储有计算机可读指令的非易失性可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行实现实施例 1 中自定义规则密码管理方法，为避免重复，这里不再赘述。或者，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行实现实施例 2 中自定义规则密码管理装置中各模块/单元的功能，为避免重复，这里不再赘述。

实施例 4

图 7 是本实施例中终端设备的示意图。如图 7 所示，终端设备 50 包括处理器 51、存储器 52 以及存储在存储器 52 中并可在处理器 51 上运行的计算机可读指令 53。处理器 51 执行计算机可读指令 53 时实现实施例 1 中自定义规则密码管理方法的各个步骤，例如图 1 所示的步骤 S10、S20 和 S30。或者，处理器 51 执行计算机可读指令 53 时实现实施例 2 中自定义规则密码管理装置各模块/单元的功能，如图 6 所示标识密码获取模块 10、目标规则文件获取模块 20 和目标密码生成模块 30 的功能。

示例性的，计算机可读指令 53 可以被分割成一个或多个模块/单元，一个或者多个模块/单元被存储在存储器 52 中，并由处理器 51 执行，以完成本申请。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 53 的指令段，该指令段用于描述计算机可读指令 53 在终端设备 50 中的执行过程。例如，计算机可读指令 53 可被分割成实施例 2 中的标识密码获取模块 10、目标规则文件获取模块 20 和目标密码生成模块 30，各模块的具体功能如实施例 2 所示，为避免重复，此处不一一赘述。

终端设备 50 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。终端设备可包括，但不仅限于，处理器 51、存储器 52。本领域技术人员可以理解，图 7 仅仅是终端设备 50 的示例，并不构成对终端设备 50 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，例如终端设备还可以包括输入输出设备、网络接入设备、总线等。

所称处理器 51 可以是中央处理单元(Central Processing Unit，CPU)，还可以是其他通用处理器、数字信号处理器 (Digital Signal Processor，DSP)、专用集成电路(Application Specific Integrated Circuit，ASIC)、现场可编程门阵列(Field-Programmable Gate Array，FPGA) 或者其他可编程逻辑器件、分立门或者晶体管

逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

存储器 52 可以是终端设备 50 的内部存储单元，例如终端设备 50 的硬盘或内存。存储器 52 也可以是终端设备 50 的外部存储设备，例如终端设备 50 上配备的插接式硬盘，智能存储卡（Smart Media Card, SMC），安全数字（Secure Digital, SD）卡，闪存卡（Flash Card）等。进一步地，存储器 52 还可以既包括终端设备 50 的内部存储单元也包括外部存储设备。存储器 52 用于存储计算机可读指令 53 以及终端设备所需的其他程序和数据。存储器 52 还可以用于暂时地存储已经输出或者将要输出的数据。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请实现上述实施例方法中的全部或部分流程，也可以通过计算机可读指令 53 来指令相关的硬件来完成，所述的计算机可读指令 53 可存储于一计算机可读存储介质中，该计算机可读指令 53 在被处理器执行时，可实现上述各个方法实施例的步骤。其中，所述计算机可读指令 53 包括计算机可读指令的代码，所述计算机可读指令的代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括：能够携带所述计算机可读指令代码的任何实体或装置、记录介质、U 盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、电载波信号、电信信号以及软件分发介质等。需要说明的是，所述计算机可读介质包含的内容可以根据司法管辖区内立法和专利实践的要求进行适当的增减，例如在某些司法管辖区，根据立法和专利实践，计算机可读介质不包括是电载波信号和电信信号。

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

1. 一种自定义规则密码管理方法，其特征在于，包括：

获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；

基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。

2. 根据权利要求 1 所述的自定义规则密码管理方法，其特征在于，在所述基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件的步骤之前，所述自定义规则密码管理方法还包括：预先创建并保存至少一个规则文件；

所述预先创建并保存至少一个规则文件的步骤包括：

获取至少一种规则设定，每一所述规则设定包括相对应的规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

根据至少一种所述规则设定创建并保存相对应的至少一个规则文件，并给所述规则文件配置相应的规则标识。

3. 根据权利要求 2 所述的自定义规则密码管理方法，其特征在于，所述获取至少一种规则设定，包括：

获取预设的至少一种规则类型，所述规则类型中存在不可逆变换规则类型；

若所述预设的至少一种规则类型存在组合所述规则设定所需的规则类型，则对组合所述规则设定所需的规则类型进行自定义排序组合，获取至少一种所述规则设定；

若所述预设的至少一种规则类型缺少组合所述规则设定所述的规则类型，则创建组合所述规则设定所需的规则类型，并对所述所需的规则类型进行自定义排序组合，获取至少一种所述规则设定。

4. 根据权利要求 2 所述的自定义规则密码管理方法，其特征在于，所述根据至少一种所述规则设定创建并保存相对应的至少一个规则文件，包括：

根据至少一种所述规则设定创建至少一个所述规则文件；

对至少一个所述规则文件的内容进行加密，并将加密后的至少一个所述规则文件保存在数据库中。

5. 根据权利要求 1 所述的自定义规则密码管理方法，其特征在于，所述基于所述密码生成指令获取目标规则标识和原始密码，包括：

根据所述密码生成指令显示标识获取界面和原始密码获取界面；

通过所述标识获取界面和原始密码界面获取所述目标规则标识和所述原始密码。

6. 一种自定义规则密码管理装置，其特征在于，包括：

标识密码获取模块，用于获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；

目标规则文件获取模块，用于基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

目标密码生成模块，用于依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。

7. 根据权利要求 6 所述的自定义规则密码管理装置，其特征在于，所述自定义规则密码管理装置还包括规则文件创建保存模块，用于预先创建并保存至少一个规则文件；

所述规则文件创建保存模块包括：

规则设定获取单元，用于获取至少一种规则设定，每一所述规则设定包括相对应的规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

规则文件创建保存单元，用于根据至少一种所述规则设定创建并保存相对应的至少一个规则文件，并给所述规则文件配置相应的规则标识。

8. 根据权利要求 7 所述的自定义规则密码管理装置，其特征在于，所述规则设定获取单元包括：

预设规则类型获取子单元，用于获取预设的至少一种规则类型，所述规则类型中存在不可逆变换规则类型；

第一规则设定获取子单元，用于若所述预设的至少一种规则类型存在组合所述规则设定所需的规则类型，则对组合所述规则设定所需的规则类型进行自定义排序组合，获取至少一种所述规则设定；

第二规则设定获取子单元，用于若所述预设的至少一种规则类型缺少组合所述规则设定所述的规则类型，则创建组合所述规则设定所需的规则类型，并对所述所需的规则类型进行自定义排序组合，获取至少一种所述规则设定。

9. 根据权利要求 7 所述的自定义规则密码管理装置，其特征在于，所述规则文件创建

保存单元，包括：

规则文件创建子单元，用于根据至少一种所述规则设定创建至少一个所述规则文件；

规则文件加密保存子单元，用于对至少一个所述规则文件的内容进行加密，并将加密后的至少一个所述规则文件保存在数据库中。

10. 根据权利要求 6 所述的自定义规则密码管理装置，其特征在于，所述标识密码获取模块，包括：

界面生成单元，用于根据所述密码生成指令显示标识获取界面和原始密码获取界面；

标识密码获取单元，用于通过所述标识获取界面和原始密码界面获取所述目标规则标识和所述原始密码。

11. 一种终端设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；

基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。

12. 根据权利要求 11 所述的终端设备，其特征在于，在所述基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件的步骤之前，所述处理器执行所述计算机可读指令时还实现如下步骤：预先创建并保存至少一个规则文件；

所述预先创建并保存至少一个规则文件的步骤包括：

获取至少一种规则设定，每一所述规则设定包括相对应的规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

根据至少一种所述规则设定创建并保存相对应的至少一个规则文件，并给所述规则文件配置相应的规则标识。

13. 根据权利要求 12 所述的终端设备，其特征在于，所述获取至少一种规则设定，包括：

获取预设的至少一种规则类型，所述规则类型中存在不可逆变换规则类型；

若所述预设的至少一种规则类型存在组合所述规则设定所需的规则类型，则对组合所

述规则设定所需的规则类型进行自定义排序组合，获取至少一种所述规则设定；

若所述预设的至少一种规则类型缺少组合所述规则设定所述的规则类型，则创建组合所述规则设定所需的规则类型，并对所述所需的规则类型进行自定义排序组合，获取至少一种所述规则设定。

14. 根据权利要求 12 所述的终端设备，其特征在于，所述根据至少一种所述规则设定创建并保存相对应的至少一个规则文件，包括：

根据至少一种所述规则设定创建至少一个所述规则文件；

对至少一个所述规则文件的内容进行加密，并将加密后的至少一个所述规则文件保存在数据库中。

15. 根据权利要求 11 所述的终端设备，其特征在于，所述基于所述密码生成指令获取目标规则标识和原始密码，包括：

根据所述密码生成指令显示标识获取界面和原始密码获取界面；

通过所述标识获取界面和原始密码界面获取所述目标规则标识和所述原始密码。

16. 一个或多个存储有计算机可读指令的非易失性可读存储介质，其特征在于，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行如下步骤：

获取密码生成指令，基于所述密码生成指令获取目标规则标识和原始密码；

基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件，其中，所述目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

依据所述规则执行逻辑，采用至少一种所述规则类型对所述原始密码进行处理，生成目标密码。

17. 根据权利要求 16 所述的非易失性可读存储介质，其特征在于，在所述基于所述目标规则标识，从至少一个规则文件中获取与所述目标规则标识相对应的目标规则文件的步骤之前，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器还执行如下步骤：预先创建并保存至少一个规则文件；

所述预先创建并保存至少一个规则文件的步骤包括：

获取至少一种规则设定，每一所述规则设定包括相对应的规则执行逻辑和至少一种规则类型，至少一种所述规则类型中存在不可逆变换规则类型；

根据至少一种所述规则设定创建并保存相对应的至少一个规则文件，并给所述规则文件配置相应的规则标识。

18. 根据权利要求 17 所述的非易失性可读存储介质，其特征在于，所述获取至少一种规则设定，包括：

获取预设的至少一种规则类型，所述规则类型中存在不可逆变换规则类型；

若所述预设的至少一种规则类型存在组合所述规则设定所需的规则类型，则对组合所述规则设定所需的规则类型进行自定义排序组合，获取至少一种所述规则设定；

若所述预设的至少一种规则类型缺少组合所述规则设定所述的规则类型，则创建组合所述规则设定所需的规则类型，并对所述所需的规则类型进行自定义排序组合，获取至少一种所述规则设定。

19. 根据权利要求 17 所述的非易失性可读存储介质，其特征在于，所述根据至少一种所述规则设定创建并保存相对应的至少一个规则文件，包括：

根据至少一种所述规则设定创建至少一个所述规则文件；

对至少一个所述规则文件的内容进行加密，并将加密后的至少一个所述规则文件保存在数据库中。

20. 根据权利要求 16 所述的非易失性可读存储介质，其特征在于，所述基于所述密码生成指令获取目标规则标识和原始密码，包括：

根据所述密码生成指令显示标识获取界面和原始密码获取界面；

通过所述标识获取界面和原始密码界面获取所述目标规则标识和所述原始密码。

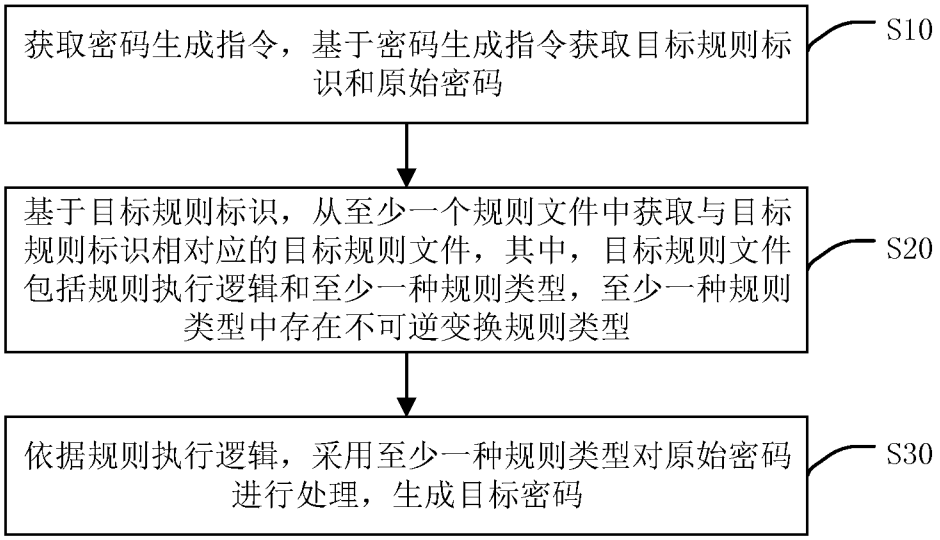

获取密码生成指令，基于密码生成指令获取目标规则标识和原始密码
S10
基于目标规则标识，从至少一个规则文件中获取与目标规则标识相对应的目标规则文件，其中，目标规则文件包括规则执行逻辑和至少一种规则类型，至少一种规则类型中存在不可逆变换规则类型
S20
依据规则执行逻辑，采用至少一种规则类型对原始密码进行处理，生成目标密码
S30

图 1

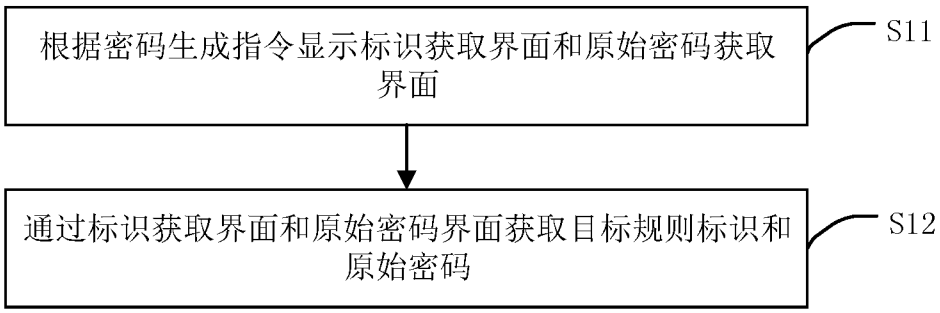

根据密码生成指令显示标识获取界面和原始密码获取界面
S11
通过标识获取界面和原始密码界面获取目标规则标识和原始密码
S12

图 2

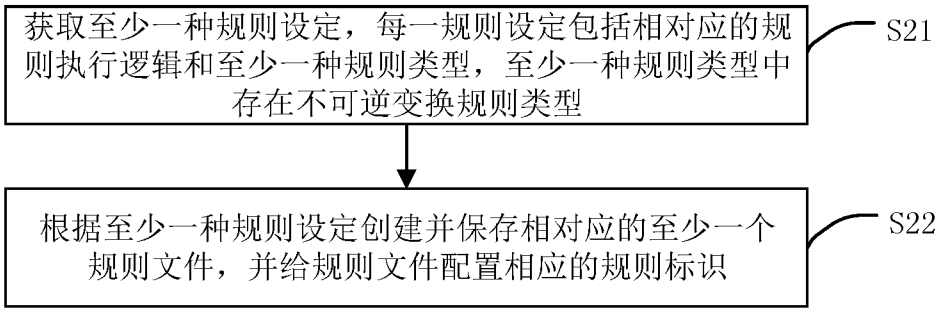

获取至少一种规则设定，每一规则设定包括相对应的规则执行逻辑和至少一种规则类型，至少一种规则类型中存在不可逆变换规则类型
S21
根据至少一种规则设定创建并保存相对应的至少一个规则文件，并给规则文件配置相应的规则标识
S22

图 3

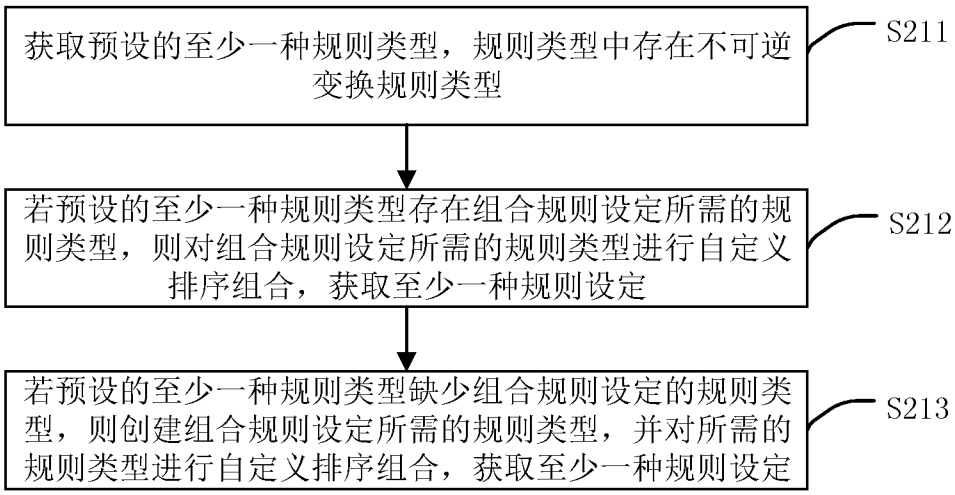

获取预设的至少一种规则类型，规则类型中存在不可逆变换规则类型
S211
若预设的至少一种规则类型存在组合规则设定所需的规则类型，则对组合规则设定所需的规则类型进行自定义排序组合，获取至少一种规则设定
S212
若预设的至少一种规则类型缺少组合规则设定的规则类型，则创建组合规则设定所需的规则类型，并对所需的规则类型进行自定义排序组合，获取至少一种规则设定
S213

图 4

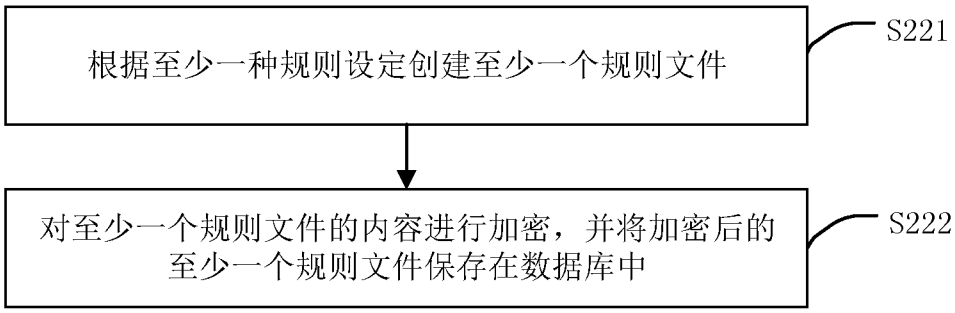

根据至少一种规则设定创建至少一个规则文件
S221
对至少一个规则文件的内容进行加密，并将加密后的至少一个规则文件保存在数据库中
S222

图 5

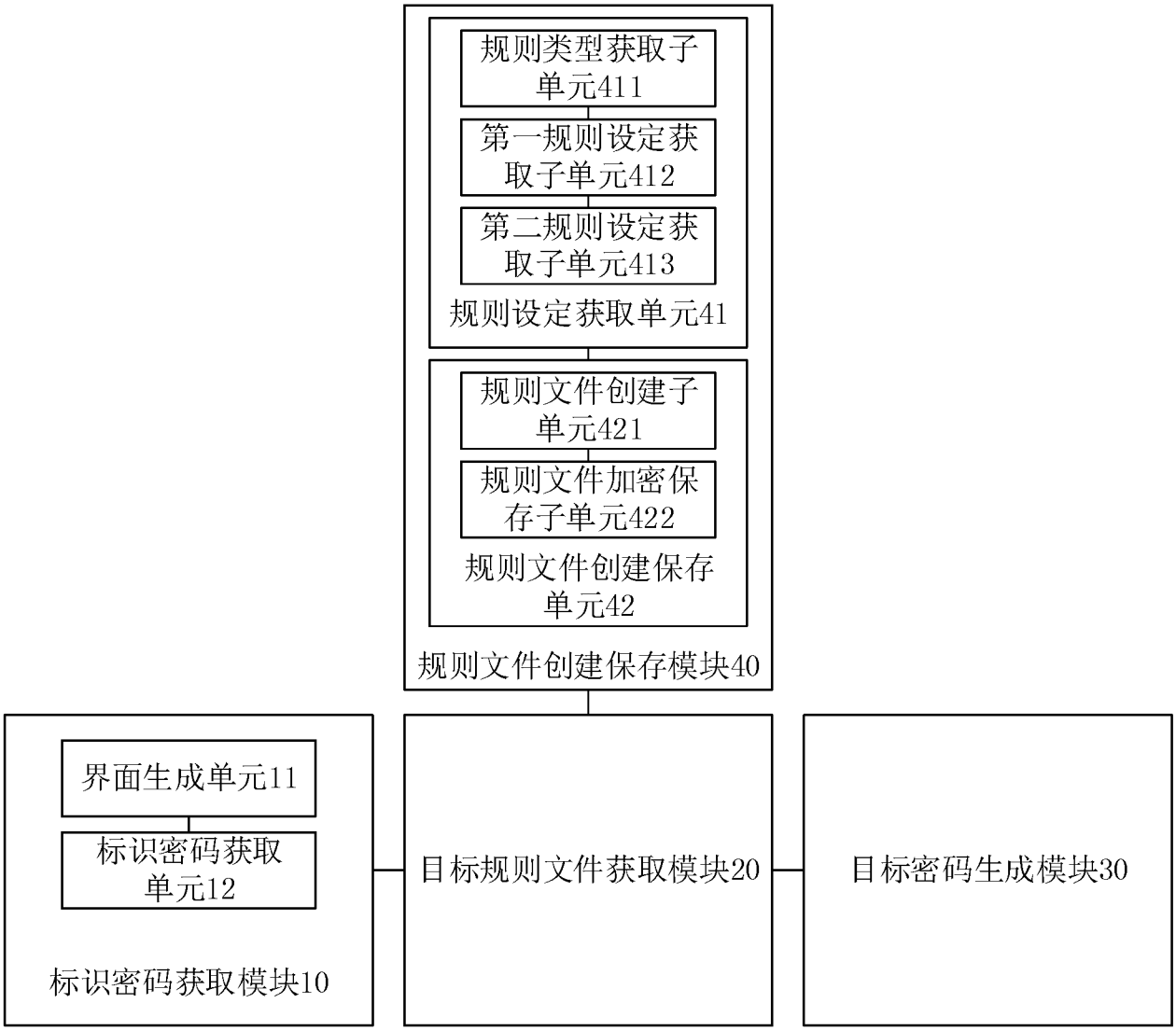

规则类型获取子单元411
第一规则设定获取子单元412
第二规则设定获取子单元413
规则设定获取单元41
规则文件创建子单元421
规则文件加密保存子单元422
规则文件创建保存单元42
规则文件创建保存模块40
界面生成单元11
标识密码获取单元12
标识密码获取模块10
目标规则文件获取模块20
目标密码生成模块30

图 6

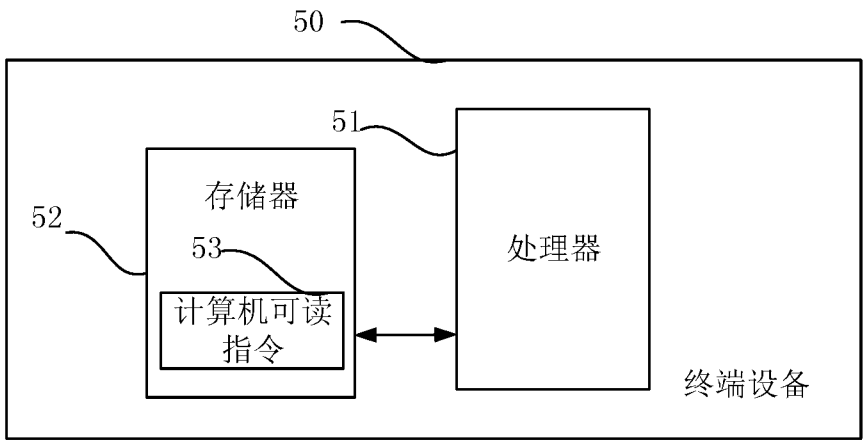

50
51
存储器
52
53
计算机可读指令
处理器
终端设备

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/094189

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/46(2013.01)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)

G06F

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; TWTXT; TWABS; DWPI; VEN; USTXT; EPTXT; WOTXT; CNKI: 自定义, 规则, 密码, 标识, 类型, 组合, 加, 反转, self-defined, rule, password, identification, type, combine, add, reverse

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 106888086 A (SHANGHAI HANZHIYOU INFORMATION TECHNOLOGY SERVICE CO., LTD.) 23 June 2017 (2017-06-23) description, paragraphs [0007]-[0041] and [0053]-[0055]	1-20
Y	CN 102316120 A (BEIJING INFORMATION SCIENCE & TECHNOLOGY UNIVERSITY) 11 January 2012 (2012-01-11) description, paragraphs [0012]-[0027], and figure 1	1-20
A	CN 105989309 A (WANG, FENGZHEN) 05 October 2016 (2016-10-05) entire document	1-20
A	US 2017083699 A1 (CHARTER COMMUNICATIONS OPERATING LLC) 23 March 2017 (2017-03-23) 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
15 November 2018	**10 December 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China (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/CN2018/094189

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106888086 A	23 June 2017	None	
CN 102316120 A	11 January 2012	None	
CN 105989309 A	05 October 2016	None	
US 2017083699 A1	23 March 2017	None	

国际检索报告

国际申请号
PCT/CN2018/094189

A. 主题的分类

G06F 21/46(2013.01)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)

G06F

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;TWTXT;TWABS;DWPI;VEN;USTXT;EPTXT;WOTXT;CNKI:自定义，规则，密码，标识，类型，组合，加，反转，self-defined, rule, password, identification, type, combine,add, reverse

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
Y	CN 106888086 A (上海瀚之友信息技术服务有限公司) 2017年 6月 23日 (2017-06-23) 说明书第7-41、53-55段	1-20
Y	CN 102316120 A (北京信息科技大学) 2012年 1月 11日 (2012-01-11) 说明书第12-27段，图1	1-20
A	CN 105989309 A (汪风珍) 2016年 10月 5日 (2016-10-05) 全文	1-20
A	US 2017083699 A1 (CHARTER COMMUNICATIONS OPERATING LLC) 2017年 3月 23日 (2017-03-23) 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
2018年 11月 15日	2018年 12月 10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 房琦 电话号码 86-(20)-28950714

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/094189

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 106888086 A	2017年 6月 23日	无	
CN 102316120 A	2012年 1月 11日	无	
CN 105989309 A	2016年 10月 5日	无	
US 2017083699 A1	2017年 3月 23日	无	