

(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 9 月 17 日 (17.09.2020)



(10) 国际公布号
WO 2020/181818 A1

(51) 国际专利分类号:
G06F 21/00 (2013.01)

(21) 国际申请号: PCT/CN2019/118412

(22) 国际申请日: 2019 年 11 月 14 日 (14.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910181682.3 2019 年 3 月 11 日 (11.03.2019) 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: 孟君(MENG, Jun); 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)。江琳(JIANG, Lin); 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: 北京中强智尚知识产权代理有限公司(BEIJING STRONG WISDOM INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市朝阳区北苑东路 19 号院 2 号楼 2608 室, Beijing 100012 (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,

(54) Title: ENCRYPTION AND DECRYPTION METHOD FOR ELECTRONIC FILE AND DEVICE

(54) 发明名称: 一种电子文件的加密、解密方法及其装置

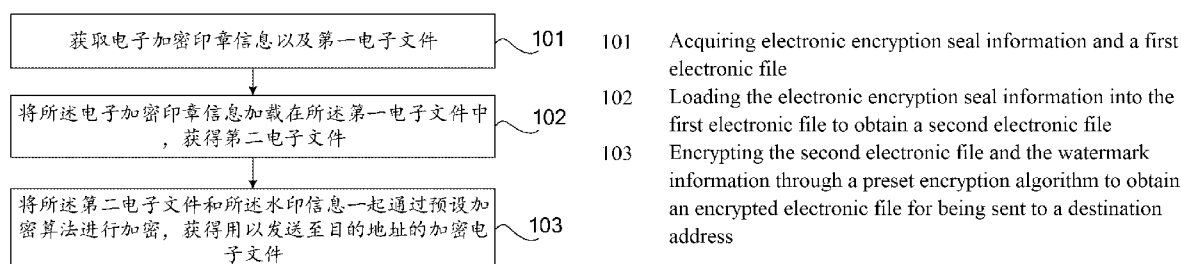


图 1

(57) Abstract: Provided are an encryption and decryption method for electronic file and device. The method comprises: acquiring electronic encryption seal information and a first electronic file (101), the electronic encryption seal information comprising information obtained after watermark information and an initial electronic seal are encrypted through a private key in an RSA key; loading the electronic encryption seal information into the first electronic file to obtain a second electronic file (102); and encrypting the second electronic file and the watermark information through a preset encryption algorithm to obtain an encrypted electronic file for being sent to a destination address (103). By encrypting the initial electronic seal and encrypting the first electronic file loaded with the electronic encryption seal information, the security of the electronic file in the process of approving and stamping the seal is improved, and the third party is prevented from tampering with the encrypted electronic file in the process of sending the encrypted electronic file to the destination address.

(57) 摘要: 一种电子文件的加密方法及其装置。该方法包括: 获取电子加密印章信息以及第一电子文件(101), 所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息; 将所述电子加密印章信息加载在所述第一电子文件中, 获得第二电子文件(102); 将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密, 获得用以发送至目的地址的加密电子文件(103)。通过对初始电子印章加密, 以及对加载有电子加密印章信息的第一电子文件进行加密, 提高了电子文件在审批并加盖印章的过程中安全性, 避免将加密电子文件向目的地址发送过程中第三方篡改加密电子文件。

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, 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)。

根据细则4.17的声明:

- 关于申请人有权申请并被授予专利(细则4.17(ii))
- 发明人资格(细则4.17(iv))

本国际公布:

- 包括国际检索报告(条约第21条(3))。

一种电子文件的加密、解密方法及其装置

本申请要求与2019年3月11日提交中国专利局、申请号为2019101816823、申请名称为“一种电子文件的加密、解密方法及其装置”的中国专利申请的优先权，其全部内容通过引用结合在申请中。

技术领域

本申请涉及加密技术领域，尤指一种电子文件的加密、解密方法及其装置。

背景技术

随着科技的发展，电子印章已经广泛的应用在人们生活中，其中，电子印章是以先进的数字技术模拟传统实物印章。

通常，在不同人员对同一文件进行审批并分别加盖印章时，人员可以对审批合格的文件加盖电子印章，从而减少纸质文件需要传输到不同地方进行印章的加盖。

然而，本申请的发明人在实现上述现有技术中发现，电子文件从第一人传输到第二人进行审批和加盖印章的过程中，该电子文件可能被第三人拦截并仿制第二人的印章，从而导致电子文件在审批并加盖印章的过程中安全性较低。

发明内容

为了解决上述技术问题，本申请提供了一种电子文件的加密、解密方法及装置，能够解决电子文件在审批并加盖印章的过程中安全性较低的问题。

为了达到本申请目的，本申请提供了一种电子文件的加密方法，包括：获取电子加密印章信息以及第一电子文件，所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；将所述电子加密印章加载在所述第一电子文件中，获得第二电子文件；将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密，获得用以发送至目的地址的加密电子文件。

本申请还提供了一种电子文件的解密方法，包括：接收加密电子文件，所述加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件；根据预设解密算法对所述加密电子文件进行解密，获得第二电子文件和第一水印信息，所述第二电子文件包括电子加密印章信息，所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；通过RSA密钥中的公钥对所述电子加密印章信息进行解密，获得第二水印信息；根据所述第一水印信息和所述第二水印信息，确定所述第一水印信息与所述第二水印信息是否相同；若相同，则确定所述加密电子文件为合法文件；若不相同，则确定所述加密电子文件为非法文件。

本申请还提供了一种电子文件的加密装置，包括：获取单元，用于获取电子加密印章信息以及第一电子文件，所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；加载单元，用于将所述电子加密印章信息加载在所述第一电子文件中，获得第二电子文件；加密单元，用于将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密，获得用以发送至目的地址的加密电子文件。

本申请还提供了一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行如上所述电子文件的加密步骤。

本申请还提供了一种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，使得一个或多个处理器执行如上所述电子文件的加密方法的步骤。

本申请还提供了一种电子文件的解密装置，包括：接收单元，用于接收加密电子文件，所述加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件；第一解密单元，用于根据预设解密算法对所述加密电子文件进行解密，获得第二电子文件和第一水印信息，所述第二电子文件包括电子加密印章信息，所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；第二解密单元，用于通过RSA密钥中的公钥对所述电子加密印章信息进行解密，获得第二水印信息；确定单元，用于根据所述第一水印信息和所述第二水印信息，确定所述第一水印信息与所述第二水印信息是否相同；若相同，则确定所述加密电子文件为合法文件；若不相同，则确定所述加密电子文件为非法文件。

本申请还提供了一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行如上所述电子文件的解密步骤。

本申请还提供了一种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,使得一个或多个处理器执行如上述所述电子文件的解密方法的步骤。

借由上述技术方案,本申请提供了一种电子文件的加密、解密方法及装置,通过获取电子加密印章信息以及第一电子文件,由于电子加密印章信息中包括通过RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息,通过将电子加密印章加载在第一电子文件中,获得第二电子文件,使得该第二电子文件具有较高的安全性,进一步再将第二电子文件和水印信息一起通过预设加密算法进行加密,获得用以发送至目的地址的加密电子文件。与现有技术中在电子文件上直接进行审批和加盖印章的方式相比,本申请实施例通过对初始电子印章进行加密,得到电子加密印章信息,以及对加载有电子加密印章信息的电子文件进行二次加密,得到加密电子文件提高了电子文件在审批并加盖印章的过程中安全性,避免将加密电子文件向目的地址发送过程中第三方篡改加密电子文件。

附图说明

附图用来提供对本申请技术方案的进一步理解,并且构成说明书的一部分,与本申请的实施例一起用于解释本申请的技术方案,并不构成对本申请技术方案的限制。

图1为本申请电子文件的加密方法一实施例的流程示意图;

图2为本申请电子文件的解密方法一实施例的流程示意图;

图3为本申请电子文件的加密装置一实施例的结构示意图;

图4为本申请电子文件的加密装置另一实施例的结构示意图;

图5为本申请电子文件的解密装置一实施例的结构示意图;

图6为本申请电子文件的解密装置另一实施例的结构示意图。

具体实施方式

为使本申请的目的、技术方案和优点更加清楚明白,下文中将结合附图对本申请的实施例进行详细说明。需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互任意组合。在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行。并且,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

图1为本申请电子文件的加密方法一实施例的流程示意图。如图1所示,本实施例的执行主体是电子文件的加密装置,其中,电子文件的加密装置可以独立设置,也可以设置在用于审批文件的服务器上。本实施例的适用场景为文件审批过程中对电子文件的进行加密。本实施例提供的电子文件的加密方法,包括:

步骤101、获取电子加密印章信息以及第一电子文件。

本实施例中的电子加密印章信息包括通过RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息,该电子文件是准备审批的文件,在该电子文件审批通过后可以对该电子文件加盖所述出事电子印章以及加载水印信息,其中,水印信息至少包括以下任意一项或其组合:审批通过时间、审批开始时间、提交人信息、审批人信息、审批部门信息。由于初始电子印章并非是直接获取的电子印章,具体可以通过对物理印章进行处理,得到存储为预设格式的数字数据,并将该预设格式的数字数据作为初始电子印章,这里的预设格式可以为.seal 格式的数字数据。举例来讲,通过将物理印章模加盖到白纸上,接着,将白纸上的盖的印记转化为图片信息,再接着经过对图片的剪裁,调色,去除点,休边等操作后,将处理后获得的图片信息存储为.seal 格式的数字数据。对于本申请实施例,在进行文件电子文件的加密操作的同时,加载的水印信息中包括用于审批文件的多个信息字段,例如,提交人信息,提交时间,各个审批环境的审批部门信息,审批时间信息和审批人信息,具体获取电子加密印章信息的过程中,可以从水印信息中提取用于审批文件的多个信息字段,并将用于审批文件的多个信息字段按照预设审批顺序进行排序组成审批链数据,并将审批链数据和初始电子印章进行加密后,获得电子加密印章信息。

示例性的,上述的信息字段可以以分隔符“分隔将数据组成审批链数据,审批链数据的组成格式如下例:“组成格式如下例:下例:例:得电子加密印:00:18/项目部 user2 2018:例:得电子加密印章信息。信息。办公室 user3 2018-08-18 15:03:06/总经办 user4 2018-08-23 14:08:15/获。随后将审批链数据和初始电子印章组合成为待加密数据,通过对待加密数据进行加密后得到电子加密印章信息。进一步的,对水印信息和初始电子印章进行加密的方法可以包括现有任何加密算法,例如,RSA 算法,通过RSA 算法可以确定密钥对,通过加密密钥可以执行加密步骤,通过解密密钥执行解密步骤。需要说明的是,为提高保密强度,RSA 密钥至少为500位长,本实施例的RSA 密钥可以采用1024位。

步骤 102、将所述电子加密印章信息加载在所述第一电子文件中，获得第二电子文件。

具体的，在该第一电子文件审批通过后，为了防止第三方拦截并篡改第一电子文件，可以将电子加密印章信息加载在电子文件中，以获得加载有初始电子印章的第二电子文件，由于第二电子文件中加载的电子加密印章信息具有较高的安全性，并非第三方可以轻易破解，从而提高了电子文件的安全性。

步骤 103、将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密，获得用以发送至目的地址的加密电子文件。

具体的，为了提高第二电子文件发送至目的地址的安全性，通过预设加密算法对第二电子文件和水印信息进行加密，获得加密电子文件。由于第二电子文件中已经覆盖有电子加密印章信息，使得利用预设加密算法对第二电子文件和水印信息进行二次加密后的加密电子文件具有更高的安全性，不易被破解。需要说明的是，该预设加密算法可以是本领域技术人预先设定的加密算法，例如 AES 算法、混沌序列算法、LSB 算法等等，具体在将第二电子文件和水印信息一起进行加密的过程中，可以通过预设加密算法对水印信息进行加密后，得到加密水印的图像，并将加密水印的图像嵌入至第二电子文件中，从而得到加密电子文件，当然还可以在将水印信息嵌入至第二电子文件后，通过预设加密算法对嵌入水印信息的第二电子文件进行加密后，得到加密电子文件。

本申请实施例提供的一种电子文件的加密方法，通过获取电子加密印章信息以及第一电子文件，由于电子加密印章信息中包括通过 RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息，通过将电子加密印章加载在第一电子文件中，获得第二电子文件，使得该第二电子文件具有较高的安全性，进一步再将第二电子文件和水印信息一起通过预设加密算法进行加密，获得用以发送至目的地址的加密电子文件。与现有技术中在电子文件上直接进行审批和加盖印章的方式相比，本申请实施例通过对初始电子印章进行加密，得到电子加密印章信息，以及对加载有电子加密印章信息的电子文件进行二次加密，得到加密电子文件提高了电子文件在审批并加盖印章的过程中安全性，避免将加密电子文件向目的地址发送过程中第三方篡改加密电子文件。

图 2 为本申请电子文件的解密方法一实施例的流程示意图。如图 2 所示，本实施例的执行主体是解密文件装置，其中，解密文件装置可以独立设置，也可以设置在用于电子文件的解密服务器上。本实施例的适用场景为文件全部审批流程结束后对第二加密电子文件进行解密。本实施例提供的电子文件的加密方法，包括：

步骤 201、接收加密电子文件，所述加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件。其中，加密电子文件是为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件，具有较高的安全性，如果不对电子文件进行解密无法直接获取电子文件中的内容。

步骤 202、根据预设解密算法对所述加密电子文件进行解密，获得第二电子文件和第一水印信息。其中，第二电子文件包括电子加密印章信息，该电子加密印章信息包括通过 RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息。对于本申请实施例，在接收到加密电子文件后，为了验证接收方并非第三方拦截，可以根据预设解密算法对加密电子文件进行解密，通过解密后可以获得第二电子文件和第一水印信息。需要说明的是，这里的预设解密算法与步骤 103 中预设加密算法为逆向过程，由于水印信息在电子文件的加密过程中使用了两次，所以通过对第二加密电子文件进行解密，获取到的是电子文件在第二次加密过程中使用的水印信息，即第一水印信息。

步骤 203、通过 RSA 密钥中的公钥对所述电子加密印章信息进行解密，获得第二水印信息。

本实施例采用非对称加密算法 RSA 算法，RSA 算法采用 1024 位密钥，即通过 RSA 加密算法确定一对 RSA 密钥，其中之一是私密密钥（SK），由各部门用于电子文件的加密终端保存，用来加密得到电子加密印章信息；另一个为公开密钥（PK），保存于打印电子文件的终端，用于对电子加密印章信息进行解密。需要说明的是，这里通过 RSA 密钥中的公钥对电子加密印章信息进行解密的过程为与步骤 101 中对初始电子印章和水印信息进行加密的过程的逆向，由于水印信息在电子文件的加密过程中使用了两次，所以通过对电子加密印章信息进行解密，获取到的是电子文件在第二次加密过程中使用的水印信息，即第二水印信息。

步骤 204、根据所述第一水印信息和所述第二水印信息，确定所述第一水印信息与所述第二水印信息是否相同。

由于加密电子文件过程中所使用的水印信息为相同的水印信息，所以对第二加密电子文件解密所提取到的第一水印信息和第二水印信息也应该是相同的水印信息，通过比对第一水印信息与第二水印信息

是否相同,可以及时发现电子文件是否为篡改。在确定第一水印信息与第二水印信息是否相同的过程中,由于第一水印信息和第二水印信息中包括用于审批文件的多个信息字段,例如,提交人信息,提交时间,各个审批环境的审批部门信息,审批时间信息和审批人信息,具体可以通过比较第一水印信息中的用于审批文件的多个信息字段与第二水印信息中用于审批文件的多个信息字段是否对应相同;若第一水印信息与第二水印信息中的多个信息字段均对应相同,则确定加密电子文件为合法文件;若存在至少一个信息字段不对应相同,则确定加密电子文件为非法文件。

步骤 205a、若相同,则确定所述加密电子文件为合法文件。对于本申请实施例,若相同,则说明电子文件在传输过程中未被篡改,确定该加密电子文件为合法文件。

与步骤 205a 相对应的有步骤 205b、若不相同,则确定所述加密电子文件为非法文件。对于本申请实施例,若不相同,则说明电子文件在传输过程中可能被篡改,确定该加密电子文件为非法文件。需要说明的是,由于在电子文件的加密过程中,可以在对初始电子印章和水印信息进行加密的同时,还可以将初始电子印章以及加密后的电子印章和水印信息进行整体加密,还可以增加与水印信息相同的新增信息,从而在所有部门盖章结束后对加密电子文件进行解密的过程中,可以首先提取解密后的新增信息,进一步的,通过 PK 对电子加密印章信息进行解密,获得解密后的水印信息,接着,将解密后的水印信息与解密后的新增信息进行比对,在比对相同后,确定该加密电子文件为合法文件,否则确定该加密电子文件为非法文件。

优选的,在上述实施例的基础上,如果加密电子文件为合法文件,说明电子文件是安全的,进一步在确定加密电子文件为合法文件之后,为了便于对电子文件的打印,可以将第一水印信息或第二水印信息通过预设转换算法,转换为目标字符或目标二维码;将目标字符或目标二维码加载在第二电子文件中输出,从而可以更直观的查看电子文件。

本申请实施例提供的一种电子文件的解密方法,通过接收加密电子文件,由于加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件,具有较高的安全性,需要根据预设解密算法对加密电子文件进行解密,从而获得第二电子文件和第一水印信息,进一步再通过 RSA 密钥中的公钥对电子加密印章信息进行解密,获得第二水印信息,通过判断第一水印信息和第二水印信息是否相同来确定加密电子文件是否为合法文件。与现有技术中在电子文件上直接进行审批和加盖印章的方式相比,本申请实施例通过对初始电子印章进行加密,得到电子加密印章信息,以及对加载有电子加密印章信息的电子文件进行二次加密,得到加密电子文件提高了电子文件在审批并加盖印章的过程中安全性,避免将加密电子文件向目的地址发送过程中第三方篡改加密电子文件。

进一步地,作为图 1 所述方法的具体实现,本申请实施例提供了一种电子文件的加密装置,如图 3 所示,所述电子文件的加密装置包括:第一获取单元 31、处理单元 32 和加密单元 33,其中,

获取单元 31,可以用于获取电子加密印章信息以及第一电子文件,所述电子加密印章信息包括通过 RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息;加载单元 32,可以用于将所述电子加密印章信息加载在所述第一电子文件中,获得第二电子文件;加密单元 33,可以用于将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密,获得用以发送至目的地址的加密电子文件。

本申请实施例提供的电子文件的加密装置,通过获取电子加密印章信息以及第一电子文件,由于电子加密印章信息中包括通过 RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息,通过将电子加密印章加载在第一电子文件中,获得第二电子文件,使得该第二电子文件具有较高的安全性,进一步再将第二电子文件和水印信息一起通过预设加密算法进行加密,获得用以发送至目的地址的加密电子文件。与现有技术中在电子文件上直接进行审批和加盖印章的方式相比,本申请实施例通过对初始电子印章进行加密,得到电子加密印章信息,以及对加载有电子加密印章信息的电子文件进行二次加密,得到加密电子文件提高了电子文件在审批并加盖印章的过程中安全性,避免将加密电子文件向目的地址发送过程中第三方篡改加密电子文件。

在具体的应用场景中,如图 4 所示,所述装置还包括:

处理单元 34,可以用于在所述获取电子加密印章信息之前,通过对物理印章进行处理,得到存储为预设格式的数字数据,将所述预设格式的数字数据作为初始电子印章。

进一步地,所述水印信息中包括用于审批文件的多个信息字段,所述获取单元 31 包括:提取模块 311,可以用于从所述水印信息中提取用于审批文件的多个信息字段;排序模块 312,可以用于将所述用于审批文件的多个信息字段按照预设审批顺序进行排序组成审批链数据;加密模块 313,可以用于将所述审批链数据和所述初始电子印章进行加密后,获得电子加密印章信息。

需要说明的是,本实施例提供的一种电子文件的加密装置所涉及各功能单元的其他相应描述,可以参考图1的对应描述,在此不再赘述。

基于上述如图1所示方法,相应的,本实施例还提供了一种存储介质,其上存储有计算机程序,该程序被处理器执行时实现上述如图1所示的电子文件的加密的方法。

进一步地,作为图2所述方法的具体实现,本申请实施例提供了一种电子文件的解密装置,如图5所示,本实施例提供的电子文件的解密装置包括:接收单元41、第一解密单元42、第二解密单元43和确定单元44;

接收单元41,可以用于接收加密电子文件,所述加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件;第一解密单元42,可以用于根据预设解密算法对所述加密电子文件进行解密,获得第二电子文件和第一水印信息,所述第二电子文件包括电子加密印章信息,所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息;第二解密单元43,可以用于通过RSA密钥中的公钥对所述电子加密印章信息进行解密,获得第二水印信息;确定单元44,可以用于根据所述第一水印信息和所述第二水印信息,确定所述第一水印信息与所述第二水印信息是否相同;若相同,则确定所述加密电子文件为合法文件;若不相同,则确定所述加密电子文件为非法文件。

本申请实施例提供的电子文件的解密装置,通过接收加密电子文件,由于加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件,具有较高的安全性,需要根据预设解密算法对加密电子文件进行解密,从而获得第二电子文件和第一水印信息,进一步再通过RSA密钥中的公钥对电子加密印章信息进行解密,获得第二水印信息,通过判断第一水印信息和第二水印信息是否相同来确定加密电子文件是否为合法文件。与现有技术中在电子文件上直接进行审批和加盖印章的方式相比,本申请实施例通过对初始电子印章进行加密,得到电子加密印章信息,以及对加载有电子加密印章信息的电子文件进行二次加密,得到加密电子文件提高了电子文件在审批并加盖印章的过程中安全性,避免将加密电子文件向目的地址发送过程中第三方篡改加密电子文件。

在具体的应用场景中,如图6所示,所述装置还包括:转换单元45,可以用于在确定所述加密电子文件为合法文件之后,将第一水印信息或所述第二水印信息通过预设转换算法,转换为目标字符或目标二维码;输出单元46,可以用于将所述目标字符或目标二维码加载在所述第二电子文件中输出。

进一步的,所述第一水印信息和所述第二水印信息中包括用于审批文件的多个信息字段,所述确定单元44包括:

比较模块441,可以用于比较所述第一水印信息中的用于审批文件的多个信息字段与所述第二水印信息中用于审批文件的多个信息字段是否对应相同;

确定模块442,可以用于若所述第一水印信息与所述第二水印信息中的多个信息字段均对应相同,则确定所述加密电子文件为合法文件;所述确定模块442,还可以用于若存在至少一个信息字段不对应相同,则确定所述加密电子文件为非法文件。

需要说明的是,本实施例提供的一种电子文件的解密装置所涉及各功能单元的其他相应描述,可以参考图2的对应描述,在此不再赘述。基于上述如图2所示方法,相应的,本实施例还提供了一种非易失性可读存储介质,其上存储有计算机可读指令,该计算机可读指令被处理器执行时实现上述如图2所示的电子文件的解密方法。基于这样的理解,本申请的技术方案可以以软件产品的形式体现出来,该软件产品可以存储在一个非易失性存储介质(可以是CD-ROM, U盘,移动硬盘等)中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例所述的方法。基于上述如图1至图2所示的方法,以及图3至图6所示的虚拟装置实施例,为了实现上述目的,本申请实施例还提供了一种计算机设备,具体可以为个人计算机、服务器、网络设备等,该实体设备包括非易失性可读存储介质和处理器;非易失性可读存储介质,用于存储计算机可读指令;处理器,用于执行计算机可读指令以实现上述如图1至图2所示的电子文件的加密、解密的方法。

可选地,该计算机设备还可以包括用户接口、网络接口、摄像头、射频(Radio Frequency, RF)电路,传感器、音频电路、Wi-Fi模块等等。用户接口可以包括显示屏(Display)、输入单元比如键盘(Keyboard)等,可选用户接口还可以包括USB接口、读卡器接口等。网络接口可选的可以包括标准的有线接口、无线接口(如蓝牙接口、Wi-Fi接口)等。本领域技术人员可以理解,本实施例提供的电子文件的加密、解密的方法对应的实体设备结构并不构成对该实体设备的限定,可以包括更多或更少的部件,或者组合某些部件,或者不同的部件布置。存储介质中还可以包括操作系统、网络通信模块。操作系统是管理上述计算机设备硬件和软件资源的程序,支持信息处理程序以及其它软件和/或程序的运

行。网络通信模块用于实现存储介质内部各组件之间的通信,以及与该实体设备中其它硬件和软件之间通信。通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到本申请可以借助软件加必要的通用硬件平台的方式来实现,也可以通过硬件实现。通过应用本申请的技术方案,与目前现有技术相比,通过对初始电子印章进行加密,得到电子加密印章信息,以及对加载有电子加密印章信息的电子文件进行二次加密,得到加密电子文件提高了电子文件在审批并加盖印章的过程中安全性,避免将加密电子文件向目的地址发送过程中第三方篡改加密电子文件。

本领域技术人员可以理解附图只是一个优选实施场景的示意图,附图中的模块或流程并不一定是实施本申请所必须的。本领域技术人员可以理解实施场景中的装置中的模块可以按照实施场景描述进行分布于实施场景的装置中,也可以进行相应变化位于不同于本实施场景的一个或多个装置中。上述实施场景的模块可以合并为一个模块,也可以进一步拆分成多个子模块。上述本申请序号仅仅为了描述,不代表实施场景的优劣。以上公开的仅为本申请的几个具体实施场景,但是,本申请并非局限于此,任何本领域的技术人员能思之的变化都应落入本申请的保护范围。

权 利 要 求 书

1.一种电子文件的加密方法，包括：

获取电子加密印章信息以及第一电子文件，所述电子加密印章信息包括通过 RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；

将所述电子加密印章信息加载在所述第一电子文件中，获得第二电子文件；

将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密，获得用以发送至目的地址的加密电子文件。

2.根据权利要求 1 所述的方法，所述水印信息中包括用于审批文件的多个信息字段，所述获取电子加密印章信息包括：

从所述水印信息中提取用于审批文件的多个信息字段；

将所述用于审批文件的多个信息字段按照预设审批顺序进行排序组成审批链数据；

将所述审批链数据和所述初始电子印章进行加密后，获得电子加密印章信息。

3.根据权利要求 1 所述的方法，在所述获取电子加密印章信息之前，所述方法还包括：

通过对物理印章进行处理，得到存储为预设格式的数字数据，将所述预设格式的数字数据作为初始电子印章。

4.一种电子文件的解密方法，包括：

接收加密电子文件，所述加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件；

根据预设解密算法对所述加密电子文件进行解密，获得第二电子文件和第一水印信息，所述第二电子文件包括电子加密印章信息，所述电子加密印章信息包括通过 RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；

通过 RSA 密钥中的公钥对所述电子加密印章信息进行解密，获得第二水印信息；

根据所述第一水印信息和所述第二水印信息，确定所述第一水印信息与所述第二水印信息是否相同；

若相同，则确定所述加密电子文件为合法文件；

若不相同，则确定所述加密电子文件为非法文件。

5.根据权利要求 4 所述的方法，所述第一水印信息和所述第二水印信息中包括用于审批文件的多个信息字段，所述根据所述第一水印信息和所述第二水印信息，确定所述第一水印信息与所述第二水印信息是否相同包括：

比较所述第一水印信息中的用于审批文件的多个信息字段与所述第二水印信息中用于审批文件的多个信息字段是否对应相同；

若所述第一水印信息与所述第二水印信息中的多个信息字段均对应相同，则确定所述加密电子文件为合法文件；

若存在至少一个信息字段不对应相同，则确定所述加密电子文件为非法文件。

6.根据权利要求 5 所述的方法，在所述确定所述加密电子文件为合法文件之后，还包括：

将第一水印信息或所述第二水印信息通过预设转换算法，转换为目标字符或目标二维码；

将所述目标字符或目标二维码加载在所述第二电子文件中输出。

7.一种电子文件的加密装置，包括：

获取单元，用于获取电子加密印章信息以及第一电子文件，所述电子加密印章信息包括通过 RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；

加载单元，用于将所述电子加密印章信息加载在所述第一电子文件中，获得第二电子文件；

加密单元，用于将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密，获得用以发送至目的地址的加密电子文件。

8.根据权利要求 7 所述的装置，所述水印信息中包括用于审批文件的多个信息字段；所述获取单元包括：

提取模块，用于从所述水印信息中提取用于审批文件的多个信息字段；

排序模块，用于将所述用于审批文件的多个信息字段按照预设审批顺序进行排序组成审批链数据；

加密模块，用于将所述审批链数据和所述初始电子印章进行加密后，获得电子加密印章信息。

9.根据权利要求 7 所述的装置，所述装置还包括：

处理单元，用于在所述获取电子加密印章信息之前，通过对物理印章进行处理，得到存储为预设格式的数字数据，将所述预设格式的数字数据作为初始电子印章。

10.一种电子文件的解密装置，包括：

接收单元，用于获取第二加密电子文件，所述第二加密电子文件包括将第二电子文件和所述水印信息一起通过预设加密算法进行加密获得的电子文件，所述第二电子文件包括加载有所述电子加密印章的电子文件，所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；

第一解密单元，用于根据预设解密算法对所述第二加密电子文件进行解密，获得电子文件和第一水印信息；

第二解密单元，用于通过RSA密钥中的公钥对所述电子加密印章信息进行解密，获得第二水印信息；

确定单元，用于根据所述第一水印信息和所述第二水印信息，确定所述第一水印信息与所述第二水印信息是否相同；若相同，则确定所述电子文件为合格的所述第二电子文件；若不相同，则确定所述电子文件为不合格文件。

11.根据权利要求10所述的装置，所述第一水印信息和所述第二水印信息中包括用于审批文件的多个信息字段；所述确定单元包括：

比较模块，用于比较所述第一水印信息中的用于审批文件的多个信息字段与所述第二水印信息中用于审批文件的多个信息字段是否对应相同；

确定模块，用于若所述第一水印信息与所述第二水印信息中的多个信息字段均对应相同，则确定所述加密电子文件为合法文件；

所述确定模块，还用于若存在至少一个信息字段不对应相同，则确定所述加密电子文件为非法文件。

12.根据权利要求11所述的装置，所述装置还包括：

转换单元，用于在所述确定所述加密电子文件为合法文件之后，将第一水印信息或所述第二水印信息通过预设转换算法，转换为目标字符或目标二维码；

输出单元，用于将所述目标字符或目标二维码加载在所述第二电子文件中输出。

13.一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述处理器执行电子文件的加密方法的步骤：获取电子加密印章信息以及第一电子文件，所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；将所述电子加密印章信息加载在所述第一电子文件中，获得第二电子文件；将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密，获得用以发送至目的地址的加密电子文件。

14.根据权利要求13所述的计算机设备，所述水印信息中包括用于审批文件的多个信息字段；所述计算机可读指令被所述处理器执行时，使得所述处理器执行所述获取电子加密印章信息包括：从所述水印信息中提取用于审批文件的多个信息字段；将所述用于审批文件的多个信息字段按照预设审批顺序进行排序组成审批链数据；将所述审批链数据和所述初始电子印章进行加密后，获得电子加密印章信息。

15.根据权利要求13所述的计算机设备，所述计算机可读指令被所述处理器执行时，使得所述处理器执行电子文件的解密方法的步骤：接收加密电子文件，所述加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件；根据预设解密算法对所述加密电子文件进行解密，获得第二电子文件和第一水印信息，所述第二电子文件包括电子加密印章信息，所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；通过RSA密钥中的公钥对所述电子加密印章信息进行解密，获得第二水印信息；根据所述第一水印信息和所述第二水印信息，确定所述第一水印信息与所述第二水印信息是否相同；若相同，则确定所述加密电子文件为合法文件；若不相同，则确定所述加密电子文件为非法文件。

16.根据权利要求15所述的计算机设备，所述第一水印信息和所述第二水印信息中包括用于审批文件的多个信息字段；所述计算机可读指令被所述处理器执行时，使得所述处理器执行所述根据所述第一水印信息和所述第二水印信息，确定所述第一水印信息与所述第二水印信息是否相同包括：比较所述第一水印信息中的用于审批文件的多个信息字段与所述第二水印信息中用于审批文件的多个信息字段是否对应相同；若所述第一水印信息与所述第二水印信息中的多个信息字段均对应相同，则确定所述加密电子文件为合法文件；若存在至少一个信息字段不对应相同，则确定所述加密电子文件为非法文件。

17.一种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，使得一个或多个处理器执行电子文件的加密方法的步骤：获取电子加密印章信息以及第一电子文件，所述电子加密印章信息包括通过RSA密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息；将所述电子加密印章信息加载在所述第一电子文件中，获得第二电子文件；将所述第二电子文件和所述水印信息一起通过预设加密算法进行加密，获得用以发送至目的地址的加密电子文件。

18.根据权利要求 17 所述的存储介质,所述水印信息中包括用于审批文件的多个信息字段;所述计算机可读指令被一个或多个处理器执行时,使得一个或多个处理器执行所述获取电子加密印章信息包括:从所述水印信息中提取用于审批文件的多个信息字段;将所述用于审批文件的多个信息字段按照预设审批顺序进行排序组成审批链数据;将所述审批链数据和所述初始电子印章进行加密后,获得电子加密印章信息。

19.根据权利要求 17 所述的存储介质,所述计算机可读指令被一个或多个处理器执行时,使得一个或多个处理器执行电子文件的解密方法的步骤:接收加密电子文件,所述加密电子文件为将第二电子文件和水印信息一起通过预设加密算法进行加密获得的电子文件;根据预设解密算法对所述加密电子文件进行解密,获得第二电子文件和第一水印信息,所述第二电子文件包括电子加密印章信息,所述电子加密印章信息包括通过 RSA 密钥中的私钥对水印信息和初始电子印章进行加密后获得的信息;通过 RSA 密钥中的公钥对所述电子加密印章信息进行解密,获得第二水印信息;根据所述第一水印信息和所述第二水印信息,确定所述第一水印信息与所述第二水印信息是否相同;若相同,则确定所述加密电子文件为合法文件;若不相同,则确定所述加密电子文件为非法文件。

20.根据权利要求 19 所述的存储介质,所述第一水印信息和所述第二水印信息中包括用于审批文件的多个信息字段;所述计算机可读指令被一个或多个处理器执行时,使得一个或多个处理器执行所述根据所述第一水印信息和所述第二水印信息,确定所述第一水印信息与所述第二水印信息是否相同包括:比较所述第一水印信息中的用于审批文件的多个信息字段与所述第二水印信息中用于审批文件的多个信息字段是否对应相同;若所述第一水印信息与所述第二水印信息中的多个信息字段均对应相同,则确定所述加密电子文件为合法文件;若存在至少一个信息字段不对应相同,则确定所述加密电子文件为非法文件。

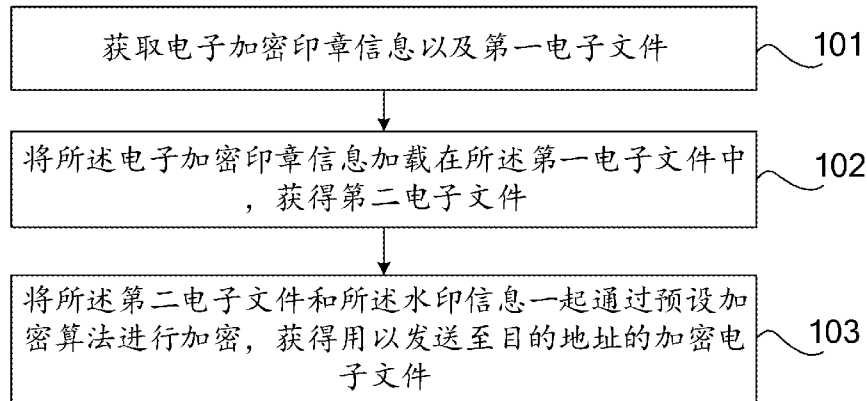


图 1

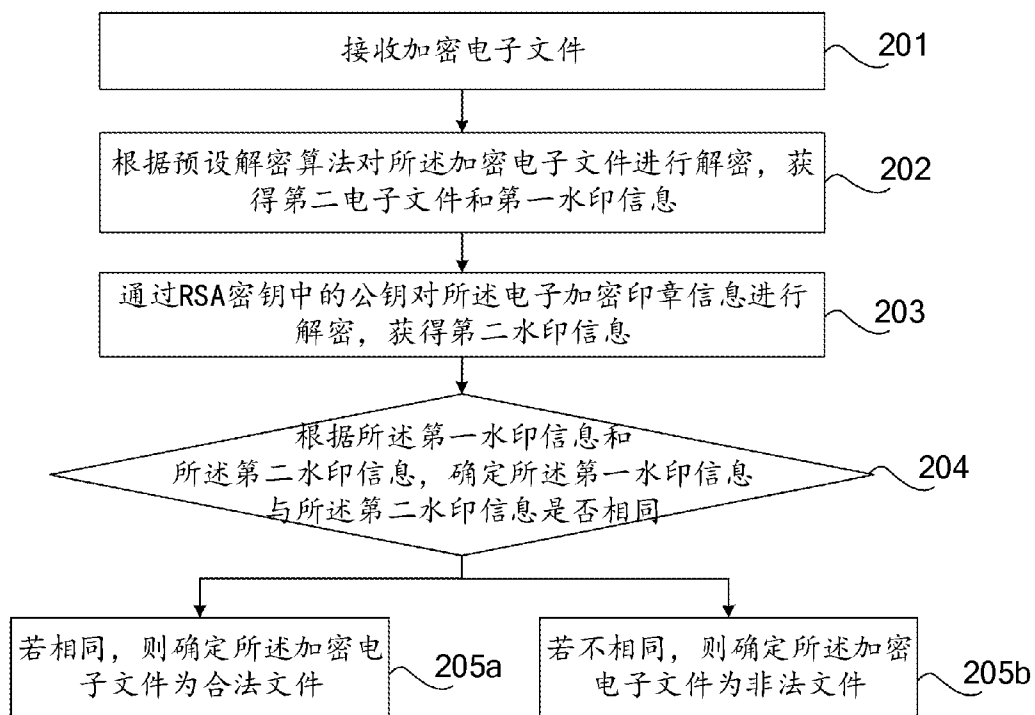


图 2

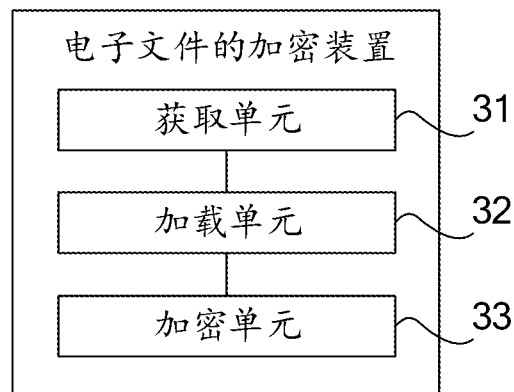


图 3

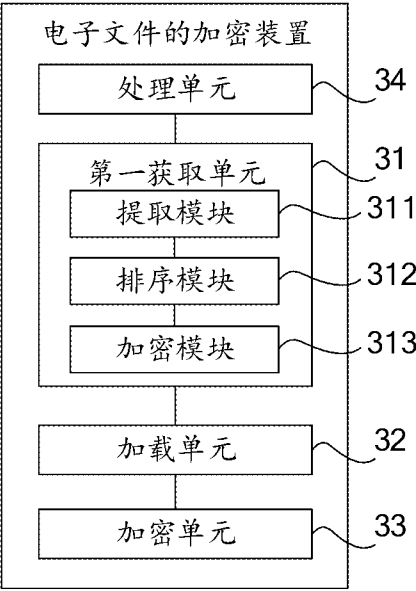


图 4

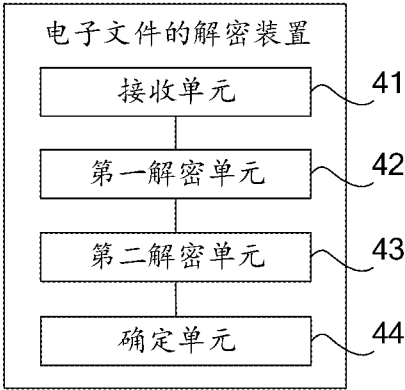


图 5

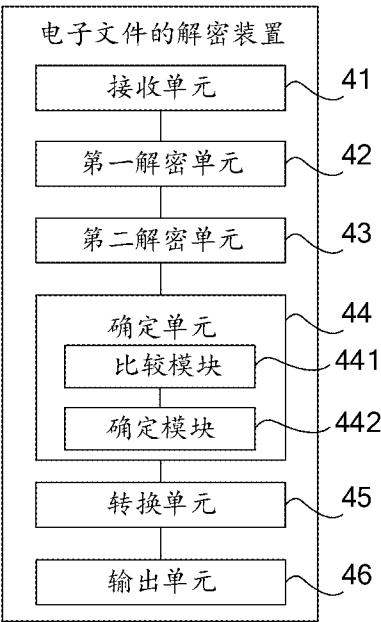


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/118412

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00(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 G06K

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)

CNPAT, CNKI, EPODOC, WPI, IEEE: 加密, 第一, 第二, 水印, 印章, 密钥, 公钥, 私钥, 篡改, first, second, waterprint, encrypt
+, decrypt+, key, tamper**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110069906 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 30 July 2019 (2019-07-30) description, paragraphs [0066]-[0132]	1-20
A	CN 105989253 A (WANFANG DATA CO., LTD. et al.) 05 October 2016 (2016-10-05) claims 1, 2, 5 and 6	1-20
A	CN 109274644 A (HUAWEI TECHNOLOGIES CO., LTD.) 25 January 2019 (2019-01-25) entire document	1-20
A	EP 1847064 A1 (YUEN, Pakkay) 24 October 2007 (2007-10-24) 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

12 February 2020

Date of mailing of the international search report

19 February 2020

Name and mailing address of the ISA/CN

**China National Intellectual Property Administration (ISA/
CN)**
**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/CN2019/118412

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110069906	A	30 July 2019	None			
CN	105989253	A	05 October 2016	None			
CN	109274644	A	25 January 2019	None			
EP	1847064	A1	24 October 2007	CA	2595313	A1	03 August 2006
				KR	20070108186	A	08 November 2007
				US	2006193472	A1	31 August 2006
				CN	101156347	A	02 April 2008
				AU	2006208377	A1	03 August 2006
				RU	2007132196	A	10 March 2009
				US	2010257368	A1	07 October 2010
				MX	2007008936	A	06 December 2007
				BR	PI0606238	A2	09 June 2009
				WO	2006079277	A1	03 August 2006
				ZA	200707007	A	26 November 2008
				JP	2008529044	A	31 July 2008
				IN	200706510	P1	07 September 2007

国际检索报告

国际申请号

PCT/CN2019/118412

A. 主题的分类

G06F 21/00 (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 G06K

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, EPDOC, WPI, IEEE: 加密, 第一, 第二, 水印, 印章, 密钥, 公钥, 私钥, 篡改, first, second, watermark, encrypt+, decrypt+, key, tamper

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 110069906 A (平安科技深圳有限公司) 2019年 7月 30日 (2019 - 07 - 30) 说明书第[0066]-[0132]段	1-20
A	CN 105989253 A (北京万方数据股份有限公司 等) 2016年 10月 5日 (2016 - 10 - 05) 权利要求1-2, 5-6	1-20
A	CN 109274644 A (华为技术有限公司) 2019年 1月 25日 (2019 - 01 - 25) 全文	1-20
A	EP 1847064 A1 (YUEN, Pak Kay) 2007年 10月 24日 (2007 - 10 - 24) 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

2020年 2月 12日

国际检索报告邮寄日期

2020年 2月 19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

姚楠

电话号码 86-(10)-53961521

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/118412

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	110069906	A	2019年 7月 30日	无			
CN	105989253	A	2016年 10月 5日	无			
CN	109274644	A	2019年 1月 25日	无			
EP	1847064	A1	2007年 10月 24日	CA	2595313	A1	2006年 8月 3日
				KR	20070108186	A	2007年 11月 8日
				US	2006193472	A1	2006年 8月 31日
				CN	101156347	A	2008年 4月 2日
				AU	2006208377	A1	2006年 8月 3日
				RU	2007132196	A	2009年 3月 10日
				US	2010257368	A1	2010年 10月 7日
				MX	2007008936	A	2007年 12月 6日
				BR	PI0606238	A2	2009年 6月 9日
				WO	2006079277	A1	2006年 8月 3日
				ZA	200707007	A	2008年 11月 26日
				JP	2008529044	A	2008年 7月 31日
				IN	200706510	P1	2007年 9月 7日