

(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
2017 年 2 月 16 日 (16.02.2017)



(10) 国际公布号
WO 2017/024628 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01) *G06F 21/60* (2013.01)
G06F 21/62 (2013.01)
- (21) 国际申请号: PCT/CN2015/088476
- (22) 国际申请日: 2015 年 8 月 30 日 (30.08.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510489174.3 2015 年 8 月 11 日 (11.08.2015) CN
- (71) 申请人: 宇龙计算机通信科技(深圳)有限公司
(YULONG COMPUTER TELECOMMUNICATION
SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中
国广东省深圳市南山区科技园北区梦溪道 2 号,
Guangdong 518057 (CN)。
- (72) 发明人: 钟焰涛 (ZHONG, Yantao); 中国广东省深
圳市南山区科技园北区梦溪道 2 号, Guangdong
518057 (CN)。 牛溢华 (NIU, Yihua); 中国广东省深
圳市南山区科技园北区梦溪道 2 号, Guangdong

518057 (CN)。 黄庆军 (HUANG, Qingjun); 中国广
东省深圳市南山区科技园北区梦溪道 2 号, Guang-
dong 518057 (CN)。 谭杨 (TAN, Yang); 中国广东省
深圳市南山区科技园北区梦溪道 2 号, Guangdong
518057 (CN)。

(74) 代理人: 北京友联知识产权代理事务所(普通合
伙) (YOU LINK INTELLECTUAL PROPERTY
LAW FIRM); 中国北京市海淀区学清路 8 号科技财
富中心 A 座 506 室尚志峰, Beijing 100192 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,
JP, KE, KG, KN, KP, KR, 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, SH, SL, SM, ST,
SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: ENCRYPTED INFORMATION STORAGE METHOD, ENCRYPTED INFORMATION STORAGE DEVICE, AND
TERMINAL

(54) 发明名称: 加密信息的存储方法、加密信息的存储装置和终端

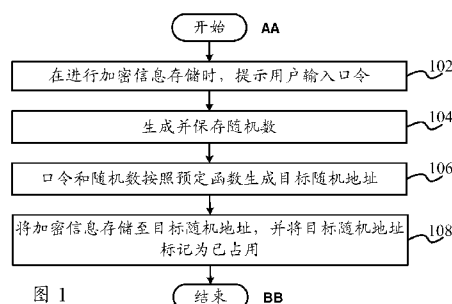


图 1

102 PROMPTING A USER TO INPUT A PASSWORD WHEN ENCRYPTED INFORMATION IS STORED
104 GENERATING AND SAVING A RANDOM NUMBER
106 THE PASSWORD AND THE RANDOM NUMBER GENERATING A TARGET RANDOM ADDRESS
ACCORDING TO A PRE-DETERMINED FUNCTION
108 STORING THE ENCRYPTED INFORMATION IN THE TARGET RANDOM ADDRESS AND
MARKING THE TARGET RANDOM ADDRESS AS BEING OCCUPIED
AA START
BB END

(57) Abstract: Provided are an encrypted information storage method, an encrypted information storage device, and a terminal. The encrypted information storage method comprises: prompting a user to input a password when encrypted information is stored; generating and saving a random number; the password and the random number generating a target random address according to a pre-determined function; and storing the encrypted information in the target random address and marking the target random address as occupied. By means of the technical solution, encrypted information can be randomly stored in a target random address, thereby avoiding the case where a lawbreaker acquires the storage position of the encrypted information to then steal the encrypted information about a user, so that the security of the encrypted information is improved.

(57) 摘要: 本发明提出了一种加密信息的存储方法、加密信息的存储装置和终端, 其中, 加密信息的存储方法包括: 在进行加密信息存储时, 提示用户输入口令; 生成并保存随机数; 口令和随机数按照预定函数生成目标随机地址; 以及将加密信息存储至目标随机地址, 并将目标随机地址标记为已占用。通过该技术方案, 能够将加密信息随机存储至目标随机地址中, 避免了不法分子获取存储加密信息的存储位置, 进而窃取用户的加密信息, 提升了加密信息的安全性。



WO 2017/024628 A1



(84) **指定国** (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, 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))。

说明书

加密信息的存储方法、加密信息的存储装置和终端

技术领域

5 本发明涉及终端技术领域，具体而言，涉及一种加密信息的存储方法、一种加密信息的存储装置和一种终端。

背景技术

10 目前，越来越多的智能终端具有生物特征识别功能，为了保证生物特征模板在终端中存储的安全性，目前有多种存储方案，例如将生物特征模板采用加密存储或将生物特征模板存储于系统的安全区域等。

但是，采用加密存储时，当用户使用密钥进行解密，或者不法分子攻击存储区域时，可能会导致生物特征模板的泄露，并且，如果黑客取得终端的系统权限存储在安全区域的生物特征模板同样会泄露。

15 因此，需要一种新的技术方案，可以将加密信息随机存储至目标随机地址中，进一步提升加密信息的安全性。

发明内容

20 本发明正是基于上述问题，提出了一种新的技术方案，可以将加密信息随机存储至目标随机地址中，进一步提升加密信息的安全性。

有鉴于此，本发明的第一方面提出了一种加密信息的存储方法，用于终端，包括：在进行加密信息存储时，提示用户输入口令；生成并保存随机数；所述口令和所述随机数按照预定函数生成目标随机地址；以及将所述加密信息存储至所述目标随机地址，并将所述目标随机地址标记为已占
25 用。

在该技术方案中，能够利用用户输入口令和随机获取的随机数，通过预定函数来生成用于存储加密信息的目标随机地址，其中，加密信息存储于终端中的用户数据分区内，用户数据分区内的存储单元以块为单位，存储加密信息的目标随机地址就是用户数据分区内的偏移地址，例如，预定

函数是哈希函数，则目标随机地址的计算公式为：

$$A=[\text{hash}(\text{password}, s) \bmod]b,$$

其中，A 是目标随机地址，hash 是哈希函数，password 是口令，s 是随机数，mod 是取模运算，b 是用户数据分区块数。

- 5 另外，该加密信息包括但不限于下列之一或其组合：生物特征模板、字符信息、手势信息等。

通过该技术方案，能够将加密信息随机存储至目标随机地址中，避免了不法分子获取存储加密信息的存储位置，进而窃取用户的加密信息，提升了加密信息的安全性。

- 10 在上述技术方案中，优选地，在所述将所述加密信息存储至所述目标随机地址之前，还包括：判断所述目标随机地址是否已经被占用；如果所述目标随机地址已经被占用，则重新生成所述随机数，并重复根据所述口令和所述随机数按照预定函数生成所述目标随机地址的步骤，否则，直接进行到将所述加密信息存储至所述目标随机地址的步骤。

- 15 在该技术方案中，在目标随机地址已经被占用时，强行将加密信息存储至该目标随机地址，则存储在该目标随机地址的原始信息就会丢失，因此，为了避免这种情况的出现，需要在获取的目标随机地址已经被占用时，重新获取目标随机地址，直至获取的目标随机未被占用，再将加密信息存储到该目标随机地址中；如果目标随机未被占用，就可以直接将加密
20 信息存储到该目标随机地址中。这样，避免了存储在目标随机地址中的原始信息丢失的问题，提高了用户体验。

- 在上述技术方案中，优选地，还包括：在读取所述加密信息时，提示用户输入所述口令；根据所述口令，获取所述随机数；根据所述口令和所述随机数，按照所述预定函数获取存储所述加密信息的所述目标随机地
25 址；以及从所述目标随机地址中读取所述加密信息。

在该技术方案中，当用户想要读取加密信息时，就可以根据提示输入相应口令，这样，终端就可以判断该相应口令与存储的口令是否一致，如果一致，就可以获取目标随机地址并读取其中的加密信息，否则，无法读取加密信息。通过该技术方案，用户能够通过正确的口令读取存储于目标

随机地址中的加密信息，为用户的读取过程提供了便利性。

在上述技术方案中，优选地，还包括：在将所述目标随机地址标记为已占用后，创建所述口令与所述目标随机地址的映射关系，并存储所述映射关系；在读取所述加密信息时，提示用户输入读取口令；判断所述读取口令与所述口令是否匹配；在判定所述读取口令与所述口令时，获取与所
5 述口令对应的映射关系，以通过所述映射关系获取所述目标随机地址；以及从所述目标随机地址中读取所述加密信息。

在该技术方案中，由于口令与目标随机地址是一一对应的，因此，可以创建口令与目标随机地址的映射关系，这样在用户想要读取加密信息
10 时，就可以输入与该口令相匹配的读取口令，并直接利用该映射关系获取目标随机地址，进而读取存储在目标随机地址中的加密信息。通过该技术方案，利用口令通过该映射关系能够直接获取目标随机地址，并读取其中的加密信息，进一步提高了读取加密信息的快捷性。

在上述技术方案中，优选地，还包括：在所述加密信息被读取之后，
15 或在接收到用户输入的新口令时，重新生成并保存新随机数；根据所述新口令和所述新随机数，按照所述预定函数生成新目标随机地址；将所述加密信息存储至所述新目标随机地址，并将所述新目标随机地址标记为已占用，同时删除保存在所述目标随机地址的所述加密信息。

在该技术方案中，如果目标随机地址中的加密信息已经被读取，则需要重新获取新随机数，并重新生成新目标随机地址将加密信息存储至其中，为了节省存储空间，还需要将原来的目标随机地址中的加密信息删除；
20

如果用户想要修改口令，就可以输入新口令，这样就可以重新生成新目标随机地址，以便加密信息能够存储到新目标随机地址中，这样防止了
25 因口令泄露而导致生物特征模板被窃取的问题，进一步保证了加密信息的安全，并且为了节省存储空间，还将原来的目标随机地址中的加密信息删除。

另外，删除方式可以用随机值覆盖目标随机地址中存储的加密信息，也可以将目标随机地址标记为空闲。

通过上述技术方案，在用户每次读取完存储至目标随机地址中的加密信息，以及用户需要更改口令之后，都能重新更换目标随机地址，避免了被不法分子窃取加密信息的问题。

5 本发明的第二方面提出了一种加密信息的存储装置，用于终端，包括：提示输入单元，用于在进行加密信息存储时，提示用户输入口令；生成单元，用于生成并保存随机数；所述生成单元还用于：所述口令和所述随机数按照预定函数生成目标随机地址；以及加密信息的存储装置还包括：存储单元，用于将所述加密信息存储至所述目标随机地址，并将所述目标随机地址标记为已占用。

10 在该技术方案中，能够利用用户输入口令和随机获取的随机数，通过预定函数来生成用于存储加密信息的目标随机地址，其中，加密信息存储于终端中的用户数据分区内，用户数据分区内的存储单元以块为单位，存储加密信息的目标随机地址就是用户数据分区内的偏移地址，例如，预定函数是哈希函数，则目标随机地址的计算公式为：

15
$$A=[\text{hash}(\text{password}, s) \bmod]b,$$

其中，A 是目标随机地址，hash 是哈希函数，password 是口令，s 是随机数，mod 是取模运算，b 是用户数据分区块数。

另外，该加密信息包括但不限于下列之一或其组合：生物特征模板、字符信息、手势信息等。

20 通过该技术方案，能够将加密信息随机存储至目标随机地址中，避免了不法分子获取存储加密信息的存储位置，进而窃取用户的加密信息，提升了加密信息的安全性。

在上述技术方案中，优选地，还包括：判断单元，用于判断所述目标随机地址是否已经被占用；所述生成单元还用于：如果所述目标随机地址
25 已经被占用，则重新生成所述随机数，并重复根据所述口令和所述随机数按照预定函数生成所述目标随机地址的步骤；所述存储单元还用于：如果所述目标随机地址未被占用，直接进行到将所述加密信息存储至所述目标随机地址的步骤。

在该技术方案中，在目标随机地址已经被占用时，强行将加密信息存

储至该目标随机地址，则存储在该目标随机地址的原始信息就会丢失，因此，为了避免这种情况的出现，需要在获取的目标随机地址已经被占用时，重新获取目标随机地址，直至获取的目标随机未被占用，再将加密信息存储到该目标随机地址中；如果目标随机未被占用，就可以直接将加密信息存储到该目标随机地址中。这样，避免了存储在目标随机地址中的原始信息丢失的问题，提高了用户体验。

在上述技术方案中，优选地，所述提示输入单元还用于：在读取所述加密信息时，提示用户输入所述口令；加密信息的存储装置还包括：获取单元，用于根据所述口令，获取所述随机数；所述获取单元还用于：根据所述口令和所述随机数，按照所述预定函数获取存储所述加密信息的所述目标随机地址；以及加密信息的存储装置还包括：读取单元，用于从所述目标随机地址中读取所述加密信息。

在该技术方案中，当用户想要读取加密信息时，就可以根据提示输入相应口令，这样，终端就可以判断该相应口令与存储的口令是否一致，如果一致，就可以获取目标随机地址并读取其中的加密信息，否则，无法读取加密信息。通过该技术方案，用户能够通过正确的口令读取存储于目标随机地址中的加密信息，为用户的读取过程提供了便利性。

在上述技术方案中，优选地，创建单元，用于在将所述目标随机地址标记为已占用后，创建所述口令与所述目标随机地址的映射关系，并存储所述映射关系；提示输入单元还用于：在读取所述加密信息时，提示用户输入读取口令；所述判断单元还用于：判断所述读取口令与所述口令是否匹配；所述加密信息的存储装置还包括：所述获取单元还用于：在判定所述读取口令与所述口令时，获取与所述口令对应的映射关系，以通过所述映射关系获取所述目标随机地址；以及所述获取单元还用于：从所述目标随机地址中读取所述加密信息。

在该技术方案中，由于口令与目标随机地址是一一对应的，因此，可以创建口令与目标随机地址的映射关系，这样在用户想要读取加密信息时，就可以输入与该口令相匹配的读取口令，并直接利用该映射关系获取目标随机地址，进而读取存储在目标随机地址中的加密信息。通过该技术

方案，利用口令通过该映射关系能够直接获取目标随机地址，并读取其中的加密信息，进一步提高了读取加密信息的快捷性。

在上述技术方案中，优选地，所述生成单元还用于：在所述加密信息被读取之后，或在接收到用户输入的新口令时，重新生成并保存新随机数；所述生成单元还用于：根据所述新口令和所述新随机数，按照所述预定函数生成新目标随机地址；所述存储单元还用于：将所述加密信息存储至所述新目标随机地址，并将所述新目标随机地址标记为已占用，同时删除保存在所述目标随机地址的所述加密信息。

在该技术方案中，如果目标随机地址中的加密信息已经被读取，则需要重新获取新随机数，并重新生成新目标随机地址将加密信息存储至其中，为了节省存储空间，还需要将原来的目标随机地址中的加密信息删除；

如果用户想要修改口令，就可以输入新口令，这样就可以重新生成新目标随机地址，以便加密信息能够存储到新目标随机地址中，这样防止了因口令泄露而导致生物特征模板被窃取的问题，进一步保证了加密信息的安全，并且为了节省存储空间，还将原来的目标随机地址中的加密信息删除。

另外，删除方式可以用随机值覆盖目标随机地址中存储的加密信息，也可以将目标随机地址标记为空闲。

通过上述技术方案，在用户每次读取完存储至目标随机地址中的加密信息，以及用户需要更改口令之后，都能重新更换目标随机地址，避免了被不法分子窃取加密信息的问题。

本发明的第三方面提出了一种终端，包括：上述第二方面中任一项所述的加密信息存取装置，因此，具有和上述第二方面中任一项所述的加密信息存取装置相同的技术效果，在此不再赘述。

通过本发明的技术方案，能够将加密信息随机存储至目标随机地址中，避免了不法分子获取存储加密信息的存储位置，进而窃取用户的加密信息，提升了加密信息的安全性。

附图说明

图 1 示出了根据本发明的一个实施例的加密信息的存储方法的流程图；

图 2 示出了根据本发明的一个实施例的加密信息的存储装置的框图；

5 图 3 示出了根据本发明的一个实施例的终端的框图；

图 4 示出了根据本发明的另一个实施例的加密信息的存储装置的框图；

图 5 示出了图 4 示出的生物特征模板注册的流程图；

图 6 示出了图 4 示出的修改用户口令的流程图；

10 图 7 示出了图 4 示出的生物特征模板使用的流程图。

具体实施方式

为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的一个实施例的加密信息的存储方法的流程图。

如图 1 所示，根据本发明的一个实施例的加密信息的存储方法，用于终端，包括：步骤 102，在进行加密信息存储时，提示用户输入口令；步骤 104，生成并保存随机数；步骤 106，口令和随机数按照预定函数生成目标随机地址；步骤 108，将加密信息存储至目标随机地址，并将目标随机地址标记为已占用。

在该技术方案中，能够利用用户输入口令和随机获取的随机数，通过预定函数来生成用于存储加密信息的目标随机地址，其中，加密信息存储于终端中的用户数据分区内，用户数据分区内的存储单元以块为单位，存储加密信息的目标随机地址就是用户数据分区内的偏移地址。

例如，预定函数是哈希函数，则目标随机地址的计算公式为：

$$A=[\text{hash}(\text{password}, s) \bmod]b,$$

其中，A 是目标随机地址，hash 是哈希函数，password 是口令，s 是随机数，mod 是取模运算，b 是用户数据分区块数。

- 5 另外，该加密信息包括但不限于下列之一或其组合：生物特征模板、字符信息、手势信息等。

通过该技术方案，能够将加密信息随机存储至目标随机地址中，避免了不法分子获取存储加密信息的存储位置，进而窃取用户的加密信息，提升了加密信息的安全性。

- 10 在上述技术方案中，优选地，在步骤 108 之前，还包括：判断目标随机地址是否已经被占用；如果目标随机地址已经被占用，则重新生成随机数，并重复根据口令和随机数按照预定函数生成目标随机地址的步骤，否则，直接进行到将加密信息存储至目标随机地址的步骤。

- 15 在该技术方案中，在目标随机地址已经被占用时，强行将加密信息存储至该目标随机地址，则存储在该目标随机地址的原始信息就会丢失，因此，为了避免这种情况的出现，需要在获取的目标随机地址已经被占用时，重新获取目标随机地址，直至获取的目标随机未被占用，再将加密信息存储到该目标随机地址中；如果目标随机未被占用，就可以直接将加密信息存储到该目标随机地址中。这样，避免了存储在目标随机地址中的原始信息丢失的问题，提高了用户体验。
- 20

在上述技术方案中，优选地，还包括：在读取加密信息时，提示用户输入口令；根据口令，获取随机数；根据口令和随机数，按照预定函数获取存储加密信息的目标随机地址；以及从目标随机地址中读取加密信息。

- 25 在该技术方案中，当用户想要读取加密信息时，就可以根据提示输入相应口令，这样，终端就可以判断该相应口令与存储的口令是否一致，如果一致，就可以获取目标随机地址并读取其中的加密信息，否则，无法读取加密信息。通过该技术方案，用户能够通过正确的口令读取存储于目标随机地址中的加密信息，为用户的读取过程提供了便利性。

在上述技术方案中，优选地，还包括：在步骤 108 之后，创建口令与

目标随机地址的映射关系，并存储映射关系；在读取加密信息时，提示用户输入读取口令；判断读取口令与口令是否匹配；在判定读取口令与口令时，获取与口令对应的映射关系，以通过映射关系获取目标随机地址；以及从目标随机地址中读取加密信息。

- 5 在该技术方案中，由于口令与目标随机地址是一一对应的，因此，可以创建口令与目标随机地址的映射关系，这样在用户想要读取加密信息时，就可以输入与该口令相匹配的读取口令，并直接利用该映射关系获取目标随机地址，进而读取存储在目标随机地址中的加密信息。通过该技术方案，利用口令通过该映射关系能够直接获取目标随机地址，并读取其中
10 的加密信息，进一步提高了读取加密信息的快捷性。

- 在上述技术方案中，优选地，还包括：在加密信息被读取之后，或在接收到用户输入的新口令时，重新生成并保存新随机数；根据新口令和新随机数，按照预定函数生成新目标随机地址；将加密信息存储至新目标随机地址，并将新目标随机地址标记为已占用，同时删除保存在目标随机地址
15 的加密信息。

 在该技术方案中，如果目标随机地址中的加密信息已经被读取，则需要重新获取新随机数，并重新生成新目标随机地址将加密信息存储至其中，为了节省存储空间，还需要将原来的目标随机地址中的加密信息删除；

- 20 如果用户想要修改口令，就可以输入新口令，这样就可以重新生成新目标随机地址，以便加密信息能够存储到新目标随机地址中，这样防止了因口令泄露而导致生物特征模板被窃取的问题，进一步保证了加密信息的安全，并且为了节省存储空间，还将原来的目标随机地址中的加密信息删除。

- 25 另外，删除方式可以用随机值覆盖目标随机地址中存储的加密信息，也可以将目标随机地址标记为空闲。

 通过上述技术方案，在用户每次读取完存储至目标随机地址中的加密信息，以及用户需要更改口令之后，都能重新更换目标随机地址，避免了被不法分子窃取加密信息的问题。

图 2 示出了根据本发明的一个实施例的加密信息的存储装置的框图。

如图 2 所示, 根据本发明的一个实施例的加密信息的存储装置 200, 用于终端, 包括: 提示输入单元 202, 用于在进行加密信息存储时, 提示用户输入口令; 生成单元 204, 用于生成并保存随机数; 生成单元 204 还用于: 口令和随机数按照预定函数生成目标随机地址; 以及加密信息的存储装置 200 还包括: 存储单元 206, 用于将加密信息存储至目标随机地址, 并将目标随机地址标记为已占用。

在该技术方案中, 能够利用用户输入口令和随机获取的随机数, 通过预定函数来生成用于存储加密信息的目标随机地址, 其中, 加密信息存储于终端中的用户数据分区内, 用户数据分区内的存储单元 206 以块为单位, 存储加密信息的目标随机地址就是用户数据分区内的偏移地址, 例如, 预定函数是哈希函数, 则目标随机地址的计算公式为:

$$A=[\text{hash}(\text{password}, s) \bmod]b,$$

其中, A 是目标随机地址, hash 是哈希函数, password 是口令, s 是随机数, mod 是取模运算, b 是用户数据分区块数。

另外, 该加密信息包括但不限于下列之一或其组合: 生物特征模板、字符信息、手势信息等。

通过该技术方案, 能够将加密信息随机存储至目标随机地址中, 避免了不法分子获取存储加密信息的存储位置, 进而窃取用户的加密信息, 提升了加密信息的安全性。

在上述技术方案中, 优选地, 还包括: 判断单元 208, 用于判断目标随机地址是否已经被占用; 生成单元 204 还用于: 如果目标随机地址已经被占用, 则重新生成随机数, 并重复根据口令和随机数按照预定函数生成目标随机地址的步骤; 存储单元 206 还用于: 如果目标随机地址未被占用, 直接进行到将加密信息存储至目标随机地址的步骤。

在该技术方案中, 在目标随机地址已经被占用时, 强行将加密信息存储至该目标随机地址, 则存储在该目标随机地址的原始信息就会丢失, 因此, 为了避免这种情况的出现, 需要在获取的目标随机地址已经被占用时, 重新获取目标随机地址, 直至获取的目标随机未被占用, 再将加密信

息存储到该目标随机地址中；如果目标随机未被占用，就可以直接将加密信息存储到该目标随机地址中。这样，避免了存储在目标随机地址中的原始信息丢失的问题，提高了用户体验。

在上述技术方案中，优选地，提示输入单元 202 还用于：在读取加密信息时，提示用户输入口令；加密信息的存储装置 200 还包括：获取单元 210，用于根据口令，获取随机数；获取单元 210 还用于：根据口令和随机数，按照预定函数获取存储加密信息的目标随机地址；以及加密信息的存储装置 200 还包括：读取单元 212，用于从目标随机地址中读取加密信息。

在该技术方案中，当用户想要读取加密信息时，就可以根据提示输入相应口令，这样，终端就可以判断该相应口令与存储的口令是否一致，如果一致，就可以获取目标随机地址并读取其中的加密信息，否则，无法读取加密信息。通过该技术方案，用户能够通过正确的口令读取存储于目标随机地址中的加密信息，为用户的读取过程提供了便利性。

在上述技术方案中，优选地，创建单元 214，用于在将目标随机地址标记为已占用后，创建口令与目标随机地址的映射关系，并存储映射关系；提示输入单元 202 还用于：在读取加密信息时，提示用户输入读取口令；判断单元 208 还用于：判断读取口令与口令是否匹配；加密信息的存储装置 200 还包括：获取单元 210，用于在判定读取口令与口令时，获取与口令对应的映射关系，以通过映射关系获取目标随机地址；以及获取单元 210 还用于：从目标随机地址中读取加密信息。

在该技术方案中，由于口令与目标随机地址是一一对应的，因此，可以创建口令与目标随机地址的映射关系，这样在用户想要读取加密信息时，就可以输入与该口令相匹配的读取口令，并直接利用该映射关系获取目标随机地址，进而读取存储在目标随机地址中的加密信息。通过该技术方案，利用口令通过该映射关系能够直接获取目标随机地址，并读取其中的加密信息，进一步提高了读取加密信息的快捷性。

在上述技术方案中，优选地，生成单元 204 还用于：在加密信息被读取之后，或在接收到用户输入的新口令时，重新生成并保存新随机数；生

成单元 204 还用于：根据新口令和新随机数，按照预定函数生成新目标随机地址；存储单元 206 还用于：将加密信息存储至新目标随机地址，并将新目标随机地址标记为已占用，同时删除保存在目标随机地址的加密信息。

- 5 在该技术方案中，如果目标随机地址中的加密信息已经被读取，则需要重新获取新随机数，并重新生成新目标随机地址将加密信息存储至其中，为了节省存储空间，还需要将原来的目标随机地址中的加密信息删除；

10 如果用户想要修改口令，就可以输入新口令，这样就可以重新生成新目标随机地址，以便加密信息能够存储到新目标随机地址中，这样防止了因口令泄露而导致生物特征模板被窃取的问题，进一步保证了加密信息的安全，并且为了节省存储空间，还将原来的目标随机地址中的加密信息删除。

15 另外，删除方式可以用随机值覆盖目标随机地址中存储的加密信息，也可以将目标随机地址标记为空闲。

通过上述技术方案，在用户每次读取完存储至目标随机地址中的加密信息，以及用户需要更改口令之后，都能重新更换目标随机地址，避免了被不法分子窃取加密信息的问题。

图 3 示出了根据本发明的一个实施例的终端的框图。

20 如图 3 所示，根据本发明的一个实施例的终端 300，包括图 2 示出的加密信息存取装置 200，因此，具有和图 2 示出的加密信息存取装置 200 相同的技术效果，在此不再赘述。

图 4 示出了根据本发明的另一个实施例的加密信息的存储装置的框图。

25 如图 4 所示，加密信息的存储装置由生物特征模板注册单元 402、生物特征模板使用单元 404 和修改用户口令单元 406 组成。

其中，上述三个单元对应三个功能操作的流程，每个流程都会触发相应的寻址操作。

图 5 示出了图 4 示出的生物特征模板注册的流程图。

如图 5 所示, 生物特征模板注册包括: 步骤 502, 用户输入生物特征, 提取生物特征模板; 步骤 504, 提示用户输入用户口令; 步骤 506, 收到用户口令后, 生成一个随机数; 步骤 508, 根据用户口令和随机数计算目标随机地址; 步骤 510, 判断目标随机地址是否空闲, 如果判断结果
5 为是则进入步骤 512, 如果判断结果为否则进入步骤 506; 步骤 512, 将生物特征模板存储至目标随机地址; 步骤 514, 保存上述随机数。其中, 随机数不能和生物特征模板一起存储, 应该保存至可以直接读取的存储地址中; 步骤 516, 将目标随机地址标记为已占用。

图 6 示出了图 4 示出的修改用户口令的流程图。

10 如图 6 所示, 为了防止口令泄露后导致生物特征模板被窃取的问题, 允许用户修改用户口令, 具体包括: 步骤 602, 确定用户输入的输入口令与用户口令一致; 步骤 604, 提示用户输入新口令; 步骤 606, 重复确认用户的新口令; 步骤 608, 生成新随机数, 并根据新口令和新随机数生成新目标随机地址; 步骤 610, 将生物特征模板存储至新目标随机地址, 保
15 存新随机数将新目标随机地址标记为已占用; 步骤 612, 删除目标随机地址中存储的生物特征模板, 具体地, 删除方式可以用随机值覆盖目标随机地址中存储的生物特征模板, 也可以将目标随机地址标记为空闲。

图 7 示出了图 4 示出的生物特征模板使用的流程图。

如图 7 所示, 生物特征模板使用必须遵循的原则:

20 (1) 先寻址、后使用;

(2) 使用后要重新计算新目标随机地址, 将生物特征模板存入新目标随机地址中;

(3) 需要将原目标随机地址中的生物特征模板删除。

具体地流程包括: 步骤 702, 提示用户输入用户口令; 步骤 704, 读
25 取上一次存储的随机数; 步骤 706, 根据用户口令和随机数计算目标随机地址; 步骤 708, 读取生物特征模板; 步骤 710, 使用生物特征模板; 步骤 712, 生成一个新随机数; 步骤 714, 根据用户口令和新随机数计算新目标随机地址; 步骤 716, 判断目标随机地址是否空闲, 如果判断结果为是则进入步骤 718, 如果判断结果为否则进入步骤 712; 步骤 718, 将生

物特征模板存储至新目标随机地址；步骤 720，保存上述新随机数；步骤 722，将新目标随机地址标记为已占用；步骤 724，删除目标随机地址中存储的生物特征模板，具体地，删除方式可以用随机值覆盖目标随机地址中存储的生物特征模板，也可以将目标随机地址标记为空闲。

5 以上结合附图详细说明了本发明的技术方案，通过本发明的技术方案，能够将加密信息随机存储至目标随机地址中，避免了不法分子获取存储加密信息的存储位置，进而窃取用户的加密信息，提升了加密信息的安全性。

10 在本发明中，术语“第一”、“第二”、“第三”仅用于描述的目的，而不能理解为指示或暗示相对重要性。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。

15 在本说明书的描述中，术语“一个实施例”、“另一个实施例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或特点包含于本实用新型的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或实例。而且，描述的具体特征、结构、材料或特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

20 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

1. 一种加密信息的存储方法，用于终端，其特征在于，包括：

在进行加密信息存储时，提示用户输入口令；

5 生成并保存随机数；

所述口令和所述随机数按照预定函数生成目标随机地址；以及

将所述加密信息存储至所述目标随机地址，并将所述目标随机地址标记为已占用。

2. 根据权利要求 1 所述的加密信息的存储方法，其特征在于，在所

10 述将所述加密信息存储至所述目标随机地址之前，还包括：

判断所述目标随机地址是否已经被占用；

如果所述目标随机地址已经被占用，则重新生成所述随机数，并重复根据所述口令和所述随机数按照预定函数生成所述目标随机地址的步骤，否则，直接进行到将所述加密信息存储至所述目标随机地址的步骤。

15 3. 根据权利要求 2 所述的加密信息的存储方法，其特征在于，还包括：

在读取所述加密信息时，提示用户输入所述口令；

根据所述口令，获取所述随机数；

20 根据所述口令和所述随机数，按照所述预定函数获取存储所述加密信息的所述目标随机地址；以及

从所述目标随机地址中读取所述加密信息。

4. 根据权利要求 3 所述的加密信息的存储方法，其特征在于，还包括：

25 在将所述目标随机地址标记为已占用后，创建所述口令与所述目标随机地址的映射关系，并存储所述映射关系；

在读取所述加密信息时，提示用户输入读取口令；

判断所述读取口令与所述口令是否匹配；

在判定所述读取口令与所述口令时，获取与所述口令对应的映射关系，以通过所述映射关系获取所述目标随机地址；以及

从所述目标随机地址中读取所述加密信息。

5. 根据权利要求 3 或 4 所述的加密信息的存储方法，其特征在于，还包括：

在所述加密信息被读取之后，或在接收到用户输入的新口令时，重新生成并保存新随机数；

根据所述新口令和所述新随机数，按照所述预定函数生成新目标随机地址；

将所述加密信息存储至所述新目标随机地址，并将所述新目标随机地址标记为已占用，同时删除保存在所述目标随机地址的所述加密信息。

10 6. 一种加密信息的存储装置，用于终端，其特征在于，包括：

提示输入单元，用于在进行加密信息存储时，提示用户输入口令；

生成单元，用于生成并保存随机数；

所述生成单元还用于：所述口令和所述随机数按照预定函数生成目标随机地址；以及

15 加密信息的存储装置还包括：

存储单元，用于将所述加密信息存储至所述目标随机地址，并将所述目标随机地址标记为已占用。

7. 根据权利要求 6 所述的加密信息的存储装置，其特征在于，还包括：

20 判断单元，用于判断所述目标随机地址是否已经被占用；

所述生成单元还用于：如果所述目标随机地址已经被占用，则重新生成所述随机数，并重复根据所述口令和所述随机数按照预定函数生成所述目标随机地址的步骤；

25 所述存储单元还用于：如果所述目标随机地址未被占用，直接进行到将所述加密信息存储至所述目标随机地址的步骤。

8. 根据权利要求 7 所述的加密信息的存储装置，其特征在于，所述提示输入单元还用于：在读取所述加密信息时，提示用户输入所述口令；

加密信息的存储装置还包括：

获取单元，用于根据所述口令，获取所述随机数；

所述获取单元还用于：根据所述口令和所述随机数，按照所述预定函数获取存储所述加密信息的所述目标随机地址；以及

加密信息的存储装置还包括：

读取单元，用于从所述目标随机地址中读取所述加密信息。

- 5 9. 根据权利要求 8 所述的加密信息的存储装置，其特征在于，还包括：

创建单元，用于在将所述目标随机地址标记为已占用后，创建所述口令与所述目标随机地址的映射关系，并存储所述映射关系；

- 10 提示输入单元还用于：在读取所述加密信息时，提示用户输入读取口令；

所述判断单元还用于：判断所述读取口令与所述口令是否匹配；

所述获取单元还用于：在判定所述读取口令与所述口令时，获取与所述口令对应的映射关系，以通过所述映射关系获取所述目标随机地址；以及

- 15 所述获取单元还用于：从所述目标随机地址中读取所述加密信息。

10. 根据权利要求 8 或 9 所述的加密信息的存储装置，其特征在于，所述生成单元还用于：在所述加密信息被读取之后，或在接收到用户输入的新口令时，重新生成并保存新随机数；

- 20 所述生成单元还用于：根据所述新口令和所述新随机数，按照所述预定函数生成新目标随机地址；

所述存储单元还用于：将所述加密信息存储至所述新目标随机地址，并将所述新目标随机地址标记为已占用，同时删除保存在所述目标随机地址的所述加密信息。

- 25 11. 一种终端，其特征在于，包括如权利要求 6 至 10 中任一项所述的加密信息存取装置。

说明书附图

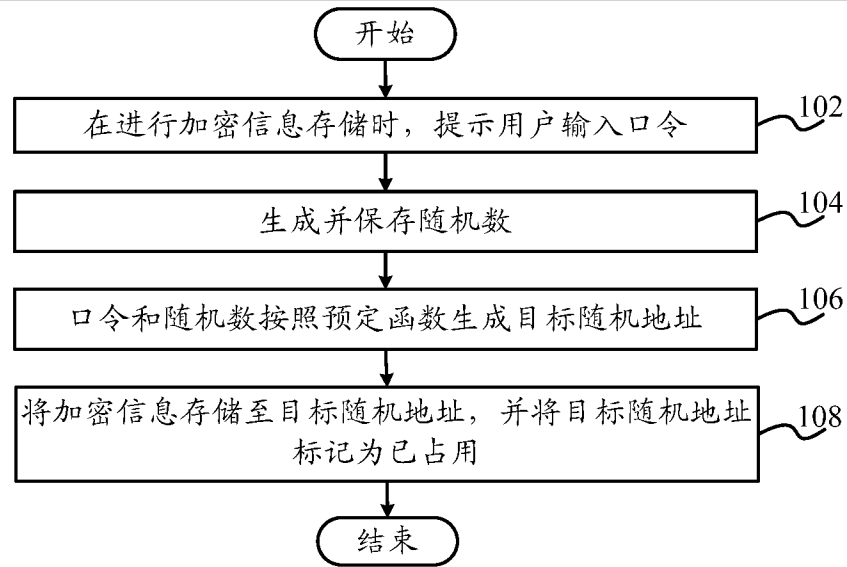


图 1



图 2



图 3

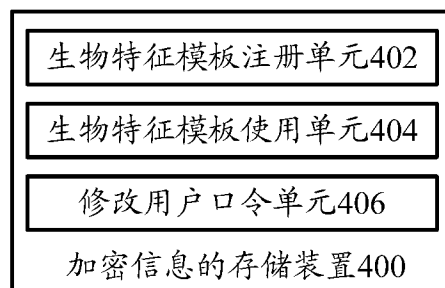


图 4

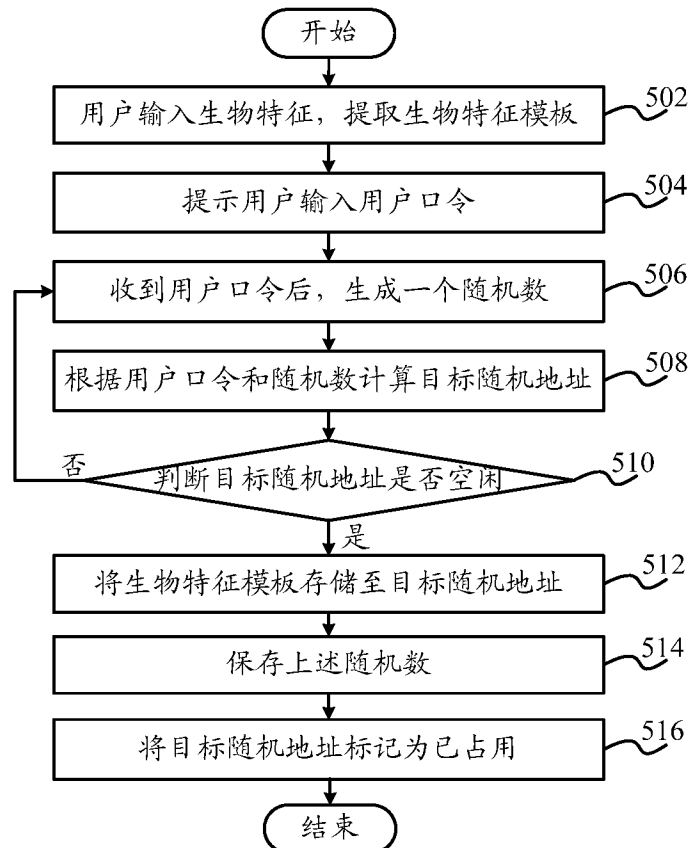


图 5

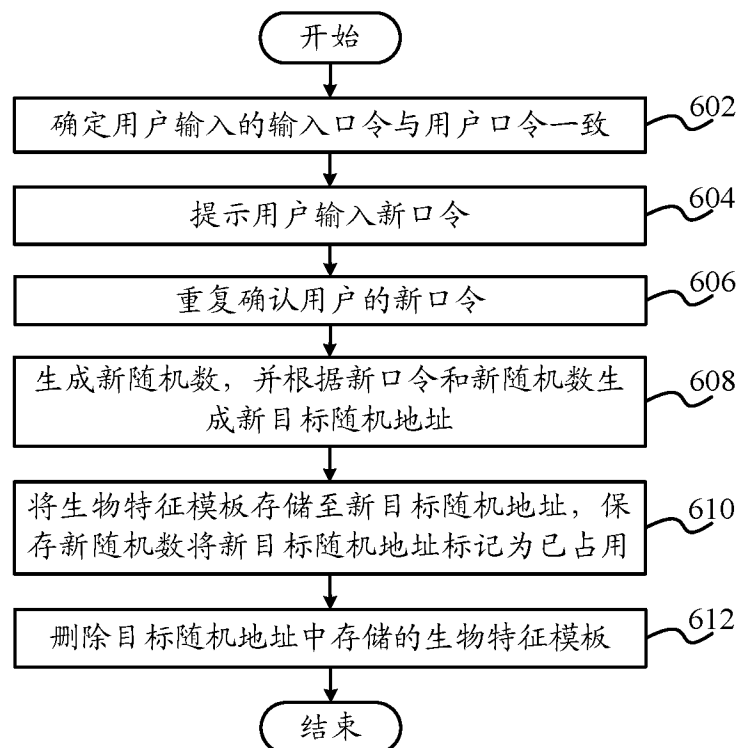


图 6

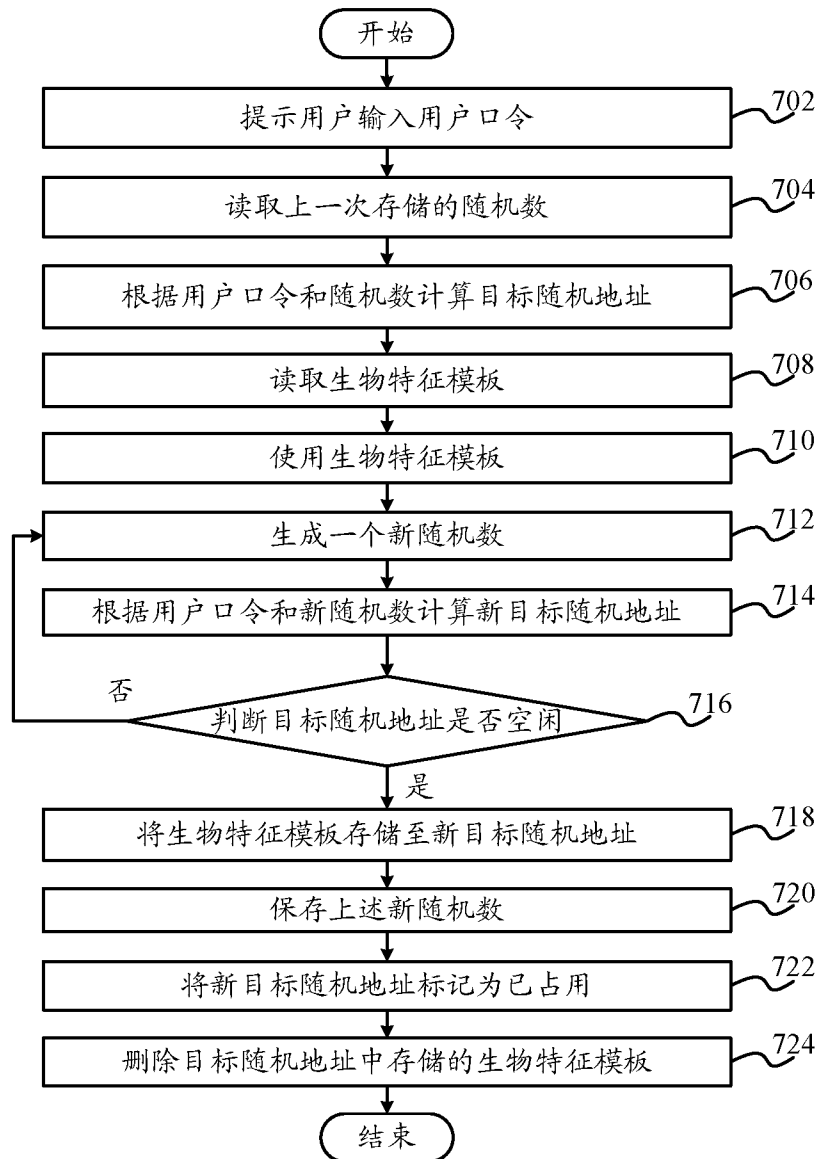


图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/088476

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i; G06F 21/62 (2013.01) i; G06F 21/60 (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)

H04L; 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; CNKI; DWPI; SIPOABS: biometric, biological, fingerprint, voice, voiceprint, retina, key, secret, password, random number, memor+, stor+, keep+, writ+, read+, client, user, comput+, generat+, calculat+, address, position, location

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000214944 A (TOSHIBA CORP.) 04 August 2000 (04.08.2000) claims 1 to 9, description, paragraphs [0021] to [0034]	1-11
A	CN 1527208 A (LENOVO BEIJING CO., LTD.) 08 September 2004 (08.09.2004) the whole document	1-11
A	CN 104573438 A (JIANGSU CINSEC INFORMATION TECHNOLOGY CO., LTD.) 29 April 2015 (29.04.2015) the whole document	1-11
A	US 8751804 B1 (DECHO CORP.) 10 June 2014 (10.06.2014) the whole document	1-11

☐ 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

21 April 2016

Date of mailing of the international search report

03 May 2016

Name and mailing address of the ISA
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

LIU, Jian

Telephone No. (86-10) 62411256

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/088476

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2000214944 A	04 August 2000	None	
CN 1527208 A	08 September 2004	CN 1234081 C	28 December 2005
CN 104573438A	29 April 2015	None	
US 8751804 B1	10 June 2014	None	

A. 主题的分类 H04L 9/32 (2006.01) i; G06F 21/62 (2013.01) i; G06F 21/60 (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) H04L; 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; CNKI; DWPI; SIPOABS: 生物, 指纹, 声波, 视网膜, 密钥, 密码, 口令, 随机数, 存储, 储存, 保存, 写入, 读出, 用户, 客户, 计算, 生成, 产生, 地址, 位置, biometric, biological, fingerprint, voice, voiceprint, retina, key, secret, password, random number, memor+, stor+, keep+, writ+, read+, client, user, comput+, generat+, calculat+, address, positon, location		
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
X	JP 2000214944 A (东芝株式会社) 2000年 8月 4日 (2000 - 08 - 04) 权利要求1-9, 说明书第[0021]-[0034]段	1-11
A	CN 1527208 A (联想北京有限公司) 2004年 9月 8日 (2004 - 09 - 08) 全文	1-11
A	CN 104573438 A (江苏华御信息技术有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-11
A	US 8751804 B1 (DECHO CORP) 2014年 6月 10日 (2014 - 06 - 10) 全文	1-11
☐ 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 2016年 4月 21日		国际检索报告邮寄日期 2016年 5月 3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		授权官员 刘俭 电话号码 (86-10) 62411256

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/088476

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)
JP	2000214944	A	2000年 8月 4日	无	
CN	1527208	A	2004年 9月 8日	CN 1234081 C	2005年 12月 28日
CN	104573438	A	2015年 4月 29日	无	
US	8751804	B1	2014年 6月 10日	无	

表 PCT/ISA/210（同族专利附件）（2009年7月）