

(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
2016 年 4 月 21 日 (21.04.2016)



(10) 国际公布号
WO 2016/058487 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2015/091247
- (22) 国际申请日: 2015 年 9 月 30 日 (30.09.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410549532.0 2014 年 10 月 16 日 (16.10.2014) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [GB/CN]; 英国开曼群岛大开曼乔治城资本大厦一座四层 847 号邮箱, Grand Cayman (GB)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 林钧燧 (LIN, Junsui) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。
- (74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.);

中国北京市朝阳区西坝河西里 28 号英特公寓 C 座 104, Beijing 100028 (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, 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)。

[见续页]

(54) Title: INFORMATION PROCESSING METHOD AND APPARATUS

(54) 发明名称: 一种信息处理方法及装置

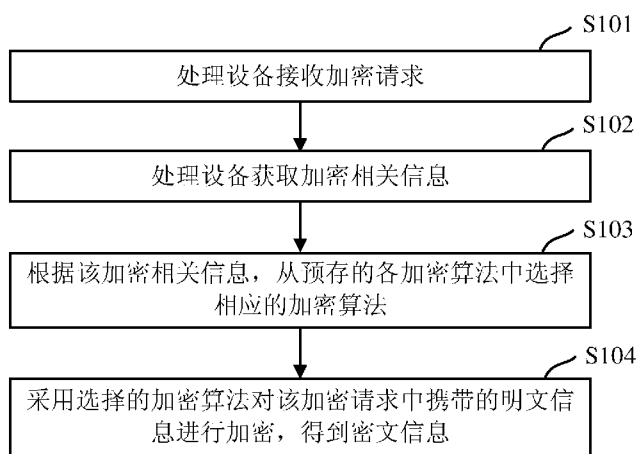


图 1 / FIG. 1

S101 RECEIVING, BY A PROCESSING DEVICE, AN ENCRYPTION REQUEST
S102 ACQUIRING, BY THE PROCESSING DEVICE, ENCRYPTION RELATED INFORMATION
S103 ACCORDING TO THE ENCRYPTION RELATED INFORMATION, SELECTING A CORRESPONDING ENCRYPTION ALGORITHM FROM VARIOUS PRE-STORED ENCRYPTION ALGORITHMS
S104 USING THE SELECTED ENCRYPTION ALGORITHM TO ENCRYPT PLAIN TEXT INFORMATION CARRIED IN THE ENCRYPTION REQUEST, TO OBTAIN CIPHER TEXT INFORMATION

(57) Abstract: Disclosed are an information processing method and apparatus. In the method, when a terminal receives an encryption request and acquires encryption related information, according to the encryption related information, a corresponding encryption algorithm is selected from various pre-stored encryption algorithms; and the selected encryption algorithm is used to encrypt plain text information carried in the encryption request, to obtain cipher text information. By means of the method, since a terminal selects an encryption algorithm according to encryption related information, while with regard to different encryption requests, the terminal may acquire different encryption related information, so as to select different encryption algorithms to encrypt plain text information carried in different encryption requests, and therefore the difficulty of an attacker decompiling and analysing an encryption program on the terminal is increased; in addition, the leakage of a single encryption algorithm and a corresponding encryption key may not threaten the security of all information stored in the terminal, thereby improving the information security.

(57) 摘要:

[见续页]

WO 2016/058487 A1

**本国际公布:**

— 包括国际检索报告(条约第 21 条(3))。

本申请公开了一种信息处理方法及装置。该方法当终端接收加密请求，并获取加密相关信息，根据该加密相关信息，从预存的各加密算法中选择相应的加密算法，以及采用选择的加密算法对该加密请求中携带的明文信息进行加密，得到密文信息。通过上述方法，由于终端是根据加密相关信息选择加密算法，而针对不同的加密请求，终端会获取到不同的加密相关信息，从而会选择不同的加密算法对不同加密请求中携带的明文信息进行加密，因此，增大了攻击者对终端上的加密程序反编译分析的难度，而且，单个加密算法与对应的加密密钥的泄露，也并不会威胁到该终端中保存的所有信息的安全，增强了信息安全性。

一种信息处理方法及装置

技术领域

本申请涉及计算机技术领域，尤其涉及一种信息处理方法及装置。

5 背景技术

随着计算机信息技术的发展，用户对信息安全的要求越来越高。

在现有技术中，终端一般采用相对安全的方式为用户存储敏感信息，如用户的个人信息、用户的应用信息等。

具体的，当终端存储这些敏感信息时，会采用某种加密算法和对应的加密
10 密钥对这些敏感信息进行加密，然后存储加密后的敏感信息。而当终端需要使用这些敏感信息时，则采用相应的解密算法和对应的解密密钥对加密后的敏感信息进行解密，从而获得这些敏感信息。

但是，由于终端对所有信息进行加密时都是使用同一种加密算法，一旦该
终端使用的加密算法和对应的加密密钥被破解或泄露，就会导致该终端中存储
15 的所有使用该加密算法加密的信息都有泄露的风险，降低了信息安全性。

发明内容

本申请实施例提供一种信息处理方法及装置，用以解决现有技术中终端对
所有信息进行加密时都是使用同一种加密算法，一旦该终端上的加密程序被攻
20 击者反编译分析，则该加密算法和对应的加密密钥可能会被破解或泄露，进而，
该终端中存储的所有使用该加密算法加密的信息都有泄露的风险，降低了信息
安全性的问题。

本申请实施例提供的一种信息处理方法，包括：

处理设备接收加密请求；并

25 获取加密相关信息；

根据所述加密相关信息，从预存的各加密算法中选择相应的加密算法；以及

采用选择的加密算法对所述加密请求中携带的明文信息进行加密，得到密文信息。

5 本申请实施例提供的一种信息处理装置，包括：

接收模块，用于接收加密请求；

获取模块，用于获取加密相关信息；

选择模块，用于根据所述加密相关信息，从预存的各加密算法中选择相应的加密算法；

10 加密模块，用于采用所述选择模块选择的加密算法对所述加密请求中携带的明文信息进行加密，得到密文信息。

本申请实施例提供的信息处理方法及装置，该方法终端接收加密请求，并获取加密相关信息，根据该加密相关信息，从预存的各加密算法中选择相应的加密算法，以及采用选择的加密算法对该加密请求中携带的明文信息进行加
15 密，得到密文信息。通过上述方法，由于终端是根据加密相关信息选择加密算法，而针对不同的加密请求，终端会获取到不同的加密相关信息，从而会选择不同的加密算法对不同加密请求中携带的明文信息进行加密，因此，增大了攻击者对终端上的加密程序反编译分析的难度，而且，单个加密算法与对应的加密密钥的泄露，也并不会威胁到该终端中保存的所有信息的安全，增强了信息
20 安全性。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不
25 当限定。在附图中：

图 1 为本申请实施例提供的信息处理过程；

图 2 为本申请实施例提供的信息处理装置结构示意图。

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，下面将结合本申请具体实
5 施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的
实施例仅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做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。

图 1 为本申请实施例提供的信息处理过程，具体包括以下步骤：

10 S101：处理设备接收加密请求。

在本申请实施例中，所述的处理设备可以是终端，也可以是服务器。其中，
所述的终端包括但不限于：个人计算机（Personal Computer，PC）、手机、平
板电脑等。所述的服务器可以是任意加解密服务提供方的服务器。

当处理设备上的应用或其它设备上的应用需要对敏感信息进行加密时，可
15 通过处理设备提供的接口发送加密请求，处理设备则接收该加密请求。其中，
处理设备可以为各应用提供统一的接口，也可以分别针对不同的应用提供不同
的接口，这些接口可预先对各应用发送的加密请求的内容格式进行定义，以便
处理设备能够正确识别接收到的加密请求，并对这些加密请求进行后续处理。

S102：处理设备获取加密相关信息。

20 所述的加密相关信息可基于加密请求和/或该处理设备自身获得，则相同
的处理设备根据不同的加密请求可获得不同的加密相关信息，不同的处理设备
根据相同的加密请求也可获得不同的加密相关信息。所述的加密相关信息用于
处理设备后续选择加密算法。

S103：处理设备根据该加密相关信息，从预存的各加密算法中选择相应的
25 加密算法。

在本申请实施例中，处理设备上预存有多种加密算法。当处理设备接收到

加密请求，并获取加密相关信息后，可按照预设选择规则对该加密相关信息进行处理，使得处理后得到的信息可与预存的某种加密算法相对应，也即，处理设备根据对该加密相关信息处理后得到的信息，可从预存的多种加密算法中唯一选择出一种特定的加密算法，用于后续对该加密请求中携带的明文信息进行加密。

进一步的，对处理设备上预存的加密算法进行说明。所述的加密算法可以是诸如 RSA、数据加密标准（Data Encryption Standard, DES）、三重数据加密标准（Triple Data Encryption Standard, 3DES）、国际数据加密算法（International Data Encryption Algorithm, IDEA）、安全哈希算法 1（Secure Hash Algorithm1, Sha1）、Sha256、Sha512、消息摘要算法第 5 版（Message Digest Algorithm5, MD5）、高级加密标准（Advanced Encryption Standard, AES）等加密算法，也可以是处理设备的开发人员自行开发的加密算法，本申请中对预存的加密算法并不做限定。

S104: 处理设备采用选择的加密算法对该加密请求中携带的明文信息进行加密，得到密文信息。

在本申请实施例，处理设备接收到的加密请求中除了携带有明文信息之外，还可携带加密密钥。则处理设备通过步骤 S103 从预存的各加密算法中选择了相应的加密算法后，则可使用该加密密钥和选择出的加密算法对该加密请求中携带的明文信息进行加密，得到密文信息。

需要说明的是，由于不同的加密算法对与其适配的加密密钥的长度的要求可能不同，例如，AES 的加密密钥长度为 128 位、或 192 位、或 256 位，而 3DES 的加密密钥长度为 112 位、或 168 位，因此，当处理设备选择出的加密算法适配的加密密钥的长度与该加密请求中携带的加密密钥的长度不相同，处理设备可将该加密请求中携带的加密密钥转换为与该加密算法适配的加密密钥的长度相同的加密密钥，再使用该加密算法和转换后的加密密钥对该加密请求中携带的明文信息进行加密。或者，处理设备也可根据该加密请求中携带

的加密密钥的长度对预存的各加密算法先做一次筛选，选出适配的加密密钥的长度与该加密请求中携带的加密密钥的长度相同的各加密算法，再根据该加密请求中携带的明文信息和/或加密相关信息，从筛选出的各加密算法中选择相应的加密算法对该明文信息进行加密，从而保证处理设备可以正常使用为该加密请求选择出的加密算法。

通过上述方法，由于处理设备是根据加密相关信息选择加密算法，而针对不同的加密请求，处理设备会获取到不同的加密相关信息，从而会选择不同的加密算法对不同加密请求中携带的明文信息进行加密，因此，增大了攻击者对处理设备上的加密程序反编译分析的难度，而且，单个加密算法与对应的加密密钥的泄露，也并不会威胁到处理设备中保存的所有信息的安全，增强了信息安全性。

进一步的，对步骤 S102 中获取加密相关信息进行说明。具体的，处理设备可获取自身的环境信息、该加密请求中携带的明文信息、发送该加密请求的应用的标识、随机数中的至少一种，作为获取到的加密相关信息，其中，所述环境信息包括该处理设备的标识。

由于同一个应用可能会向不同的处理设备发送相同的加密请求，因此，为了使得每一个处理设备后续为该加密请求选择不同的加密算法，处理设备可获取自身的环境信息（也即，该处理设备的标识），作为加密相关信息。以处理设备为手机为例对这种情况进行说明，处理设备的标识可以是该手机的移动设备国际身份码（International Mobile Equipment Identity, IMEI），IMEI 可以唯一标识一台手机，由于不同的手机的 IMEI 不同，因此即使不同的手机接收到同一个应用发送的相同的加密请求，每一个手机根据获得的自身的 IMEI，从预存的各加密算法中选择出的加密算法也会不同。

当然，本申请中所述的环境信息除了包括处理设备的标识以外，还可包括该处理设备的其他硬件或软件信息，如介质访问控制（Media Access Control, MAC）地址、该处理设备的操作系统的序列号等。

类似的，由于不同的加密请求中携带的明文信息可能不同，因此，处理设备也可将加密请求中携带的明文信息作为加密相关信息。则处理设备可根据加密请求中携带的明文信息，从预存的各加密算法中选择相应的加密算法，当不同的加密请求中携带的明文信息不同时，处理设备为各加密请求选择的加密算法也会不同。

类似的，由于同一个处理设备可接收到不同的应用发送的加密请求，因此，处理设备还可获取发送加密请求的应用的标识，作为加密相关信息。其中，发送加密请求的应用的标识可携带在加密请求中，即，处理设备还可获取加密请求中携带的发送加密请求的应用的标识。具体的，应用的标识可以是应用的数字签名，该数字签名唯一标识一个应用，也即，不同的应用的数字签名不同，则处理设备针对接收到的不同的应用发送的各加密请求，根据获取到的发送每一个加密请求的应用的数字签名，从预存的各加密算法中选择出的加密算法也会不同。

类似的，处理设备还可获取随机数作为加密相关信息，该随机数可携带在加密请求中，即，处理设备可获取加密请求中携带的随机数。当然，随机数还可由处理设备自行生成。对于不同的加密请求，处理设备获取到的随机数不同，从预存的各加密算法中选择出的加密算法也会不同。

以上是分别针对处理设备接收加密请求后，获取的加密信息包括了该处理设备的标识、该加密请求中携带的明文信息、发送该加密请求的应用的标识、随机数中的一种的情况进行分析的，显然，处理设备也可以获取这四种信息的任意组合作为加密相关信息，从而，只要处理设备获取的上述组合的信息不全相同，则处理设备针对每一个加密请求，根据获取到的上述组合的信息，从预存的各加密算法中选择出的加密算法就会不同。

进一步的，在上述步骤 103 中，当处理设备接收到加密请求，并获取加密相关信息后，可根据该加密相关信息，按照预设选择规则对该加密相关信息进行处理，进而，根据处理后得到的信息选择加密算法。所述的预设选择规则可

以在处理设备上预先配置，在本申请实施例中，针对其中一种可行的预设选择规则进行说明。

具体的，处理设备确定该加密相关信息的 hash 值，确定该 hash 值对预存加密算法的数量取模的模值，选择预设编号为该模值的加密算法。

5 例如，假定某手机上预存有编号为 0~7 的共 8 种加密算法，如下表 1 所示。

加密算法编号	加密算法名称
0	RSA
1	DES
2	3DES
3	AES
4	RC4
5	IDEA
6	Sha1
7	Sha256

表 1

在上述表 1 中，8 种加密算法分别为 RSA、DES、3DES、AES、RC4、IDEA、Sha1、Sha256。

10 当手机分别接收到应用 A 发送的加密请求，以及应用 B 发送的加密请求时，手机针对每一个加密请求，分别获取加密相关信息（加密相关信息包括：该加密请求中携带的明文信息、发送该加密请求的应用的数字签名、该手机的 IMEI），并将每一个加密请求对应的加密相关信息视为一个数据块，该数据块可以表示为一个二进制值，使用单向散列算法（如，MD5 算法）计算出每一个加密请求对应的该二进制值的 hash 值。

15 该手机为应用 A 发送的加密请求计算出 hash 值 a，并对计算 hash 值 a 对 8（即为该手机上预存的加密算法的数量）取模的模值，假定该模值为 1，则该手机选择出表 1 中编号为 1 的加密算法 DES，并用加密算法 DES 和该加密请求中携带的加密密钥对该加密请求中携带的明文信息进行加密。

该手机为应用 B 发送的加密请求计算出 hash 值 b，并对计算 hash 值 b 对 8 取模的模值，假定该模值为 3，则该手机选择出表 1 中编号为 3 的加密算法 AES，并用加密算法 AES 和该加密请求中携带的加密密钥对该加密请求中携带的明文信息进行加密。

5 在此对计算 hash 值所使用的单向散列算法进行说明。使用单向散列算法可以将任意长度的二进制值转换为固定长度的较小二进制值（这种转换是单向的），也即，hash 值。且只要原始二进制值发生改变，该原始二进制值对应的 hash 值也会发生改变。常用的单向散列算法包括：消息摘要算法 5（Message Digest Algorithm 5, MD5）、安全哈希算法（Secure Hash Algorithm, SHA）、
10 消息认证代码（Message Authentication Code, MAC）等。针对同一个原始二进制值，使用不同的单向散列算法计算出的 hash 值的长度可能不同，如使用 MD5 计算出的 hash 值的长度为 128 位、使用 SHA 计算出的 hash 值的长度为 160 位等。用二进制表示的 hash 值的长度很长，书写不便，因此，通常将 hash 值用 16 进制的形式表示，例如，使用 MD5 计算出的某 hash 值用 16 进制的形式
15 可以表示为 0xC8825DB10F2590EAAAD3B435B51404EE。

通过上述说明的预设选择规则，由于所述的 hash 值对预存加密算法的数量取模后，所得模值可能的取值的数量等于处理设备上预存加密算法的数量，则可将这两个数量进行一一映射，例如，用模值的可能的取值作为预存的各加密算法的预设编号。处理设备针对接收到的不同的加密请求，只要获取的加密
20 相关信息不同，则该加密相关信息的 hash 值不同，该对预存加密算法的数量取模的模值就有很大概率不同，从而，处理设备选择的预设编号为该模值的加密算法也会有很大概率不同。因此，处理设备通过上述的预设选择规则，可以实现根据获取的加密相关信息，从预存的各加密算法中唯一确定出一种特定的加密算法，用于后续对应该明文信息进行加密。

25 进一步的，处理设备使用为加密请求选择的加密算法对该加密请求中携带的明文信息进行加密，得到密文信息后，还需保存该密文信息、该加密相关信

息以及选择的加密算法的对应关系，以用于后续对该密文信息进行解密。

当某应用需要对密文信息进行解密，以获得相应的明文信息时，可通过处理设备提供的接口向处理设备发送解密请求，其中，该解密请求中可携带解密密钥、密文信息等。当处理设备接收到解密请求时，查找与该解密请求中携带的密文信息对应的加密算法，采用与查找到的加密算法相对应的解密算法对该解密请求中携带的密文信息进行解密。

需要说明的是，和步骤 S103 中的情况类似，当与要使用的解密算法适配的解密密钥的长度与该解密请求中携带的解密密钥的长度不相同时，处理设备可将该解密请求中携带的解密密钥转换为与该解密算法适配的解密密钥的长度相同的解密密钥，再使用该解密算法和转换后的解密密钥对该解密请求中携带的密文信息进行解密，从而保证处理设备可以正常使用该解密算法。

进一步的，在本申请实施例中，为了提高信息安全性，处理设备在对解密请求中携带的密文信息进行解密之前，还可获取解密相关信息，用于后续判断该解密请求是否合法。其中，该解密相关信息中包括该处理设备自身的环境信息和发送所述解密请求的应用的标识中的至少一种。

处理设备获取解密相关信息后，查找与该解密请求中携带的密文信息对应的加密相关信息，确定查找到的加密相关信息中指定类型的信息与获取的解密相关信息中指定类型的信息相同，也即，处理设备查找与该解密请求中携带的密文信息对应的加密相关信息，判断查找到的加密相关信息中指定类型的信息与获取的解密相关信息中指定类型的信息是否相同，若是，则对该密文信息进行解密，否则，拒绝该解密请求。

其中，所述的指定类型的信息可以是加密相关信息中应用的标识，也即，当处理设备确定加密相关信息中的发送加密请求的应用的标识与解密相关信息中的发送解密请求的应用的标识相同时，才对该密文信息进行解密。在这种情况下通过上述的验证可确保：基于某应用发送加密请求，处理设备对明文信息进行加密得到密文信息后，仅在该同一个应用发起解密请求的条件下，处理

设备才可对该密文信息进行解密。从而，提高了各个应用私有的加密信息的安全性。

所述的指定类型的信息也可以是处理设备获取的自身的标识，也即，当处理设备确定加密相关信息中的处理设备的标识与解密相关信息中的处理设备的标识相同时，才对该密文信息进行解密。在这种情况下通过上述的验证可确保：由某处理设备对明文信息进行加密后所得的密文信息，仅能由同一个处理设备才可对该密文信息进行解密。从而，提高了各处理设备对应的加密信息的安全性。

例如，假定所述的指定类型的信息为加密相关信息中的应用的标识和加密相关信息中的处理设备的标识。应用 A 向手机发送了加密请求，该手机接收到该加密请求后，针对该加密请求获取加密相关信息，包括：应用 A 的数字签名、该手机的 IMEI、随机数。该手机按照预设选择规则，根据该加密请求中携带的上述信息从预存的加密算法中选择出加密算法 A 对该明文信息进行加密，得到密文信息，该手机保存该密文信息、加密算法 A、应用 A 的数字签名、该手机的 IMEI 这几者的对应关系。

应用 A 后续又向该手机发送携带有该密文信息的解密请求，该手机接收到该解密请求后，针对该解密请求获取解密相关信息，包括：应用 A 的数字签名、该手机的 IMEI。进而，手机查找到与该密文信息对应的加密算法 A、应用 A 的数字签名，由于解密请求也携带了应用 A 的数字签名，则该手机可确定与该密文信息相关的加密请求和解密请求均由同一应用（也即，应用 A）发送，从而，该手机可确定应用 A 为该密文信息的合法拥有者。因此，手机 A 采用加密算法 A 对应的解密算法对该密文信息解密，可成功获得明文信息，并将获得的明文信息返回给应用 A。

而假定另一应用 B 也向该手机发送携带有该密文信息的解密请求，该手机接收到该解密请求后，针对该解密请求获取解密相关信息，包括：应用 B 的数字签名、该手机的 IMEI。进而，手机查找到与该密文信息对应的加密算法 A、

应用 A 的数字签名, 由于应用 B 发送的解密请求中携带了应用 B 的数字签名, 则该手机可确定与该密文信息相关的加密请求、解密请求由不同的应用发送, 从而, 该手机可确定应用 B 不为该密文信息的合法拥有者。因此, 该手机拒绝应用 B 发送的解密请求。

5 显然, 由应用 A 通过手机进行加密的密文信息只能仍由应用 A 通过该手机进行解密。

另外, 某应用也有可能将自己的敏感信息授权给其它的特定应用使用。在这种情况下, 该应用可在加密相关信息中也携带其它的特定应用的标识, 此时, 处理设备获取的加密相关信息中除了包括发送该加密请求的应用的标识以外,
10 还包括其它的特定应用的标识。

相应的, 当处理设备采用选择出的加密算法对加密请求中携带的明文信息进行加密后, 保存所述密文信息、所述加密相关信息以及选择的加密算法的对应关系, 当处理设备接收到解密请求时, 获取解密相关信息, 该解密相关信息中包括发送该解密请求的应用的标识。处理设备查找与所述解密请求中携带的
15 密文信息对应的加密算法和加密相关信息, 判断获取的解密相关信息中的发送该解密请求的应用的标识是否与查找到的加密相关信息中的至少一个应用的标识(该至少一个应用的标识包括发送该加密请求的应用的标识和其它的特定应用的标识)相同, 若相同, 则采用与查找到的加密算法相对应的解密算法对该解密请求中携带的密文信息进行解密, 得到对应的明文信息。这样, 其它的
20 特定应用也可以对该加密信息进行解密, 并使用得到的明文信息。

以上为本申请实施例提供的基于图像的信息呈现方法, 基于同样的思路, 本申请实施例还提供相应的信息处理装置, 如图 2 所示。

图 2 为本申请实施例提供的基于图像的信息呈现装置结构示意图, 具体包括:

25 具体的上述如图 2 所示的装置可以位于终端或服务器上。

接收模块 201, 用于接收加密请求;

获取模块 202, 用于获取加密相关信息;

选择模块 203, 用于根据所述加密相关信息, 从预存的各加密算法中选择相应的加密算法;

加密模块 204, 用于采用所述选择模块 203 选择的加密算法对所述加密请求中携带的明文信息进行加密, 得到密文信息。

所述获取模块 202 具体用于, 获取所述处理设备的环境信息、所述加密请求中携带的明文信息、发送所述加密请求的应用的标识、随机数中的至少一种, 作为获取到的加密相关信息; 其中, 所述环境信息包括所述处理设备的标识。

所述选择模块 203 具体用于, 确定所述加密相关信息的 hash 值, 确定所述 hash 值对预存加密算法的数量取模的模值, 选择预设标号为所述模值的加密算法。

所述装置还包括:

保存模块 205, 用于保存所述密文信息、所述加密相关信息以及选择的加密算法的对应关系;

解密模块 206, 用于当接收到解密请求时, 查找与所述解密请求中携带的密文信息对应的加密算法, 采用与查找到的加密算法相对应的解密算法对所述解密请求中携带的密文信息进行解密, 得到对应的明文信息。

所述解密模块 206 还用于, 在采用与查找到的加密算法相对应的解密算法对所述解密请求中携带的密文信息进行解密之前, 获取解密相关信息, 查找与
所述解密请求中携带的密文信息对应的加密相关信息, 确定查找到的加密相关信息中指定类型的信息与获取的解密相关信息中指定类型的信息相同; 其中, 所述解密相关信息中包括所述处理设备自身的环境信息和发送所述解密请求的应用的标识中的至少一种。

本领域内的技术人员应明白, 本发明的实施例可提供为方法、系统、或计算机程序产品。因此, 本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且, 本发明可采用在一个或多个其中包

含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其

他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带, 磁带磁
5 磁盘存储或其他磁性存储设备或任何其他非传输介质, 可用于存储可以被计算
设备访问的信息。按照本文中的界定, 计算机可读介质不包括暂存电脑可读媒
体 (transitory media), 如调制的数据信号和载波。

还需要说明的是, 术语“包括”、“包含”或者其任何其他变体意在涵盖非
排除性的包含, 从而使得包括一系列要素的过程、方法、商品或者设备不仅包
括那些要素, 而且还包括没有明确列出的其他要素, 或者是还包括为这种过程、
10 方法、商品或者设备所固有的要素。在没有更多限制的情况下, 由语句“包括
一个……”限定的要素, 并不排除在包括所述要素的过程、方法、商品或者设
备中还存在另外的相同要素。

本领域技术人员应明白, 本申请的实施例可提供为方法、系统或计算机程
序产品。因此, 本申请可采用完全硬件实施例、完全软件实施例或结合软件和
15 硬件方面的实施例的形式。而且, 本申请可采用在一个或多个其中包含有计算
机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、
光学存储器等)上实施的计算机程序产品的形式。

以上所述仅为本申请的实施例而已, 并不用于限制本申请。对于本领域技
术人员来说, 本申请可以有各种更改和变化。凡在本申请的精神和原理之内所
20 作的任何修改、等同替换、改进等, 均应包含在本申请的权利要求范围之内。

权 利 要 求 书

1、一种信息处理方法，其特征在于，包括：

处理设备接收加密请求；并

获取加密相关信息；

5 根据所述加密相关信息，从预存的各加密算法中选择相应的加密算法；以及

采用选择的加密算法对所述加密请求中携带的明文信息进行加密，得到密文信息。

2、如权利要求 1 所述的方法，其特征在于，获取加密相关信息，具体包
10 括：

所述处理设备获取自身的环境信息、所述加密请求中携带的明文信息、发送所述加密请求的应用的标识、随机数中的至少一种，作为获取到的加密相关信息；

其中，所述环境信息包括所述处理设备的标识。

15 3、如权利要求 1 所述的方法，其特征在于，从预存的各加密算法中选择相应的加密算法，具体包括：

确定所述加密相关信息的 hash 值；

确定所述 hash 值对预存加密算法的数量取模的模值；

选择预设编号为所述模值的加密算法。

20 4、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

保存所述密文信息、所述加密相关信息以及选择的加密算法的对应关系；

当处理设备接收到解密请求时，查找与所述解密请求中携带的密文信息对应的加密算法，采用与查找到的加密算法相对应的解密算法对所述解密请求中携带的密文信息进行解密，得到对应的明文信息。

25 5、如权利要求 4 所述的方法，其特征在于，采用与查找到的加密算法相对应的解密算法对所述解密请求中携带的密文信息进行解密之前，所述方法还

包括:

获取解密相关信息;所述解密相关信息中包括所述处理设备自身的环境信息和发送所述解密请求的应用的标识中的至少一种;

查找与所述解密请求中携带的密文信息对应的加密相关信息;

5 确定查找到的加密相关信息中指定类型的信息与获取的解密相关信息中指定类型的信息相同。

6、一种信息处理装置,其特征在于,包括:

接收模块,用于接收加密请求;

获取模块,用于获取加密相关信息;

10 选择模块,用于根据所述加密相关信息,从预存的各加密算法中选择相应的加密算法;

加密模块,用于采用所述选择模块选择的加密算法对所述加密请求中携带的明文信息进行加密,得到密文信息。

7、如权利要求6所述的装置,其特征在于,所述获取模块具体用于,获取
15 所述处理设备的环境信息、所述加密请求中携带的明文信息、发送所述加密请求的应用的标识、随机数中的至少一种,作为获取到的加密相关信息;其中,所述环境信息包括所述处理设备的标识。

8、如权利要求6所述的装置,其特征在于,所述选择模块具体用于,确定所述加密相关信息的hash值,确定所述hash值对预存加密算法的数量取模
20 的模值,选择预设标号为所述模值的加密算法。

9、如权利要求6所述的装置,其特征在于,所述装置还包括:

保存模块,用于保存所述密文信息、所述加密相关信息以及选择的加密算法的对应关系;

解密模块,用于当接收到解密请求时,查找与所述解密请求中携带的密文
25 信息对应的加密算法,采用与查找到的加密算法相对应的解密算法对所述解密请求中携带的密文信息进行解密,得到对应的明文信息。

10、如权利要求 9 所述的装置，其特征在于，所述解密模块还用于，在采用与查找到的加密算法相对应的解密算法对所述解密请求中携带的密文信息进行解密之前，获取解密相关信息，查找与所述解密请求中携带的密文信息对应的加密相关信息，确定查找到的加密相关信息中指定类型的信息与获取的解密相关信息中指定类型的信息相同；其中，所述解密相关信息中包括所述处理设备自身的环境信息和发送所述解密请求的应用的标识中的至少一种。

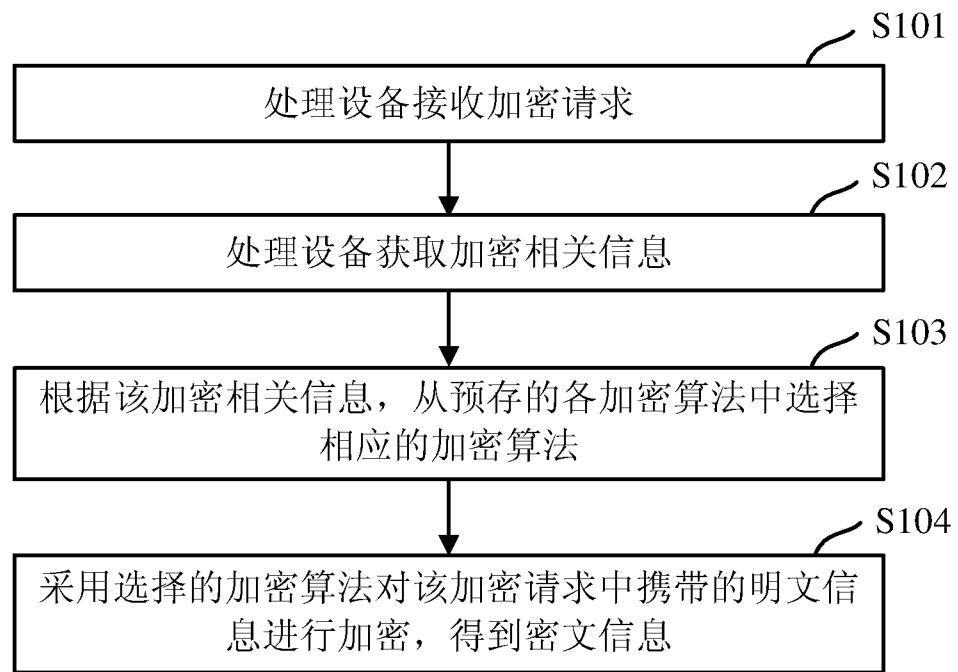


图 1

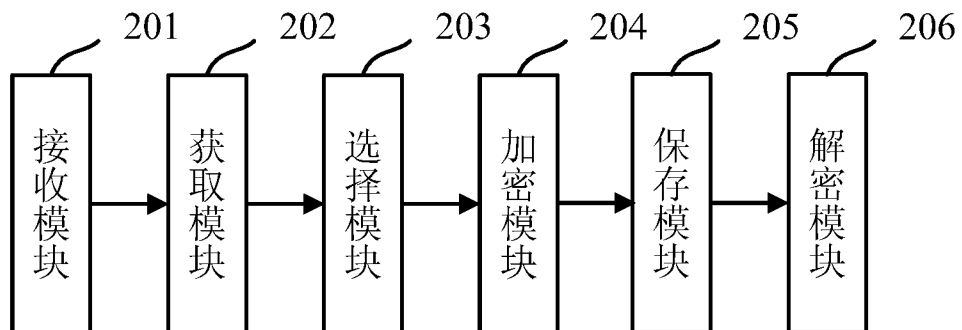


图 2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/091247

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; 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: encrypt, decrypt, key, secret, identification, random, hash, modulus, module value

SIPOABS; VEN; EPTXT; WOTXT; USTXT: encrypt+, decrypt+, key, ID, identifi+, random, hash, mod, module

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1747383 A (HUAWEI TECHNOLOGIES CO., LTD.), 15 March 2006 (15.03.2006), description, page 2, paragraph 4 to page 10, paragraph 1	1, 2, 4-7, 9, 10
X	US 2008123859 A1 (MAMIDWAR, R.), 29 May 2008 (29.05.2008), description, paragraphs 17-35	1, 2, 4-7, 9, 10
X	CN 102523087 A (BAIDU ONLINE NETWORK TECHNOLOGY (BEIJING) CO., LTD.), 27 June 2012 (27.06.2012), description, paragraphs 30-132	1, 2, 4-7, 9, 10
A	WO 2010024379 A1 (NEC CORP.), 04 March 2010 (04.03.2010), the whole document	1-10
A	WO 2011034703 A2 (GM GLOBAL TECH OPERATIONS INC.), 24 March 2011 (24.03.2011), the whole document	1-10
A	US 2010174909 A1 (MEMORY EXPERTS INT INC.), 08 July 2010 (08.07.2010), the whole document	1-10
A	US 2014075199 A1 (SONY CORP.), 13 March 2014 (13.03.2014), the whole document	1-10

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“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	“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
“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)	“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
“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	“&” document member of the same patent family

Date of the actual completion of the international search 15 December 2015 (15.12.2015)	Date of mailing of the international search report 13 January 2016 (13.01.2016)
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 SUN, Yan Telephone No.: (86-10) 62411365

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/091247

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008229103 A1 (UNIV MICHIGAN STATE), 18 September 2008 (18.09.2008), the whole document	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/091247

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1747383 A	15 March 2006	CN 100574186 C	23 December 2009
US 2008123859 A1	29 May 2008	US 8213602 B2	03 July 2012
CN 102523087 A	27 June 2012	CN 102523087 B	11 February 2015
WO 2010024379 A1	04 March 2010	JP 5556659 B2	23 July 2014
WO 2011034703 A2	24 March 2011	US 2011066859 A1	17 March 2011
		WO 2011034703 A3	16 June 2011
		DE 112010003661 B4	27 August 2015
		DE 112010003661 T5	18 October 2012
		US 8452969 B2	28 May 2013
US 2010174909 A1	08 July 2010	US 8989383 B2	24 March 2015
		US 2015215126 A1	30 July 2015
US 2014075199 A1	13 March 2014	CN 103678995 A	26 March 2014
		JP 2014052588 A	20 March 2014
US 2008229103 A1	18 September 2008	US 8966252 B2	24 February 2015

国际检索报告

国际申请号

PCT/CN2015/091247

A. 主题的分类

H04L 9/32 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04L; 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: 加密, 解密, 密钥, 秘密, 标识, 随机, 散列, hash, 取模, 模值 SIPOABS; VEN; EPTXT; WOTXT; USTXT: encrypt+, decrypt+, key, ID, identifi+, random, hash, mod, module

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	CN 1747383 A (华为技术有限公司) 2006年 3月 15日 (2006 - 03 - 15) 说明书第2页第4段-第10页第1段	1, 2, 4-7, 9, 10
X	US 2008123859 A1 (MAMIDWAR RAJESH) 2008年 5月 29日 (2008 - 05 - 29) 说明书第17-35段	1, 2, 4-7, 9, 10
X	CN 102523087 A (百度在线网络技术北京有限公司) 2012年 6月 27日 (2012 - 06 - 27) 说明书第30-132段	1, 2, 4-7, 9, 10
A	WO 2010024379 A1 (NEC CORP) 2010年 3月 4日 (2010 - 03 - 04) 全文	1-10
A	WO 2011034703 A2 (GM GLOBAL TECH OPERATIONS INC) 2011年 3月 24日 (2011 - 03 - 24) 全文	1-10
A	US 2010174909 A1 (MEMORY EXPERTS INT INC) 2010年 7月 8日 (2010 - 07 - 08) 全文	1-10
A	US 2014075199 A1 (SONY CORP) 2014年 3月 13日 (2014 - 03 - 13) 全文	1-10

☒ 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

2015年 12月 15日

国际检索报告邮寄日期

2016年 1月 13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

授权官员

孙燕

传真号 (86-10) 62019451

电话号码 (86-10) 62411365

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	US 2008229103 A1 (UNIV MICHIGAN STATE) 2008年 9月 18日 (2008 - 09 - 18) 全文	1-10

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/091247

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	1747383	A	2006年 3月 15日	CN	100574186	C	2009年 12月 23日
US	2008123859	A1	2008年 5月 29日	US	8213602	B2	2012年 7月 3日
CN	102523087	A	2012年 6月 27日	CN	102523087	B	2015年 2月 11日
WO	2010024379	A1	2010年 3月 4日	JP	5556659	B2	2014年 7月 23日
WO	2011034703	A2	2011年 3月 24日	US	2011066859	A1	2011年 3月 17日
				WO	2011034703	A3	2011年 6月 16日
				DE	112010003661	B4	2015年 8月 27日
				DE	112010003661	T5	2012年 10月 18日
				US	8452969	B2	2013年 5月 28日
US	2010174909	A1	2010年 7月 8日	US	8989383	B2	2015年 3月 24日
				US	2015215126	A1	2015年 7月 30日
US	2014075199	A1	2014年 3月 13日	CN	103678995	A	2014年 3月 26日
				JP	2014052588	A	2014年 3月 20日
US	2008229103	A1	2008年 9月 18日	US	8966252	B2	2015年 2月 24日

表 PCT/ISA/210 (同族专利附件) (2009年7月)