数据加密方法、数据解密方法、装置、终端和存储介质

本公开要求在2020年08月07日提交中国专利局、申请号为202010790159.3的中国专利申请的优先权，以上申请的全部内容通过引用结合在本公开中。

技术领域

本申请实施例涉及安全技术，例如涉及一种数据加密方法、数据解密方法、装置、终端和存储介质。

背景技术

在移动终端中安装的应用在存储具有敏感性质的数据时，为了保护用户的个人隐私，通常使用对称密钥算法、非对称密钥算法等算法对数据进行加密。

然而，无论加密算法设计得有多么安全和牢固，一旦密钥被泄露，攻击者可以直接使用密钥调用加密算法解密数据，可见，数据的加解密操作存在着安全性风险。

发明内容

本申请实施例提供一种数据加密方法、数据解密方法、装置、终端和存储介质，以在维持计算开销、存储开销的情况下，提高移动终端中数据的安全性。

第一方面，本申请实施例提供了一种数据加密方法，包括:

在非可信执行环境中，确定应用请求加密的源数据;

在所述非可信执行环境中，生成与所述源数据对应的参考数据，所述参考数据是加密所述源数据的过程中一次性使用的数据;

在可信执行环境中，读取为所述应用生成的主密钥;

在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

在所述非可信执行环境中，使用所述安全数据对所述源数据进行加密，得到目标数据。

第二方面，本申请实施例还提供了一种数据解密方法，包括:

在非可信执行环境中，确定应用请求解密的目标数据;

在所述非可信执行环境中，读取与所述目标数据关联的参考数据，所述参考数据是解密所述目标数据的过程中一次性使用的数据;

在可信执行环境中，读取为所述应用生成的主密钥;

在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据；

在所述非可信执行环境中，使用所述安全数据对所述目标数据进行解密，获得源数据。

第三方面，本申请实施例还提供了一种数据加密装置，包括：

源数据确定模块，设置为在非可信执行环境中，确定应用请求加密的源数据；

参考数据生成模块，设置为在所述非可信执行环境中，生成与所述源数据对应的参考数据，所述参考数据是加密所述源数据的过程中一次性使用的数据；

主密钥读取模块，设置为在可信执行环境中，读取为所述应用生成的主密钥；

安全数据生成模块，设置为在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据；

源数据加密模块，设置为在所述非可信执行环境中，使用所述安全数据对所述源数据进行加密，得到目标数据。

第四方面，本申请实施例还提供了一种数据解密装置，包括：

目标数据确定模块，设置为在非可信执行环境中，确定应用请求解密的目标数据；

参考数据读取模块，设置为在所述非可信执行环境中，读取与所述目标数据关联的参考数据，所述参考数据是解密所述目标数据的过程中一次性使用的数据；

主密钥读取模块，设置为在可信执行环境中，读取为所述应用生成的主密钥；

安全数据生成模块，设置为在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据；

目标数据解密模块，设置为在所述非可信执行环境中，使用所述安全数据对所述目标数据进行解密，获得源数据。

第五方面，本申请实施例还提供了一种移动终端，所述移动终端包括：

一个或多个处理器；

存储器，设置为存储一个或多个程序；

所述一个或多个处理器，设置为执行所述一个或多个程序以实现如第一方面所述的数据加密方法或者如第二方面所述的数据解密方法。

第六方面，本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如第一方面所述的数据加密方法或者如第二方面所述的数据解密方法。

附图说明

图 1 为本申请实施例一提供的一种数据加密方法的流程图；

图 2 为本申请实施例一提供的一种移动终端的环境示意图；

图 3 为本申请实施例一提供的一种加密的流程示意图；

图 4 为本申请实施例一提供的一种 KGF 算法的示例图；

图 5 为本申请实施例一提供的一种 AES 的加密示意图；

图 6 是本申请实施例二提供的一种数据加密方法的流程图；

图 7 是本申请实施例三提供的一种数据解密方法的流程图；

图 8 为本申请实施例三提供的一种解密的流程示意图；

图 9 为本申请实施例三提供的一种 AES 的解密示意图；

图 10 为本申请实施例四提供的一种数据加密装置的结构示意图；

图 11 为本申请实施例五提供的一种数据解密装置的结构示意图；

图 12 为本申请实施例六提供的一种移动终端的结构示意图。

具体实施方式

相关技术中，无论加密算法设计得有多么安全和牢固，一旦密钥被泄露，攻击者可以直接使用密钥调用加密算法解密数据，所以，加密算法的安全性的重点之一，在于所使用密钥的安全保存。

在相关技术中，应用的密钥主要是以硬编码方式预埋在应用的代码中，如 Android（安卓）的 Java 层、Native 层。为了减轻这种无保护的密码存储方式所受到的威胁，通常使用代码混淆机制，如 OLLVM（Obfuscator-LLVM），OLLVM 是一个开源的代码混淆编译器，混淆代码逻辑以提高代码逆向阅读的困难度。

但是，代码混淆机制只能对代码逻辑进行混淆，无法混淆预埋密钥这种数组变量或常量，该类存储方式有以下三个缺点：

（1）密钥无任何单独的安全保护，仅依赖于对代码的安全加固，往往容易被攻击者静态分析提取密钥，攻击者容易通过移动终端的漏洞获取权限。

（2）可能被攻击者逆向代码后，不直接提取密钥，使用上层函数代码直接调用启动密钥的函数，对数据直接解密。

（3）由于不易变更或实行每个应用实例使用不同密钥，所以同一版本的应用或者所有版本的应用预埋的密钥都是一致的，攻击者可以把数据从一个应用导出，放在另一个已被破解的应用上进行数据解密，即数据离开移动终端仍可被解密。

就上述安全性风险而言，本申请实施例公开一种数据加密方法、数据解密方法、装置、终端和存储介质，可较好地应对此类数据安全风险。

下面结合附图和实施例对本申请进行说明。

实施例一

图 1 为本申请实施例一提供的一种数据加密方法的流程图，本实施例可使用一次性的密钥对数据进行加密，该方法可以由数据加密装置来执行，该数据加密装置可以由软件和/或硬件实现，可配置在移动终端中，移动终端例如手机、平板电脑、智能穿戴设备等，智能穿戴设备例如智能眼镜、智能手表等。

在本实施例中，如图 2 所示，移动终端包括如下两种环境:

一、非可信执行环境 210

非可信执行环境是移动终端通用的环境，运行通用的操作系统（Operating System，OS），例如，Android（安卓）、iOS、Linux 等等，非可信执行环境为上层的第三方应用（application，APP）提供服务。

非可信执行环境存在一定的安全隐患，如基于 OS 实现的应用隔离容易被绕过，OS 代码庞大，容易出现漏洞（BUG），OS 可以看到应用内部的数据，缺乏隔离意味着应用无法安全存储密钥、敏感数据。

二、可信执行环境 220

其中，可信执行环境是移动终端中处理器上的一个安全区域，可信执行环境提供一个隔离于非可信执行环境的执行环境，独立运行可信操作系统（Trusted OS）。

隔离是可信执行环境的本质属性，隔离可以是通过软件，也可以是硬件实现，隔离环境下可应用更多的软件、硬件、网际互连协议（Internet Protocol，IP）、总线一体的安全机制。

对于硬件机制的保护，并不规定某一种硬件实现方法，非可信执行环境不可直接访问可信执行环境，但可作为可信执行环境的客户端（Client）通过应用程序接口（Application Programming Interface，API）向可信执行环境的 Trusted OS 请求安全服务。

可信执行环境由 Global Platform（GP）等实现标准化，可在多种平台上移

植，GP 定义了可信执行环境的保护轮廓（Protection Profile），定义了所需的硬件保护强度。

可信执行环境对于密钥使用安全存储机制，保证认证性、完整性和机密性。

可信执行环境中可以同时支持安全加载并执行多个可信应用（Trusted Application，TA），TA 之间相互隔离，保证加载到可信执行环境的代码及数据的机密性、完整性，Trusted OS 提供可信执行环境中的内部 API（Internal API）为 TA 提供服务。

针对不同的 OS，可信执行环境也有所不同，例如，若 OS 为 iOS 系统，则可信执行环境为 Secure Enclave，又例如，若 OS 为 Android 系统，可信执行环境为 TEE（Trusted Execution Environment），非可信执行环境为 REE（Rich Execution Environment）。

如图 1 所示，该方法包括如下步骤:

S101、在非可信执行环境中，确定应用请求加密的源数据。

在非可信执行环境（如 REE）中安装一个或多个应用（APP），该应用可以为通用操作系统的应用，也可以为第三方应用，例如，摄像应用、浏览器、电子邮箱、记事本、通讯录、购物应用、短视频应用等。

其中，通用操作系统也可记为非可信操作系统，例如，Android、iOS、Linux 等。

应用在运行的过程中，会产生不同安全级别的数据，这些数据通常为明文（plaintext），部分或全部数据因安全级别较高、业务需求等因素而待生成并存储的数据，可以作为源数据，等待加密。

在不同的场景中，源数据的形式可有所不同。

例如，对于浏览器，用户在使用账号、密码（又称口令）登录网站时，浏览器可以记录账号、密码，网站在验证账号、密码成功之后会返回 Cookie，账号、密码与 Cookie 均可以作为源数据加密存储。

又例如，对于记事本，用户记录一些待处理的事项，这些事项可以作为源数据加密存储。

又例如，对于通讯录，用户记录联系人信息，如名称、手机号码、头像等，一般情况下，用户解锁移动终端之后可浏览该联系人信息，其他应用在授权的情况下可读取联系人信息，对于部分较为隐私的联系人信息，可作为源数据加密存储。

上述应用及应用对应的待加密的源数据只是作为示例，在实施本申请实施

例时，可以根据实际情况设置其他应用及其他应用对应的待加密的源数据，例如，用户身份信息、支付信息、音视频数据等。另外，除了上述应用及待加密的源数据外，本领域技术人员还可以根据实际需要采用其它应用及待加密的源数据。

S102、在非可信执行环境中，生成与所述源数据对应的参考数据，所述参考数据是加密所述源数据的过程中一次性使用的数据。

如图 3 所示，在非可信执行环境（如 REE）中接收到应用请求加密的源数据之后，可在非可信执行环境中针对源数据生成在本次加密有效的数据，作为参考数据。

在一实施例中，所谓本次加密有效的数据，是指针对本次加密源数据的操作具有唯一性的数据，即参考数据为一次性的数据，并不重复使用。

在一种方式中，可在非可信执行环境（如 REE）中，通过 rand()函数等方式随机生成一数值 Nonce，作为参考数据。

为保证安全性，该随机的数值 Nonce 的长度可选为 32 字节或大于 32 字节。

在另一种方式中，可在非可信执行环境（如 REE）中，通过 Calendar.getInstance()、new Time()等函数从通用操作系统中读取当前的时间戳 Timestamp，作为参考数据。

上述两种方式中随机的数值 Nonce、时间戳 Timestamp，可以单独使用，也可以组合使用。组合使用时，可以保证本实施例的加密机制整体的抗碰撞性和前向性。

此外，除了上述两种方式之外，还可以使用其他方式生成参考数据，例如，对随机生成的数据进行偏移、异或等操作，通过预设的映射函数将当前的时间戳进行映射等。

S103、在可信执行环境中，读取为应用生成的主密钥。

如图 3 所示，在可信执行环境（如 TEE）中，为非可信执行环境（如 REE）中的应用设置有密钥，为便于区分，该密钥可以称为主密钥 SK，该主密钥 SK 可用于生成本次对源数据加密的安全数据。

非可信执行环境中存在应用，可信执行环境中存在与应用对应的主密钥 SK。

一般情况下，应用与主密钥 SK 是一一对应的关系，即一个应用对应一个主密钥 SK，相应地，可在数据库中建立应用的标识（如包名）与主密钥 SK 之间的映射关系。

在对源数据进行加密时，在非可信执行环境（如 REE）中可通过可信执行

环境（如 TEE）提供的 API，将应用的标识、参考数据发送至可信执行环境（如 TEE）中，请求可信执行环境（如 TEE）中的 TA 使用参考数据生成安全数据，使用该安全数据加密源数据。

此时，可信执行环境（如 TEE）中的 TA 可在数据库中，查找该应用的标识所映射的主密钥 SK。

S104、在可信执行环境中，使用主密钥对参考数据进行加密处理，获得安全数据。

如图 3 所示，在可信执行环境（如 TEE）中，TA 提供密钥生成函数 KGF（Key Generation Function），该密钥生成函数 KFG 可用于生成安全数据，对此，以参考数据（如随机的数值 Nonce、时间戳 Timestamp）作为输入，使用主密钥 SK 对参考数据进行加密处理，将加密处理之后输出的数据设置为安全数据。

安全数据应用于对称密钥算法，安全数据中至少包含密钥，为便于区分，安全数据中的密钥称为副密钥，当然，除了副密钥之外，安全数据根据对称密钥算法的不同，还可以包含其他数据。

对参考数据进行的加密处理除了包含加密操作之外，为提高安全性，还可以包含其他操作，例如，添加其他维度的数据，执行异或操作，执行偏移操作，等等。

在本申请的一个实施例中，S104 可以包括如下步骤，步骤一、步骤二及步骤三。三个步骤如下:

步骤一、在可信执行环境中，将参考数据与预设的标签组合，得到目标数组。

如图 4 所示，以 KGF 算法为例，可以由开发人员自定义一个字符串，作为标签 Label，存储在移动终端的可信执行环境（如 TEE）中。

该标签 Label 为待生成的一次性的安全数据的人为命名，标签 Label 可用于表示安全数据的类型，增加输入数据的维度、以提高安全性，同时也方便开发人员记忆和减少安全数据的误操作。

在一个示例中，在标签 Label 为 secret 时，secret 表示安全数据的类型为密钥，为便于区分，该密钥可以称为副密钥。

在另一个示例中，在标签 Label 为 iv 时，iv 表示安全数据的类型为副密钥、向量。

在可信执行环境（如 TEE）中，TA 表现为编码器 Encoder 的形式，将参考数据（如随机的数值 Nonce、时间戳 Timestamp）、标签 Label 按照既定的顺序，

粘接编码为一个 Hex 数组，作为目标数组 M。

示例性地，M=Nonce || Timestamp || Label。

步骤二、在可信执行环境中，使用主密钥将目标数组加密，得到候选数据。

如图 4 所示，可使用可信执行环境（如 TEE）提供的安全密码函数，使用主密钥将目标数组 M 加密，得到密文形式的数组 T，数组 T 作为候选数据，即 T=Enc（SK，M），Enc 表示加密函数。

以 TEE 作为可信执行环境的示例，TEE 提供的安全密码函数包括 HMAC（Hash-based Message Authentication Code，与密钥相关的哈希运算）算法、AES（Advanced Encryption Standard，高级加密标准）算法、RSA 加密算法、ECDSA（Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法）签名算法、RSA 签名算法，等等。HMAC 与 AES 的计算速度较快，可选用该两种安全密码函数。

步骤三、在可信执行环境中，对候选数据规整为指定长度的数据，将指定长度的数据作为与标签匹配的安全数据。

在可信执行环境（如 TEE）中，TA 表现为规整器 Regulator 的形式。

如图 4 所示，由于候选数据 T 可能是任意长度，而后续加密所需的安全数据长度是固定的，规整器 Regulator 以候选数据 T 为输入，计算输出指定长度的字符串，作为一次性的安全数据，该安全数据的类型以标签 Label 定义。

其中，规整器 Regulator 可使用单向散列函数将候选数据规整为安全数据，即输出的字符串为摘要数据，单向散列函数可记为 Hash（T），单向散列函数可计算任意长度数据，生成 L 字节固定长度的摘要信息 $B_0B_1B_2...B_{L-2}B_{L-1}$，L 为正整数，例如，MD5（Message Digest Algorithm，消息摘要算法第五版）可输出 16B 的摘要数据、SHA（Secure Hash Algorithm，安全哈希算法）1 输出 20B 的摘要数据、SHA224 输出 28B 的摘要数据、SHA256 输出 32B 的摘要数据、SHA384 输出 48B 的摘要数据、SHA512 输出 64B 的摘要数据，等等。

例如，安全数据包括副密钥（One-Time Key），或，副密钥和向量（One-Time IV）。

响应于标签为第一值（如 iv），在可信执行环境（如 TEE）中，使用单向散列函数对候选数据计算第一指定长度的摘要数据，第一指定长度的摘要数据作为副密钥（One-Time Key）、向量（One-Time IV），该副密钥、向量适用于对称密钥算法中的 AES 算法。

响应于标签为第二值（如 secret），在可信执行环境（如 TEE）中，使用单

向散列函数对候选数据计算第二指定长度的摘要数据，第二指定长度的摘要数据作为副密钥（One-Time Key），该副密钥适用于该对称密钥算法中的非 AES 算法，例如，RC4、Chacha20，等等。

图 4 中，若标签为第一值（如 iv）或第二值（如 secret），摘要数据中将有副密钥（One-Time Key）；若标签为第一值（如 iv），摘要数据中将有向量（One-Time IV）。换言之，若标签为第一值（如 iv），摘要数据中可同时有副密钥（One-Time Key）、向量（One-Time IV）。

S105、在非可信执行环境中，使用安全数据对源数据进行加密，得到目标数据。

在本实施例中，如图 3 所示，可信执行环境（如 TEE）中的 TA 针对应用待加密的源数据生成安全数据之后，将安全数据输出至非可信执行环境（如 REE），在非可信执行环境（如 REE）中，使用对称密钥算法加密源数据，加密之后的密文即为目标数据。

图 3 中示出，源数据 301 与目标数据 302。

例如，安全数据包括副密钥（One-Time Key），或，副密钥和向量（One-Time IV）。

在一种实施方式中，在非可信执行环境中，调用对称密钥算法中的 AES 算法、使用向量作为初始化向量（Initialization Vector，IV）、与副密钥共同将源数据加密为目标数据。

如图 5 所示，在 AES 算法的 CBC（Cipher Block Chaining，加密块链）模式中，实现分组加密，将源数据切分为多个明文块，如明文块 0、明文块 1……。针对每个明文块，将明文块与加密向量进行异或处理之后，加密器使用副密钥进行加密，输出密文块，密文块可为二进制的数组，如密文块 0、密文块 1……。密文块组合之后即为目标数据。

其中，对于第 1 个明文块（即明文块 0），加密向量属于初始化向量 IV，即为安全数据中的向量，对于第 n 个明文块（即明文块 1……），加密向量为第 n-1 个密文块，$n>1$。

在另一种实施方式中，在非可信执行环境中，调用对称密钥算法中的非 AES 算法、使用副密钥将源数据加密为目标数据。其中，非 AES 算法如 RC4、Chacha20 等。

上述加密算法及安全参数只是作为示例，在实施本申请实施例时，可以根据实际情况设置其他加密算法及其安全参数。

在本实施例中，在非可信执行环境中，确定应用请求加密的源数据，生成与源数据对应的参考数据，参考数据是加密所述源数据的过程中一次性使用的数据；在可信执行环境中，读取为应用生成的主密钥，使用主密钥对参考数据进行加密处理，获得安全数据；在非可信执行环境中，使用安全数据对源数据加密，得到目标数据。

在本实施例中，可信执行环境是基于硬件级别的安全芯片实现，攻击者难以攻破安全芯片，使得可信执行环境的安全强度高，可以保证主密钥、安全数据的安全性。

主密钥是针对应用生成的，使得同一版本的应用或者所有版本的应用所使用的主密钥不相同，而参考数据在本次加解密有效，使得基于主密钥与参考数据生成的安全数据具有一次性的特性，该一次性的安全数据不直接存储，而是在可信执行环境生成，满足选择明文攻击（Chosen-Plaintext Attack，CPA）的安全性，并且，无法被逆向破解。

由于安全数据具有一次性的特性，其他移动终端无法针对同一个源数据生成相同的安全数据，因此，即便加密之后的目标数据离开移动终端后，也无法被其他移动终端解密。

由于可信执行环境内部实施强制访问控制保护，且可信执行环境内部无法被非可信执行环境直接访问，所以，攻击者无法调用启动主密钥的函数对数据进行解密，达到防止非法调用攻击的目标。

此外，在可信执行环境中生成安全数据，由于安全数据的数据量少，可以保证在可信执行环境的计算开销低；在非可信执行环境中，基于性能比安全芯片更高的处理器、使用安全数据对源数据进行加解密，保证在可信执行环境的计算开销低，保证整体的计算开销低。

例如，可信执行环境为独立的安全芯片的运行环境，非可信执行环境为不同于安全芯片的其他硬件上的运行环境。

例如，安全芯片可为，专门为可信执行环境使用的独立硬件芯片。非可信执行环境是在除安全芯片以外的手机硬件上运行，比如手机内存、中央处理器、存储卡等，可不为单独的芯片。

可信执行环境、非可信执行环境在大部分的移动终端有部署，并且，移动终端提供的密码算法是可复用的，使得兼容性在可接受的程度内，不需要额外部署库文件，存储开销小。

除了将应用的密钥以硬编码方式预埋在应用的代码中之外，还可能存在如下两种方式:

一、应用使用白盒密码技术对密钥进行加密存储。

白盒密码技术是指能够抵抗白盒攻击的密码技术，而白盒攻击是指攻击者对移动终端拥有完全的控制能力，能够观测和更改程序运行时的内部数据，这种攻击环境称为白盒攻击环境。

大多移动终端的环境（如 Android、iOS 等）在很多情况下就是一个白盒攻击环境，保护密钥安全是白盒密码技术的一个基本需求。白盒密码技术通常使用 AES 算法，可以保证密钥在不以明文形式出现的条件下，对敏感数据完成加解密，提高密钥存储的安全性，适用于移动终端的场景。

白盒密码技术虽然可以解决密钥被逆向代码静态分析、被提取的威胁情形，但是，仍然无法解决密钥硬编码在代码方式上的缺点，即使用上层函数代码直接调用启动密钥的函数，对数据直接解密；数据离开移动终端仍可被解密。

此外，白盒密码技术的库大约需要 350KB 存储空间，给应用的安装包存储增加了至少 350KB，一些对于安装包大小较为敏感的应用难以承受。

二、在基于硬件安全芯片的可信执行环境对密钥进行加密存储。

移动终端部署使用了基于安全芯片的可信执行环境，可信执行环境是中央处理器（Central Processing Unit，CPU）上的一块区域，可信执行环境的作用是给数据和代码的执行提供一个更安全的空间，并保证数据和代码的机密性和完整性。

iOS 系统使用的 Secure Enclave 是一种可信执行环境，Android 系统 6.0+，API Level 23+之后，Android 系统也要求移动终端部署可信执行环境 TEE 及安全硬件芯片。

一些加密方式使用基于硬件安全芯片的可信执行环境的 AES 加密服务，对一些敏感的个人数据直接进行加密存储，比如，人脸模型参数、银行卡信息等。但是，安全芯片属于一个独立的硬件，成本高，计算能力有限，使用可信执行环境的加密服务，对于大量的数据和文件直接加密，效率低，时间开销高。

测试结果表明，对 100KB 数据，使用 TEE 的 AES-128 加解密时间开销为 6.2 秒，TEE 的 RSA-2048 加解密时间开销为 45 秒。然而个人敏感数据，可能包含较大的音视频文件，大文件或数据加密对应的时间开销过高难以承受。

此外，TEE 的加解密服务，也无法直接支持 CPA 安全性。支持 CPA 安全性可表现为，两段内容相同的明文，加密得到两段内容不同的密文。故而，需

要每次加密前额外调用一次 TEE 的密钥生成存储服务，增加了时间开销。

综合对比“应用的密钥以硬编码方式预埋在应用的代码”、“应用使用白盒密码技术对密钥进行加密存储”、“在基于硬件安全芯片的可信执行环境对密钥进行加密存储”与“本实施例”，如表 1 所示。

表 1 四类处理方式的对比

	密钥硬编码至代码	白盒密码技术	基于安全芯片的可信执行环境	本实施例
安全强度	不明确	AES-128	安全芯片	安全芯片
整体安全性	可能被代码逆向破解、可能被非法调用破解	可能被非法调用破解	无法被代码逆向破解、无法被非法调用破解	无法被代码逆向破解、无法被非法调用破解
数据离开设备失效	否	否	是	是
计算开销	很快	较快	很慢	很快
存储开销	小	350KB	小	小
兼容性	好	好	Android 6.0 API 23+仅限于 AES、RSA 加解密算法	Android 6.0 API 23+所支持的任意密码算法均可使用

其中，安全芯片的安全强度高于 AES-128 的安全强度；Android 6.0 API 23+、所支持的任意密码算法均可使用，使得兼容性较好，属于产品可接受的程度。

综上，本实施例在安全强度、整体安全性、数据离开设备失效、计算开销、存储开销均表现优良。

实施例二

图 6 为本申请实施例二提供的一种数据加密方法的流程图，本实施例以前述实施例为基础，本实施例增加注册主密钥、管理主密钥及参考数据的处理操作，本实施例描述的方法包括如下步骤：

S601、检测在非可信执行环境中安装应用的第一操作。

若本实施例应用于通用操作系统，则可以通过调用通用操作系统的函数监测在非可信执行环境（如 REE）中安装应用的第一操作，即第一操作又称安装操作。

以 Android 为例，应用在安装的时候，Android 操作系统会发送广播，基于

该广播机制，可以定义表示安装应用的广播，广播信息可为应用被安装，应用以包名表示。可在 AndroidManifest 注册表示安装应用的广播，若接收到表示安装应用的广播，则表示检测到在非可信执行环境（如 REE）中安装应用的操作。

若本实施例应用于应用本身，则在应用的安装包被执行时，可以认为是在，检测在非可信执行环境（如 REE）中安装应用的第一操作。

S602、响应于第一操作，在可信执行环境中为应用生成主密钥。

在非可信执行环境（如 REE）中安装应用时，可通过可信执行环境（如 TEE）提供的 API 调用可信执行环境（如 TEE）中密钥生成和存储服务，针对该应用生成一个随机的密钥，作为主密钥 SK，并且主密钥 SK 在可信执行环境（如 TEE）中长期存储，即在可信执行环境（如 TEE）的数据库中建立该应用的标识（如包名）与主密钥 SK 之间的映射关系。

例如，主密钥 SK 可以使用 HMAC、AES、RSA、ECDSA 等算法中的任意一种密钥，也可以根据后续对源数据进行加密的算法而选择。

其中，HMAC 的密钥长度一般大于或等于 16 字节，AES 的密钥长度一般大于或等于 16 字节，RSA 的密钥长度一般大于或等于 256 字节，以确保最低等同 AES-128 的主流商用密码的安全强度。

S603、在非可信执行环境中，确定应用请求加密的源数据。

S604、在非可信执行环境中，生成与源数据对应的参考数据，所述参考数据是加密所述源数据的过程中一次性使用的数据。

S605、在可信执行环境中，读取为应用生成的主密钥。

S606、在可信执行环境中，使用主密钥对参考数据进行加密处理，获得安全数据。

S607、在非可信执行环境中，使用安全数据对源数据进行加密，得到目标数据。

S608、在非可信执行环境中，关联存储目标数据与参考数据。

在非可信执行环境（如 REE）中，在使用安全数据对源数据进行加密，得到目标数据之后，在应用的安装目录下，或者，在独立的存储区域中，除了存储目标数据之外，还存储本次加密所使用的参考数据，建立目标数据与参考数据之间的关联关系，该关联关系表示该参考数据用于加密该目标数据。

目标数据与参考数据之间的存储结构可以自主定义，例如，利用随机的数值 Nonce、时间戳 Timestamp 加密源数据得到目标数据 C，存储时可以把固定长度的 Nonce、Timestamp 作为文件头与目标数据 C 写在一起，即

Nonce|Timestamp|C；或者，存储时可以把固定长度的 Nonce、Timestamp 作为文件尾与目标数据 C 写在一起，即 C|Nonce|Timestamp。

S609、检测删除目标数据的第二操作。

S610、响应于第二操作，在非可信执行环境中删除目标数据与参考数据。

在应用的运行过程中，用户会主动请求删除部分目标数据，或者，应用会自动删除自身的目标数据，或者，第三方应用（如清理应用）也会请求删除应用的目标数据。

例如，浏览器中的 Cookie 作为源数据加密为目标数据，浏览器中设置了自动清理过期的 cookie 的机制，浏览器在检测到 cookie 过期之后，删除该 cookie，即相应地删除该目标数据。

又例如，记事本中记录的事项作为源数据加密为目标数据，用户在发现该事项已经处理之后，在记事本中删除该事项，即相应地删除该目标数据。

又例如，通讯录中的联系人信息作为源数据加密为目标数据，清理应用在检测到存在相同的联系人信息之后，删除相同的联系人信息中的一个联系人信息，即相应地删除该目标数据。

如果检测到删除目标数据的第二操作，则可以在非可信执行环境（如 REE）中查找相应的目标数据，并删除该目标数据，在删除目标数据之后，参考数据失效，此时，可定位该目标数据所映射的参考数据，将该参考数据随同该目标数据删除，保证失效数据及时清理，降低存储开销。

所谓失效，是指删除与参考数据关联的目标数据之后，使用主密钥与该参考数据也无法对其他目标数据进行解密。

S611、检测卸载应用的第三操作。

若本实施例应用于通用操作系统，则可以通过调用通用操作系统的函数监测在非可信执行环境（如 REE）中卸载应用的第三操作，即第三操作又称卸载操作。

以 Android 为例，应用在卸载的时候，Android 操作系统会发送广播，基于该广播发送机制，可以定义表示安装应用的广播，广播如应用被卸载， 应用可以包名表示。可在 AndroidManifest 注册表示卸载应用的广播，若接收到表示卸载应用的广播，则表示检测到在非可信执行环境（如 REE）中卸载应用的操作。

若本实施例应用于应用本身，则在应用的卸载程序被执行时，可以认为检测在非可信执行环境（如 REE）中卸载应用的第一操作。

S612、响应于第三操作，在可信执行环境中删除为应用生成的主密钥。

S613、响应于第三操作，在非可信执行环境中删除目标数据与参考数据。

在检测到卸载应用的第三操作之后，主密钥、目标数据与参考数据失效，并不作为配置文件而保留在移动终端中，保证失效数据及时清理，降低存储开销。

所谓失效，是指在卸载应用完成之后，若重新安装相同的应用，则会重新生成一个新的主密钥、重新针对相同的源数据生成新的参考数据、新的目标数据，使用新的主密钥与新的参考数据无法对原有的目标数据进行解密。

一方面，可通过可信执行环境（如 TEE）提供的 API 请求删除在可信执行环境（如 TEE）中为应用生成的主密钥，另一方面，在非可信执行环境（如 REE）中删除该应用下所存储的所有目标数据与所有参考数据。

例如，可删除与卸载的应用对应的目标数据与参考数据。

实施例三

图 7 为本申请实施例三提供的一种数据解密方法的流程图，本实施例使用一次性的密钥对数据进行解密，该方法可以由数据解密装置来执行，该数据解密装置可以由软件和/或硬件实现，可配置在移动终端中，例如，手机、平板电脑、智能穿戴设备（如智能眼镜、智能手表等），等等，该移动终端包括非可信执行环境、可信执行环境，该方法包括如下步骤:

S701、在非可信执行环境中，确定应用请求解密的目标数据。

在非可信执行环境（如 REE）中安装一个或多个应用（APP），应用在运行的过程中，会根据不同的业务需求而请求使用相应的数据。

在本实施例中，该数据以密文的形式存储在非可信执行环境（如 REE）中，称为目标数据，此时，可从在非可信执行环境（如 REE）中读取该目标数据，等待解密。

S702、在非可信执行环境中，读取与所述目标数据关联的参考数据，所述参考数据是解密所述目标数据的过程中一次性使用的数据。

如图 8 所示，使用参考数据加密得到目标数据，该目标数据与参考数据关联存储在非可信执行环境（如 REE）中。

在对目标数据解密时，可从非可信执行环境（如 REE）中，基于该关联关系查找该目标数据对应的参考数据。

在一实施例中，参考数据本次解密有效，本次解密有效的数据，是指针对本次解密目标数据的操作具有唯一性的数据，即参考数据为一次性的数据，并

不重复使用。

在一实施例中，该参考数据为随机生成一数值 Nonce 和/或加密目标数据时的时间戳。

目标数据与参考数据之间的存储结构可以自主定义，在解密时，可以按照该存储结构读取参考数据，例如，存储时可以把固定长度的 Nonce、Timestamp 作为文件头与目标数据 C 写在一起，即 Nonce|Timestamp|C，则在解密时，可先读取文件头固定长度的字符串，作为 Nonce 和 Timstamp，剩余的字符串为 C；或者，存储时可以把固定长度的 Nonce、Timestamp 作为文件尾与目标数据 C 写在一起，即 C|Nonce|Timestamp，则在解密时，可先读取文件尾固定长度的字符串，作为 Nonce 和 Timstamp，剩余的字符串为 C。

S703、在可信执行环境中，读取为应用生成的主密钥。

如图 8 所示，在对目标数据进行解密时，在非可信执行环境（如 REE）中可通过可信执行环境（如 TEE）提供的 API，将应用的标识、参考数据发送至可信执行环境（如 TEE）中，请求可信执行环境（如 TEE）中的 TA 使用参考数据生成安全数据，使用该安全数据解密目标数据。

此时，可信执行环境（如 TEE）中的 TA 可在数据库中，查找该应用的标识所映射的主密钥 SK。

S704、在可信执行环境中，使用主密钥对参考数据进行加密处理，获得安全数据。

如图 8 所示，在可信执行环境（如 TEE）中，TA 提供密钥生成函数 KGF，该密钥生成函数 KGF 可用于生成安全数据，对此，以参考数据（如随机的数值 Nonce、时间戳 Timestamp）作为输入，使用主密钥 SK 对参考数据进行加密处理，将加密处理后输出的数据设置为安全数据。

在本申请的一个实施例中，在可信执行环境（如 TEE）中，将参考数据与预设的标签组合为目标数组，其中，标签用于表示安全数据的类型。

在可信执行环境（如 TEE）中，使用主密钥将目标数组加密为候选数据。

在可信执行环境（如 TEE）中，对候选数据规整为指定长度的数据，作为与标签匹配的安全数据。

在一个示例中，安全数据的类型包括副密钥，或，副密钥和向量，则在本示例中，若标签为第一值，则在可信执行环境中，对候选数据计算第一指定长度的摘要数据，作为副密钥、向量；或者，若标签为第二值，则在可信执行环境中，对候选数据计算第二指定长度的摘要数据，作为副密钥。

例如，第一指定长度的摘要数据作为副密钥、向量，是指第一指定长度的摘要数据中同时包含副密钥、向量，第二指定长度的摘要数据作为副密钥，是指第二指定长度的摘要数据中包含副密钥。

在本申请实施例中，由于 S704 与 S104 的应用基本相似，简化描述，相关之处参见 S104 的部分说明即可，本申请实施例在此不加以详述。

S705、在非可信执行环境中，使用安全数据对目标数据进行解密，获得源数据。

如图 8 所示，可信执行环境（如 TEE）中的 TA 针对应用待解密的目标数据生成安全数据之后，将安全数据输出至非可信执行环境（如 REE），在非可信执行环境（如 REE）中，使用对称密钥算法解密目标数据 801，解密之后的明文即为源数据 802。

例如，安全数据包括副密钥（One-Time Key），或，副密钥和向量（One-Time IV）。

在一种实施方式中，在非可信执行环境（如 REE）中，调用对称密钥算法中的 AES 算法、使用该向量作为初始化向量 IV、该向量与副密钥共同将目标数据解密为源数据。

如图 9 所示，在 AES 算法的 CBC 模式中，实现分组解密，将目标数据切分为多个密文块，如密文块 0、密文块 1……，针对每个密文块，解密器使用副密钥进行解密之后，将解密结果与加密向量进行异或处理之后，输出明文块，如明文块 0、明文块 1……，明文块组合之后的组合结果即为源数据。

其中，对于第 1 个明文块（即明文块 0），加密向量属于初始化向量 IV，即为安全数据中的向量，对于第 n（n＞1）个明文块（即明文块 n-1），例如明文块 1……，加密向量为第 n-1 个密文块（即密文块 n-2），例如密文块 0……。

在另一种实施方式中，在非可信执行环境中，调用对称密钥算法中的非 AES 算法、使用副密钥将目标数据解密为源数据。

上述解密算法及安全参数只是作为示例，在实施本申请实施例时，可以根据实际情况设置其他解密算法及安全参数。另外，除了上述解密算法及其安全参数外，本领域技术人员还可以根据实际需要采用其它解密算法及安全参数。

在本实施例中，在非可信执行环境中，确定应用请求解密的目标数据；在非可信执行环境中，读取与目标数据关联的参考数据，所述参考数据是解密所述目标数据的过程中一次性使用的数据；在可信执行环境中，读取为应用生成的主密钥；在可信执行环境中，使用主密钥对参考数据进行加密处理，获得安

全数据；在非可信执行环境中，使用安全数据对目标数据进行解密，获得源数据。

可信执行环境是基于硬件级别的安全芯片实现，攻击者难以攻破安全芯片，使得可信执行环境的安全强度高，可以保证主密钥、安全数据的安全性。

主密钥是针对应用生成的，使得同一版本的应用或者所有版本的应用所使用的主密钥不相同，而参考数据在本次加解密有效，使得基于主密钥与参考数据生成的安全数据具有一次性的特性，该一次性的安全数据不直接存储，而是在可信执行环境生成，满足 CPA 的安全性，并且无法被逆向破解。

由于安全数据具有一次性的特性，其他移动终端无法针对同一个源数据生成相同的安全数据，因此，即便加密之后的目标数据离开移动终端后，也无法被其他移动终端解密。

由于可信执行环境内部实施强制访问控制保护，且可信执行环境内部无法被非可信执行环境直接访问，所以，攻击者无法调用启动主密钥的函数对数据进行解密，达到防止非法调用攻击的目标。

此外，在可信执行环境中生成安全数据，由于安全数据的数据量少，可以保证在可信执行环境的计算开销低，在非可信执行环境中基于性能比安全芯片更高的处理器、使用安全数据对源数据进行加解密，保证在可信执行环境的计算开销低，保证整体的计算开销低。

最后，可信执行环境、非可信执行环境在大多移动终端有部署，并且，可复用移动终端提供的密码算法，使得兼容性在可接受的程度内，不需要额外部署库文件，存储开销小。

在本申请的一个实施例中，该方法还包括:

检测在非可信执行环境中安装应用的第一操作;

响应于第一操作，在可信执行环境中为应用生成主密钥。

在本申请的一个实施例中，该方法还包括:

在非可信执行环境中，关联存储目标数据与参考数据。

在本申请的一个实施例中，该方法还包括:

检测删除目标数据的第二操作;

响应于第二操作，在非可信执行环境中删除目标数据与参考数据。

在本申请的一个实施例中，该方法还包括:

检测卸载应用的第三操作;

响应于第三操作，在可信执行环境中删除为应用生成的主密钥;

响应于第三操作，在非可信执行环境中删除所有目标数据与所有参考数据。

在本申请实施例中，由于第一操作、第二操作、第三操作的响应与实施例二的应用基本相似，相似内容参见实施例二的部分说明即可，本申请实施例在此不加以详述。

实施例四

图 10 为本申请实施例四提供的一种数据加密装置的结构示意图，该装置可以包括如下模块:

源数据确定模块 1001，设置为在非可信执行环境中，确定应用请求加密的源数据;

参考数据生成模块 1002，设置为在所述非可信执行环境中，生成与所述源数据对应的参考数据，所述参考数据是加密所述源数据的过程中一次性使用的数据;

主密钥读取模块 1003，设置为在可信执行环境中，读取为所述应用生成的主密钥;

安全数据生成模块 1004，设置为在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

源数据加密模块 1005，设置为在所述非可信执行环境中，使用所述安全数据对所述源数据进行加密，得到目标数据。

在本申请的一个实施例中，所述参考数据生成模块 1002 包括:

随机数值生成子模块，设置为在所述非可信执行环境中，随机生成一数值，作为参考数据;

和/或，

时间戳读取子模块，设置为在所述非可信执行环境中，读取当前的时间戳，作为参考数据。

在本申请的一个实施例中，所述安全数据生成模块 1004 包括:

目标数组组合子模块，设置为在所述可信执行环境中，将所述参考数据与预设的标签组合，得到目标数组，所述标签用于表示安全数据的类型;

候选数据生成子模块，设置为使用所述主密钥将所述目标数组加密，得到候选数据;

候选数据规整子模块，设置为对所述候选数据规整为指定长度的数据，将所述指定长度的数据作为与所述标签匹配的安全数据。

在本申请的一个实施例中，所述安全数据的类型包括副密钥，或，副密钥和向量;

所述候选数据规整子模块包括:

第一摘要计算单元，设置为在所述可信执行环境中，响应于所述标签为第一值，对所述候选数据计算第一指定长度的摘要数据，所述第一指定长度的摘要数据作为副密钥、向量;

或者，

第二摘要计算单元，设置为在所述可信执行环境中，响应于所述标签为第二值，对所述候选数据计算第二指定长度的摘要数据，所述第二指定长度的摘要数据作为副密钥。

在本申请的一个实施例中，所述安全数据包括副密钥，或，副密钥和向量;

所述源数据加密模块 1005 包括:

第一对称加密子模块，设置为在所述非可信执行环境中，调用对称密钥算法中的高级加密标准 AES 算法、使用所述向量作为初始化向量、与所述副密钥共同将所述源数据加密为目标数据;

或者，

第二对称加密子模块，设置为在所述非可信执行环境中，调用对称密钥算法中的非 AES 算法、使用所述副密钥将所述源数据加密为目标数据。

在本申请的一个实施例中，还包括:

安装操作检测模块，设置为检测在非可信执行环境中安装应用的第一操作;

主密钥生成模块，设置为响应于所述第一操作，在可信执行环境中为所述应用生成主密钥。

在本申请的一个实施例中，还包括:

关联存储模块，设置为在所述非可信执行环境中，关联存储所述目标数据与所述参考数据。

在本申请的一个实施例中，还包括:

删除操作检测模块，设置为检测删除所述目标数据的第二操作;

关联删除模块，设置为响应于所述第二操作，在所述非可信执行环境中删除所述目标数据与所述参考数据。

在本申请的一个实施例中，还包括:

卸载操作检测模块，设置为检测卸载所述应用的第三操作;

主密钥删除模块，设置为响应于所述第三操作，在所述可信执行环境中删

除为所述应用生成的主密钥;

全量数据删除模块，设置为响应于所述第三操作，在所述非可信执行环境中删除所述目标数据与所述参考数据。

本申请实施例所提供的数据加密装置可执行本申请任意实施例所提供的数据加密方法，具备执行方法相应的功能模块和有益效果。

实施例五

图 11 为本申请实施例五提供的一种数据解密装置的结构示意图，该装置可以包括如下模块:

目标数据确定模块 1101，设置为在非可信执行环境中，确定应用请求解密的目标数据;

参考数据读取模块 1102，设置为在非可信执行环境中，读取与所述目标数据关联的参考数据，所述参考数据是解密所述目标数据的过程中一次性使用的数据;

主密钥读取模块 1103，设置为在可信执行环境中，读取为所述应用生成的主密钥;

安全数据生成模块 1104，设置为在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

目标数据解密模块 1105，设置为在所述非可信执行环境中，使用所述安全数据对所述目标数据进行解密，获得源数据。

在本申请的一个实施例中，所述安全数据生成模块 1104 包括:

目标数组组合子模块，设置为在所述可信执行环境中，将所述参考数据与预设的标签组合，得到目标数组，所述标签用于表示安全数据的类型;

候选数据生成子模块，设置为使用所述主密钥将所述目标数组加密，得到候选数据;

候选数据规整子模块，设置为对所述候选数据规整为指定长度的数据，将所述指定长度的数据作为与所述标签匹配的安全数据。

在本申请的一个实施例中，所述安全数据的类型包括副密钥，或，副密钥和向量;

所述候选数据规整子模块包括:

第一摘要计算单元，设置为在所述可信执行环境中，响应于所述标签为第一值，对所述候选数据计算第一指定长度的摘要数据，所述第一指定长度的摘

要数据作为副密钥、向量;

或者,

第二摘要计算单元,设置为在所述可信执行环境中,响应于所述标签为第二值,对所述候选数据计算第二指定长度的摘要数据,所述第二指定长度的摘要数据作为副密钥。

在本申请的一个实施例中,所述安全数据包括副密钥,或,副密钥和向量;

所述目标数据解密模块 1105 包括:

第一对称解密子模块,设置为在所述非可信执行环境中,调用对称密钥算法中的高级加密标准 AES 算法、使用所述向量作为初始化向量、与所述副密钥共同将所述目标数据解密为源数据;

或者,

第二对称解密子模块,设置为在所述非可信执行环境中,调用对称密钥算法中的非 AES 算法、使用所述副密钥将所述目标数据解密为源数据。

在本申请的一个实施例中,还包括:

安装操作检测模块,设置为检测在非可信执行环境中安装应用的第一操作;

主密钥生成模块,设置为响应于所述第一操作,在可信执行环境中为所述应用生成主密钥。

在本申请的一个实施例中,还包括:

关联存储模块,设置为在所述非可信执行环境中,关联存储所述目标数据与所述参考数据。

在本申请的一个实施例中,还包括:

删除操作检测模块,设置为检测删除所述目标数据的第二操作;

关联删除模块,设置为响应于所述第二操作,在所述非可信执行环境中删除所述目标数据与所述参考数据。

在本申请的一个实施例中,还包括:

卸载操作检测模块,设置为检测卸载所述应用的第三操作;

主密钥删除模块,设置为响应于所述第三操作,在所述可信执行环境中删除所述应用生成的主密钥;

全量数据删除模块,设置为响应于所述第三操作,在所述非可信执行环境中删除所有的所述目标数据与所有的所述参考数据。

本申请实施例所提供的数据解密装置可执行本申请任意实施例所提供的数据解密方法,具备执行方法相应的功能模块和有益效果。

实施例六

图 12 为本申请实施例六提供的一种移动终端的结构示意图。如图 12 所示，该移动终端包括处理器 1200、存储器 1201、通信模块 1202、输入装置 1203 和输出装置 1204；移动终端中处理器 1200 的数量可以是一个或多个，图 12 中以一个处理器 1200 为例；移动终端中的处理器 1200、存储器 1201、通信模块 1202、输入装置 1203 和输出装置 1204 可以通过总线或其他方式连接，图 12 中以通过总线连接为例。

存储器 1201 作为一种计算机可读存储介质，可用于存储软件程序、计算机可执行程序以及模块，如本实施例中的数据加密方法、数据解密方法对应的模块，例如，如图 10 所示的数据加密装置中的源数据确定模块 1001、参考数据生成模块 1002、主密钥读取模块 1003、安全数据生成模块 1004 与源数据加密模块 1005；如图 11 所示的数据解密装置中目标数据确定模块 1101、参考数据读取模块 1102、主密钥读取模块 1103、安全数据生成模块 1104 与目标数据解密模块 1105。处理器 1200 通过运行存储在存储器 1201 中的软件程序、指令以及模块，执行移动终端的多种功能应用以及数据处理，即实现上述的数据加密方法、数据解密方法。

存储器 1201 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序，操作系统可为通用操作系统和可信操作系统中的至少一个；存储数据区可存储根据移动终端的使用所创建的数据等。此外，存储器 1201 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他非易失性固态存储器件。在一些实例中，存储器 1201 可包括相对于处理器 1200 远程设置的存储器，这些远程存储器可以通过网络连接至移动终端。上述网络的实例包括互联网、企业内部网、局域网、移动通信网及组合等。

通信模块 1202，设置为与显示屏建立连接，并实现与显示屏的数据交互。

输入装置 1203 可设置为接收输入的数字或字符信息，以及产生与移动终端的用户设置以及功能控制有关的键信号输入，还可以是用于获取图像的摄像头以及获取音频数据的拾音设备。

输出装置 1204 可以包括扬声器等音频设备。

输入装置 1203 和输出装置 1204 的组件可以根据实际情况设定。

处理器 1200 通过运行存储在存储器 1201 中的软件程序、指令以及模块，

执行移动终端的多种功能应用以及数据处理，即实现上述的数据加密方法、数据解密方法。

本实施例提供的移动终端，可执行本申请任一实施例提供的数据加密方法、数据解密方法，实现相应的功能和有益效果。

实施例七

本申请实施例七还提供一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现一种数据加密方法或数据解密方法。

该数据加密方法包括:

在非可信执行环境中，确定应用请求加密的源数据;

在所述非可信执行环境中，生成与所述源数据对应的参考数据，所述参考数据是加密所述源数据的过程中一次性使用的数据;

在可信执行环境中，读取为所述应用生成的主密钥;

在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

在所述非可信执行环境中，使用所述安全数据对所述源数据进行加密，得到目标数据。

该数据解密方法包括:

在非可信执行环境中，确定应用请求解密的目标数据;

在所述非可信执行环境中，读取与所述目标数据关联的参考数据，所述参考数据是解密所述目标数据的过程中一次性使用的数据;

在可信执行环境中，读取为所述应用生成的主密钥;

在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

在所述非可信执行环境中，使用所述安全数据对所述目标数据进行解密，获得源数据。

本申请实施例所提供的计算机可读存储介质中的计算机程序不限于如上所述的方法操作，本申请实施例还可以执行本申请任意实施例所提供的数据加密方法、数据解密方法中的相关操作。

通过以上关于实施方式的描述，所属领域的技术人员可以清楚地了解到，本申请可借助软件及通用硬件来实现，也可以通过硬件实现。基于这样的理解，

本申请实施例本质上或者说对相关技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如计算机的软盘、只读存储器（Read-Only Memory, ROM）、随机存取存储器（Random Access Memory, RAM）、闪存（FLASH）、硬盘或光盘等，该计算机软件产品可包括多个指令用以使得一台移动终端执行本申请多个实施例所述的方法，移动终端可以是个人计算机，服务器，或者网络设备等。

上述数据加密装置、数据解密装置的实施例中，所包括的多个单元和模块只是按照功能逻辑进行划分的，但并不局限于上述的划分，只要能够实现相应的功能即可；另外，每个功能单元的名称也只是为了便于相互区分。

权 利 要 求 书

1、一种数据加密方法，包括:

在非可信执行环境中，确定应用请求加密的源数据;

在所述非可信执行环境中，生成与所述源数据对应的参考数据，所述参考数据是加密所述源数据的过程中一次性使用的数据;

在可信执行环境中，读取为所述应用生成的主密钥;

在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

在所述非可信执行环境中，使用所述安全数据对所述源数据进行加密，得到目标数据。

2、根据权利要求 1 所述的方法，其中，所述在所述非可信执行环境中，生成与所述源数据对应的参考数据，包括:

在所述非可信执行环境中，随机生成一数值，作为参考数据;

和/或，

在所述非可信执行环境中，读取当前的时间戳，作为参考数据。

3、根据权利要求 1 所述的方法，其中，所述在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据，包括:

在所述可信执行环境中，将所述参考数据与预设的标签组合，得到目标数组，所述标签用于表示安全数据的类型;

在所述可信执行环境中，使用所述主密钥将所述目标数组加密，得到候选数据;

在所述可信执行环境中，对所述候选数据规整为指定长度的数据，将所述指定长度的数据作为与所述标签匹配的安全数据。

4、根据权利要求 3 所述的方法，其中，所述安全数据的类型包括副密钥，或，副密钥和向量;

所述在所述可信执行环境中，对所述候选数据规整为指定长度的数据，将所述指定长度的数据作为与所述标签匹配的安全数据，包括:

在所述可信执行环境中，响应于所述标签为第一值，对所述候选数据计算第一指定长度的摘要数据，所述第一指定长度的摘要数据作为副密钥、向量;

或者，

在所述可信执行环境中，响应于所述标签为第二值，对所述候选数据计算第二指定长度的摘要数据，所述第二指定长度的摘要数据作为副密钥。

5、根据权利要求 1 所述的方法，其中，所述安全数据包括副密钥，或，副

密钥和向量;

所述在所述非可信执行环境中，使用所述安全数据对所述源数据进行加密，得到目标数据，包括:

在所述非可信执行环境中，调用对称密钥算法中的高级加密标准 AES 算法、使用所述向量作为初始化向量、与所述副密钥共同将所述源数据加密为目标数据;

或者，

在所述非可信执行环境中，调用对称密钥算法中的非 AES 算法、使用所述副密钥将所述源数据加密为目标数据。

6、根据权利要求 1-5 任一项所述的方法，还包括:

在所述非可信执行环境中，关联存储所述目标数据与所述参考数据。

7、根据权利要求 6 所述的方法，还包括:

检测删除所述目标数据的第二操作;

响应于所述第二操作，在所述非可信执行环境中删除所述目标数据与所述参考数据。

8、根据权利要求 1-5 任一项所述的方法，还包括:

检测卸载所述应用的第三操作;

响应于所述第三操作，在所述可信执行环境中删除为所述应用生成的主密钥;

响应于所述第三操作，在所述非可信执行环境中删除所述目标数据与所述参考数据。

9、一种数据解密方法，包括:

在非可信执行环境中，确定应用请求解密的目标数据;

在所述非可信执行环境中，读取与所述目标数据关联的参考数据，所述参考数据是解密所述目标数据的过程中一次性使用的数据;

在可信执行环境中，读取为所述应用生成的主密钥;

在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

在所述非可信执行环境中，使用所述安全数据对所述目标数据进行解密，获得源数据。

10、根据权利要求 9 所述的方法，还包括:

在所述非可信执行环境中，关联存储所述目标数据与所述参考数据。

11、根据权利要求 10 所述的方法，还包括:

检测删除所述目标数据的第二操作;

响应于所述第二操作，在所述非可信执行环境中删除所述目标数据与所述参考数据。

12、一种数据加密装置，包括:

源数据确定模块，设置为在非可信执行环境中，确定应用请求加密的源数据;

参考数据生成模块，设置为在所述非可信执行环境中，生成与所述源数据对应的参考数据，所述参考数据是加密所述源数据的过程中一次性使用的数据;

主密钥读取模块，设置为在可信执行环境中，读取为所述应用生成的主密钥;

安全数据生成模块，设置为在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

源数据加密模块，设置为在所述非可信执行环境中，使用所述安全数据对所述源数据进行加密，得到目标数据。

13、根据权利要求 12 所述的装置，其中，所述参考数据生成模块包括:

随机数值生成子模块，设置为在所述非可信执行环境中，随机生成一数值，作为参考数据;

和/或，

时间戳读取子模块，设置为在所述非可信执行环境中，读取当前的时间戳，作为参考数据。

14、一种数据解密装置，包括:

目标数据确定模块，设置为在非可信执行环境中，确定应用请求解密的目标数据;

参考数据读取模块，设置为在所述非可信执行环境中，读取与所述目标数据关联的参考数据，所述参考数据是解密所述目标数据的过程中一次性使用的数据;

主密钥读取模块，设置为在可信执行环境中，读取为所述应用生成的主密钥;

安全数据生成模块，设置为在所述可信执行环境中，使用所述主密钥对所述参考数据进行加密处理，获得安全数据;

目标数据解密模块，设置为在所述非可信执行环境中，使用所述安全数据

对所述目标数据进行解密，获得源数据。

15、根据权利要求 14 所述的装置，其中，所述安全数据生成模块包括:

目标数组组合子模块，设置为在所述可信执行环境中，将所述参考数据与预设的标签组合，得到目标数组，所述标签用于表示安全数据的类型;

候选数据生成子模块，设置为使用所述主密钥将所述目标数组加密，得到候选数据;

候选数据规整子模块，设置为对所述候选数据规整为指定长度的数据，将所述指定长度的数据作为与所述标签匹配的安全数据。

16、一种移动终端，所述移动终端包括:

一个或多个处理器;

存储器，设置为存储一个或多个程序;

所述一个或多个处理器，设置为执行所述一个或多个程序以实现如权利要求 1-8 中任一所述的数据加密方法或者如权利要求 9-11 中任一所所述的数据解密方法。

17、一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1-8 中任一所述的数据加密方法或者如权利要求 9-11 中任一所所述的数据解密方法。