

## 加密方法、装置及电子设备

### 相关申请的交叉引用

[01]本公开要求于 2022 年 3 月 21 日递交的、申请号为 202210280533.4 的中国专利申请的优先权，其全部内容在此通过引用并入本文中。

### 技术领域

[02]本公开涉及数据安全技术，特别涉及加密方法、装置及电子设备。

### 背景技术

[03]通常，每一软件都单独配备有专用于对该软件进行加密的加密媒介。这里的软件可泛指实现至少一种功能的程序（可按照特定顺序组织计算机数据和指令）。这里的加密媒介是通过密码、系统密钥或硬件密钥等参数（通常加密参数）来“限制和保护用户对软件使用”的媒介。

[04]在相关应用中，每一软件被配备的加密媒介仅被限定对该软件自身进行加密保护，并不能对该软件相关联的关联数据进行加密。这里，与软件相关联的关联数据比如为软件在被使用时待加载的软件配置信息、软件在被运行后产生的结果信息、在软件上新增加的功能等等。也即，上述关联数据虽然与软件相关联，但关联数据的加密均独立于软件自身的加密，不同关联数据的加密分别依赖于其被配备的对应的加密媒介进行加密，以软件依赖于加密媒介 a 加密为例，则软件在被使用时待加载的软件配置信息依赖于加密媒介 b 加密、软件在被运行后产生的结果信息依赖于加密媒介 c 加密、在软件上新增加的功能依赖于加密媒介 d 加密。如此，当软件加载上述软件配置信息、结果信息、软件上新增加的功能时，则需要加密媒介 a 融合加密媒介 b、加密媒介 c、加密媒介 d，即同时需要有 4 个加密媒介，加密非常繁琐。

### 发明内容

[05]本公开提供了加密方法、装置及电子设备，以实现软件、以及独立于该软件的其他软件使用同一加密媒介进行加密。

[06]本公开实施例提供一种加密方法，该方法包括：在当前已部署的用于对目标软件进

行加密保护的加密媒介中的用户私有区中记录私有加密信息；所述加密媒介还记录有专用于对所述目标软件进行加密保护的目标软件加密信息；在检测到针对所述目标软件相关联的关联数据进行加密的加密触发时，依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密；其中，所述关联数据的加密独立于所述目标软件的加密，所述关联数据包括以下至少一个：所述目标软件的软件配置信息、所述目标软件在被运行后产生的结果信息、自定义功能软件、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息；所述自定义功能软件通过在所述目标软件上增加用于实现自定义功能的程序实现。

[07]本公开实施例提供一种加密装置，该装置包括：部署单元，用于在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区中记录私有加密信息；所述加密媒介还记录有专用于对所述目标软件进行加密保护的目标软件加密信息；处理单元，用于在检测到针对所述目标软件相关联的关联数据进行加密的加密触发时，依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密；其中，所述关联数据的加密独立于所述目标软件的加密，所述关联数据包括以下至少一个：所述目标软件的软件配置信息、所述目标软件在被运行后产生的结果信息、自定义功能软件、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息；所述自定义功能软件通过在所述目标软件上增加用于实现自定义功能的程序实现。

[08]本公开实施例还提供了一种电子设备。该电子设备包括：处理器和机器可读存储介质；所述机器可读存储介质存储有能够被所述处理器执行的机器可执行指令；所述处理器用于执行机器可执行指令，以实现上述公开的方法的步骤。

[09]由以上技术方案可以看出，本公开中，通过在目标软件被配备的加密媒介中的用户私有区中记录私有加密信息，通过该私有加密信息对目标软件相关联的关联数据进行加密，实现了目标软件、以及目标软件相关联的关联数据使用同一加密媒介加密，降低加密复杂度，提高加密便利。

## 附图说明

[10]此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

[11]图 1 为本公开实施例提供的加密媒介的示例图。

[12]图 2 为本公开实施例提供的方法流程图。

[13]图 3 为本公开实施例提供的加密媒介另一示例图。

[14]图 4a 为本公开实施例提供的用户私有区记录私有加密信息的示例图。

[15]图 4b 为本公开实施例提供的用户私有区记录私有加密信息的另一示例图。

[16]图 5a 为本公开实施例提供的解密关联数据的示意图。

[17]图 5b 为本公开实施例提供的解密关联数据的另一示意图。

[18]图 6 为本公开实施例提供的装置结构图。

[19]图 7 为本公开实施例提供的电子设备结构图。

### 具体实施方式

[20]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是本公开的一些方面相一致的装置和方法的例子。

[21]在本公开使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本公开。在本公开中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。

[22]为了使本领域技术人员更好地理解本公开实施例提供的技术方案，下面先对本公开实施例涉及的加密媒介进行描述：

[23]在应用中，如图 1 所示，加密媒介包含但不限于如下区域：

[24]1) 专有读写区：只被授权于原始开发人员，允许原始开发人员写入数据和读取数据。在应用中，专有读写区记录了专用于对与加密媒介相匹配的软件进行加密的加密信息（也称软件加密信息）。

[25]2) 公共只读区：允许原始开发人员写入数据和读取数据，允许用户进行数据读取。公共只读区一般作为记录原始开发人员对外表达的信息的途径，让用户知晓原始开发人员想让用户知晓的信息，如最常见的加密媒介的基本信息（型号、开发商等等）。

[26]基于如上描述的加密媒介，在应用中，针对每一软件，可基于该软件被单独配备的

加密媒介在专有读写区记录的软件加密信息，比如密钥、密码等，对该软件进行加密，以对软件自身进行保护。但如背景技术中描述的，与软件相关联的关联数据虽然与软件关联，但其加密均独立于软件自身的加密，不同关联数据的加密分别依赖于其被配备的不同加密媒介进行加密，比如背景技术中描述的软件依赖于加密媒介 a 加密，软件在被使用时待加载的软件配置信息依赖于加密媒介 b 加密、软件在被运行后产生的结果信息依赖于加密媒介 c 加密、在软件上新增加的功能依赖于加密媒介 d 加密。

[27]基于此，当软件加载其相关联的关联数据时，软件被配备的加密媒介就需要融合关联数据被配备的加密媒介，比如当上述软件融合上述软件配置信息、结果信息、软件上新增加的功能时，则需要加密媒介 a 融合加密媒介 b、加密媒介 c、加密媒介 d，即同时需要有 4 个加密媒介，加密非常繁琐，也会引起极大的不便。

[28]为解决上述技术问题，本实施例提供了能解决上述技术问题的加密方法。

[29]图 2 举例示出了本公开实施例提供的加密方法。

[30]参见图 2，图 2 为本公开实施例提供的方法流程图。可选地，在本实施例中，该方法可应用于电子设备。这里，电子设备可为对软件进行管理或控制的设备，本实施例并不具体限定。

[31]如图 2 所示，该流程可包括以下步骤：

[32]步骤 201，在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区中记录私有加密信息。

[33]这里，目标软件可泛指任一软件。

[34]可选地，在本实施例中，为了解决上述技术问题，则可针对目标软件配备的加密媒介进行如下改进：在加密媒介中设置用户私有区。图 3 示出了在如图 1 所示的加密媒介中增加了用户私有区。可选地，在本实施例中，用户私有区在加密媒介中的具体位置并不限定，只要保证不与加密媒介中现有已划分的区域比如专有读写区、公共只读区等冲突即可。

[35]在本实施例中，用户私有区被授权于记录私有加密信息。

[36]为了实现在上述用户私有区中记录私有加密信息，作为一个实施例，可针对上述目标软件配套增加相应的外部接口，以实现通过该外部接口在用户私有区中记录私有加密信息。具体地，如图 4a 所示，在用户私有区中记录私有加密信息可包括：通过新设置

的上述目标软件对应的外部接口，接收外部写入至用户私有区的私有加密信息。即实现了在用户私有区中记录私有加密信息。

[37]作为另一实施例，还可借用目标软件对应的软件交互界面来实现在用户私有区中记录私有加密信息。具体地，如图 4b 所示，在用户私有区中记录私有加密信息可包括：通过目标软件对应的软件交互界面接收外部输入的待写入至用户私有区的私有加密信息，将该私有加密信息写入上述用户私有区。即最终实现了在用户私有区中记录私有加密信息。

[38]需要说明的是，在本实施例中，用户私有区中记录的私有加密信息可基于实际需求被动态修改、删除等。

[39]步骤 202，在检测到针对目标软件相关联的关联数据进行加密的加密触发时，执行步骤 203。

[40]在本实施例中，上述关联数据与目标软件相关联，但关联数据的加密独立于目标软件的加密。可选地，在本实施例中，关联数据包括以下至少一个：目标软件的软件配置信息、目标软件在被运行后产生的结果信息、自定义功能软件、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息。需要说明的是，在本实施例中，上述与目标软件相关联的关联数据可根据实际需求定义，比如，上述关联数据也可不涵盖自定义功能软件，而仅涵盖自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息，等等，本实施例并不一一限定。

[41]在本实施例中，自定义功能软件通过在目标软件上新增加用于实现自定义功能的程序实现，比如在目标软件上新增用户自定义的工具、或者用户自定义的信息等，该新增的用户自定义的工具、或者用户自定义的信息等可统称自定义功能软件。

[42]按照相关技术中的加密方式，软件的每一关联数据在加密时需配备有对应的加密媒介。而本实施例中，不再针对软件的关联数据配备对应的加密媒介，通过在软件被配备的加密媒介中扩展用户私有区来实现对关联数据的加密，具体见步骤 203。这里暂不赘述。

[43]在本实施例中，上述电子设备会对外提供一个界面，该界面可为上述目标软件的交互界面，也可为对目标软件进行管理的管理界面（不同于该目标软件的交互界面）。但不管哪一界面，在本实施例中，在检测到针对目标软件相关联的关联数据进行加密的加密触发时（例如，在上述界面上设置关联数据相关联的触发标识（比如按钮等），如果

检测到上述触发标识被触发，则检测到对该关联数据进行加密的加密触发)，可及时获知相对应的关联数据以进行加密。

[44]步骤 203，依据加密媒介中上述用户私有区记录的与该关联数据相对应的私有加密信息，对该关联数据进行加密。

[45]作为一个实施例，上述用户私有区可记录一个私有加密信息。该私有加密信息可用于对目标软件相关联的所有关联数据进行加密。也就是说，上述用户私有区记录的私有加密信息与所有该目标软件的关联数据相对应。

[46]作为一个实施例，上述用户私有区可记录两个以上私有加密信息，以对应至少两个不同关联数据，比如，上述用户私有区可记录以下三个私有加密信息：密钥 a1、密钥 a2、密钥 a3，目标软件的软件配置信息与上述用户私有区记录的密钥 a1 对应，目标软件在被运行后产生的结果信息与密钥 a2 对应，自定义功能软件与密钥 a3 对应，则在针对目标软件相关联的关联数据进行加密时，先识别该关联数据具体是什么，比如关联数据为软件配置信息，则基于上述用户私有区记录的密钥 a1 对软件配置信息进行加密，再比如关联数据为上述结果信息，则基于上述用户私有区记录的密钥 a2 对结果信息进行加密，依次类推。

[47]需要说明的是，在本实施例中，自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息对应的私有加密信息可相同，比如都可为自定义功能软件对应的私有加密信息。当然，自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息对应的私有加密信息也可不同，比如上述用户私有区可额外定义两类私有加密信息，其中一类为自定义功能软件的软件配置信息对应的私有加密信息，另一类为自定义功能软件在被运行后产生的结果信息所对应的私有加密信息，等，本实施例并不一一限定。

[48]最终，通过上述步骤 203，本实施例实现了通过软件被配备的加密媒介对与软件相关联的关联数据进行加密。

[49]通过图 2 所示流程可以看出，在本实施例中，通过在目标软件被配备的加密媒介中的用户私有区中记录私有加密信息，通过该私有加密信息对目标软件相关联的关联数据进行加密，实现了目标软件、以及目标软件相关联的关联数据使用同一加密媒介加密，降低加密复杂度，提高加密便利。

[50]可选地，在本实施例中，若所述关联数据包括以下至少一个：目标软件在被运行时

的软件配置信息、目标软件在被运行后产生的结果信息、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息，则在上述步骤 203 依据加密媒介中用户私有区记录的与关联数据相对应的私有加密信息对关联数据进行加密之后，该方法进一步包括：在接收到需将上述被加密的关联数据加载至所述目标软件上运行的加载触发时，按照重叠加密对应的解密方式对被加密的关联数据进行解密。具体如图 5a 所示。

[51]如图 5a 所示，在按照重叠加密对应的解密方式对被加密的关联数据进行解密时，从上述目标软件被配备的加密媒介中读取目标软件加密信息和上述被加密的关联数据相对应的私有加密信息，并分别对读取的目标软件加密信息和私有加密信息进行校验，若校验通过，则将被加密的关联数据解密并加载至目标软件上运行；否则，显示加载失败。

[52]可选地，在本实施例中，在上述步骤 203 依据加密媒介中用户私有区记录的与关联数据相对应的私有加密信息对关联数据进行加密时，会记录当前使用的私有加密信息以及当前记录的目标软件加密信息。基于此，上述对读取的目标软件加密信息和私有加密信息进行校验可包括：检查当前读取的目标软件加密信息是否为之前已记录的在上述步骤 203 在对关联数据进行加密时的目标软件加密信息，以及检查当前读取的私有加密信息是否为之前已记录的在上述步骤 203 在对关联数据进行加密时的私有加密信息，如果是，则确定校验通过，否则，校验失败。

[53]可以看出，在本实施例中，若上述关联数据包括以下至少一个：目标软件在被运行时的软件配置信息、目标软件在已被运行后产生的结果信息、自定义功能软件的软件配置信息、自定义功能软件在已被运行后产生的结果信息，则在上述步骤 203 中虽然利用私有加密信息对关联数据进行加密，其隐含着关联数据的重叠加密。对应地，一旦需要加载该关联数据时，则需要如上描述，按照重叠加密对应的解密方式对被加密的关联数据进行解密。

[54]在本实施例中，若关联数据至少包括：自定义功能软件；则在上述步骤 203 依据加密媒介中用户私有区记录的与关联数据相对应的私有加密信息对关联数据进行加密之后，该方法进一步包括：在接收到使用目标软件提供的功能的触发时，按照分布式加密对应的解密提供该功能。具体如图 5b 所示。

[55]如图 5b 所示，当接收到使用基于目标软件新开发的自定义功能软件提供的自定义功能的触发时，从加密媒介中读取被加密的自定义功能软件相对应的私有加密信息，对读取的私有加密信息进行校验，若校验通过，则对自定义功能软件进行解密并允许使用自定义功能软件提供的自定义功能，否则，禁止使用自定义功能软件提供的自定义功能；

而当接收到使用目标软件提供的原有功能的触发时，从加密媒介中读取目标软件加密信息，对读取的目标软件加密信息进行校验，若校验通过，则允许使用目标软件提供的原有功能，否则，禁止使用目标软件提供的原有功能。这里，对读取的私有加密信息进行校验、对读取的目标软件加密信息进行校验如上描述，不再赘述。

[56]在本实施例中，即使在用户私有区中记录私有加密信息，该用户私有区中记录的私有加密信息也并非一直不变，也可被更新或者删除。

[57]本实施例中，可通过新设置的目标软件对应的外部接口，或者通过目标软件对应的软件交互界面接收外部输入的用于更新用户私有区中私有加密信息的更新消息，并依据更新消息更新用户私有区中已记录的私有加密信息；比如将用户私有区中已记录的私有加密信息更新为该更新消息携带的私有加密信息等。由此实现了更新用户私有区中的私有加密信息。

[58]本实施例中，当通过新设置的目标软件对应的外部接口或者通过目标软件对应的软件交互界面，接收删除指令时，可依据删除指令删除用户私有区中已记录的私有加密信息。由此实现了删除用户私有区中的私有加密信息。

[59]以上对本公开实施例提供的方法进行了描述，下面对本公开实施例提供的装置进行描述：

[60]参见图 6，图 6 为本公开实施例提供的加密装置结构图。如图 6 所示，该装置可包括：

[61]部署单元，用于在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区中记录私有加密信息；所述加密媒介还记录有专用于对所述目标软件进行加密保护的目标软件加密信息；

[62]处理单元，用于在检测到针对所述目标软件相关联的关联数据进行加密的加密触发时，依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密；

[63]其中，所述关联数据的加密独立于所述目标软件的加密，所述关联数据包括以下至少一个：所述目标软件的软件配置信息、所述目标软件在被运行后产生的结果信息、自定义功能软件、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息；所述自定义功能软件通过在所述目标软件上增加用于实现自定义功能的程序实现。

[64]可选地，当在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区记录私有加密信息时，所述部署单元用于：

[65]通过新设置的所述目标软件对应的外部接口，接收外部写入至所述用户私有区的所述私有加密信息；或者，

[66]通过所述目标软件对应的软件交互界面接收外部输入的待写入至所述用户私有区的所述私有加密信息，将所述私有加密信息写入所述用户私有区。

[67]可选地，若所述关联数据包括以下至少一个：所述目标软件在被运行时的软件配置信息、所述目标软件在被运行后产生的结果信息、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息，则处理单元在依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密之后，进一步在接收到将被加密的所述关联数据加载至所述目标软件上运行的加载触发时，从所述加密媒介中读取所述目标软件加密信息、以及被加密的所述关联数据相对应的私有加密信息，并分别对读取的目标软件加密信息和私有加密信息进行校验，若校验通过，则将被加密的所述关联数据解密并加载至所述目标软件上运行；否则，显示加载失败。

[68]若所述关联数据至少包括：所述自定义功能软件，处理单元在依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密之后，进一步在接收到使用所述自定义功能软件提供的自定义功能的触发时，从所述加密媒介中读取被加密的所述自定义功能软件相对应的私有加密信息，对读取的私有加密信息进行校验，若校验通过，则对所述自定义功能软件进行解密并允许使用所述自定义功能软件提供的自定义功能，否则，禁止使用所述自定义功能软件提供的自定义功能以及，在接收到使用所述目标软件提供的原有功能的触发时，从所述加密媒介中读取所述目标软件加密信息，对所述目标软件加密信息进行校验，若校验通过，则允许使用所述目标软件提供的原有功能，否则，禁止使用所述目标软件提供的原有功能。

[69]可选地，部署单元在用户私有区中记录私有加密信息之后，进一步通过所述目标软件对应的外部接口，或者通过所述目标软件对应的软件交互界面接收外部输入的用于更新所述用户私有区中私有加密信息的更新消息；依据所述更新消息更新所述用户私有区中已记录的私有加密信息；或者，通过所述目标软件对应的外部接口，或者通过所述目标软件对应的软件交互界面，接收删除指令，依据所述删除指令删除所述用户私有区中已记录的私有加密信息。

[70]本公开实施例还提供了图 6 所示装置的硬件结构。参见图 7，图 7 为本公开实施例提供的电子设备结构图。如图 7 所示，该硬件结构可包括处理器和机器可读存储介质，机器可读存储介质存储有能够被所述处理器执行的机器可执行指令；所述处理器用于执行机器可执行指令，以实现本公开上述示例公开的方法。

[71]基于与上述方法同样的申请构思，本公开实施例还提供一种机器可读存储介质，所述机器可读存储介质上存储有若干计算机指令，所述计算机指令被处理器执行时，能够实现本公开上述示例公开的方法。

[72]示例性的，上述机器可读存储介质可以是任何电子、磁性、光学或其它物理存储装置，可以包含或存储信息，如可执行指令、数据，等等。例如，机器可读存储介质可以是：RAM（Random Access Memory，随机存取存储器）、易失存储器、非易失性存储器、闪存、存储驱动器（如硬盘驱动器）、固态硬盘、任何类型的存储盘（如光盘、dvd 等），或者类似的存储介质，或者它们的组合。

[73]上述实施例阐明的系统、装置、模块或单元，具体可以由计算机实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[74]为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本公开时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[75]本领域内的技术人员应明白，本公开的实施例可提供为方法、系统、或计算机程序产品。因此，本公开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，本公开实施例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。

[76]本公开是参照根据本公开实施例的方法、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。应理解可以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、嵌入式处理机或其它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它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。

[77]而且，这些计算机程序指令也可以存储在能引导计算机或其它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者多个流程和/或方框图一个方框或者多个方框中指定的功能。

[78]这些计算机程序指令也可装载到计算机或其它可编程数据处理设备上，使得在计算机或者其它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，从而在计算机或其它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。

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

### 权利要求书

1、一种加密方法，包括：

在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区记录私有加密信息；所述加密媒介还记录有专用于对所述目标软件进行加密的目标软件加密信息；

在检测到针对所述目标软件相关联的关联数据进行加密的加密触发时，依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密；

其中，所述关联数据的加密独立于所述目标软件的加密，所述关联数据包括以下至少一个：所述目标软件的软件配置信息、所述目标软件在被运行后产生的结果信息、自定义功能软件、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息；所述自定义功能软件通过在所述目标软件上增加用于实现自定义功能的程序实现。

2、根据权利要求1所述的方法，其中，所述在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区记录私有加密信息包括：

通过所述目标软件对应的外部接口，接收外部写入至所述用户私有区的所述私有加密信息；或者，

通过所述目标软件对应的软件交互界面接收外部输入的待写入至所述用户私有区的所述私有加密信息，将所述私有加密信息写入所述用户私有区。

3、根据权利要求1所述的方法，其中，

若所述关联数据包括以下至少一个：所述目标软件在被运行时的软件配置信息、所述目标软件在被运行后产生的结果信息、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息，则在依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密之后，该方法进一步包括：

在接收到将被加密的所述关联数据加载至所述目标软件上运行的加载触发时，从所述加密媒介中读取所述目标软件加密信息、以及被加密的所述关联数据相对应的私有加密信息，并分别对读取的目标软件加密信息和私有加密信息进行校验，若校验通过，则将被加密的所述关联数据解密并加载至所述目标软件上运行。

4、根据权利要求1所述的方法，其中，

若所述关联数据至少包括：所述自定义功能软件；在依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密之后，该

方法进一步包括:

在接收到使用所述自定义功能软件提供的自定义功能的触发时,从所述加密媒介中读取被加密的所述自定义功能软件相对应的私有加密信息,对读取的私有加密信息进行校验,若校验通过,则对所述自定义功能软件进行解密并允许使用所述自定义功能软件提供的自定义功能,若校验不通过,禁止使用所述自定义功能软件提供的自定义功能。

5、根据权利要求4所述的方法,其中,该方法进一步包括:

在接收到使用所述目标软件提供的原有功能的触发时,从所述加密媒介中读取所述目标软件加密信息,对所述目标软件加密信息进行校验,若校验通过,则对所述目标软件解密并允许使用所述目标软件提供的原有功能,若校验不通过,禁止使用所述目标软件提供的原有功能。

6、根据权利要求1至5任一所述的方法,其中,在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区记录私有加密信息之后,该方法进一步包括:

通过所述目标软件对应的外部接口,或者通过所述目标软件对应的软件交互界面接收外部输入的用于更新所述用户私有区中私有加密信息的更新消息;

依据所述更新消息更新所述用户私有区中已记录的私有加密信息。

7、根据权利要求1至5任一所述的方法,其中,在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区记录私有加密信息之后,该方法进一步包括:

通过所述目标软件对应的外部接口,或者通过所述目标软件对应的软件交互界面,接收删除指令;

依据所述删除指令删除所述用户私有区中已记录的私有加密信息。

8、一种加密装置,包括:

部署单元,用于在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区中记录私有加密信息;所述加密媒介还记录有专用于对所述目标软件进行加密的目标软件加密信息;

处理单元,用于在检测到针对所述目标软件相关联的关联数据进行加密的加密触发时,依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密;

其中,所述关联数据的加密独立于所述目标软件的加密,所述关联数据包括以下至少一个:所述目标软件的软件配置信息、所述目标软件在被运行后产生的结果信息、自定义功能软件、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息;所述自定义功能软件通过在所述目标软件上增加用于实现自定义功能的程序实

现。

9、根据权利要求 8 所述的加密装置，其中，当在当前已部署的用于对目标软件进行加密保护的加密媒介中的用户私有区记录私有加密信息时，所述部署单元用于：

通过所述目标软件对应的外部接口，接收外部写入至所述用户私有区的所述私有加密信息；或者，

通过所述目标软件对应的软件交互界面接收外部输入的待写入至所述用户私有区的所述私有加密信息，将所述私有加密信息写入所述用户私有区。

10、根据权利要求 8 所述的加密装置，其中，

若所述关联数据包括以下至少一个：所述目标软件在被运行时的软件配置信息、所述目标软件在被运行后产生的结果信息、自定义功能软件的软件配置信息、自定义功能软件在被运行后产生的结果信息，则所述处理单元在依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密之后，进一步用于在接收到将被加密的所述关联数据加载至所述目标软件上运行的加载触发时，从所述加密媒介中读取所述目标软件加密信息、以及被加密的所述关联数据相对应的私有加密信息，并分别对读取的目标软件加密信息和私有加密信息进行校验，若校验通过，则将被加密的所述关联数据解密并加载至所述目标软件上运行。

11、根据权利要求 8 所述的加密装置，其中，

若所述关联数据至少包括：所述自定义功能软件，所述处理单元在依据所述加密媒介中所述用户私有区记录的与所述关联数据相对应的私有加密信息对所述关联数据进行加密之后，进一步用于在接收到使用所述自定义功能软件提供的自定义功能的触发时，从所述加密媒介中读取被加密的所述自定义功能软件相对应的私有加密信息，对读取的私有加密信息进行校验，若校验通过，则对所述自定义功能软件进行解密并允许使用所述自定义功能软件提供的自定义功能，若校验不通过，禁止使用所述自定义功能软件提供的自定义功能。

12、根据权利要求 11 所述的加密装置，其中，

所述处理单元进一步用于在接收到使用所述目标软件提供的原有功能的触发时，从所述加密媒介中读取所述目标软件加密信息，对所述目标软件加密信息进行校验，若校验通过，则允许使用所述目标软件提供的原有功能，若校验不通过，禁止使用所述目标软件提供的原有功能。

13、根据权利要求 8 至 12 任一所述的加密装置，其中，部署单元在用户私有区中记录私有加密信息之后，进一步通过所述目标软件对应的外部接口，或者通过所述目标

软件对应的软件交互界面接收外部输入的用于更新所述用户私有区中私有加密信息的更新消息；依据所述更新消息更新所述用户私有区中已记录的私有加密信息。

14、根据权利要求 8 至 12 任一所述的加密装置，其中，部署单元在用户私有区中记录私有加密信息之后，进一步通过所述目标软件对应的外部接口，或者通过所述目标软件对应的软件交互界面，接收删除指令，依据所述删除指令删除所述用户私有区中已记录的私有加密信息。

15、一种电子设备，包括：处理器和机器可读存储介质；

所述机器可读存储介质存储有能够被所述处理器执行的机器可执行指令；

所述处理器用于执行机器可执行指令，以实现权利要求 1-7 任一项的方法步骤。

16、一种非易失性存储介质，其上存储有计算机指令，当所述计算机指令被处理器调用时，所述处理器执行权利要求 1-7 任一项所述的方法步骤。