ENCRYPTION METHOD AND APPARATUS, AND ELECTRONIC DEVICE

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present disclosure claims the priority of the Chinese patent application filed on March 21, 2022, with application number 202210280533.4, the entire contents of which are incorporated herein by reference.

TECHNICAL FIELD

[0002] The present disclosure relates to data security technology, in particular to an encryption method and apparatus, and an electronic device.

BACKGROUND

[0003] Usually, each software is equipped with a dedicated encryption medium for encrypting the software. The software here can generally refer to a program (where computer data and instructions can be organized in a specific order) that implements at least one function. The encryption medium here is a medium that performs restriction and protection on software usage of users through parameters (general encryption parameters) such as passwords, system keys, or hardware keys.

[0004] In related applications, the encryption medium provided for a software is only limited to encrypting and protecting the software itself, and cannot encrypt associated data associated with the software. Here, the associated data associated with the software can be software configuration information to be loaded when the software is used, result information generated after the software is run, and a newly added function on the software, etc. That is, although the associated data mentioned above is associated with the software, the encryption of the associated data is independent of the software's own encryption. The encryption of different associated data depends on the respective encryption medium with which the associated data is equipped. Taking the software depending on an encryption medium *a* for encryption as an example, the software configuration information to be loaded when the software is used depends on an encryption medium *b* for encryption, the result information generated after the software is run depends on an encryption medium *c* for encryption, and the newly added function on the software depends on an encryption medium *d* for encryption. Therefore, when the software loads the software configuration information, the result information, and the newly added function, it is necessary to merge the encryption medium *a* with the encryption medium *b*, the encryption medium *c* and the encryption medium *d*, that is, four encryption media are

needed at the same time, and encryption is very cumbersome.

SUMMARY

[0005] The present disclosure provides encryption methods and apparatuses, and electronic devices to enable software and other software independent of the software to be encrypted using the same encryption medium.

[0006] The embodiments of the present disclosure provide an encryption method, including: recording private encryption information in a user private region of an encryption medium currently deployed, where the encryption medium is for encryption of a target software, and the encryption medium further records target software encryption information configured to encrypt the target software; and in response to detection of an encryption trigger for encrypting associated data associated with the target software, encrypting the associated data according to private encryption information corresponding to the associated data recorded in the user private region of the encryption medium; where encryption of the associated data is independent of encryption of the target software, and the associated data includes at least one of: software configuration information of the target software, result information generated after the target software is run, a custom function software, software configuration information of the custom function software, and result information generated after the custom function software is run, where the custom function software is implemented by adding a program for implementing a custom function on the target software.

[0007] The embodiments of the present disclosure provide an encryption apparatus, including: a deploying unit, configured to record private encryption information in a user private region of an encryption medium currently deployed, where the encryption medium is for encryption of a target software, and the encryption medium further records target software encryption information configured to encrypt the target software; and a processing unit, configured to, in response to detection of an encryption trigger for encrypting associated data associated with the target software, encrypt the associated data according to private encryption information corresponding to the associated data recorded in the user private region of the encryption medium; where encryption of the associated data is independent of encryption of the target software, and the associated data includes at least one of: software configuration information of the target software, result information generated after the target software is run, a custom function software, software configuration information of the custom function software, and result information generated after the custom function software is run, where the

custom function software is implemented by adding a program for implementing a custom function on the target software.

[0008] The embodiments of the present disclosure further provide an electronic device. The electronic device includes one or more processors and one or more machine readable storage media; where the one or more machine readable storage media store a machine executable instruction that can be executed by the one or more processors; and the one or more processors are configured to execute the machine executable instruction to implement the above method.

[0009] From the above technical solutions, it can be seen that in the present disclosure, private encryption information is recorded in the user private region in the encryption medium provided for the target software. By encrypting the associated data of the target software through the private encryption information, the target software and its associated data are encrypted using the same encryption medium, which reduces encryption complexity and improves encryption convenience.

BRIEF DESCRIPTION OF DRAWINGS

[0010] Accompanying drawings herein are incorporated into and constitute a part of the specification, illustrate embodiments consistent with the present disclosure, and are combined with the description to explain the principle of the present disclosure.

[0011] FIG. 1 is a schematic diagram of an encryption medium according to embodiments of the present disclosure.

[0012] FIG. 2 is a method flowchart according to embodiments of the present disclosure.

[0013] FIG. 3 is schematic of another encryption medium according to embodiments of the present disclosure.

[0014] FIG. 4a is a schematic diagram of a user private region recording private encryption information according to embodiments of the present disclosure.

[0015] FIG. 4b is a schematic diagram of a user private region recording private encryption information according to embodiments of the present disclosure.

[0016] FIG. 5a is a schematic diagram of decrypting associated data according to embodiments of the present disclosure.

[0017] FIG. 5b is a schematic diagram of decrypting associated data according to embodiments of the present disclosure.

[0018] FIG. 6 is a structural diagram of an apparatus according to embodiments of the present disclosure.

[0019] FIG. 7 is a structural diagram of an electronic device according to embodiments of the

present disclosure.

DETAILED DESCRIPTION

[0020] Embodiments will be described in detail here with the examples thereof expressed in the drawings. When the following descriptions involve the drawings, like numerals in different drawings represent like or similar elements unless stated otherwise. Embodiments described in the illustrative examples below are not intended to represent all embodiments consistent with the present disclosure. Rather, they are merely embodiments of devices and methods consistent with some aspects of the present disclosure.

[0021] Terms used in the present disclosure is only for the purpose of describing particular embodiments and is not intended to limit the present disclosure. As used in the present disclosure, the singular forms “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise.

[0022] In order to enable those skilled in the art to better understand the technical solution provided in the embodiments of the present disclosure, the following will first describe the encryption medium involved in the embodiments of the present disclosure.

[0023] In the application, as shown in FIG. 1, the encryption medium includes but is not limited to the following regions 1) and 2).

[0024] 1) Dedicated read and write region: authorized only to original developers, allowing original developers to write and read data. In applications, the dedicated read and write region records encryption information (also known as software encryption information) specifically designed to encrypt software that matches the encryption medium.

[0025] 2) Public read-only region: allowing original developers to write and read data, and allowing users to read data. The public read-only region is generally used as a method to record the information expressed by the original developer to the outside world, allowing users to know the information that the original developer wants users to know, such as the most common basic information (model, developer, etc.) of the encryption medium.

[0026] Based on the encryption medium described above, in applications, for each software, the software can be encrypted based on the software encryption information (such as keys, passwords, etc.) recorded in the dedicated read and write region in the encryption medium separately provided for the software, to protect the software. However, as described in the background, although the associated data is associated with the software, the encryption of the associated data is independent of the encryption of the software. The encryption of different associated data depends on different encryption media which are provided for encryption. For

example, the software described in the background depends on an encryption medium *a* for encryption, the software configuration information to be loaded when the software is used depends on an encryption medium *b* for encryption, the result information generated after the software is run depends on an encryption medium *c* for encryption, and the newly added function on the software depends on an encryption medium *d* for encryption.

[0027] Based on this, when the software loads its associated data, the encryption medium equipped for the software needs to integrate the encryption media equipped for the associated data. For example, when the above software integrates the software configuration information, result information, and newly added functions, the encryption medium *a* needs to integrate the encryption medium *b*, the encryption medium *c*, and the encryption medium *d*, which requires four encryption media at the same time. The encryption is very cumbersome and can cause great inconvenience.

[0028] To solve the above technical problem, this embodiment provides an encryption method that can solve the above technical problem.

[0029] FIG. 2 illustrates the encryption method according to embodiments of the present disclosure.

[0030] Referring to FIG. 2, FIG. 2 is a method flowchart according to embodiments of the present disclosure. Optionally, in this embodiment, the method can be applied to an electronic device. Here, the electronic device can be a device that manages or controls a software, which is not limited in the embodiments of the present disclosure.

[0031] As shown in FIG. 2, the method may include the following steps 201 to 203.

[0032] In step 201, private encryption information is recorded in a user private region of an encryption medium currently deployed, where the encryption medium is for encryption of a target software.

[0033] The target software can generally refer to any one software.

[0034] Optionally, in this embodiment, to address the aforementioned technical problem, the following improvements can be made to the encryption medium provided for the target software: setting a user private region in the encryption medium. FIG. 3 illustrates an addition of a user private region in the encryption medium shown in FIG. 1. Optionally, in this embodiment, a specific location of the user private region in the encryption medium is not limited, as long as the specific location of the user private region does not conflict with existing partitioned regions in the encryption medium, such as the dedicated read and write region and the public read-only region, etc.

[0035] In this embodiment, the user private region is authorized to record private encryption information.

[0036] To achieve the recording of private encryption information in the user private region mentioned above, as an embodiment, a corresponding external interface can be added to the target software to achieve the recording of private encryption information in the user private region through the external interface. Specifically, as shown in FIG. 4a, recording the private encryption information in the user private region may include receiving, through the newly set external interface for the target software, the private encryption information written externally to the user private region. This enables the recording of the private encryption information in the user private region.

[0037] As another embodiment, a software interaction interface for the target software can also be used to record the private encryption information in the user private region. Specifically, as shown in FIG. 4b, recording the private encryption information in the user private region may include receiving, through a software interaction interface for the target software, external input of the private encryption information to be written into the user private region, and writing the private encryption information into the user private region. This enables the recording of the private encryption information in the user private region.

[0038] It should be noted that in this embodiment, the private encryption information recorded in the user private region can be dynamically modified, or deleted, etc. based on actual needs.

[0039] In step 202, in response to detection of an encryption trigger for encrypting associated data associated with the target software, step 203 is executed.

[0040] In this embodiment, the associated data is associated with the target software, but the encryption of the associated data is independent of the encryption of the target software. Optionally, in this embodiment, the associated data includes at least one of: software configuration information of the target software, result information generated after the target software is run, a custom function software, software configuration information of the custom function software, and result information generated after the custom function software is run. It should be noted that in this embodiment, the associated data associated with the target software mentioned above can be defined according to actual needs. For example, the associated data may not include custom function software, but only include software configuration information of the custom function software, and result information generated after the custom function software is run, etc, which is not limited in the embodiment.

[0041] In this embodiment, the custom function software is implemented by adding a program for implementing a custom function on the target software, such as adding a user-defined tool or user-defined information in the target software. The newly added user-defined tool or user-defined information can be collectively referred to as the custom function software.

[0042] According to encryption methods in relative arts, each associated data of the software needs to be provided with a respective encryption medium during encryption. In this embodiment, a corresponding encryption medium is no longer provided for the associated data of the software. The encryption of the associated data is achieved by adding a user private region in the encryption medium provided for the software, as detailed in step 203, which is not described here.

[0043] In this embodiment, the above-mentioned electronic device can provide an interface to the outside world, which can be an interaction interface of the target software or a management interface (different from the interaction interface) for managing the target software. However, no matter which interface, in this embodiment, when an encryption trigger for encrypting the associated data associated with the target software is detected (for example, a trigger identifier (such as a button) associated with the associated data is set in the above interface, and if it is detected that the trigger identifier is triggered, an encryption trigger for encrypting the associated data is detected), the corresponding associated data can be obtained in a timely manner for encryption.

[0044] In step 203, the associated data is encrypted according to private encryption information corresponding to the associated data recorded in the user private region of the encryption medium.

[0045] As an embodiment, the user private region mentioned above can record one piece of private encryption information. The piece of private encryption information can be used to encrypt all associated data associated with the target software. That is, the private encryption information recorded in the user private region corresponds to all associated data of the target software.

[0046] As an embodiment, the user private region can record two or more pieces of private encryption information to correspond to at least two different associated data. For example, the user private region can record the following three pieces of private encryption information: key a1, key a2, and key a3. The software configuration information of the target software corresponds to key a1 recorded in the user private region. The result information generated after the target software is run corresponds to key a2, and the custom function software corresponds to key a3. When the associated data associated with the target software is

encrypted, the specific associated data is identified first. For example, if the associated data is software configuration information, the software configuration information is encrypted based on the key a1 recorded in the user private region. For example, if the associated data is the result information, the result information is encrypted based on the key a2 recorded in the user private region, and so on.

[0047] It should be noted that in this embodiment, the private encryption information for the software configuration information of the custom function software and the private encryption information for the result information generated after the custom function software is run can be the same, and for example, both can be private encryption information for the custom function software. Of course, the private encryption information for the software configuration information of the custom function software and the private encryption information for the result information generated after the custom function software is run can also be different. For example, the user private region can further define two types of private encryption information. One type is the private encryption information for the software configuration information of the custom function software, and the other one is the private encryption information for the result information generated after the custom function software is run, which is not limited in the embodiment.

[0048] Finally, through the above step 203, this embodiment achieves the encryption of associated data associated with the software through the encryption medium provided for the software.

[0049] From the process shown in FIG. 2, it can be seen that in this embodiment, private encryption information is recorded in the user private region in the encryption medium equipped for the target software. By encrypting the associated data associated with the target software through the private encryption information, the target software and its associated data are encrypted using the same encryption medium, which reduces encryption complexity and improves encryption convenience.

[0050] In some embodiments, step 202 may not be executed, and step 203 may be directly executed after step 201 is executed.

[0051] Optionally, in this embodiment, the associated data includes at least one of: software configuration information of the target software when the target software is running, result information generated after the target software is run, software configuration information of the custom function software, and result information generated after the custom function software is run, and after the step 203 of encrypting the associated data according to the private encryption information corresponding to the associated data recorded in the user private region

of the encryption medium, the method further includes: when the loading trigger for loading the encrypted associated data into the target software for operation is received, the encrypted associated data is decrypted according to the decryption method corresponding to overlapping encryption, as shown in FIG. 5a.

[0052] As shown in FIG. 5a, if the encrypted associated data is decrypted according to the decryption method corresponding to overlapping encryption, the target software encryption information and private encryption information for the encrypted associated data are read from the encryption medium provided for the target software, the target software encryption information and the private encryption information are separately verified, and in response to determining that the verification is successful, the encrypted associated data is decrypted and the associated data is loaded into the target software for operation, otherwise, loading failure is displayed.

[0053] Optionally, in this embodiment, in step 203 above, when the associated data is encrypted according to private encryption information corresponding to the associated data recorded in the user private region of the encryption medium, the currently used private encryption information and the currently recorded target software encryption information can be recorded. Based on this, the verification of the read target software encryption information and private encryption information can include checking whether the currently read target software encryption information is the previously recorded target software encryption information when encrypting the associated data in step 203, and checking whether the currently read private encryption information is the previously recorded private encryption information when encrypting the associated data in step 203, and if so, it is determined that the verification is successful, otherwise, the verification fails.

[0054] It can be seen that in this embodiment, if the associated data includes at least one of: software configuration information of the target software when the target software is running, result information generated after the target software has been run, software configuration information of the custom function software, and result information generated after the custom function software has been run, in step 203 above, although private encryption information is used to encrypt the associated data, it implies overlapping encryption of the associated data. Correspondingly, once the associated data needs to be loaded, it is necessary to decrypt the encrypted associated data according to the decryption method corresponding to overlapping encryption, as described above.

[0055] In this embodiment, the associated data at least includes: the custom function software; and after the step 203 of encrypting the associated data according to the private encryption

information corresponding to the associated data recorded in the user private region of the encryption medium, the method further includes: when a trigger of use of the function provided by the target software is received, the function is provided according to the decryption corresponding to distributed encryption, as shown in FIG. 5b.

[0056] As shown in FIG. 5b, in response to receiving a trigger of use of a custom function provided by the custom function software developed based on the target software, private encryption information for encrypted custom function software is read from the encryption medium, the private encryption information is verified, and in response to determining that the verification is successful, the custom function software is decrypted and the use of the custom function provided by the custom function software is allowed; otherwise, the use of the custom function provided by the custom function software is prohibited. In response to receiving a trigger of use of an original function provided by the target software, the target software encryption information is read from the encryption medium, the target software encryption information is verified, and in response to determining that the verification is successful, the target software is decrypted and the use of the original function provided by the target software is allowed; in response to determining that the verification fails, the use of the original function provided by the target software is prohibited. Verifying the private encryption information and verifying the target software encryption information are described as above, which is not repeated.

[0057] In this embodiment, even if the private encryption information is recorded in the user private region, the private encryption information recorded in the user private region is not always unchanged and can also be updated or deleted.

[0058] In this embodiment, through an external interface for the target software, or through a software interaction interface for the target software, external input of an update message for updating the private encryption information in the user private region can be received; and according to the update message, private encryption information recorded in the user private region can be updated. For example, the recorded private encryption information in the user private region is updated with the private encryption information carried by the update message. This enables updating the private encryption information in the user private region.

[0059] In this embodiment, through an external interface for the target software, or through a software interaction interface for the target software, a deletion instruction can be received; and according to the deletion instruction, recorded private encryption information in the user private region can be deleted. This achieves the deletion of private encryption information from the user private region.

[0060] The above describes the method provided in the embodiments of the present disclosure, and the following describes an apparatus provided in the embodiments of the present disclosure.

[0061] Referring to FIG. 6, FIG. 6 is a structural diagram of an encryption apparatus according to embodiments of the present disclosure. As shown in FIG. 6, the apparatus may include:

[0062] a deploying unit, configured to record private encryption information in a user private region of an encryption medium currently deployed, where the encryption medium is for encryption of a target software, and the encryption medium further records target software encryption information configured to encrypt the target software; and

[0063] a processing unit, configured to, in response to detection of an encryption trigger for encrypting associated data associated with the target software, encrypt the associated data according to private encryption information corresponding to the associated data recorded in the user private region of the encryption medium;

[0064] where encryption of the associated data is independent of encryption of the target software, and the associated data includes at least one of: software configuration information of the target software, result information generated after the target software is run, a custom function software, software configuration information of the custom function software, and result information generated after the custom function software is run, where the custom function software is implemented by adding a program for implementing a custom function on the target software.

[0065] Optionally, when recording the private encryption information in the user private region of the encryption medium currently deployed, where the encryption medium is for encryption of the target software, the deploying unit is further configured to:

[0066] receive, through a newly set external interface corresponding to the target software, the private encryption information written externally to the user private region; or

[0067] receive, through a software interaction interface for the target software, external input of the private encryption information to be written into the user private region, and writing the private encryption information into the user private region.

[0068] Optionally, the associated data includes at least one of: software configuration information of the target software when the target software is running, result information generated after the target software is run, software configuration information of the custom function software, and result information generated after the custom function software is run, and after encrypting the associated data according to the private encryption information

corresponding to the associated data recorded in the user private region of the encryption medium, the processing unit is further configured to: in response to receiving a loading trigger to load encrypted associated data into the target software for operation, read the target software encryption information and private encryption information for the encrypted associated data from the encryption medium, separately verify the target software encryption information and the private encryption information, and in response to determining that the verification is successful, decrypt the encrypted associated data and load the associated data into the target software for operation, otherwise, display loading failure.

[0069] The associated data at least includes: the custom function software; and after encrypting the associated data according to the private encryption information corresponding to the associated data recorded in the user private region of the encryption medium, the processing unit is further configured to: in response to receiving a trigger of use of a custom function provided by the custom function software, read private encryption information for encrypted custom function software from the encryption medium, verify the private encryption information, and in response to determining that the verification is successful, decrypt the custom function software and allow the use of the custom function provided by the custom function software; in response to determining that the verification fails, prohibit the use of the custom function provided by the custom function software; and in response to receiving a trigger of use of an original function provided by the target software, read the target software encryption information from the encryption medium, verify the target software encryption information, and in response to determining that the verification is successful, allow the use of the original function provided by the target software; in response to determining that the verification fails, prohibit the use of the original function provided by the target software.

[0070] Optionally, after recording the private encryption information in the user private region, the deploying unit is further configured to: receive, through an external interface for the target software, or through a software interaction interface for the target software, external input of an update message for updating the private encryption information in the user private region; and update, according to the update message, recorded private encryption information in the user private region; or receive, through an external interface for the target software, or through a software interaction interface for the target software, a deletion instruction; and delete, according to the deletion instruction, recorded private encryption information in the user private region.

[0071] The embodiments of the present disclosure further provide a hardware structure of the apparatus shown in FIG. 6. Referring to FIG. 7, FIG. 7 is a structural diagram of an electronic

device according to embodiments of the present disclosure. As shown in FIG. 7, the electronic device may include: one or more processors and one or more machine readable storage media; where the one or more machine readable storage media store a machine executable instruction that can be executed by the one or more processors; and the one or more processors are configured to execute the machine executable instruction to implement the method according to the embodiments of the present disclosure.

[0072] According to the same concept as the above method, the embodiments of the present disclosure further provide a machine readable storage medium, on which a number of computer instructions are stored. When the computer instructions are executed by the processor, the method according to any one of the above embodiments of the present disclosure can be implemented.

[0073] For example, the machine-readable storage medium can be any electronic, magnetic, optical, or other physical storage device that can contain or store information such as executable instructions, data, and so on. For example, the machine-readable storage medium may be a Radom Access Memory (RAM), a volatile memory, a non-volatile memory, a flash memory, a storage drive (e.g. hard disk drive), a solid state hard disk, any type of storage disk (e.g., compact disk, Digital Video Disk (DVD)), or a similar storage medium, or a combination thereof.

[0074] The systems, apparatuses, modules, or units elucidated in the above embodiments can be implemented specifically by a computer entity, or by a product with certain functions. A typical implementation device is a computer, which can take the form of a personal computer, laptop, cellular phone, camera phone, smart phone, personal digital assistant, media player, navigation device, email sending and receiving device, game console, tablet computer, wearable device, or any combination of these devices.

[0075] For the convenience of description, the above devices are divided into various units according to their functions and described respectively. It is, of course, possible to implement the functions of each unit in the same or multiple software and/or hardware when implementing the present disclosure.

[0076] It should be understood by those skilled in the art that embodiments of the present disclosure may be provided as methods, systems, or computer program products. Accordingly, the present disclosure may take the form of an entirely hardware embodiment, an entirely software embodiment, or an embodiment combining software and hardware aspects. Furthermore, the present disclosure may employ the form of a computer program product implemented on one or more computer-usable storage media (including, but not limited to, disk

storage, CD-ROM, optical storage, etc.), where the one or more computer-usable storage media having computer-usable program code.

[0077] the present disclosure is described with reference to flowcharts and/or block diagrams of methods, devices (systems), and computer program products according to embodiments of the present disclosure. It is to be understood that each process and/or block in the flowchart and/or block diagram, and the combination of processes and/or blocks in the flowchart and/or block diagram, may be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general-purpose computer, a specialized computer, an embedded processor, or other programmable data processing device to produce a machine such that instructions executed by the processor of the computer or other programmable data processing device produce an apparatus for implementing a function specified in one or more processes of the flowchart and/or one or more blocks of the block diagram.

[0078] These computer program instructions may also be stored in a computer-readable memory capable of directing the computer or other programmable data processing device to operate in a particular manner such that the instructions stored in the computer-readable memory produce an article of manufacture including an instruction apparatus that implements the function specified in one or more processes of the flowchart and/or one or more blocks of the block diagram.

[0079] These computer program instructions may be provided to a processor of a general-purpose computer, a specialized computer, an embedded processor, or other programmable device to produce a machine such that instructions executed by the processor of the computer or other programmable device produce an apparatus for implementing a function specified in one or more processes of the flowchart and/or one or more blocks of the block diagram.

[0080] The above description is only embodiments of the present disclosure and is not intended to limit the present disclosure. For those skilled in the art, various modifications and changes may be made in the present disclosure. Any modification, equivalent replacement, improvement, etc. present the spirit and principle of the present disclosure shall be included in the scope of the claims of the present disclosure.

CLAIMS

1. An encryption method, comprising:

recording private encryption information in a user private region of an encryption medium currently deployed, wherein the encryption medium is for encryption of a target software, and the encryption medium further records target software encryption information configured to encrypt the target software; and

encrypting the associated data according to private encryption information corresponding to associated data recorded in the user private region of the encryption medium;

wherein encryption of the associated data is independent of encryption of the target software, and the associated data comprises at least one of: software configuration information of the target software, result information generated after the target software is run, a custom function software, software configuration information of the custom function software, and result information generated after the custom function software is run, wherein the custom function software is implemented by adding a program for implementing a custom function on the target software.

2. The method according to claim 1, wherein recording the private encryption information in the user private region of the encryption medium currently deployed, wherein the encryption medium is for encryption of the target software comprises:

receiving, through an external interface for the target software, the private encryption information written externally to the user private region; or

receiving, through a software interaction interface for the target software, external input of the private encryption information to be written into the user private region, and writing the private encryption information into the user private region.

3. The method according to any one of claims 1-2, further comprising:

in response to running the target software, verifying the target software encryption information, and running the target software in response to determining that the verification is successful;

in response to loading the associated data, verifying the private encryption information corresponding to the associated data, and loading the associated data in response to determining that the verification is successful.

4. The method according to any one of claims 1-3, wherein,

the associated data comprises at least one of: software configuration information of the target software when the target software is running, result information generated after the target software is run, software configuration information of the custom function software, and result information generated after the custom function software is run, and after encrypting the associated data according to the private encryption information corresponding to the associated data recorded in the user private region of the encryption medium, the method further comprises:

in response to receiving a loading trigger to load encrypted associated data into the target software for operation, reading the target software encryption information and private encryption information for the encrypted associated data from the encryption medium, separately verifying the target software encryption information and the private encryption information, and in response to determining that the two verifications are successful, decrypting the encrypted associated data and loading the associated data into the target software for operation.

5. The method according to any one of claims 1-4, wherein the associated data at least comprises: the custom function software; and after encrypting the associated data according to the private encryption information corresponding to the associated data recorded in the user private region of the encryption medium, the method further comprises:

in response to receiving a trigger of use of a custom function provided by the custom function software, reading private encryption information for encrypted custom function software from the encryption medium, verifying the private encryption information, and in response to determining that the verification is successful, decrypting the custom function software and allowing the use of the custom function provided by the custom function software; in response to determining that the verification fails, prohibiting the use of the custom function provided by the custom function software.

6. The method according to claim 5, further comprising:

in response to receiving a trigger of use of an original function provided by the target software, reading the target software encryption information from the encryption medium, verifying the target software encryption information, and in response to determining that the verification is successful, decrypting the target software and allowing the use of the original function provided by the target software; in response to determining that the verification fails, prohibiting the use of the original function provided by the target software.

7. The method according to any one of claims 1 to 6, wherein after recording the private encryption information in the user private region of the encryption medium currently deployed, wherein the encryption medium is for encryption of the target software, the method further comprising:

receiving, through an external interface for the target software, or through a software interaction interface for the target software, external input of an update message for updating the private encryption information in the user private region; and updating, according to the update message, recorded private encryption information in the user private region; or

receiving, through an external interface for the target software, or through a software interaction interface for the target software, a deletion instruction; and deleting, according to the deletion instruction, recorded private encryption information in the user private region.

8. The method according to any one of claims 1-7, wherein after encrypting the associated data according to the private encryption information corresponding to the associated data recorded in the user private region of the encryption medium, the method further comprises:

in response to receiving a loading trigger to load encrypted associated data into the target software for operation, reading the target software encryption information and private encryption information for the encrypted associated data from the encryption medium, separately verifying the target software encryption information and the private encryption information, and in response to determining that the two verifications are successful, decrypting the encrypted associated data and loading the associated data into the target software for operation.

9. The method according to any one of claims 1-8, wherein the associated data comprises at least one of: the custom function software, software configuration information of the custom function software, and result information generated after the custom function software is run, and after encrypting the associated data according to the private encryption information corresponding to the associated data recorded in the user private region of the encryption medium, the method further comprises:

in response to receiving a loading trigger to load encrypted associated data into the target software for operation, reading private encryption information for the encrypted associated data from the encryption medium, verifying the private encryption information, and in response to determining that the verification is successful, decrypting the encrypted associated data and

loading the associated data into the target software for operation.

10. The method according to any one of claims 1-9, wherein the user private region records pieces of private encryption information, and each of pieces of private encryption information is provided with a corresponding type of associated data;

in response to detecting an encrypting trigger for encrypting associated data associated with the target software, the method further comprises:

identifying a type of the associated data;

determining private encryption information corresponding to the associated data in the user private region according to the type of the associated data; and

encrypting the associated data according to the private encryption information corresponding to the associated data recorded in the user private region.

11. An encryption apparatus, comprising:

a deploying unit, configured to record private encryption information in a user private region of an encryption medium currently deployed, wherein the encryption medium is for encryption of a target software, and the encryption medium further records target software encryption information configured to encrypt the target software; and

a processing unit, configured to encrypt associated data according to private encryption information corresponding to the associated data recorded in the user private region of the encryption medium;

wherein encryption of the associated data is independent of encryption of the target software, and the associated data comprises at least one of: software configuration information of the target software, result information generated after the target software is run, a custom function software, software configuration information of the custom function software, and result information generated after the custom function software is run, wherein the custom function software is implemented by adding a program for implementing a custom function on the target software.

12. An electronic device, comprising one or more processors and one or more machine readable storage media; wherein

the one or more machine readable storage media store a machine executable instruction that can be executed by the one or more processors; and

the one or more processors are configured to execute the machine executable instruction

to implement the method according to any one of claims 1 to 10.

13. A non-volatile storage medium on which a computer instruction is stored, wherein when the computer instruction is called by one or more processors, the one or more processors execute the method according to any one of claims 1 to 10.