US 20120246460A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2012/0246460 A1**

(43) **Pub. Date: Sep. 27, 2012**

Liu

(54) **ENCRYPTION DEVICE AND METHOD FOR CONTROLLING DOWNLOAD AND ACCESS OPERATIONS PERFORMED TO A MOBILE TERMINAL**

(75) Inventor: **Ke Liu**, Shenzhen (CN)

(73) Assignee: **ZTE CORPORATION**, Shenzhen, Guangdong (CN)

(21) Appl. No.: **13/258,375**

(22) PCT Filed: **Apr. 28, 2010**

(86) PCT No.: **PCT/CN2010/072301**

§ 371 (c)(1),
(2), (4) Date: **May 3, 2012**

(30) **Foreign Application Priority Data**

Nov. 5, 2009 (CN) 200910237219.2

Publication Classification

(51) **Int. Cl.**
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **713/150**

(57) **ABSTRACT**

An encryption device and method for controlling download and access operations performed to a mobile terminal are disclosed. A switch circuit (**102**) is disposed on download channels (**107**, **108**) between the master chip (**101**) of the mobile terminal and the connector (**103**) of the mobile terminal, an access software (**105**) is opened and an encryption chip (**106**) is accessed by using a dongle (**112**), the on-off of the switch circuit (**102**) is controlled by setting states of the encryption chip (**106**), so as to control the on-off of download channels (**107**, **108**) to control the download and access operations performed to the mobile terminal by a computer (**104**). According to the device and method, hackers cannot crack the internal procedure of the memory of the mobile terminal using substitute code segments, thereby effectively improving the security and reliability of the download and access operations performed to the mobile terminal.

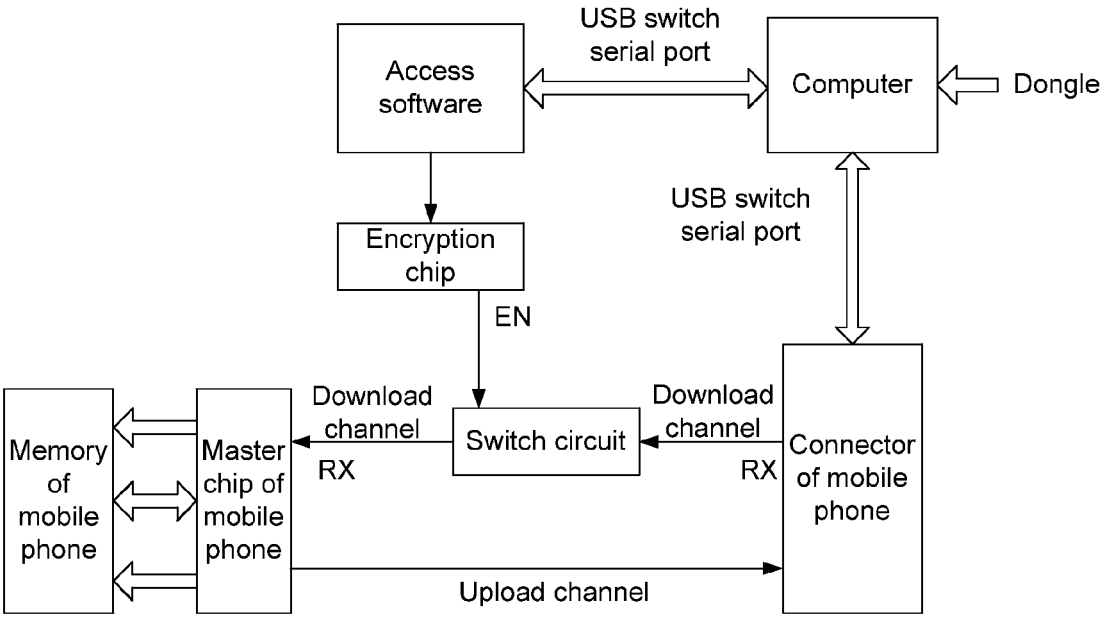


Fig. 1

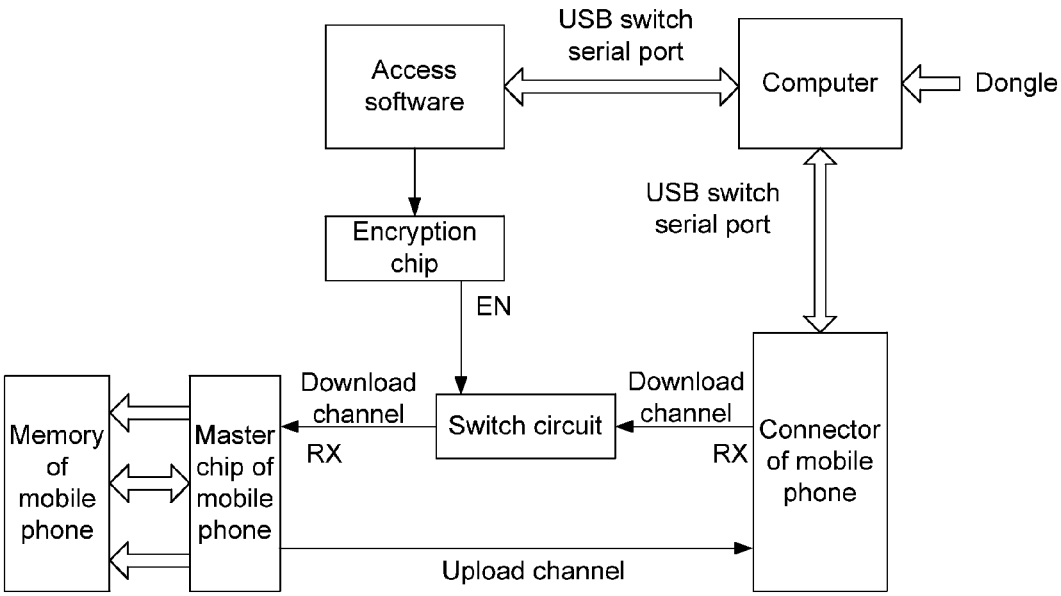
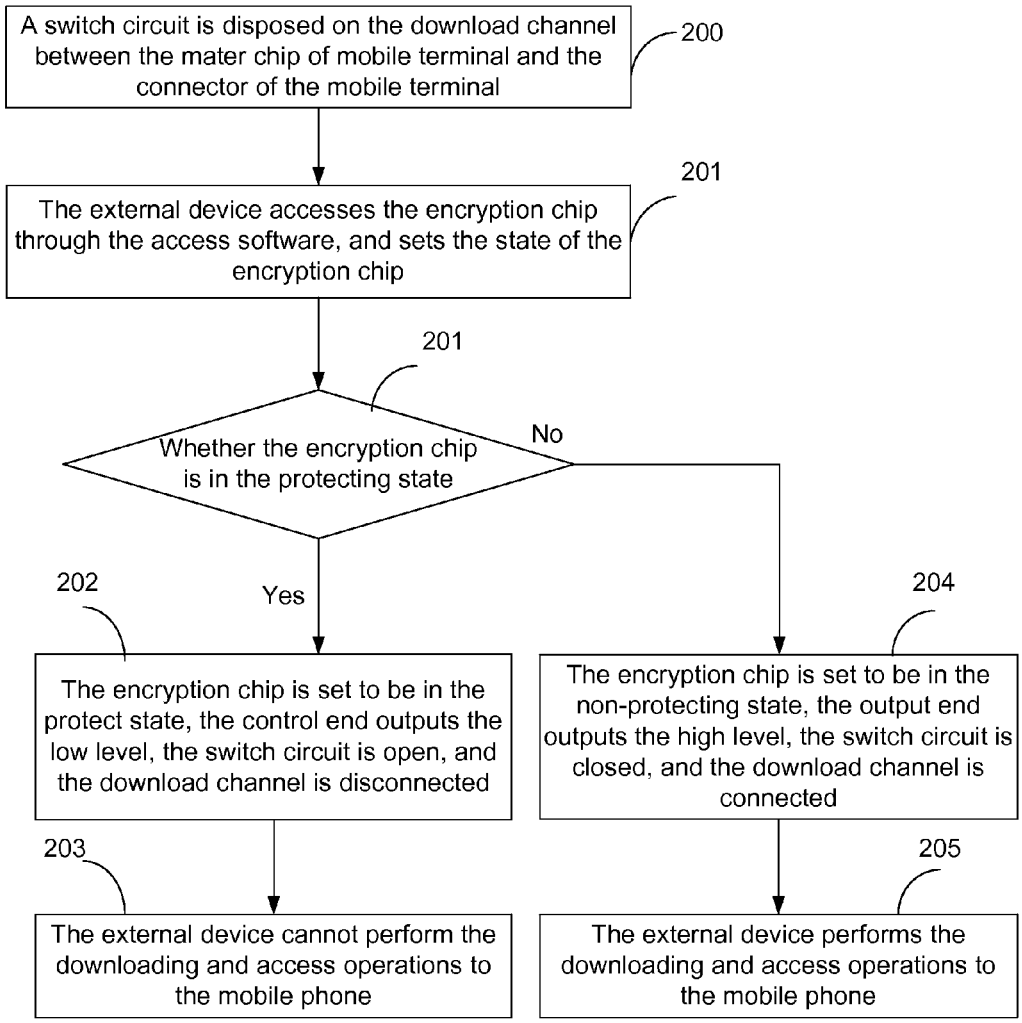

Access software
USB switch serial port
Computer
Dongle
Encryption chip
USB switch serial port
EN
Memory of mobile phone
Master chip of mobile phone
Download channel
RX
Switch circuit
Download channel
RX
Connector of mobile phone
Upload channel

Fig. 2


A switch circuit is disposed on the download channel between the mater chip of mobile terminal and the connector of the mobile terminal
200
The external device accesses the encryption chip through the access software, and sets the state of the encryption chip
201
201
Whether the encryption chip is in the protecting state
No
Yes
202
The encryption chip is set to be in the protect state, the control end outputs the low level, the switch circuit is open, and the download channel is disconnected
204
The encryption chip is set to be in the non-protecting state, the output end outputs the high level, the switch circuit is closed, and the download channel is connected
203
The external device cannot perform the downloading and access operations to the mobile phone
205
The external device performs the downloading and access operations to the mobile phone

ENCRYPTION DEVICE AND METHOD FOR CONTROLLING DOWNLOAD AND ACCESS OPERATIONS PERFORMED TO A MOBILE TERMINAL

TECHNICAL FIELD

[0001] The disclosure relates to encryption technique of mobile terminals, and in particular to an encryption device and method for controlling download and access operations performed to a mobile terminal.

BACKGROUND

[0002] With the fast development of mobile terminal, the amount of mobile phone users is increased day by day. In order to prevent hackers from carrying out download operation on the mobile phone through a computer and from accessing the internal procedure of the memory of the mobile terminal by accessing the master chip of the mobile phone so as to crack the lock network locking card function of the mobile is phone, the mobile phone usually needs to be protected through encryption added by a manufacturer.

[0003] In the prior art, Message-Digest Algorithm 5 (MD5) is usually adopted as cryptographic algorithm for carrying out encryption on the internal procedure of the memory of the mobile terminal. Since the cryptographic algorithm is an exhaustive encryption algorithm, when the mobile phone is turned on, the encrypted procedure is required to be decrypted before the mobile phone runs, which leads to long turn-on time of the mobile phone due to long decryption time. To reduce the turn-on time of the mobile phone, just a few important codes in the internal procedure of the memory of the mobile phone are encrypted under normal conditions. However, for the hackers familiar with the internal procedure of the memory of the mobile phone, the encrypted code segment is easily replaced by a substitute code segment to run the whole procedure, so that download and access operations performed to the mobile phone is performed by the computer through the connector of the mobile phone.

[0004] Another encryption manner combined with a platform is as follows: after the serial number of the chip of the mobile phone is bond with that of the memory of the mobile phone, a ciphertext is stored in the memory, and the serial numbers of the ciphertext are verified after every turn-on operation; if the serial numbers obtained after verifying are identical to that of the master chip of the mobile phone and that of the memory of the mobile phone, the procedure runs. However, the encryption manner is still adopted for the encryption of a few code segments, and similarly can be decrypted by the hackers; therefore, the security of the mobile phone is reduced.

[0005] The above encryption manners are both adopted for the encryption of a few code segments in the internal procedure of the memory of the mobile phone, and belong to software encryption manner; the encrypted procedure can be decrypted as long as the encrypted code segment is replaced by the substitute code segment by the hackers, and the download and access operations can be performed to the mobile phone through the connector of the mobile phone, so as to seriously influence the security of the mobile phone; therefore, it is especially important to look for a more high-effective encryption manner.

SUMMARY

[0006] Therefore, the main purpose of the disclosure is to provide an encryption device and method for controlling download and access operations performed to a mobile terminal, through which the encrypted code segments in the memory of the mobile terminal cannot be replaced, so that the security of the download and access operations performed to the mobile terminal is improved.

[0007] To achieve the purpose, following technical solutions of the disclosure are provided.

[0008] In one aspect, an encryption device for controlling download and access operations performed to a mobile terminal is provided, which includes a switch circuit and an encryption chip. The switch circuit is disposed on a download channel between a master chip of the mobile terminal and a connector of the mobile terminal and is configured to control an on-off of the download channel. The encryption chip is disposed on a mainboard of the mobile terminal and is configured to control an on-off of the switch circuit through states of the encryption chip.

[0009] Preferably, the switch circuit includes an N channel insulated gate field effect transistor, a drain electrode of the field effect transistor is connected with a read pin of the master chip of the mobile terminal through a pull-up resistor, a source electrode of the field effect transistor is connected with a read pin of the connector of the mobile terminal, and a gate electrode of the field effect transistor is connected with a control end of the encryption chip.

[0010] Preferably, the encryption chip has a protecting state and a non-protecting state. When the encryption chip is set to be in the protecting state, the control end of the encryption chip outputs a low level, the switch circuit is closed, and the download channel is connected; when the encryption chip is set to be in the non-protecting state, the control end of the encryption chip outputs a high level, the switch circuit is open, and the download channel is disconnected.

[0011] Preferably, a power supply source of the encryption chip is provided by an output power source of the master chip of the mobile terminal.

[0012] Preferably, the device further includes an access software and a dongle. The access software is connected with an external device and the encryption chip, through the access software, the external device accesses the encryption chip. The dongle is configured to protect access security of the access software.

[0013] In another aspect, an encryption method for controlling download and access operations performed to the mobile terminal is provided, which includes the following steps: disposing a switch circuit on a download channel between a master chip of is the mobile terminal and a connector of the mobile terminal, and connecting or disconnecting the download channel by controlling an on-off of the switch circuit according to states of an encryption chip.

[0014] Preferably, before setting the state of the encryption chip, the method further includes the following steps: the external device opens an access software through a dongle, accesses the encryption chip through the access software, and sets the state of the encryption chip.

[0015] Preferably, the switch circuit includes an N channel insulated gate field effect transistor, a drain electrode of the field-effect transistor is connected with a read pin of the master chip of the mobile terminal through a pull-up resistor, a source electrode of the field effect transistor is connected with the read pin of the connector of the mobile terminal, and a gate electrode of the field effect transistor is connected with a control end of the encryption chip.

[0016] Preferably, the step of controlling the on-off of the switch circuit according to states of the encryption chip includes that: when the encryption chip is set to be in a protecting state, a control end of the encryption chip outputs a low level, the switch circuit is open, and the download channel is disconnected; when the encryption chip is set to be in a non-protecting state, a control end of the encryption chip outputs a high level, the switch circuit is closed, and the download channel is connected.

[0017] Preferably, a power supply source of the encryption chip is provided by an output power source of the master chip of the mobile terminal.

[0018] According to the encryption device and method for controlling download and access operations of the mobile terminal, a switch circuit is disposed on the download channel between the master chip of the mobile terminal and the connector of the mobile terminal, the access software is opened and the encryption chip is accessed by using the dongle, the on-off of the switch circuit is controlled by setting states of the encryption chip, so as to control the on-off of the download channel to achieve the purpose for controlling the download and access operations performed to the mobile terminal by a computer.

[0019] According to the device and method of the disclosure, the mobile terminal is encrypted for protection, through a combination of hardware encryption and software encryption, so that it is impossible for hackers to replace and crack the encryption procedure of the memory of the mobile terminal using substitute code segments, so as to effectively improve the security and reliability of the download and access is operations performed to the mobile terminal.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] FIG. **1** shows a structural diagram of an encryption device for controlling download and access operations performed to the mobile terminal of the disclosure; and

[0021] FIG. **2** shows a flowchart of an encryption method for controlling download and access operations performed to the mobile terminal of the disclosure.

DETAILED DESCRIPTION

[0022] The main idea of the disclosure is that: a switch circuit is disposed on the download channel between the master chip of the mobile terminal and the connector of the mobile terminal, and the on-off of the switch circuit is controlled through the states of the encryption chip to control the on-off of the download channel so as to control the download and access operations performed to the mobile terminal by the external device, thereby improving the security and reliability of the mobile terminal.

[0023] The device and method of the disclosure are detailed below in conjunction with the specific embodiment. In the embodiment, the mobile terminal is a mobile phone.

[0024] According to the present disclosure, the encryption device for controlling the download and access operations performed to the mobile terminal, as shown in FIG. **1**, includes a switch circuit and an encryption chip.

[0025] The switch circuit is disposed on a download channel between the master chip of the mobile terminal and the connector of the mobile terminal and is configured to control the on-off of the download channel; that is, when the switch circuit is closed, the download channel is connected; when the switch circuit is open, the download channel is disconnected.

[0026] According to the PN junction characteristic of semiconductor, field effect transistor can be divided into P channel field effect transistor and N channel field effect transistor. In the embodiment, the switch circuit comprises an N channel insulated gate field effect transistor (MOS transistor, for short); the MOS transistor has three electrodes of source electrode S, drain electrode D and gate electrode G which are respectively S electrode, D electrode and G electrode for short. The D electrode of the MOS transistor is connected with the read pin RX of the master pin of the mobile phone through a pull-up resistor; the S electrode of the MOS is transistor is connected with the read pin RX of the connector of the mobile phone; and the G electrode of the MOS transistor is connected with the control end EN of the encryption chip. The on-off of the switch circuit is controlled through the output level of the control end EN of the encryption chip so as to control the on-off of the download channel.

[0027] When the control end EN outputs a high level, that is, when the G electrode has a high level, the MOS transistor is turned on, the switch circuit is closed, the download channel between the master chip of the mobile phone and the connector of the mobile phone is connected, and the external device such as the computer can perform download and access operations to the mobile phone. When the control end EN outputs a low level, that is, the G electrode has a low level, the MOS transistor is turned off, the switch circuit is open, the download channel between the master chip of the mobile phone and the connector of the mobile phone is disconnected, and the external device such as the computer cannot perform download or access operations to the mobile phone. The resistance value of the pull-up resistor is not specially limited, but the D electrode could produce relatively large sink current if the resistance value is too small so as to cause influence on the switch circuit; preferably, the resistance value of the pull-up resistor is 100 kilohms.

[0028] The encryption chip is disposed on the mainboard of the mobile phone for controlling the on-off of the switch circuit through the states of the encryption chip.

[0029] Here, the control end EN of the encryption chip is connected with the G electrode of the MOS transistor, and the output level of the control end EN of the encryption chip is controlled through the states of the encryption chip so as to control the on-off of the switch circuit. The state of the encryption chip can be set to be a protecting state and a non-protecting state; when the encryption chip is set to be in the protecting state, the control end EN of the encryption chip outputs a low level, the switch circuit is open; when the encryption chip is set to be in non-protecting state, the control end EN of the encryption chip outputs a high level, the switch circuit is closed. The power supply source of the encryption chip is provided by the output power source of the master chip of the mobile phone, so as to guarantee that the encryption chip is simultaneously powered on when the master chip of the mobile phone is powered on, no matter the information saved on the mobile phone is downloaded or accessed.

[0030] In the disclosure, a control procedure programmed in advance in the computer is is downloaded inside the encryption chip through a special download wire for the encryption chip so as to control the state of the encryption chip; moreover, the state of the encryption chip can be modified by modifying the key of the encryption chip. The control

procedure is used for controlling the state of the encryption chip; the control procedure also needs to be encrypted for protection; and the encryption manner can be an exhaustive encryption manner in the prior art without description here in detail. The control procedure after being encrypted for protection is programmed independently and is completely independent of the internal procedure of the memory of the mobile phone, and is not easy to be obtained and cracked by the hackers.

[0031] The device further includes a dongle and an access software.

[0032] The dongle is a special tool for opening the access software by the computer and is used the access software in order to protect the access security of the access software; and the access software can be opened just by inserting the dongle into the computer and then inputting correct passwords.

[0033] The access software is a special access tool for the encryption chip and is used with the encryption chip and the dongle for accessing the encryption chip. The control procedure programmed in advance in the computer is downloaded inside the encryption chip through the special download wire for the encryption chip after the access software is opened through the dongle by the computer, or the state of the encryption chip is set by modifying the key of the encryption chip.

[0034] Based on the device, the disclosure provides an encryption method for controlling the download and access operations to the mobile terminal. as shown in FIG. **2**, the method comprises the following steps.

[0035] Step **200**: A switch circuit is disposed on the download channel between the master chip of the mobile terminal and the connector of the mobile terminal.

[0036] In the step, the switch circuit consists of an N channel insulated gate field effect transistor (MOS transistor, for short); the MOS transistor has three electrodes of source electrode S, drain electrode D and gate electrode G which are respectively S electrode, D electrode and G electrode for short. The D electrode of the MOS transistor is connected with the read pin RX of the master pin of the mobile phone through a pull-up resistor; the S electrode of the MOS transistor is connected with the read pin RX of the connector of the mobile phone; and the G electrode of the MOS transistor is connected with the control end EN of the encryption chip. The is on-off of the switch circuit is controlled through the output level of the control end EN of the encryption chip so as to control the on-off of the download channel.

[0037] When the control end EN outputs a high level, that is, when the G electrode has a high level, the MOS transistor is turned on, the switch circuit is closed, the download channel between the master chip of the mobile phone and the connector of the mobile phone is connected, and the external device such as the computer can perform download and access operations to the mobile phone. When the control end EN outputs a low level, that is, the G electrode has a low level, the MOS transistor is turned off, the switch circuit is open, the download channel between the master chip of the mobile phone and the connector of the mobile phone is disconnected, and the external device such as the computer cannot perform download and access operations to the mobile phone. The resistance value of the pull-up resistor is not specially limited, but the D electrode could produce relatively large sink current if the resistance value is too small so as to cause influence on the switch circuit; preferably, the resistance value of the pull-up resistor is 100 kilohms.

[0038] Step **201**: An external device accesses the encryption chip through an access software, and sets the state of the encryption chip; determining whether the encryption chip is set to be in the protecting state, Step **202** is performed when the encryption chip is set to be in the protecting state; and Step **204** is performed when the encryption chip is set to be in the non-protecting state;

[0039] in the step, the external device, such as a computer, accesses the encryption chip through the access software so as to set the state of the encryption chip. The dongle is a special tool for opening the access software by the computer in order to protect the access security of the access software; and the access software can be opened just by inserting the dongle into the computer and then inputting correct passwords so as to access the encryption chip. If the dongle is not inserted in the computer, the access software cannot be opened, and the encryption chip also cannot be accessed. Under normal conditions, the dongle cannot be obtained and cracked easily by the hackers, so the access security and reliability of the access software can be guaranteed.

[0040] The control procedure programmed in advance in the computer is downloaded inside the encryption chip through the special download wire for the encryption chip after the access software is opened through the dongle by the compute. The control procedure is used for controlling the state of the encryption chip. The control is procedure also needs to be encrypted for protection; and the encryption manner can be an exhaustive encryption manner in the prior art without description here in detail. The control procedure after being encrypted for protection is programmed independently and is completely independent of the internal procedure of the memory of the mobile phone, and cannot be obtained and cracked easily by the hackers.

[0041] Moreover, the state of the encryption chip can be modified through the key of the encryption chip. The state of the encryption chip can be set to be the protecting state or the non-protecting state. When the encryption chip is in the protecting state, the control end EN of the encryption chip outputs a low level; when the encryption chip is in the non-protecting state, the control end EN of the encryption chip outputs a high level. After the configuration of the state of the encryption chip is finished, the download wire can be pulled out to quit the access software and the dongle; the encryption chip is disconnected with the computer so that a person without the dongle cannot modify the control procedure inside the encryption chip so as to achieve the protection function for the state of the encryption chip.

[0042] Here, a USB signal is converted into a RS232 serial signal through a USB switch serial port for realizing data transmission when the encryption chip is accessed through the special download wire by the computer. When the encryption chip is in the protecting state, the Step **202** is performed; when the encryption chip is in the non-protecting sate, the Step **204** is performed.

[0043] Steps **202-203**: the encryption chip is set to be in the protecting state, the control end outputs a low level, the switch circuit is open, the download channel is disconnected, the external device cannot perform the download and access operations to the mobile phone, and the current processing procedure is completed.

[0044] In the embodiment, the power supply source of the encryption chip is provided by the output power source of the master chip of the mobile phone, thus the encryption chip can be powered on simultaneously when the master chip of the

mobile phone is powered on no matter the information saved on the mobile phone is downloaded or accessed, so as to control the on-off of the download channel in order to achieve the protection function for the master chip.

[0045] In the step, when the master chip of the mobile phone is powered on, the encryption chip is powered on simultaneously. When the encryption chip is set to be in the protecting state, the control end EN of the encryption chip outputs a low level; is since the control end EN is connected with the G electrode of the MOS transistor, the G electrode of the MOS transistor is also at a low level; the MOS transistor is turned off, the switch circuit is open, and the download channel between the master chip of the mobile phone and the connector of the mobile phone is turned off. The external device, such as the computer, cannot carry out download operation to the mobile phone through the connector of the mobile phone, and cannot access the master chip of the mobile phone through the connector of the mobile phone so as to access the internal procedure of the memory of the mobile phone.

[0046] Under normal conditions, the encryption chip is in the protecting state when the mobile phone leaves the factory in order to prevent others from carrying out download operation to the mobile phone at random and from accessing the master chip of the mobile phone at random without permission so as to access the internal procedure of the memory of the mobile phone.

[0047] Steps **204-205**: the encryption chip is set to be in the non-protecting state, the control end outputs a high level, the switch circuit is closed, the download channel is connected, and the external device can perform the download and access operations to the mobile phone.

[0048] In the step, when the encryption chip is in the non-protecting state, the control end EN of the encryption chip outputs the high level, that is, the G electrode of the MOS transistor is at the high level, the MOS transistor is turned on, the switch circuit is closed, and the download channel between the master chip of the mobile phone and the connector of the mobile phone performs data transmission through RS232 serial signals.

[0049] In the embodiment, if the state of the encryption chip needs to be modified, from the protecting state to the non-protecting state, or from the non-protecting state to the protecting sate, the dongle is required to be inserted in the external device, such as the computer, again and then correct passwords are input, and the access software is opened. The encryption chip is accessed by the computer through the special download wire for the encryption chip, and the key of the encryption chip is modified in order to reset the sates of the encryption chip; the download wire can be pulled out after the setting is completed, and the access software and the dongle are quit in order to protect the state of the encryption chip from being modified by others.

[0050] Moreover, the switch circuit of the disclosure is disposed on the download channel of the master chip and the connector of the mobile phone so as to just is control the on-off of the download channel. Therefore, the mobile phone is protected only when the external device, such as the computer, performs download and access operations to the mobile phone. The mobile phone is not damaged when the mater chip of the mobile phone uploads data to the computer through the connector of the mobile phone, thus no switch circuit is disposed on the upload channel between the mater chip of the mobile phone and the connector of the mobile phone.

[0051] The above is only the preferred embodiment of the disclosure and not intended to limit the scope of protection of the disclosure. Any modifications, equivalent replacements, improvements without departing from the spirit and principle of the disclosure shall fall within the scope of protection of the disclosure.

1. An encryption device for controlling download and access operations performed to a mobile terminal, comprising: a switch circuit and an encryption chip, wherein,

the switch circuit is disposed on a download channel between a master chip of the mobile terminal and a connector of the mobile terminal and is configured to control an on-off of the download channel, and

the encryption chip is disposed on a mainboard of the mobile terminal and is configured to control an on-off of the switch circuit through states of the encryption chip.

2. The encryption device according to claim **1**, wherein the switch circuit comprises an N channel insulated gate field effect transistor, a drain electrode of the field effect transistor is connected with a read pin of the master chip of the mobile terminal through a pull-up resistor, a source electrode of the field effect is transistor is connected with a read pin of the connector of the mobile terminal, and a gate electrode of the field effect transistor is connected with a control end of the encryption chip.

3. The encryption device according to claim **1**, wherein the encryption chip has a protecting state and a non-protecting state;

when the encryption chip is set to be in the protecting state, the control end of the encryption chip outputs a low level, the switch circuit is open, and the download channel is disconnected; when the encryption chip is set to be in the non-protecting state, the control end of the encryption chip outputs a high level, the switch circuit is closed, and the download channel is connected.

4. The encryption device according to claim **1**, wherein a power supply source of the encryption chip is provided by an output power source of the master chip of the mobile terminal.

5. The encryption device according to claim **1**, further comprising an access software and a dongle; wherein,

the access software is connected with an external device and the encryption chip, through which the external device accesses the encryption chip, and

the dongle is configured to protect access security of the access software.

6. An encryption method for controlling download and access operations performed to the mobile terminal, comprising:

disposing a switch circuit on a download channel between a master chip of the mobile terminal and a connector of the mobile terminal; and

connecting or disconnecting the download channel by controlling an on-off of the switch circuit according to states of an encryption chip.

7. The encryption method according to claim **6**, further comprising steps, preceding the step of setting the states of the encryption chip, of: opening, by the external device, an access software through a dongle, accessing the encryption chip through the access software, and setting the states of the encryption chip.

8. The encryption method according to claim **6**, wherein the switch circuit comprises an N channel insulated gate field effect transistor, a drain electrode of the field effect transistor is connected with a read pin of the master chip of the mobile

terminal through a pull-up resistor, a source electrode of the field effect is transistor is connected with a read pin of the connector of the mobile terminal, and a gate electrode of the field effect transistor is connected with a control end of the encryption chip.

9. The encryption method according to claim **6**, wherein controlling the on-off of the switch circuit according to states of the encryption chip comprises: when the encryption chip is set to be in a protecting state, a control end of the encryption chip outputting a low level, the switch circuit being open, and the download channel being disconnected; when the encryption chip is set to be in a non-protecting state, the control end of the encryption chip outputting a high level, the switch circuit being closed, and the download channel being connected.

10. The encryption method according to claim **6**, wherein a power supply source of the encryption chip is provided by an output power source of the master chip of the mobile terminal.

11. The encryption device according to claim **3**, wherein a power supply source of the encryption chip is provided by an output power source of the master chip of the mobile terminal.

12. The encryption device according to claim **2**, further comprising an access software and a dongle; wherein,

the access software is connected with an external device and the encryption chip, through which the external device accesses the encryption chip, and

the dongle is configured to protect access security of the access software.

13. The encryption device according to claim **3**, further comprising an access software and a dongle; wherein,

the access software is connected with an external device and the encryption chip, through which the external device accesses the encryption chip, and

the dongle is configured to protect access security of the access software.

14. The encryption method according to claim **7**, wherein controlling the on-off of the switch circuit according to states of the encryption chip comprises: when the encryption chip is set to be in a protecting state, a control end of the encryption chip outputting a low level, the switch circuit being open, and the download channel being disconnected; when the encryption chip is set to be in a non-protecting state, the control end of the encryption chip outputting a high level, the switch circuit being closed, and the download channel being connected.

15. The encryption method according to claim **8**, wherein controlling the on-off of the switch circuit according to states of the encryption chip comprises: when the encryption chip is set to be in a protecting state, a control end of the encryption chip outputting a low level, the switch circuit being open, and the download channel being disconnected; when the encryption chip is set to be in a non-protecting state, the control end of the encryption chip outputting a high level, the switch circuit being closed, and the download channel being connected.

* * * * *