(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 549 678 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
26.06.2019 Bulletin 2019/26

(21) Application number: **10858325.3**

(22) Date of filing: **08.12.2010**

(51) Int Cl.:
G06F 21/72 $^{(2013.01)}$ ***G06F 21/44*** $^{(2013.01)}$
H04L 9/32 $^{(2006.01)}$ ***H04W 12/00*** $^{(2009.01)}$
H04W 12/12 $^{(2009.01)}$ ***G06F 21/51*** $^{(2013.01)}$
H04W 88/02 $^{(2009.01)}$

(86) International application number:
PCT/CN2010/079579

(87) International publication number:
WO 2012/048493 (19.04.2012 Gazette 2012/16)

(54) METHOD AND APPARATUS FOR PROTECTING SOFTWARE OF MOBILE TERMINAL

VERFAHREN UND VORRICHTUNG ZUM SCHUTZ VON SOFTWARE EINES MOBILEN ENDGERÄTS

PROCÉDÉ ET APPAREIL DE PROTECTION DE LOGICIEL DE TERMINAL MOBILE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **14.10.2010 CN 201010509953**

(43) Date of publication of application:
23.01.2013 Bulletin 2013/04

(73) Proprietor: **ZTE Corporation**
Shenzhen, Guangdong 518057 (CN)

(72) Inventor: **LIN, Hua**
Shenzhen
Guangdong 518057 (CN)

(74) Representative: **V.O.**
P.O. Box 87930
2508 DH Den Haag (NL)

(56) References cited:

CN-A- 1 553 729	**CN-A- 1 913 680**
CN-A- 101 098 540	**CN-A- 101 777 106**
US-A1- 2006 143 446	**US-A1- 2007 101 156**

- **ZOU ZHIGE ET AL.: 'The GPIO of TMS320VC5402 and Its Application' ELECTRONICS ENGINEER vol. 29, no. 4, 30 August 2003, pages 39 - 41, XP008167161**

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] The disclosure relates to a security technology for a mobile terminal, particularly to a method and an apparatus for protecting software of a mobile terminal.

BACKGROUND

[0002] At present, mobile phones have become indispensable tools in the daily life of most people with the rapid development of the mobile terminal market. Most mobile phone manufacturers and operators have applied software protection to protect their own interests and enable mobile phone users to use certain services or networks in a period of time.

[0003] Currently, mobile phone manufacturers mainly employ software for encryption. program encryption is carried out using an encryption algorithm similar to MD5 (the fifth version of Message-Digest Algorithm), which consumes more resources because encryption and decryption are involved each time. Another common method is to combine encryption with a platform, that is, encrypt the chip ID of a main chip bound with the chip ID of a Flash to obtain a ciphertext and save the ciphertext in the Flash, and verify the ciphertext each time a mobile phone is turned on. However, dangers, such as easily hacked, and leakage of secret keys, may exist in this method.

[0004] Generally, a hacker cracks a mobile phone by illegally downloading new mobile phone software. Algorithms have bugs no matter how powerful they are. Therefore, if a hacker utilizes program bugs to get around or damage original software and directly download new mobile phone software and updates programs in a Flash, then it is meaningless to establish algorithms, no matter how powerful they are, in mobile software; such case happens occasionally.

[0005] It is noted that patent publication US 2007/101156 A1 discloses methods and systems for associating an embedded security chip with a computer.

[0006] It is further noted that patent publication US 2006/143446 A1 discloses a system and a method to lock TPM always 'on' using a monitor.

SUMMARY

[0007] In view of this, the main purpose of the disclosure is to provide a method and an apparatus for protecting software of a mobile terminal to prevent the software of the mobile terminal from being cracked, thus the security of the mobile terminal is greatly improved and the interests of operators and manufacturers are protected.

[0008] To achieve the purpose above, the technical solution of the disclosure is realized as follows.

[0009] A method for protecting software of a mobile terminal is provided in the disclosure, including: mounting an encryption chip in the mobile terminal, and further including:

> when the mobile terminal is turned on, detecting whether or not the encryption chip is invalid;
> when the encryption chip is not invalid, authenticating, by the encryption chip, the software of the mobile terminal through interaction with a main chip; and
> when the authentication is not passed, controlling, by the encryption chip, a functional module of the mobile terminal through a hardware protection circuit.

[0010] In the solution above, the detecting whether or not the encryption chip is invalid may include: determining, by the main chip, whether or not the encryption chip is invalid according to whether or not information sent by the encryption chip is received in a set period of time; if the information is received, determining that the encryption chip is not invalid; otherwise, determining that the encryption chip is invalid;
or reading, by the main chip, a status of a General Purpose Input Output (GPIO) interface of the encryption chip, and determining, by the main chip, whether or not the encryption chip is invalid; when the status of the GPIO interface changes according to a preset period, determining that the encryption chip is not invalid; when the status of the GPIO interface does not change according to a preset period, determining that the encryption chip is invalid;
or determining, by the main chip, whether or not the encryption chip is invalid according to whether or not a secret key configured to authenticate the software of the mobile terminal is received in a set period of time is received; if the secret key is received, then determining that the encryption chip is not invalid; otherwise, determining that the encryption chip is invalid.

[0011] In the solution above, the authenticating, by the encryption chip, the software of the mobile terminal through interaction with a main chip includes:

> sending, by the encryption chip, a secret key configured to authenticate the software of the mobile terminal to the main chip; after the main chip receives said secret key, searching, by the main chip, a secret key matched with said secret key in the main chip itself; returning, by the main chip, the matched secret key or an authentication passed message to the encryption chip when a secret key matched with said secret key is found; and returning, by the main chip, an authentication failure message or not returning the matched secret key to the encryption chip when the secret key matched with said secret key is not found or not searched;
> when the encryption chip receives the authentication failure message or does not receive the matched secret key in a set period of time, then indicating that the authentication is not passed; when the encryp-

tion chip receives the authentication passed message or the matched secret key, then indicating that the authentication is passed; wherein the secret key configured to authenticate the software of the mobile terminal and the secret key matched with said secret key are secret keys matched with each other and are respectively preset by a computer in the encryption chip and in the main chip;
or wherein the authenticating, by the encryption chip, the software of the mobile terminal through interaction with the main chip comprises:

reading, by the encryption chip, a status of a GPIO interface of the main chip;
when the status of the GPIO interface changes according to a preset period, then indicating that the authentication is passed; when the status of the GPIO interface does not change according to the preset period, then indicating that the authentication is not passed.

[0012] In the solution above, the controlling, by the encryption chip, a functional module of the mobile terminal through a hardware protection circuit may include: controlling, by the encryption chip, an analog switch in the hardware protection circuit through a control line to turn off a Flash, and/or lock a keyboard, and/or turn off a Liquid Crystal Display (LCD), and/or turn off an audio function, and/or turn off a Subscriber Identity Module (SIM) card access.

[0013] In the solution above, the method may further include: when the encryption chip is detected to be invalid, protecting and controlling the functional module of the mobile terminal through software.

[0014] In the solution above, the protecting and controlling the functional module of the mobile terminal through software may include: turning off, by the main chip of the mobile terminal, a network service port, and/or an LCD port, and/or a audio functional port, and/or a keyboard response port through the software of the mobile terminal.

[0015] In the solution above, the method may further include: setting a timer in the encryption chip; starting timing again each time the timer times out; and detecting again whether or not the encryption chip is invalid and authenticating the software of the mobile terminal again.

[0016] The disclosure provides an apparatus for protecting software of a mobile terminal according to claim 7.

[0017] In the solution above, the hardware protection circuit may include a control line and an analog switch; wherein the analog switch is set on a signal line of the functional module of the mobile terminal; and the control line is configured to transmit a control signal which is used by the encryption chip to control the analog switch; and
the functional module of the mobile terminal may include: a Flash, and/or an LCD module, and/or a keyboard module, and/or an audio module, and/or an SIM card module.

[0018] In the solution above, the main chip of the mobile terminal may be further configured to, when the encryption chip is detected to be invalid, protect and control the functional module of the mobile terminal through software;
wherein the protecting and controlling the functional module of the mobile terminal through software includes: turning off a network service port, and/or an LCD port, and/or an audio functional port, and/or a keyboard response port through the software of the mobile terminal.

[0019] A method and an apparatus for protecting software of a mobile terminal are provided in the disclosure. An encryption chip is mounted in the mobile terminal. When the mobile terminal is turned on, whether or not the encryption chip is invalid is detected; when it is not invalid, the encryption chip authenticates the software of the mobile terminal through interaction with a main chip; when the authentication is not passed, the encryption chip controls a functional module of the mobile terminal through a hardware protection circuit. In this way, the software of the mobile terminal can be prevented from being cracked and the functions of the mobile terminal can be protected from illegal usage, thus the security of the mobile terminal is greatly improved and the interests of operators and manufacturers are protected.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020]

Fig. 1 is a flowchart of realization of a method for protecting software of a mobile terminal in the disclosure;

Fig. 2 is a schematic diagram illustrating connections in a hardware protection circuit of the disclosure; and

Fig. 3 is a structural diagram of realization of an apparatus for protecting software of mobile terminal in the disclosure.

DETAILED DESCRIPTION

[0021] The basic idea of the disclosure is that: an encryption chip is mounted in a mobile terminal; when the mobile terminal is turned on, whether or not the encryption chip is invalid is detected; when it is not invalid, the encryption chip authenticates software of the mobile terminal through interaction with a main chip; when the authentication is not passed, the encryption chip controls a functional module of the mobile terminal through a hardware protection circuit.

[0022] The encryption chip supports online writing and multiple programming, and is provided with at least one communication interface and one control interface. Generally, a 51 core-based chip, or a Peripheral Interface Controller (PIC) chip and etc. can be employed as an encryption chip. A special tool is required to write the writeable area of the encryption chip. The communication interface is configured to communicate with the main chip of the mobile terminal. The control interface is configured to connect the hardware protection circuit.

[0023] The disclosure is described in details according to the accompanying drawings and specific embodiments as below.

[0024] The method for protecting software of a mobile terminal in the disclosure is as shown in Fig. 1. The method includes the following steps.

[0025] Step 101: an encryption chip is mounted in the mobile terminal;

specifically, in the mobile terminal, a chip where the software of the mobile terminal is located is the main chip. The encryption chip is connected with the main chip of the mobile terminal through an existing interface on the mobile terminal. Communication modes, which apply GPIO, Inter-Integrated Circuit (I2C), parallel interfaces and serial interfaces, and etc., are utilized for interaction between the main chip and the encryption chip. Information in the encryption chip cannot be modified by the main chip, and an interface of the encryption chip is connected to a computer. The interface can be a serial interface or other interfaces, through which the computer writes a corresponding secret key into the encryption chip. In order to facilitate production, the interface can apply a test point method, and a hardware protection circuit needs to be set for the encryption chip. As shown in Fig. 2, the functional modules of the mobile terminal, such as a Flash, an LCD module, a keyboard module, an audio module and an SIM card module, and etc., are connected with the main chip of the mobile terminal through signal lines respectively. An analog switch is set on a key signal line of each functional module and the analog switch is turned on or turned off by the encryption chip using a control line, thus realizing on-off control of the functional modules of the mobile terminal and protecting functions of the mobile terminal. The signal line includes a power line, a data line, an address line, a control line, a row-column scan line, and an audio line, etc. The control line is configured to transmit a control signal which is used by the encryption chip to control the analog switch.

[0026] Specifically, for the Flash, an analog switch is added on the power line of the Flash. When the authentication performed by the encryption chip on the software of the mobile terminal is not passed, the power supply of the Flash can be cut off by the analog switch to make the mobile terminal invalid. Generally, the analog switch can apply a triode. The LCD module is controlled as the same as the Flash, and it is only needed to control the power source of the LCD module through an analog switch. Of course, a data line or an address line of the LCD module can be controlled by a module switch. When the authentication performed by the encryption chip on the software of the mobile terminal is not passed, the data line or the address line of the LCD module can be cut off through the analog switch or the module switch, to make the LCD module invalid. The method for controlling the keyboard module is the same. When there is a full-keyboard chip, when the authentication performed by the encryption chip on the software of the mobile terminal is not passed, a full-keyboard chip can be stopped working only by cutting off the power source of the full-keyboard chip through an analog switch, or a control can be realized only by cutting off part of row-column scan lines of the full-keyboard chip through an analog switch. A method of controlling the audio module can be that an analog switch is added to an audio line, a SPEAKER, a RECEIVER and an MIC signal line connected with the main chip of the mobile terminal, and on-off control can be realized by the analog switch. For the SIM card module, it is only needed to add an analog switch on a clock line or a data line of the SIM card module, thus the encryption chip can disconnect the data line through an analog switch to make the SIM card function invalid. The method of adding an analog switch as described above can be applied to other functional modules of the mobile terminal, and the encryption chip can control each functional module of the mobile terminal by controlling analog switches, so as to protect the hardware.

[0027] Further, matched secret keys can be set in the encryption chip and in the main chip by the computer respectively to perform interactive authentication on the software of the mobile terminal.

[0028] In the step that matched secret keys are set in the encryption chip and in the main chip respectively; a Flash ID, and/or an International Mobile Equipment Identity (IMEI), and/or an encryption chip serial number, and etc. can be read by the computer, and the Flash ID, and/or the IMEI, and/or the encryption chip serial number, and etc. can be combined to produce "one computer one code" secret keys. The produced secret keys are saved in the encryption chip and in the main chip of the mobile terminal respectively, as matched secret keys for communication handshaking. Generally, the Flash ID, and/or the IMEI, and/or the encryption chip serial number, and etc. are combined by addition processing, or exclusive-or processing;

or the computer sets a Triple DES (TDES) algorithm to be applied between the encryption chip and the mobile terminal, and predetermines a 16-byte authentication key and saves the key in the encryption chip and the mobile terminal respectively. When the encryption chip sends the secret key configured to authenticate the software of the mobile terminal, the following steps are performed:

> encryption operation: perform 3DES operation on KEY and a random number (RAND) to obtain an eight-byte result R, i.e. R=KEY$^{\oplus}$ RAND, form command data (CHV value): CHV value=R; sending a verification command and the RAND: sending a verification command (a0 20 00 01 08 R) and the RAND to the mobile terminal;
>
> when the mobile terminal obtains the verification command and the RAND, the following steps are

performed:

decryption operation: perform 3DES decryption operation ON the KEY and the R to obtain an eight-byte result RN, i.e. RN=key®R, the obtained RN is a decryption result; matching operation: RAND=RN, indicating it is correct, and returning SW1SW2="authentication passed", otherwise, returning SW1SW2="authentication not passed", or not returning a value in a predetermined period of time;

further, before the computer reads the Flash ID, and/or the IMEI, and/or the encryption chip serial number, and etc. or sets application of the TDES algorithm, the computer needs to perform softdog authentication, and after the authentication is passed, the computer reads the Flash ID, and/or the IMEI, and/or the encryption chip serial number, and etc. or set the TDES algorithm to be applied.

[0029] In this step, since the software of the mobile terminal may be cracked, it should be ensured that a circuit module of the encryption chip can work normally and the hardware protection circuit can be started when the software of the mobile terminal is cracked. Therefore, this step further includes selecting a power source for the encryption chip. The power source can supply power when the mobile terminal is turned on, and at the same time ensure that power can be supplied to the encryption chip effectively when the software of the mobile terminal is cracked. In addition, the power source does not depend on the software of the mobile terminal to supply power for the mobile terminal. Generally, the power source may be a battery or a supply power which supplies power for the Flash.

[0030] Step 102: when the mobile terminal is turned on, whether or not the encryption chip is invalid is detected. When the encryption chip is invalid, Step 103 is executed; when the encryption chip is not invalid, Step 104 is executed.

[0031] In this step, in the operation of detecting whether or not the encryption chip is invalid generally is that the main chip determines whether or not the encryption chip is invalid according to whether or not information sent by the encryption chip is received in a set period of time. If the information is received, it indicates that the encryption chip is not invalid. If the information is not received, it indicates that the encryption chip is invalid. The information sent by the encryption chip can be predetermined information which determines that the encryption chip is not invalid; here, the set period of time can be a predetermined fixed period of time, which can be 10 seconds or 30 seconds, etc.

[0032] Or a changing period of a status of a GPIO interface of the encryption chip is preset, the encryption chip, according to the period, sets its own GPIO interface high or low. The main chip reads the status of the GPIO interface of the encryption chip and determines whether or not the encryption chip is invalid. When the status of the GPIO interface changes according to the preset period, it indicates that the encryption chip is not invalid; When the status of the GPIO interface does not change according to the preset period, it indicates that the encryption chip is invalid.

[0033] Before executing this step, a step in Step 104 that the encryption chip sends a secret key configured to authenticate the software of the mobile terminal to the main chip, may be executed. The main chip, according to whether or not the secret key configured to authenticate the software of the mobile terminal is received in a set period of time, determines whether or not the encryption chip is invalid; if the secret key is received, the encryption chip is determined to be not invalid; if the secret key is not received, the encryption chip is determined to be invalid.

[0034] Step 103: a functional module of the mobile terminal is protected and controlled by software, then the flow ends;

specifically, the main chip of the mobile terminal turns off a network service port, and/or an LCD port, and/or an audio functional port, and/or a keyboard response port, and etc. through the software of the mobile terminal, to make the functional module such as a network service module, and/or an LCD module, and/or an audio functional module, and/or a keyboard module, and etc. of the mobile terminal invalid.

[0035] Step 104: the encryption chip authenticates the software of the mobile terminal through interaction with the main chip; when the authentication is not passed, the functional module of the mobile terminal is protected and controlled by hardware;

specifically, when the main chip of the mobile terminal, according to the received information which determines that the encryption chip is not invalid, determines that the encryption chip is not invalid, it sends a detection passed message to the encryption chip. After receiving the detection passed message, the encryption chip sends a secret key configured to authenticate the software of the mobile terminal to the main chip. After receiving the secret key, the main chip searches in itself a secret key matched with said secret key. When the secret key matched with said secret key is found, it indicates that the version of the software of the mobile terminal in the main chip is not changed or the software of the mobile terminal in the main chip is not cracked, and the matched secret key or an authentication passed message is returned to the encryption chip; when the secret key matched with said secret key is not found or not searched, it indicates that the version of the software of the mobile terminal in the main chip has been changed or the software of the mobile terminal in the main chip has been cracked, and an authentication failure message is returned or the matched secret key is not returned to the encryption chip. When the encryption chip, in a set period of time, receives the authentication failure message or does not receive the matched secret key, it indicates that the authentication is not passed and the encryption chip controls an analog switch in a hardware protection circuit through a control line to turn off a Flash, and/or lock a keyboard, and/or turn off an LCD, and/or turn off an audio function, and/or turn off an SIM card access, and etc. The detection of a matched secret key includes a decryption operation and a matching operation performed during the application of the TDES algorithm. When the authentication passed message or the matched secret key is received, the authentication is passed and the mobile terminal works normally;

the detection passed message is a predetermined message indicating that the encryption chip is valid;

generally, the set period of time is 5 seconds, or 10 seconds, etc.

[0036] When the main chip of the mobile terminal, according to the secret key sent by the encryption chip and configured to authenticate the software of the mobile terminal, determines that the encryption chip is not invalid, searches in the main chip itself a secret key matched with said secret key. When the matched secret key is found, it indicates that the version of the software of the mobile terminal in the main chip is not changed or the software of the mobile terminal in the main chip is not cracked, and the matched secret key or an authentication passed message is returned to the encryption chip; when the secret key matched with said secret key is not found or not searched, it indicates that the version of the software of the mobile terminal in the main chip has been changed or the software of the mobile terminal in the main chip has been cracked, and an authentication failure message is returned or a matched secret key is not returned to the encryption chip. When the encryption chip, in a set period of time, receives the authentication failure message or does not receive the matched secret key, it indicates that the authentication is not passed and the encryption chip controls the analog switch in the hardware protection circuit through a control line to turn off the Flash, and/or lock the keyboard, and/or turn off the LCD, and/or turn off the audio function, and/or turn off the SIM card access, etc. When the authentication passed message or the matched secret key is received, it indicates that the authentication is passed and the mobile terminal works normally;

if a changing period of a status of a GPIO interface of the main chip of the mobile terminal is preset, the main chip according to the period, sets its own GPIO interface high or low. After the main chip determines that the encryption chip is not invalid, a detection passed message is sent to the encryption chip. After receiving the detection passed message, the encryption chip reads the status of the GPIO interface of the main chip. When the status of the GPIO interface changes according to the preset period, it indicates that the authentication is passed, and the mobile terminal works normally. When the status of the GPIO interface does not change according to the preset period, it indicates that the authentication is not passed, and the encryption chip controls the analog switch in the hardware protection circuit through a control line to turn off the Flash, and/or lock the keyboard, and/or turn off the LCD, and/or turn off the audio function, and/or turn off the SIM card access, etc.

[0037] The method above further includes: a timer is set in the encryption chip; the timer starts timing again each time the timer times out; and whether or not the encryption chip is invalid is detected over again and the software of the mobile terminal is authenticated again.

[0038] In order to achieve the method above, the disclosure further provides an apparatus for protecting software of a mobile terminal. As shown in Fig. 3, the apparatus includes: a main chip 31 of the mobile terminal, an encryption chip 32 and a hardware protection circuit 33; wherein

the main chip 31 of the mobile terminal is configured to, when the mobile terminal is turned on, detect whether or not the encryption chip 32 is invalid, interact with the encryption chip 32 when the encryption chip is not invalid, and authenticate the software of the mobile terminal;

the encryption chip 32 is configured to interact with the main chip 31 of the mobile terminal, authenticate the software of the mobile terminal, and notify the hardware protection circuit 33 to control a functional module of the mobile terminal when the authentication is not passed;

the hardware protection circuit 33 is configured to, according to the notification from the encryption chip 32, control the functional module of the mobile terminal;

specifically, the hardware protection circuit 33 includes a control line and an analog switch. The analog switch is set on a key signal line of the functional module of the mobile terminal. The control line is configured to transmit a control signal which is used by the encryption chip to control the analog switch. Here, the encryption chip can control the on/off of the analog switch through the control line to realize on/off control of the functional module of the mobile terminal and protect the functions of the mobile terminal. The functional module of the mobile terminal includes: a Flash, and/or a LCD module, and/or a keyboard module, and/or an audio module, and/or an SIM card module, and etc.

[0039] The main chip 31 of the mobile terminal detects whether or not the encryption chip 32 is invalid. Generally, the main chip 31 of the mobile terminal determines whether or not the encryption chip 32 is invalid according to whether or not information sent by the encryption chip 32 is received in a set period of time. If the information is received, the encryption chip is determined not to be invalid; if the information is not received, the encryption chip is determined to be invalid. The information sent by the encryption chip 32 can be predetermined information which determines that the encryption chip 32 is not invalid;

accordingly, the encryption chip 32 is further configured to send the predetermined information which determines that the encryption chip is not invalid to the main chip 31 of the mobile terminal.

[0040] The information which determines that the encryption chip 32 is not invalid can be a secret key sent by the encryption chip 32 and configured to authenticate the software of the mobile terminal;

or a changing period of a status of a GPIO interface of the encryption chip 32 is preset; the encryption chip 32, according to the period, sets its own GPIO interface high or low. The main chip 31 of the mobile terminal, according to a read status of the GPIO interface of the encryption chip 32, determines whether or not the encryption chip is invalid. When the status of the GPIO interface changes according to the preset period, the encryption chip is determined not invalid; when the status of the GPIO interface does not change according to the preset period, the encryption chip is determined invalid.

[0041] The main chip 31 of the mobile terminal is further configured to protect and control a functional module of the mobile terminal through software when the encryption chip 32 is detected to be invalid;

the main chip 31 of the mobile terminal protects and controls the functional module of the mobile terminal through software, specifically including: the main chip 31 of the mobile terminal turns off a network service port, and/or an LCD port, and/or an audio functional port, and/or a keyboard response port, and etc. through the software of the mobile terminal, to make the functional module such as a network service module, and/or an LCD module, and/or an audio functional module, and/or a keyboard module ,and etc. of the mobile terminal invalid.

[0042] The encryption chip 32 interacts with the main chip 31 of the mobile terminal to authenticate the software of the mobile terminal, specifically including: the encryption chip 32 sends a secret key configured to authenticate the software of the mobile terminal to the main chip 31 of the mobile terminal; when the encryption chip 32 receives an authentication failure message or does not receive a matched secret key sent by the main chip 31 of the mobile terminal in a set period of time, it indicates that the authentication is not passed; when an authentication passed message or the matched secret key is received, it indicates that the authentication is passed;

accordingly, the main chip 31 of the mobile terminal is further configure to, after receiving the secret key configured to authenticate the software of the mobile terminal from the encryption chip 32, search in the main chip itself a secret key matched with said secret key. When the secret key matched with said secret key is found, it indicates that the version of the software of the mobile terminal in the main chip 31 of the mobile terminal is not changed or the software of the mobile terminal in the main chip 31 is not cracked, and the matched secret key or an authentication passed message is returned to the encryption chip 32. When the secret key matched with said secret key is not found or not searched, it indicates that the version of the software of the mobile terminal in the main chip 31 of the mobile terminal has been changed or the software of the mobile terminal in the main chip 31 has been cracked, and an authentication failure message is returned or a matched secret key is not returned to the encryption chip 32;

or the encryption chip 32 reads a status of a GPIO interface of the main chip 31 of the mobile terminal; when the status of the GPIO interface changes according to a preset period, it indicates that the authentication is passed; the status of the GPIO interface does not change according to the preset period, it indicates that the authentication is not passed;

accordingly, the main chip 31 of the mobile terminal is further configured to preset a changing period of the status of the GPIO interface, and sets its own GPIO high or low according to the period.

[0043] Further, the apparatus further includes a computer 34 configured to set secret keys matched with each other in the encryption chip 32 and in the main chip 31 of the mobile terminal, respectively;

specifically, the computer 34 reads a Flash ID, and/or an IMEI, and/or an encryption chip serial number, and etc., and combines the Flash ID, and/or the IMEI, and/or the encryption chip serial number to produce "one computer one code" secret keys. The produced secret keys are saved in the encryption chip 32 and in the main chip 31 of the mobile terminal respectively, as matched secret keys for communication handshaking. Generally, the Flash ID, and/or the IMEI, and/or the encryption chip serial number, and etc. are combined by addition processing, or exclusive-or processing;

or the computer 34 sets a TDES algorithm to be applied between the encryption chip 32 and the main chip 31 mobile terminal, predetermines a 16-byte authentication key saved in the encryption chip 32 and in the main chip 31 of the mobile terminal respectively;

accordingly, when the encryption chip 32 sends a secret key configured to authenticate the software of the mobile terminal, the following steps are included:

> encryption operation: performing 3DES operation on KEY and RAND to obtain an eight-byte result R, i.e. R=KEY⊕ RAND; forming command data (CHV value): CHV value=R; sending a verification command and the RAND: sending the verification command (a0 20 00 01 08 R) and the RAND to the mobile terminal;
>
> accordingly, when the main chip 31 of the mobile terminal obtains the verification command and the RAND, the following steps are performed:
>
>> decryption operation: performing 3DES decryption operation on the KEY and the R to obtain an eight-byte result RN, i.e. RN=key®R, the obtained RN is a decryption result; performing matching operation: RAND=RN, indicating it is correct, and returning SW1SW2="authentication passed"; otherwise, returning SW1SW2="authentication not passed", or not

returning a value in a predetermined period of time;

further, the computer 34 is further configured to, before reading the Flash ID, and/or the IMEI, and/or the encryption chip serial number, etc. or setting application of the TDES algorithm, perform softdog authentication; after the authentication is passed, read the Flash ID, and/or the IMEI, and/or the encryption chip serial number, and etc. or set the TDES algorithm to be applied.

[0044] Further, the encryption chip 32 is further configured to set a timer. The timer starts timing again each time the timer times out, and triggers the main chip 31 of the mobile terminal and the encryption chip 32 to detect again whether the encryption chip is invalid and authenticate the software of the mobile terminal again.

[0045] The method of the disclosure can protect the functions of the mobile terminal from illegal usage when the encryption chip is cracked or dismantled. In addition, when the authentication performed by the encryption chip on the software of the mobile terminal is not passed, the hardware protection circuit is started to control a functional module of the mobile terminal. In this way, the software of the mobile terminal can be better prevented from being cracked, thus the security of the mobile terminal is greatly improved and the interests of operators and manufacturers are protected.

[0046] The above is only the preferred embodiment of the disclosure and not intended to limit the scope of protection of the invention, which is defined by the claims.

Claims

1. A method for protecting software of a mobile terminal, comprising:

   when the mobile terminal is turned on, detecting whether or not an encryption chip is invalid (102), wherein the encryption chip is mounted in the mobile terminal (101) and information in the encryption chip cannot be modified by a main chip of the mobile terminal;
   when the encryption chip is not invalid, authenticating, by the encryption chip, the software of the mobile terminal through interaction with the main chip; and when the authentication is not passed, controlling, by the encryption chip, a functional module of the mobile terminal through a hardware protection circuit (104);
   wherein

   (a) the authenticating, by the encryption chip, the software of the mobile terminal through interaction with the main chip comprises: sending, by the encryption chip, to the main chip a secret key configured to authenticate the software of the mobile terminal; after the main chip receives said secret key, searching, by the main chip, a secret key matched with said secret key in the main chip itself; returning, by the main chip, the matched secret key or an authentication passed message to the encryption chip when the secret key matched with said secret key is found; and returning, by the main chip, an authentication failure message or not returning the matched secret key to the encryption chip when the secret key matched with said secret key is not found or not searched;
   when the encryption chip receives the authentication failure message or does not receive the matched secret key in a set period of time, then indicating that the authentication is not passed; when the encryption chip receives the authentication passed message or the matched secret key, indicating that the authentication is passed; wherein said secret key configured to authenticate the software of the mobile terminal and the secret key matched with said secret key are secret keys matched with each other and are respectively preset by a computer in the encryption chip and in the main chip;
   or
   (b) the authenticating, by the encryption chip, the software of the mobile terminal through interaction with the main chip comprises:
   reading, by the encryption chip, a status of a General Purpose Input Output, GPIO, interface of the main chip; when the status of the GPIO interface changes according to a preset period, indicating that the authentication is passed; when the status of the GPIO interface does not change according to the preset period, indicating that the authentication is not passed.

2. The method according to claim 1, wherein the detecting whether or not the encryption chip is invalid comprises: determining, by the main chip, whether or not the encryption chip is invalid according to whether or not information sent by the encryption chip is received in a set period of time; if the information is received, determining that the encryption chip is not invalid; otherwise, determining that the encryption chip is invalid;
   or reading, by the main chip, a status of a General Purpose Input Output, GPIO, interface of the encryption chip, and determining, by the main chip, whether or not the encryption chip is invalid; when the status of the GPIO interface changes according to a preset

period, determining that the encryption chip is not invalid; when the status of the GPIO interface does not change according to a preset period, determining that the encryption chip is invalid;
or determining, by the main chip, whether or not the encryption chip is invalid according to whether or not a secret key configured to authenticate the software of the mobile terminal is received in a set period of time; if the secret key is received, then determining that the encryption chip is not invalid; otherwise, determining that the encryption chip is invalid.

3. The method according to claim 1, wherein the controlling, by the encryption chip, a functional module of the mobile terminal through a hardware protection circuit comprises: controlling, by the encryption chip, an analog switch in the hardware protection circuit through a control line to turn off a Flash, and/or lock a keyboard, and/or turn off a Liquid Crystal Display, LCD, and/or turn off an audio function, and/or turn off a Subscriber Identity Module, SIM, card access.

4. The method according to claim 1, further comprising: when the encryption chip is detected to be invalid, protecting and controlling the functional module of the mobile terminal through software.

5. The method according to claim 4, wherein the protecting and controlling the functional module of the mobile terminal through software comprises: turning off, by the main chip of the mobile terminal, a network service port, and/or an LCD port, and/or an audio functional port, and/or a keyboard response port through the software of the mobile terminal.

6. The method according to any one of claims 1 to 5, further comprising: setting a timer in the encryption chip; starting timing again each time the timer times out; and detecting again whether or not the encryption chip is invalid and authenticating the software of the mobile terminal again.

7. An apparatus for protecting software of a mobile terminal, comprising a main chip of the mobile terminal (31), an encryption chip (32) and a hardware protection circuit (33); wherein
the main chip of the mobile terminal (31) is configured to, when the mobile terminal is turned on, detect whether or not the encryption chip (32) is invalid, interact with the encryption chip (32) when the encryption chip (32) is not invalid, and authenticate the software of the mobile terminal;
the encryption chip (32) is configured to interact with the main chip of the mobile terminal (31), authenticate the software of the mobile terminal, and notify the hardware protection circuit (33) to control a functional module of the mobile terminal when the authentication is not passed wherein the encryption chip (32) is mounted in the mobile terminal and information in the encryption chip (32) cannot be modified by the main chip of the mobile terminal (31); and
the hardware protection circuit (33) is configured to, according to the notification from the encryption chip (32), control the functional module of the mobile terminal;
wherein

(a) the encryption chip (32) is configured to send to the main chip of the mobile terminal (31) a secret key configured to authenticate the software of the mobile terminal; wherein the encryption chip (32) is further configured to: when, in a set period of time, it receives an authentication failure message or does not receive a matched secret key sent by he main chip of the mobile terminal (31), indicate that the authentication is not passed; and when it receives an authentication passed message or the matched secret key, indicate that the authentication is passed;
accordingly, the main chip of the mobile terminal (31) is further configured to, after receiving said secret key configured to authenticate the software of the mobile terminal from the encryption chip (32), search a secret key matched with said secret key in the main chip itself; return the matched secret key or an authentication passed message to the encryption chip (32) when the secret key matched with said secret key is found; and return an authentication failure message or not return the matched secret key to the encryption chip (32) when the secret key matched with said secret key is not found or not searched;
accordingly, the apparatus further comprises a computer (34) configured to set secret keys matched with each other in the encryption chip (32) and in the main chip of the mobile terminal (31), respectively;
or
(b) the encryption chip (32) is configured to read a status of a General Purpose Input Output, GPIO, interface of the main chip of the mobile terminal (31); wherein the encryption chip (32) is further configured to: when the status of the GPIO interface changes according to a preset period, indicate that the authentication is passed; and when the status of the GPIO interface does not change according to the preset period, indicate that the authentication is not passed;
accordingly, the main chip of the mobile terminal (31) is further configured to preset a changing period of the status of the GPIO interface, and to set its own GPIO high or low according to the period.

8. The apparatus according to claim 7, wherein the

main chip of the mobile terminal (31) is configured to, according to whether or not information sent by the encryption chip (32) is received in a set period of time, determine whether or not the encryption chip (32) is invalid; if the information is received, determine the encryption chip (32) is not invalid; if the information is not received, determine the encryption chip (32) is invalid; accordingly, the encryption chip (32) is further configured to send predetermined information which determines that the encryption chip (32) is not invalid to the main chip of the mobile terminal (31);
or the main chip of the mobile terminal (31) is configured to, according to a read status of a General Purpose Input Output, GPIO, interface of the encryption chip (32), determine whether or not the encryption chip (32) is invalid; when the status of the GPIO interface changes according to a preset period, determine the encryption chip (32) is not invalid; when the status of the GPIO interface does not change according to the preset period, determine the encryption chip (32) is invalid.

9. The apparatus according to claim 7, wherein the hardware protection circuit (33) comprises a control line and an analog switch; wherein the analog switch is set on a signal line of the functional module of the mobile terminal; and the control line is configured to transmit a control signal which is used by the encryption chip (32) to control the analog switch; and
the functional module of the mobile terminal comprises: a Flash, and/or a Liquid Crystal Display, LCD, module, and/or a keyboard module, and/or an audio module, and/or a Subscriber Identity Module, SIM, card module.

10. The apparatus according to claim 7, wherein the main chip of the mobile terminal (31) is further configured to, when the encryption chip (32) is detected to be invalid, protect and control the functional module of the mobile terminal through software;
wherein the protecting and controlling the functional module of the mobile terminal through software comprises: turning off a network service port, and/or an LCD port, and/or an audio functional port, and/or a keyboard response port through the software of the mobile terminal.

11. The apparatus according to any one of claims 7 to 10, wherein the encryption chip (32) is further configured to set a timer; wherein the timer is configured to start timing again each time the timer times out, and to trigger the main chip of the mobile terminal (31) and the encryption chip (32) to detect again whether the encryption chip (32) is invalid and authenticate the software of the mobile terminal again.

Patentansprüche

1. Verfahren zum Schützen von Software eines mobilen Endgeräts, Folgendes umfassend:

wenn das mobile Endgerät eingeschaltet wird, Erkennen, ob ein Verschlüsselungs-Chip ungültig ist oder nicht, (102) wobei der Verschlüsselungs-Chip in das mobile Endgerät montiert ist (101) und Informationen auf dem Verschlüsselungs-Chip durch einen Haupt-Chip des mobilen Endgeräts nicht modifiziert werden können;
wenn der Verschlüsselungs-Chip nicht ungültig ist, Authentifizieren der Software des mobilen Endgeräts durch den Verschlüsselungs-Chip mittels Interaktion mit dem Haupt-Chip, und wenn das Authentifizieren nicht erfolgreich war, Steuern eines Funktionsmoduls des mobilen Endgeräts durch den Verschlüsselungs-Chip mittels einer Hardware-Schutzschaltung (104), wobei

(a) das Authentifizieren der Software des mobilen Endgeräts durch den Verschlüsselungs-Chip mittels Interaktion mit dem Haupt-Chip Folgendes umfasst: Senden eines geheimen Schlüssels, der dafür konfiguriert ist, die Software des mobilen Endgeräts zu authentifizieren, durch den Verschlüsselungs-Chip an den Haupt-Chip; nachdem der Haupt-Chip den geheimen Schlüssel empfangen hat, Suchen eines geheimen Schlüssels, der mit dem geheimen Schlüssel in dem Haupt-Chip selbst übereinstimmt, durch den Haupt-Chip; Zurücksenden des übereinstimmenden geheimen Schlüssels oder einer Authentifizierung-erfolgreich-Nachricht an den Verschlüsselungs-Chip durch den Haupt-Chip, wenn der geheime Schlüssel gefunden wird, der mit dem geheimen Schlüssel übereinstimmt; und Zurücksenden einer Authentifizierung-fehlgeschlagen-Nachricht oder kein Zurücksenden des übereinstimmenden geheimen Schlüssels an den Verschlüsselungs-Chip durch den Haupt-Chip, wenn der geheime Schlüssel, der mit dem geheimen Schlüssel übereinstimmt, nicht gefunden wird oder nicht gesucht wird;

wenn der Verschlüsselungs-Chip die Authentifizierung-fehlgeschlagen-Nachricht empfängt oder den übereinstimmenden Sicherheitsschlüssel nicht in einer eingestellten Zeitspanne empfängt, Anzeigen, dass das Authentifizieren nicht erfolgreich war; wenn der Verschlüsselungs-Chip die Authentifizierung-erfolgreich-Nachricht oder den übereinstimmenden geheimen Schlüssel empfängt, Anzeigen, dass die Authentifizierung erfolgreich war; wobei der geheime Schlüssel, der dafür konfiguriert ist, die Software des mobilen Endgeräts zu authentifizieren, und der geheime Schlüssel, der mit dem geheimen Schlüssel übereinstimmt, geheime Schlüssel sind, die miteinander übereinstimmen und jeweils im Vorhinein durch einen Computer in dem Verschlüsselungs-Chip und dem Haupt-Chip eingestellt werden; oder

(b) das Authentifizieren der Software des mobilen Endgeräts durch den Verschlüsselungs-Chip mittels Interaktion mit dem Haupt-Chip Folgendes umfasst: Lesen eines Status einer GIPO-(General-Purpose-Input-Output-)Schnittstelle des Haupt-Chips durch den Verschlüsselungs-Chip; wenn sich der Status der GIPO-Schnittstelle gemäß einer voreingestellten Zeitspanne ändert, Anzeigen, dass die Authentifizierung erfolgreich war,; wenn sich der Status der GIPO-Schnittstelle gemäß der voreingestellten Zeitspanne nicht ändert, Anzeigen, dass die Authentifizierung nicht erfolgreich war.

2. Verfahren nach Anspruch 1, wobei das Erkennen, ob der Verschlüsselungs-Chip ungültig ist oder nicht, Folgendes umfasst: Bestimmen durch den Haupt-Chip, ob der Verschlüsselungs-Chip ungültig ist oder nicht, je nachdem, ob Informationen, die von dem Verschlüsselungs-Chip gesendet werden, in einer eingestellten Zeitspanne empfangen werden oder nicht; wenn die Informationen empfangen werden, Bestimmen, dass der Verschlüsselungs-Chip nicht ungültig ist; sonst Bestimmen, dass der Verschlüsselungs-Chip ungültig ist;

oder Lesen eines Status einer GIPO-(General-Purpose-Input-Output-)Schnittstelle des Verschlüsselungs-Chips durch den Haupt-Chip und Bestimmen durch den Haupt-Chip, ob der Verschlüsselungs-Chip ungültig ist oder nicht; wenn sich der Status der GIPO-Schnittstelle gemäß einer voreingestellten Zeitspanne ändert, Bestimmen, dass der Verschlüsselungs-Chip nicht ungültig ist; wenn sich der Status der GIPO-Schnittstelle nicht gemäß einer eingestellten Zeitspanne ändert, Bestimmen, dass der Verschlüsselungs-Chip ungültig ist;

oder Bestimmen durch den Haupt-Chip, ob der Verschlüsselungs-Chip ungültig oder nicht ist, je nachdem, ob ein geheimer Schlüssel, der dafür konfiguriert ist, die Software des mobilen Endgeräts zu authentifizieren, in einer eingestellten Zeitspanne empfangen wird; wenn der geheime Schlüssel empfangen wird, Bestimmen, dass der Verschlüsselungs-Chip nicht ungültig ist; sonst Bestimmen, dass der Verschlüsselungs-Chip ungültig ist.

3. Verfahren nach Anspruch 1, wobei das Steuern eines Funktionsmoduls des mobilen Endgeräts durch den Verschlüsselungs-Chip mittels einer Hardware-Schutzschaltung Folgendes umfasst: Steuern eines analogen Schalters in der Hardware-Schutzschaltung durch den Verschlüsselungs-Chip mittels einer Steuerleitung zum Abschalten eines Flash und/oder Sperren einer Tastatur und/oder Abschalten einer Flüssigkristallanzeige (LCD) und/oder Abschalten einer Audiofunktion und/oder Abschalten eines SIM-(Subscriber-Identity-Module-)Kartenzugriffs.

4. Verfahren nach Anspruch 1, ferner Folgendes umfassend: wenn erkannt wird, dass der Verschlüsselungs-Chip ungültig ist, Schützen und Steuern des Funktionsmoduls des mobilen Endgeräts mittels Software.

5. Verfahren nach Anspruch 4, wobei das Schützen und Steuern des Funktionsmoduls des mobilen Endgeräts mittels Software Folgendes umfasst: Abschalten eines Netzwerkdienst-Anschlusses und/oder eines LCD-Anschlusses und/oder eines Audiofunktionsanschlusses und/oder eines Tastaturreaktionsanschlusses durch den Haupt-Chip des mobilen Endgeräts mittels der Software des mobilen Endgeräts.

6. Verfahren nach einem der Ansprüche 1 bis 5, ferner Folgendes umfassend: Einstellen eines Zeitgebers in dem Verschlüsselungs-Chip; erneutes Starten einer Zeitsteuerung jedes Mal, wenn die Zeit des Zeitgebers abläuft; und erneutes Erkennen, ob der Verschlüsselungs-Chip ungültig ist oder nicht und erneutes Authentifizieren der Software des mobilen Endgeräts.

7. Vorrichtung zum Schützen von Software eines mobilen Endgeräts, einen Haupt-Chip des mobilen Endgeräts (31), einen Verschlüsselungs-Chip (32) und eine Hardware-Schutzschaltung (33) umfassend, wobei

der Haupt-Chip des mobilen Endgeräts (31) dafür konfiguriert ist, wenn das mobile Endgerät eingeschaltet wird, zu erkennen, ob der Verschlüsselungs-Chip (32) ungültig ist oder nicht, mit dem Verschlüsselungs-Chip (32) zu interagieren, wenn der Verschlüsselungs-Chip (32) nicht ungültig ist, und die Software des mobilen Endgeräts zu authentifizieren;

der Verschlüsselungs-Chip (32) dafür konfiguriert ist, mit dem Haupt-Chip des mobilen Endgeräts (31) zu interagieren, die Software des mobilen Endgeräts zu authentifizieren und die Hardware-Schutzschaltung (33) zu benachrichtigen, ein Funktionsmodul des mobilen Endgeräts zu steuern, wenn die Authentifizierung nicht erfolgreich war, wobei der Verschlüsselungs-Chip (32) in das mobile Endgerät montiert ist und Informationen in dem Verschlüsselungs-Chip (32) durch den Haupt-Chip des mobilen

Endgeräts (31) nicht modifiziert werden können; und die Hardware-Schutzschaltung (33) dafür konfiguriert ist, das Steuermodul des mobilen Endgeräts gemäß der Benachrichtigung von dem Verschlüsselungs-Chip (32) zu steuern;
wobei

(a) der Verschlüsselungs-Chip (32) dafür konfiguriert ist, einen geheimen Schlüssel, der dafür konfiguriert ist, die Software des mobilen Endgeräts zu authentifizieren, an den Haupt-Chip des mobilen Endgeräts (31) zu senden; wobei der Verschlüsselungs-Chip (32) ferner für Folgendes konfiguriert ist: wenn er in einer eingestellten Zeitspanne eine Authentifizierung-fehlgeschlagen-Nachricht empfängt oder keinen übereinstimmenden geheimen Schlüssel empfängt, der von dem Haupt-Chip des mobilen Endgeräts (31) gesendet wird, Anzeigen, dass das Authentifizieren nicht erfolgreich war; und wenn er eine Authentifizierung-erfolgreich-Nachricht oder den übereinstimmenden geheimen Schlüssel empfängt, Anzeigen, dass das Authentifizieren erfolgreich war;
der Haupt-Chip des mobilen Endgeräts (31) dementsprechend ferner dafür konfiguriert ist, nach dem Empfangen des geheimen Schlüssels, der dafür konfiguriert ist, die Software des mobilen Endgeräts zu authentifizieren, von dem Verschlüsselungs-Chip (32), einen geheimen Schlüssel zu suchen, der mit dem geheimen Schlüssel in dem Haupt-Chip selbst übereinstimmt; den übereinstimmenden geheimen Schlüssel oder eine Authentifizierung-erfolgreich-Nachricht an den Verschlüsselungs-Chip (32) zurückzusenden, wenn der mit dem geheimen Schlüssel übereinstimmende geheime Schlüssel gefunden wird; und eine Authentifizierung-fehlgeschlagen-Nachricht zurückzusenden oder den übereinstimmenden geheimen Schlüssel nicht an den Verschlüsselungs-Chip (32) zurückzusenden, wenn der mit dem geheimen Schlüssel übereinstimmende geheime Schlüssel nicht gefunden oder nicht gesucht wird;
die Vorrichtung dementsprechend ferner einen Computer (34) umfasst, der dafür konfiguriert ist, in dem Verschlüsselungs-Chip (32) und dem Haupt-Chip des mobilen Endgeräts (31) jeweils geheime Schlüssel einzustellen, die miteinander übereinstimmen;
oder
(b) der Verschlüsselungs-Chip (32) dafür konfiguriert ist, einen Status einer GIPO-(General-Purpose-Input-Output-)Schnittstelle des Haupt-Chips des mobilen Endgeräts (31) zu lesen, wobei der Verschlüsselungs-Chip (32) ferner für Folgendes konfiguriert ist:
wenn sich der Status der GIPO-Schnittstelle gemäß einer voreingestellten Zeitspanne ändert, Anzeigen, dass die Authentifizierung erfolgreich war; und wenn sich der Status der GIPO-Schnittstelle gemäß der voreingestellten Zeitspanne nicht ändert, Anzeigen, dass die Authentifizierung nicht erfolgreich war;
der Haupt-Chip des mobilen Endgeräts (31) dementsprechend ferner dafür konfiguriert ist, im Vorhinein eine Zeitspanne für die Änderung des Status der GIPO-Schnittstelle einzustellen und seine eigene GIPO gemäß der Zeitspanne hoch oder niedrig einzustellen.

8. Vorrichtung nach Anspruch 7, wobei der Haupt-Chip des mobilen Endgeräts (31) dafür konfiguriert ist, je nachdem, ob Informationen, die von dem Verschlüsselungs-Chip (32) gesendet werden, in einer eingestellten Zeitspanne empfangen werden oder nicht, zu bestimmen, ob der Verschlüsselungs-Chip (32) ungültig ist oder nicht; wenn die Informationen empfangen werden, Bestimmen, dass der Verschlüsselungs-Chip (32) nicht ungültig ist; wenn die Informationen nicht empfangen werden, Bestimmen, dass der Verschlüsselungs-Chip ungültig ist; wobei der Verschlüsselungs-Chip (32) dementsprechend ferner dafür konfiguriert ist, die festgelegten Informationen, welche bestimmen, dass der Verschlüsselungs-Chip (32) nicht ungültig ist, an den Haupt-Chip des mobilen Endgeräts (31) zu senden;
oder der Haupt-Chip des mobilen Endgeräts (31) dafür konfiguriert ist, gemäß einem Lesestatus einer GIPO-(General-Purpose-Input-Output-)Schnittstelle des Verschlüsselungs-Chips (32) zu bestimmen, ob der Verschlüsselungs-Chip ungültig ist oder nicht; wenn sich der Status der GIPO-Schnittstelle gemäß einer voreingestellten Zeitspanne ändert, zu bestimmen, dass der Verschlüsselungs-Chip (32) nicht ungültig ist; wenn sich der Status der GIPO-Schnittstelle gemäß der voreingestellten Zeitspanne nicht ändert, zu bestimmen, dass der Verschlüsselungs-Chip (32) ungültig ist.

9. Vorrichtung nach Anspruch 7, wobei die Hardware-Schutzschaltung (33) eine Steuerleitung und einen analogen Schalter umfasst; wobei der analoge Schalter auf eine Signalleitung des Funktionsmoduls des mobilen Endgeräts gesetzt ist; und die Steuerleitung dafür konfiguriert ist, ein Steuersignal zu übertragen, das durch den Verschlüsselungs-Chip (32) verwendet wird, um den analogen Schalter zu steuern; und
das Funktionsmodul des mobilen Endgeräts Folgendes umfasst: einen Flash und/oder ein Flüssigkristallanzeige-(LCD-)Modul und/oder ein Tastaturmodul und/oder ein Audiomodul und/oder ein SIM-(Subscriber-Identity-Module-)Kartenmodul.

10. Vorrichtung nach Anspruch 7, wobei der Haupt-Chip des mobilen Endgeräts (31) ferner dafür konfiguriert ist, wenn erkannt wird, dass der Verschlüsselungs-Chip (32) ungültig ist, das Funktionsmodul des mobilen Endgeräts mittels Software zu schützen und zu steuern;
wobei das Schützen und Steuern des Funktionsmoduls des mobilen Endgeräts mittels Software Folgendes umfasst: Abschalten eines Netzwerkdienst-Anschlusses und/oder eines LCD-Anschlusses und/oder eines Audiofunktionsanschlusses und/oder eines Tastaturreaktionsanschlusses mittels der Software des mobilen Endgeräts.

11. Vorrichtung nach einem der Ansprüche 7 bis 10, wobei der Verschlüsselungs-Chip (32) ferner dafür konfiguriert ist, einen Zeitgeber einzustellen; wobei der Zeitgeber dafür konfiguriert ist, eine Zeitsteuerung jedes Mal dann erneut zu starten, wenn die Zeit des Zeitgebers abläuft, und den Haupt-Chip des mobilen Endgeräts (31) und den Verschlüsselungs-Chip (32) anzusteuern, um erneut zu erkennen, ob der Verschlüsselungs-Chip (32) ungültig ist, und die Software des mobilen Endgeräts zu authentifizieren.

Revendications

1. Méthode pour protéger un logiciel d'un terminal mobile, comprenant :

lorsque le terminal mobile est allumé, le fait de détecter si une puce de cryptage est invalide ou non (102), dans laquelle la puce de cryptage est montée dans le terminal mobile (101) et des informations dans la puce de cryptage ne peuvent pas être modifiées par une puce principale du terminal mobile ;
lorsque la puce de cryptage n'est pas invalide, l'authentification, par la puce de cryptage, du logiciel du terminal mobile par le biais d'une interaction avec la puce principale ; et lorsque l'authentification n'est pas réussie, la commande, par la puce de cryptage, d'un module fonctionnel du terminal mobile par le biais d'un circuit de protection matérielle (104) ;
dans laquelle

(a) l'authentification, par la puce de cryptage, du logiciel du terminal mobile par le biais d'une interaction avec la puce principale comprend : l'envoi, par la puce de cryptage, à la puce principale d'une clé secrète configurée pour authentifier le logiciel du terminal mobile ; après que la puce principale reçoit ladite clé secrète, la recherche, par la puce principale, d'une clé secrète appariée avec ladite clé secrète dans la puce principale elle-même ; le renvoi, par la puce principale, de la clé secrète appariée ou d'un message d'authentification réussie à la puce de cryptage lorsque la clé secrète appariée avec ladite clé secrète est trouvée ; et le renvoi, par la puce principale, d'un message d'échec d'authentification ou le nonrenvoi de la clé secrète appariée à la puce de cryptage lorsque la clé secrète appariée avec ladite clé secrète n'est pas trouvée ou pas recherchée ;
lorsque la puce de cryptage reçoit le message d'échec d'authentification ou ne reçoit pas la clé secrète appariée dans une période de temps définie, le fait d'indiquer alors que l'authentification n'est pas réussie ;
lorsque la puce de cryptage reçoit le message d'authentification réussie ou la clé secrète appariée, le fait d'indiquer que l'authentification est réussie ; dans laquelle ladite clé secrète configurée pour authentifier le logiciel du terminal mobile et la clé secrète appariée avec ladite clé secrète sont des clés secrètes appariées l'une avec l'autre et sont prédéfinies respectivement par un ordinateur dans la puce de cryptage et dans la puce principale ;
ou
(b) l'authentification, par la puce de cryptage, du logiciel du terminal mobile par le biais d'une interaction avec la puce principale comprend : la lecture, par la puce de cryptage, d'un statut d'une interface d'entrée-sortie à usage général, GPIO, de la puce principale ; lorsque le statut de l'interface GPIO change en fonction d'une période prédéfinie, le fait d'indiquer que l'authentification est réussie ; lorsque le statut de l'interface GPIO ne change pas en fonction de la période prédéfinie, le fait d'indiquer que l'authentification n'est pas réussie.

2. Méthode selon la revendication 1, dans laquelle le fait de détecter si la puce de cryptage est invalide ou non comprend : le fait de déterminer, par la puce principale, si la puce de cryptage est invalide ou non en fonction de si des informations envoyées par la puce de cryptage sont reçues ou non dans une période de temps définie ; si les informations sont reçues, le fait de déterminer que la puce de cryptage n'est pas invalide ; sinon, le fait de déterminer que la puce de cryptage est invalide ;
ou la lecture, par la puce principale, d'un statut d'une interface d'entrée-sortie à usage général, GPIO, de la puce de cryptage, et le fait de déterminer, par la puce principale, si la puce de cryptage est invalide ou non ; lorsque le statut de l'interface GPIO change en fonction d'une période prédéfinie, le fait de déter-

miner que la puce de cryptage n'est pas invalide ; lorsque le statut de l'interface GPIO ne change pas en fonction d'une période prédéfinie, le fait de déterminer que la puce de cryptage est invalide ;
ou le fait de déterminer, par la puce principale, si la puce de cryptage est invalide ou non en fonction de si une clé secrète configurée pour authentifier le logiciel du terminal mobile est reçue ou non dans une période de temps définie; si la clé secrète est reçue, le fait de déterminer alors que la puce de cryptage n'est pas invalide ; sinon, le fait de déterminer que la puce de cryptage est invalide.

3. Méthode selon la revendication 1, dans laquelle la commande, par la puce de cryptage, d'un module fonctionnel du terminal mobile par le biais d'un circuit de protection matérielle comprend : la commande, par la puce de cryptage, d'un commutateur analogique dans le circuit de protection matérielle par le biais d'une ligne de commande pour éteindre une flash, et/ou verrouiller un clavier, et/ou éteindre un afficheur à cristaux liquides, LCD, et/ou éteindre une fonction audio, et/ou éteindre un accès de carte de module d'identité d'abonné, SIM.

4. Méthode selon la revendication 1, comprenant en outre : lorsqu'il est détecté que la puce de cryptage est invalide, la protection et la commande du module fonctionnel du terminal mobile par le biais d'un logiciel.

5. Méthode selon la revendication 4, dans laquelle la protection et la commande du module fonctionnel du terminal mobile par le biais d'un logiciel comprennent : le fait d'éteindre, par la puce principale du terminal mobile, un port de service réseau, et/ou un port LCD, et/ou un port fonctionnel audio, et/ou un port de réponse de clavier par le biais du logiciel du terminal mobile.

6. Méthode selon l'une quelconque des revendications 1 à 5, comprenant en outre : le réglage d'un temporisateur dans la puce de cryptage ; le démarrage d'une temporisation à nouveau chaque fois que le temporisateur arrive à expiration ; et le fait de détecter à nouveau si la puce de cryptage est invalide ou non et l'authentification à nouveau du logiciel du terminal mobile.

7. Appareil pour protéger un logiciel d'un terminal mobile, comprenant une puce principale du terminal mobile (31), une puce de cryptage (32) et un circuit de protection matérielle (33) ; dans lequel
la puce principale du terminal mobile (31) est configurée pour, lorsque le terminal mobile est allumé, détecter si la puce de cryptage (32) est invalide ou non, interagir avec la puce de cryptage (32) lorsque la puce de cryptage (32) n'est pas invalide, et authentifier le logiciel du terminal mobile ;
la puce de cryptage (32) est configurée pour interagir avec la puce principale du terminal mobile (31), authentifier le logiciel du terminal mobile, et notifier au circuit de protection matérielle (33) de commander un module fonctionnel du terminal mobile lorsque l'authentification n'est pas réussie, dans lequel la puce de cryptage (32) est montée dans le terminal mobile et des informations dans la puce de cryptage (32) ne peuvent pas être modifiées par la puce principale du terminal mobile (31) ; et
le circuit de protection matérielle (33) est configuré pour, en fonction de la notification en provenance de la puce de cryptage (32), commander le module fonctionnel du terminal mobile ;
dans lequel

(a) la puce de cryptage (32) est configurée pour envoyer à la puce principale du terminal mobile (31) une clé secrète configurée pour authentifier le logiciel du terminal mobile ; dans lequel la puce de cryptage (32) est en outre configurée pour : lorsque, dans une période de temps définie, elle reçoit un message d'échec d'authentification ou ne reçoit pas de clé secrète appariée envoyée par la puce principale du terminal mobile (31), indiquer que l'authentification n'est pas réussie ; et lorsqu'elle reçoit un message d'authentification réussie ou la clé secrète appariée, indiquer que l'authentification est réussie ;
en conséquence, la puce principale du terminal mobile (31) est en outre configurée pour, après la réception de ladite clé secrète configurée pour authentifier le logiciel du terminal mobile en provenance de la puce de cryptage (32), rechercher une clé secrète appariée avec ladite clé secrète dans la puce principale elle-même ; renvoyer la clé secrète appariée ou un message d'authentification réussie à la puce de cryptage (32) lorsque la clé secrète appariée avec ladite clé secrète est trouvée ; et renvoyer un message d'échec d'authentification ou ne pas renvoyer la clé secrète appariée à la puce de cryptage (32) lorsque la clé secrète appariée avec ladite clé secrète n'est pas trouvée ou pas recherchée ;
en conséquence, l'appareil comprend en outre un ordinateur (34) configuré pour définir des clés secrètes appariées l'une avec l'autre dans la puce de cryptage (32) et dans la puce principale du terminal mobile (31), respectivement ;
ou
(b) la puce de cryptage (32) est configurée pour lire un statut d'une interface d'entrée-sortie à usage général, GPIO, de la puce principale du terminal mobile (31) ; dans lequel la puce de cryptage (32) est en outre configurée pour : lorsque le statut de l'interface GPIO change en fonc-

tion d'une période prédéfinie, indiquer que l'authentification est réussie ; et lorsque le statut de l'interface GPIO ne change pas en fonction de la période prédéfinie, indiquer que l'authentification n'est pas réussie ;
en conséquence, la puce principale du terminal mobile (31) est en outre configurée pour prédéfinir une période de changement du statut de l'interface GPIO, et pour définir sa propre GPIO haute ou basse en fonction de la période.

8. Appareil selon la revendication 7, dans lequel la puce principale du terminal mobile (31) est configurée pour, en fonction de si des informations envoyées par la puce de cryptage (32) sont reçues ou non dans une période de temps définie, déterminer si la puce de cryptage (32) est invalide ou non ; si les informations sont reçues, déterminer que la puce de cryptage (32) n'est pas invalide ; si les informations ne sont pas reçues, déterminer que la puce de cryptage (32) est invalide ; en conséquence, la puce de cryptage (32) est en outre configurée pour envoyer des informations prédéterminées qui déterminent que la clé de cryptage (32) n'est pas invalide à la puce principale du terminal mobile (31) ;
ou la puce principale du terminal mobile (31) est configurée pour, en fonction d'un statut lu d'une interface d'entrée-sortie à usage général, GPIO, de la puce de cryptage (32), déterminer si la puce de cryptage (32) est invalide ou non ; lorsque le statut de l'interface GPIO change en fonction d'une période prédéfinie, déterminer que la puce de cryptage (32) n'est pas invalide ; lorsque le statut de l'interface GPIO ne change pas en fonction de la période prédéfinie, déterminer que la puce de cryptage (32) est invalide.

9. Appareil selon la revendication 7, dans lequel le circuit de protection matérielle (33) comprend une ligne de commande et un commutateur analogique ; dans lequel le commutateur analogique est réglé sur une ligne de signal du module fonctionnel du terminal mobile ; et la ligne de commande est configurée pour transmettre un signal de commande qui est utilisé par la puce de cryptage (32) pour commander le commutateur analogique ; et
le module fonctionnel du terminal mobile comprend : une flash, et/ou un module d'afficheur à cristaux liquides, LCD, et/ou un module de clavier, et/ou un module audio, et/ou un module de carte de module d'identité d'abonné, SIM.

10. Appareil selon la revendication 7, dans lequel la puce principale du terminal mobile (31) est en outre configurée pour, lorsqu'il est détecté que la puce de cryptage (32) est invalide, protéger et commander le module fonctionnel du terminal mobile par le biais d'un logiciel ;
dans lequel la protection et la commande du module fonctionnel du terminal mobile par le biais d'un logiciel comprennent : le fait d'éteindre un port de service réseau, et/ou un port LCD, et/ou un port fonctionnel audio, et/ou un port de réponse de clavier par le biais du logiciel du terminal mobile.

11. Appareil selon l'une quelconque des revendications 7 à 10, dans lequel la puce de cryptage (32) est en outre configurée pour régler un temporisateur ; dans lequel le temporisateur est configuré pour démarrer une temporisation à nouveau chaque fois que le temporisateur arrive à expiration, et pour déclencher la puce principale du terminal mobile (31) et la puce de cryptage (32) pour détecter à nouveau si la puce de cryptage (32) est invalide et authentifier à nouveau le logiciel du terminal mobile.

Fig. 1

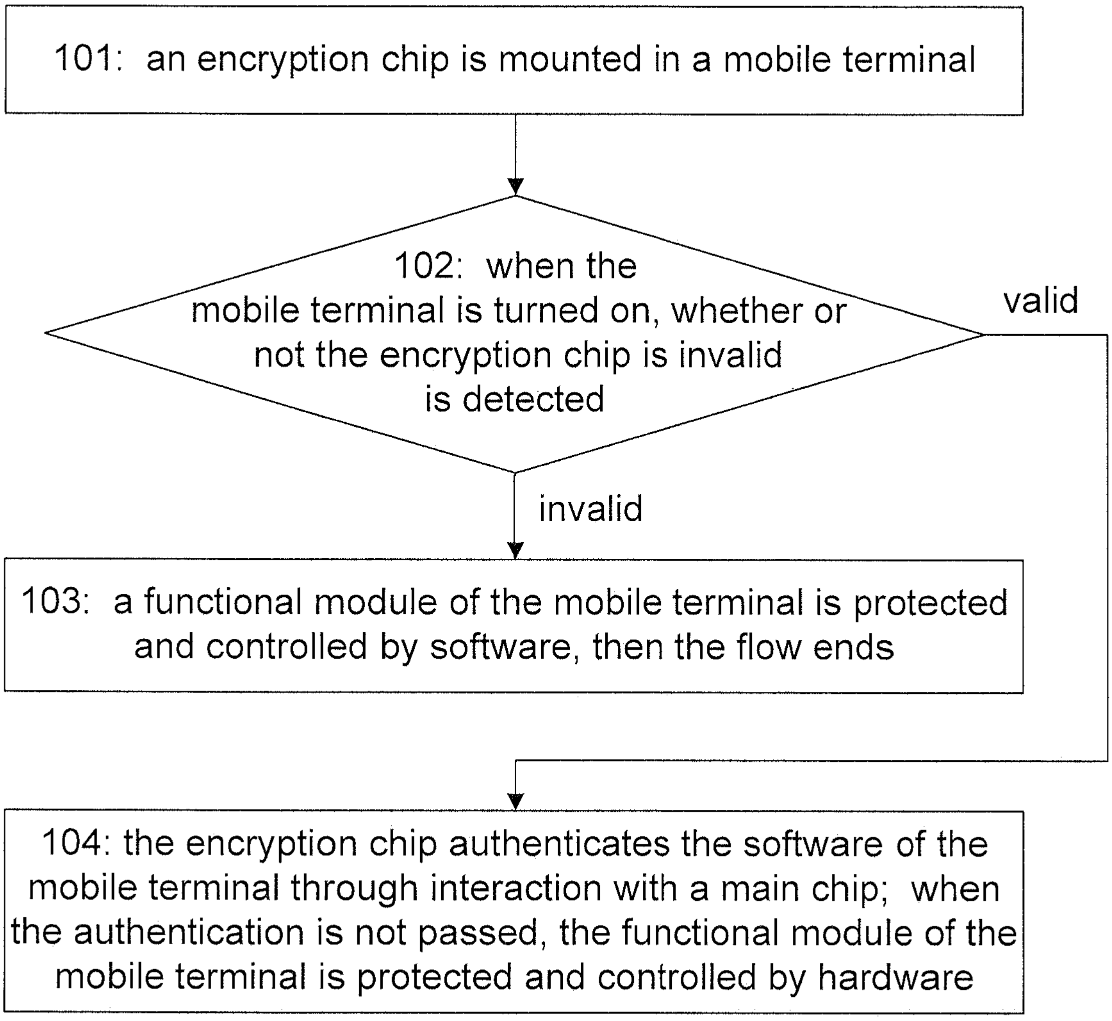

101: an encryption chip is mounted in a mobile terminal
102: when the mobile terminal is turned on, whether or not the encryption chip is invalid is detected
valid
invalid
103: a functional module of the mobile terminal is protected and controlled by software, then the flow ends
104: the encryption chip authenticates the software of the mobile terminal through interaction with a main chip; when the authentication is not passed, the functional module of the mobile terminal is protected and controlled by hardware

Fig. 2

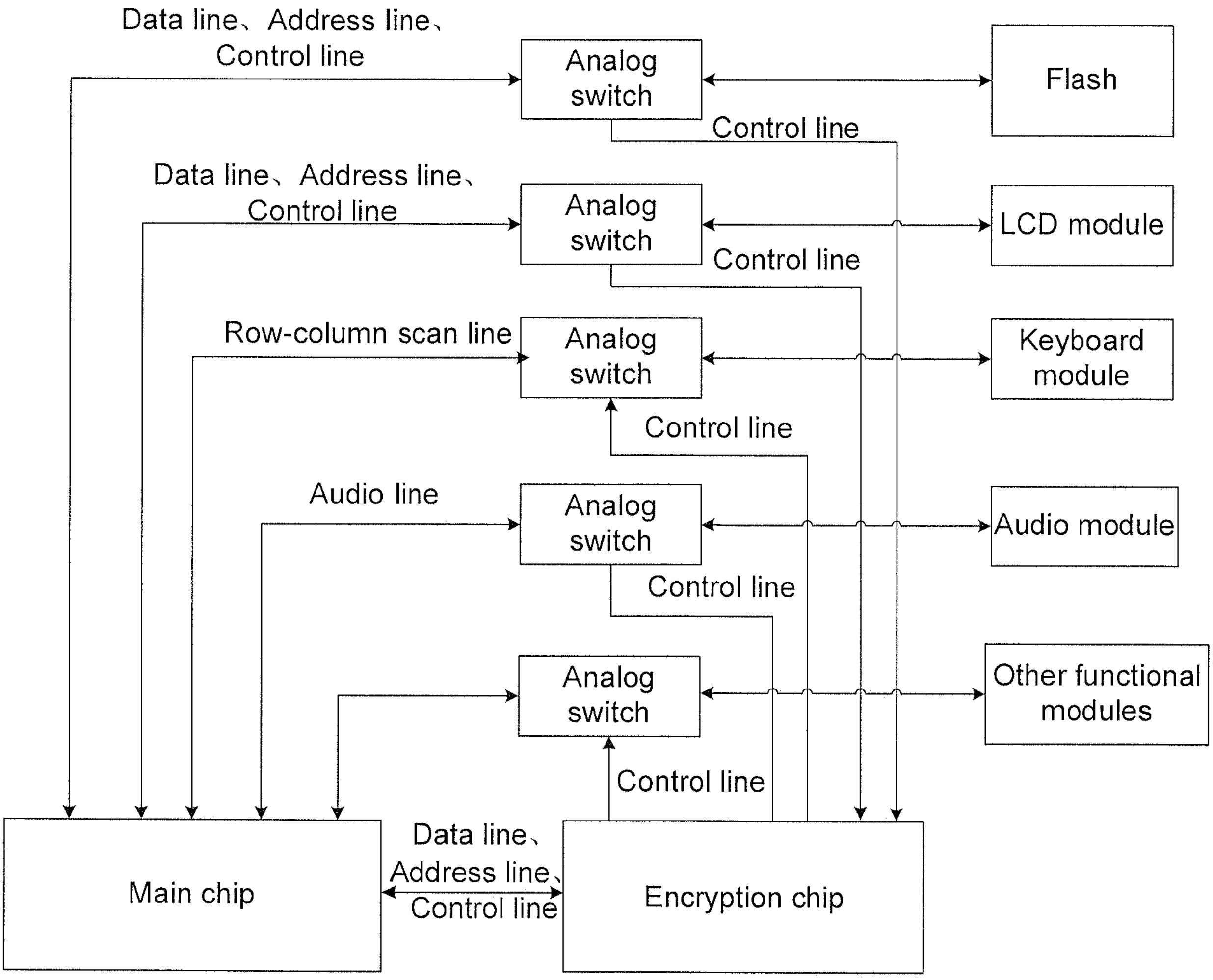
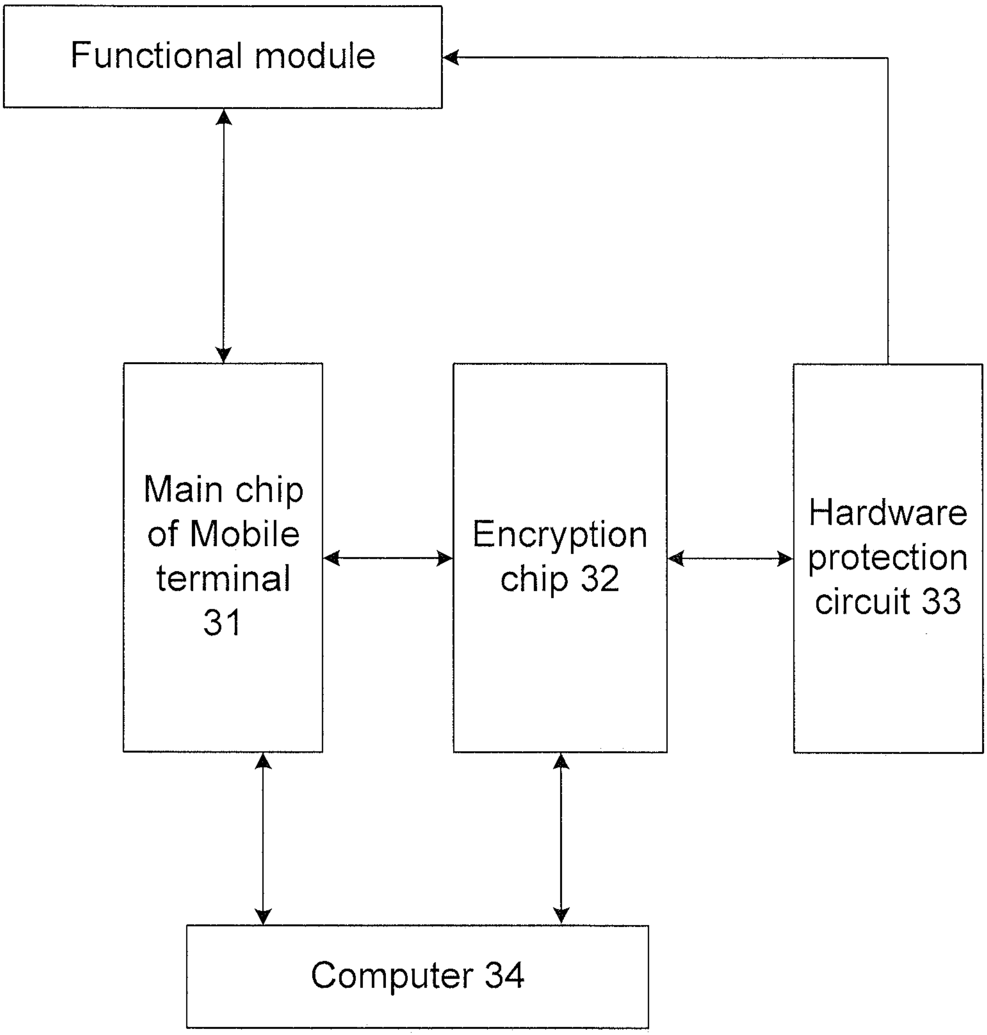

Data line、Address line、
Control line
Analog switch
Flash
Control line
Data line、Address line、
Control line
Analog switch
LCD module
Control line
Row-column scan line
Analog switch
Keyboard module
Control line
Audio line
Analog switch
Audio module
Control line
Analog switch
Other functional modules
Control line
Main chip
Data line、
Address line、
Control line
Encryption chip

Fig. 3


Functional module
Main chip of Mobile terminal 31
Encryption chip 32
Hardware protection circuit 33
Computer 34

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2007101156 A1 **[0005]**
- US 2006143446 A1 **[0006]**