A memory protection method is provided with a user input key. The user input key is compared with an internal private key in a memory security circuit having an integral connection with a solid-state memory for controlling data flow therefrom.
FIG. 1

FIG. 2
FIG. 3

CHALLENGE 306

MEMORY CONTROLLER 304

KEY 310

MPS 302

SECURITY SYSTEM 300

RESPONSE 308

FIG. 4

FACTORY KEY ERASE 402

POWER APPLIED 404

USER INPUT KEY ERASED 406

MPS UNLOCKED 408

PRIVATE KEY WRITTEN MPS 412

NEW PRIVATE KEY ACCEPTED 410

MPS LOCKED 414

PERFORM UNLOCK SEQUENCE 416
FIG. 5

POWER APPLIED 502

USER KEY ERASED 504

USER INPUTS USER KEY 522

USER KEY = PRIVATE KEY 508

MEMORY NOT ENABLED 516

INCREMENT FAILED ATTEMPTS 518

FAILED ATTEMPTS > LIMIT 520

ERASE MEMORY 524

ACCESS PERMITTED 514

CLEAR FAILED ATTEMPTS 512
POWER APPLIED 602

USER KEY ERASED 604

WRITE USER KEY TO MPS 606

USER KEY = PRIVATE KEY 608

NO

MPS REMAINS LOCKED 610

NEW PRIVATE KEY REJECTED 612

YES

MPS UNLOCKED 616

NEW PRIVATE KEY WRITTEN TO MPS 618

NEW PRIVATE KEY ACCEPTED 620

MPS LOCKED 622

PERFORM UNLOCK SEQUENCE 624

FIG. 6
FIG. 7

FIG. 8

PROVIDING A USER INPUT KEY

COMPARING THE USER INPUT KEY WITH AN INTERNAL PRIVATE KEY IN A MEMORY SECURITY CIRCUIT HAVING AN INTEGRAL CONNECTION WITH A SOLID-STATE MEMORY FOR CONTROLLING DATA FLOW THEREFROM
TECHNICAL FIELD

[0001] The present invention relates generally to integrated circuits devices, and more particularly to memory devices.

BACKGROUND ART

[0002] A critical issue with almost all aspects of computer use and mobile electronic device use, including portable memory storage devices is security. This also applies to security in any electronic products, such as portable memory devices (e.g., Universal Serial Bus memory drives), camcorders, digital cameras, iPods, MP3 players, smart phones, palm computers, gaming devices, etc., having important information in memory. Whether it is logging into an email account, protecting personal medical or financial info, family pictures, etc. or accessing bank information, information must be supplied to gain access to personal data. Much money and effort has been applied to guarding personal, corporate, and government information from hackers and others.

[0003] Encryption is used to hide sensitive information. It is a complex process used to hide information stored on various types of storage media such as solid-state non-volatile memory devices (e.g. Flash drives), hard drives, and other media.

[0004] Software encryption is typically performed on a host computer prior to saving data to a mass storage device. Software encryption consumes system resources and, thus, requires high performance hardware to reduce system computing burden. Since the data is always accessible (although encrypted), it can eventually be hacked.

[0005] Encryption can also be performed on the storage media itself. This reduces the impact on computer resources and the possibility of a successful hacking attempt. The downside is that it adds expense to the mass storage module.

[0006] However, all of these systems have problems in being inconvenient to use.

[0007] Solutions to these problems have been long sought but prior developments have not taught or suggested any solutions and, thus, solutions to these problems have long eluded those skilled in the art.

DISCLOSURE OF THE INVENTION

[0008] The present invention provides a memory protection method including: providing a user input key; and comparing the user input key with an internal private key in a memory security circuit having an integral connection with a solid-state memory for controlling data flow therefrom.

[0009] The present invention provides a memory protection system including a user input key storage; an internal private key storage; a comparator having integral connections with the user input key storage and the internal private key storage; and a solid-state memory having an integral connection with the comparator for allowing access to data therein when the contents of the internal private key storage and the user input key storage match.

[0010] Certain embodiments of the invention have other aspects in addition to or in place of those mentioned above. The aspects will become apparent to those skilled in the art from a reading of the following detailed description when taken with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 is a view of a memory protection system (MPS) in accordance with an embodiment of the present invention;
[0012] FIG. 2 is a view of a MPS in accordance with a further embodiment of the present invention;
[0013] FIG. 3 is a view of a challenge-response security system incorporating a MPS in accordance with a further embodiment of the present invention;
[0014] FIG. 4 is a flow-chart showing initial operations of a MPS upon arrival from a factory;
[0015] FIG. 5 is a flow chart depicting how a MPS may be programmed to require that the user input key be provided within a certain number of attempts;
[0016] FIG. 6 is a flow chart showing the steps to change an internal private key of a MPS; FIG. 7 is a view of an embodiment of the present invention incorporated in a universal serial bus (USB) Flash drive; and
[0017] FIG. 8 is a flow chart of a memory protection method in accordance with an embodiment of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

[0018] The following embodiments are described in sufficient detail to enable those skilled in the art to make and use the invention. It is to be understood that other embodiments would be evident based on the present disclosure, and that system, process, or mechanical changes may be made without departing from the scope of the present invention.

[0019] In the following description, numerous specific details are given to provide a thorough understanding of the invention. However, it will be apparent that the invention may be practiced without these specific details. In order to avoid obscuring the present invention, some well-known circuits, system configurations, and process steps are not disclosed in detail.

[0020] Likewise, the drawings showing embodiments of the system are semi-diagrammatic and not to scale and, particularly, some of the dimensions are for the clarity of presentation and are shown exaggerated in the drawing FIGs.

[0021] The term “system” is defined to mean a device or method for practicing embodiments of the present invention and includes both device circuits and method steps.

[0022] In the present disclosure, the following definitions are used:

Solid-state memory—any type of memory implemented in a semiconductor material including, without limitation, NAND Flash, NOR Flash, EPROM, NVRAM, RAM, etc.

Memory security circuit—an integrated circuit for protecting a solid-state memory in accordance with an embodiment of the present invention.

Protected memory chip—a solid-state memory and a memory security circuit chip in the same integrated circuit die.

Protected memory package—a solid-state memory chip and a memory security circuit chip in a single integrated circuit package.
MPS—a Memory Protection System, which can be a protected memory chip, protected memory package, or other protected memory configuration.

Key—a binary code of arbitrary length.

User input key—a key that originates from a user, which may be a direct translation of what was input or may be a derivation thereof.

Internal private key—a key kept internally in the memory security circuit and not accessible from outside the integrated circuit except under specified conditions.

Integral Connection—an electrical connection to a solid-state memory that cannot be broken without impacting the functionality of a solid-state memory.

[0023] Referring now to FIG. 1, therein is shown a memory protection system (MPS 100) in accordance with an embodiment of the present invention. The MPS 100 includes a user input key input 102 with an integral connection to a user input key storage 104 for storing a user input key. The MPS 100 also includes an internal private key storage 106 for storing an internal private key. The user input key storage 104 and the internal private key storage 106 have integral connections to a compare circuit 108 for comparing the contents of the user input key storage 104 and the internal private key storage 106. The compare circuit 108 has an integral connection to a solid-state memory 112.

[0024] When the contents of the user input key storage 104 and the internal private key storage 106 match, the compare circuit 108 provides a memory enable output 110 to the solid-state memory 112. When the memory enable output 110 is received by the solid-state memory 112, the solid-state memory 112 will provide its contents to an integrally connected memory output 114. When the contents do not match, the memory enable output 110 is not provided and the solid-state memory 112 is not accessible or locked.

[0025] The user input key storage 104, the internal private key storage 106, and the compare circuit 108 form a memory security circuit 116.

[0026] The solid-state memory 112 and the memory security circuit 116 are manufactured on the same integrated circuit chip and cannot be physically separated without destroying the functionality of the solid-state memory 112. Thus, the memory security circuit 116 provides a “security gate” that seals access to the internal contents of the solid-state memory 112. The contents of the solid-state memory 112 are not accessible or “visible” so the contents of the solid-state memory 112 do not need to be encrypted (the contents are invisible by “design”).

[0027] The solid-state memory 112 hides data from view. If one is unable to view data, hacking is not possible. The MPS 100 restricts access to its contents until the memory security circuit 116 unlocks access with the correct interaction. If the memory security circuit 116 is unable to supply the memory enable output 110 because the correct interaction or user input key is not provided, the contents of the solid-state memory 112 remains locked and hidden from view.

[0028] Since the compare circuit 108 makes comparisons using the internal private key in the internal private key storage 106, if the internal private key storage 106 is blank, the solid-state memory 112 is accessible without a need to supply a user input key at the input 102.

[0029] Thus, erasing the MPS 100 will also erase its internal private key in the internal private key storage 106. Then, when the MPS 100 powers up, the user input key storage 104 is initialized to an equivalent erased state. At this point, the MPS 100 behaves as any other unprotected memory device that can be freely written and read to as long as there’s no internal private key stored in the internal private key storage 106.

[0030] Writing an internal private key to the internal private key storage 106 is possible only under the special situation when the MPS 100 is unlocked or is blank. When an internal private key is entered, the MPS 100 will lock and restrict further access to the solid-state memory 112 until a user input key is provided to the user input key storage 104 that matches the internal private key storage 106. With a protected memory chip or protected memory package in the MPS 100, the solid-state memory 112 is encapsulated and made tamper proof from the outside world.

[0031] The input 102 and the output 114 provide for simple access to the MPS 100, such that it can be used in other devices. For example, a secure solid-state memory can be easily added to a cell phone without the added burden of implementing complex encryption algorithms by simply replacing the cell phone memory with the MPS 100. The MPS 100, and not the system of the cell phone, imposes security.

[0032] Referring now to FIG. 2, therein is shown a MPS 200 in accordance with a further embodiment of the present invention. The MPS 200 has input/output (110) ports 202 with an integral connection to an I/O control circuit 204. The I/O control circuit 204 has an integral connection to a user input key register 206 for storing a user input key (206) and an internal private key register 208 for storing an internal private key (208). The user input key register 206 and the internal private key register 208 have an integral connection to a logic circuit, such as an XOR gate 210. The XOR gate 210 has an integral connection to a control circuit 212.

[0033] The I/O ports 202, the user input key register 206, the internal private key register 208, the logic circuit 210, and the control circuit 212 are integral components in a memory security circuit 213 having integral connections to a solid-state memory 216.

[0034] The control circuit 212 provides an enable/disable signal 214 to the solid-state memory 216 having an integral connection to the I/O control circuit 204. The solid-state memory 216 only provides data along a data path 218 to the I/O control circuit 204 when enabled.

[0035] The MPS 200 may be integrated using an existing NAND Flash memory. The XOR gate 210 compares the user input key and the internal private key in which the result is zero. Other compare operations can also be used to determine a match.

[0036] Both the user input key and the internal private key can be input over the I/O ports 202 using the same mechanism. For example, for a NAND Flash memory, an operation is preceded with a command (e.g., write-sector). A command is then followed with the appropriate data. In this case, the commands “write-user-key” and “write-private-key” are created to perform the operations through the I/O ports 202. The “write-user-key” will operate at any time, but the “write-private-key” will work only when the MPS 200 is unlocked.

[0037] The above mechanism does not have to be followed in the strictest sense. User input and internal private keys can be set through separate I/O ports 202 with their own unique timing requirements. There are many ways to write data to internal registers, which may exist in the peripheral circuitry of solid-state memories. In the MPS 200, the MPS 200 is locked by removing power or by clearing the user input key register 206. A user cannot read the internal private key reg-
ister 208, and the internal private key in the internal private key register 208 is saved across power cycles. The user cannot set a new internal private key until the MPS 200 is unlocked.

- **0038**: The user input key and the internal private key can be of any length and structure, but longer keys are more secure.

- **0039**: Erasing the MPS 200 will also erase the internal private key register 208. This is especially true where the solid-state memory 216 has private and public zones and may be set up to have multiple private zones with multiple corresponding internal private keys to allow access to those multiple private zones.

- **0040**: Referring now to FIG. 3, therein is shown a challenge-response security system 300 incorporating a MPS 302 in accordance with a further embodiment of the present invention. A “challenge-response” is an authentication technique in which an individual is prompted (the “challenge”) to provide some private information (the “response”). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the “challenge”), which the user enters into the smart card. The smart card then displays a new code (the “response”) that the user can present to gain access to the security system.

- **0041**: The challenge-response security system 300 includes a memory controller 304, such as a universal serial bus (USB) controller. The memory controller 304 issues a challenge 306 and the user provides a response 308 to the memory controller 304. The challenge-response may be conducted directly with the user (supplied with an input mechanism or biometric input) or indirectly through a computer. For example, a computer may request a pass-code that is then passed to the memory controller 304. The memory controller 304 processes the pass-code sent from the computer to create a user input key 310 that is then sent on to the MPS 302. A correct user input key 310 will unlock the MPS 302 and allow free access to its internal solid-state memory. A challenge-response may also take the form of a fingerprint or other biometric information or an electromechanical input mechanism (e.g., PIN input).

- **0042**: Referring now to FIG. 4, therein is shown a flow chart 400 showing initial operations of the MPS upon arrival from a factory. The flow chart 400 starts at the factory with an internal private key being erased in a block 402.

- **0043**: On delivery to a user, the user applies power in a block 404. After power is applied in the block 404, a user input key is erased in a block 406. This causes the MPS 200 to be unlocked in a block 408.

- **0044**: The user then writes a private key to the MPS in a block 412 and the new private key is accepted in a block 410. With the new private key being accepted in the block 410, the MPS is now locked in a block 414, and it is necessary to perform an unlock sequence in a block 416 to perform further operations on the MPS.

- **0045**: If the user writes a blank private key, e.g., no new private key, to the MPS in the block 412, this erases the internal private key and the MPS is not locked in the block 414. This means that the solid-state memory is unlocked across power cycles and the unlock sequence does not have to be performed in the block 416.

- **0046**: The MPS is shipped from a factory in the erased (unlocked) state with a blank internal private key. Since the user input key gets erased on power up, full access is granted for the first power up. In other words, since both the user input key and the internal private key have been erased and match, full access is given to the erased solid-state memory:

- **0047**: This feature is also useful in being able to recover the use of the solid-state memory if a PIN password is forgotten. By erasing the solid-state memory, all stored information is secure in being erased along with the previously set private key being erased. The solid-state memory is fully functional to be able to accept a new private key and new information.

- **0048**: Referring now to FIG. 5, therein is shown a flow chart 500 showing how a MPS may be programmed to require the user input key being provided within a certain number of attempts.

- **0049**: Power is applied in a block 502, which causes the user input key to be erased in a block 504. The user input key is then compared with the internal private key in a decision block 508. If the user input key matches the internal private key, the solid-state memory is enabled in a block 510, the number of failed attempts is cleared in a block 512, and full access is permitted to the solid-state memory in a block 514.

- **0050**: However, if the user input key does not match the internal private key in the decision block 508, the solid-state memory is not enabled in a block 516 and the number of failed attempts is incremented in a block 518. A check is then made to see if the number of failed attempts has been exceeded in a decision block 520.

- **0051**: If the failed attempts have not exceeded a preset limit, the user is allowed to supply another user input key in a block 522 for another comparison of the new user input key with the internal private key in the decision block 508.

- **0052**: If the failed attempts exceed the limit in the decision block 520, the solid-state memory is erased in a block 524. Once the solid-state memory is erased in the block 524, full access to the erased solid-state memory is permitted in the block 514.

- **0053**: If a 64-bit key (4,294,967,294 values) is used to lock the MPS and three unsuccessful attempts are permitted prior to erasure, a hacker has a 6.9×10^-8% chance of accessing the memory by trial and error.

- **0054**: If the user decides to keep the solid-state memory locked after power is applied in the block 502, the user may decide to input a user key in the block 522 that does not match the private key. Thus, when a user is temporarily not using the device in which the MPS is incorporated or attached, an unauthorized user is prevented from accessing the solid-state memory.

- **0055**: Referring now to FIG. 6, therein is shown a flow chart 600 which shows the steps in changing an internal private key of a MPS.

- **0056**: Power is applied in a block 602 and the user input key is erased in a block 604. The new user input key is written to the MPS in a block 606.

- **0057**: If the user input key is different from the internal private key in a decision block 608, the MPS remains locked in a block 610 and the new private key is rejected in a block 612.

- **0058**: If the user input key is the same as the internal private key in the decision block 608, the MPS is unlocked in a block 616. At this time, a new private key may be written to the MPS in a block 618. If the MPS remains locked in the block 610, the new private key is rejected in the block 612. However, if the MPS is unlocked in the block 616, the new private key is accepted in a block 620. The MPS then is locked
in a block 622 and the unlock sequence must be performed in a block 624 to access the solid-state memory.

[0059] Referring now to FIG. 7, therein is shown an embodiment of the present invention incorporated in a USB Flash drive 700. The USB Flash drive 700 would be used with a laptop or other computer. The USB Flash drive 700 includes a USB connector 706, which would be plugged into a USB port in the computer 702.

[0060] A pass-code 708 would be sent from the computer 702 or a pass-code 726 from the input mechanism 724 to a memory controller 712 in the USB Flash drive 700. The pass-code 708 or the pass-code 726 is translated in a key translator 714 to provide a user input key 716 to a MPS 718. The MPS 718 enabled data would pass bi-directionally across a data link 720 to the memory controller 712 and bi-directionally on the USB connector 706 across a data link 722.

[0061] An input mechanism 724 can be incorporated in the USB Flash drive 700 for authenticating the user. The input mechanism 724 can include an electro-mechanical combination input, biometric input (fingerprint or iris scan), or any other input.

[0062] Referring now to FIG. 8, therein is shown a flow chart of a memory protection method 800 in accordance with an embodiment of the present invention. The method 800 includes providing a user input key in a block 802; and comparing the user input key with an internal private key in a memory security circuit having an integral connection with a solid-state memory for controlling data flow therefrom in a block 804.

[0063] While the invention has been described in conjunction with a specific best mode, it is to be understood that many alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended to embrace all such alternatives, modifications, and variations that fall within the scope of the included claims. All matters hitherto set forth herein or shown in the accompanying drawings are to be interpreted in an illustrative and non-limiting sense.

1. A memory protection method comprising:
   - providing a user input key; and
   - comparing the user input key with an internal private key in a memory security circuit having an integral connection with a solid-state memory for controlling data flow therefrom.

2. The method as claimed in claim 1 further comprising:
   - erasing the internal private key to keep the solid-state memory unlocked.

3. The method as claimed in claim 1 further comprising:
   - providing a new user input key different from the internal private key to keep the solid-state memory locked.

4. The method as claimed in claim 1 further comprising:
   - writing a new internal private key; and
   - accessing the solid-state memory with the new internal private key.

5. The method as claimed in claim 1 further comprising:
   - inputting an incorrect user input key a predetermined number of times; and
   - erasing the solid-state memory when the predetermined number of times is exceeded.

6. A memory protection method comprising:
   - inputting and outputting a plurality of input and output signals through an input/output control circuit to provide a user input key, an internal private key, and data;
   - storing the user input key and the internal private key in storage having an integral connection to the input/output control circuit;
   - comparing the user input key and the internal private key in a logic circuit having an integral connection to the storage;
   - controlling a control circuit when the user input key and the internal private key match to output an enable signal to a solid-state memory having an integral connection to the control circuit; and
   - outputting the data to the input/output control circuit from the solid-state memory in response to the enable signal.

7. The method as claimed in claim 6 further comprising:
   - erasing the internal private key when power is turned off and on.

8. The method as claimed in claim 6 further comprising:
   - writing a new user input key different from the internal private key to keep the solid-state memory locked while power is on.

9. The method as claimed in claim 6 further comprising:
   - erasing the internal private key;
   - erasing the solid-state memory and the user input key when the internal private key is erased;
   - writing a new internal private key; and
   - accessing the solid-state memory with the new internal private key.

10. The method as claimed in claim 6 further comprising:
    - inputting an incorrect user input key a predetermined number of times;
    - erasing the solid-state memory when the predetermined number of times is exceeded;
    - writing a new internal private key; and
    - accessing the solid-state memory with the new internal private key.

11. A memory protection system comprising:
    - a user input key storage;
    - an internal private key storage;
    - a comparator having integral connections with the user input key storage and the internal private key storage; and
    - a solid-state memory having an integral connection with the comparator for allowing access to data therein when the contents of the internal private key storage and the user input key storage match.

12. The system as claimed in claim 11 further comprising:
    - circuitry for erasing the internal private key to keep the solid-state memory unlocked.

13. The system as claimed in claim 11 further comprising:
    - circuitry for providing a new user input key different from the internal private key to keep the solid-state memory locked.

14. The system as claimed in claim 11 further comprising:
    - circuitry for erasing the internal private key;
    - circuitry for writing a new internal private key; and
    - circuitry for accessing the solid-state memory with the new internal private key.

15. The system as claimed in claim 11 further comprising:
    - circuitry for inputting an incorrect user input key a predetermined number of times; and
    - circuitry for erasing the solid-state memory when the predetermined number of times is exceeded.
16. A memory protection system comprising:
an input/output control circuit for inputting and outputting
a plurality of input and output signals to provide a user
input key, an internal private key, and data;
registers for storing the user input key and the internal
private key, the registers having an integral connection to
the input/output control circuit;
a logic circuit for comparing the user input key and the
internal private key, the logic circuit having an integral
connection to the registers;
a control circuit for outputting an enable signal when the
user input key and the internal private key match, the
control circuit having an integral connection to the logic
circuit; and
a solid-state memory for outputting the data to the input/
output control circuit in response to the enable signal,
the solid-state memory having an integral connection to
the control circuit.

17. The system as claimed in claim 16 further comprising:
circuitry for erasing the internal private key to keep the
solid-state memory locked when power is turned off
and on.

18. The system as claimed in claim 16 further comprising:
circuitry for writing a new user input key different from the
internal private key to keep the solid-state memory
locked while power is on.

19. The system as claimed in claim 16 further comprising:
circuitry for erasing the internal private key;
circuitry for erasing the solid-state memory and the user
input key when the internal private key is erased;
circuitry for writing a new internal private key; and
circuitry for accessing the solid-state memory with the new
internal private key.

20. The system as claimed in claim 16 further comprising:
circuitry for inputting an incorrect user input key a prede-
determined number of times;
circuitry for erasing the solid-state memory when the pre-
determined number of times is exceeded;
circuitry for writing a new internal private key; and
accessing the solid-state memory with the new internal
private key.