The system includes a second nonvolatile memory including data to be transferred to the volatile memory.

**Abstract:** The disclosure includes a system and method of using a processor and protected memory. In a particular embodiment, the system includes a processor, a volatile memory accessible to the processor, and a first nonvolatile memory accessible to the processor. The first nonvolatile memory includes a first portion of memory that is protected and is readable when a shield bit indicates an unshielded mode of operation, but is unreadable when the shield bit indicates a shielded mode of operation and a second portion of memory that is unprotected and that is readable regardless of the value of the shield bit. The system includes a second nonvolatile memory including data to be transferred to the volatile memory.
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
SYSTEM AND METHOD OF USING A PROTECTED NON-VOLATILE MEMORY

FIELD OF THE DISCLOSURE

The present disclosure relates generally to use of protected non-volatile memory.

BACKGROUND

Electronic device providers that use software programmable devices have concerns related to software security. To address these security concerns, such devices often use security techniques such as authentication and encryption. While authentication and encryption are useful tools, such methods rely upon the protection of one or more keys that are used to authenticate or decrypt program data. Often the keys needed to be protected are stored within a memory, such as a non-volatile memory, of the electronic device that is sold and deployed. Upon deployment of the electronic device or even during development, the memory containing the keys may be accessed by unauthorized third parties causing a security risk. Thus, there is a need for an improved system and method of protecting the security of software program data and the associated keys to security programs that protect the program data, where such keys are stored in non-volatile memory.

BRDSF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram that illustrates a system that has access to a partially protected non-volatile memory device;

FIG. 2 is a block diagram that provides further details of a portion of the system of FIG. 1; and

FIG. 3 is a flow chart of a method of activating a processor device having access to a partially protected non-volatile memory.

DETAILED DESCRIPTION OF THE DRAWINGS

Referring to FIG. 1, a data processing system 100 is shown. The system 100 includes a processor device 102, a volatile memory 104, a first non-volatile memory 106, and a second non-volatile memory 108. The system 100 also includes control registers 110 and a JTAG interface 130 to a JTAG control module 112. The processor device 102 is coupled for access to the control registers 110 and has an input to receive an external test clock input over the JTAG interface 130. The processor device 102 includes test protection logic 126 that interfaces to the JTAG test interface 130. The processor device 102 is coupled to the volatile memory 104 via a memory bus 114. In a particular embodiment, the volatile memory 104 is a random access memory (RAM) device. The processor device 102 is coupled to the first non-volatile memory 106 via the memory bus 114 and via intermediate shield logic 122. The shield logic 122 couples the first non-volatile memory 106 to the memory bus 114 and has an input of a ROM shield bit 124. The ROM shield bit 124 may be stored and programmed as one of the controls registers 110 or may be implemented in a separate write-once memory device. The processor
device 102 is coupled to the second non-volatile memory 108 via the memory bus 114. The first non-volatile memory 106 includes a first interface 120 to shield logic 122 and an external interface 118 to the memory bus 114. The second non-volatile memory 108 includes an interface 116 to the memory bus 114.

The first non-volatile memory 106 includes a first shielded portion of memory 150 that is a shielded portion and a second portion of memory 160. The shielded portion 150 includes a stored key set data 152. In a particular embodiment, the key data 152 includes an authentication key, an encryption key, key set extraction data, and key set extraction program logic needed to retrieve and use the key set information. The second non-volatile memory 108 may be implemented in a particular embodiment as a flash memory and includes data, such as boot program code 140. In a particular embodiment, the first non-volatile memory 106 may be implemented as a read-only memory (ROM).

In a particular embodiment, the boot program code 140 includes a plurality of interspersed authentication words. The plurality of authentication words are used during a transfer of the boot program code from the second non-volatile memory 108 to the random access memory 104 and provides a method of authenticating the validity of the boot program code to detect third party unauthorized use or hacking attempts. In a particular embodiment, the authentication words are assessed and validated using an authentication key found within the key set 152 of the shielded portion 150 of the non-volatile memory 106.

During operation, upon power up of the system 100, the shielded portion 150 of the non-volatile memory 106 is in an unshielded mode that allows for read access to the key set 152. During initialization in the unshielded mode, the processor 102 may retrieve the key set 152 and may use the keys within the key set to perform a transfer process where the application program code 140 is transferred from the second non-volatile memory 108 to the random access memory 104. The key set may include both an authentication key and/or a decryption key. The authentication key may be used to authenticate the validity of the program code and to access and compare transferred data with first authentication words, and the decryption key may be used to decrypt the program code if such code has been previously encrypted. Thus, the key set 152 may be used by the processor device 102 to provide for a secure initial transfer of the program code 140 from the non-volatile memory 108 to the random access memory 104.

After the program code has been transferred into the random access memory 104, but before execution of the program code by the processor 102, the ROM shield bit 124 may be set by the processor 102. By setting the ROM shield bit 124, the shielded portion 150 of the first non-volatile memory 106 enters a shielded mode where the key set 152 is unreadable. In this situation, the shield logic 122 prevents access to the shielded portion 150 of the first non-volatile memory 106 and instead may provide an error code or a fixed value that indicates the shielded and unreadable memory condition. After the ROM shield bit 124 has been set and the shielded portion 150 of the first non-volatile memory 106 enters the shield mode to restrict access to the key set 152, the processor device 102 may transition from a supervisory mode to a user operator mode and may then execute instructions from the random
access memory 104. Thereafter, the processor device 102 in the user mode executes instructions
during normal operation. During the user execution mode and normal operation, it should be noted that
the shielded portion 150 remains in the shielded mode thereby restricting access to the key set 152.
Thus, the ROM shield bit 124 and the shielded portion 150 of the first non-volatile memory 106,
5 together with the key set 152, provides for enhanced security of the program code transfer to the
random access memory 104.

An unauthorized third party may attempt access to the key set 152 via a test interface such as the JTAG
control interface 130. To restrict such unauthorized access, the processor device 102 includes the test
protection logic 126. The test protection logic 126 is responsive to an external clock input and may
detect an attempted unauthorized access of the shielded portion 150. In a particular embodiment, the
processor device 102, in response to detection by the test protection logic 126 of a number of clock
cycles exceeding a threshold, may set the ROM shield bit 124. In a particular example, the detection
threshold is less than forty clock cycles, such as a setting of twenty clock cycles. In the case of a JTAG
instruction, the minimum JTAG instruction would require a number of clock cycles that is greater than
twenty. Thus, the threshold of less than forty and preferably twenty clock cycles may be used to detect
and then respond to an unauthorized attempt to access the key set 152 via the JTAG interface.

Referring to FIG. 2, a particular embodiment of a portion of the system 100 that illustrates functionality
of the first non-volatile memory 106 and the shield logic 122 is shown. The first non-volatile memory
106 is coupled to a read multiplexer (MUX) 202 via a first interface 120. The MUX 202 is coupled to
the memory bus 114 via interface 118. The MUX 202 has an input of a fixed value 206 that may be an
error code or other indication of a shielded condition. The MUX 202 includes a select input that is
provided by logic module 204. The logic module 204 is responsive to a ROM shield bit 124 that may
be provided by a write once memory 220. The logic module 204 is also responsive to an address code
118 provided from the memory bus 114 via the memory interface 118.

During operation, the ROM shield bit 124 is provided to the logic module 204 to indicate the state of
the shielded portion 150 of the non-volatile memory 106. The logic module 204 also receives
addresses from the memory bus 114. When the address requested from the memory bus 114 is outside
of the shielded portion of memory 150, then data, such as boot program or other data from within the
non-shielded portion of memory 160, is provided from the first non-volatile memory 106 through the
MUX 202 to the memory bus 114 over interface 118.

However, when the address requested from the memory bus 114 is an address within the shielded
portion of memory 150 and when the ROM shield bit has been set, the logic module 204 provides a
selector to the MUX 202 to only provide the fixed value 206 as an output over interface 118 to the
memory bus 114. In this condition, the contents of the shielded portion of the memory 150 are in a
security shielded state and are protected from access. In addition, to avoid unauthorized modifications
to the ROM shield bit 124, the ROM shield bit may be stored and programmed in a write once memory
220. With a write once memory, once the ROM shield bit has been set, the memory may not be
modified. Use of the write once memory thereby provides enhanced security for maintaining shielding
of the first portion 150 of the non-volatile memory 106. In a particular embodiment, the shielded portion of memory 150 includes an authentication key, a decryption key, and a key set extraction program and data as needed for retrieval of the key set from the non-volatile memory during the non-shielded operating mode. Thus, the non-volatile memory 106 includes a first portion of memory 150 that is protected and is readable when a shield bit indicates an unshielded mode of operation, but is unreadable when the shield bit indicates a shielded mode of operation. In addition, the non-volatile memory 106 includes a second portion 160 that is unprotected and that is readable regardless of the value of the shield bit 124.

Referring to FIG. 3, a method of activating a processor device having access to a non-volatile memory is shown. The method includes powering up the processor device, as shown at 302. In a particular embodiment, the processor device is coupled to a read only memory (ROM) that has a protected portion of memory that is shieldable but where the protected portion is in an unshielded mode upon power up. The method further includes reading key set data from the protected portion of the non-volatile memory that is in the unshielded mode of operation, as shown at 304, and transferring data from a second non-volatile memory, such as a flash memory, to a main memory, such as a random access memory (RAM). This step also includes accessing key set extraction data and using the key set extraction data and program logic to access the key set to perform authentication and decryption operations as needed for transfer of the data, as shown at 306. In a particular illustrative example, the transferred data is an application program that includes program instructions to be executed by the processor.

The method further includes setting a shield bit to thereby set the protected portion of the non-volatile memory to a shield mode where the key set is unreadable. The protected portion of the memory is set to the shielded mode after the data transfer has been completed but prior to execution of the transferred program code in the RAM by the processor.

The method further includes executing program data by the processor where such program data includes instructions that were transferred to the RAM, as shown at 310. During program code execution by the processor from the RAM, the processor device may be executing in a user mode and in such user mode the shielded portion of the non-volatile memory remains set to prevent unauthorized access to the key set. Thus, the illustrated method of activating the processor device provides for an initial secured transfer of program code from a non-volatile memory to random access memory useable by the processor device.

The above disclosed subject matter is to be considered illustrative, and not restrictive, and the appended claims are intended to cover all such modifications, enhancements, and other embodiments which fall within the true spirit and scope of the present invention. Thus, to the maximum extent allowed by law, the scope of the present invention is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.
WHAT IS CLAIMED IS:

1. A system comprising:
   
a processor;
   
a volatile memory accessible to the processor;
   
a first nonvolatile memory accessible to the processor, the first nonvolatile memory including a first portion of memory that is protected and is readable when a shield bit indicates an unshielded mode of operation, but is unreadable when the shield bit indicates a shielded mode of operation and a second portion of memory that is unprotected and that is readable regardless of the value of the shield bit; and
   
a second nonvolatile memory, the second nonvolatile memory including data to be transferred to the volatile memory.

2. The system of claim 1, wherein a key set is stored within the first portion, the key set to perform at least one of authentication and decryption of the data in the second nonvolatile memory upon transfer to the volatile memory.

3. The system of claim 1, wherein the data to be transferred is program code.

4. The system of claim 3, wherein the program code includes a plurality of authentication words.

5. The system of claim 3, wherein the shield bit is set after performing an operation to transfer the program code from the second nonvolatile memory to the volatile memory but before execution by the processor of the program code.

6. The system of claim 5, wherein the shield bit is set prior to execution of a first instruction of the program code.

7. The system of claim 1, further comprising external test interface protection logic, the external test interface protection logic responsive to an external test clock input, and wherein the shield bit is set after detection of a number of cycles of the external test clock input exceeds a threshold.

8. The system of claim 7 wherein the threshold is less than 40 clock cycles.

9. The system of claim 8, wherein the threshold is 20 clock cycles and wherein the external test clock input is a JTAG clock associated with a JTAG instruction.

10. The system of claim 2, wherein the key set is associated with a unique product manufacturer.

11. The system of claim 1, wherein the second portion of the first nonvolatile memory includes audio data.
12. The system of claim 2, wherein the key set includes an authentication key and a decryption key.

13. The system of claim 1, wherein the first nonvolatile memory is read only memory and the second nonvolatile memory is flash memory.

14. A memory device comprising:

- a first portion of memory that is protected and is readable when a shield bit indicates an unshielded mode of operation, but is unreadable when the shield bit indicates a shielded mode of operation; and
- a second portion of memory that is unprotected and that is readable regardless of the value of the shield bit.

15. The memory device of claim 14, further comprising a read multiplexer coupled to the first portion of memory, the multiplexer controlled at least in part in response to the shield bit.

16. The memory device of claim 15, wherein the multiplexer outputs a value from the first portion of memory during the unshielded mode of operation and wherein the multiplexer outputs a fixed output value indicating an error condition during the shielded mode of operation.

17. The memory device of claim 14, wherein the shield bit is stored in a write once memory device so that the shield bit is not user modifiable after a single write operation.

18. A method of activating a processor device having access to a read only memory, the method comprising:

- powering up the processor device, wherein the read only memory has a protected portion of memory that is shieldable but that is in an unshielded mode upon powerup;
- reading a key set from the protected portion of memory in connection with performing a data transfer to a random access memory (RAM); and
- after performing the data transfer, setting the protected portion of the memory to a shielded mode where the key set is no longer readable from the read only memory.

19. The method of claim 18, wherein after reading the key set, the key set is used to perform authentication and decryption with respect to the data transferred to the RAM.

20. The method of claim 18, wherein the data transferred to the RAM includes program instructions and further comprising executing the program instructions by the processor device.

21. The method of claim 18, wherein the protected portion further includes key set extraction data that is readable when the protected portion is in the unshielded mode.
22. The method of claim 18, wherein a shield bit associated with the protected portion of the memory is stored in a write once memory.
FIG. 1
FIG. 3

1. POWERING UP PROCESSOR

2. READING KEY SET FROM PROTECTED PORTION OF NON-VOLATILE MEMORY IN AN UNSHIELDED MODE OF OPERATION

3. TRANSFER DATA FROM SECOND NON-VOLATILE MEMORY (E.G. FLASH) TO RAM AND USE KEY SET TO PERFORM AUTHENTICATION AND DECRYPTION

4. SETTING SHIELD BIT TO SET THE PROTECTED PORTION OF THE MEMORY TO A SHIELDED MODE WHERE THE KEY SET IS UNREADABLE

5. EXECUTE PROGRAM DATA BY THE PROCESSOR WHERE THE PROGRAM DATA WAS TRANSFERRED TO THE RAM