SECURE TESTING OF SEMICONDUCTOR DEVICE

Abstraction

A method includes testing, by a processor, a secure portion of a semiconductor device through a first interface between the processor and the semiconductor device; and sending, by the processor, a pass or fail indication of a result of the testing of the secure portion of the semiconductor device to the tester through a second interface between the processor and the tester.
Figure 2
Encrypt image with encryption key

Deliver encrypted image to OEM

OEM writes encrypted image to embedded flash

Write encrypted image to flash

Deliver flash with encrypted image to OEM for embedding

Decrypt image in secure portion

Re-encrypt image in secure portion

Re-write encrypted image to flash

Figure 3
Figure 4
Figure 5
Couple semiconductor device to first interface of HSM

Couple tester to second interface of HSM

Test secure portion of semiconductor device with HSM using test key

Inject encryption keys into secure portion

Allow direct communication between semiconductor device and tester

Test non-secure portion by tester

Figure 6
SECURE TESTING OF SEMICONDUCTOR DEVICE

TECHNICAL FIELD

[0001] The technical field of the present disclosure relates to information security and, in particular, to secure testing of semiconductor devices.

BACKGROUND

[0002] Maintaining security in processors can be critical for various reasons. Such security may be desirable to maintain secrecy of certain aspects of proprietary code, prevent malicious code from interfering with processing and avoid unintended interaction with other processing code.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] For a more complete understanding of various examples, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0004] FIG. 1 is an example schematic representation of a manufacturing flow;

[0005] FIG. 2 is an example schematic representation of another manufacturing flow;

[0006] FIG. 3 is a flow chart illustrating an example delivery of secure processing code in the manufacturing flows of FIGS. 1 and 2;

[0007] FIG. 4 is an example schematic representation of a testing arrangement;

[0008] FIG. 5 is an example schematic representation of another testing arrangement; and

[0009] FIG. 6 is a flow chart of an example testing process.

DETAILED DESCRIPTION

[0010] In various embodiments, a semiconductor device, such as a chip or chipset, that may be used in various communication devices is provided. Semiconductor devices may include various components, such as circuitry, memory, etc. Some semiconductor devices may include an embedded flash memory which may be used to store various processing code, for example.

[0011] In various embodiments described herein, a semiconductor device, such as a chip or a chipset, may be manufactured without an embedded flash memory. Instead, an external flash memory may be coupled to the semiconductor device subsequent to fabrication and testing of the semiconductor device. In other examples, the embedded flash memory may be included in the semiconductor device prior to testing.

[0012] Referring now to FIG. 1, an example schematic representation of a manufacturing flow is illustrated. In the example of FIG. 1, a controlled or certified manufacturing flow arrangement 100 may be used to design, fabricate and test semiconductor devices. The flow arrangement 100 begins with the design of the physical circuitry, processing code and other components and/or functionality of a semiconductor device in a secure zone 110. The secure zone 110 may be a physical or virtual location with access limited to certain individuals and/or entities. From the secure zone 110, design information of a semiconductor device may be transmitted to a fabrication facility 140. In some embodiments, the design information may be transmitted via a stream of data in, for example, a graphic data system (GDS-II) format. The fabrication facility 140 may produce semiconductor devices that are then delivered to a testing facility 150. In various embodiments, the secure zone 110, fabrication facility 140 and the testing facility 150 may be remotely located to each other, or two or more facilities may be co-located.

[0013] Referring again to the secure zone 110, a secure processing code, also known as an image, may be generated and encrypted to produce encrypted processing code, or an encrypted image 130. The encrypted image 130 may include, for example, operating system patches for customization of the destination semiconductor device. In various embodiments, the encrypted image 130 may also include, without limitation, customized or pre-personalized applets or confidential customer data.

[0014] In encrypting the image, various encryption strategies may be used. For example, in one embodiment, the code is encrypted using the Triple Data Encryption Standard (3DES) algorithm. In one embodiment, in order to facilitate customization or pre-personalization of a destination device, an identifier associated with a device or a set of devices may be used in the encryption process. For example, a serial number or a set of serial numbers may be used as the identifier.

[0015] Referring now to the testing facility 150, as noted above, the fabricated semiconductor devices are delivered to testing facility 150 from the fabrication facility 140 for testing. Additionally, a hardware security module (HSM) 120 containing certain encryption keys may be delivered to the testing facility. In this regard, the HSM 120 may be a hardware component which includes encryption keys associated with the encrypted image 130. As described below, the encryption keys may be used for testing of a secure portion of a semiconductor device using the HSM.

[0016] The semiconductor devices are tested by operators at the testing facility 150 through one or more tests 152. Upon successful completion of the testing, the HSM places (e.g., writes, stores or injects) the encryption keys into the semiconductor device 154. As described below, the keys may be injected into a secure portion of the semiconductor device. The semiconductor devices, such as the semiconductor device 190, may then be delivered to an original equipment manufacturer (OEM) 160 for implementing, for example, into a communication device.

[0017] The encrypted image 130 is typically stored on a flash memory. As noted above, in various embodiments, the semiconductor device design may not include an embedded flash memory. Accordingly, in accordance with the illustrated example of FIG. 1, the encrypted image 130 is transmitted to the OEM 160 for storage in a memory device, such as an external flash memory 170.

[0018] The semiconductor device 190 fabricated using the manufacturing flow 100 to the OEM 160 includes a non-secure portion 192, also referred to herein as a peripheral processing system (PPS), and a secure portion 194, also referred to herein as a secure processing system (SPS). The secure portion 194 may include functionality associated with secure processing by the semiconductor device 190. For example, as illustrated in FIG. 1, the secure portion 194 may include the encryption keys injected into the semiconductor device 190 by the HSM 120.

[0019] As illustrated in FIG. 1, the encrypted image 130 received by the OEM 160 may be written to the flash memory 170 through the non-secure portion 192 of the semiconductor device 190 (arrow 182). The encrypted image 130 in the flash memory 170 may be verified by decrypting the encrypted...
image in the secure portion 194 of the semiconductor device 190 using the encryption keys injected into the secure portion 194 (arrow 184). In this regard, code may be provided in the secure portion 194 to perform the decryption using the encryption keys.

[0020] Thus, the semiconductor device 190 may be securely customized, or pre-personalized, in the secure zone. For example, the encrypted image 130 may be associated with a specific semiconductor device, and the encryption keys used to decrypt the encrypted image at the secure portion 194 of the semiconductor device 190 may also be accordingly associated with the specific semiconductor device. In one example, the encryption keys may be associated with, for example, a serial number of the target semiconductor device. Thus, the verification may ensure that the pre-personalization of the encrypted image 130 corresponds to the proper semiconductor device 190. The secure portion 194 may then re-encrypt the image for writing to the flash memory 170 (arrow 186). In this regard, the re-encryption by the secure portion 194 may be accomplished using encryption keys that may be generated by the secure portion 194 and that may be unique to each semiconductor device.

[0021] Since the encryption keys are generated by the secure portion 194 and may be unique to each semiconductor device, they may be unknown to any other entity and may thus be unbreakable. Therefore, the encrypted image 130 may be securely delivered to an external flash memory 170.

[0022] In other embodiments, as illustrated in FIG. 2, the encrypted image 130 may be written to a flash memory 170 during, for example, manufacture of the flash memory 170. In this regard, the encrypted image 130 may be delivered to a manufacturer of the flash memory 170 or to a post-manufacturing entity of the flash memory 170. The flash memory 170 with the encrypted image 130 may then be delivered to the OEM 160 for association with the semiconductor device 190 (e.g., installation on a user equipment having the semiconductor device 190). As with the example of FIG. 1, the secure portion 194 of the semiconductor device 190 may decrypt and verify the encrypted image 130 (arrow 184) and re-encrypt the decrypted image using encryption keys generated by the secure portion 194 for writing back onto the flash memory 170 (arrow 186).

[0023] Referring now to FIG. 3, a flow chart illustrates an example delivery of secure processing code in the manufacturing flows of FIGS. 1 and 2. The image may be encrypted with an encryption key (block 10) at, for example, a secure zone 110. As noted above, any of a variety of encryption techniques may be used to encrypt the image. In one embodiment, the encrypted image is delivered to an OEM (block 12), where the encrypted image may be written on a flash memory that is embedded in a user equipment having a semiconductor device associated with the encrypted image (block 14). As noted above, the flash memory may be external to a semiconductor device that is delivered to the OEM.

[0024] In another embodiment, the encrypted image is written to a flash memory (block 16) during, for example, manufacturing of the flash memory. The flash memory with the encrypted image may then be delivered to the OEM for coupling to a semiconductor device (block 18).

[0025] At the OEM, the encrypted image may be decrypted in a secure portion of the semiconductor device (block 20) by, for example, code provided in the secure portion to perform decryption using the encryption key. As noted above with reference to FIGS. 1 and 2, the semiconductor device may be provided with the encryption key used to decrypt the image for verification, for example. The secure portion of the semiconductor device may then re-encrypt the decrypted image (block 22) for re-writing the re-encrypted image to the flash memory (block 24). As noted above, the re-encryption of the decrypted image may be accomplished using any of a variety of encryption techniques. Further, the encryption keys used for the re-encryption may be generated by the secure portion of the semiconductor device to provide additional security. As noted above, since the encryption keys are generated by the secure portion and may be unique to each semiconductor device, the encryption keys may be unknown to any other entity and may thus be unbreakable.

[0026] Referring now to FIG. 4, an example schematic representation of a testing arrangement is illustrated. As described above with reference to FIGS. 1 and 2, the semiconductor devices may be delivered from the fabrication facility 140 to a testing facility 150. Such testing facilities may be used to test various devices, such as semiconductor devices. Further, such testing facilities may be used to test devices that may have secure and non-secure portions. Traditional testing may use a test key which may serve as an encryption key used during the testing. The test key may be embedded on the device, such as a semiconductor device, which may be referred to during testing as a device under test (DUT).

[0027] In various examples, sensitive information, such as test keys or encryption keys to be injected into a secure portion, may be provided in the HSM 120. In this regard, test keys may include encryption keys that are used specifically for testing of the DUT and may not be injected into the DUT for any other use. Additionally, other encryption keys that are injected into the secure portion may be used to decrypt and verify an encrypted image, as described above. In various examples, when a load board having one or more DUTs and one or more HSMs is removed from the tester 210, all sensitive information is securely removed from the tester 210.

[0028] Referring again to FIG. 4, the tester 210 is shown connected to a load board 220. The load board 220 may accommodate one or more DUTs, such as the semiconductor device 190. As noted above, the semiconductor device 190 includes a non-secure portion 192 and a secure portion 194. The load board 220 may further accommodate one or more HSMs, such as HSM 120. While FIG. 4 illustrates a load board 220 having a single semiconductor device 190 and a single HSM 120, various examples may include any desired number of semiconductor devices and any appropriate number of HSMs. The HSM 120 illustrated in FIG. 4 is provided with a first interface 124 for communication with the semiconductor device 190 and a second interface 126 for communication with the tester 210. The HSM 120 may also include a processor, such as a secure testing processor 122, configured to perform various functions such as, for example, perform testing of the secure portion 194 of the semiconductor device 190, as described below. Further, the secure testing processor 122 may also be configured to control operation of the HSM 120 and control communication with the semiconductor device 190 and/or the tester 210. The secure testing processor 122 may also be provided with a memory for storage, for example, of data such as encryption keys.

[0029] In various examples, the testing of the non-secure portion 192 may be performed by the tester 210, while testing of the secure portion 194 may be performed by the HSM 120 without providing access to the secure portion to the tester.
210. Thus, as illustrated in the example of FIG. 4, the HSM 120 may allow direct communication between the tester 210 and the non-secure portion 192 of the semiconductor device 190. In this regard, the tester 210 may send signals to and receive signals from the non-secure portion 192 of the semiconductor device 190, as illustrated by the line 224 in FIG. 4. As illustrated in FIG. 4, the direct communication between the non-secure portion 192 and the tester 210 may be performed through the HSM 120, through the interfaces 124, 126. In this regard, the HSM 120 may serve merely as a conduit for the communication between the non-secure portion 194 and the tester 210. In other examples, the communication between the non-secure portion 194 and the tester 210 may completely bypass the HSM 120.

[0030] For testing of the secure portion 194, the secure portion 194 may be isolated from the tester 210. As illustrated in the example of FIG. 4, the testing of the secure portion 194 may be performed by the secure testing processor 122 of the HSM 120. In this regard, the HSM 120 or the secure testing processor 122 may be provided with secure testing keys which may be delivered (e.g., injected or installed) into the secure portion 194 for purposes of testing. Any necessary testing of the secure portion 194 may be performed by the secure testing processor 122 of the HSM 120 with communication through the first interface 124, as illustrated by the line 222 in FIG. 4. The results of the testing of the secure portion 194 may be communicated to the tester 210 by the HSM 120 through the second interface 126 as, for example, a simple pass or fail indication. In one example, the result may be communicated as a 1-bit signal where a “0” is indicative of a pass and a “1” is indicative of a fail (or vice versa).

[0031] In one example, as illustrated in FIG. 5, the tester 210 may test the non-secure portion 192 by commanding the HSM 120 to position a relay 230 to allow direct communication between the tester 210 and the non-secure portion 192 of the semiconductor device 190. In response, the HSM 120 may position the relay 230 to a tester input/output position 234. When the tester 210 wishes the secure portion 194 to be tested, the tester 210 may command the HSM 120 to switch the relay 230 to an interface 232 between the HSM 120 and the semiconductor device 190. The HSM 120 may then establish a secure channel with the secure portion 194 using a test key. The secure portion 192 and the non-secure portion 194 may be tested in any order. For example, in some cases, the non-secure portion 194 may be tested first, while in other cases, the secure portion 192 may be tested first.

[0032] Thus, in accordance with the examples of FIGS. 4 and 5, the testing of the secure portion 194 may be performed under the control of the HSM 120. During or after successful testing of the secure portion 194, the HSM may inject the secure testing keys into the secure portion 194. The HSM 120 may communicate the results of the testing of the secure portion 194 to the tester 210 with a simple indication of “pass” or “fail”. As noted above, in some examples, the indication may be a 1-bit signal. Thus, the tester may be informed of the testing results without being given any information on the reasons for the results.

[0033] Upon completion of the testing, the load board is removed from the tester. Along with the load board, all secure information (e.g., the secure portion 194 of the semiconductor device 190 and the test keys for testing of the secure portion) are also removed. Thus, the tester 210 is never provided with access to any secure information. For example, the test keys and encryption keys provided in the HSM 120 are kept isolated from the tester 210.

[0034] Referring now to FIG. 6, a flowchart illustrating an example process for secure testing of semiconductor device is provided. As illustrated in FIG. 6, a semiconductor device may be coupled to an HSM through a first interface (block 610). For example, the semiconductor device 190 shown in FIGS. 4 and 5 may be coupled to the HSM 120 through the first interface 124.

[0035] Referring again to FIG. 6, a tester may be coupled to the HSM through a second interface (block 612). For example, as illustrated in FIGS. 4 and 5, the tester 210 may be coupled to the load board 220 and the HSM 120 through the second interface 126.

[0036] The secure portion of the semiconductor device may then be tested by the HSM using a test key which may have been provided with the HSM (block 614). For example, as noted above, in various examples, test keys and/or other secure information may be provided in the HSM 120. Thus, during the testing, all secure information is kept isolated from the tester. Further, as noted above, a simple “pass” or “fail” indication of the results of the testing of the secure portion may be communicated by the HSM 120 to the tester 210 through the second interface 126.

[0037] In various examples, the HSM may inject encryption keys into the secure portion (block 616). As noted above, the HSM may include secure information, such as encryption keys, that are injected into the secure portion. Again, this allows isolation of all secure information from the tester during testing. The encryption keys may be used to decrypt processing code, such as the encrypted image 130, as illustrated by the arrow 184 in FIGS. 1 and 2.

[0038] The HSM may position a relay switch, such as relay switch 230 of FIG. 5, to allow direct communication between the non-secure portion of the semiconductor device and the tester (block 618). As noted above, this allows the tester to test the non-secure portion of the semiconductor device (block 620). The positioning of the relay switch by the HSM may be in response to commands from the tester, for example. While FIG. 6 illustrates an example in which the secure portion is tested before the non-secure portion, those skilled in the art will appreciate that the order of testing may be reversed. For example, the non-secure portion may be tested and then the relay switch may be positioned to allow the processor of the HSM to test the secure portion. Thus, the secure portion of the semiconductor device may be tested and various keys (e.g., encryption keys) may be provided to the secure portion in a secure manner without the need for placing the tester in a secure location.

[0039] The various diagrams may depict an example architectural or other configuration for the various embodiments, which is done to aid in understanding the features and functionality that can be included in embodiments. The present disclosure is not restricted to the illustrated example architectures or configurations, and the desired features can be implemented using a variety of alternative architectures and configurations. Indeed, it will be apparent to one of skill in the arts how alternative functional, logical or physical partitioning and configurations can be implemented to implement various embodiments. Also, a multitude of different constituent module names other than those depicted herein can be applied to the various partitions. Additionally, with regard to flow diagrams, operational descriptions and method claims, the order in which the steps are presented herein shall not mandate that
various embodiments be implemented to perform the recited functionality in the same order unless the context dictates otherwise.

[0040] It should be understood that the various features, aspects and/or functionality described in one or more of the individual embodiments are not limited in their applicability to the particular embodiment with which they are described, but instead can be applied, alone or in various combinations, to one or more of the other embodiments, whether or not such embodiments are described and whether or not such features, aspects and/or functionality are presented as being a part of a described embodiment. Thus, the breadth and scope of the present disclosure should not be limited by any of the above-described exemplary embodiments.

[0041] Terms and phrases used in this document, and variations thereof, unless otherwise expressly stated, should be construed as open ended as opposed to limiting. As examples of the foregoing: the term “including” should be read as meaning “including, without limitation” or the like; the term “example” is used to provide exemplary instances of the item in discussion, not an exhaustive or limiting list thereof; the terms “a” or “an” should be read as meaning “at least one;” “one or more” or the like; and adjectives such as “conventional,” “traditional,” “normal,” “standard,” “known” and terms of similar meaning should not be construed as limiting the item described to a given time period or to an item available as of a given time, but instead should be read to encompass conventional, traditional, normal, or standard technologies that may be available or known now or at any time in the future. Likewise, where this document refers to technologies that would be apparent or known to one of ordinary skill in the art, such technologies encompass those apparent or known to the skilled artisan now or at any time in the future.

[0042] Additionally, the various embodiments set forth herein are described in terms of exemplary block diagrams, flow charts and other illustrations. As will become apparent to one of ordinary skill in the art after reading this document, the illustrated embodiments and their various alternatives can be implemented without confinement to the illustrated examples. For example, block diagrams and their accompanying description should not be construed as mandating a particular architecture or configuration.

[0043] Moreover, various embodiments described herein are described in the general context of method steps or processes, which may be implemented in one embodiment by a computer program product, embodied in, e.g., a non-transitory computer-readable memory, including computer-executable instructions, such as program code, executed by computer systems in networked environments. A computer-readable memory may include removable and non-removable storage devices including, but not limited to, Read Only Memory (ROM), Random Access Memory (RAM), compact discs (CDs), digital versatile discs (DVD), etc. Generally, program modules may include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Computer-executable instructions, associated data structures, and program modules represent examples of program code for executing steps of the methods disclosed herein. The particular sequence of such executable instructions or associated data structures represents examples of corresponding acts for implementing the functions described in such steps or processes.

[0044] As used herein, the term module can describe a given unit of functionality that can be performed in accordance with one or more embodiments. As used herein, a module might be implemented utilizing any form of hardware, software, or a combination thereof. For example, one or more processors, controllers, application-specific integrated circuits (ASICs), programmable logic arrays (PLAs), programmable array logic (PALs), complex programmable logic devices (CPLDs), field-programmable gate arrays (FPGAs), logical components, software routines or other mechanisms might be implemented to make up a module. In implementation, the various modules described herein might be implemented as discrete modules or the functions and features described can be shared in part or in total among one or more modules. In other words, as would be apparent to one of ordinary skill in the art after reading this description, the various features and functionality described herein may be implemented in any given application and can be implemented in one or more separate or shared modules in various combinations and permutations. Even though various features or elements of functionality may be individually described or claimed as separate modules, one of ordinary skill in the art will understand that these features and functionality can be shared among one or more common software and hardware elements, and such description shall not require or imply that separate hardware or software components are used to implement such features or functionality. Where components or modules of the invention are implemented in whole or in part using software, in one embodiment, these software elements can be implemented to operate with a computing or processing module capable of carrying out the functionality described with respect thereto. The presence of broadening words and phrases such as “one or more,” “at least,” “but not limited to” or other like phrases in some instances shall not be read to mean that the narrower case is intended or required in instances where such broadening phrases may be absent.

What is claimed is:

1. An apparatus, comprising:
a first interface configured to communicate with a semiconductor device;
a second interface configured to communicate with a tester; and
a processor configured to test a secure portion of the semiconductor device,
wherein the processor is configured to send a result of testing of the secure portion of the semiconductor device to the tester through the second interface.

2. The apparatus of claim 1, wherein the processor is configured to provide an encryption key into the secure portion, the encryption key being associated with a processing code.

3. The apparatus of claim 1, wherein the processor is configured to isolate the tester from the secure portion of the semiconductor device.

4. The apparatus of claim 1, wherein the processor includes a test key configured to facilitate testing of the secure portion.

5. The apparatus of claim 1, further comprising:
a relay switch configured to selectively allow communication between the tester and a non-secure portion of the semiconductor device.

6. The apparatus of claim 5, wherein the relay switch is configured to selectively allow the tester to test the non-secure portion of the semiconductor device.
7. The apparatus of claim 5, wherein the processor is configured to receive instructions from the tester to operate the relay switch.

8. The apparatus of claim 5, wherein the relay switch is configured to isolate the tester from the secure portion of the semiconductor device.

9. The apparatus of claim 5, wherein the communication between the tester and the non-secure portion of the semiconductor device passes through the first interface and the second interface.

10. A method, comprising:
    testing, by a processor, a secure portion of a semiconductor device through a first interface between the processor and the semiconductor device; and
    sending, by the processor, a pass or fail indication of a result of the testing of the secure portion of the semiconductor device to the tester through a second interface between the processor and the tester.

11. The method of claim 10, further comprising:
    providing, by the processor, an encryption key into the secure portion, the encryption key being associated with a processing code.

12. The method of claim 10, further comprising isolating the tester from the secure portion of the semiconductor device.

13. The method of claim 10, wherein the testing the secure portion comprises using a test key by the processor to facilitate testing the secure portion.

14. The method of claim 10, further comprising:
    operating a relay switch to allow communication between the tester and a non-secure portion of the semiconductor device.

15. The method of claim 14, wherein operating the relay switch is responsive to receiving, by the processor, instructions from the tester to operate the relay switch.

16. A computer program product, embodied on a non-transitory computer-readable medium, comprising:
    computer code for testing a secure portion of a device by a processor, and
    computer code for sending results of the testing from the processor to a tester, wherein the results include an indication of pass or fail, and wherein the tester is isolated from the secure portion of the device.

17. The computer program product of claim 16, further comprising:
    computer code for allowing communication between the tester and a non-secure portion of the device.

18. The computer program product of claim 17, wherein the computer code for allowing communication between the tester and the non-secure portion of the device comprises:
    computer code for operating a relay switch.

19. The computer program product of claim 18, further comprising:
    computer code for receiving instructions from the tester to operate the relay switch.

20. The computer program product of claim 16, wherein the computer code for testing the secure portion comprises:
    computer code for using a test key to facilitate testing the secure portion.

* * * * *

* * * * *