(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 August 2009 (20.08.2009)

PCT

(10) International Publication Number
WO 2009/101483 A1

(51) International Patent Classification:
G06F 12/14 (2006.01) *G11C 21/00* (2006.01)
G11C 7/24 (2006.01) *G11C 16/22* (2006.01)

(21) International Application Number:
PCT/IB2008/050560

(22) International Filing Date:
15 February 2008 (15.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **FREESCALE SEMICONDUCTOR, INC.** [US/US]; 6501 William Cannon Drive West, Austin, Texas 78735 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ROZEN, Anton** [IL/IL]; Tzivoni 62, 70700 Gedera (IL). **ASHKENAZI, Asaf** [IL/US]; 9241 La Siesta Bend, Austin, Texas 78749 (US). **KUZMIN, Dan** [IL/IL]; Rahavat ILAN 18/32, 54056 Givat Shmuel (IL). **PRIEL, Michael** [IL/IL]; Shmuel Hanagid 18/15, 46498 Hertzelia (IL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) **Title**: SEMICONDUCTOR DEVICE AND METHOD FOR STORING DATA

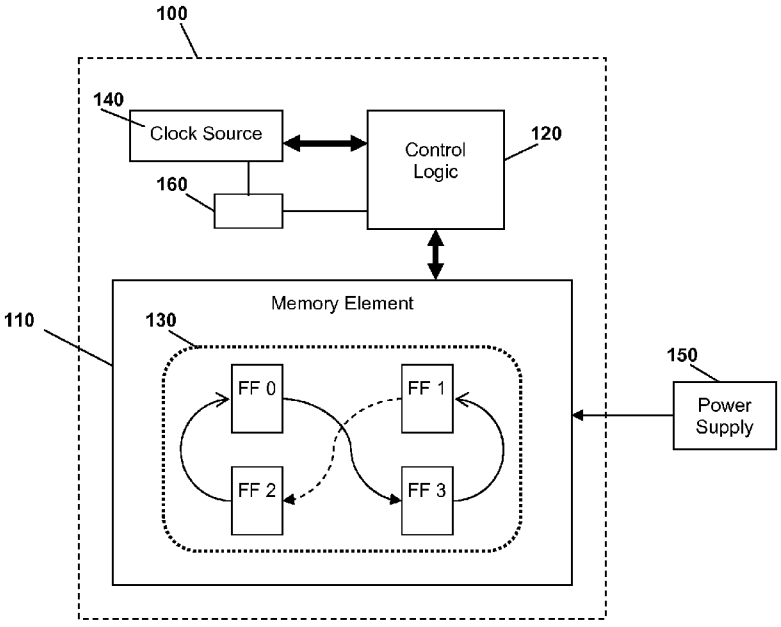

FIG. 1

(57) **Abstract**: A semiconductor device (100) comprises at least one memory element (1 10) for storing data, and control logic (120) arranged to control the storage of the data in the at least one memory element (110). The at least one memory element (110) comprises a plurality of memory locations (130) for storing the data. The control logic (120) is arranged to routinely relocate the data from one memory location (130) to another memory location (130). In this manner, the semiconductor device may be protected from infrared security key data tampering.

WO 2009/101483 A1

Published:

— *with international search report (Art. 21(3))*

TITLE: SEMICONDUCTOR DEVICE AND METHOD FOR STORING DATA

Field of the Invention

The invention relates to a method and apparatus for storing data, and more particularly to a method and apparatus for securely storing data, such as security key data.

Background of the Invention

In the field of modern cryptography, it is known to use a security key to control an operation and/or access to secured application execution, such as used within Point of Sale terminals and Digital Rights Management (DRM). By way of example, in an encryption operation, a key may specify a particular transformation of 'plaintext' into 'ciphertext', or vice versa during a decryption operation.

It is often difficult to keep the details of a security system, and in particular its algorithms, secret. Thus, the security of an encryption system, in most cases, relies on some security key being kept secret. Consequently, the ability to maintain the secrecy of a security key is therefore of great importance within any security system. Accordingly, significant steps have been taken to ensure the secrecy of security keys stored within memory elements of devices.

One well known technique for maintaining the secrecy of a security key stored in memory is for the security key to be stored in volatile memory, which requires power to maintain the stored information. In this manner, if the power supply to the memory is interrupted, for example caused by physical tampering of the memory element's semiconductor device packaging, the security key information is lost. As a result, an un-authorised person attempting to discover the security key information, by way of physical tampering of the memory element, is substantially thwarted.

A problem with existing key-guarding solutions such as this is that, with the development of infra-red (IR) tools and the like, it has become possible to determine transistor states within semiconductor device packages, without a need for physical tampering. IR radiation (photon emission) can strongly indicate the transistor state within a semiconductor device. By locating the IR source, and associating its location with a specific transistor, the information held by, for example, a flip-flop within a memory element may be determined. As a consequence, by identifying memory locations storing security key information, security key information may be determined without a need for physical tampering of the memory element.

This problem is often further compounded since security key information is often stored within dedicated semiconductor devices, which are typically small in size. As a result, identifying the location of transistors storing security key information, and determining their state is particularly achievable with available IR tools.

Summary of the Invention

In accordance with aspects of the invention, there is provided a semiconductor device and a method for storing data in memory as defined in the appended Claims.

Specific embodiments of the invention are set forth in the dependent claims.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter.

Brief Description of the Drawings

Further details, aspects and embodiments of the invention will be described, by way of example only, with reference to the drawings.

FIG. 1 illustrates an example of a semiconductor device according to some embodiments of the invention.

FIG. 2 illustrates an example of a method for storing data in memory according to some embodiments of the invention.

FIG. 3 illustrates an example of a semiconductor device according to an alternative embodiment of the invention.

Description of Embodiments

Embodiments of the invention will be described in terms of storing security key data. Although embodiments of the invention will be described in terms of security key data, it will be appreciated that the memory arrangement herein described may be embodied in any apparatus that incorporates data storage, and in particular secure data storage.

Embodiments of the invention propose a method and apparatus for storing data in memory. The memory comprises a plurality of memory locations for storing the data; such that the data may be routinely relocated from one memory location to another memory location.

For clarity purposes only, the hereinafter 'routine' relocation of data, is envisaged as encompassing a periodic or intermittent relocation of data based on some rule or algorithm, and in particular to provide protection against unauthorized reading of data form memory. Furthermore, for clarity purposes only, it is envisaged that data relocation can be not only from flipflop (FF) to FF, but also within standard memory devices that include memory cells.

Referring now to FIG. 1, there is illustrated an example of a semiconductor device 100 according to an example of an embodiment of the invention. The semiconductor device 100 may comprise memory element 110 and may comprise control logic 120 arranged to control storage of the data in the memory element 110. The memory element 110 may comprise a plurality of memory locations 130. The control logic 120 may be arranged to routinely relocate the data from one memory location 130 to another memory location 130.

In accordance with an example of an embodiment of the invention, the data to be stored may comprise security key data, the secrecy of which is required to be maintained.

As previously mentioned, a problem with prior art key-guarding techniques is that, with the development of infra-red (IR) tools and the like, it has become possible to determine transistor states within semiconductor device packages, without the need for physical tampering. By locating the IR source, and associating its location with a specific transistor, the information held by, for example, a flip-flop within a memory element may be determined. As a consequence, by identifying memory locations storing security key data, security key data may be determined without the need for physical tampering of the memory element.

However, for the semiconductor device 100 of the FIG. 1, the routine relocation of data from one memory location to another memory location means that the ability to identify memory locations storing security key data may be substantially reduced, significantly impeding any attempt to determine security key data. In this manner, protection may be provided against infrared (IR) data detection techniques, since IR data revealing requires some time to accumulate IR-emission information from a silicon device. Moving security key data bits from location to location at a rate faster than that which will allow IR-emission information to be accumulated substantially thwarts such attempts to determine security key data.

In accordance with an example of an embodiment of the invention, the memory element 110 comprises volatile memory. In this manner, if a power supply 150 to the memory element 110 is interrupted, for example caused by physical tampering of the semiconductor device 100, the data may be lost. As a result, an un-authorised person attempting to discover the data by way of physical tampering of the memory element 110 is substantially thwarted.

The memory element 110 may comprise a plurality of flip-flop bistable multivibrators, where each flip-flop may be arranged to store one bit of data. In this manner, in a case where a 128 bit security key is stored in the memory element 110, the security key may be stored using 128 flip-flops.

In one example of an embodiment of the invention, the control logic 120 may comprise a state-machine, for example implemented using CMOS logic. Such a state-machine may be clock-controlled. As previously mentioned, the control logic 120 is arranged to control the storage of the data in the memory element 110, and to routinely relocate the data from one memory location to another memory location. For the illustrated embodiment, the control logic 120 may be operably coupled to a Clock Source/Clock Generator 140 located within the semiconductor device 100, and may be arranged to periodically relocate the data from one memory location 130 to another memory location 130 based on say a clock signal received from the Clock Source/Clock Generator 140. For example, the control logic 120 may be arranged to relocate the data at a rate of several KHz.

The semiconductor device 100 may further comprise clock monitoring circuitry 160, operably coupled to the Clock Source/Clock Generator 140, which may be arranged to detect tampering of the Clock Source/Clock Generator 140. For example, the clock monitoring circuitry 160 may comprise an independent internal ring-oscillator.

For the illustrated embodiment, the clock monitoring circuitry 160 is operably coupled to the control logic 120, and arranged to provide an indication to the control logic 120 when tampering of the Clock Source/Clock Generator 140 has been detected. In this manner, the control logic 120 may be further arranged, upon detection of any tampering of the Clock Source/Clock Generator 140, to cause the data to be erased from the memory element 110.

For example, in a case where the memory element 110 comprises volatile memory, the control logic 120 may cause the power supply 150 to the memory element 110 to be interrupted. Alternatively, the control logic 120 may cause all flip-flops of the memory element 110 to be set to the same value, either '1' or '0'. In this manner, if an unauthorised person attempts to halt, or slow down the relocation of the data by tampering with the Clock Source/Clock Generator 140, such tampering may be detected by the clock monitoring circuitry 160, and the data subsequently erased.

In accordance with one example of an embodiment of the invention, the control logic 120 may be arranged to associate the plurality of memory locations 130 within a chain, and to relocate the data from one memory location 130 to another memory location 130 by shifting the data to the next memory location 130 in the chain.

For example, for the embodiment illustrated in FIG. 1, four memory locations 130 are illustrated, and designated FF0 to FF3, and have been associated within a looped chain of FF0, FF3, FF1, FF2, FF0, FF3, etc. In the case where the data is stored in memory location FF0, when the control logic is required to relocate the data, the control logic 120 identifies the next memory location within the chain, which for the illustrated embodiment would be FF3, and relocates the data by shifting it along the chain. As a result, for the illustrated embodiment, the data would be relocated to memory location FF3.

In an alternative example of an embodiment of the invention, the control logic 120 may be arranged to relocate the data based on a more complex location algorithm. For example, such a location algorithm may determine in which direction data is to be shifted along the chain. In this manner, the direction in which the data is shifted may be varied, for example substantially randomly, making the location of the data within the memory element 110 more difficult to predict.

Alternatively, memory locations 130 may be associated in a more complex arrangement than a linear chain. For example, in a case where each memory location 130 comprises a flip-flop, the output of each flip-flop may be connectable to the input of each other flip-flop. Here, the control logic 120 may be arranged to control to which input the output of each flip-flop is connected during relocation of the data.

In this manner, the control logic 120 may relocate data according to any form of suitable relocation algorithm. In particular, substantially non-repeating location patterns for data storage may be implemented, providing improved protection against dynamic IR data detection. As will be appreciated by a skilled artisan, the control logic 120 retains information relating to the location(s) of the data bits, in order for the data to be retrieved when required, and to enable the control logic 120 to relocate the data.

In accordance with one example of an embodiment of the invention, data to be stored may comprise a plurality of data bits. For example, in the case of a 128-bit security key, the data comprises 128 bits. Accordingly, each memory location 130 within the memory element 110 may be capable of storing a plurality of data bits, for example all 128 bits of data in the case of a 128-bit security key, and the control logic 120 may be arranged to relocate all 128 bits of data from one memory location 130 to another memory location 130.

Alternatively, in accordance with an alternative example of an embodiment of the invention, data to be stored in the memory element 110 may be divided up and stored within multiple memory locations 130. For example, in the case of a 128-bit security key, the data may be divided into four blocks of 32 bits, each 32-bit block being stored within a memory location 130. In this manner, the control logic 120 may be arranged to relocate all four 32-bit blocks synchronously from their current memory locations 130 to new memory locations. For example, in the case where the control logic 120 associates the memory locations 130 within a chain, the control logic 120 may relocate all four of the 32-bit blocks of data by synchronously shifting each block to the next respective memory location 130 in the chain. Alternatively, the control logic 120 may relocate blocks of data individually, and at different times.

In a yet further alternative example of an embodiment of the invention, each memory location 130 may comprise a single flip-flop component for storing a single bit of data. In this manner, the control logic 120 may be arranged to relocate individual bits of data.

For the illustrated embodiment, the memory locations 130 are provided within a single memory element 110. However, as will be appreciated by a skilled artisan, the memory locations 130 may be provided within a plurality of memory elements without detracting from the memory arrangement described herein.

Referring now to FIG. 2, there is illustrated an example of a method 200 for storing data in memory in accordance with an example of an embodiment of the invention. The memory may comprise a plurality of memory locations for storing the data. The method may comprise routinely relocating the data from one memory location to another memory location.

The method 200 starts at step 210 with the receipt of a clock signal. Next, in step 220, it is determined whether any tampering of the source of the clock signal has been detected. If it is determined that tampering of the source of the clock signal has been detected, the method moves to step 230 and the data is erased, and the method ends.

However, if it is determined that tampering of the source of the clock signal has not been detected, the method moves on to step 240.

In step 240, it is determined whether the data is to be relocated. For example, the data may be relocated on a periodic basis, whereby the period is defined by a specific number of clock cycles.

For the illustrated embodiment, it is determined whether the data is to be relocated based on a counter, which indicates a number of times that a clock signal has been received, and thereby the number of clock cycles that have occurred. If the counter value is less than a predetermined value, sufficient clock cycles have not occurred, and therefore it is determined that the data is not to be relocated.

Accordingly, the method moves to step 250, where the counter is incremented, and the method continues. However, if the counter value is equal to the predetermined value, in step 240, sufficient clock cycles have occurred, and therefore it is determined that the data is to be relocated. Accordingly, the method moves to step 260.

In step 260, the (or each) new memory location to which the data is to be relocated is determined. For example, a plurality of memory locations may be associated within a chain, and relocating the data may comprise shifting data to the next respective memory location in the chain.

Accordingly, step 260 may comprise identifying the next memory location in the chain. Alternatively, a more complex location algorithm may be used to determine the new memory location. Next, in step 270, the data is relocated. Finally, in step 280, the counter is reset, and the method ends, for this particular cycle.

Referring now to FIG. 3, there is illustrated an example of a semiconductor device 300 according to an alternative example of an embodiment of the invention. The semiconductor device 300 may comprise memory element 310 and may comprise control logic 320, which may be arranged to control storage of data in the memory element 310. The memory element 310 may comprise a plurality of memory locations 330, such that the control logic 320 may be arranged to routinely relocate the data from one memory location 130 to another memory location 330.

The control logic 320 may be operably coupled to a Clock Source/Clock Generator 340 located within the semiconductor device 300, and may be arranged to periodically relocate the data from one memory location 330 to another memory location 330 based on, say, a 32KHz clock signal received from the Clock Source/Clock Generator 340. It is envisaged in one example of an embodiment of the invention that the Clock Source/Clock Generator 340 may also comprise clock monitor logic. The semiconductor device 300 may further comprise clock monitoring circuitry 360, operably coupled to the Clock Source/Clock Generator 340, and arranged to detect tampering of the Clock Source/Clock Generator 340.

In accordance with the example of the alternative embodiment illustrated in FIG. 3, the memory element 310 may comprise a plurality of dummy memory locations 335 for storing dummy data, and the control logic 320 may be further arranged to routinely relocate the dummy data from one dummy memory location 335 to another dummy memory location 335. In this manner, the relocation of dummy data acts as a disruption to attempts to discover the actual data stored in memory locations 130, thereby providing additional data protection. Dummy memory locations 335 may be geometrically located between (real) data memory locations 330, to further obfuscate the stored data.

In accordance with a yet further example of an embodiment of the invention, in order to further restrict a potential attacker from identifying sufficient key material information, for example based on periodical measurements of specific FFs, additional randomiser logic 135 is incorporated and operably coupled to control logic 320. The randomiser logic 135 may be arranged to randomize an initial state / location of the key (where the first state in the state machine is unknown, and/or randomize each state machine key location transition (for example, suppress transition according to a random bit). In this manner, uncertainty and/or randomness is added to the key location.

It will be understood that the method and apparatus for storing data, as described above, aim to provide at least the advantage of improved protection against IR data detection techniques.

The invention may also be implemented in a computer program for running on a computer system, at least including code portions for performing steps of a method according to the invention when run on a programmable apparatus, such as a computer system or enabling a programmable apparatus to perform functions of a device or system according to the invention. The term “program,” as used herein, is defined as a sequence of instructions designed for execution on a computer system. A program, or computer program, may include a subroutine, a function, a procedure, an object method, an object implementation, an executable application, an applet, a servlet, a source code, an object code, a shared library/dynamic load library and/or other sequence of instructions designed for execution on a computer system. The computer program may be provided on a data carrier, such as a CD-rom or diskette, stored with data loadable in a memory of a computer system, the data representing the computer program. The data carrier may include, for example and without limitation, any number of the following: magnetic storage media including disk and tape storage media; optical storage media such as compact disk media (e.g., CD ROM, CD R, etc.) and digital video disk storage media; nonvolatile memory storage media including semiconductor-based memory units such as FLASH memory, EEPROM, EPROM, ROM; ferromagnetic digital memories; MRAM; volatile storage media including registers, buffers or caches, main memory, RAM, etc.; and data transmission media including computer networks, point-to-point telecommunication equipment, and carrier wave transmission media, just to

name a few. Such computer readable media may be permanently, removably or remotely coupled to an information processing system.

It will be appreciated by a skilled artisan that the invention is independent from any particular memory type used, and the usage of specific memory types in the described embodiments are only for illustrative purposes.

In particular, it is envisaged that the aforementioned memory system can be applied by a semiconductor manufacturer to any semiconductor device architecture supporting an improved method and apparatus for storing data. It is further envisaged that, for example, a semiconductor manufacturer may employ the aforementioned design in a stand-alone device, or application-specific semiconductor device (ASIC) and/or any other sub-system element employing an integrated circuit to support an improved method and apparatus for storing data.

It will be appreciated that any suitable distribution of functionality between different functional units or controllers or logic or memory elements, may be used without detracting from the embodiments herein described. Hence, references to specific functional devices or elements are only to be seen as references to suitable means for providing the described functionality, rather than indicative of a strict logical or physical structure or organization.

Aspects of the invention may be implemented in any suitable form including hardware, software, firmware or any combination of these. The elements and components of an example of an embodiment of the invention may be physically, functionally and logically implemented in any suitable way. Indeed, the functionality may be implemented in a single unit or integrated circuit (IC), in a plurality of units or ICs or as part of other functional units.

Although embodiments of the invention have been described in connection with the topologies in the figures, it is not intended to be limited to the specific form set forth herein. Rather, the scope of the invention is limited only by the accompanying claims. Additionally, although a feature may appear to be described in connection with particular embodiments, one skilled in the art would recognize that various features of the described embodiments may be combined in accordance with the invention. In the claims, the term ‘comprising’ does not exclude the presence of other elements or steps.

Furthermore, although individual features may be included in different claims, these may possibly be advantageously combined, and the inclusion in different claims does not imply that a combination of features is not feasible and/or advantageous. Also, the inclusion of a feature in one category of claims does not imply a limitation to this category, but rather indicates that the feature is equally applicable to other claim categories, as appropriate.

Furthermore, the order of features in the claims does not imply any specific order in which the features must be performed and in particular the order of individual steps in a method claim does not imply that the steps must be performed in this order. Rather, the steps may be performed in any suitable order. In addition, singular references do not exclude a plurality. Thus, references to ‘a’, ‘an’, ‘first’, ‘second’ etc. do not preclude a plurality.

Claims

1. A semiconductor device (100) comprising at least one memory element (110) for storing data, and control logic (120) arranged to control a storage of data in the at least one memory element (110); the at least one memory element (110) comprising a plurality of memory locations (130) for storing the data and which control logic (120) is arranged to routinely relocate the data from one memory location (130) to another memory location (130).

2. The semiconductor device (100) of Claim 1 wherein the data comprises security key data.

3. The semiconductor device (100) of Claim 1 or Claim 2 wherein the at least one memory element (110) comprises volatile memory.

4. The semiconductor device (100) of any preceding Claim wherein the memory element (110) comprises at least one flip-flop bistable multivibrator.

5. The semiconductor device (100) of any preceding Claim wherein the control logic (120) is arranged to associate the plurality of memory locations (130) within a chain, and to relocate the data from one memory location (130) to another memory location (130) by shifting the data to a subsequent memory location (130) in the chain.

6. The semiconductor device (100) of any preceding Claim wherein the control logic (120) is arranged to relocate the data from one memory location to another memory location (130) based on a location algorithm.

7. The semiconductor device (100) of any preceding Claim wherein the control logic (120) is operably coupled to a Clock Source (140), and is arranged to periodically relocate the data from one memory location (130) to another memory location (130) based on a clock signal received from the Clock Source (140).

8. The semiconductor device (100) of Claim 7 wherein the semiconductor device (100) comprises clock monitoring circuitry (160), operably coupled to the Clock Source (140), and arranged to detect tampering of the Clock Source (140).

9. The semiconductor device (100) of Claim 8 wherein the clock monitoring circuitry (160) is operably coupled to the control logic (120) such that the control logic (120), upon

detection of tampering of the Clock Source (140) by the clock monitoring circuitry (160), causes the data to be erased from the at least one memory element (110).

10. The semiconductor device (100) of any preceding Claim wherein the at least one memory element (110) further comprises a plurality of dummy memory locations (370) for storing dummy data.

11. The semiconductor device (100) of Claim 10 wherein the control logic (120) is further arranged to routinely relocate the dummy data from one dummy memory location (380) to another dummy memory location (380).

12. The semiconductor device (100) of any preceding Claim wherein the control logic (120) is operably coupled to randomiser logic (335) arranged to randomise a routine relocation of the data.

13. The semiconductor device (100) of any preceding wherein the control logic comprises a state machine.

14. A method (200) for storing data in memory, the memory comprising a plurality of memory locations for storing the data;

wherein the method comprises routinely relocating the data (270) from one memory location to another memory location.

15. A computer program product loadable in a memory of a programmable apparatus, which computer program product includes program code portions for executing one or more steps of the method claimed in claim 14 when run by said programmable apparatus.

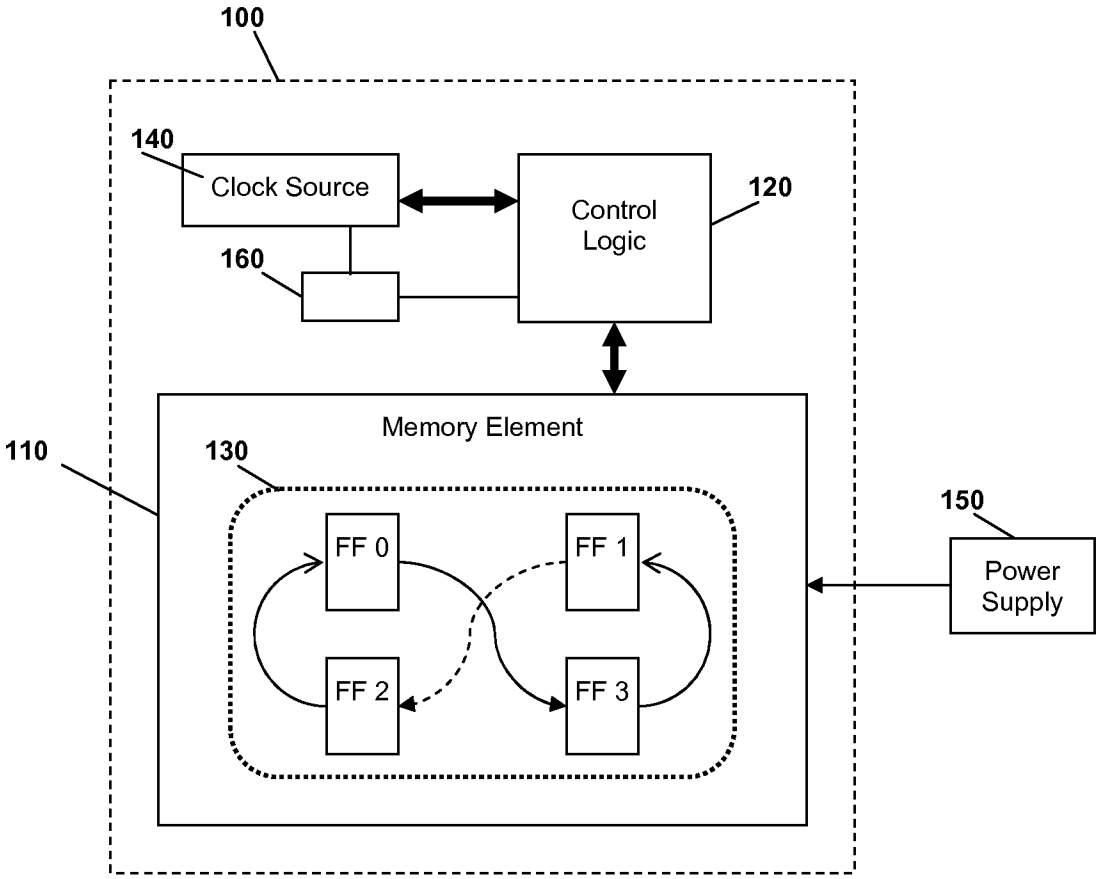
100
140
Clock Source
120
Control Logic
160
Memory Element
110
130
FF 0
FF 1
FF 2
FF 3
150
Power Supply

FIG. 1

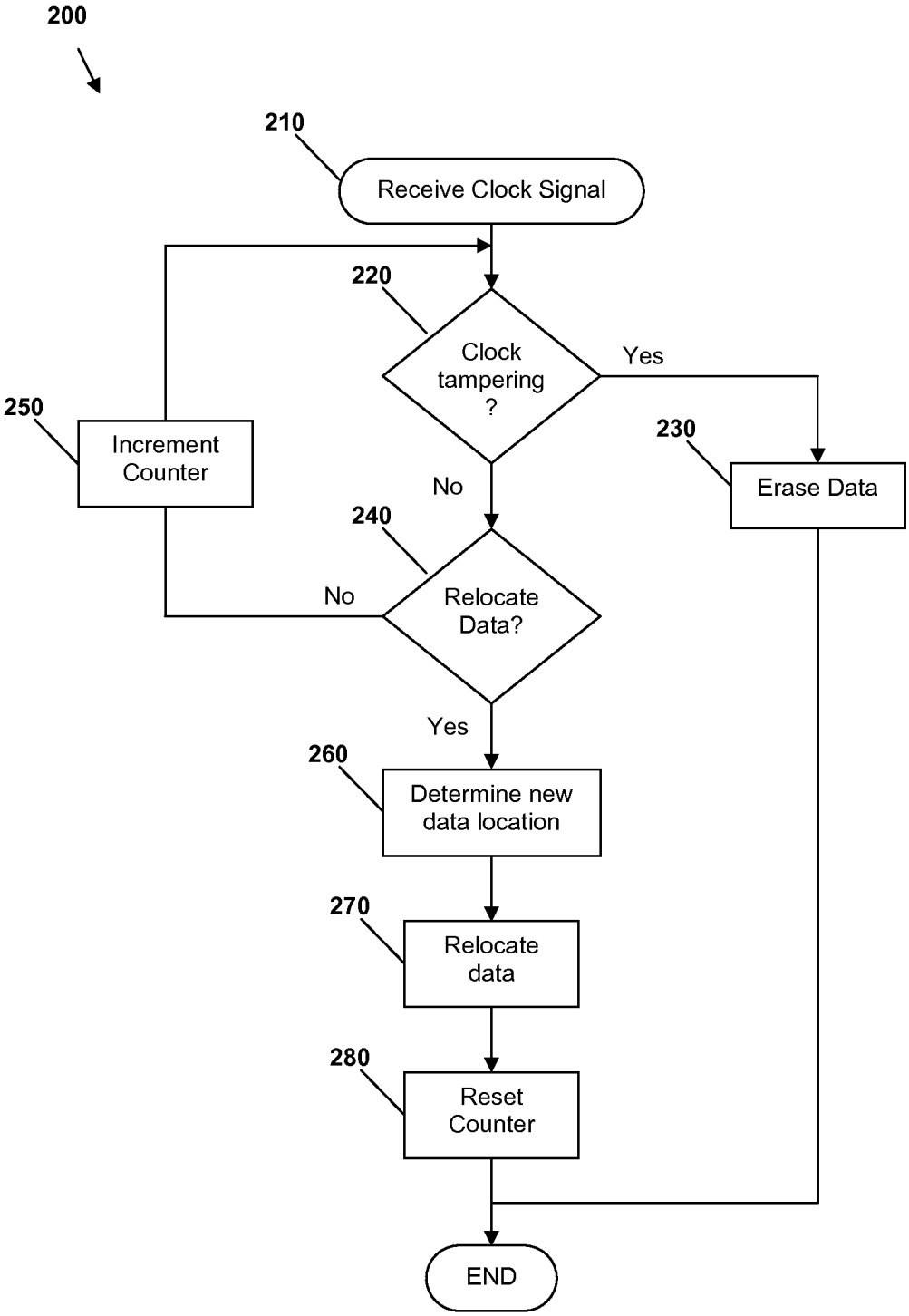
200
210
Receive Clock Signal
220
Clock tampering ?
Yes
230
Erase Data
No
250
Increment Counter
240
Relocate Data?
No
Yes
260
Determine new data location
270
Relocate data
280
Reset Counter
END

FIG. 2

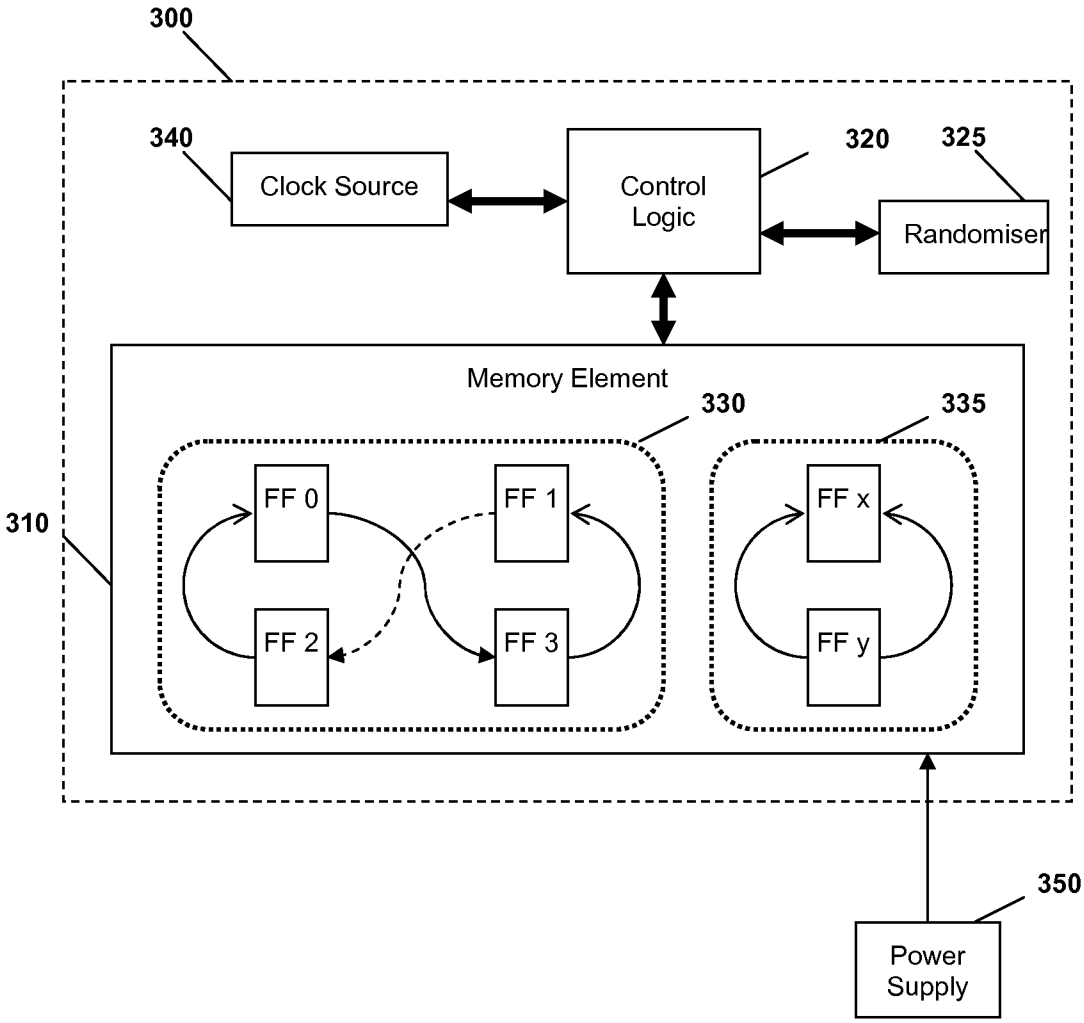
300
340
Clock Source
Control Logic
320
325
Randomiser
Memory Element
330
335
310
FF 0
FF 1
FF 2
FF 3
FF x
FF y
350
Power Supply

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2008/050560

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F12/14 G11C7/24 G11C21/00 G11C16/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F G06K G11C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7 003 673 B1 (DIENER SEBASTIEN [FR] ET AL) 21 February 2006 (2006-02-21) the whole document	1-9, 12-15
Y		10,11
Y	US 6 792 528 B1 (HOU CHIEN-TZU [US]) 14 September 2004 (2004-09-14) abstract; figure 7	10,11
X	EP 0 908 810 B (GEN INSTRUMENT CORP [US]) 1 March 2006 (2006-03-01) paragraphs [0057] - [0059], [0118] - [0126], [0174], [0175], [0199]	1,3,4, 10-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 June 2008	24/07/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Trifonov, Antoniy

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2008/050560

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7003673 B1	21-02-2006	AT 265708 T	15-05-2004
		DE 69916795 D1	03-06-2004
		DE 69916795 T2	31-03-2005
		EP 1055174 A1	29-11-2000
		FR 2787216 A1	16-06-2000
		WO 0036511 A1	22-06-2000
US 6792528 B1	14-09-2004	DE 10103804 A1	22-11-2001
		FR 2809201 A1	23-11-2001
		GB 2367657 A	10-04-2002
EP 0908810 B	01-03-2006	CA 2249554 A1	10-04-1999
		CN 1236132 A	24-11-1999
		DE 69833594 T2	28-12-2006
		EP 0908810 A2	14-04-1999
		IL 126448 A	14-08-2002
		TW 445402 B	11-07-2001
		US 6061449 A	09-05-2000