US 20250258936A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2025/0258936 A1**

SEOK et al. (43) **Pub. Date: Aug. 14, 2025**

(54) **ELECTRONIC CIRCUIT FOR ENCRYPTING MEMORY DEVICE AND ENCRYPTION METHOD USING THE SAME**

(71) Applicant: **Samsung Electronics Co., Ltd.**, Suwon-si, Gyeonggi-do (KR)

(72) Inventors: **Jaehyup SEOK**, Suwon-si (KR); **Jonghyun PARK**, Suwon-si (KR); **Ingoo HEO**, Suwon-si (KR)

(73) Assignee: **Samsung Electronics Co., Ltd.**, Suwon-si, Gyeonggi-do (KR)

(21) Appl. No.: **18/999,082**

(22) Filed: **Dec. 23, 2024**

(30) **Foreign Application Priority Data**

Feb. 13, 2024 (KR) 10-2024-0020468

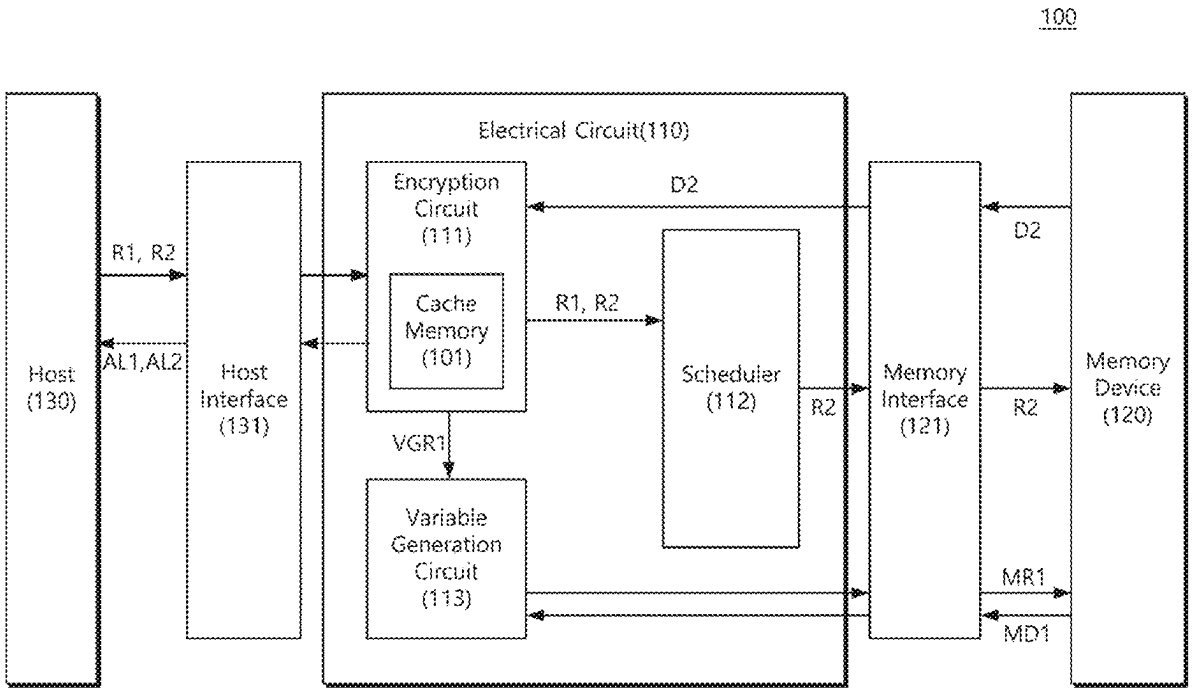
Publication Classification

(51) **Int. Cl.**
G06F 21/60 (2013.01)
H04L 9/08 (2006.01)

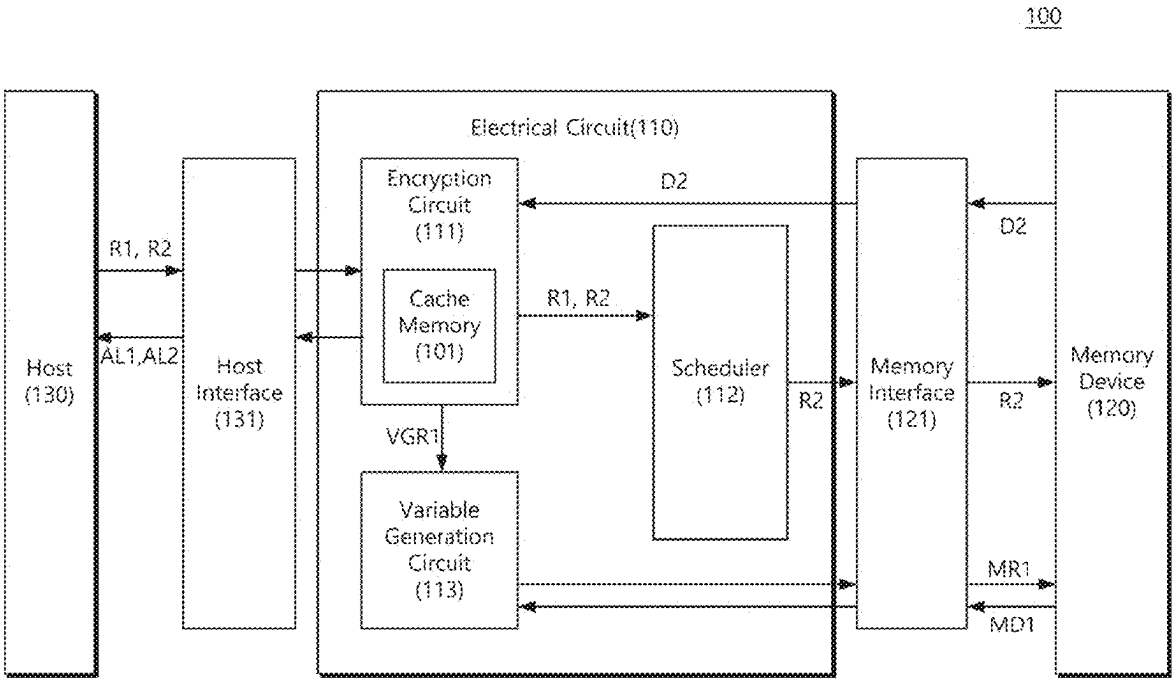
(52) **U.S. Cl.**
CPC ***G06F 21/602*** (2013.01); ***H04L 9/0869*** (2013.01)

(57) **ABSTRACT**

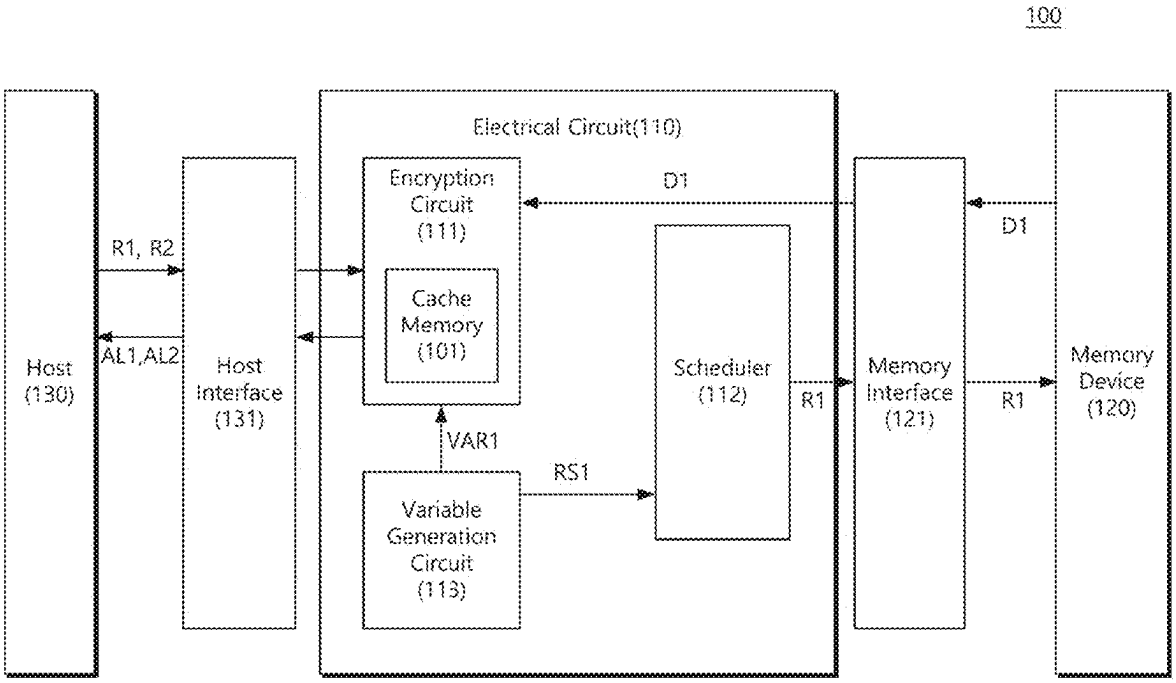
The electronic circuit includes an encryption circuit that includes a cache memory storing an encryption variable and receives a first encryption request for first data stored in a first area and a second encryption request for second data stored in a second area, a scheduler that transmits the second encryption request to the memory device when a first encryption variable for the first area is not stored in the cache memory and a second encryption variable for the second area is stored in the cache memory, and a variable generation circuit that generates the first encryption variable while the encryption circuit encrypts the second data received from the memory device based on the second encryption variable based on and/or in response to the second encryption request, and the scheduler transmits the first encryption request to the memory device in response to a determination that the first encryption variable is generated.



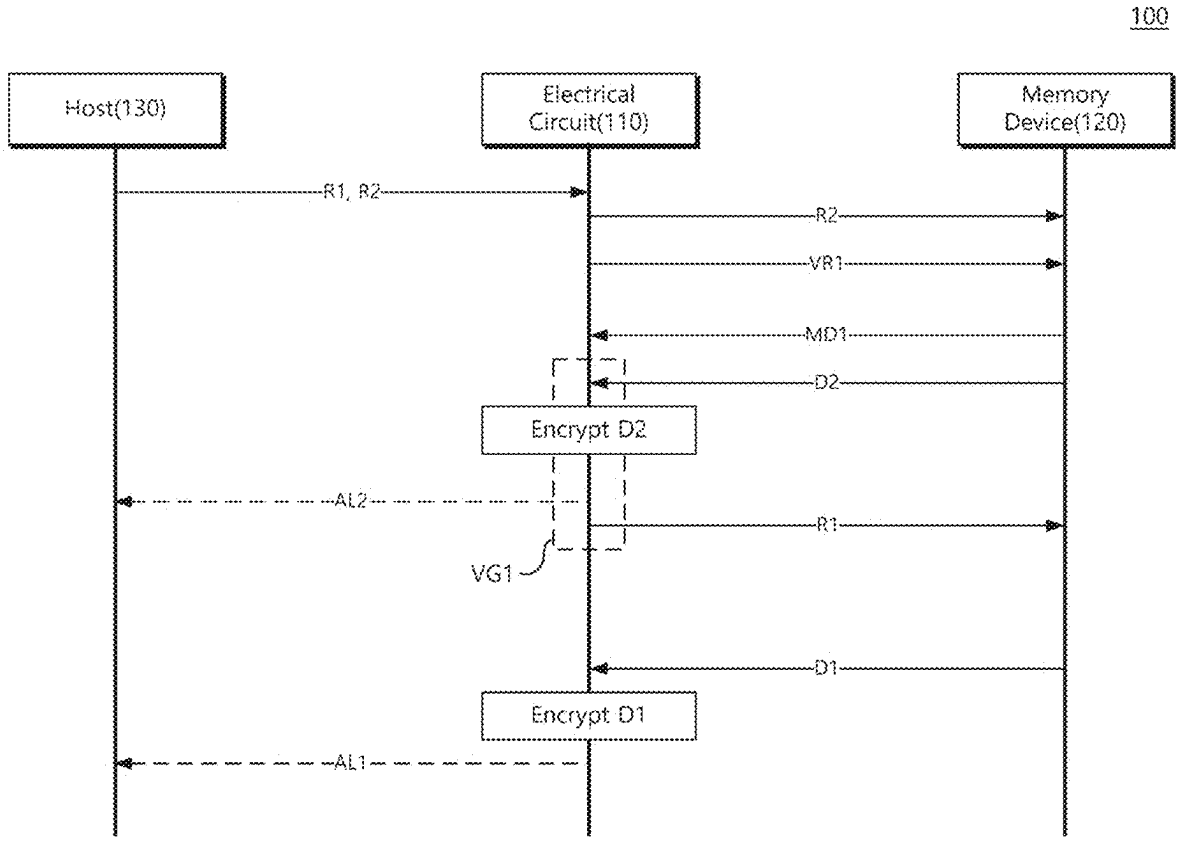
【FIG. 1A】


100
Electrical Circuit(110)
Host (130)
R1, R2
AL1,AL2
Host Interface (131)
Encryption Circuit (111)
Cache Memory (101)
VGR1
Variable Generation Circuit (113)
R1, R2
Scheduler (112)
D2
R2
Memory Interface (121)
D2
R2
MR1
MD1
Memory Device (120)

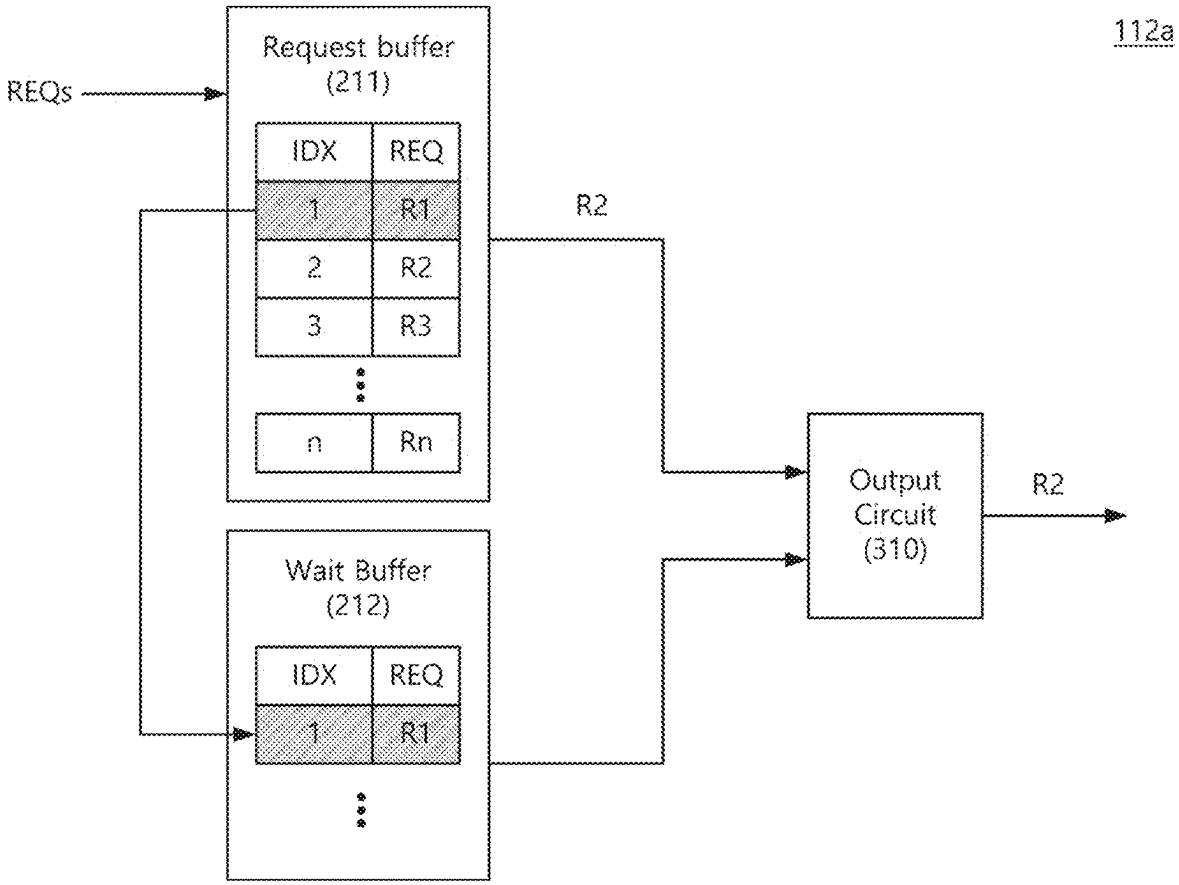
【FIG. 1B】


100
Electrical Circuit(110)
Encryption Circuit (111)
Cache Memory (101)
D1
D1
R1, R2
AL1,AL2
Host (130)
Host Interface (131)
Scheduler (112)
R1
Memory Interface (121)
R1
Memory Device (120)
VAR1
RS1
Variable Generation Circuit (113)

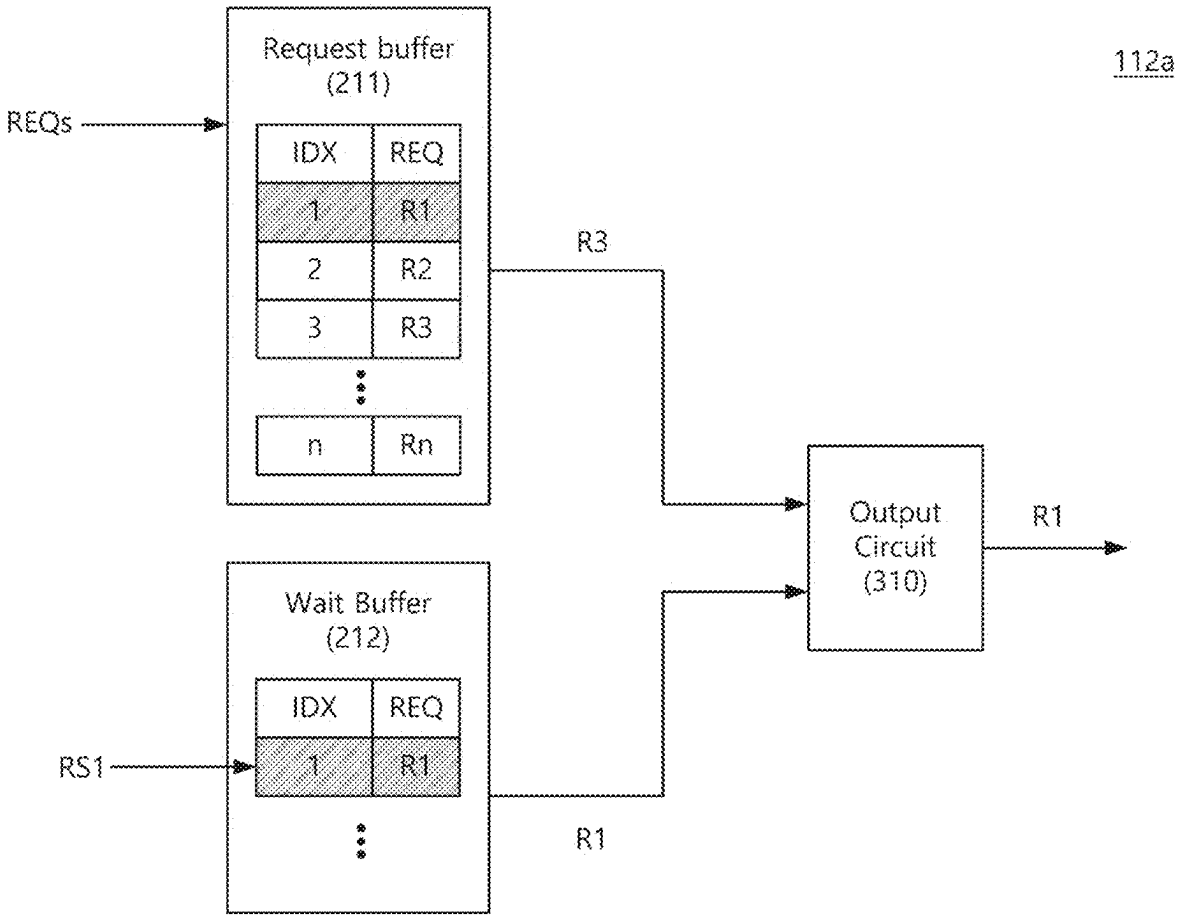
【FIG. 2】


100
Host(130)
Electrical Circuit(110)
Memory Device(120)
R1, R2
R2
VR1
MD1
D2
Encrypt D2
AL2
R1
VG1
D1
Encrypt D1
AL1

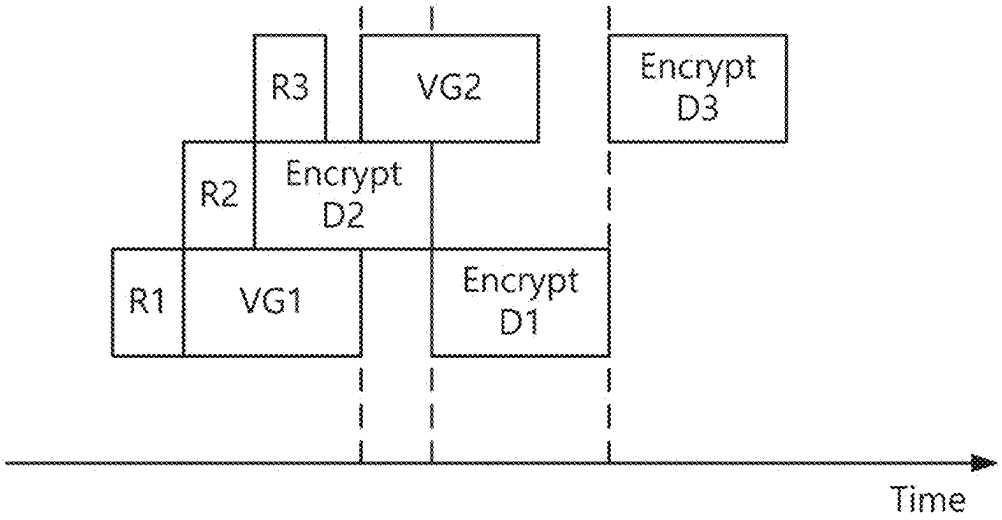
【FIG. 3A】


112a
REQs
Request buffer
(211)
IDX
REQ
1
R1
2
R2
3
R3
n
Rn
R2
Output
Circuit
(310)
R2
Wait Buffer
(212)
IDX
REQ
1
R1

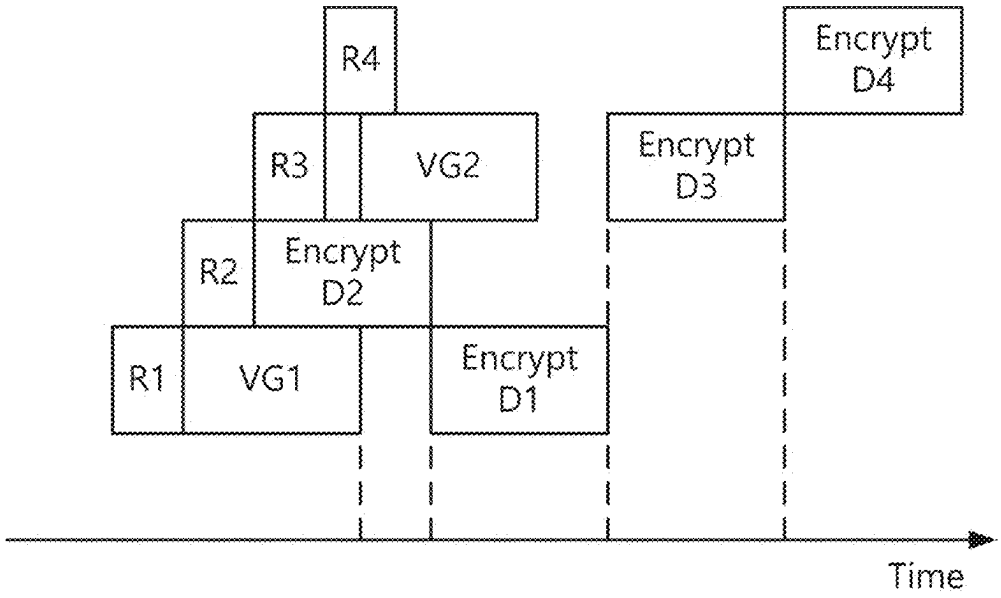
【FIG. 38】


Request buffer
(211)
112a
REQs
IDX
REQ
1
R1
2
R2
3
R3
n
Rn
R3
Output
Circuit
(310)
R1
Wait Buffer
(212)
IDX
REQ
1
R1
RS1
R1

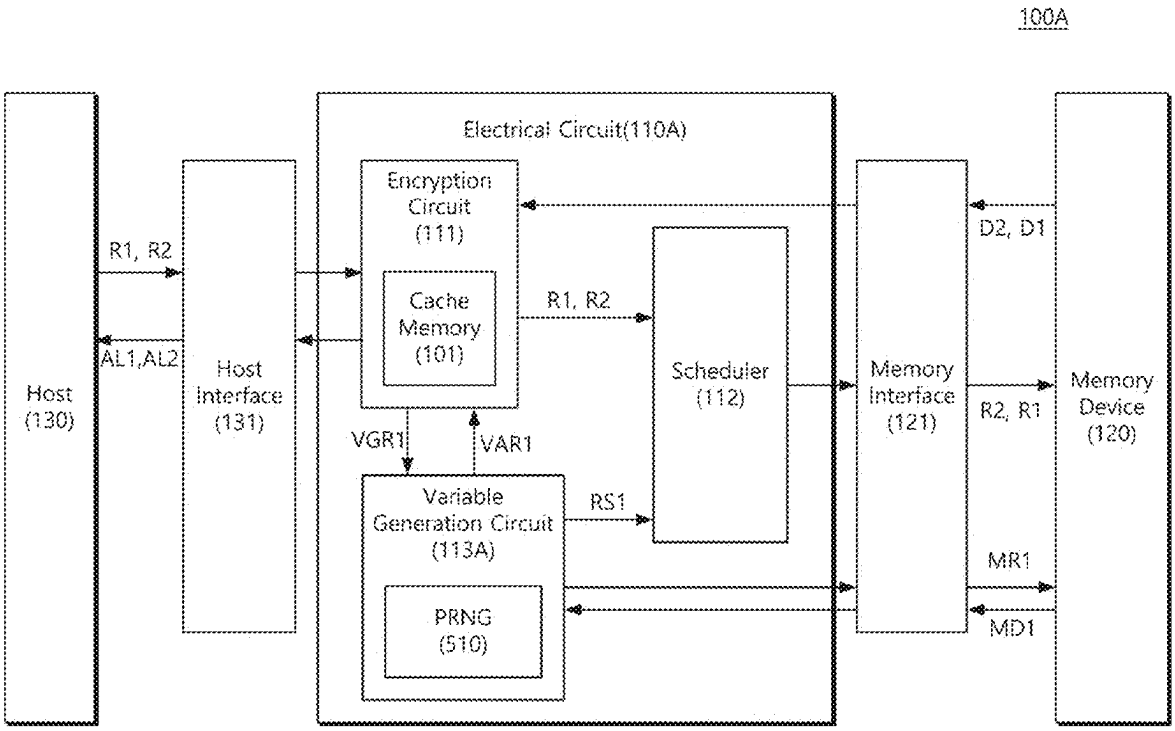
【FIG. 4A】



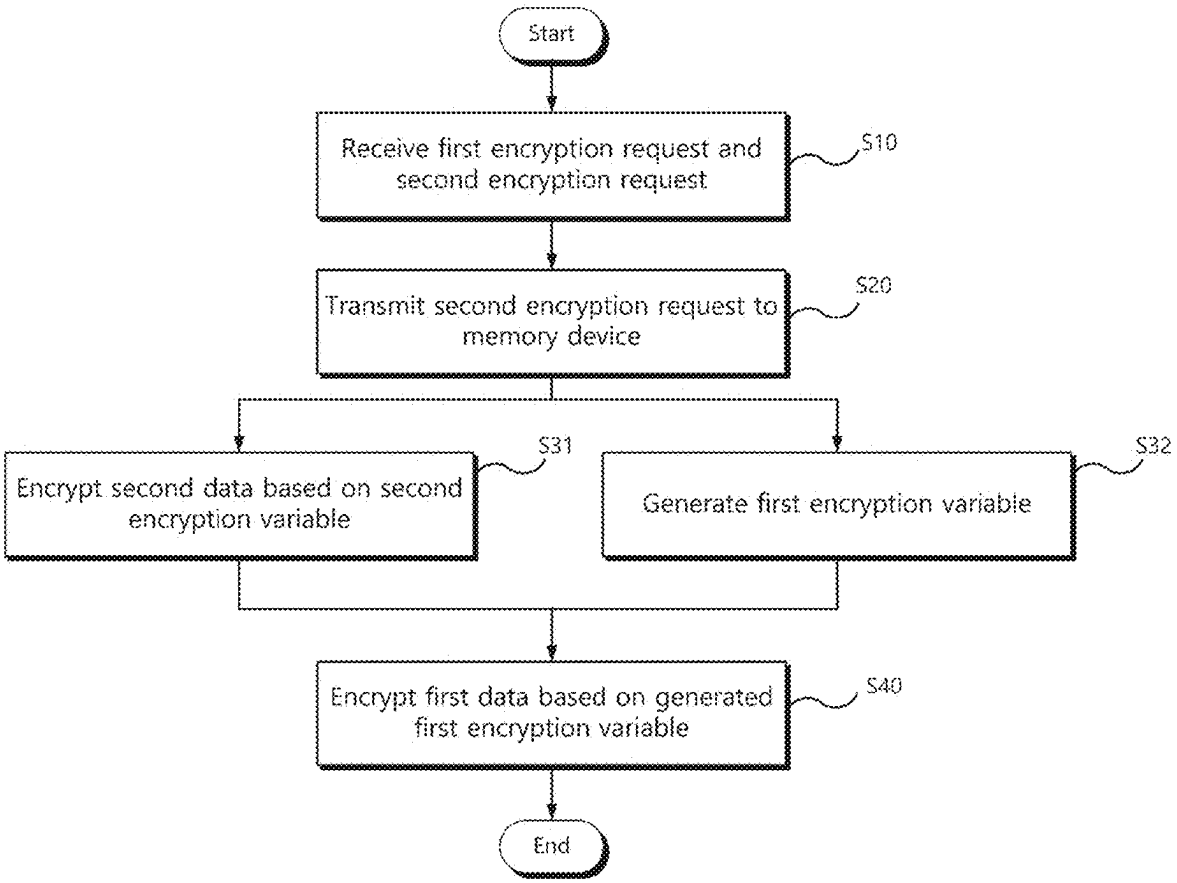
【FIG. 4B】


R4
Encrypt
D4
R3
VG2
Encrypt
D3
R2
Encrypt
D2
R1
VG1
Encrypt
D1
Time

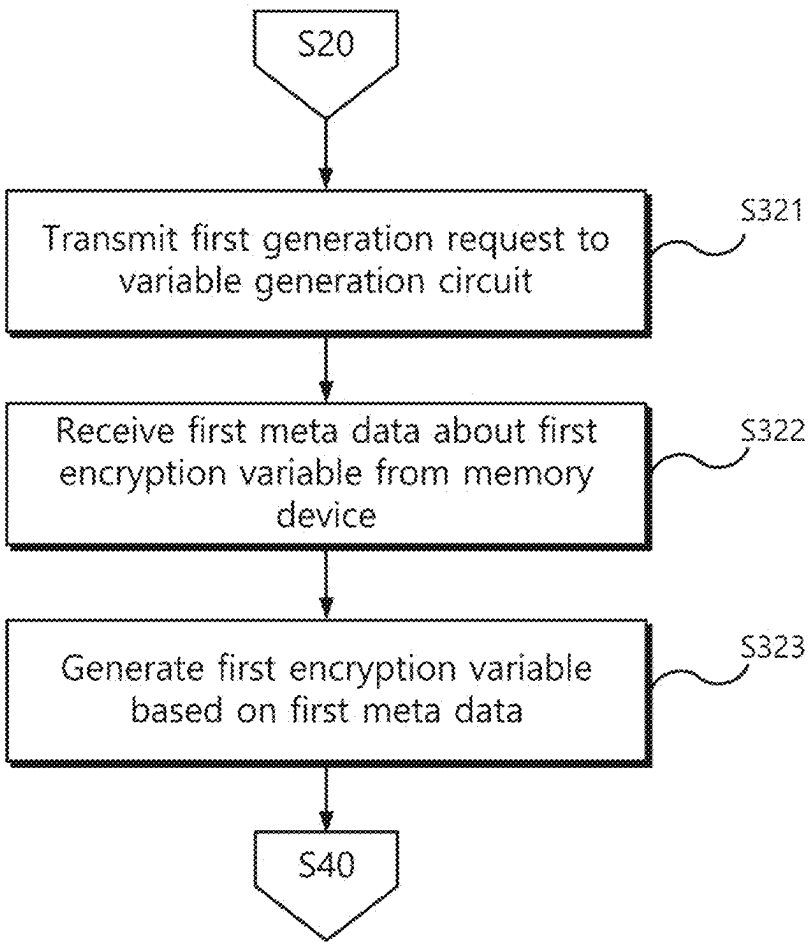
【FIG. 5】


100A
Electrical Circuit(110A)
Host (130)
R1, R2
AL1,AL2
Host Interface (131)
Encryption Circuit (111)
Cache Memory (101)
R1, R2
Scheduler (112)
VGR1
VAR1
Variable Generation Circuit (113A)
PRNG (510)
RS1
Memory Interface (121)
D2, D1
R2, R1
MR1
MD1
Memory Device (120)

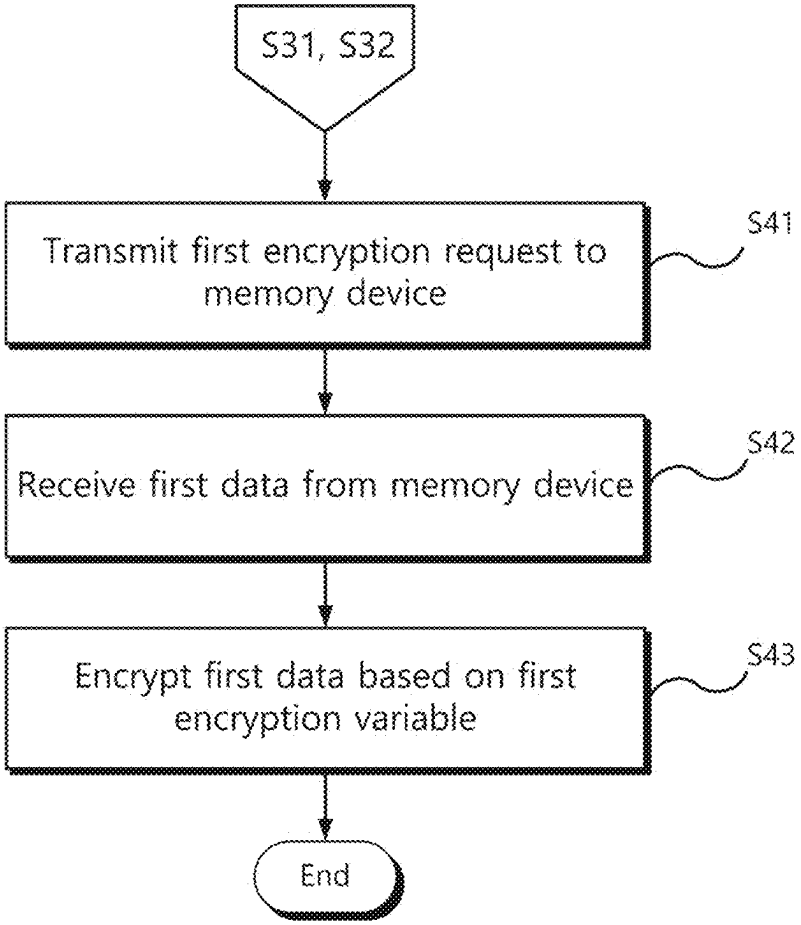
【FIG. 6】


Start
Receive first encryption request and second encryption request
S10
Transmit second encryption request to memory device
S20
Encrypt second data based on second encryption variable
S31
Generate first encryption variable
S32
Encrypt first data based on generated first encryption variable
S40
End

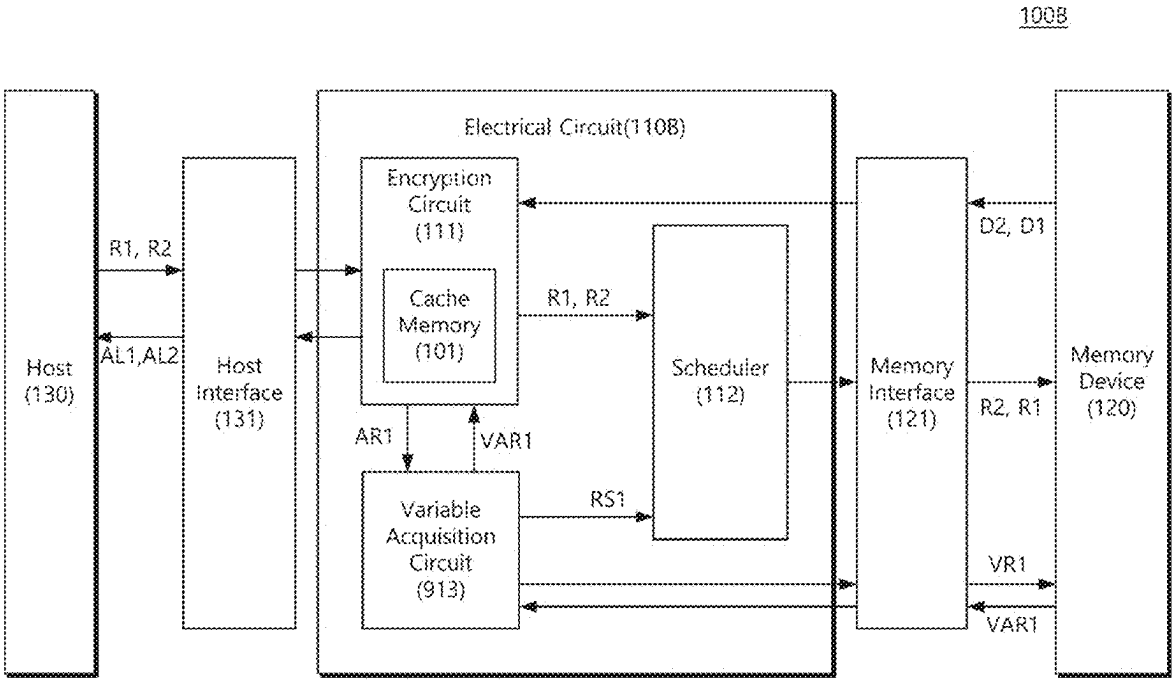
【FIG. 7】


S20
Transmit first generation request to variable generation circuit
S321
Receive first meta data about first encryption variable from memory device
S322
Generate first encryption variable based on first meta data
S323
S40

【FIG. 8】


S31, S32
Transmit first encryption request to memory device
S41
Receive first data from memory device
S42
Encrypt first data based on first encryption variable
S43
End

【FIG. 9】


1008
Host (130)
R1, R2
AL1,AL2
Host Interface (131)
Electrical Circuit(1108)
Encryption Circuit (111)
Cache Memory (101)
AR1
VAR1
Variable Acquisition Circuit (913)
R1, R2
RS1
Scheduler (112)
Memory Interface (121)
D2, D1
R2, R1
VR1
VAR1
Memory Device (120)

ELECTRONIC CIRCUIT FOR ENCRYPTING MEMORY DEVICE AND ENCRYPTION METHOD USING THE SAME

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority under 35 U.S.C. § 119 to Korean Patent Application No. 10-2024-0020468 filed on Feb. 13, 2024, in the Korean Intellectual Property Office, the disclosures of which are incorporated by reference herein in their entireties.

BACKGROUND

[0002] Embodiments of the present disclosure described herein relate to an electronic circuit for encrypting a memory device, and more particularly, relate to an encryption method using the same.

[0003] Nowadays, security and protection of data stored in a memory device are becoming important.

[0004] Consequently, there is an increasing demand on an intellectual property (IP) or an electronic circuit designed to encrypt data stored in a memory device.

[0005] In particular, in cases wherein a host (or system) connected to a memory device is required, in some cases, one or more electronic circuit support encryption for the memory device based on a plurality of encryption variables.

[0006] However, as the number of hosts connected to the memory device and the number of applications supported by the memory device increase, the number of encryption variables which the electronic circuit requires may increase.

[0007] When the electronic circuit stores all encryption variables required for the memory device, the size of the electronic circuit may increase.

[0008] Accordingly, an encrypting method is used in which the electronic circuit stores only some of the encryption variables required for the memory device and acquires (or generates) encryption variables not stored therein from the memory device to perform encryption.

[0009] However, in this case, as the electronic circuit acquires the encryption variables from the memory device based on and/or in response to an order requested for each of a plurality of encryption requests and performs the encryption, the encryption performance (e.g., speed) of the electronic circuit may be degraded.

SUMMARY

[0010] Embodiments of the present disclosure provide an electronic circuit which reduces time required to encrypt data stored in a memory device in response to a plurality of encryption requests.

[0011] According to at least one embodiment, an electronic circuit configured to communicate with a memory device includes an encryption circuit including a cache memory storing an encryption variable for some of a plurality of areas of the memory device, and configured to receive a plurality of encryption requests including a first encryption request for first data stored in a first area of the plurality of areas of the memory device and a second encryption request for second data stored in a second area of the plurality of areas of the memory device, a scheduler that transmits the second encryption request to the memory device when a first encryption variable for the first area is not stored in the cache memory and a second encryption variable for the second area is stored in the cache memory, and a variable generation circuit configured to generate the first encryption variable while the encryption circuit encrypts the second data received from the memory device based on the second encryption variable in response to the second encryption request, and the scheduler transmits the first encryption request to the memory device in response to a determination that the first encryption variable is generated.

[0012] According to at least one embodiment, an encrypting method of a memory system including an electrical circuit and a memory device including a plurality of areas includes receiving a plurality of encryption requests including a first encryption request for first data stored in a first area of the plurality of areas and a second encryption request for second data stored in a second area of the plurality of areas, transmitting the second encryption request to the memory device in response to a determination that a first encryption variable for the first area is not stored in a cache memory of the electrical circuit and a second encryption variable for the second area is stored in the cache memory, generating the first encryption variable while encrypting the second data received from the memory device based on the second encryption variable, and encrypting the first data based on the generated first encryption variable.

[0013] According to at least one embodiment, an electronic circuit configured to communicate with a memory device including a plurality of areas includes an encryption circuit that includes an encryption circuit including a cache memory storing an encryption variable for some of the plurality of areas of the memory device and configured to receive a first encryption request for first data stored in a first area of the plurality of areas and a second encryption request for second data stored in a second area of the plurality of areas, a scheduler that transmits the second encryption request to the memory device when a first encryption variable for the first area is not stored in the cache memory and a second encryption variable for the second area is stored in the cache memory, and a variable acquisition circuit that receives the first encryption variable from the memory device, wherein the electronic circuit is configured such that the encryption circuit encrypts the second data received from the memory device based on the second encryption variable in response to the second encryption request while the variable acquisition circuit receives the first encryption variable and wherein the scheduler is configured to transmit the first encryption request to the memory device in response to a determination that the first encryption variable is received by the variable acquisition circuit.

BRIEF DESCRIPTION OF THE FIGURES

[0014] The above and other objects and features of the present disclosure will become apparent by describing in detail embodiments thereof with reference to the accompanying drawings.

[0015] FIG. **1**A is a block diagram illustrating a memory system which encrypts data based on an encryption variable stored in a cache memory, according to at least one embodiment of the present disclosure.

[0016] FIG. **1**B is a block diagram illustrating a memory system which encrypts data by generating an encryption variable, according to at least one embodiment.

[0017] FIG. **2** illustrates requests and data which an electronic circuit exchanges with a host and a memory device to encrypt data stored in a memory device, according to at least one embodiment.

[0018] FIG. **3**A illustrates a configuration in which a scheduler stores a first encryption request among a plurality of encryption requests in a wait buffer, according to at least one embodiment.

[0019] FIG. **3**B illustrates a configuration in which a wait buffer outputs a first encryption request to an output circuit in response to a first preparation signal, according to at least one embodiment.

[0020] FIG. **4**A illustrates a sequence in which an electronic circuit encrypts data stored in a memory device in response to each of first to third encryption requests which is sequentially transmitted, according to at least one embodiment.

[0021] FIG. **4**B illustrates a configuration for encrypting fourth data in response to a fourth encryption request transmitted following a third encryption request, according to at least one embodiment.

[0022] FIG. **5** is a block diagram illustrating an electronic circuit further including a variable generation circuit, according to at least one embodiment.

[0023] FIG. **6** is a flowchart illustrating an encryption method for a memory device, according to at least one embodiment.

[0024] FIG. **7** is a flowchart illustrating a method of generating a first encryption variable, according to at least one embodiment.

[0025] FIG. **8** is a flowchart illustrating a method of encrypting first data based on and/or in response to a first encryption request, according to at least one embodiment.

[0026] FIG. **9** is a flowchart illustrating a memory system which includes a system-on-chip including a variable acquisition circuit, according to another embodiment.

DETAILED DESCRIPTION

[0027] Hereinafter, embodiments of the present disclosure will be described clearly and in detail so that a person skilled in the technical field of the present disclosure may easily practice the embodiments of the present disclosure.

[0028] In the present disclosure, expressions such as "first", "second", and the like may modify various components regardless of order and/or importance, and are only used to distinguish one component from another component, and do not limit the order or importance of corresponding components.

[0029] FIG. **1**A is a block diagram illustrating a memory system which encrypts data based on an encryption variable stored in a cache memory, according to at least one embodiment of the present disclosure. FIG. **1**B is a block diagram illustrating the memory system for encrypting data by generating the encryption variable, according to at least one embodiment. FIG. **2** illustrates requests and data exchanged by an electronic circuit with a host and a memory device to encrypt data stored in the memory device, according to at least one embodiment.

[0030] Referring to FIG. **1**A and FIG. **1**B together, a memory system **100** according to at least one embodiment may include an electronic circuit **110** and a memory device **120**, The memory system **100** may further include and/or be connected to a host **130**. For example, in the memory system **100**, some of the above-described components (e.g., the host **130**) may be omitted and/or replaced with other components.

[0031] Here, the electronic circuit **110** may be configured to communicate with the host **130** through a host interface **131**. For example, the host interface **131** may support at least one protocol of an advanced extendable interface (AXI), an advanced high performance bus (AHB), and an AXI coherency extension (ACE), and/or the like; but is not limited thereto.

[0032] Additionally, the electronic circuit **110** may be configured to communicate with the memory device **120** through a memory interface **121**.

[0033] According to at least one embodiment, the memory system **100** may refer to an integrated circuit, an electronic device or system, a smart phone, a tablet PC, a computer, a server, a workstation, a portable communication terminal, a personal digital assistant (PDA), a portable multimedia player (PMP), and a computing device, a virtual machine, a virtual computing device thereof and/or the like. Alternatively, the memory system **100** may be some of the components included in a computing system such as a graphic card.

[0034] According to at least one embodiment, the memory system **100** may include the memory device **120** which stores data.

[0035] Here, the memory device **120** is provided as a dynamic random access memory (DRAM) such as a double data rate synchronous dynamic random access memory (DDR SDRAM), a low power double data rate (LPDDR) SDRAM, a graphics double data rate (GDDR) SDRAM, and a Rambus dynamic random access memory (RDRAM). However, embodiments of the present disclosure are not limited thereto, and as an example, the memory device **120** may include a nonvolatile memory such as a flash memory, a magnetic RAM (MRAM), a ferroelectric RAM (FeRAM), a phase change RAM (PRAM), and/or the like a resistive RAM (ReRAM).

[0036] The memory system **100** may include the host **130** communicating with the electronic circuit **110**.

[0037] According to at least one embodiment, the host **130** may be configured to transmit encryption requests R**1** and R**2** for the memory device **120** to the electronic circuit **110** through the host interface **131**.

[0038] More specifically, the host **130** may transmit the encryption requests R**1** and R**2** for at least some of a plurality of areas of the memory device **120** to the electronic circuit **110**.

[0039] The host **130** may transmit the encryption requests R**1** and R**2** for stored data in association with at least some of a plurality of applications supported by the memory device **120** to the electronic circuit **110**.

[0040] In addition, the host **130** may receive notifications AL**1** and AL**2** output from the electronic circuit **110** in response to a determination that encryption of the memory device **120** is completed through the host interface **131**.

[0041] As such, communication between the host **130** and the electronic circuit **110** may be referred to as "bi-directional communication".

[0042] Here, for example, the host **130** may refer to as one of an "application processor (AP)", a "central processing unit (CPU)", an "external system", and/or the like; but is not limited thereto.

[0043] The memory system **100** may include the electronic circuit **110** configured to encrypt data stored in the memory device **120**, e.g., in response to the encryption requests R**1** and R**2** transmitted from the host **130**.

[0044] According to at least one embodiment, the electronic circuit **110** may receive the plurality of encryption requests R**1** and R**2** from the host **130** through the host interface **131**.

[0045] More specifically, the electronic circuit **110** may encrypt at least some of the data stored in the memory device **120** in response to the encryption requests R**1** and R**2** transmitted from the host **130**.

[0046] For example, in response to each of the plurality of encryption requests R**1** and R**2** transmitted from the host **130**, the electronic circuit **110** may encrypt data stored in an area of the memory device **120** specified by each encryption request.

[0047] The electronic circuit **110** according to at least one embodiment may be configured to transmit at least some of the plurality of encryption requests R**1** and R**2** received from the host **130** to the memory device **120**.

[0048] More specifically, the electronic circuit **110** may transmit at least some of the plurality of encryption requests R**1** and R**2** to the memory device **120** through the memory interface **121**.

[0049] For example, the electronic circuit **110** may transmit at least some of the first encryption request R**1** and the second encryption request R**2** sequentially transmitted from the host **130** to the memory device **120**.

[0050] The memory device **120** may be further configured to transmit data D**1** and D**2** stored in an area specified by the encryption requests R**1** and R**2** to the electronic circuit **110** in response to the encryption requests R**1** and R**2** transmitted from the electronic circuit **110**.

[0051] Furthermore, the electronic circuit **110** may encrypt the data D**1** and D**2** transmitted from the memory device **120**.

[0052] The electronic circuit **110** may include an encryption circuit **111**, a scheduler **112**, and a variable generation circuit **113**.

[0053] More specifically, the electronic circuit **110** may include the encryption circuit **111** which encrypts the data D**1** and D**2** received from the memory device **120**.

[0054] According to at least one embodiment, the encryption circuit **111** may include a cache memory **101** which stores encryption variables for some of the plurality of areas of the memory device **120**.

[0055] However, according to at least one embodiment, the cache memory **101** may be implemented in the electronic circuit **110** as a separate configuration from the encryption circuit **111** and may be connected to the encryption circuit **111**.

[0056] For example, the cache memory **101** may store a second encryption variable corresponding to a second area among the plurality of areas of the memory device **120**.

[0057] Here, for example, the encryption variable may include at least one of a key and an initialization vector (IV) for encrypting data stored in each area of the memory device **120**. However, the encryption variable is not limited to the above-described example, and may be referred to as a "various security parameter" used to encrypt the data stored in the memory device **120**.

[0058] In addition, the encryption circuit **111** may receive the encryption requests R**1** and R**2** for the memory device **120** from the host interface **131** (and/or the host **130**).

[0059] For example, the encryption circuit **111** may receive the first encryption request R**1** for the first data D**1** stored in a first area of the memory device **120** and the second encryption request R**2** for the second data D**2** stored in the second area from the host **130**.

[0060] Therefore, the encryption circuit **111** may sequentially receive the first encryption request R**1** and the second encryption request R**2**.

[0061] Furthermore, the encryption circuit **111** may transmit the encryption requests R**1** and R**2** to the scheduler **112**.

[0062] Additionally, the encryption circuit **111** may determine whether an encryption variable for an area of the memory device **120** is stored in the cache memory **101**, for which each of the encryption requests R**1** and R**2** requests encryption.

[0063] Accordingly, the encryption circuit **111** may transmit data including information on whether the encryption variables corresponding to each encryption request are stored in the cache memory **101** to the scheduler **112** together with the encryption requests R**1** and R**2**.

[0064] For example, the encryption circuit **111** may transmit data including information that a first encryption variable VAR**1** for the first area is not stored in the cache memory **101** to the scheduler **112** together with the first encryption request R**1**.

[0065] Additionally, the encryption circuit **111** may transmit data including information that the second encryption variable for the second area is stored in the cache memory **101** to the scheduler **112** together with the second encryption request R**2**.

[0066] Additionally, the electronic circuit **110** may include the scheduler **112** which transmits at least some of the encryption requests R**1** and R**2** transmitted from the encryption circuit **111** to the memory device **120**.

[0067] According to at least one embodiment, the scheduler **112** may transmit an encryption request of which the encryption variable corresponding to an area requesting encryption is stored in the cache memory **101** to the memory device **120**.

[0068] For example, referring to FIG. **1**A, when the second encryption variable corresponding to the second area is stored in the cache memory **101**, the scheduler **112** may transmit the second encryption request R**2** requesting encryption for the second area from among the encryption requests R**1** and R**2** to the memory device **120**.

[0069] Here, in response to the second encryption request R**2**, the memory device **120** may transmit the second data D**2** stored in the second area to the encryption circuit **111** (and/or the electronic circuit **110**).

[0070] Furthermore, the encryption circuit **111** may encrypt the second data D**2** based on the second encryption variable.

[0071] More specifically, the encryption circuit **111** may encrypt the second data D**2** received from the memory device **120** based on the second encryption variable stored in the cache memory **101**.

[0072] Additionally, referring to FIG. **2**, the electronic circuit **110** may transmit the second notification AL**2** including information that encryption for the second data D**2** is completed to the host **130** in response to a determination that the encryption for the second data D**2** is completed.

[0073] Additionally, according to at least one embodiment, when the encryption variable corresponding to an area requesting encryption is not stored in the cache memory **101**, the encryption circuit **111** may transmit a request for generating the encryption variable to the variable generation circuit **113**.

[0074] For example, when the first encryption variable VAR**1** is not stored in the cache memory **101**, the encryption circuit **111** may transmit a first generation request VGR**1** for the first encryption variable VAR**1** to the variable generation circuit **113** in response to the first encryption request R**1**.

[0075] Additionally, the electronic circuit **110** according to at least one embodiment may include the variable generation circuit **113** which generates the encryption variable for each of the plurality of areas of the memory device **120**.

[0076] More specifically, referring to FIG. **1**A, the variable generation circuit **113** may generate the first encryption variable VAR**1** corresponding to the first area of the memory device **120** in response to the first generation request VGR**1** transmitted from the encryption circuit **111**.

[0077] According to at least one embodiment, the variable generation circuit **113** may transmit a first meta request MR**1** to the memory device **120** in response to the first generation request VGR**1**. The first meta request MR**1** may include request for first metadata MD**1** from the memory device **120**.

[0078] Here, the variable generation circuit **113** may store location information on a location of the memory device **120**, at which the first metadata MD**1** for the first area is stored.

[0079] Accordingly, the variable generation circuit **113** may transmit the first meta request MR**1** including the location information of the first metadata MD**1** to the memory device **120**.

[0080] Additionally, in response to the first meta request MR**1** the memory device **120** may transmit the stored first metadata MD**1** corresponding to the first encryption variable VAR**1** to the variable generation circuit **113** (and/or the electronic circuit **110**).

[0081] Furthermore, the variable generation circuit **113** may generate the first encryption variable VAR**1** based on the first metadata MD**1** received from the memory device **120**.

[0082] Here, the variable generation circuit **113** may generate the first encryption variable VAR**1** in response to the first encryption request R**1** while the encryption circuit **111** encrypts the second data D**2** based on the second encryption variable.

[0083] That is, referring to FIG. **2**, the variable generation circuit **113** may perform a first generation operation VG**1** for generating the first encryption variable VAR**1** while the encryption circuit **111** encrypts the second data D**2**.

[0084] Furthermore, referring to FIG. **1**B, the variable generation circuit **113** may transmit the first encryption variable VAR**1** to the encryption circuit **111** in response to a determination that the first encryption variable VAR**1** is generated.

[0085] Here, the encryption circuit **111** may store the first encryption variable VAR**1** transmitted from the variable generation circuit **113** in the cache memory **101**.

[0086] For example, the encryption circuit **111** may delete one of encryption variables stored in the cache memory **101** and store the first encryption variable VAR**1** in the cache memory **101**.

[0087] In addition, in response to a determination that the first encryption variable VAR**1** is generated, the variable generation circuit **113** may transmit a first preparation signal RS**1** including information that the first encryption variable VAR**1** is generated to the scheduler **112**.

[0088] According to at least one embodiment, the scheduler **112** may transmit the first encryption request R**1** to the memory device **120** in response to the first preparation signal RS**1**.

[0089] Here, the memory device **120** may transmit the first data D**1** stored in the first area to the encryption circuit **111** (and/or the electronic circuit **110**) in response to the first encryption request R**1** requesting encryption of the first area.

[0090] Furthermore, the encryption circuit **111** may encrypt the first data D**1** based on the first encryption variable VAR**1**.

[0091] More specifically, the encryption circuit **111** may encrypt the first data D**1** received from the memory device **120** based on the first encryption variable VAR**1** received from the variable generation circuit **113**.

[0092] Additionally, referring to FIG. **2**, the electronic circuit **110** may transmit the first notification AL**1** including information that encryption of the first data D**1** is completed to the host **130** in response to a determination that the encryption of the first data D**1** is completed.

[0093] Referring to the above-described configurations, when the electronic circuit **110** sequentially receives the first encryption request R**1** and the second encryption request R**2**, the electronic circuit **110** may encrypt the second data D**2** based on the second encryption variable stored in the cache memory **101**.

[0094] Additionally, the electronic circuit **110** may generate the first encryption variable VAR**1** not stored in the cache memory **101** while encrypting the second data D**2** based on the previously stored second encryption variable.

[0095] Furthermore, the electronic circuit **110** may encrypt the first data D**1** in response to a determination that encryption of the second data D**2** is completed and the first encryption variable VAR**1** is generated.

[0096] That is, while the electronic circuit **110** is first performing encryption in response to encryption request of which the encryption variable is stored from among the plurality of encryption requests, the electronic circuit **110** may generate the encryption variable in response to the encryption request of which the encryption variable is not stored.

[0097] Through this, the electronic circuit **110** according to at least one embodiment of the present disclosure may reduce the time required to encrypt the data stored in the memory device **120** in response to the plurality of encryption requests R**1** and R**2**.

[0098] Additionally, the electronic circuit **110** may improve encryption performance (e.g., speed) for encrypting data stored in the memory device **120** while the size of cache memory **101** (or the electronic circuit **110**) is maintained (and/or reduced).

[0099] FIG. **3**A illustrates a configuration in which a scheduler stores a first encryption request among a plurality of encryption requests in a wait buffer, according to at least one embodiment. FIG. **3**B illustrates a configuration in which a wait buffer outputs the first encryption request to an output circuit in response to a first preparation signal, according to at least one embodiment.

[0100] Referring to FIG. **3**A and FIG. **3**B together, a scheduler **112***a* according to at least one embodiment may include a request buffer **211**, a wait buffer **212**, and an output circuit **310**.

[0101] Here, the scheduler **112***a* of FIG. **3**A and FIG. **3**B may be understood as an example of the scheduler **112** of FIG. **1**A and FIG. **1**B.

[0102] More specifically, the scheduler **112***a* may include the request buffer **211** which stores a plurality of encryption requests REQs received from the encryption circuit **111**.

[0103] According to at least one embodiment, the scheduler **112***a* may sequentially store the plurality of encryption requests REQs in the request buffer **211** based on and/or in response to an order received from the encryption circuit **111**.

[0104] For example, the scheduler **112***a* may store the first encryption request R**1** to an n-th encryption request Rn sequentially received from the encryption circuit **111** in the request buffer **211** based on the order in which they are received.

[0105] Here, the scheduler **112***a* may store the plurality of encryption requests REQs in the request buffer **211** together with an index IDX based on the order received from the encryption circuit **111**.

[0106] Additionally, the scheduler **112***a* may include the wait buffer **212** which stores encryption requests, of which an encryption variable corresponding to an encryption request area is not stored, in the cache memory **101** (or the encryption circuit **111**), from among the plurality of encryption requests REQs.

[0107] For example, when the first encryption variable VAR**1** for the first area is not stored in the cache memory **101**, the scheduler **112***a* may store the first encryption request R**1** requesting encryption for the first area in the wait buffer **212**.

[0108] Here, the scheduler **112***a* may store encryption requests, of which the encryption variable corresponding to the area requesting encryption is not stored in the cache memory **101**, in the wait buffer **212** together with the index IDX which is based on the order received from the encryption circuit **111**.

[0109] According to at least one embodiment, the request buffer **211** may sequentially output the encryption requests for an area in association with which an encryption variable is stored in the cache memory **101** from among the encryption requests R**1** to Rn stored in the request buffer **211**.

[0110] For example, referring to FIG. **3**A, when the second encryption variable is stored in the cache memory **101**, the request buffer **211** may first output the second encryption request R**2** for the second area.

[0111] Subsequently, referring to FIG. **3**B, when the third encryption variable is stored in the cache memory **101**, the request buffer **211** may output a third encryption request R**3** for the third area.

[0112] Additionally, the wait buffer **212** may output an encryption request, of which an encryption variable is generated, from among encryption requests stored in the wait buffer **212**.

[0113] For example, referring to FIG. **3**B, the wait buffer **212** may output the first encryption request R**1** stored in the wait buffer **212** in response to the first preparation signal RS**1**.

[0114] Here, the first preparation signal RS**1** may be understood as a signal output to the scheduler **112***a* in response to a determination that the first encryption variable VAR**1** is generated by the variable generation circuit **113**.

[0115] Additionally, the scheduler **112***a* may further include the output circuit **310** which outputs an encryption request output from the request buffer **211** and the wait buffer **212** to the memory device **120** (and/or the memory interface **121**).

[0116] For example, referring to FIG. **3**A, while the first encryption request R**1** is stored in the wait buffer **212**, the output circuit **310** may output the second encryption request R**2** output from the request buffer **211** to the memory device **120**.

[0117] Additionally, the output circuit **310** may sequentially output the encryption requests output from the request buffer **211** and the wait buffer **212** to the memory device **120** (and/or the memory interface **121**) based on the order (and/or an index IDX) entered into the scheduler **112***a*.

[0118] For example, referring to FIG. **3**B, when the request buffer **211** outputs the third encryption request R**3** and the wait buffer **212** outputs the first encryption request R**1**, the output circuit **310** may output the first encryption request R**1** to the memory device **120**.

[0119] Additionally, the output circuit **310** may output the first encryption request R**1** and then output the third encryption request R**3** to the memory device **120**.

[0120] That is, when the encryption requests are output from each of the request buffer **211** and the wait buffer **212**, the output circuit **310** may sequentially output the encryption requests to the memory device **120** (or the memory interface **121**) based on the order in which the encryption requests are input to the scheduler **112***a*.

[0121] Here, in response to the encryption request output from the output circuit **310**, the memory device **120** may transmit data stored in an area in which each encryption request requires encryption to the electronic circuit **110**.

[0122] Furthermore, the electronic circuit **110** (and/or the encryption circuit **111**) may sequentially encrypt the data transferred from the memory device **120** in response to the encryption variable corresponding to the area in which each data is stored based on and/or in response to each encryption request.

[0123] Referring to the above-described configurations, the scheduler **112***a* may store the plurality of encryption requests REQs sequentially received in the request buffer **211**. Additionally, the scheduler **112***a* may store the encryption requests, of which the encryption variable is not stored in the cache memory **101**, in the wait buffer **212**, from among the plurality of encryption requests REQs which are sequentially received.

[0124] Additionally, the scheduler **112***a* may output the encryption request, of which an encryption variable is generated, from among encryption requests stored in the wait buffer **212**, while the scheduler **112***a* sequentially outputs the encryption requests stored in the cache memory **101**.

[0125] Furthermore, the encryption circuit **111** may sequentially encrypt data received from the memory device **120** based on and/or in response to the encryption request sequentially output by the scheduler **112***a*.

[0126] That is, while the electronic circuit **110** is first performing the encryption in response to the encryption request of which the encryption variable is stored from among the plurality of encryption requests REQs, the elec-

tronic circuit **110** may generate the encryption variable in response to the encryption request of which the encryption variable is not stored.

[0127] Therefore, the electronic circuit **110** may encrypt the data stored in the memory device **120** within a relatively short span of time compared to the case of performing the encryption after the electronic circuit **110** sequentially obtains the encryption variables for each of the plurality of encryption requests REQs. Additionally, since only a subset (e.g., one of the encryption variables) is stored in the cache memory **101**, the size and/or resource requirements of the cache memory **101** may be maintained and/or reduced.

[0128] Accordingly, the electronic circuit **110** according to at least one embodiment of the present disclosure may reduce the time required to encrypt the data stored in the memory device **120** in response to the plurality of encryption requests REQs while maintaining a smaller cache memory **101**.

[0129] FIG. **4**A illustrates processes in which the electronic circuit encrypts data stored in the memory device in response to each of the first encryption request to the third encryption request sequentially transmitted, according to at least one embodiment. FIG. **4**B illustrates a configuration of encrypting fourth data in response to a fourth encryption request transmitted following the third encryption request R**3**, according to at least one embodiment.

[0130] Referring to FIG. **4**A and FIG. **4**B together, the electronic circuit **110** according to at least one embodiment may encrypt the data stored in an area in which each encryption request requires encryption in response to each of the encryption requests R**1** to R**4** sequentially received.

[0131] Referring to FIG. **4**A, the electronic circuit **110** according to at least one embodiment may encrypt the first data D**1** to third data D**3** in response to sequentially receiving the first encryption request R**1** to the third encryption request R**3**.

[0132] According to at least one embodiment, the encryption circuit **111** may sequentially receive the first encryption request R**1** to the third encryption request R**3** for the memory device **120** from the host interface **131**.

[0133] For example, the encryption circuit **111** may sequentially receive, from the host **130**, the first encryption request R**1** for the first data D**1** stored in the first area of the memory device **120**, the second encryption request R**2** for the second data D**2** stored in the second area of the memory device **120**, and the third encryption request R**3** for the third data D**3** stored in a third area of the memory device **120**.

[0134] According to at least one embodiment, the electronic circuit **110** may first encrypt the second data D**2** stored in the second area in response to the second encryption request R**2** of which the encryption variable is stored from among the first encryption request R**1** to the third encryption request R**3** sequentially received.

[0135] Here, it is assumed that the cache memory **101** stores the second encryption variable for the second area and does not store the first encryption variable for the first area and does not store the third encryption variable for the third area.

[0136] For example, the electronic circuit **110** (and/or the encryption circuit **111**) may encrypt the second data D**2** stored in the second area based on the second encryption variable previously stored in the cache memory **101** based on and/or in response to the second encryption request R**2**.

[0137] Additionally, while the electronic circuit **110** encrypts the second data D**2**, the electronic circuit **110** may generate the first encryption variable corresponding to the first area based on and/or in response to the first encryption request R**1** of which the encryption variable is not stored.

[0138] For example, the encrypting the second data D**2** based on the second encryption variable and the generation of the first generation operation VG**1** (generating the first encryption variable VAR**1**) may overlap. For example, while the electronic circuit **110** encrypts the second data D**2** based on the second encryption variable, the electronic circuit **110** may perform the first generation operation VG**1** for generating the first encryption variable VAR**1**.

[0139] Additionally, while the electronic circuit **110** encrypts the second data D**2**, the electronic circuit **110** may generate the third encryption variable corresponding to the third area based on and/or in response to the third encryption request R**3** of which the encryption variable is not stored.

[0140] For example, the electronic circuit **110** may perform a second generation operation VG**2** for generating the third encryption variable in response to a determination that the first encryption variable VAR**1** is generated while the electronic circuit **110** encrypts the second data D**2**.

[0141] Additionally, the encryption circuit **111** may encrypt the first data D**1** in response to a determination that the first encryption variable VAR**1** is generated and encryption for the second data D**2** is completed.

[0142] More specifically, in response to a determination that the first encryption variable VAR**1** is generated at a time point when (or after) the encryption of the second data D**2** is completed, the scheduler **112** may transmit the first encryption request R**1** to the memory device **120**.

[0143] Furthermore, the encryption circuit **111** may encrypt the first data D**1** received from the memory device **120** based on the first encryption variable VAR**1** based on and/or in response to the first encryption request R**1**.

[0144] Additionally, the encryption circuit **111** may encrypt the third data D**3** in response to a determination that the third encryption variable is generated and that encryption of the first data D**1** is completed.

[0145] More specifically, in response to a determination that the third encryption variable is generated at a time point when (or after) the encryption of the first data D**1** is completed, the scheduler **112** may transmit the third encryption request R**3** to the memory device **120**.

[0146] Furthermore, the encryption circuit **111** may encrypt the third data D**3** received from the memory device **120** based on the third encryption variable in response to the third encryption request R**3**.

[0147] According to at least one embodiment, when the cache memory **101** stores the third encryption variable for the third area, the encryption circuit **111** may encrypt the third data D**3** based on the prestored third encryption variable.

[0148] For example, when the first encryption variable VAR**1** is generated at the time point when the encryption of the second data D**2** is completed, the scheduler **112** may transmit the first encryption request R**1** to the memory device **120**.

[0149] Furthermore, the encryption circuit **111** may encrypt the first data D**1** received from the memory device **120** based on and/or in response to the first encryption request R**1**.

[0150] For another example, when the first encryption variable VAR**1** is not generated at the time point when the encryption of the second data D**2** is completed, the scheduler **112** may transmit the third encryption request R**3** to the memory device **120**. In other words, the scheduler may transmit the first encryption request R**1** or third encryption request R**3** based on the readiness of the first encryption variable VAR**1**.

[0151] Furthermore, the encryption circuit **111** may encrypt the third data D**3** received from the memory device **120** based on and/or in response to the third encryption request R**3**.

[0152] Additionally, referring to FIG. **4**B, according to at least one embodiment, when the encryption circuit **111** receives an additional encryption request (e.g., a fourth encryption request R**4** following the third encryption request R**3**), the encryption circuit **111** may encrypt fourth data D**4** based on a fourth encryption variable.

[0153] More specifically, when the encryption circuit **111** receives the fourth encryption request R**4** following the third encryption request R**3**, the fourth data D**4** may be encrypted based on the fourth encryption variable previously stored in the cache memory **101**.

[0154] Here, the example provides that the cache memory **101** stores the fourth encryption variable for the fourth area.

[0155] For example, the encryption circuit **111** may encrypt the fourth data D**4** in response to the end of the encryption of the third data D**3**.

[0156] Referring to the above-described configurations, when the electronic circuit **110** sequentially receives the first encryption request R**1** to the fourth encryption request R**4**, the electronic circuit **110** may first encrypt the second data D**2** stored in the second area based on the second encryption variable stored in the cache memory **101**.

[0157] Additionally, the electronic circuit **110** may sequentially generate the first encryption variable VAR**1** and a third encryption variable VAR**3** not stored in the cache memory **101** while (e.g., in parallel to) the electronic circuit **110** encrypts the second data D**2** based on the previously stored second encryption variable.

[0158] Furthermore, the electronic circuit **110** may sequentially encrypt the first data D**1** and the third data D**3** in response to a determination that each encryption variable is generated. Additionally, the electronic circuit **110** may encrypt the fourth data D**4** in response to the encryption of the third data D**3**.

[0159] That is, the electronic circuit **110** may generate the encryption variable in response to the encryption request of which the encryption variable is not stored from among the plurality of encryption requests while the electronic circuit **110** is first performing the encryption in response to the encryption request of which the encryption variable is stored.

[0160] Furthermore, the electronic circuit **110** may sequentially encrypt the data based on the encryption variable generated while performing the encryption based on the prestored encryption variable.

[0161] Through this, the electronic circuit **110** according to at least one embodiment of the present disclosure may reduce the time required to encrypt the data stored in the memory device **120** in response to the plurality of encryption requests R**1** and R**2**.

[0162] Additionally, the electronic circuit **110** may improve the encryption performance (e.g., the speed) for encrypting the data stored in the memory device **120** while the size of the cache memory **101** (or the electronic circuit **110**) is maintained (and/or reduced).

[0163] FIG. **5** is a block diagram illustrating the electronic circuit further including a random number generating circuit, according to at least one embodiment.

[0164] Referring to FIG. **5**, a memory system **100**A according to at least one embodiment may include an electronic circuit **110**A, the memory device **120**, and the host **130**.

[0165] Here, the memory system **100**A of FIG. **5** may be understood as an example of the memory system **100** illustrated in FIG. **1**A and FIG. **1**B. Accordingly, the same reference numerals are used for configurations which are the same as or substantially the same as the above-described configurations, and descriptions overlapping the above-described contents may be omitted for brevity and/or repeated for clarity and/or emphasis.

[0166] The electronic circuit **110**A may include the encryption circuit **111**, the scheduler **112**, and a variable generation circuit **113**A.

[0167] According to at least one embodiment, the encryption circuit **111** may receive the encryption requests R**1** and R**2** for the memory device **120** from the host **130**.

[0168] For example, the encryption circuit **111** may sequentially receive the first encryption request R**1** for the first data D**1** stored in the first area of the memory device **120** and the second encryption request R**2** for the second data D**2** stored in the second area from the host **130**.

[0169] Additionally, the encryption circuit **111** may transmit the received encryption requests R**1** and R**2** to the scheduler **112**.

[0170] The scheduler **112** may first transmit, to the memory device **120**, the second encryption request R**2** of which the second encryption variable is previously stored from among the encryption requests R**1** and R**2** received from the encryption circuit **111**.

[0171] Subsequently, the encryption circuit **111** may encrypt the second data D**2** received from the memory device **120** based on the prestored second encryption variable based on and/or in response to the second encryption request R**2**.

[0172] Additionally, the encryption circuit **111** may transmit a generation request to generate the encryption variable to the variable generation circuit **113**A in response to the encryption request of which the encryption variable corresponding to the area requesting encryption is not stored in the cache memory **101**.

[0173] For example, when the first encryption variable VAR**1** is not stored in the cache memory **101**, the encryption circuit **111** may transmit the first generation request VGR**1** for the first encryption variable VAR**1** to the variable generation circuit **113**A.

[0174] Additionally, the electronic circuit **110**A may include the variable generation circuit **113**A which is configured to generate the encryption variable for each of the plurality of areas of the memory device **120**.

[0175] For example, the variable generation circuit **113**A may generate the first encryption variable VAR**1** corresponding to the first area of the memory device **120** in response to the first generation request VGR**1** transmitted from the encryption circuit **111**.

[0176] The variable generation circuit **113**A may transmit the first meta request MR**1** requesting the first metadata MD**1** to the memory device **120** in response to the first generation request VGR**1**.

[0177] In response to the first meta request MR**1**, the memory device **120** may transmit the stored first metadata MD**1** corresponding to the first encryption variable VAR**1** to the variable generation circuit **113**A (or the electronic circuit **110**).

[0178] Additionally, the variable generation circuit **113**A may further include a random number generation circuit (PRNG) **510**.

[0179] The random number generation circuit **510** according to at least one embodiment may be configured to output a random number based on a specified (e.g., a preset and/other otherwise determined) probability.

[0180] For example, the random number generation circuit **510** may generate a pseudo random number based on the specified probability. Accordingly, the random number generation circuit **510** may be referred to as a "pseudo random number generator (PRNG)".

[0181] Therefore, the variable generation circuit **113**A may generate the first encryption variable VAR**1** based on at least the first metadata MD**1** received from the memory device **120** and the random number generated from the random number generation circuit **510**.

[0182] Here, the variable generation circuit **113**A may generate the first encryption variable VAR**1** while the encryption circuit **111** encrypts data (e.g., the second data D**2**) based on an encryption variable which is prestored in the cache memory **101** (e.g., the second encryption variable).

[0183] Additionally, the variable generation circuit **113**A may transmit the first encryption variable VAR**1** to the encryption circuit **111** in response to a determination that the first encryption variable VAR**1** is generated.

[0184] Additionally, in response to a determination that the first encryption variable VAR**1** is generated, the variable generation circuit **113**A may transmit the first preparation signal RS**1** including the information that the first encryption variable VAR**1** is generated to the scheduler **112**.

[0185] Furthermore, the scheduler **112** may transmit the first encryption request R**1** to the memory device **120** in response to the first preparation signal RS**1**.

[0186] Additionally, the encryption circuit **111** may encrypt the first data D**1** received from the memory device **120** based on the first encryption variable VAR**1** based on and/or in response to the first encryption request R**1**.

[0187] Referring to the above-described configurations, while the electronic circuit **110**A is performing the encryption in response to the encryption request of which the encryption variable is stored, the electronic circuit **110**A may generate the encryption variable in response to the encryption request of which the encryption variable is not stored, from among the plurality of encryption requests.

[0188] Therefore, the electronic circuit **110**A according to at least one embodiment of the present disclosure may reduce the time required to encrypt the data stored in the memory device **120** in response to the plurality of encryption requests R**1** and R**2**, while the size of cache memory **101** (or the electronic circuit **110**A) is maintained (and/or reduced).

[0189] Additionally, the variable generation circuit **113**A according to at least one embodiment may generate the encryption variable based on the random number generated according to the specified probability from the random number generation circuit **510**.

[0190] Therefore, the electronic circuit **110**A according to at least one embodiment of the present disclosure may enhance security of the data of the memory device **120** encrypted by the encryption variable.

[0191] FIG. **6** is a flowchart illustrating a method of encrypting a memory device, according to at least one embodiment. FIG. **7** is a flowchart illustrating a method of generating the first encryption variable (operation S**32** of FIG. **6**), according to at least one embodiment. FIG. **8** is a flowchart illustrating a method of encrypting the first data based on and/or in response to the first encryption request (operation S**40**), according to at least one embodiment.

[0192] Referring to FIG. **6** to FIG. **8** together, the electronic circuit **110** (or the memory system **100**) according to at least one embodiment may encrypt the data stored in the plurality of areas of the memory device **120** in response to the plurality of encryption requests R**1** and R**2**.

[0193] In operation S**10**, the electronic circuit **110** receives the first encryption request R**1** and the second encryption request R**2**.

[0194] More specifically, the electronic circuit **110** (or the encryption circuit **111**) may receive the first encryption request R**1** for the first data D**1** stored in the first area of the memory device **120** and the second encryption request R**2** for the second data D**2** stored in the second area of the memory device **120** from the host **130**.

[0195] Here, for example, the electronic circuit **110** may sequentially receive the first encryption request R**1** for the first area and the second encryption request R**2** for the second area of the memory device **120**.

[0196] In operation S**20**, the electronic circuit **110** transmits the second encryption request R**2** to the memory device **120**.

[0197] More specifically, when the prestored encryption variable stored in the cache memory **101** is the second encryption variable, the electronic circuit **110** (or the scheduler **112**) may transmit the second encryption request R**2** requesting the encryption for the second area of the encryption requests R**1** and R**2** to the memory device **120**.

[0198] In other words, in the example, the cache memory **101** does not store the first encryption variable for the first area, but stores the second encryption variable for the second area.

[0199] That is, the electronic circuit **110** may first transmit the encryption request of which the encryption variable for the area requesting encryption from among the received encryption requests R**1** and R**2** is stored in the cache memory **101** to the memory device **120**.

[0200] Furthermore, in operation S**31**, the electronic circuit **110** encrypts the second data D**2** based on the second encryption variable.

[0201] More specifically, the electronic circuit **110** may encrypt the second data D**2** received from the memory device **120** based on and/or in response to the second encryption request R**2** based on the prestored second encryption variable.

[0202] Additionally, in operation S**32**, the electronic circuit **110** generates the first encryption variable VAR**1**.

[0203] More specifically, referring to FIG. **6** and FIG. **7** together, the electronic circuit **110** may generate the first encryption variable VAR**1** based on the first metadata MD**1**

stored in the memory device **120** (S**32**) corresponding to the first encryption variable VAR**1**.

[0204] In operation S**321**, the encryption circuit **111** transmits the first generation request VGR**1** to the variable generation circuit **113**.

[0205] More specifically, when the first encryption variable VAR**1** is not stored in the cache memory **101**, the encryption circuit **111** may transmit the first generation request VGR**1** to the variable generation circuit **113**.

[0206] In operation S**322**, the variable generation circuit **113** receives the first metadata MD**1** associated with the first encryption variable VAR**1** from the memory device **120**.

[0207] More specifically, the variable generation circuit **113** may transmit the first meta request MR**1** requesting the first metadata MD**1** to the memory device **120** in response to the first generation request VGR**1**.

[0208] Additionally, in response to the first meta request MR**1**, the memory device **120** may transmit the stored first metadata MD**1** corresponding to the first encryption variable VAR**1** to the variable generation circuit **113** (or the electronic circuit **110**).

[0209] Furthermore, in operation S**323**, the variable generation circuit **113** generates the first encryption variable VAR**1** based on the first metadata MD**1** received from the memory device **120**.

[0210] According to at least one embodiment, the variable generation circuit **113** may further include the random number generation circuit **510** for generating the random number according to the specified probability.

[0211] In this case, the variable generation circuit **113** may generate the first encryption variable VAR**1** based on the first metadata MD**1** and the random number generated from the random number generation circuit **510**.

[0212] According to at least one embodiment, the variable generation circuit **113** may transmit a signal for requesting the first encryption variable VAR**1** to the memory device **120** in response to the first generation request VGR**1**.

[0213] Additionally, the memory device **120** may transmit the first encryption variable VAR**1** to the variable generation circuit **113** (and/or the electronic circuit **110**) in response to the signal received from the electronic circuit **110**.

[0214] According to at least one embodiment, while the encryption circuit **111** encrypts the second data D**2** based on the second encryption variable, the variable generation circuit **113** may generate the first encryption variable VAR**1** in response to the first encryption request R**1**.

[0215] That is, in operation S**31** and operation S**32** according to at least one embodiment, at least some of each operation may be simultaneously performed (e.g., in parallel).

[0216] Additionally, the variable generation circuit **113** may transmit the first encryption variable VAR**1** to the encryption circuit **111**.

[0217] In operation S**40**, the electronic circuit **110** encrypts the first data D**1** based on the generated first encryption variable VAR**1**.

[0218] More specifically, referring to FIG. **6** and FIG. **8** together, the electronic circuit **110** (or the scheduler **112**) may encrypt the first data D**1** in response to a determination that the first encryption variable VAR**1** is generated (S**40**).

[0219] In operation S**41**, the scheduler **112** according to at least one embodiment transmits the first encryption request R**1** to the memory device **120**.

[0220] More specifically, the scheduler **112** may transmit the first encryption request R**1** stored in the wait buffer **212** to the memory device **120** in response to a determination that the first preparation signal RS**1** is received from the variable generation circuit **113**.

[0221] Here, the first preparation signal RS**1** may be understood as the signal which is output to the scheduler **112***a* in response to a determination that the first encryption variable VAR**1** is generated by the variable generation circuit **113**.

[0222] Additionally, the memory device **120** may transmit the first data D**1** stored in the first area to the electronic circuit **110** in response to the first encryption request R**1**.

[0223] Therefore, in operation S**42**, the electronic circuit **110** according to at least one embodiment receives the first data D**1** from the memory device **120**.

[0224] Additionally, in operation S**43**, the encryption circuit **111** according to at least one embodiment encrypts the first data D**1** based on the first encryption variable VAR**1**.

[0225] More specifically, the encryption circuit **111** may encrypt the first data D**1** received from the memory device **120** based on the first encryption variable VAR**1** generated through the variable generation circuit **113**.

[0226] Referring to the above-described configurations, when the electronic circuit **110** sequentially receives the first encryption request R**1** and the second encryption request R**2**, the electronic circuit **110** may encrypt the second data D**2** based on the second encryption variable stored in the cache memory **101**.

[0227] Additionally, while the electronic circuit **110** encrypts the second data D**2** based on the previously stored second encryption variable, the electronic circuit **110** may generate the first encryption variable VAR**1** not stored in the cache memory **101**.

[0228] Furthermore, the electronic circuit **110** may encrypt the first data D**1** in response to a determination that the encryption of the second data D**2** is completed and the first encryption variable VAR**1** is generated.

[0229] That is, while the electronic circuit **110** is first performing the encryption in response to the encryption request of which the encryption variable is stored from among the plurality of encryption requests, the electronic circuit **110** may generate the encryption variable in response to the encryption request of which the encryption variable is not stored.

[0230] Therefore, the electronic circuit **110** according to at least one embodiment of the present disclosure may reduce the time required to encrypt the data stored in the memory device **120** in response to the plurality of encryption requests R**1** and R**2** while the size of cache memory **101** (or the electronic circuit **110**) is maintained (and/or reduced).

[0231] FIG. **9** is a flowchart illustrating the memory system including a system-on-chip including a variable acquisition circuit, according to another embodiment.

[0232] Referring to FIG. **9**, a memory system **100**B according to at least one embodiment may include an electronic circuit **110**B, the memory device **120**, and the host **130**.

[0233] Here, the electronic circuit **110**B may communicate with the host **130** through the host interface **131**. Additionally, the electronic circuit **110**A may communicate with the memory device **120** through the memory interface **121**.

[0234] Here, the memory system **100**B of FIG. **9** may be understood as an example of the memory system **100**

illustrated in FIG. **1**A and FIG. **1**B. Accordingly, the same reference numerals are used for configurations which are the same as or substantially the same as the above-described configurations, and descriptions overlapping the above-described contents are omitted for brevity and/or repeated for clarity and/or emphasis.

[0235] The electronic circuit **110**B may include the encryption circuit **111**, the scheduler **112**, and a variable acquisition circuit **913**.

[0236] According to at least one embodiment, the encryption circuit **111** may receive the encryption requests R**1** and R**2** for the memory device **120** from the host **130**.

[0237] For example, the encryption circuit **111** may sequentially receive the first encryption request R**1** for the first data D**1** stored in the first area of the memory device **120** and the second encryption request R**2** for the second data D**2** stored in the second area from the host **130**.

[0238] Additionally, the encryption circuit **111** may transmit the received encryption requests R**1** and R**2** to the scheduler **112**.

[0239] The scheduler **112** may first transmit the second encryption request R**2** of which the second encryption variable is previously stored from among the encryption requests R**1** and R**2** received from the encryption circuit **111**.

[0240] Subsequently, the encryption circuit **111** may encrypt the second data D**2** received from the memory device **120** based on the prestored second encryption variable based on and/or in response to the second encryption request R**2**.

[0241] Additionally, the encryption circuit **111** may transmit the request for generating the encryption variable to the variable acquisition circuit **913** in response to the encryption request of which the encryption variable corresponding to the area requesting encryption is not stored in the cache memory **101**.

[0242] For example, when the first encryption variable VAR**1** is not stored in the cache memory **101**, the encryption circuit **111** may transmit a first acquisition request AR**1** for the first encryption variable VAR**1** to the variable acquisition circuit **913** in response to the first encryption request R**1**.

[0243] The electronic circuit **110**B may include the variable acquisition circuit **913** configured to generate the encryption variable for each of the plurality of areas of the memory device **120**.

[0244] According to at least one embodiment, the variable acquisition circuit **913** may acquire the first encryption variable VAR**1** corresponding to the first area of the memory device **120** in response to the first acquisition request AR**1** transmitted from the encryption circuit **111**.

[0245] The variable acquisition circuit **913** may transmit a first variable request VR**1** requesting the first encryption variable VAR**1** to the memory device **120** in response to the first acquisition request AR**1**.

[0246] Here, the memory device **120** may transmit the first encryption variable VAR**1** of the first area to the variable acquisition circuit **913** (or the electronic circuit **110**) in response to the first variable request VR**1**.

[0247] Accordingly, the variable acquisition circuit **913** may acquire the first encryption variable VAR**1** from the memory device **120**.

[0248] Here, while the encryption circuit **111** encrypts the second data D**2** based on the second encryption variable, the variable acquisition circuit **913** may acquire the first encryption variable VAR**1** from the memory device **120**.

[0249] Furthermore, the variable acquisition circuit **913** may transmit the first encryption variable VAR**1** to the encryption circuit **111** in response to a determination that the first encryption variable VAR**1** is acquired.

[0250] Additionally, in response to a determination that the first encryption variable VAR**1** is acquired, the variable acquisition circuit **913** may transmit the first preparation signal RS**1** including the information that the first encryption variable VAR**1** is acquired to the scheduler **112**.

[0251] Furthermore, the scheduler **112** may transmit the first encryption request R**1** to the memory device **120** in response to the first preparation signal RS**1**.

[0252] Additionally, the encryption circuit **111** may encrypt the first data D**1** received from the memory device **120** based on the first encryption variable VAR**1** based on and/or in response to the first encryption request R**1**.

[0253] Referring to the above-described configurations, while the electronic circuit **110**B is performing the encryption in response to the encryption request of which the encryption variable is stored from among the plurality of encryption requests, the electronic circuit **110**B may acquire the encryption variable in response to the encryption request of which the encryption variable is not stored.

[0254] Therefore, the electronic circuit **110**B according to at least one embodiment of the present disclosure may reduce the time required to encrypt the data stored in the memory device **120** in response to the plurality of encryption requests R**1** and R**2**, while the size of cache memory **101** (or the electronic circuit **110**B) is maintained (and/or reduced).

[0255] As described above, when the electronic circuit **110** (and/or **110**A and/or **110**B) according to at least one embodiment of the present disclosure sequentially receives the first encryption request R**1** and the second encryption request R**2**, the electronic circuit **110** may encrypt the second data D**2** based on the second encryption variable stored in the cache memory **101**.

[0256] Additionally, the electronic circuit **110** (and/or **110**A and/or **110**B) may generate the first encryption variable VAR**1** not stored in the cache memory **101** while the electronic circuit **110** encrypts the second data D**2** based on the previously stored second encryption variable.

[0257] Furthermore, the electronic circuit **110** (and/or **110**A and/or **110**B) may encrypt the first data D**1** in response to a determination that the encryption of the second data D**2** is completed and the first encryption variable VAR**1** is generated.

[0258] That is, while the electronic circuit **110** (and/or **110**A and/or **110**B) is first performing the encryption in response to the encryption request of which the encryption variable is stored, the electronic circuit **110** (and/or **110**A and/or **110**B) may generate the encryption variable in response to the encryption request of which the encryption variable is not stored from among the plurality of encryption requests.

[0259] Through this, the electronic circuit **110** (and/or **110**A and/or **110**B) according to at least one embodiment of the present disclosure may reduce the time required to encrypt the data stored in the memory device **120** in response to the plurality of encryption requests R**1** and R**2**.

[0260] Additionally, the electronic circuit **110** may improve the encryption performance (e.g., the speed) for

encrypting the data stored in the memory device **120** while the size of cache memory **101** (or the electronic circuit **110**) is maintained (or reduced).

[0261] The electronic circuit according to the present disclosure may reduce the time required to encrypt the data stored in the memory device in response to the plurality of encryption requests.

[0262] In addition to the above-described embodiments, embodiments which may be simply designed or easily changed will be included in the present disclosure. Additionally, the present disclosure will also include technologies which may be easily modified and implemented by using embodiments. Therefore, the scope of the present disclosure should not be limited to the above-described embodiments, but should be determined not only by the scope of the claims to be described later but also by those which are equivalent to the scope of the claims of this disclosure.

[0263] In addition, the functional elements described above, such as those including "unit", " . . . er/or", "circuit", "host", "logic", etc., described in the specification refer to elements that process at least one function or operation, and may be implemented as processing circuitry such as hardware, software, or a combination of hardware and software, unless expressly indicated otherwise. For example, the processing circuitry more specifically may include, but is not limited to, electrical components such as at least one of transistors, resistors, capacitors, etc., /or electronic circuits including said components, a central processing unit (CPU), an arithmetic logic unit (ALU), a digital signal processor, a microcomputer, a field programmable gate array (FPGA), a System-on-Chip (SoC), a programmable logic unit, a microprocessor, application-specific integrated circuit (ASIC), etc. and/or may include active and/or passive components such as gates, transistors, resistors, capacitors, etc., and/or electronic circuits including one or more of said components.

[0264] While the present disclosure has been described with reference to example embodiments thereof, it will be apparent to those of ordinary skill in the art that various changes and modifications may be made thereto without departing from the spirit and scope of the present disclosure as set forth in the following claims.

What is claimed is:

1. An electronic circuit configured to communicate with a memory device, comprising:

an encryption circuit including a cache memory storing an encryption variable for some of a plurality of areas of the memory device, and configured to receive a plurality of encryption requests including a first encryption request for first data stored in a first area of the plurality of areas of the memory device and a second encryption request for second data stored in a second area of the plurality of areas of the memory device;

a scheduler configured to transmit the second encryption request to the memory device when a first encryption variable for the first area is not stored in the cache memory and a second encryption variable for the second area is stored in the cache memory; and

a variable generation circuit configured to generate the first encryption variable while the encryption circuit encrypts the second data received from the memory device based on the second encryption variable in response to the second encryption request,

wherein the scheduler transmits the first encryption request to the memory device in response to a determination that the first encryption variable is generated.

2. The electronic circuit of claim **1**, wherein the encryption circuit is configured to:

receive the second data from the memory device; and

encrypt the second data based on the second encryption variable.

3. The electronic circuit of claim **2**, wherein the encryption circuit is configured to:

transmit a first generation request to the variable generation circuit when the first encryption variable is not stored in the cache memory;

acquire the first encryption variable from the variable generation circuit;

receive the first data from the memory device; and

encrypt the first data based on the first encryption variable in response to a determination that the encryption of the second data is completed.

4. The electronic circuit of claim **3**, wherein the variable generation circuit is configured to:

acquire first metadata for the first area from the memory device in response to the first generation request; and

generate the first encryption variable for the first area based on the first metadata.

5. The electronic circuit of claim **4**, wherein the variable generation circuit further includes a random number generation circuit configured to output a random number based on a probability,

wherein the variable generation circuit is configured to generate the first encryption variable based on the random number output from the random number generation circuit and the first metadata.

6. The electronic circuit of claim **4**, wherein the variable generation circuit is configured to store location information on a location of the memory device, at which the first metadata for the first area is stored.

7. The electronic circuit of claim **1**, wherein the scheduler includes:

a request buffer configured to store encryption requests, from among the plurality of encryption requests, received through the encryption circuit;

a wait buffer configured to store encryption requests, from among the plurality of encryption requests, of which an encryption variable for an area requesting encryption is not stored in the cache memory; and

an output circuit configured to sequentially output the encryption requests stored in the request buffer and the wait buffer to the memory device.

8. The electronic circuit of claim **7**, wherein the variable generation circuit is configured to transmit a first preparation signal to the scheduler in response to the determination that the first encryption variable is generated, and

wherein the wait buffer is configured to output the first encryption request to the output circuit in response to the first preparation signal.

9. The electronic circuit of claim **1**, wherein, when the encryption circuit receives a third encryption request for a third area following the first encryption request and the second encryption request, and a third encryption variable for the third area is stored in the cache memory, the scheduler is configured to transmit one of the first encryption request or the third encryption request based on a determination of whether the first encryption is generated such that

the first encryption request is transmitted to the memory device at a time point when encryption of the second area is completed and the first encryption variable is generated; and

the third encryption request is transmitted to the memory device at a time point when the encryption of the second area is completed and the first encryption variable is not generated.

10. The electronic circuit of claim **1**, wherein, when the encryption circuit receives a third encryption request for a third area following the first encryption request and the second encryption request, and a third encryption variable for the third area is not stored in the cache memory,

the variable generation circuit is configured to generate the third encryption variable, and

the scheduler is configured to transmit the third encryption request to the memory device in response to a determination that an encryption of the first area is completed and the third encryption variable is generated.

11. An encrypting method of a memory system including an electrical circuit and a memory device including a plurality of areas, the method comprising:

receiving a plurality of encryption requests including a first encryption request for first data stored in a first area of the plurality of areas and a second encryption request for second data stored in a second area of the plurality of areas;

transmitting the second encryption request to the memory device in response to a determination that a first encryption variable for the first area is not stored in a cache memory of the electrical circuit and a second encryption variable for the second area is stored in the cache memory;

generating the first encryption variable while encrypting the second data received from the memory device based on the second encryption variable; and

encrypting the first data based on the generated first encryption variable.

12. The method of claim **11**, wherein the generating of the first encryption variable further includes:

transmitting a first generation request to a variable generation circuit of the electrical circuit in response to the determination that the first encryption variable is not stored in the cache memory;

receiving first metadata for the first encryption variable from the memory device in response to the first generation request; and

generating the first encryption variable based on the first metadata.

13. The method of claim **12**, wherein the generating of the first encryption variable further includes:

generating a random number, based on a probability, in response to receiving the first metadata; and

generating the first encryption variable based on the first metadata and the random number.

14. The method of claim **11**, wherein the encrypting of the first data further incudes:

transmitting the first encryption request to the memory device in response to a determination that the first encryption variable is generated;

receiving the first data from the memory device; and

encrypting the first data received from the memory device based on the first encryption variable after the encryption of the second data is completed.

15. The method of claim **11**, further comprising:

receiving, after the first encryption request and the second encryption request, a third encryption request for third data stored in a third area of the plurality of areas; and

encrypting one of the first data or the third data based on a determination of whether the first encryption is generated, such that the first data is encrypted based on the first encryption variable at a time point when encryption for the second area is completed and in response to a determination that the first encryption variable is generated and the third data stored in the third area is encrypted based on a third encryption variable stored in the cache memory at a time point when the encryption for the second area is completed and in response to a determination that the first encryption variable is not generated.

16. An electronic circuit configured to communicate with a memory device including plurality of areas, comprising:

an encryption circuit including a cache memory storing an encryption variable for some of the plurality of areas of the memory device and configured to receive a first encryption request for first data stored in a first area of the plurality of areas and a second encryption request for second data stored in a second area of the plurality of areas;

a scheduler configured to transmit the second encryption request to the memory device when a first encryption variable for the first area is not stored in the cache memory and a second encryption variable for the second area is stored in the cache memory; and

a variable acquisition circuit configured to receive the first encryption variable from the memory device,

wherein the electronic circuit is configured such that the encryption circuit encrypts the second data received from the memory device based on the second encryption variable in response to the second encryption request while the variable acquisition circuit receives the first encryption variable, and

wherein the scheduler is configured to transmit the first encryption request to the memory device in response to a determination that the first encryption variable is received by the variable acquisition circuit.

17. The electronic circuit of claim **16**, wherein the encryption circuit is configured to:

receive the second data from the memory device; and

encrypt the second data based on the second encryption variable and the second data.

18. The electronic circuit of claim **17**, wherein the encryption circuit is configured to:

transmit first acquisition request to the variable acquisition circuit in response to a determination that the first encryption variable is not stored in the cache memory;

acquire the first encryption variable through the variable acquisition circuit;

receive the first data from the memory device in response to a determination that encryption of the second data is completed; and

encrypt the first data based on the first encryption variable and the first data.

19. The electronic circuit of claim **16**, wherein the variable acquisition circuit is configured to transmit a first

preparation signal to the scheduler in response to a determination that the first encryption variable is acquired from the memory device, and

wherein the scheduler is configured to transmit the first encryption request to the memory device in response to the first preparation signal.

20. The electronic circuit of claim **18**, wherein, while the encryption circuit encrypts the second data, the variable acquisition circuit is configured to:

transmit a first variable request to the memory device; and

acquire the first encryption variable from the memory device.

* * * * *