(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년07월20일
(11) 등록번호 10-2557993
(24) 등록일자 2023년07월17일

(51) 국제특허분류(Int. Cl.)
G06F 21/72 (2013.01) *G06F 21/78* (2013.01)
(52) CPC특허분류
G06F 21/72 (2013.01)
G06F 21/78 (2013.01)
(21) 출원번호 10-2018-0117870
(22) 출원일자 2018년10월02일
심사청구일자 2021년09월03일
(65) 공개번호 10-2020-0038145
(43) 공개일자 2020년04월10일
(56) 선행기술조사문헌
JP2007115390 A*
KR101032576 B1*
KR1020180091296 A*
US20110314354 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
허인구
경기도 용인시 수지구 달맞이로 23, B동 301호(죽전동, 지동빌라)
서윤범
경기도 화성시 동탄반석로 277, 119동 805호(석우동, 동탄예당마을 우미린제일풍경채)
(뒷면에 계속)
(74) 대리인
리앤목특허법인

전체 청구항 수 : 총 18 항 심사관 : 구대성

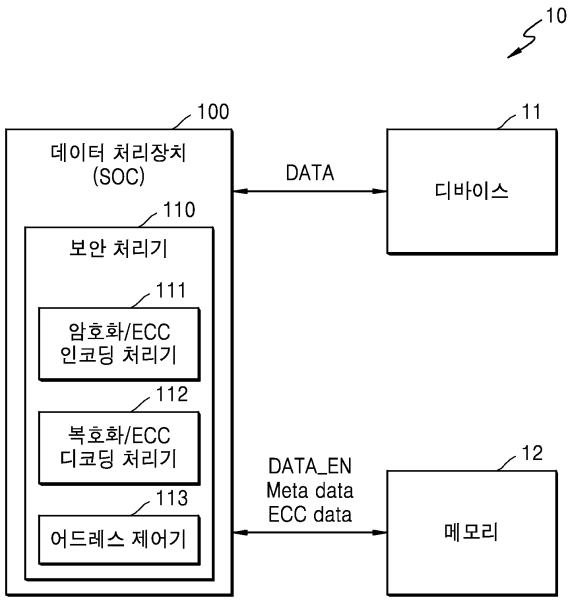
(54) 발명의 명칭 **메모리 이용 효율을 향상한 보안 처리기를 포함하는 시스템 온 칩, 메모리 시스템 및 시스템 온 칩의 동작방법**

(57) 요 약

정보 저장 효율을 향상한 보안 처리기를 포함하는 시스템 온 칩, 메모리 시스템 및 시스템 온 칩의 동작방법이 개시된다. 본 개시의 기술적 사상의 일측면에 따른 시스템 온 칩은 중앙 처리 유닛(CPU) 및 보안 처리기를 구비하고, 상기 보안 처리기는 메타 데이터를 이용하여 데이터에 대한 암호화 동작을 수행하고, 암호화 데이터 및 상

(뒷면에 계속)

대 표 도 - 도1



기 메타 데이터에 대한 ECC 인코딩 처리를 통해 ECC 데이터를 생성하는 암호화/ECC 인코딩 처리기와, 상기 ECC 데이터를 이용한 ECC 디코딩 처리를 통해 상기 암호화 데이터와 상기 메타 데이터를 추출하고, 상기 메타 데이터를 이용하여 상기 암호화 데이터에 대한 복호화 동작을 통해 상기 데이터를 복원하는 복호화/ECC 디코딩 처리기 및 상기 데이터의 저장에 관련된 제1 어드레스를 수신하고 이에 기반하여 제2 어드레스를 생성하며, 상기 제2 어드레스에 따라 상기 메타 데이터 및 상기 ECC 데이터가 메모리 내의 동일 영역에 저장되도록 어드레스 생성 동작을 수행하는 어드레스 제어기를 구비하는 것을 특징으로 한다.

(72) 발명자

정영진

경기도 성남시 분당구 동판교로 156, 914동 503호 (삼평동, 봇들마을9단지금호어울림아파트)

현진수

서울특별시 동작구 사당로27길 130, 108동 401호(사당동, 이수역리가아파트)

명 세 서

청구범위

청구항 1

시스템의 전반적인 동작을 제어하는 중앙 처리 유닛(Central processing unit, CPU); 및

데이터에 대한 암/복호화 동작 및 ECC(Error Correction Code) 동작을 수행하는 보안 처리기를 구비하고,

상기 보안 처리기는,

메타 데이터를 이용하여 데이터에 대한 암호화 동작을 수행하고, 암호화 데이터 및 상기 메타 데이터에 대한 ECC 인코딩 처리를 통해 ECC 데이터를 생성하는 암호화/ECC 인코딩 처리기;

상기 ECC 데이터를 이용한 ECC 디코딩 처리를 통해 상기 암호화 데이터와 상기 메타 데이터를 추출하고, 상기 메타 데이터를 이용하여 상기 암호화 데이터에 대한 복호화 동작을 통해 상기 데이터를 복원하는 복호화/ECC 디코딩 처리기; 및

상기 암호화 데이터의 저장에 관련된 제1 어드레스를 수신하고, 상기 메타 데이터 및 상기 ECC 데이터의 사이즈와 상기 제1 어드레스에 기반하여 제2 어드레스를 생성하며, 상기 제1 어드레스에 따라 상기 암호화 데이터가 어느 하나의 제1 메모리 칩의 제1 영역에 저장되고, 상기 제2 어드레스에 따라 상기 메타 데이터 및 상기 ECC 데이터가 상기 제1 메모리 칩의 상기 제1 영역과 상이한 제2 영역에 저장되도록 어드레스 생성 동작을 수행하는 어드레스 제어기를 구비하는 것을 특징으로 하는 시스템 온 칩.

청구항 2

제1항에 있어서,

외부로부터 상기 데이터에 대한 기록 요청 또는 독출 요청을 수신하고, 상기 어드레스 제어기가 상기 외부로부터의 요청의 종류에 따라 상기 어드레스 생성 동작을 수행하도록 제어 정보를 출력하는 메인 컨트롤러를 더 구비하는 것을 특징으로 하는 시스템 온 칩.

청구항 3

제1항에 있어서,

상기 암호화/ECC 인코딩 처리기로부터 다수의 암호화 데이터들 및 ECC 데이터들을 수신하고, 또한 상기 어드레스 제어기로부터 상기 ECC 데이터들에 대응하는 다수의 제2 어드레스들을 수신하고, 데이터 및 어드레스의 출력 동작을 스케줄링하는 어드레스 스케줄러를 더 구비하는 것을 특징으로 하는 시스템 온 칩.

청구항 4

제3항에 있어서,

상기 암호화/ECC 인코딩 처리기는, 서로 다른 타이밍에 생성되는 상기 메타 데이터 및 상기 ECC 데이터를 저장하는 버퍼를 포함하고, 상기 버퍼에 저장된 상기 메타 데이터 및 상기 ECC 데이터를 병렬하게 상기 어드레스 스케줄러로 제공하는 것을 특징으로 하는 시스템 온 칩.

청구항 5

제3항에 있어서,

상기 어드레스 스케줄러는, 상기 다수의 암호화 데이터들 및 이에 대응하는 제1 어드레스들을 출력하고, 그 이후에 상기 다수의 암호화 데이터들에 대응하는 메타 데이터들 및 ECC 데이터들과 이에 대응하는 제2 어드레스가 출력되도록 스케줄링을 수행하는 것을 특징으로 하는 시스템 온 칩.

청구항 6

제1항에 있어서,

상기 ECC 데이터는, 상기 암호화 데이터를 이용하여 생성된 제1 ECC 데이터와, 상기 메타 데이터를 이용하여 생성된 제2 ECC 데이터를 포함하고,

상기 제1 ECC 데이터 및 상기 제2 ECC 데이터는 상기 제2 어드레스에 응답하여 상기 제1 메모리 칩에 함께 저장되는 것을 특징으로 하는 시스템 온 칩.

청구항 7

제6항에 있어서,

상기 메타 데이터, 상기 제1 ECC 데이터 및 상기 제2 ECC 데이터 중 적어도 일부는 상기 제1 메모리 칩의 동일한 로우에 저장되도록 상기 제2 어드레스가 생성되는 것을 특징으로 하는 시스템 온 칩.

청구항 8

제6항에 있어서,

상기 메타 데이터, 상기 제1 ECC 데이터 및 상기 제2 ECC 데이터 중 적어도 일부는 상기 제1 메모리 칩의 동일한 칼럼에 저장되도록 상기 제2 어드레스가 생성되는 것을 특징으로 하는 시스템 온 칩.

청구항 9

제1항에 있어서,

상기 제1 메모리 칩의 상기 제1 영역과 상기 제2 영역은 논리적으로 구분되고,

상기 제2 어드레스에 의해 상기 메타 데이터 및 상기 ECC 데이터가 동시에 상기 제2 영역에 저장되는 것을 특징으로 하는 시스템 온 칩.

청구항 10

제1항에 있어서,

상기 어드레스 제어기는 상기 생성된 제2 어드레스를 저장하는 어드레스 저장 회로를 포함하고,

상기 데이터에 대한 독출 동작 시, 상기 어드레스 제어기는 상기 데이터의 독출에 관련된 제1 어드레스를 수신하고, 상기 수신된 제1 어드레스에 대응하는 상기 제2 어드레스를 상기 어드레스 저장 회로로부터 독출하여 제공하는 것을 특징으로 하는 시스템 온 칩.

청구항 11

제1항에 있어서,

상기 제1 메모리 칩은 상기 시스템 온 칩의 외부에 배치되고, 상기 제1 메모리 칩과 통신하는 메모리 컨트롤러를 더 구비하고,

암호화 동작이 수행되지 않는 데이터에 대한 저장 동작 시, 상기 데이터는 상기 보안 처리기를 경유함이 없이 상기 메모리 컨트롤러를 통해 상기 제1 메모리 칩으로 제공되고,

암호화 동작이 수행되는 데이터에 대한 저장 동작 시, 상기 데이터는 상기 보안 처리기 및 상기 메모리 컨트롤러를 통해 상기 제1 메모리 칩으로 제공되는 것을 특징으로 하는 시스템 온 칩.

청구항 12

삭제

청구항 13

외부로부터 데이터 및 이에 대응하는 제1 어드레스를 수신하는 단계;

메타 데이터를 이용하여 상기 데이터에 대한 암호화 동작을 수행함으로써 암호화 데이터를 생성하는 단계;

상기 암호화 데이터 및 상기 메타 데이터에 대한 ECC(Error Correction Code) 인코딩 처리를 통해 ECC 데이터를 생성하는 단계; 및

상기 메타 데이터 및 상기 ECC 데이터의 사이즈와 상기 제1 어드레스에 기반하여, 상기 메타 데이터 및 상기 ECC 데이터의 어느 하나의 제1 메모리 칩 내에서의 저장 위치를 나타내는 제2 어드레스를 생성하는 단계를 구비하고,

상기 제1 어드레스는, 상기 암호화 데이터가 상기 제1 메모리 칩의 제1 영역에 저장되도록 하는 정보를 포함하고,

상기 제2 어드레스는, 상기 메타 데이터 및 상기 ECC 데이터가 상기 제1 메모리 칩의 상기 제1 영역과 상이한 제2 영역에 저장되고, 상기 메타 데이터 및 상기 ECC 데이터의 적어도 일부가 상기 제1 메모리 칩 내에서의 동일 로우 또는 동일 칼럼에 저장되도록 하는 정보를 포함하는 것을 특징으로 하는 시스템 온 칩의 동작방법.

청구항 14

제13항에 있어서,

상기 ECC 데이터는, 상기 암호화 데이터를 이용하여 생성된 제1 ECC 데이터와, 상기 메타 데이터를 이용하여 생성된 제2 ECC 데이터를 포함하고,

상기 메타 데이터, 상기 제1 ECC 데이터 및 상기 제2 ECC 데이터가 상기 제1 메모리 칩 내에서의 동일 로우 또는 동일 칼럼에 저장되도록 상기 제2 어드레스가 생성되는 것을 특징으로 하는 시스템 온 칩의 동작방법.

청구항 15

제13항에 있어서,

상기 제2 어드레스를 생성하는 단계는, 암호화 단위의 데이터에 대응하여 생성되는 상기 메타 데이터 및 상기 ECC 데이터를 포함하는 데이터 단위에 대응하여 생성되는 어드레스인 것을 특징으로 하는 시스템 온 칩의 동작방법.

청구항 16

제13항에 있어서,

상기 제2 어드레스를 생성하는 단계는, 상기 제1 어드레스에 대응하여 생성된 상기 제2 어드레스를 저장하는 단계를 포함하고,

상기 제1 어드레스에 대응하는 데이터의 독출 요청을 수신하는 단계;

저장된 어드레스들 중 상기 제1 어드레스에 대응하는 제2 어드레스를 이용하여 상기 메타 데이터 및 상기 ECC 데이터의 적어도 일부를 상기 제1 메모리 칩으로부터 함께 독출하는 단계를 더 구비하는 것을 특징으로 하는 시스템 온 칩의 동작방법.

청구항 17

메모리와 통신하는 메모리 컨트롤러를 포함하는 메모리 시스템에 있어서,

상기 메모리 컨트롤러는,

메타 데이터를 이용하여 데이터에 대한 암호화 동작을 수행하고, 암호화 데이터 및 상기 메타 데이터에 대한 ECC 인코딩 처리를 통해 ECC 데이터를 생성하는 암호화/ECC 인코딩 처리기;

상기 ECC 데이터를 이용한 ECC 디코딩 처리를 통해 상기 암호화 데이터와 상기 메타 데이터를 추출하고, 상기 메타 데이터를 이용하여 상기 암호화 데이터에 대한 복호화 동작을 통해 상기 데이터를 복원하는 복호화/ECC 디코딩 처리기;

상기 암호화 데이터의 저장에 관련된 제1 어드레스를 수신하고, 상기 메타 데이터 및 상기 ECC 데이터의 사이즈와 상기 제1 어드레스에 기반하여 제2 어드레스를 생성하며, 상기 제1 어드레스에 따라 상기 암호화 데이터가 어느 하나의 제1 메모리 칩의 제1 영역에 저장되고, 상기 제2 어드레스에 따라 상기 메타 데이터 및 상기 ECC 데이터가 상기 제1 메모리 칩의 상기 제1 영역과 상이한 제2 영역에 저장되도록 어드레스 생성 동작을 수행하는

어드레스 제어기; 및

상기 제1 및 제2 어드레스에 따라 상기 메모리와 데이터 억세스를 위한 인터페이스를 수행하는 인터페이스 회로를 구비하는 것을 특징으로 하는 메모리 시스템.

청구항 18

제17항에 있어서,

상기 ECC 데이터는, 상기 암호화 데이터를 이용하여 생성된 제1 ECC 데이터와, 상기 메타 데이터를 이용하여 생성된 제2 ECC 데이터를 포함하고,

상기 제1 ECC 데이터 및 상기 제2 ECC 데이터는 상기 제2 어드레스에 응답하여 상기 제1 메모리 칩에 함께 저장되는 것을 특징으로 하는 메모리 시스템.

청구항 19

제17항에 있어서,

상기 메모리 시스템은 상기 제1 메모리 칩을 포함하는 DRAM(Dynamic Random Access Memory) 장치를 더 구비하고,

상기 제1 영역 및 상기 제2 영역은 논리적으로 구분되고, 상기 제2 어드레스에 의해 상기 메타 데이터 및 상기 ECC 데이터가 상기 제2 영역에 저장되는 것을 특징으로 하는 메모리 시스템.

청구항 20

삭제

발명의 설명

기 술 분 야

[0001] 본 개시의 기술적 사상은 시스템 온 칩에 관한 것으로서, 자세하게는 메모리 이용 효율을 향상한 보안 처리기를 포함하는 시스템 온 칩, 메모리 시스템 및 시스템 온 칩의 동작방법에 관한 것이다.

배 경 기 술

[0002] 전자 시스템에서 정보를 저장하는 양이 증대됨에 따라 데이터를 처리하는 시스템 온 칩(System On Chip, SOC) 및 메모리의 개수가 증가하고 있다. 일 예로서, 높은 온도 조건을 견뎌야 함과 함께 정보의 높은 보안이 필요로 되는 자동차(Automotive)향 시스템 온 칩 및 메모리에는 ECC(Error Correction Code) 기능 및 정보에 대한 암/복호화 기능이 적용됨으로써 중요 정보들에 대한 보안 공격으로부터 보호의 필요성이 존재한다.

[0003] 상기와 같은 ECC 기능 및 암/복호화 기능을 적용하기 위해서는 실제 데이터(원본 데이터) 이외에 부가적인 데이터(예컨대, 메타 데이터 및 ECC 데이터 등)가 생성되고 이를 메모리에 저장할 필요가 있다. 그러나, ECC 기능과 암/복호화 기능이 별개로 수행됨에 따라 메타 데이터 및 ECC 데이터가 별도로 관리되며, 이에 따라 메모리 이용 효율성이 저하됨과 함께 부가적인 데이터의 기록/독출 시간의 증가에 따른 시스템 성능의 저하가 발생될 수 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명의 기술적 사상이 해결하려는 과제는, 데이터의 암호화 처리에 소요되는 시간 및 전력을 감소하고 메모리를 효율적으로 이용할 수 있는 보안 처리기를 포함하는 시스템 온 칩, 메모리 시스템 및 시스템 온 칩의 동작 방법을 제공하는 데 있다.

과제의 해결 수단

[0005] 상기와 같은 목적을 달성하기 위하여, 본 개시의 기술적 사상의 일측면에 따른 시스템 온 칩은 중앙 처리 유닛(CPU) 및 데이터에 대한 암/복호화 동작 및 ECC 동작을 수행하는 보안 처리기를 구비하고, 상기 보안 처리기는 메타 데이터를 이용하여 데이터에 대한 암호화 동작을 수행하고, 암호화 데이터 및 상기 메타 데이터에 대한 ECC 인코딩 처리를 통해 ECC 데이터를 생성하는 암호화/ECC 인코딩 처리기와, 상기 ECC 데이터를 이용한 ECC 디코딩 처리를 통해 상기 암호화 데이터와 상기 메타 데이터를 추출하고, 상기 메타 데이터를 이용하여 상기 암호화 데이터에 대한 복호화 동작을 통해 상기 데이터를 복원하는 복호화/ECC 디코딩 처리기 및 상기 데이터의 저장에 관련된 제1 어드레스를 수신하고 이에 기반하여 제2 어드레스를 생성하며, 상기 제2 어드레스에 따라 상기 메타 데이터 및 상기 ECC 데이터가 메모리 내의 동일 영역에 저장되도록 어드레스 생성 동작을 수행하는 어드레스 제어기를 구비하는 것을 특징으로 한다.

발명의 효과

[0006] 본 발명의 기술적 사상의 보안 처리기를 포함하는 시스템 온 칩, 메모리 시스템 및 시스템 온 칩의 동작방법에 따르면, 메모리에 저장되는 정보에 대한 보안 기능이 적용되는 시스템에서 데이터 암/복호화 등의 정보 처리에 소요되는 시간 및 전력을 감소할 수 있는 효과가 있다.

[0007] 또한, 본 발명의 기술적 사상의 보안 처리기를 포함하는 시스템 온 칩, 메모리 시스템 및 시스템 온 칩의 동작방법에 따르면, 다양한 종류의 정보들이 일괄적으로 관리되어 메모리에 저장되거나 메모리로부터 독출될 수 있으므로, 메모리 이용 효율을 향상함과 함께 메모리에 저장되는 정보의 양을 증가시킬 수 있는 효과가 있다.

도면의 간단한 설명

[0008] 도 1은 본 발명의 예시적인 실시예에 따른 시스템 온 칩 및 이를 포함하는 정보 처리 시스템을 나타내는 블록도이다.

도 2는 도 1의 데이터 처리 시스템에서 메모리의 정보 저장의 일 예를 나타내는 블록도이다.

도 3 및 도 4는 메타 데이터 ECC 데이터가 별개로 관리되는 경우와 함께 관리되는 경우에서의 메모리에 저장되는 예를 나타내는 블록도이다.

도 5는 본 발명의 예시적인 실시예에 따른 시스템 온 칩의 동작방법을 나타내는 플로우차트이다.

도 6 및 도 7은 암호화 동작 및 ECC 인코딩 동작의 구체적인 일 예를 나타내는 개념도 및 플로우차트이다.

도 8은 복호화 동작 및 ECC 디코딩 동작의 구체적인 일 예를 나타내는 플로우차트이다.

도 9 및 도 10은 본 발명의 예시적인 실시예에 따른 보안 처리기의 구체적인 구현 예를 나타내는 블록도이다.

도 11은 본 발명의 예시적인 실시예의 보안 처리기의 일 동작 예를 나타내는 블록도이다.

도 12a,b는 본 발명의 예시적인 실시예들에 따라 메타 데이터 및 ECC 데이터가 메모리에 저장되는 일 예를 나타내는 블록도이다.

도 13은 본 발명의 변형 가능한 실시예에 따른 보안 처리기를 나타내는 블록도이다.

도 14는 본 발명의 다른 변형 가능한 실시예에 따른 보안 처리기를 나타내는 블록도이다.

도 15는 본 발명의 예시적인 실시예에 따른 보안 처리기가 사이드밴드 ECC 방식에 적용되는 예를 나타내는 블록도이다.

도 16은 본 발명의 예시적인 실시예에 따른 시스템 온 칩의 일 구현 예를 나타내는 블록도이다.

도 17은 본 발명의 변형 가능한 예시적인 실시예에 따른 시스템 온 칩의 일 구현 예를 나타내는 블록도이다.

도 18은 본 발명의 예시적인 실시예에 따른 보안 처리기가 자동차에 채용되는 자율 주행 시스템 내에 구현되는 예를 나타내는 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0009] 이하, 첨부한 도면을 참조하여 본 발명의 실시 예에 대해 상세히 설명한다.

[0010] Connected Car, V2X, ADAS(Advanced Driver Assistance System)와 같은 기술들로 인해 자동차에 탑재되는 시스

템 온 칩(System On Chip, SOC) 및 메모리의 수가 급격히 증가하고 있다. 메모리로서 DRAM(Dynamic Random Access Memory)을 예로 들면, 자동차 향 DRAM은 타 제품군과는 달리 가혹한 온도조건을 견뎌야 함과 함께 기능적 측면에서의 안전성도 보장될 필요가 있으며, 이에 따라 DRAM에 ECC(Error Correction Code) 기능이 적용될 필요가 있다. 또한, ADAS(Advanced Driver Assistance System)에 채용되는 SOC(예컨대, ADAS SOC)가 처리하는 자율주행 정보, 결제 정보등과 같은 중요 정보들에 해당하므로, 보안 공격으로부터 정보들을 보호하기 위해 암복호화 기능이 적용될 필요가 있다.

[0011] 시스템 온 칩(SOC) 및 메모리에 ECC 기능 및 암호화 기능이 적용될 때, 실제 데이터(예컨대, 원본 데이터)와 함께 부가적인 데이터가 요구로 되고, 원본 데이터를 암호화한 암호화 데이터와 함께 상기 부가적인 데이터가 메모리에 저장될 필요가 있다. 일 예로서, ECC 기능이 적용되는 경우, ECC 알고리즘 및 오류 정정 범위에 따라 32bit 의 데이터 당 최소 1 bit에서 많게는 10 bit 이상의 추가 패리티(Parity) 또는 신드롬(Syndrome)이 필요로될 수 있다. 또한, 암호화 기능이 적용되는 경우, 보다 안전한 암호화를 위해 버전(Version) 정보가 암호화 동작에 이용되거나 충실도 검사(Integrity Check)를 위해 MAC(Message Authentication Code)이 암호화 동작에 작용될 수 있으며, 상기 암호화 동작에 이용되는 메타 데이터(Meta data)들이 암호화 데이터와 함께 메모리에 저장될 수 있다.

[0012] 도 1은 본 발명의 예시적인 실시예에 따른 시스템 온 칩 및 이를 포함하는 정보 처리 시스템을 나타내는 블록도이다. 일 예로서, 정보 처리 시스템(10)은 데이터 처리 장치(100)로서 반도체 칩으로 구현되는 시스템 온 칩, 데이터 처리 장치(100)로 이미지 등의 데이터(DATA)를 전송하는 디바이스(11) 및 메모리(12)를 포함할 수 있다. 디바이스(11)는 다양한 종류의 데이터(DATA)를 제공하는 구성일 수 있으며, 일 예로서 정보 처리 시스템(10)이 자율 운행 시스템(또는, 자율 운행 모듈)에 해당하는 경우 디바이스(11)는 카메라 렌즈를 이용해 촬상 동작을 수행하는 카메라 장치일 수 있다. 또한, 정보 처리 시스템(10)이 자율 운행 시스템에 해당하는 경우 상기 데이터 처리 장치(100)는 ADAS(Advanced Driver Assistance System) SOC 로 지칭될 수 있다.

[0013] 이하의 본 발명의 실시예들에서는 ECC 기능과 암복호화 기능이 통합적으로 수행 및 관리되는 방법이 제시된다. 일 예로, ECC 기능과 암복호화 기능을 통합적으로 수행하는 장치를 통해 각 기능을 위해 요구되는 부가적인 데이터인 ECC 데이터와 메타 데이터를 통합하여 관리함으로써, 메모리(12)의 저장 공간 및 대역폭(Bandwidth)을 효율적으로 활용하는 방법이 제시된다. ECC 데이터와 메타 데이터는 그 용도와 목적이 상이하지만, 실제 메모리(12)로부터 독출되는 타이밍 및 접근 패턴(Access Pattern)은 유사할 수 있다. 이에 따라, ECC 데이터와 메타 데이터를 함께 관리함으로써, 상기 ECC 기능 및 암/복호화 기능을 개별적으로 적용하는 경우에 비해 성능 및 전력 소모의 향상을 가져올 수 있다.

[0014] 메모리(12)는 다양한 종류의 휘발성 메모리 또는 비휘발성 메모리로 구현될 수 있으며, 일 예로서 메모리(12)는 DDR SDRAM(Double Data Rate Synchronous Dynamic Random Access Memory), LPDDR(Low Power Double Data Rate) SDRAM, GDDR(Graphics Double Data Rate) SDRAM, RDRAM(Rambus Dynamic Random Access Memory) 등 다양한 종류의 DRAM으로 구현될 수도 있을 것이다.

[0015] 데이터 처리 장치(100)는 보안 처리기(110)를 포함할 수 있으며, 보안 처리기(110)는 암호화/ECC 인코딩 처리기(111), 복호화/ECC 디코딩 처리기(112) 및 어드레스 제어기(113)를 포함할 수 있다. 암호화/ECC 인코딩 처리기(111)는 데이터 처리 장치(100) 자체적으로 생성한 데이터나 디바이스(11)로부터의 데이터(DATA)에 대한 암호화 동작을 수행할 수 있으며, 데이터 처리 장치(100)의 제어 하에서 암호화 데이터(DATA_EN)가 메모리(12)에 저장될 수 있다.

[0016] 암호화/ECC 인코딩 처리기(111)는 다양한 방식에 따라 암호화 동작을 수행할 수 있다. 일 예로서, AES(Advanced Encryption Standard), DES(Data Encryption Standard) 등의 대칭키 알고리즘에 기반하는 암호화 동작이 수행되거나, RSA(Rivest Shamir Adleman), ECC(Elliptic Curve Cryptography) 등의 비대칭키 알고리즘에 기반하는 다양한 종류의 암호화 동작이 수행될 수 있으며, 본 발명의 실시예들은 상기 암호화 동작의 종류에 한정될 필요는 없다. 또한, 암호화 동작에 관련하여 메타 데이터(Meta data)가 이용될 수 있으며, 상기 메타 데이터(Meta data) 또한 메모리(12)에 저장될 수 있다. 이와 유사하게, 복호화/ECC 디코딩 처리기(112)는 메모리(12)로부터 독출된 암호화 데이터(DATA_EN)에 대한 복호화 동작을 수행하고 이를 통해 원본 데이터를 생성할 수 있다. 일 예로서, 암호화 동작에 적용된 알고리즘을 기반으로 하여 암호화 데이터(DATA_EN) 및 메타 데이터(Meta data)를 이용한 연산을 통해 복호화 처리를 수행함으로써 원본 데이터를 생성할 수 있다.

[0017] 한편, 본 발명의 실시예들에 따라 데이터(DATA)에 대한 보안 기능을 적용함에 있어서 ECC(Error Correction Code) 인코딩 및 디코딩을 포함하는 ECC 동작이 더 적용될 수 있다. 일 예로서, 암호화/ECC 인코딩 처리기(11

1)는 메모리(12)에 대한 기록 동작에서 ECC 인코딩 처리를 수행할 수 있으며, 또한 복호화/ECC 디코딩 처리기(112)는 메모리(12)에 대한 독출 동작에서 ECC 디코딩 처리를 수행할 수 있다. 일 실시예에 따라, 데이터(DATA)의 메모리(12)에 대한 기록 과정에서, 암호화/ECC 인코딩 처리기(111)는 암호화 동작을 먼저 수행한 후, 암호화 데이터(DATA_EN) 및 메타 데이터(Meta data)에 대한 ECC 인코딩 처리를 통해 ECC 데이터(ECC data)를 생성할 수 있으며, ECC 데이터(ECC data)는 암호화 데이터(DATA_EN)에 관련된 제1 ECC 데이터와 메타 데이터(Meta data)에 관련된 제2 ECC 데이터를 포함할 수 있다.

[0018] 데이터 처리 장치(100)는 상기와 같이 생성된 암호화 데이터(DATA_EN), 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 메모리(12)에 저장하기 위한 제어 동작을 수행할 수 있다. 일 예로서, 어드레스 제어기(113)는 메모리(12) 내에서 메타 데이터(Meta data) 및 ECC 데이터(ECC data)가 저장되는 위치를 지시하는 어드레스를 생성할 수 있다. 또한, 어드레스 제어기(113)는 메모리(12) 내에서 암호화 데이터(DATA_EN)가 저장되는 위치를 지시하는 어드레스를 생성할 수 있다.

[0019] 일 예로서, 보안 처리기(110)는 데이터(DATA)에 대한 기록 요청과 함께 메모리(12) 내에서 데이터(DATA)의 저장 위치를 나타내는 제1 어드레스를 수신할 수 있으며, 어드레스 제어기(113)는 제1 어드레스를 기반으로 메타 데이터(Meta data) 및 ECC 데이터(ECC data)의 저장 위치를 나타내는 제2 어드레스를 생성할 수 있다. 예시적인 실시예에 따라, 보안 처리기(110)는 외부로부터의 요청에 따라 암호화 데이터(DATA_EN)를 메모리(12) 내에서 제1 어드레스가 지시하는 위치에 저장되도록 제어 동작을 수행할 수 있다. 변형 가능한 실시예로서, 어드레스 제어기(113)는 제1 어드레스를 기반으로 암호화 데이터(DATA_EN)의 저장 위치를 나타내는 제3 어드레스를 더 생성할 수 있으며, 암호화 데이터(DATA_EN)는 메모리(12) 내에서 제3 어드레스가 나타내는 위치에 저장될 수도 있을 것이다.

[0020] 전술한 실시예에 따라 메타 데이터(Meta data) 및 ECC 데이터(ECC data)가 통합적으로 관리됨에 따라, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)는 제2 어드레스가 지시하는 위치에 함께 저장될 수 있다. 상기 통합적인 관리는, 메타 데이터(Meta data) 및 ECC 데이터(ECC data) 각각에 대한 어드레스 생성이 별개로 수행되는 것이 아니라, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 포함하는 데이터 단위에 대응하여 어드레스를 생성하는 동작을 포함할 수 있다. 상기 제2 어드레스에 의해 지시되는 메모리(12)의 저장 공간의 사이즈에 따라 하나 또는 그 이상의 제2 어드레스가 생성될 수 있으며, 메타 데이터(Meta data) 및 ECC 데이터(ECC data) 중 적어도 일부는 하나의 제2 어드레스에 의해 함께 메모리(12)에 저장될 수 있다.

[0021] 예시적인 실시예에 따라, 메타 데이터(Meta data) 및 ECC 데이터(ECC data) 중 적어도 일부는 메모리(12)의 동일 로우에 위치하는 저장 공간에 저장되거나, 또는 동일 칼럼에 위치하는 저장 공간에 저장될 수 있다. 이에 따라, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 저장함에 소요되는 시간(예컨대, 기록 사이클)이 감소될 수 있으며, 또한 암호화 데이터(DATA_EN)를 복호화하기 위해 이용되는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 독출하는 데 소요되는 시간(예컨대, 독출 사이클)이 감소될 수 있다.

[0022] 한편, 데이터(DATA)에 대한 기록 또는 독출 요청이 수신됨에 따라, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)의 저장을 위한 어드레스를 생성하는 동작이 암호화/ECC 인코딩 처리기(111) 및 복호화/ECC 디코딩 처리기(112)와 무관하게 어드레스 제어기(113)에 의해 수행될 수 있다. 일 예로서, 데이터(DATA)에 대한 기록 동작 시 암호화 데이터(DATA_EN)의 생성에 이용되는 메타 데이터(Meta data)와, ECC 동작에 의해 생성되는 ECC 데이터(ECC data)의 사이즈가 기 설정된 값을 가질 수 있으며, 상기 사이즈에 기반하여 메타 데이터(Meta data)와 ECC 데이터(ECC data)를 일괄적으로 저장하기 위한 제2 어드레스가 생성될 수 있다. 일 실시예에 따라, 메모리(12)의 저장 공간은 제1 및 제2 영역들(미도시)을 포함할 수 있으며, 암호화 데이터(DATA_EN)는 제1 어드레스에 응답하여 제1 영역에 저장되고, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)는 제2 어드레스에 응답하여 제2 영역에 저장될 수 있다.

[0023] 상기와 같은 본 발명의 예시적인 실시예에 따르면, 메타 데이터(Meta data)와 ECC 데이터(ECC data)가 통합하여 관리될 수 있으므로 메모리(12)가 효율적으로 이용될 수 있으며, 또한 억세스 효율이 향상될 수 있다.

[0024] 한편, 도 1에는 암호화/ECC 인코딩 처리기(111)와 복호화/ECC 디코딩 처리기(112)가 별개의 기능 블록으로 도시되었으나, 본 발명의 실시예는 이에 국한될 필요가 없다. 일 예로서, 암호화 처리기, 복호화 처리기, ECC 인코딩 처리기 및 ECC 디코딩 처리기는 각각 별개의 기능 블록으로 도시도어도 무방하다. 또는, 암호화 및 복호화 처리기가 동일한 기능 블록으로 도시되고, ECC 인코딩 처리기 및 ECC 디코딩 처리기가 동일한 기능 블록으로 도시될 수도 있을 것이다.

[0025] 한편, 보안 처리기(110)는 하드웨어 구성 요소들을 포함함으로써 하드웨어적인 신호 처리를 통해 그 기능이 구현될 수 있다. 또는, 보안 처리기(110)는 프로세서가 프로그램을 실행함에 의해 그 기능이 소프트웨어적으로 구현될 수 있으며, 또는 하드웨어와 소프트웨어의 결합을 통해 그 기능이 구현될 수도 있을 것이다.

[0026] 도 2는 도 1의 데이터 처리 시스템에서 메모리의 정보 저장의 일 예를 나타내는 블록도이다.

[0027] 도 1 및 도 2를 참조하면, 어드레스 제어기(113)는 암호화 데이터(DATA_EN)의 저장에 이용되는 제1 어드레스(ADD1)와 메타 데이터(Meta data) 및 ECC 데이터(ECC data)의 저장에 이용되는 제2 어드레스(ADD2)를 제공할 수 있으며, DRAM 등으로 구현 가능한 메모리(12)는 제1 영역 및 제2 영역을 포함할 수 있다. 암호화 데이터(DATA_EN)의 저장에 이용되는 제1 어드레스(ADD1)는 어드레스 제어기(113)에서 생성된 어드레스일 수 있다. 또는, 변형 가능한 예로서, 외부로부터 제1 어드레스(ADD1)가 어드레스 제어기(113)로 제공되고, 어드레스 제어기(113)는 제1 어드레스(ADD1)를 바이패스하여 메모리(12)로 제공할 수도 있다. 도 2에서는, 어드레스 제어기(113)로부터의 제1 어드레스(ADD1) 및 제2 어드레스(ADD2)가 메모리 컨트롤러(120)를 통해 메모리(12)로 제공되는 예가 도시되며, 메모리 컨트롤러(120)는 데이터 처리 장치(100) 내에 구비되는 구성일 수 있다.

[0028] 어드레스 제어기(113)는 외부로부터 제1 어드레스(ADD1)를 수신하고, 상기 제1 어드레스(ADD1)를 이용하여 메타 데이터(Meta data) 및 ECC 데이터(ECC data)의 저장에 이용되는 제2 어드레스(ADD2)를 생성할 수 있다. 일 예로서, 데이터 기록 동작을 예로 들면, 어드레스 제어기(113)는 SOC 내부의 소정의 기능 블록(예컨대, CPU)의 제어 하에서 생성되는 제1 어드레스(ADD1)를 수신할 수 있다.

[0029] 제1 어드레스(ADD1)는 메모리(12) 내에서 암호화 데이터(DATA_EN)가 저장되는 위치를 나타낼 수 있으며, 암호화 동작 및 ECC 동작을 통해 생성되는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)는 암호화 데이터(DATA_EN)에 비해 소정의 비율에 해당하는 사이즈를 가질 수 있다. 어드레스 제어기(113)는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)가 저장되는 제2 영역의 위치 및 저장 공간의 사이즈를 산출할 수 있으며, 산출 결과에 따라 제2 어드레스(ADD2)를 생성하여 메모리 컨트롤러(120)로 제공할 수 있다. 일 예로서, 제2 어드레스(ADD2)는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)의 저장이 시작되는 위치와 함께, 저장에 이용되는 사이즈의 정보를 포함할 수 있다.

[0030] 일 구현 예로서, 어드레스 제어기(113)는 어드레스 산출기(113_1) 및 어드레스 저장 회로(113_2)를 포함할 수 있다. 어드레스 산출기(113_1)는 전술한 제1 어드레스(ADD1), 부가 데이터의 사이즈(또는, 부가 데이터의 데이터 사이즈 대비 비율) 등의 정보를 참조하여 제2 어드레스(ADD2)를 산출할 수 있다. 또한, 어드레스 저장 회로(113_2)는 제1 어드레스(ADD1)에 대응하는 제2 어드레스(ADD2)를 저장할 수 있으며, 상기 제1 어드레스(ADD1)에 대한 데이터 독출 요청이 수신될 때 기 산출되어 저장된 제2 어드레스(ADD2)가 메모리(12)로 제공될 수 있다.

[0031] 메모리 컨트롤러(120)는 메모리(12)와 통신할 수 있으며, 메모리(12)로 커맨드 및 어드레스를 제공함과 함께 소정의 대역폭에 따라 암호화 데이터(DATA_EN), 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 메모리(12)로 전송하고, 또한 메모리(12)로부터 독출할 수 있다. 소정의 정의되는 사이즈 단위에 따라 데이터(DATA)에 대한 암호화 동작이 수행될 수 있으며, 제1 데이터를 예로 들면 제1 데이터를 암호화한 제1 암호화 데이터(DATA_EN_1)는 메모리(12)의 제1 영역에 저장되고, 제1 암호화 데이터(DATA_EN_1)에 대응하는 메타 데이터(Meta data_1) 및 ECC 데이터(ECC data_1)는 메모리(12)의 제2 영역에 저장될 수 있다. 만약 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 합한 사이즈가 메모리(12)와 메모리 컨트롤러(120) 사이의 데이터 대역폭 보다 작은 경우에는, 1 회의 기록 동작을 통해 메타 데이터(Meta data) 및 ECC 데이터(ECC data)가 메모리(12)의 제2 영역에 함께 기록될 수 있다.

[0032] 도 3 및 도 4는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)가 별개로 관리되는 경우와 함께 관리되는 경우에서의 메모리에 저장되는 예를 나타내는 블록도이다.

[0033] 도 3을 참조하면, 암/복호화 동작과 ECC 동작이 별개로 수행되는 경우, 암/복호화기와 ECC 처리기는 분리되어 구현됨에 따라 서로 독립적으로 기능을 수행할 수 있으며, 암/복호화기로부터의 메타 데이터와 ECC 처리기로부터의 ECC 데이터의 저장을 위한 어드레스가 별개로 생성됨에 따라 메타 데이터와 ECC 데이터가 메모리 내에서 서로 무관한 위치에 저장될 수 있다.

[0034] 일 예로서, 데이터의 암호화 동작은 캐쉬 라인 별로 수행될 수 있으며, 하나의 캐쉬 라인이 64B로 구성되고 암호화 알고리즘으로서 128b 단위로 처리되는 블록 암호의 표준인 AES가 이용되는 경우, 하나의 캐쉬 라인의 데이터는 4 개의 128 bit의 암호화 데이터로서 암호화 및 복호화 동작이 수행될 수 있다. 또한, 암호화 동작은 다양한 운용 모드들에 따라 수행될 수 있으며, 일 예로서 CTR(CounTeR) 모드가 이용되는 경우에는 암호화 동작과 관

련하여 이용되는 키 스트림(Key Stream)은 69 bit의 비표(Nonce), 32 bit의 어드레스(Address_ 및 27bit의 버전 카운터(Version Counter)를 포함할 수 있다. 이 때, 27 bit의 버전 카운터(Version Counter)는 해당 캐쉬 라인에 새로운 데이터가 기록될 때마다 증가하므로, 암호화 동작과 관련하여 27 bit의 버전 카운터(Version Counter)는 메타 데이터로서 메모리에 저장될 수 있다.

[0035] 메모리는 다수의 영역들을 포함하고, 일 예로서 제1 영역(암호화 데이터 영역), 제2 영역(메타 데이터 영역) 및 제3 영역(ECC 데이터 영역)을 포함할 수 있다. 128b 단위의 암호화 데이터(Ciphertext)는 제1 영역에 저장될 수 있다. 또한, 암호화 동작과 ECC 동작이 별개로 수행됨에 따라 메타 데이터와 ECC 데이터는 별개의 영역에 저장될 수 있으며, 일 예로서 메타 데이터는 제2 영역에 저장되고 ECC 데이터는 제3 영역에 저장될 수 있다. 또한, 충실도 검사를 위해 64B의 암호화 데이터(Ciphertext)에 대해 56 bit의 메시지 인증 코드(Message Authentication Code, MAC)가 생성될 수 있으며, 버전 카운터 및 MAC이 메타 데이터로서 제2 영역에 저장될 수 있다. MAC은 다양한 알고리즘을 통해 생성될 수 있으며, 일 예로서 SHA, SHA256, SHA384 등의 알고리즘이나 MD5 알고리즘 등이 MAC 생성에 적용될 수 있다. 한편, 암호화 데이터(Ciphertext)의 독출 시 MAC이 함께 독출될 수 있으며, 암호화 데이터(Ciphertext)로부터 계산된 MAC과 메모리로부터 독출된 MAC을 비교함에 의해 위변조 여부가 검출될 수 있다. 일 실시예에 따라, 버전 카운터 및 MAC은 암호화됨이 없이 메모리에 저장될 수 있다.

[0036] 한편, ECC 처리 또한 다양한 종류의 알고리즘에 의해 수행될 수 있으며, 일 예로서 128 bit 단위에 대하여 하나의 에러 정정 및 두 개의 에러 검출이 가능한 SEC-DED(single-bit error correction and double-bit error detection) 적용될 수 있다. SEC-DED 의 예에서, 128 bit 당 9 bit 의 ECC 데이터가 생성될 수 있으며, 64B의 암호화 데이터(Ciphertext)에 대해 36bit의 ECC 데이터가 생성될 수 있다. 또한, ECC 처리는 메타 데이터에 대해서도 수행될 수 있으며, 전체 83bit의 메타 데이터에 대하여 9bit의 ECC 데이터가 생성될 수 있다. 이에 따라, 45bit의 ECC 데이터가 생성되고, 상기 ECC 데이터는 메모리의 제3 영역에 저장될 수 있다. 도 3에 도시된 예에 따르면, 메타 데이터와 ECC 데이터는 서로 무관하게 별개의 영역에 저장될 수 있다. 또한, ECC 처리기는 ECC 인코딩이 수행될 암호화 데이터(Ciphertext)와 메타 데이터를 서로 별개의 데이터로 판단하므로, 암호화 데이터(Ciphertext)에 대한 ECC 데이터(예컨대, 제1 ECC 데이터)와 메타 데이터에 대한 ECC 데이터(예컨대, 제2 ECC 데이터)는 제3 영역 내에서 서로 무관한 위치에 저장될 수 있다.

[0037] 한편, 도 4를 참조하면, 본 발명의 실시예들에 따라 메타 데이터와 ECC 데이터가 통합적으로 관리될 수 있으며, 일 예로서 메타 데이터와 ECC 데이터에 대한 일괄적인 억세스를 위한 어드레스가 생성될 수 있다. 예컨대, 메타 데이터와 제1 ECC 데이터 및 제2 ECC 데이터가 메모리 내의 동일 영역에 집적되어 저장될 수 있으며, 이에 따라 상대적으로 적은 횟수의 억세스를 통해 메타 데이터와 제1 ECC 데이터 및 제2 ECC 데이터가 메모리에 저장되거나 또는 메모리로부터 독출될 수 있다. 일 예로서, 메모리는 암호화 데이터(Ciphertext)를 저장하는 제1 영역을 포함하고, 또한 메타 데이터와 제1 ECC 데이터 및 제2 ECC 데이터는 메모리의 동일한 영역(예컨대, 제2 영역)에 맵핑되도록 어드레스 생성 동작이 제어될 수 있다. 도 4에서는 메모리의 하나의 로우에 구비되는 메모리 사이즈가 56 bit의 MAC, 27bit의 버전 카운터 및 45bit의 ECC 데이터를 합한 사이즈보다 큼에 따라, 상기 메타 데이터 및 ECC 데이터가 메모리의 하나의 로우에 저장되는 예가 도시된다.

[0038] 메모리와 메모리 컨트롤러 사이에서 데이터를 송수신하기 위한 대역폭(예컨대, 데이터 대역폭)은 다양한 사이즈를 가질 수 있으며, 상기 대역폭에 따라 메모리와 메모리 컨트롤러 사이에서의 입출력 단위가 정의될 수 있다. 메타 데이터와 ECC 데이터를 합한 사이즈가 대역폭보다 작음에 따라 메타 데이터와 ECC 데이터가 하나의 입출력 단위로 관리될 수 있으며, 이를 통해 도 3에 도시된 실시예에 비해 데이터의 암호화 및 복호화 처리에서 필요로 되는 메모리의 억세스 횟수가 감소될 수 있다.

[0039] 한편, 도 3 및 도 4의 예에서는 암호화 동작의 예로서 CTR 모드가 예시되었으나, 본 발명의 실시예들은 이에 국한될 필요가 없으며, Electric CodeBook mode(ECB 모드), Cipher Block Chaining mode(CBC 모드), Cipher-FeedBack mode(CFB 모드), Output-FeedBack mode(OFB 모드) 등 다양한 종류의 모드가 적용되어도 무방할 것이다.

[0040] 도 5는 본 발명의 예시적인 실시예에 따른 시스템 온 칩의 동작방법을 나타내는 플로우차트이다. 도 5에서는 데이터 기록 동작이 예시되나, 어드레스 생성 및 데이터 억세스 동작은 데이터 독출 동작에서도 동일 또는 유사하게 수행될 수 있을 것이다.

[0041] 도 5를 참조하면, 시스템 온 칩은 전술한 실시예들에 따른 보안 처리기를 구비하고, 보안 처리기는 데이터에 대한 암/복호화 동작 및 ECC 동작을 수행할 수 있다. 또한, 데이터에 대한 암/복호화 동작 및 ECC 동작을 통해 다양한 종류의 부가 데이터가 생성될 수 있으며, 일 예로서 암/복호화 동작에 관련된 메타 데이터 및 ECC 처리 동

작에 관련된 ECC 데이터가 생성될 수 있다.

[0042] 외부로부터의 데이터 억세스 요청이 시스템 온 칩으로 제공됨에 따라(S11), 시스템 온 칩 내의 구성 요소(예컨대, 중앙 처리 유닛(CPU))는 기록이 수행될 데이터(예컨대, 원본 데이터) 및 데이터의 저장 위치를 나타내는 어드레스(예컨대, 제1 어드레스)를 보안 처리기로 제공할 수 있다. 또한, 보안 처리기는 암호화 데이터의 저장에 이용되는 제1 어드레스를 기반으로 제2 어드레스를 생성할 수 있으며(S12), 일 예로서 제2 어드레스는 원본 데이터에 대응하는 부가 데이터(예컨대, 메타 데이터 및 ECC 데이터)의 사이즈를 고려하여 생성될 수 있다. 예컨대, 제2 어드레스는 메타 데이터 및 ECC 데이터 저장의 시작 위치 및 사이즈 정보를 포함함에 따라, 메모리 컨트롤러는 보안 처리기로부터의 제2 어드레스가 지시하는 위치에 메타 데이터 및 ECC 데이터를 저장할 수 있다.

[0043] 한편, 보안 처리기는 수신된 원본 데이터에 대한 암호화 동작을 통해 암호화 데이터 및 메타 데이터를 생성할 수 있으며(S13), 또한 암호화 데이터 및 메타 데이터에 대한 ECC 인코딩 처리를 통해 ECC 데이터를 생성할 수 있다(S14). 전술한 실시예에서와 같이, ECC 데이터는 암호화 데이터에 대한 ECC 인코딩 처리에 따른 제1 ECC 데이터와 메타 데이터에 대한 ECC 인코딩 처리에 따른 제2 ECC 데이터를 포함할 수 있다.

[0044] 보안 처리기는 메모리를 두 개의 영역으로 관리할 수 있으며, 일 예로서 암호화 데이터가 저장되는 영역(예컨대, 제1 영역)과 메타 데이터 및 ECC 데이터가 저장되는 영역(예컨대, 제2 영역)이 구분되도록 어드레스 생성 동작을 수행할 수 있다. 상기 보안 처리기의 제어에 기반하여, 제1 어드레스에 따라 암호화 데이터는 메모리의 제1 영역에 저장되고(S15), 제2 어드레스에 따라 메타 데이터 및 ECC 데이터는 메모리의 제2 영역에 저장될 수 있다(S16).

[0045] 한편, 전술한 실시예들에 따라, 어느 하나의 암호화 데이터에 대응하는 메타 데이터 및 ECC 데이터는 메모리 내의 동일 로우 또는 동일 칼럼에 저장될 수 있다. 또한, 메모리 컨트롤러와 메모리 사이의 통신에 있어서, 메타 데이터 및 ECC 데이터의 사이즈가 데이터 대역폭 보다 작음에 따라, 어느 하나의 암호화 데이터에 대응하는 메타 데이터 및 ECC 데이터는 1 회의 억세스 동작을 통해 메모리에 저장될 수도 있다.

[0046] 도 6 및 도 7은 암호화 동작 및 ECC 인코딩 동작의 구체적인 일 예를 나타내는 개념도 및 플로우차트이다. 이하의 실시예들에서는, 암호화 동작의 일 예로서 CTR 모드가 예시되나, 전술한 바와 같이 본 발명의 실시예들은 암호화 동작의 종류에 한정될 필요가 없다.

[0047] 도 6에 도시된 바와 같이, 데이터를 암호화하여 메모리에 저장함에 있어서, 기존에 메모리에 저장된 버전 카운터를 독출할 필요가 있으며, 이를 위해 기 저장된 암호화 데이터에 대한 메타 데이터 및 ECC 데이터에 대한 독출 동작이 수행될 수 있다. 또한, 69 bit의 Nonce, 32 bit의 Address 및 27bit의 버전 카운터를 이용하여 데이터에 대한 암호화 동작(예컨대, AES 알고리즘을 이용한 암호화 동작)에 이용되는 128 bit의 키 스트림을 생성할 수 있으며, 128 bit의 원본 데이터(Plaintext)와 128 bit의 키 스트림을 이용한 연산(예컨대, XOR)을 통해 암호화 데이터(Ciphertext)가 생성될 수 있다. 또한, 27bit의 버전 카운터에 대한 9 bit의 ECC 데이터와 함께, 128 bit의 암호화 데이터(Ciphertext)에 대한 36 bit의 ECC 데이터가 생성될 수 있으며, 또한 128 bit의 암호화 데이터(Ciphertext)와 MAC 키를 통한 연산에 의해 56 bit의 MAC이 생성될 수 있다.

[0048] 상기와 같은 암호화 동작 및 ECC 인코딩 동작에 따른 전체 플로우는 도 7에 도시된 바와 같다. 예컨대, 128 bit * 4 에 해당하는 데이터(예컨대, 제1 내지 제4 데이터)의 암호화 동작을 예로 들면, 메타 데이터 및 ECC 데이터가 메모리로부터 독출되고(S21), ECC 디코딩 동작을 통해 메타 데이터가 추출되며(S22), 버전 카운터를 포함하는 키 스트림 생성 동작이 수행될 수 있다(S23). 또한, 키 스트림을 이용한 암호화 동작이 수행되고(S24), 제1 암호화 데이터에 대한 ECC 인코딩 동작이 수행되고(S25), 제1 암호화 데이터가 메모리에 기록될 수 있다(S26).

[0049] 이와 유사하게, 제2 암호화 데이터에 대한 ECC 인코딩 동작 및 제2 암호화 데이터의 기록 동작이 수행되며(S27, S28), 제3 암호화 데이터에 대한 ECC 인코딩 동작 및 제3 암호화 데이터의 기록 동작이 수행되며(S29, S30), 또한 제4 암호화 데이터에 대한 ECC 인코딩 동작 및 제4 암호화 데이터의 기록 동작이 수행될 수 있다(S31, S32). 또한, 전술한 실시예들에 따라 암호화 데이터를 이용한 MAC 연산을 통해 MAC이 생성되고(S33), 버전 카운터 및 MAC을 포함하는 메타 데이터에 대한 ECC 인코딩 동작이 수행되며(S34), 상기 생성된 메타 데이터와 ECC 데이터가 메모리에 저장될 수 있다.

[0050] 데이터 처리에 있어서 도 7에 도시된 플로우에서 데이터의 기록 및 독출 동작이 통상적으로 많은 시간과 전력이 소모로 될 수 있으나, 본 발명의 예시적인 실시예에 따르면 메타 데이터 및 ECC 데이터가 메모리로부터 일괄적으로 독출될 수 있으며, 또한 메타 데이터와 ECC 데이터가 메모리에 일괄적으로 저장될 수 있으므로, 데이터 처리에 있어서 소요되는 시간 및 전력이 감소될 수 있다.

[0051] 도 8은 복호화 동작 및 ECC 디코딩 동작의 구체적인 일 예를 나타내는 플로우차트이다. 본 발명의 실시예에 적용될 수 있는 복호화 동작 및 ECC 디코딩 동작의 개념은 전술한 도 6에서의 암호화 동작 및 ECC 인코딩 동작의 역순으로 수행될 수 있으므로, 이에 대한 구체적인 도시는 생략된다.

[0052] 도 8에 도시된 바와 같이, 예컨대, 128 bit * 4 에 해당하는 암호화 데이터에 대한 복호화 동작을 예로 들면, 버전 카운터 및 MAC을 포함하는 메타 데이터와 ECC 데이터가 메모리로부터 함께 독출될 수 있으며(S41), 함께 독출된 정보는 보안 처리기가 일시적으로 보유할 수 있다. 또한, ECC 디코딩 동작을 통해 메타 데이터가 추출되며(S42), 버전 카운터를 포함하는 키 스트림 생성 동작이 수행될 수 있다(S43). 또한, 메모리로부터 ECC 인코딩된 제1 암호화 데이터가 독출되고(S44), ECC 디코딩 동작을 수행함에 의해 제1 암호화 데이터가 추출될 수 있다(S45). 이와 유사하게, 제2 암호화 데이터에 대한 독출 동작 및 ECC 디코딩 동작을 통해 제2 암호화 데이터가 추출되고(S46, S47), 제3 암호화 데이터에 대한 독출 동작 및 ECC 디코딩 동작을 통해 제3 암호화 데이터가 추출되고(S48, S49), 또한 제4 암호화 데이터에 대한 독출 동작 및 ECC 디코딩 동작을 통해 제4 암호화 데이터가 추출될 수 있다(S50, S51). 또한, 전술한 실시예들에 따라 암호화 데이터를 이용한 MAC 연산을 통해 MAC이 생성되고, 생성된 MAC과 메모리로부터 독출된 MAC에 대한 비교 동작이 수행될 수 있으며(S52), 키 스트림을 이용한 복호화 동작이 수행될 수 있다(S53).

[0053] 상기와 같은 실시예에 따르면, 메타 데이터, 암호화 데이터에 대한 ECC 데이터 및 메타 데이터에 대한 ECC 데이터를 독출하기 위한 과정이 하나의 독출 동작을 통해 처리될 수 있으며, 이에 따라 메모리의 억세스 회수가 감소될 수 있고, 이를 통해 암호화 데이터의 복호화 과정에서 소요되는 시간 및 전력이 감소될 수 있다.

[0054] 도 9 및 도 10은 본 발명의 예시적인 실시예에 따른 보안 처리기의 구체적인 구현 예를 나타내는 블록도이다.

[0055] 도 9를 참조하면, 보안 처리기(300)는 메인 컨트롤러(310), 암호화 및 ECC 인코딩 모듈(320), 복호화 및 ECC 디코딩 모듈(330), 어드레스 생성기(340) 및 어드레스/데이터 스케줄러(350)를 구비할 수 있다. 암호화 및 ECC 인코딩 모듈(320)은 도 1의 암호화/ECC 인코딩 처리기(111)에 상응하고, 복호화 및 ECC 디코딩 모듈(330)은 도 1의 복호화/ECC 디코딩 처리기(112)에 상응하는 구성일 수 있다. 또한, 어드레스 생성기(340)는 도 1의 어드레스 제어기(113)에 포함되는 구성일 수 있다.

[0056] 예시적인 실시예에 따라 보안 처리기(300)는 시스템 온 칩(또는, ADAS SOC) 내에 구비되는 구성일 수 있으며, 시스템 온 칩 내에 구비되는 CPU(미도시)에 의해 보안 처리기(300)의 동작이 제어될 수 있다. 또는, 변형 가능한 실시예에 따라, 보안 처리기(300)는 메모리를 제어하는 메모리 컨트롤러에 구비되는 구성일 수도 있다. 또는, 변형 가능한 실시예에 따라, 시스템 온 칩은 보안 처리기(300) 및 메모리 컨트롤 모듈을 포함할 수 있으며, 도 9에 도시된 구성들 중 일부의 구성은 보안 처리기(300) 내에 구비되고, 다른 일부의 구성은 메모리 컨트롤 모듈 내에 구비될 수도 있을 것이다.

[0057] 시스템 온 칩은 외부의 디바이스로부터 데이터의 독출 및 저장을 요청받을 수 있으며, 본 발명의 실시예들에 따라 보안 처리기(300)는 저장이 요청된 원본 데이터에 대해 암호화 동작 및 ECC 인코딩 처리를 수행함으로써 암호화 데이터를 메모리(미도시)에 저장할 수 있으며, 또한 메모리로부터 암호화 데이터를 독출하고 독출된 암호화 데이터에 대한 복호화 동작 및 ECC 디코딩 처리를 통해 원본 데이터를 생성하여 이를 시스템 온 칩 내부에서 이용하거나 또는 원본 데이터를 외부의 디바이스로 제공할 수 있다. 메인 컨트롤러(310)는 보안 처리기(300)가 본 발명의 실시예들에 따른 동작을 수행할 수 있도록 보안 처리기(300) 내부의 전반적인 동작을 제어할 수 있다.

[0058] 시스템 온 칩으로 데이터 억세스 요청이 제공됨에 따라, 보안 처리기(300)는 시스템 온 칩의 내부 구성(예컨대, CPU)으로부터 제1 어드레스(ADD1) 및 기록 데이터(Write Data)를 수신하고, 또한 독출 데이터(Read Data)를 제공할 수 있다. 어드레스 생성기(340)는 전술한 실시예들에 따라 제1 어드레스(ADD1)로부터 메타 데이터(Meta data) 및 ECC 데이터(ECC data)가 저장될 위치를 나타내는 제2 어드레스(ADD2)를 산출할 수 있으며, 외부로부터의 제1 어드레스(ADD1)와 어드레스 생성기(340)로부터의 제2 어드레스(ADD2)가 어드레스/데이터 스케줄러(350)로 제공될 수 있다. 변형 가능한 실시예에 따라, 어드레스 생성기(340)는 외부로부터의 제1 어드레스(ADD1)에 기반하여 암호화 데이터가 저장될 위치를 나타내는 어드레스를 새로이 생성할 수 있으며, 새로이 생성된 어드레스가 어드레스/데이터 스케줄러(350)로 제공될 수도 있을 것이다.

[0059] 전술한 실시예들에 따라, 데이터의 독출 및 기록 동작에서 메모리에 대한 억세스 회수가 다를 수 있으며, 일 예로서 데이터의 기록 동작의 경우 원본 데이터에 대한 암호화 동작을 위해 필요로 되는 메타 데이터가 메모리로부터 독출되는 과정이 추가될 수 있다. 메인 컨트롤러(310)는 데이터의 독출 또는 기록 동작에 따라 메모리 억

세스 동작이 달라질 수 있으므로, 독출 또는 기록 동작에 기반하는 제어 정보를 어드레스 생성기(340)로 제공할 수 있다. 즉, 어드레스 생성기(340)는 제1 어드레스(ADD1) 및 제어 정보에 기반하여 적어도 하나의 어드레스를 산출하고 이를 저장할 수 있다. 또한, 외부로부터의 독출 요청에 따른 제1 어드레스(ADD1)가 수신될 때, 어드레스 생성기(340)는 내부에 저장된 어드레스 정보를 참조로 하여 제1 어드레스(ADD1)에 대응하는 적어도 하나의 어드레스를 생성하고 이를 어드레스/데이터 스케줄러(350)로 제공할 수 있다.

[0060] 한편, 암호화 및 ECC 인코딩 모듈(320)은 전술한 실시예들에 따라 데이터에 대한 암호화 동작 및 ECC 인코딩 처리를 수행할 수 있으며, 암호화 데이터, 메타 데이터 및 ECC 데이터를 어드레스/데이터 스케줄러(350)로 제공할 수 있다. 또한, 복호화 및 ECC 디코딩 모듈(330)은 메모리로부터 독출된 암호화 데이터, 메타 데이터 및 ECC 데이터를 이용하여 복호화 동작 및 ECC 디코딩 처리를 수행할 수 있으며, 또한 충실도 검사를 위한 MAC 생성 및 비교 동작을 수행할 수 있다.

[0061] 메인 컨트롤러(310)는 어드레스 생성기(340)에 대한 제어 동작과 함께, 암/복호화 동작 및 ECC 동작에 관련된 전체 과정을 제어할 수 있다. 일 예로서, 암/복호화 동작을 위한 정보를 관리하거나, 보안 처리 결과에 따른 경고(alarm) 동작을 관리하거나, 또는 ECC 동작을 통해 발견된 에러에 대한 관리 동작을 수행할 수 있다.

[0062] 한편, 어드레스/데이터 스케줄러(350)는 메모리 동작과 관련하여 버스 트랜잭션(Bus Transaction)을 스케줄링할 수 있다. 일 예로서, 외부의 디바이스로부터 다수의 데이터들에 대한 억세스 요청들이 제공될 수 있으며, 어드레스/데이터 스케줄러(350)는 다수의 암호화 데이터들 및 이에 대응하는 메타 데이터 및 ECC 데이터가 메모리에 저장되거나 메모리로부터 독출될 수 있도록 데이터 및 어드레스에 대한 출력 동작을 스케줄링할 수 있다. 어드레스/데이터 스케줄러(350)로부터의 데이터 및 어드레스는 메모리 컨트롤러(미도시)를 통해 외부의 메모리로 제공될 수 있다.

[0063] 한편, 도 9에 도시된 보안 처리기(300)의 기능은 하드웨어적인 회로 또는 소프트웨어적으로 수행될 수 있으며, 또는 하드웨어 및 소프트웨어의 조합에 의해 수행될 수도 있을 것이다. 일 예로서, 보안 처리기(300)의 기능이 소프트웨어적으로 수행되는 경우, 메인 컨트롤러(310)는 프로그램을 실행할 수 있는 프로세서를 포함할 수 있으며, 보안 처리기(300) 내부 또는 외부의 메모리에 로딩된 프로그램을 실행함에 의해 전술한 실시예에서의 기능들이 수행될 수 있을 것이다.

[0064] 도 10에는 암호화 및 ECC 인코딩 모듈(320)과 복호화 및 ECC 디코딩 모듈(330)의 구체적인 일 구현 예가 도시된다. 도 10을 참조하면, 암호화 및 ECC 인코딩 모듈(320)은 암호화 엔진(321), MAC 생성기(322) 및 ECC 인코더(323)를 포함할 수 있다. 또한, 복호화 및 ECC 디코딩 모듈(330)은 복호화 엔진(331), MAC 생성기(332), MAC 비교기(333) 및 ECC 디코더(334)를 포함할 수 있다. ECC 인코더(323)는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 일괄적으로 어드레스/데이터 스케줄러(350)로 제공하기 위한 기능(예컨대, wrapping)을 수행할 수 있으며, 일 예로서 그 내부에 버퍼가 구비됨에 따라 순차적으로 수신되는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 상기 버퍼에 저장하고, 버퍼에 저장된 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 일괄적으로 어드레스/데이터 스케줄러(350)로 제공할 수 있다. 이와 유사하게, 복호화 및 ECC 디코딩 모듈(330)은 일괄적으로 독출된 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 일시 저장하는 버퍼를 구비하고, 서로 다른 타이밍에 메타 데이터(Meta data) 및 ECC 데이터(ECC data)를 대응하는 처리 블록으로 제공하는 기능(예컨대, unwrapping)을 수행할 수 있다.

[0065] 도 11은 본 발명의 예시적인 실시예의 보안 처리기의 일 동작 예를 나타내는 블록도이다.

[0066] 도 11을 참조하면, 보안 처리기는 어드레스/데이터 스케줄러(400)를 포함하고, 데이터 기록 동작 시 전술한 실시예들에 따른 암호화 데이터, 메타 데이터, ECC 데이터 및 어드레스를 수신할 수 있다. 일 예로, 서로 다른 암호화 데이터로서 제1 암호화 데이터(DATA_EN_1)와 함께, 이에 대응하는 제1 메타 데이터(Meta data_1) 및 제1 ECC 데이터(ECC data_1)가 어드레스/데이터 스케줄러(400)로 제공될 수 있다. 또한, 그 이후에 제2 암호화 데이터(DATA_EN_2) 및 이에 대응하는 제2 메타 데이터(Meta data_2) 및 제2 ECC 데이터(ECC data_2)가 어드레스/데이터 스케줄러(400)로 제공될 수 있다. 이와 함께, 어드레스 생성기(미도시)로부터 어드레스들이 어드레스/데이터 스케줄러(400)로 더 제공될 수 있다.

[0067] 어드레스/데이터 스케줄러(400)는 메모리에 대한 저장 동작에 관련하여 데이터 및 어드레스의 출력 동작을 스케줄링할 수 있다. 일 예로서, 제1 메타 데이터(Meta data_1) 및 제1 ECC 데이터(ECC data_1)와 제2 메타 데이터(Meta data_2) 및 제2 ECC 데이터(ECC data_2)를 합한 사이즈가 메모리 컨트롤러와 메모리(이상, 미도시) 사이의 대역폭보다 작은 경우에는, 상기 메타 데이터들 및 ECC 데이터들이 함께 메모리에 저장될 수 있도록 스케줄

링이 수행될 수 있다. 일 예로서, 어드레스/데이터 스케줄러(400)는 제1 암호화 데이터(DATA_EN_1)와 이에 대응하는 제1 어드레스(ADD1_1), 제2 암호화 데이터(DATA_EN_2)와 이에 대응하는 제1 어드레스(ADD1_2)를 출력하고 난 후, 상기 제1 및 제2 암호화 데이터들(DATA_EN_1, DATA_EN_2)에 관련된 상기 메타 데이터들 및 ECC 데이터들과 이에 대응하는 제2 어드레스(ADD2)를 출력할 수 있다. 즉, 어드레스/데이터 스케줄러(400)의 스케줄링에 기반하여, 적어도 두 개의 암호화 데이터들에 관련된 메타 데이터들 및 ECC 데이터들이 일괄적으로 메모리에 저장되거나 메모리로부터 독출될 수 있다.

[0068] 도 12a,b는 본 발명의 예시적인 실시예들에 따라 메타 데이터 및 ECC 데이터가 메모리에 저장되는 일 예를 나타내는 블록도이다.

[0069] 도 12a를 참조하면, 데이터 암호화 동작에 따라 암호화 데이터(DATA_EN)가 생성되고, 암호화 데이터(DATA_EN)는 메모리로서 DRAM의 제1 영역에 저장될 수 있다. 또한, 암호화 데이터(DATA_EN)에 대응하는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)는 어드레스 생성 동작에 기반하여 메모리의 제2 영역에 저장될 수 있다.

[0070] 만약, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)가 상대적으로 적은 개수의 로우에 저장되도록 어드레스 생성 동작이 수행되는 경우, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)의 적어도 일부는 동일한 로우에 저장될 수 있다. 일 예로서, ECC 데이터(ECC data)가 암호화 데이터(DATA_EN)에 대한 제1 ECC 데이터(ECC data_1)와 메타 데이터(Meta data)에 대한 제2 ECC 데이터(ECC data_2)를 포함할 때, 어드레스 생성기로부터의 로우 어드레스(R_ADD2_1)에 응답하여 메타 데이터(Meta data)와 제1 ECC 데이터(ECC data_1)가 동일한 로우에 저장되고, 또한 어드레스 생성기로부터의 로우 어드레스(R_ADD2_2)에 응답하여 제2 ECC 데이터(ECC data_2)가 인접한 로우에 저장될 수 있을 것이다.

[0071] 한편, 도 12b는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)가 상대적으로 적은 개수의 칼럼에 저장되도록 어드레스 생성 동작이 수행되는 경우가 예시되며, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)의 적어도 일부는 동일한 칼럼에 저장될 수 있다. 일 예로서, 어드레스 생성기로부터의 칼럼 어드레스(C_ADD2_1)에 응답하여 메타 데이터(Meta data)와 제1 ECC 데이터(ECC data_1)가 동일한 칼럼에 저장되고, 또한 어드레스 생성기로부터의 칼럼 어드레스(C_ADD2_2)에 응답하여 제2 ECC 데이터(ECC data_2)가 인접한 칼럼에 저장될 수 있을 것이다.

[0072] 본 발명의 실시예들은 도 12a,b에 도시된 저장 방식에 한정될 필요는 없으며, 메타 데이터 및 ECC 데이터의 사이즈를 고려하여 더 많은 개수의 로우 또는 칼럼들에 저장될 수도 있을 것이며, 또한 동일한 로우나 동일한 칼럼에 저장되는 데이터의 종류는 가변될 수도 있을 것이다.

[0073] 도 13은 본 발명의 변형 가능한 실시예에 따른 보안 처리기를 나타내는 블록도이다. 도 13에서는 데이터에 대한 암호화 동작이 선택적으로 적용되는 예가 도시된다.

[0074] 도 13을 참조하면, 보안 처리기(500)는 메인 컨트롤러(510), 어드레스 생성기(520), 암호화 및 ECC 인코딩 모듈(530) 및 어드레스/데이터 스케줄러(540)를 구비할 수 있다. 또한, 메인 컨트롤러(510)는 보안 처리기(500)의 전반적인 동작을 제어할 수 있으며, 암호화 및 ECC 인코딩 모듈(530)은 암호화 엔진(531), MAC 생성기(532) 및 ECC 인코더(533)를 포함할 수 있다.

[0075] 데이터를 메모리에 저장함에 있어서, 상기 데이터에 대한 암호화 처리 여부는 보안 처리기(500)가 판단하거나, 또는 보안 처리기(500)를 포함하는 시스템 온 칩(미도시)이 판단할 수 있다. 시스템 온 칩이 암호화 여부를 판단하는 것으로 가정할 때, 데이터에 대한 기록 동작에 있어서 암호화 여부를 나타내는 정보(Info_EN)가 메인 컨트롤러(510)로 제공될 수 있으며, 메인 컨트롤러(510)는 상기 정보(Info_EN)에 기반하여 암호화 및 ECC 인코딩 모듈(530)의 동작을 제어할 수 있다.

[0076] 일 예로서, 제1 데이터(DATA1)에 대해서는 암호화 동작이 수행되고, 제2 데이터(DATA2)에 대해서는 암호화 동작이 수행되지 않는 경우를 가정하면 다음과 같다. 암호화 엔진(531)은 제1 데이터(DATA1)에 대해 암호화 동작을 수행하고, 암호화 데이터를 MAC 생성기(532)로 제공함과 함께, 암호화 데이터 및 메타 데이터(예컨대, 버전 카운터 등의 정보)를 ECC 인코더(533)로 제공할 수 있다. 또한, MAC 생성기(532)로부터의 MAC은 메타 데이터로서 ECC 인코더(533)로 제공될 수 있으며, ECC 인코더(533)는 암호화 데이터에 대한 제1 ECC 데이터 및 메타 데이터에 대한 제2 ECC 데이터를 생성할 수 있다. 한편, 제2 데이터(DATA2)에 대해서는 암호화 동작이 수행됨이 없이 ECC 인코더(533)가 제2 데이터(DATA2)에 대한 ECC 데이터를 생성할 수 있다.

[0077] 메인 컨트롤러(510)는 상기 정보(Info_EN)에 기반하여 어드레스 생성기(520)의 동작을 제어할 수 있다. 어드레스 생성기(520)는 전술한 실시예들에 따라 제1 및 제2 데이터들(DATA1, DATA2)의 저장에 관련된 어드레스(예컨

대, 제1 어드레스)를 이용하여 제2 어드레스를 산출할 수 있으며, 제1 데이터(DATA1)에 관련하여서는 메타 데이터 및 ECC 데이터의 저장을 위한 제2 어드레스(ADD2_1)를 산출할 수 있으며, 반면에 제2 데이터(DATA2)에 관련하여서는 ECC 데이터의 저장을 위한 제2 어드레스(ADD2_2)를 산출할 수 있다. 상기와 같이 생성된 데이터 및 어드레스는 어드레스/데이터 스케줄러(540)로 제공될 수 있다.

[0078] 어드레스 생성기(520)는 제1 데이터(DATA1)에 관련된 제2 어드레스(ADD2_1)를 생성함에 있어서 더 많은 데이터의 저장을 위한 정보를 갖도록 어드레스 생성 동작을 수행할 수 있다. 반면에, 제2 데이터(DATA2)에 관련된 제2 어드레스(ADD2_2)를 생성하는 경우에는 상대적으로 작은 데이터의 저장을 위한 정보를 갖도록 어드레스 생성 동작을 수행할 수 있다. 이에 따라, 암호화 동작이 수행되지 않는 경우에는 더 많은 데이터들에 관련된 ECC 데이터가 메모리의 동일 로우 또는 동일 칼럼에 저장될 수 있다. 또한, 전술한 실시예들에 따라 어드레스/데이터 스케줄러(540)는 어드레스 및/또는 데이터의 출력의 순서를 조절할 수 있으며, 암호화 동작이 수행되지 않는 경우에는 상대적으로 많은 수의 데이터들 및 이에 대응하는 어드레스를 출력한 후, 상기 많은 수의 데이터들에 관련된 ECC 데이터들이 일괄적으로 메모리로 함께 제공될 수 있도록 스케줄링을 수행할 수 있을 것이다.

[0079] 도 14는 본 발명의 다른 변형 가능한 실시예에 따른 보안 처리기를 나타내는 블록도이다.

[0080] 도 14를 참조하면, 보안 처리기(600)는 메인 컨트롤러(610), 어드레스 생성기(620), 암호화 및 ECC 인코딩 모듈(630) 및 복호화 및 ECC 디코딩 모듈(630)를 구비할 수 있다. 또한, 메인 컨트롤러(610)는 보안 처리기(600)의 전반적인 동작을 제어할 수 있으며, 보안 처리기(600) 또는 보안 처리기(600)를 포함하는 시스템 온 칩의 제어에 기반하여 암/복호화 동작에 이용되는 알고리즘 및 ECC 동작에 이용되는 알고리즘이 선택될 수 있다. 또한, 암/복호화 동작에 이용되는 알고리즘 및 ECC 동작에 이용되는 알고리즘에 따라 메타 데이터의 사이즈가 변동될 수 있으며, 또한 ECC 데이터의 사이즈가 변동될 수 있다.

[0081] 메인 컨트롤러(610)의 제어에 기반하여 상기 알고리즘의 종류가 선택됨에 따라, 메인 컨트롤러(610)는 암호화 및 ECC 인코딩 모듈(630)로 암호화 알고리즘 정보(Algo_EN)와 ECC 인코딩 알고리즘 정보(Algo_ECC_E)를 제공할 수 있다. 또한, 메인 컨트롤러(610)는 복호화 및 ECC 디코딩 모듈(630)로 복호화 알고리즘 정보(Algo_DE)와 ECC 디코딩 알고리즘 정보(Algo_ECC_D)를 제공할 수 있다. 또한, 메인 컨트롤러(610)는 상기 선택된 알고리즘에 따라 암호화 동작 및 ECC 동작에서 생성되는 부가 데이터의 사이즈에 관련된 정보(Info_size)를 어드레스 생성기(620)로 제공할 수 있으며, 어드레스 생성기(620)는 제2 어드레스를 생성함에 있어서 상기 정보(Info_size)를 더 참조할 수 있다.

[0082] 만약, 제1 데이터에 대해 상대적으로 많은 제1 사이즈를 갖는 부가 데이터가 생성되고, 제2 데이터에 대해 상대적으로 작은 제2 사이즈를 갖는 부가 데이터가 생성되는 경우를 가정하면, 어드레스 생성기(620)는 서로 다른 사이즈의 부가 데이터를 생성하기 위한 제2 어드레스들(ADD2_1, ADD2_2)을 각각 생성할 수 있다. 일 예로서, 부가 데이터의 사이즈가 작은 경우에는, 메타 데이터 및 ECC 데이터가 상대적으로 적은 개수의 로우 또는 칼럼에 저장될 수 있으며, 또한 더 많은 데이터들에 관련된 부가 데이터(메타 데이터 및 ECC 데이터)가 메모리의 동일 로우 또는 동일 칼럼에 저장될 수 있을 것이다. 또한, 전술한 실시예들에 따라 부가 데이터의 사이즈에 기반하여 어드레스/데이터 스케줄러(미도시)의 스케줄링 동작이 변동될 수도 있을 것이다.

[0083] 도 15는 본 발명의 예시적인 실시예에 따른 보안 처리기가 사이드밴드(Sideband) ECC 방식에 적용되는 예를 나타내는 블록도이다.

[0084] 전술한 실시예들에서, 암호화 데이터와 부가 데이터는 동일한 메모리(예컨대, 동일한 DRAM 칩) 내에서 서로 다른 영역에 저장되는 예가 제시되었으며, 이는 메모리의 공간을 논리적으로 나누어 ECC 데이터의 저장 공간을 할당하는 In-line ECC 방식에 상응할 수 있다. 한편, 본 발명의 실시예는 다른 ECC 방식에 상응하도록 암호화 데이터 및 부가 데이터의 저장 동작이 관리될 수 있으며, 일 예로 ECC 데이터를 일반 데이터(예컨대, 유저 데이터)와 서로 다른 별개의 DRAM 칩에 저장하는 사이드밴드(Sideband) ECC 방식과 동일 또는 유사하게 상기 저장 동작이 관리될 수 있다. DRAM 칩은 다양한 종류의 스펙에 따른 데이터 억세스 동작을 수행할 수 있으며, 일 예로서 LPDDR(예컨대, LPDDR4, LPDDR4X, LPDDR5 등)이 적용될 수 있다.

[0085] 일 예로서, 도 15를 참조하면, 데이터 처리 시스템(700)은 시스템 온 칩(710) 및 다수의 메모리들을 포함하고, 시스템 온 칩(710)은 전술한 실시예들에 따른 보안 처리기(711)를 포함할 수 있다. 또한, 다수의 메모리들은 암호화 데이터를 저장하는 하나 이상의 제1 DRAM 칩들(721, 722)과, 메타 데이터 및 ECC 데이터 등을 포함하는 부가 데이터를 저장하는 하나 이상의 제2 DRAM 칩들(731, 732)을 포함할 수 있다. 도 15에서는 두 개의 제1 DRAM 칩들(721, 722)과 두 개의 제2 DRAM 칩들(731, 732)이 예시되나, 본 발명의 실시예들은 이에 국한될 필요가 없

으며, 다양한 개수의 제1 DRAM 칩 및 제2 DRAM 칩이 데이터 처리 시스템(700)에 구비될 수도 있을 것이다.

[0086] 소정 단위의 암호화 데이터(DATA_EN)는 제1 DRAM 칩들(721, 722) 중 적어도 하나에 저장될 수 있으며, 또한 보안 처리기(711) 내의 어드레스 생성기(미도시)에서 생성되는 어드레스들에 따라 메타 데이터(Meta data) 및 ECC 데이터(ECC data)는 제2 DRAM 칩들(731, 732) 중 적어도 하나에 저장될 수 있다. 예시적인 실시예에 따라, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)는 암호화 데이터(DATA_EN)와는 서로 별개의 DRAM 칩에 저장될 수 있으므로, 보안 처리기(711) 내의 어드레스 생성기는 DRAM 칩의 위치를 나타내는 칩 어드레스를 더 생성할 수 있다. 이에 따라, 칩 어드레스는 메타 데이터(Meta data) 및 ECC 데이터(ECC data)에 대해 일괄적으로 생성될 수 있다.

[0087] 한편, 상기와 같이 사이드밴드(Sideband) ECC 방식에 상응하게 데이터가 관리됨에 따라, 메타 데이터(Meta data) 및 ECC 데이터(ECC data)만을 위한 별도의 대역폭이 제공될 수 있으므로 데이터 억세스 횟수가 감소되고 또한 억세스 속도가 증가될 수 있다. 또한, 제2 DRAM 칩의 양산 규격으로 인해 사용되지 못하고 버려지는 저장 공간이 메타 데이터(Meta data)의 저장을 위해 활용될 수 있으며, 이에 따라 메모리의 이용 효율이 향상될 수 있다.

[0088] 도 16은 본 발명의 예시적인 실시예에 따른 시스템 온 칩의 일 구현 예를 나타내는 블록도이다. 이하의 실시예들에서 설명되는 시스템 온 칩은 어플리케이션 프로세서를 포함할 수 있다.

[0089] 도 16을 참조하면, 시스템 온 칩(800)은 CPU(Central processing unit, 810), 디스플레이 콘트롤러(820), ROM(read only memory, 830), 메모리 콘트롤러(840) 및 RAM(random access memory, 850)을 포함할 수 있다. 또한, 시스템 온 칩(800)은 GPU(Graphic processing unit, 860)를 더 포함할 수 있으며, 또한 시스템 온 칩(800)이 모뎀(770)을 더 포함하는 경우 시스템 온 칩(800)은 ModAP으로 지칭될 수 있다. 이외에도, 시스템 온 칩(800)은 전원 관리 유닛(power management unit) 및 클락 유닛(clock unit) 등 다양한 종류의 기능 블록들을 더 포함할 수 있다.

[0090] CPU(810)는 ROM(830) 및/또는 RAM(850)에 저장된 프로그램들이나 데이터를 처리 또는 실행할 수 있다. 예컨대, CPU(810)는 동작 클락에 따라 상기 프로그램들 및 데이터를 처리 또는 실행할 수 있다. CPU(810)는 멀티-코어 프로세서(multi-core processor)로 구현될 수 있다. 상기 멀티-코어 프로세서는 두 개 또는 그 이상의 독립적인 프로세서들(예컨대, 코어들(cores))을 갖는 하나의 컴퓨팅 컴포넌트(computing component)이고, 상기 프로세서들 각각은 프로그램 명령들(program instructions)을 읽고 실행할 수 있다.

[0091] ROM(830)은 프로그램들 및/또는 데이터를 불휘발성하게 저장할 수 있다. ROM(830)은 EPROM(erasable programmable read-only memory) 또는 EEPROM(electrically erasable programmable read-only memory)으로 구현될 수 있다. 또한, RAM(850)은 프로그램들, 데이터 및 명령들(instructions)을 일시적으로 저장할 수 있다. 예컨대, ROM(830)에 저장된 프로그램들 및/또는 데이터는 CPU(810)의 제어에 따라 RAM(850)에 일시적으로 저장될 수 있다. RAM(850)은 DRAM(dynamic RAM) 또는 SRAM(static RAM) 등의 메모리로 구현될 수 있다.

[0092] 메모리 콘트롤러(840)는 외부 메모리 장치와 인터페이스하는 인터페이스 회로(841)를 포함하며, 데이터 억세스 요청에 따라 외부 메모리 장치를 제어하여 데이터를 기록하거나 독출한다. 또한, 디스플레이 콘트롤러(820)는 디스플레이 장치를 구동함으로써 화면의 표시 동작을 제어할 수 있다.

[0093] 본 발명의 실시예에 따라, 보안 처리기(842)는 시스템 온 칩(800) 내의 다양한 위치들에 구비될 수 있으며, 도 16에서는 보안 처리기(842)가 메모리 콘트롤러(840) 내부에 구현되는 예가 도시된다. 즉, 전술한 실시예들에서의 보안 처리기(842)의 기능은 메모리 콘트롤러(840)에 의해 수행될 수 있다. 메모리 콘트롤러(840)는 암호화 데이터 및 메타 데이터/ECC 데이터를 저장하기 위한 제어 동작을 수행할 수 있으며, 일 예로서 암호화 데이터 및 메타 데이터/ECC 데이터는 시스템 온 칩(800) 내의 RAM(850)에 저장되거나 또는 외부 메모리 장치에 저장될 수 있다. 또한, 메타 데이터/ECC 데이터는 통합하여 관리될 수 있으며, 일 예로서 외부 메모리 장치의 저장 공간이 논리적으로 제1 영역과 제2 영역으로 분리되어 관리되고, 메타 데이터/ECC 데이터는 제2 영역에 함께 저장될 수 있다. 또는, 외부 메모리 장치는 다수의 메모리 칩들을 포함할 수 있으며, 메타 데이터/ECC 데이터는 서로 동일한 메모리 칩에 저장되도록 관리될 수도 있을 것이다.

[0094] 한편, 도 16의 실시예에서는 메모리 콘트롤러(840)가 시스템 온 칩(800) 내의 구성인 것으로 도시되었으나, 본 발명의 실시예는 이에 국한될 필요가 없다. 일 예로서, 메모리 콘트롤러(840)는 별개의 반도체 칩으로 구현되고, 별개의 반도체 칩으로 구현된 메모리 콘트롤러(840) 내에 본 발명의 예시적인 실시예들에 따른 보안 처리기(842)가 구비될 수 있다. 또한, 별개의 반도체 칩으로 구현되는 메모리 콘트롤러(840)와 메모리(예컨대,

외부의 메모리 장치)가 본 발명의 실시예들에 따른 메모리 시스템(MEM SYS)을 구성할 수 있다.

[0095] 도 17은 본 발명의 변형 가능한 예시적인 실시예에 따른 시스템 온 칩의 일 구현 예를 나타내는 블록도이다. 도 16에 도시된 구성 요소들 중 일부는 설명의 편의상 도 17에 도시되지 않았으나, 본 발명의 실시예들에 따른 시스템 온 칩은 다른 다양한 구성 요소들을 더 포함할 수도 있을 것이다. 또한, 도 17에 도시된 시스템 온 칩의 구성 및 동작 예를 설명함에 있어서, 전술한 실시예에서와 중복되는 설명은 생략된다.

[0096] 도 17을 참조하면, 시스템 온 칩(900)은 CPU(910), GPU(920), 디스플레이 콘트롤러(930), 보안 처리기(940) 및 메모리 컨트롤러(950)를 포함할 수 있다. 메모리 컨트롤러(950)의 일 예로서 DRAM 컨트롤러가 예시된다. 또한, 메모리 컨트롤러(950)는 외부의 메모리 장치를 제어할 수 있으며, 외부의 메모리 장치는 저장되는 데이터의 종류에 따라 다수의 영역들로 분류될 수 있다.

[0097] CPU(910)는 시스템 온 칩(900)의 전반적인 동작을 제어할 수 있으며, 일 예로서 억세스가 요구되는 데이터 및 어드레스를 보안 처리기(940)로 제공하거나, 또는 메모리 컨트롤러(950)로 제공할 수 있다. 일 예로서, 다양한 종류의 데이터들이 외부의 메모리 장치에 저장될 수 있으며, 만약 암호화가 필요로 되지 않는 데이터는 CPU(910) 및 메모리 컨트롤러(950)를 통한 경로(Plain Data Path)를 거쳐 외부의 메모리 장치로 제공될 수 있다. 반면에, 암호화가 필요로 되는 데이터는 CPU(910) 및 보안 처리기(940)를 통한 경로(Encrypted Data Path)를 거쳐 외부의 메모리 장치로 제공될 수 있다.

[0098] 도 17에 도시된 시스템 온 칩(900)은 다양한 방식에 따라 데이터를 처리할 수 있다. 만약, 암호화가 필요로 되지 않는 데이터에 대해 ECC 동작이 적용되는 경우에는, 메모리 컨트롤러(950)가 데이터(DATA)에 대한 ECC 동작을 통해 ECC 데이터를 생성할 수 있을 것이다. 반면에, 암호화가 필요로 되는 데이터는 보안 처리기(940)에 의해 전술한 실시예들에 따라 처리되어 암호화 데이터(DATA_EN) 및 이에 대응하는 메타 데이터/ECC 데이터(Meta/ECC data)가 생성될 수 있을 것이다. 또한, 메타 데이터/ECC 데이터(Meta/ECC data)는 외부의 메모리 장치의 동일한 영역에 저장되도록 어드레스 생성 동작이 수행될 수 있을 것이다.

[0099] 도 18은 본 발명의 예시적인 실시예에 따른 보안 처리기가 자동차에 채용되는 자율 주행 시스템 내에 구현되는 예를 나타내는 블록도이다. 도 18에 도시된 시스템은 자율 주행 시스템(1000)에 해당할 수 있으며, 자율 주행 시스템(1000)은 센서 정보 수집부(1100), 네비게이션 정보 수집부(1200), 자율 주행 모듈(1300), 중앙 처리 장치(1400) 및 메모리(1500)를 포함할 수 있다. 또한, 자율 주행 모듈(1300)은 뉴럴 네트워크 장치(1310) 및 보안 처리 모듈(1320)를 포함할 수 있다.

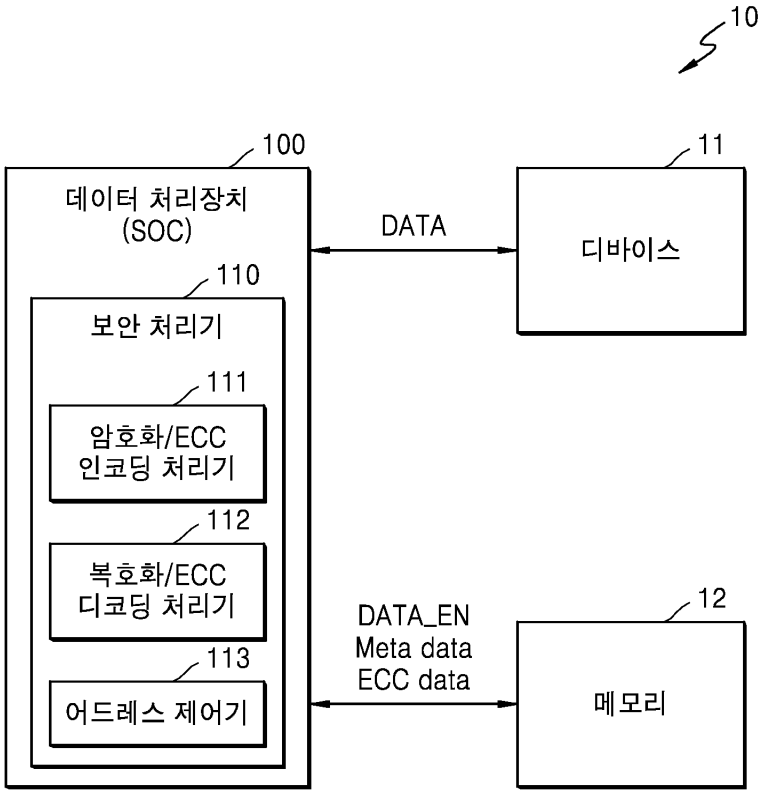
[0100] 뉴럴 네트워크 장치(1310)는 각종 영상 정보 및 음성 정보를 이용한 뉴럴 네트워크 동작을 수행하고, 수행 결과를 기초로 영상 인식 결과 및 음성 인식 결과 등의 정보 신호를 생성할 수 있다. 일 예로서, 센서 정보 수집부(1100)는 카메라나 마이크 등의 각종 영상 정보 및 음성 정보를 수집할 수 있는 장치들을 포함하고, 이를 자율 주행 모듈(1300)로 제공할 수 있다. 또한, 네비게이션 정보 수집부(1200)는 자동차 운행과 관련된 각종 정보(예컨대, 위치 정보 등)를 자율 주행 모듈(1300)로 제공할 수 있다. 뉴럴 네트워크 장치(1310)는 센서 정보 수집부(1100) 및/또는 네비게이션 정보 수집부(1200)로부터의 정보를 입력으로 하여, 다양한 종류의 뉴럴 네트워크 모델을 실행함으로써 상기 정보 신호를 생성할 수 있다. 센서 정보 수집부(1100)가 카메라나 마이크를 포함할 때, 자율 주행 모듈(1300)의 보안 처리기(1320)는 센서 정보 수집부(1100)로부터의 음성 데이터나 이미지 데이터에 대한 보안 처리로서 암/복호화 동작 및 ECC 동작을 수행할 수 있으며, 전술한 실시예들에 따라 암호화 데이터, 메타 데이터/ECC 데이터를 메모리(1500)에 저장할 수 있다.

[0101] 도 18에서는 자율 주행 시스템에 본 발명의 실시예가 적용된 예가 설명되었으나, 본 발명의 실시예들은 IoT, 감시카메라, 등 카메라 센서에 보안 기능이 필요한 제품들에 적용이 가능하다.

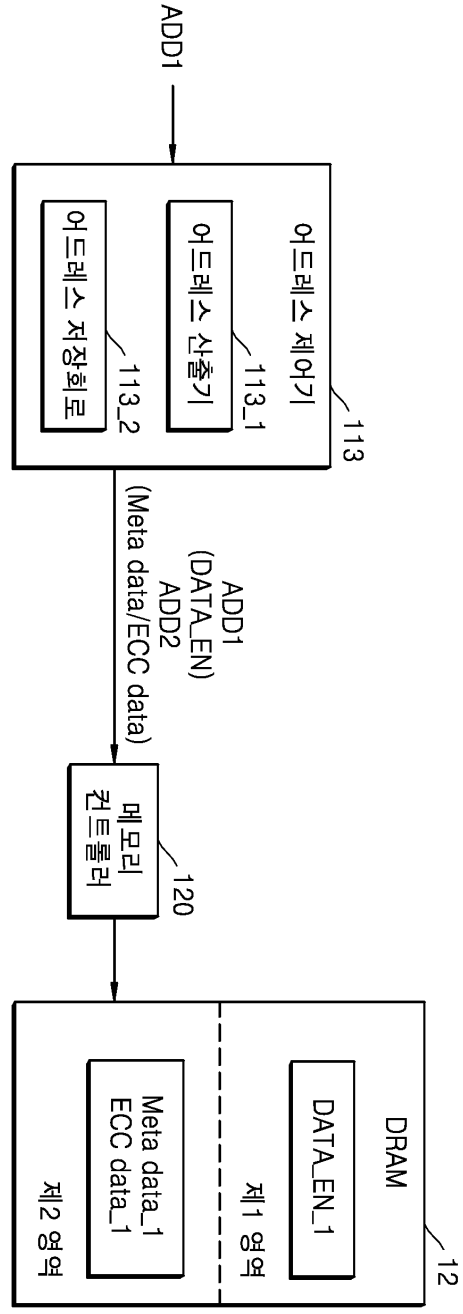
[0102] 이상에서와 같이 도면과 명세서에서 예시적인 실시예들이 개시되었다. 본 명세서에서 특정한 용어를 사용하여 실시예들을 설명되었으나, 이는 단지 본 개시의 기술적 사상을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 개시의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 개시의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

도면

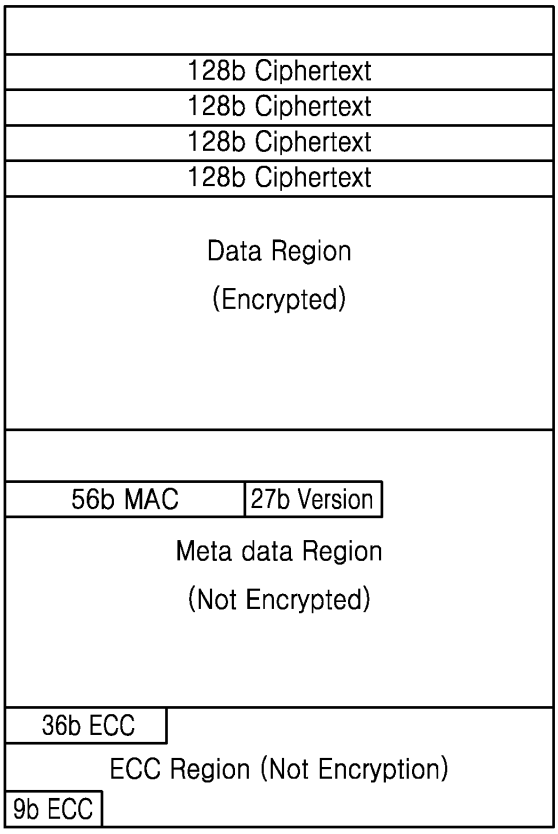
도면1


10
100
데이터 처리장치
(SOC)
110
보안 처리기
111
암호화/ECC
인코딩 처리기
112
복호화/ECC
디코딩 처리기
113
어드레스 제어기
DATA
11
디바이스
DATA_EN
Meta data
ECC data
12
메모리

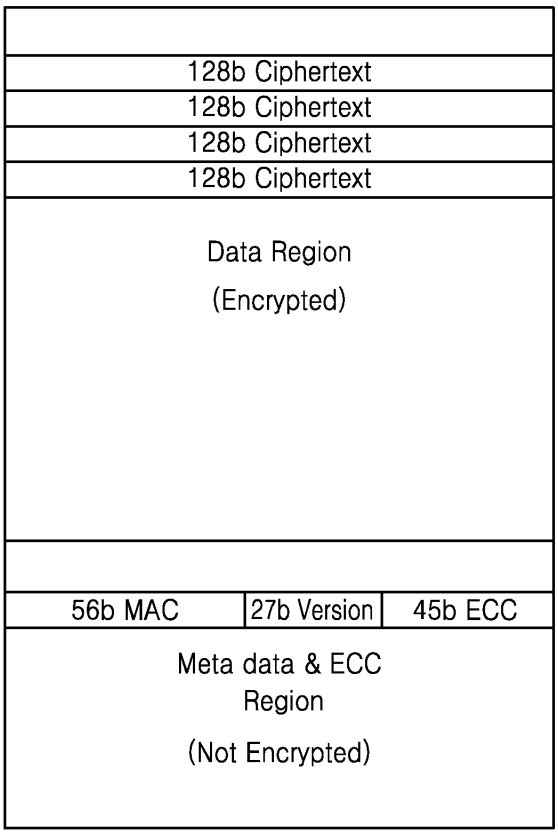
도면2


ADD1
어드레스 제어기
113
어드레스 산출기
113_1
어드레스 저장회로
113_2
ADD1
(DATA_EN)
ADD2
(Meta data/ECC data)
메모리
컨트롤러
120
DRAM
12
DATA_EN_1
제1 영역
Meta data_1
ECC data_1
제2 영역

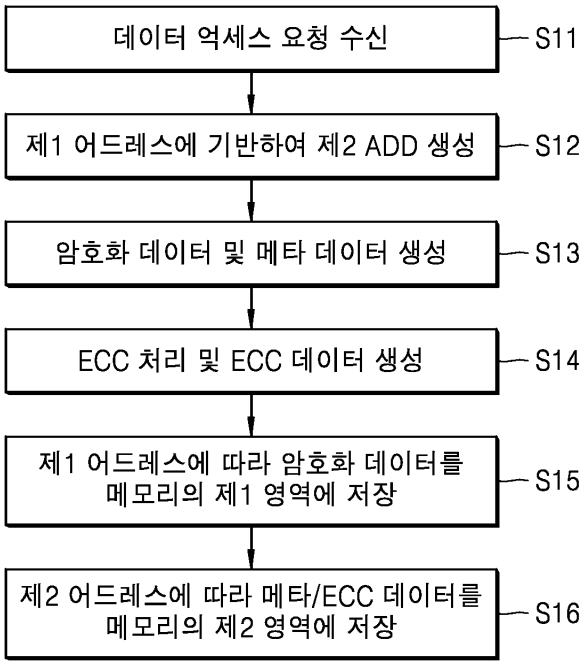
도면3


128b Ciphertext
128b Ciphertext
128b Ciphertext
128b Ciphertext
Data Region
(Encrypted)
56b MAC
27b Version
Meta data Region
(Not Encrypted)
36b ECC
ECC Region (Not Encryption)
9b ECC

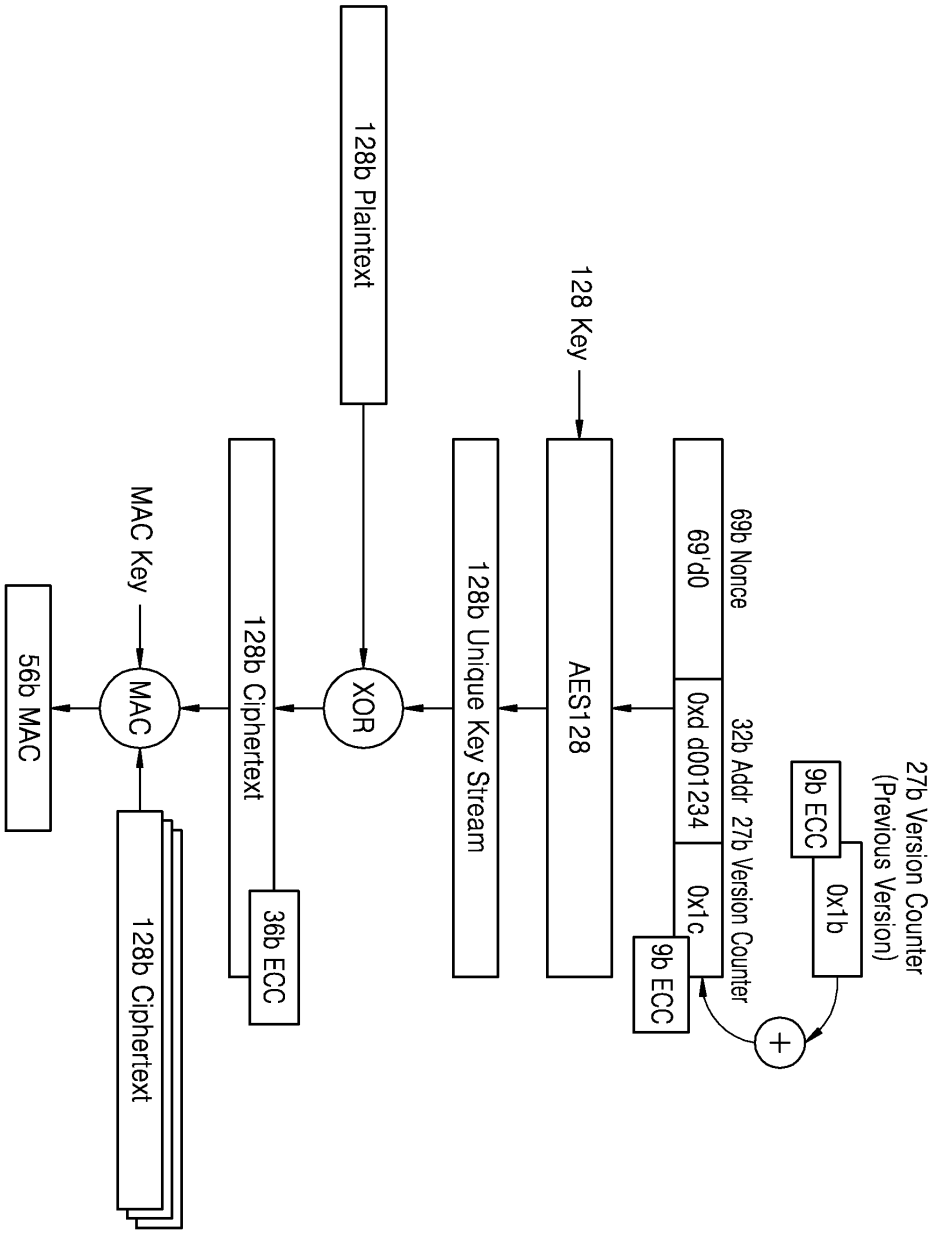
도면4


128b Ciphertext
128b Ciphertext
128b Ciphertext
128b Ciphertext
Data Region
(Encrypted)
56b MAC
27b Version
45b ECC
Meta data & ECC
Region
(Not Encrypted)

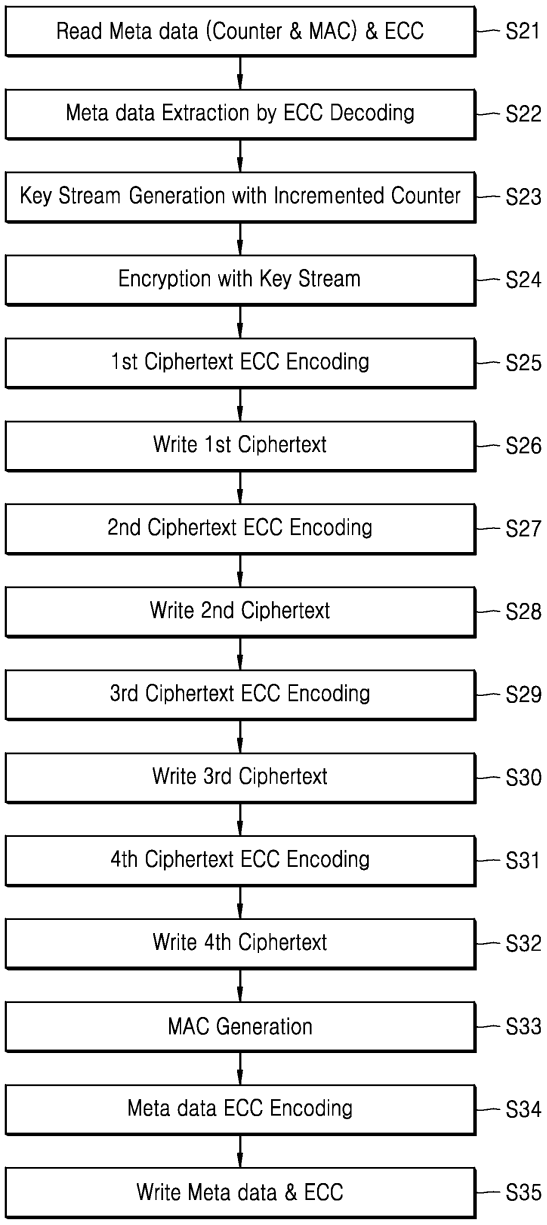
도면5


데이터 억세스 요청 수신
S11
제1 어드레스에 기반하여 제2 ADD 생성
S12
암호화 데이터 및 메타 데이터 생성
S13
ECC 처리 및 ECC 데이터 생성
S14
제1 어드레스에 따라 암호화 데이터를 메모리의 제1 영역에 저장
S15
제2 어드레스에 따라 메타/ECC 데이터를 메모리의 제2 영역에 저장
S16

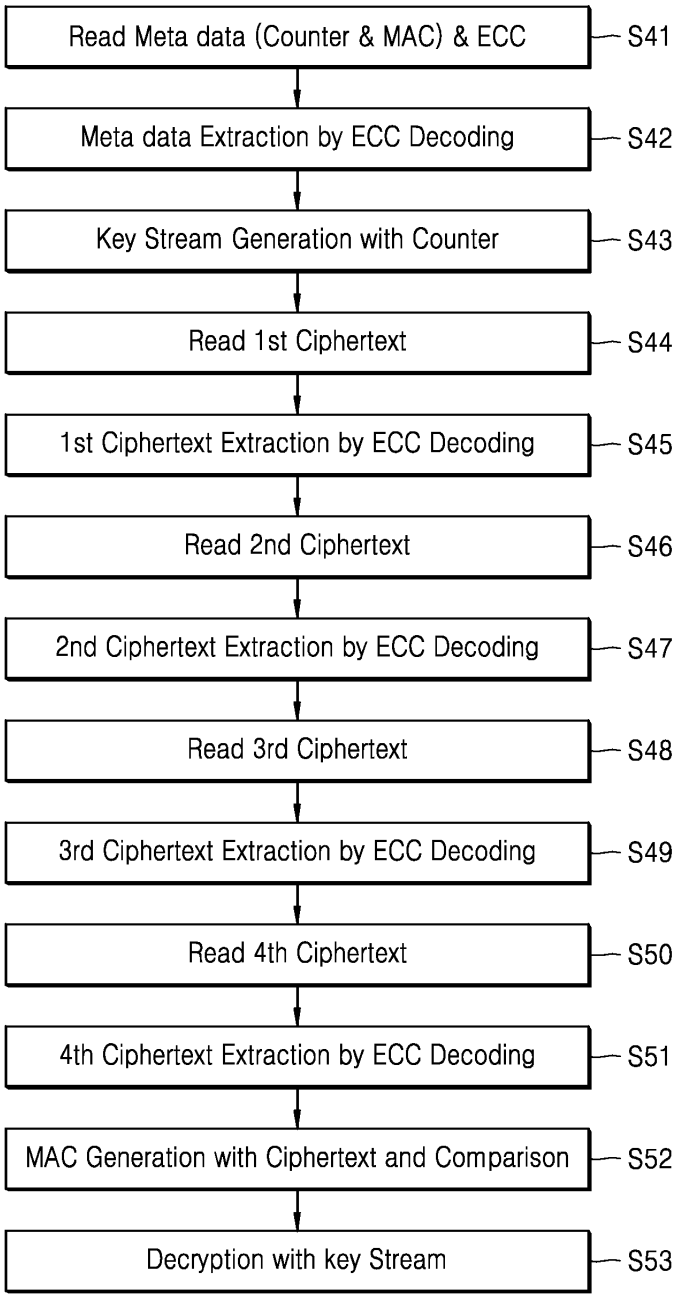
도면6


128b Plaintext
128 Key
69b Nonce
69'd0
0xd d001234
32b Addr
27b Version Counter
0x1c
9b ECC
9b ECC
0x1b
27b Version Counter
(Previous Version)
AES128
128b Unique Key Stream
XOR
128b Ciphertext
36b ECC
MAC Key
MAC
56b MAC
128b Ciphertext

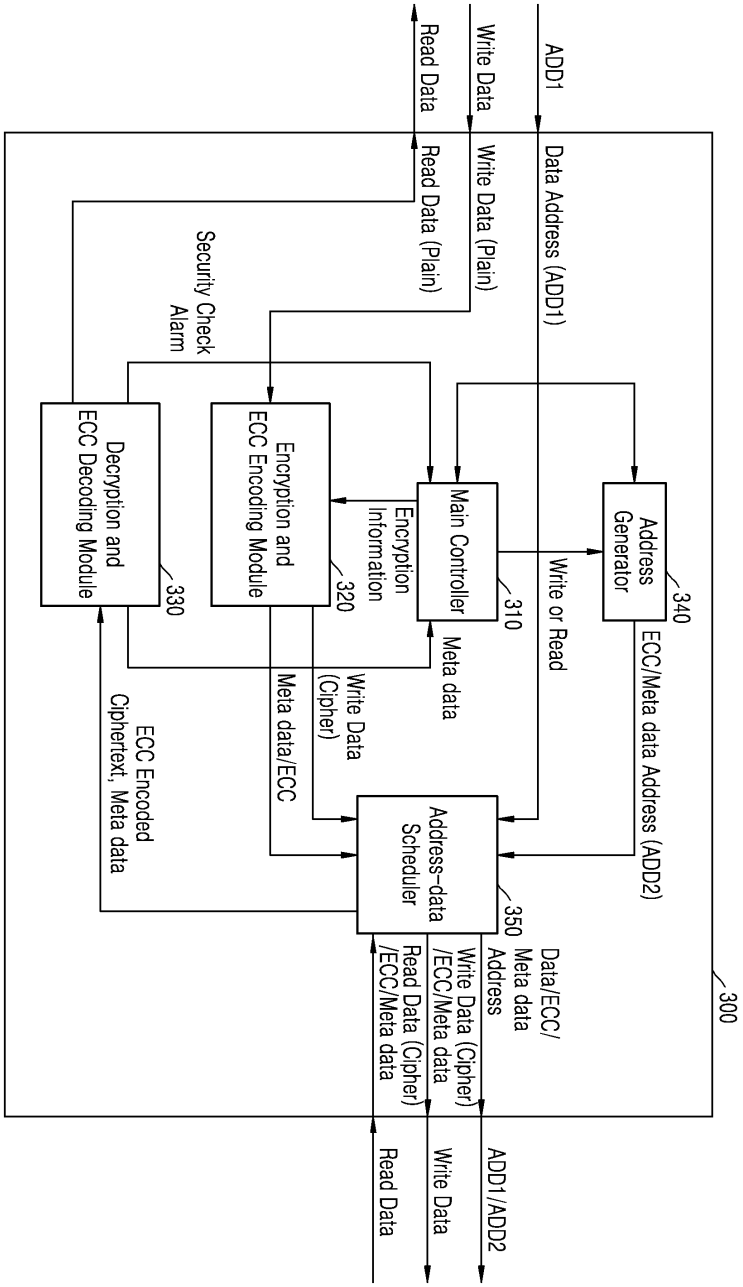
도면7


Read Meta data (Counter & MAC) & ECC
S21
Meta data Extraction by ECC Decoding
S22
Key Stream Generation with Incremented Counter
S23
Encryption with Key Stream
S24
1st Ciphertext ECC Encoding
S25
Write 1st Ciphertext
S26
2nd Ciphertext ECC Encoding
S27
Write 2nd Ciphertext
S28
3rd Ciphertext ECC Encoding
S29
Write 3rd Ciphertext
S30
4th Ciphertext ECC Encoding
S31
Write 4th Ciphertext
S32
MAC Generation
S33
Meta data ECC Encoding
S34
Write Meta data & ECC
S35

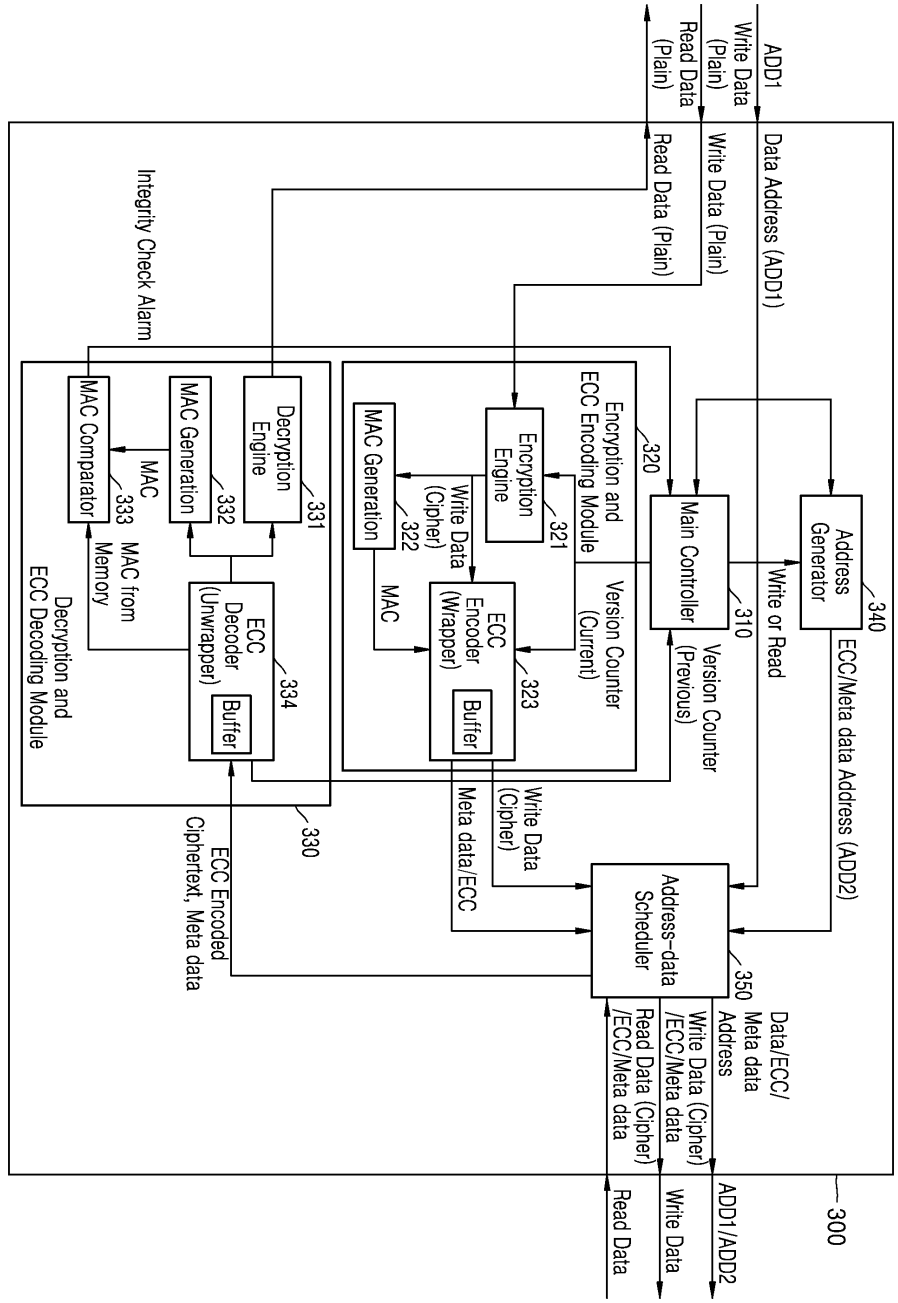
도면8


Read Meta data (Counter & MAC) & ECC
S41
Meta data Extraction by ECC Decoding
S42
Key Stream Generation with Counter
S43
Read 1st Ciphertext
S44
1st Ciphertext Extraction by ECC Decoding
S45
Read 2nd Ciphertext
S46
2nd Ciphertext Extraction by ECC Decoding
S47
Read 3rd Ciphertext
S48
3rd Ciphertext Extraction by ECC Decoding
S49
Read 4th Ciphertext
S50
4th Ciphertext Extraction by ECC Decoding
S51
MAC Generation with Ciphertext and Comparison
S52
Decryption with key Stream
S53

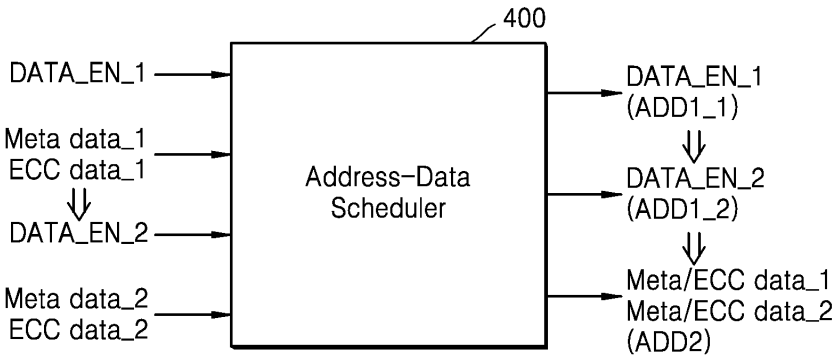
도면9


ADD1
Write Data
Read Data
Data Address (ADD1)
Write Data (Plain)
Read Data (Plain)
Security Check Alarm
Main Controller
310
Address Generator
340
Write or Read
ECC/Meta data Address (ADD2)
Encryption and ECC Encoding Module
320
Encryption Information
Meta data
Decryption and ECC Decoding Module
330
Write Data (Cipher)
Meta data/ECC
ECC Encoded Ciphertext, Meta data
Address-data Scheduler
350
Data/ECC/ Meta data Address
Write Data (Cipher) /ECC/Meta data
Read Data (Cipher) /ECC/Meta data
300
ADD1/ADD2
Write Data
Read Data

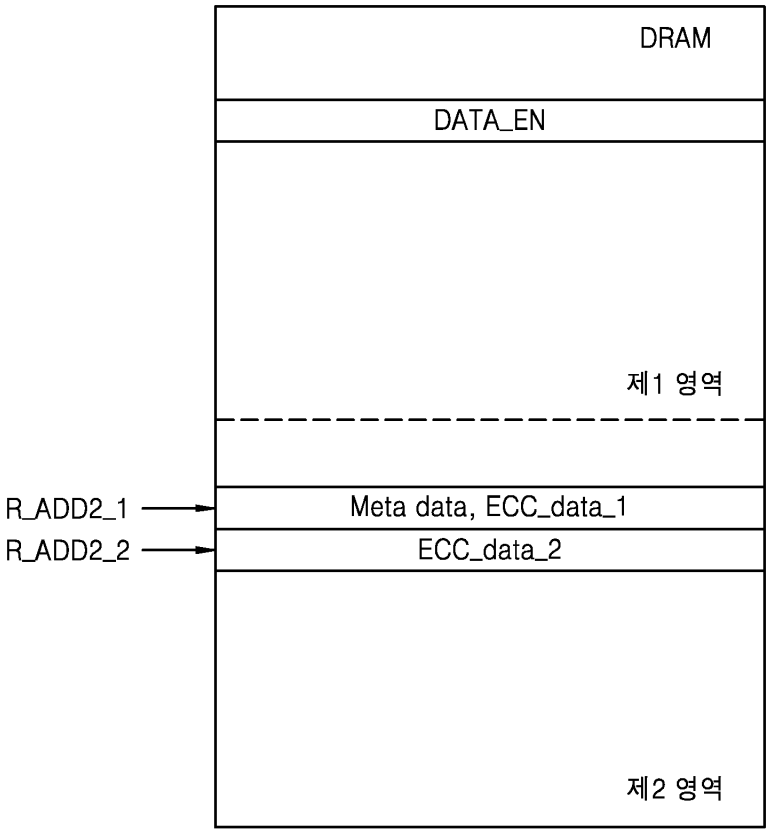
도면10


ADD1
Write Data (Plain)
Read Data (Plain)
Data Address (ADD1)
Write Data (Plain)
Read Data (Plain)
Integrity Check Alarm
MAC Comparator
MAC
333
MAC Generation
332
Decryption Engine
331
MAC from Memory
Decryption and ECC Decoding Module
ECC Decoder (Unwrapper)
Buffer
334
330
MAC Generation
322
Write Data (Cipher)
Encryption Engine
321
Encryption and ECC Encoding Module
320
MAC
ECC Encoder (Wrapper)
Buffer
323
Version Counter (Current)
Main Controller
310
Version Counter (Previous)
Write or Read
Address Generator
340
ECC/Meta data Address (ADD2)
Write Data (Cipher)
Meta data/ECC
Address-data Scheduler
350
ECC Encoded Ciphertext, Meta data
Data/ECC/ Meta data Address
Write Data (Cipher) /ECC/Meta data
Read Data (Cipher) /ECC/Meta data
ADD1/ADD2
Write Data
Read Data
300

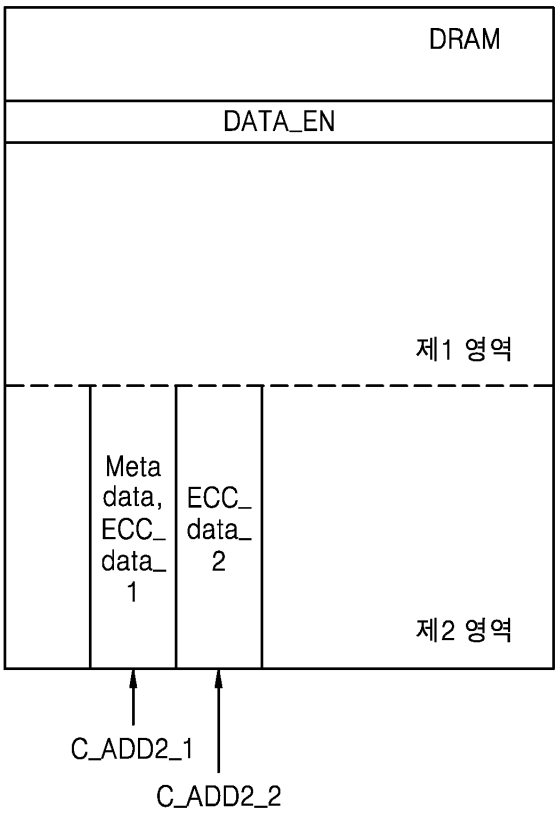
도면11


400
DATA_EN_1
Meta data_1
ECC data_1
DATA_EN_2
Meta data_2
ECC data_2
Address-Data Scheduler
DATA_EN_1 (ADD1_1)
DATA_EN_2 (ADD1_2)
Meta/ECC data_1
Meta/ECC data_2
(ADD2)

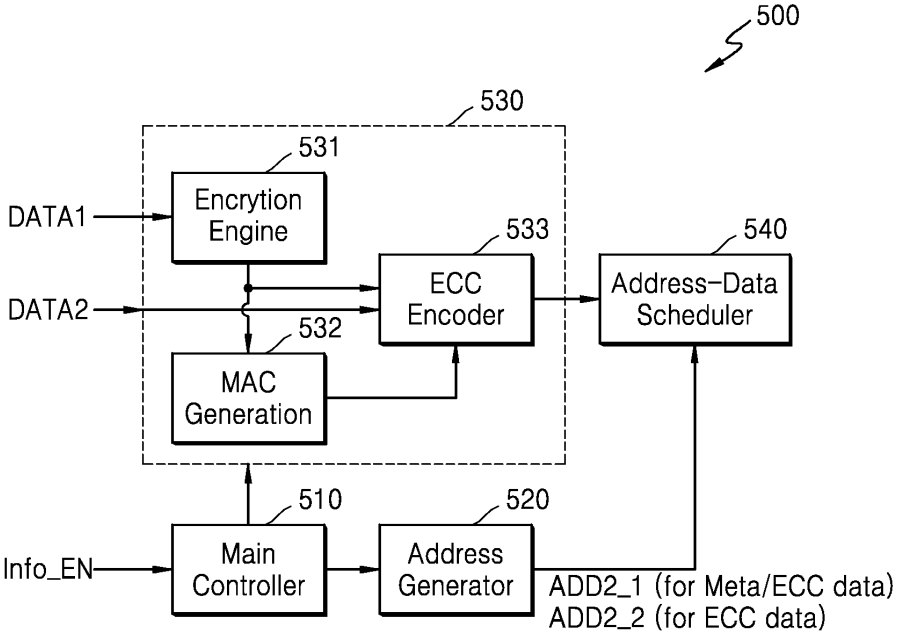
도면12a


DRAM
DATA_EN
제1 영역
R_ADD2_1
R_ADD2_2
Meta data, ECC_data_1
ECC_data_2
제2 영역

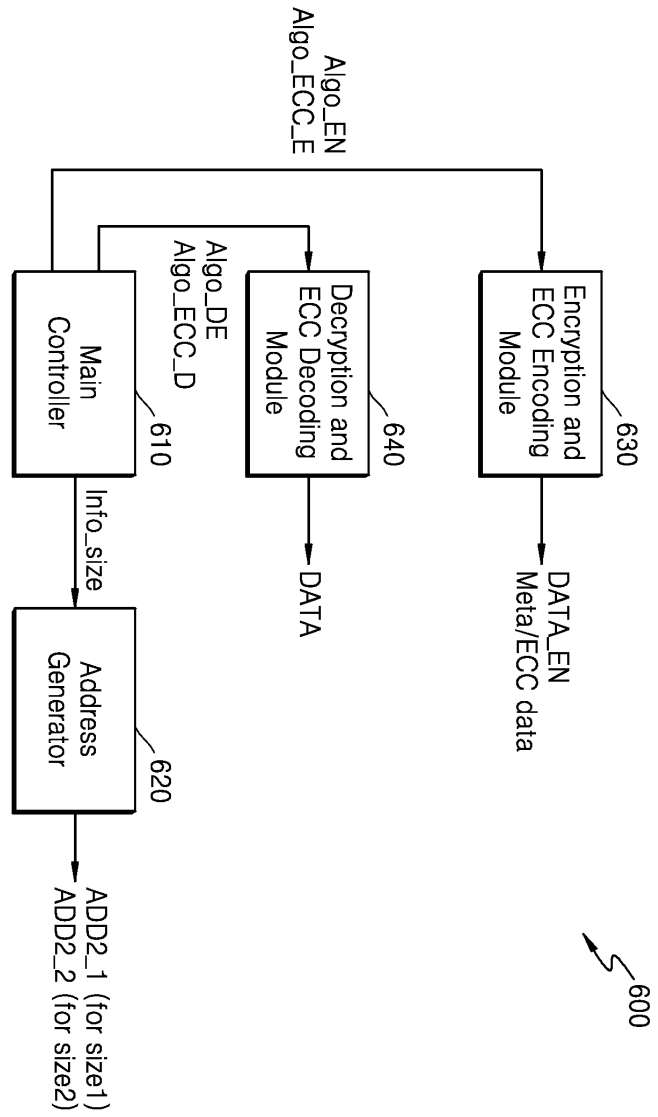
도면12b


DRAM
DATA_EN
제1 영역
Meta data, ECC_ data_ 1
ECC_ data_ 2
제2 영역
C_ADD2_1
C_ADD2_2

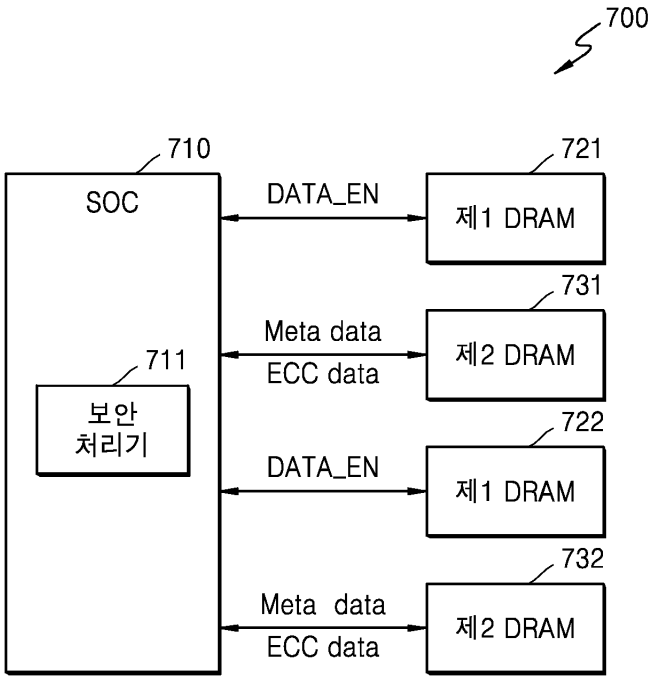
도면13


500
530
531
Encrytion Engine
DATA1
DATA2
533
ECC Encoder
540
Address-Data Scheduler
532
MAC Generation
510
520
Info_EN
Main Controller
Address Generator
ADD2_1 (for Meta/ECC data)
ADD2_2 (for ECC data)

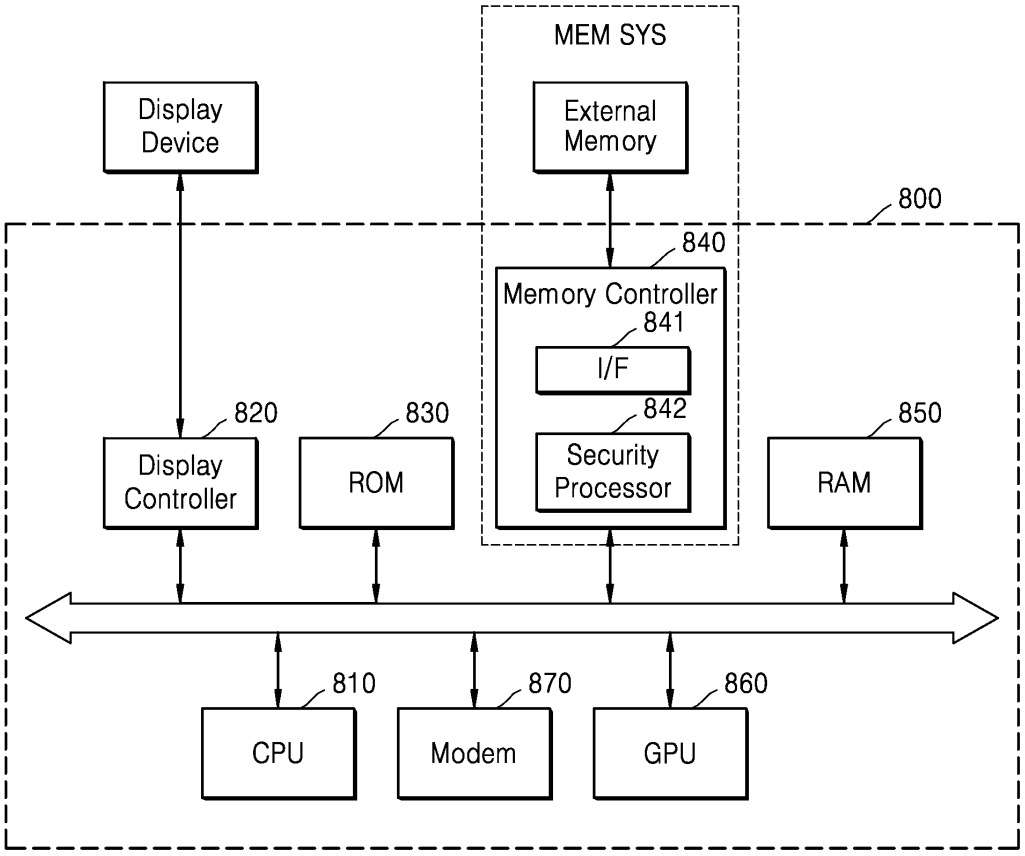
도면14


Algo_EN
Algo_ECC_E
Algo_DE
Algo_ECC_D
Main Controller
610
Decryption and ECC Decoding Module
640
Encryption and ECC Encoding Module
630
Info_size
DATA
DATA_EN
Meta/ECC data
Address Generator
620
ADD2_1 (for size1)
ADD2_2 (for size2)
600

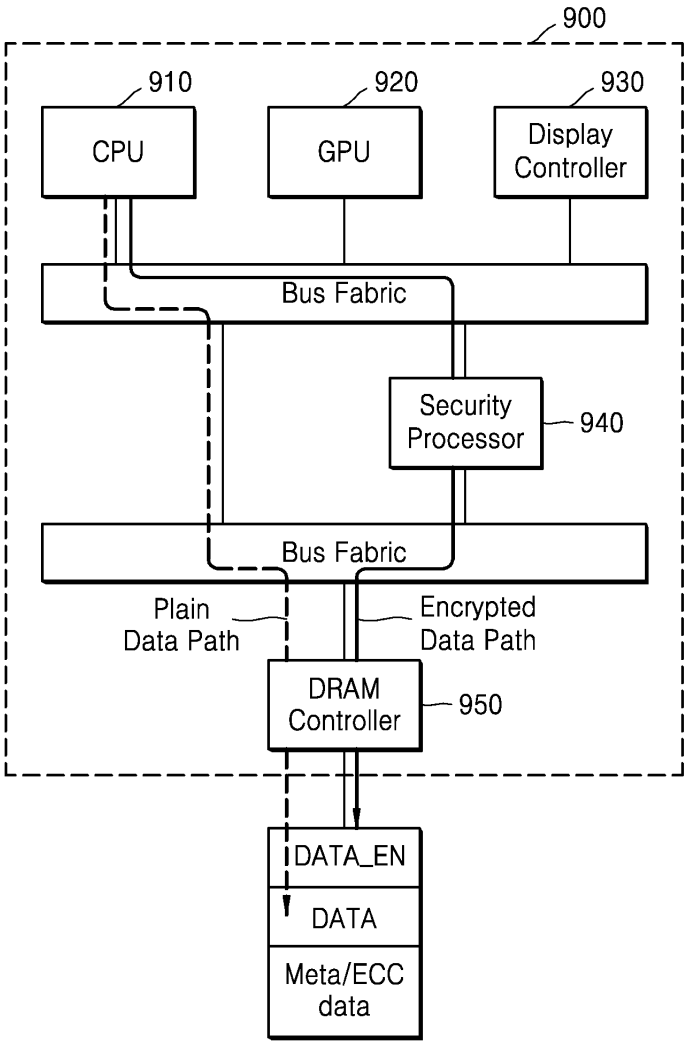
도면15


700
710
SOC
711
보안
처리기
DATA_EN
721
제1 DRAM
Meta data
ECC data
731
제2 DRAM
DATA_EN
722
제1 DRAM
Meta data
ECC data
732
제2 DRAM

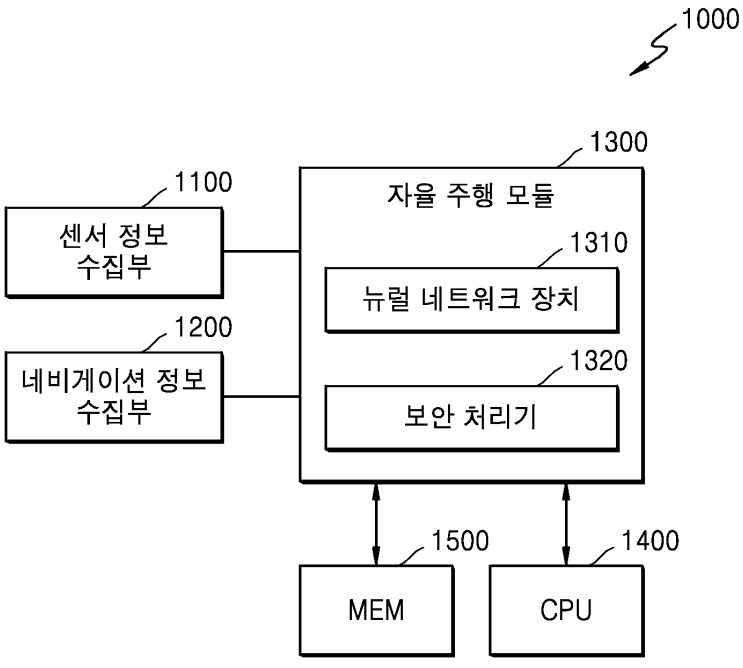
도면16


MEM SYS
Display
Device
External
Memory
800
840
Memory Controller
841
I/F
842
Security
Processor
820
Display
Controller
830
ROM
850
RAM
810
CPU
870
Modem
860
GPU

도면17


900
910
CPU
920
GPU
930
Display Controller
Bus Fabric
Security Processor
940
Bus Fabric
Plain Data Path
Encrypted Data Path
DRAM Controller
950
DATA_EN
DATA
Meta/ECC data

도면18


1000
1300
자율 주행 모듈
1100
센서 정보 수집부
1310
뉴럴 네트워크 장치
1200
네비게이션 정보 수집부
1320
보안 처리기
1500
MEM
1400
CPU