(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0012285
(43) 공개일자 2011년02월09일

(51) Int. Cl.
G06F 9/38 (2006.01) *G06F 9/46* (2006.01)
(21) 출원번호 10-2009-0069948
(22) 출원일자 2009년07월30일
심사청구일자 2009년07월30일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
정용화
대전 유성구 지족동 877 열매마을아파트 505동 402호
이성주
서울 마포구 성산2동 한맥아이홈 47-14 302호
이은지
경상북도 경산시 정평동 130 현대타운 106-602
(74) 대리인
특허법인충현

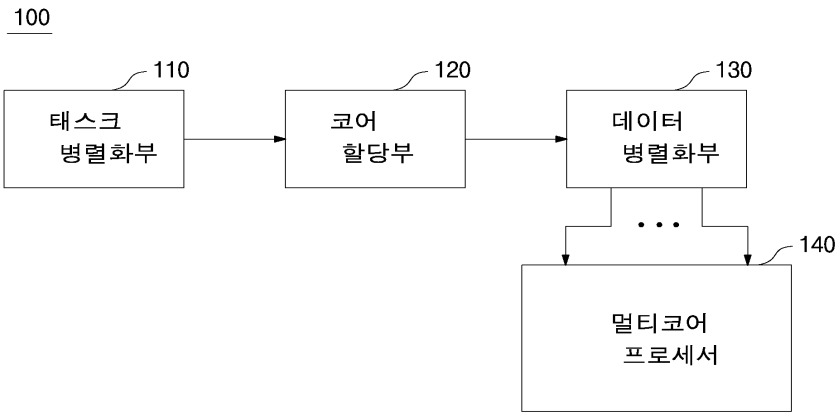
전체 청구항 수 : 총 20 항

(54) 범용 멀티코어 프로세서를 이용한 ＡＥＳ-ＣＣＭ 병렬처리 장치 및 방법

(57) 요 약

본 발명은 AES-CCM 병렬처리 기술에 관한 것으로서, 본 발명에 따른 AES-CCM 병렬처리 장치는, AES-CCM의 처리 대상 태스크(task)에 대해 범용 멀티코어 프로세서의 코어를 할당하는 코어 할당부; 및 상기 할당된 코어의 개수에 대응하여 상기 처리 대상 태스크에 대한 데이터 병렬화(data parallelism)를 수행하는 데이터 병렬화부를 포함하고, 상기 범용 멀티코어 프로세서는, 상기 데이터 병렬화된 상기 처리 대상 태스크를 상기 할당된 코어를 통해 병렬적으로 수행하는 것을 특징으로 하여, 데이터 기밀성 및 무결성을 동시에 보장함은 물론, 처리 속도 및 자원 효율성을 개선하고 프로세서 호환성을 제공한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 20090302185256
부처명 한국산업기술재단
연구관리전문기관
연구사업명 지역혁신인력양성사업
연구과제명 (1차년도)베터리로 동작하는 감시카메라용 비디오 압축 특성을 이용한 정보보호 및 상황 인지 연구를 통한 최적화
기여율
주관기관 고려대학교
연구기간 2009년 05월 01일 ~ 2010년 04월 30일

특허청구의 범위

청구항 1

AES-CCM의 처리 대상 태스크(task)에 대해 범용 멀티코어 프로세서의 코어를 할당하는 코어 할당부; 및

상기 할당된 코어의 개수에 대응하여 상기 처리 대상 태스크에 대한 데이터 병렬화(data parallelism)를 수행하는 데이터 병렬화부를 포함하고,

상기 범용 멀티코어 프로세서는, 상기 데이터 병렬화된 상기 처리 대상 태스크를 상기 할당된 코어를 통해 병렬적으로 수행하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 2

제1항에 있어서,

상기 코어 할당부는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 없는 경우, 상기 처리 대상 태스크에 대해 상기 범용 멀티코어 프로세스의 코어들 중 2 이상을 할당하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 3

제1항에 있어서,

상기 코어 할당부는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 있는 경우, 상기 처리 대상 태스크에 대해 상기 범용 멀티코어 프로세스의 코어들 중 하나의 코어를 할당하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 4

제1항에 있어서,

상기 코어 할당부는, 상기 범용 멀티코어 프로세스의 코어들 중에서, 상기 처리 대상 태스크가 CTR(Counter)인 경우 2 이상의 코어를 할당하고, 상기 처리 대상 태스크가 CBC-MAC(Cipher Block Chaining-Message Authentication Code)인 경우 하나의 코어를 할당하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 5

제4항에 있어서,

상기 코어 할당부는, 상기 처리 대상 태스크가 상기 CTR인 경우, 상기 범용 멀티코어 프로세스의 코어 전체를 할당하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 6

제5항에 있어서,

상기 범용 멀티코어 프로세서는, 상기 CTR 및 상기 CBC-MAC에 대한 처리 수행시, 상기 CTR 또는 상기 CBC-MAC에 대한 처리를 먼저 수행하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 7

제1항에 있어서,

상기 데이터 병렬화부는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 있는 경우, 상기 데이터 병렬화를 수행하지 않는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 8

제1항에 있어서,

상기 데이터 병렬화부는, 상기 처리 대상 태스크가 CBC-MAC인 경우, 상기 데이터 병렬화를 수행하지 않는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 9

제1항에 있어서,

상기 AES-CCM 병렬처리 장치는, 상기 AES-CCM의 처리 대상 태스크들 중, CTR 및 CBC-MAC에 대한 태스크 병렬화(task parallelism)를 수행하는 태스크 병렬화부를 더 포함하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 10

제9항에 있어서,

상기 코어 할당부는, 상기 범용 멀티코어 프로세스의 코어들 중에서, 상기 CBC-MAC에 대해서는 하나의 코어를 할당하고, 상기 CTR에 대해서는 1 또는 2 이상의 코어를 할당하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 11

제10항에 있어서,

상기 데이터 병렬화부는, 상기 CTR에 대해서만 상기 데이터 병렬화를 수행하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 12

제10항에 있어서,

상기 범용 멀티코어 프로세서는, 상기 CTR 및 상기 CBC-MAC에 대한 처리를 병렬적으로 수행하는 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치.

청구항 13

범용 멀티코어 프로세서를 사용하는 컴퓨터 시스템에서, AES-CCM의 처리 대상 태스크(task)에 대해 상기 범용 멀티코어 프로세서의 코어를 할당하는 코어 할당 단계;

상기 컴퓨터 시스템에서, 상기 할당된 코어의 개수에 대응하여 상기 처리 대상 태스크에 대한 데이터 병렬화(data parallelism)를 수행하는 데이터 병렬화 단계; 및

상기 범용 멀티코어 프로세서에서, 상기 데이터 병렬화된 상기 처리 대상 태스크를 상기 할당된 코어를 통해 병렬적으로 처리하는 처리 단계를 포함하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 방법.

청구항 14

제13항에 있어서,

상기 코어 할당 단계는, 상기 범용 멀티코어 프로세스의 코어들 중에서, 상기 처리 대상 태스크가 CTR인 경우 2 이상의 코어를 할당하고, 상기 처리 대상 태스크가 CBC-MAC인 경우 하나의 코어를 할당하는 단계인 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 방법.

청구항 15

제14항에 있어서,

상기 코어 할당 단계는, 상기 처리 대상 태스크가 상기 CTR인 경우, 상기 범용 멀티코어 프로세스의 코어 전체를 할당하는 단계인 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 방법.

청구항 16

제15항에 있어서,

상기 처리 단계는, 상기 CTR 및 상기 CBC-MAC에 대한 처리 수행시, 상기 CTR 또는 상기 CBC-MAC에 대한 처리를 먼저 수행하는 단계인 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 방법.

청구항 17

제13항에 있어서,

상기 데이터 병렬화 단계는, 상기 처리 대상 태스크가 CBC-MAC인 경우, 상기 데이터 병렬화를 수행하지 않는 단계인 것을 특징으로 하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 방법.

청구항 18

범용 멀티코어 프로세서를 사용하는 컴퓨터 시스템에서, AES-CCM의 처리 대상 태스크들 중, CTR 및 CBC-MAC에 대한 태스크 병렬화(task parallelism)를 수행하는 태스크 병렬화 단계;

상기 컴퓨터 시스템에서, 상기 범용 멀티코어 프로세스의 코어들 중에서, 상기 CBC-MAC에 대해서는 하나의 코어를 할당하고, 상기 CTR에 대해서는 1 또는 2 이상의 코어를 할당하는 코어 할당 단계;

상기 컴퓨터 시스템에서, 상기 할당된 코어의 개수에 대응하여 상기 CTR에 대한 데이터 병렬화(data parallelism)를 수행하는 데이터 병렬화 단계; 및

상기 범용 멀티코어 프로세서에서, 상기 데이터 병렬화된 CTR 및 상기 CBC-MAC를 상기 할당된 코어를 통해 병렬적으로 처리하는 처리 단계를 포함하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 방법.

청구항 19

제13항 내지 제18항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

청구항 20

제19항에 있어서,

상기 프로그램은, 병렬적으로 작동하는 소프트웨어의 작성에 사용되는 표준 API(Application Programming Interface)인 Pthread(POSIX Threads)를 통해 프로그래밍된 것을 특징으로 하는 컴퓨터 판독가능 기록매체.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 AES-CCM 병렬처리 기술에 관한 것으로서, 더욱 상세하게는, 범용 멀티코어 프로세서를 이용하여 AES-CCM를 병렬처리함으로써, 데이터 기밀성 및 무결성을 동시에 보장함은 물론, 처리 속도 및 자원 효율성을 개선하고 프로세서 호환성을 지니는 AES-CCM 병렬처리 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 디지털 정보사회가 고도화되고 전자상거래가 활성화됨에 따라, 암호·인증 기술은 현재, 인터넷을 기반으로 한 사회·경제적 활동의 안전성과 신뢰성, 그리고 사용자 프라이버시 보호 등을 위한 핵심 기술로서 인식되고 있다. 또한, 최근 MPEG 비디오 스트림 등 대용량 데이터 이용이 증가함에 따라, 이러한 암호·인증 기술을 이용한 대용량 데이터 정보 보호 문제가 이슈화되고 있다.

[0003] 대용량 데이터 정보 보호를 위해서는, 데이터의 기밀성(confidentiality)을 보장하는 기법은 물론, 그 외에 HMAC(Keyed-Hash Message Authentication Code) 등과 같은 메시지 인증 기법을 추가적으로 적용할 필요가 있다. 즉, 메시지 인증을 할 수 있는 암호화 알고리즘을 적용하여 대용량 데이터의 무결성(Integrity)을 동시에 보장해야 한다.

[0004] 이와 같이, 데이터의 기밀성 및 무결성을 동시에 보장하기 위한 방법으로는, 블록 암호화 운용모드(Block mode of operation)를 이용하는 방법이 있다.

[0005] 미국 국립표준기술원(NIST: National Institute of Standards and Technology)이 차세대 국제 표준 암호로서 채택한 AES(Advanced Encryption Standard)는 데이터의 무결성과 기밀성을 보장하기 위해 5가지 운용모드를 표준으로 규정하고 있다. 즉, ECB(Electronic Code Book), CBC(Cipher Block Chaining), CFB(Cipher FeedBack), OFD(Output FeedBack) 및 CTR(Counter)을 규정하고 있다.

[0006] 상기 다양한 표준 운영모드들 중 CTR 모드와 CBC-MAC 모드를 조합한 AES-CCM(Counter with CBC-MAC)은, 상기 조합된 두 모드의 기능이 결합되어 하나의 솔루션에서 암호화 및 메시지 무결성을 제공한다. 즉, 기밀성 기능과 키 관리(Key Management) 기능, 메시지 무결성(Message Integrity) 기능을 동시에 수행할 수 있다. 이러한 AES-CCM은, 무선랜(Wireless LAN) 보안 표준인 IEEE 802.11i와 WPA에서 공통으로 채택하고 있으며, WPA에서는 선택사항으로 규정되어 있고, WPA2에서는 강제 사항으로 규정되어 있다.

[0007] 한편, 상기 AES-CCM은, 위에서 언급한 바와 같이 이미 검증된 두 가지 표준 기술을 사용하기 때문에 높은 신뢰성을 나타내는 이점이 있다. 또한, 일반적으로 인증 및 암호화에 다른 키를 사용하는 것과는 달리, 하나의 키만을 사용할 수 있는 장점이 있다. 또한, 암호화 없이 무결성 검증만을 필요로 하는 데이터가 포함된 경우에도 AES-CCM을 이용하면, 추가적인 암호문 오버헤드 없이 암호화할 수 있어 데이터를 다루기가 용이하다는 장점이 있다. 나아가, AES-CCM은 암호화 함수 하나만을 사용하여 암호화 및 복호화를 모두 수행하기 때문에 비교적 작은 크기의 코드로 구현 할 수 있다는 장점이 있다. 이러한 장점들은, 다른 운용모드들에 비해 AES-CCM의 융통성 있는 적용을 가능하게 한다.

[0008] 그러나, 기존 기술은, 암호화 및 메시지 무결성을 위해 두 가지 작업을 필요로 하는 AES-CCM을 처리함에 있어 단일 코어를 이용하는 점에서, 암호화 프로세스 및 컴퓨팅 시간이 지연되고 처리 속도가 떨어지는 문제점이 있다.

[0009] 또한, 기존 기술은, AES-CCM 처리 속도를 고려하여 전용 하드웨어 칩을 사용하는 점에서, 자원 효율성이 떨어지며 호환성을 저해하는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

[0010] 따라서, 본 발명이 해결하고자 하는 첫 번째 기술적 과제는, 범용 멀티코어 프로세서를 이용하여 AES-CCM를 병렬처리함으로써, 데이터 기밀성 및 무결성을 동시에 보장함은 물론, 처리 속도 및 자원 효율성을 개선하고 프로세서 호환성을 지니는 AES-CCM 병렬처리 장치를 제공하는 것이다.

[0011] 본 발명이 해결하고자 하는 두 번째 기술적 과제는, 범용 멀티코어 프로세서를 이용하여 AES-CCM를 병렬처리함으로써, 데이터 기밀성 및 무결성을 동시에 보장함은 물론, 처리 속도 및 자원 효율성을 개선하고 프로세서 호환성을 지니는 AES-CCM 병렬처리 방법을 제공하는 것이다.

과제 해결수단

[0012] 상기와 같은 첫 번째 기술적 과제를 해결하기 위하여 본 발명은, AES-CCM의 처리 대상 태스크(task)에 대해 범용 멀티코어 프로세서의 코어를 할당하는 코어 할당부; 및 상기 할당된 코어의 개수에 대응하여 상기 처리 대상 태스크에 대한 데이터 병렬화(data parallelism)를 수행하는 데이터 병렬화부를 포함하고, 상기 범용 멀티코어 프로세서는, 상기 데이터 병렬화된 상기 처리 대상 태스크를 상기 할당된 코어를 통해 병렬적으로 수행하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치를 제공한다.

[0013] 일 실시예에 있어서, 상기 코어 할당부는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 없는 경우, 상기 처리 대상 태스크에 대해 상기 범용 멀티코어 프로세스의 코어들 중 2 이상을 할당한다.

[0014] 일 실시예에 있어서, 상기 코어 할당부는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 있는 경우, 상기 처리 대상 태스크에 대해 상기 범용 멀티코어 프로세스의 코어들 중 하나의 코어를 할당한다.

[0015] 일 실시예에 있어서, 상기 코어 할당부는, 상기 범용 멀티코어 프로세스의 코어들 중에서, 상기 처리 대상 태스크가 CTR(Counter)인 경우 2 이상의 코어를 할당하고, 상기 처리 대상 태스크가 CBC-MAC(Cipher Block Chaining-Message Authentication Code)인 경우 하나의 코어를 할당한다.

[0016] 일 실시예에 있어서, 상기 코어 할당부는, 상기 처리 대상 태스크가 상기 CTR인 경우, 상기 범용 멀티코어 프로

세스의 코어 전체를 할당한다.

[0017] 일 실시예에 있어서, 상기 범용 멀티코어 프로세서는, 상기 CTR 및 상기 CBC-MAC에 대한 처리 수행시, 상기 CTR 또는 상기 CBC-MAC에 대한 처리를 먼저 수행한다.

[0018] 일 실시예에 있어서, 상기 데이터 병렬화부는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 있는 경우, 상기 데이터 병렬화를 수행하지 않는다.

[0019] 일 실시예에 있어서, 상기 데이터 병렬화부는, 상기 처리 대상 태스크가 CBC-MAC인 경우, 상기 데이터 병렬화를 수행하지 않는다.

[0020] 일 실시예에 있어서, 상기 AES-CCM 병렬처리 장치는, 상기 AES-CCM의 처리 대상 태스크들 중, CTR 및 CBC-MAC에 대한 태스크 병렬화(task parallelism)를 수행하는 태스크 병렬화부를 더 포함한다.

[0021] 일 실시예에 있어서, 상기 코어 할당부는, 상기 범용 멀티코어 프로세스의 코어들 중에서, 상기 CBC-MAC에 대해서는 하나의 코어를 할당하고, 상기 CTR에 대해서는 1 또는 2 이상의 코어를 할당한다.

[0022] 일 실시예에 있어서, 상기 데이터 병렬화부는, 상기 CTR에 대해서만 상기 데이터 병렬화를 수행한다.

[0023] 일 실시예에 있어서, 상기 범용 멀티코어 프로세서는, 상기 CTR 및 상기 CBC-MAC에 대한 처리를 병렬적으로 수행한다.

[0024] 상기와 같은 두 번째 기술적 과제를 해결하기 위하여 본 발명은, 범용 멀티코어 프로세서를 사용하는 컴퓨터 시스템에서, AES-CCM의 처리 대상 태스크(task)에 대해 상기 범용 멀티코어 프로세서의 코어를 할당하는 코어 할당 단계; 상기 컴퓨터 시스템에서, 상기 할당된 코어의 개수에 대응하여 상기 처리 대상 태스크에 대한 데이터 병렬화(data parallelism)를 수행하는 데이터 병렬화 단계; 및 상기 범용 멀티코어 프로세서에서, 상기 데이터 병렬화된 상기 처리 대상 태스크를 상기 할당된 코어를 통해 병렬적으로 처리하는 처리 단계를 포함하는 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 방법을 제공한다.

[0025] 본 발명의 다른 일 태양에 있어서, 본 발명에 따른 AES-CCM 병렬처리 방법은, 범용 멀티코어 프로세서를 사용하는 컴퓨터 시스템에서, AES-CCM의 처리 대상 태스크들 중, CTR 및 CBC-MAC에 대한 태스크 병렬화(task parallelism)를 수행하는 태스크 병렬화 단계; 상기 컴퓨터 시스템에서, 상기 범용 멀티코어 프로세스의 코어들 중에서, 상기 CBC-MAC에 대해서는 하나의 코어를 할당하고, 상기 CTR에 대해서는 1 또는 2 이상의 코어를 할당하는 코어 할당 단계; 상기 컴퓨터 시스템에서, 상기 할당된 코어의 개수에 대응하여 상기 CTR에 대한 데이터 병렬화(data parallelism)를 수행하는 데이터 병렬화 단계; 및 상기 범용 멀티코어 프로세서에서, 상기 데이터 병렬화된 CTR 및 상기 CBC-MAC를 상기 할당된 코어를 통해 병렬적으로 처리하는 처리 단계를 포함한다.

[0026] 일 실시예에 있어서, 본 발명은, 상기 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체로 구현될 수 있다.

[0027] 일 실시예에 있어서, 상기 프로그램은, 병렬적으로 작동하는 소프트웨어의 작성에 사용되는 표준 API(Application Programming Interface)인 Pthread(POSIX Threads)를 통해 프로그래밍된다.

효 과

[0028] 본 발명은, AES-CCM를 병렬처리함으로써, 데이터 기밀성 및 무결성을 동시에 보장함은 물론, 처리 속도 및 자원 효율성을 개선하는 이점을 제공한다.

[0029] 또한, 범용 멀티코어 프로세서를 이용함으로써, 별도의 하드웨어를 필요로 하지 않고 비용 효율적인 솔루션 개발을 가능하게 하는 이점을 제공한다.

[0030] 나아가, Pthread를 사용함으로써, 다양한 CPU에 적용될 수 있는 호환성을 지닌다는 이점을 제공한다.

발명의 실시를 위한 구체적인 내용

[0031] 이하, 본 발명의 기술적 과제의 해결 방안을 명확화하기 위해 첨부도면을 참조하여 본 발명의 바람직한 실시예를 상세하게 설명한다. 다만, 본 발명을 설명함에 있어서 관련 공지기술에 관한 설명이 오히려 본 발명의 요지를 불명료하게 할 수 있다고 판단되는 경우 그에 관한 설명을 생략하기로 한다. 또한, 후술하는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자 등의 의도 또는 관례 등에 따라 달라질 수 있을 것이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0032] 도 1에는 본 발명에 따른 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치의 일례가 블록도로 도시되어 있다.

[0033] 도 1에 도시된 바와 같이, 본 발명에 따른 AES-CCM 병렬처리 장치(100)는, 코어 할당부(120), 데이터 병렬화부(130) 및 범용 멀티코어 프로세서(140)를 포함하며, 태스크 병렬화부(110)를 더 포함할 수 있다.

[0034] 우선, 상기 AES-CCM 병렬처리 장치(100)가 수행하는 AES-CCM 처리 과정을 분석한다.

[0035] 도 2에는 AES-CCM의 처리 과정이 순서도로 도시되어 있다.

[0036] 도 2에 도시된 바와 같이, AES-CCM의 처리 과정은, 키 초기화 과정(S210), 메시지 헤더 검증 처리 과정(S220), CTR 및 CBC-MAC을 이용하여 메시지 암호화/인증을 수행하는 과정(S230), 및 MAC 계산을 통해 MAC 값을 검증하는 과정(S240)을 포함한다.

[0037] 상기 키 초기화 과정(S210) 및 메시지의 헤더 검증 처리 과정(S220)의 경우, 작은 데이터를 처리하기 때문에 전체 수행시간에 큰 영향을 미치지 않는다. 또한, 상기 MAC 계산 과정(S240)도 암호화 처리가 된 블록을 XOR 연산만 하는 과정이기 때문에 굳이 병렬처리할 이유가 없다. 실제 구현에 있어서, 데이터 처리량이 적은 태스크를 병렬화하는 경우 오히려 병렬화에 따른 복잡한 처리 과정이 효율성을 저해할 수 있다.

[0038] 한편, 상기 메시지 암호화/인증 과정(S230)은, CTR(Counter)을 이용하여 메시지를 암호화하는 계산과 CBC-MAC(Cipher Block Chaining-Message Authentication Code Protocol)을 이용하여 MAC 블록을 생성하는 계산을 수행한다. 상기 메시지 암호화/인증 과정(S230)은, 전체 메시지를 암호화/인증 블록의 개수만큼 처리해야하기 때문에 AES-CCM 전체 수행시간의 대부분을 차지하게 된다. 또한, 상기 두 과정은 모두 AES 암호화를 이용하고 같은 크기의 메시지를 처리하기 때문에 거의 비슷한 수행 시간이 소요된다.

[0039] 따라서, 본 발명은, AES-CCM에 있어서, 특히 상기 메시지 암호화/인증 과정(S230)을 효율적으로 병렬처리하고자 하는 것이다.

[0040] 도 3에는 CTR 운용모드의 처리 과정이 도시되어 있다.

[0041] 도 3에 도시된 바와 같이, CTR은 임의의 수(Nonce)와 카운터(Counter)를 이용해 만든 블록을 일정한 값으로 증가하여 암호화에 사용하기 때문에 블록 암호를 스트림 암호처럼 사용할 수 있게 해준다. 특히, 키와 Nonce를 미리 계산할 수 있기 때문에 데이터를 실시간 암호화할 수 있으며, 처리 과정에서 데이터 간에 종속성을 지니지 않는다. 아래에서 다시 설명하겠지만, 본 발명에 따른 병렬처리 장치 및 방법은, 상기 CTR의 데이터 독립성을 고려하여 상기 CTR에 대해 데이터 병렬화(data-level parallelism 또는 data parallelism)를 수행한다.

[0042] 도 4에는 CBC-MAC 운용모드의 처리 과정이 도시되어 있다.

[0043] 도 4에 도시된 바와 같이, 무결성을 보장하는 방법인 CBC-MAC는, 한 메시지 블록을 초기 벡터(IV)와 같이 암호화하는 것을 시작으로 그 값을 다음 암호화에 이용하는 체이닝(Chaining) 기법인 CBC(Cipher Block Chaining)를 이용한다. CBC-MAC은, CBC의 마지막 암호화된 블록을 메시지의 무결성을 인증하는 코드인 MAC으로 사용하는 방법이다. CBC는 블록 암호화 데이터의 독립성을 제거하는 체이닝을 수행하기 때문에 일부 데이터가 변조되었을 때 나머지 데이터들에게도 변조를 전파하는 특성을 가진다. 즉, CBC의 마지막 블록을 MAC으로 사용하여 변조를 확인하면 데이터의 무결성을 검증할 수 있다. 아래에서 다시 설명하겠지만, 상기 CBC-MAC 데이터 종속성을 고려하여 상기 CBC-MAC에 대해서는 데이터 병렬화를 수행하지 않는다.

[0044] 도 5에는 AES-CCM 운용모드의 전체 처리 과정이 도시되어 있다.

[0045] 도 5에 도시된 바와 같이, AES-CCM은 하나의 키(key)로 기밀성과 무결성을 동시에 보장할 수 있다. 즉, AES-CCM은 운용모드 중 하나인 상기 CTR을 이용하여 데이터의 기밀성을 제공하면서, 상기 CBC-MAC을 이용하여 메시지 인증 및 무결성을 제공한다. 먼저, CBC를 이용하여 MAC으로 사용할 암호화 블록을 만들고, CTR을 이용해 메시지를 암호화한다. 실시예에 따라, 상기 CBC 및 상기 CTR의 처리 순서는 조정될 수 있다.

[0046] 도 6에는 본 발명에 따른 AES-CCM 병렬처리 방법의 일례가 순서도로 도시되어 있다.

[0047] AES-CCM 전체 수행시간의 대부분을 차지하는 상기 메시지 암호화/인증 과정(S230)에서 데이터 병렬화(data-level parallelism)를 활용하기 위해서는 데이터 사이의 종속성이 없어야 한다. 그러나, CTR 모드와 달리, CBC-MAC의 경우 블록간의 체이닝으로 종속성이 존재하므로, 데이터 병렬화가 가능한 CTR만을 병렬처리하는 방법을 생각할 수 있다.

[0048] 도 1 및 도 6을 참조하면, 우선, 상기 코어 할당부(120)는, AES-CCM의 처리 대상 태스크(task)에 대해 상기 범용 멀티코어 프로세서(140)의 코어를 할당한다(S610). 이 경우, 상기 코어 할당부(120)는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 없는 경우, 상기 처리 대상 태스크에 대해 상기 범용 멀티코어 프로세스(140)의 코어들 중 2 이상을 할당할 수 있다. 반면, 상기 코어 할당부(120)는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 있는 경우, 상기 처리 대상 태스크에 대해 상기 범용 멀티코어 프로세서(140)의 코어들 중 하나의 코어를 할당할 수 있다.

[0049] 일 실시예에 있어서, 상기 코어 할당부(120)는, 상기 범용 멀티코어 프로세서(140)의 코어들 중에서, 상기 처리 대상 태스크가 CTR(Counter)인 경우 2 이상의 코어를 할당하고, 상기 처리 대상 태스크가 CBC-MAC(Cipher Block Chaining-Message Authentication Code)인 경우 하나의 코어를 할당할 수 있다. 물론, 상기 코어 할당부(120)는, 상기 처리 대상 태스크가 상기 CTR인 경우, 상기 범용 멀티코어 프로세스의 코어 전체를 할당할 수 있다.

[0050] 그 다음, 상기 데이터 병렬화부(130)는, 상기 할당된 코어의 개수에 대응하여 상기 처리 대상 태스크에 대한 데이터 병렬화(data level parallelism 또는 data parallelism)를 수행한다(S620). 이 경우, 상기 데이터 병렬화부(130)는, 상기 처리 대상 태스크의 데이터들 간에 종속성이 있는 경우, 상기 데이터 병렬화를 수행하지 않는다. 즉, 상기 데이터 병렬화부(130)는, 상기 처리 대상 태스크가 CBC-MAC인 경우, 상기 데이터 병렬화를 수행하지 않는다.

[0051] 그 다음, 상기 범용 멀티코어 프로세서(140)는, 상기 데이터 병렬화된 상기 처리 대상 태스크를 상기 할당된 코어를 통해 병렬적으로 수행한다(S630). 이 경우, 상기 범용 멀티코어 프로세서(140)는, 태스크들 간 병렬처리는 수행하지 않는다. 즉, 상기 CTR 및 상기 CBC-MAC에 대한 처리 수행시, 상기 CTR 또는 상기 CBC-MAC에 대한 처리를 먼저 수행한다.

[0052] 도 7에는 도 6의 AES-CCM 병렬처리 방법에 따른 범용 멀티코어 프로세서(140)의 처리 과정이 도시되어 있다.

[0053] 도 7에 도시된 바와 같이, 상기 범용 멀티코어 프로세서(140)는 쿼드 코어(Quad Core) 프로세서일 수 있으며, 4개의 코어 전체에서 상기 CTR을 데이터 병렬화하여 처리한 후, 하나의 코어에서 상기 CBC-MAC 블록 생성을 수행할 수 있다.

[0054] 도 8에는 본 발명에 따른 AES-CCM 병렬처리 방법의 다른 일례가 순서도로 도시되어 있다.

[0055] 상기 CTR 및 상기 CBC-MAC에 대한 태스크 병렬화 및 상기 CTR에 대한 데이터 병렬화를 동시에 수행하는 경우, AES-CCM 수행시간을 더욱 감소시킬 수 있다.

[0056] 도 1 및 도 8을 참조하면, 본 발명에 따른 AES-CCM 병렬처리 장치(100)는, 상기 태스크 병렬화부(110)를 더 포함하여, 상기 AES-CCM의 처리 대상 태스크들 중, CTR 및 CBC-MAC에 대한 태스크 병렬화(task parallelism)를 수행하는 할 수 있다(S810).

[0057] 그러면, 상기 코어 할당부(120)는, 상기 범용 멀티코어 프로세서(140) AES-CCM의 처리 대상 태스크(task)에 대해 상기 범용 멀티코어 프로세서(140)의 코어를 할당한다(S820). 특히, 상기 코어 할당부(120)는, 상기 범용 멀티코어 프로세서(140)의 코어들 중에서, 상기 CBC-MAC에 대해서는 하나의 코어를 할당하고, 상기 CTR에 대해서는 1 또는 2 이상의 코어를 할당할 수 있다. 물론, 상기 코어 할당부(120)는, 상기 CTR에 대해 상기 CBC-MAC에 할당된 코어 이외에 나머지 모든 코어를 할당할 수도 있다.

[0058] 그 다음, 상기 데이터 병렬화부(130)는, 상기 할당된 코어의 개수에 대응하여 상기 처리 대상 태스크에 대한 데이터 병렬화를 수행한다(S830). 특히, 상기 데이터 병렬화부(130)는, 상기 CTR에 대해서만 상기 데이터 병렬화를 수행할 수 있다. 앞에서 언급한 바와 같이, 상기 CBC-MAC는 데이터 종속성이 존재하기 때문이다.

[0059] 그 다음, 상기 범용 멀티코어 프로세서(140)는, 상기 데이터 병렬화된 상기 처리 대상 태스크를 상기 할당된 코어를 통해 병렬적으로 수행한다(S840). 특히, 상기 범용 멀티코어 프로세서(140)는, 상기 CTR 및 상기 CBC-MAC에 대한 처리를 병렬적으로 수행한다.

[0060] 도 9에는 도 8의 AES-CCM 병렬처리 방법에 따른 범용 멀티코어 프로세서(140)의 처리 과정이 도시되어 있다.

[0061] 도 9에 도시된 바와 같이, 상기 범용 멀티코어 프로세서(140)는 쿼드 코어(Quad Core) 프로세서일 수 있으며, 4개의 코어들 중 상기 CTR에 대해 3개, 상기 CBC-MAC에 대해 1개의 코어를 할당하여 상기 CTR 및 상기 CBC-MAC에 대한 처리를 병렬적으로 수행할 수 있다.

[0062] 한편, 본 발명은 컴퓨터로 판독할 수 있는 기록매체에 컴퓨터가 읽어들일 수 있는 프로그램 코드로서 구현하는 것이 가능하다. 이 경우, 프로그램은, 병렬적으로 작동하는 소프트웨어의 작성에 사용되는 표준 API(Application Programming Interface)인 Pthread(POSIX Threads)를 통해 프로그래밍될 수 있다. 상기 Pthread를 사용하는 경우, 다양한 멀티코어 CPU에서 동작하도록 병렬프로그램의 호환성을 제공할 수 있다.

[0063] 본 발명이 이러한 소프트웨어를 통해 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 또한, 프로그램 또는 코드 세그먼트들은 컴퓨터의 프로세서 판독가능 매체에 저장되거나 전송 매체 또는 통신망을 통해 반송파와 결합된 컴퓨터 데이터 신호로 전송될 수 있다.

[0064] 컴퓨터 판독가능 기록매체에는 컴퓨터 시스템에 의해 읽혀질 수 있는 데이터를 저장하는 모든 종류의 기록장치가 포함된다. 예컨대, 컴퓨터 판독가능 기록매체에는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 포함될 수 있다. 또한, 컴퓨터 판독가능 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 컴퓨터가 읽어들일 수 있는 코드를 분산방식으로 저장하고 실행되도록 할 수 있다.

[0065] 또한, 본 발명은 시스템 온 칩(system on chip) 기술로 구현하여 상기 마이크로프로세서로 하여금 상술한 AES-CCM 병렬처리 동작을 수행하도록 할 수 있다. 본 발명을 마이크로프로세서로 구현하면 각종 시스템의 크기를 줄일 수 있고, 조립 과정을 단순화시킬 수 있으며, 제조 비용을 절감할 수 있는 등의 이점이 있다.

[0066] 이하, 본 발명의 현저한 효과를 검증한다.

[0067] 도 10에는 본 발명에 따른 AES-CCM 병렬처리 수행시간 측정 실험 결과가 그래프로 도시되어 있다.

[0068] 상기 실험에 있어서, Intel Core2 Quad CPU 2.33GHz의 실험환경에서 다양한 크기의 데이터를 암/복호화하였다. 실험에 이용되는 키 길이는 128bit, 초기벡터(IV)는 12byte, 그리고 태그는 16byte를 사용하였다. 데이터를 10MB부터 50MB까지, 10MB씩 증가시켜 가면서 단일코어를 이용하는 기존의 방법(SEQ)과 비교 측정하였으며, 본 발명에 따른 AES-CCM 병렬처리 방법으로서, CTR에 대해 데이터 병렬화를 수행하는 방법(CTR)과, CTR 및 CBC-MAC에 대해 태스크 병렬화 및 데이터 병렬화 를 동시에 수행하는 (CTR+CBC)방법을 사용하였다.

[0069] 도 10에 도시된 바와 같이, 본 발명은, AES-CCM에서 CTR에만 데이터 병렬화(data-level parallelism)을 이용할 경우 기존의 방법에 비해 수행시간이 약 35%정도 감소함을 알 수 있으며, CTR 및 CBC-MAC에 대해 태스트 병렬화(task-level parallelism) 및 데이터 병렬화를 동시에 활용할 경우 수행시간이 약 50%정도까지 현저히 감소함을 알 수 있다.

[0070] 한편, 최근 반도체 집적도 증가에 따라, standalone PC 뿐만 아니라 임베디드 시스템에서도 범용 멀티코어 CPU를 탑재하는 추세에 있다. 이러한 추세에서, 본 발명에 따라 범용 멀티코어 CPU를 활용하여 AES-CCM을 병렬처리한다면, 전용 하드웨어 칩을 전제로 하는 기존의 솔루션들보다 비용 효율적인 솔루션을 확보할 수 있는 방안을 제시할 수 있을 것으로 기대된다.

[0071] 상술한 바와 같이, 본 발명은, AES-CCM를 병렬처리함으로써, 데이터 기밀성 및 무결성을 동시에 보장함은 물론, 처리 속도 및 자원 효율성을 개선하는 이점을 제공한다. 또한, 범용 멀티코어 프로세서를 이용함으로써, 별도의 하드웨어를 필요로 하지 않고 비용 효율적인 솔루션 개발을 가능하게 하는 이점을 제공한다. 나아가, Pthread를 사용함으로써, 다양한 CPU에 적용될 수 있는 호환성을 지닌다는 이점을 제공한다.

[0072] 지금까지 본 발명에 대해 실시예들을 참고하여 설명하였다. 그러나 당업자라면 본 발명의 본질적인 기술적 사상으로부터 벗어나지 않는 범위에서 본 발명이 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 즉, 본 발명의 진정한 기술적 범위는 첨부된 특허청구범위에 나타나 있으며, 그와 균등범위 내에 있는 모든 차이점은 본 발명에 포함되는 것으로 해석되어야 할 것이다.

도면의 간단한 설명

[0073] 도 1은 본 발명에 따른 범용 멀티코어 프로세스를 이용한 AES-CCM 병렬처리 장치의 일례를 나타낸 블록도.

[0074] 도 2는 AES-CCM의 처리 과정을 나타낸 순서도.

[0075] 도 3은 CTR 운용모드의 처리 과정을 나타낸 도면.

[0076] 도 4는 CBC-MAC 운용모드의 처리 과정을 나타낸 도면.

[0077] 도 5는 AES-CCM 운용모드의 전체 처리 과정을 나타낸 도면.

[0078] 도 6은 본 발명에 따른 AES-CCM 병렬처리 방법의 일례를 나타낸 순서도.

[0079] 도 7은 도 6의 AES-CCM 병렬처리 방법에 따른 범용 멀티코어 프로세서의 처리 과정을 나타낸 도면.

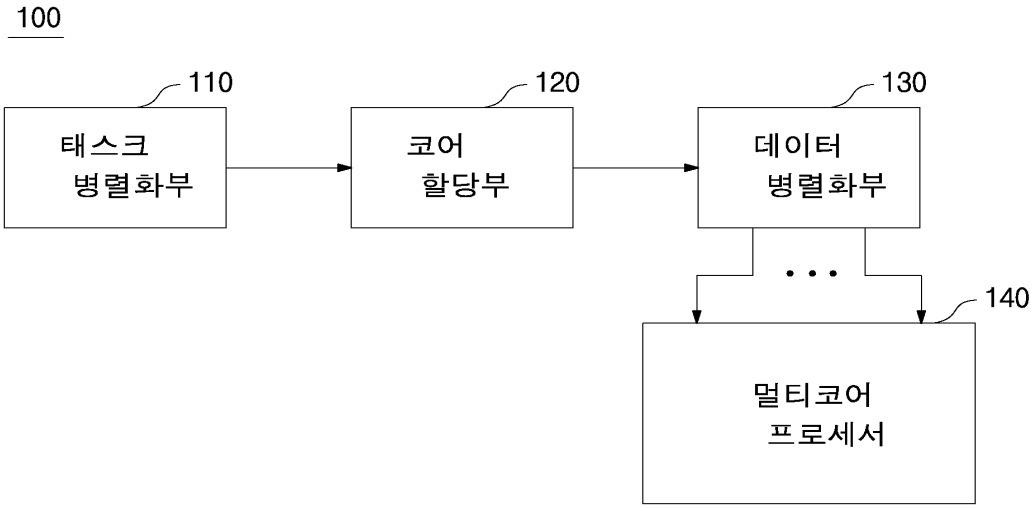
[0080] 도 8은 본 발명에 따른 AES-CCM 병렬처리 방법의 다른 일례를 나타낸 순서도.

[0081] 도 9는 도 8의 AES-CCM 병렬처리 방법에 따른 범용 멀티코어 프로세서의 처리 과정을 나타낸 도면.

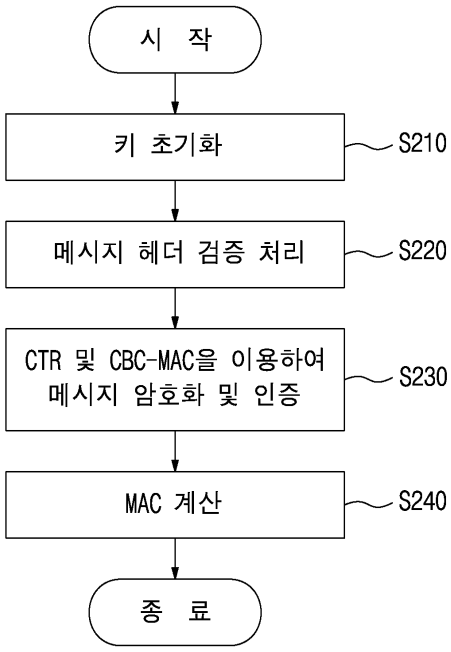
[0082] 도 10은 본 발명에 따른 AES-CCM 병렬처리 수행시간 측정 실험 결과를 나타낸 그래프.

도면

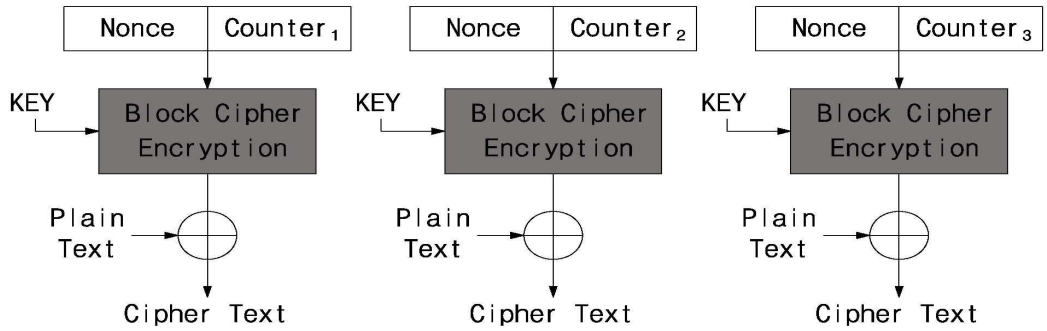
도면1



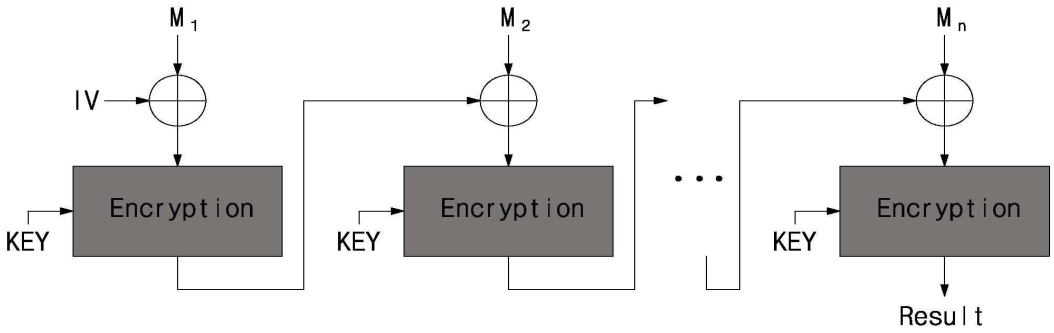
도면2



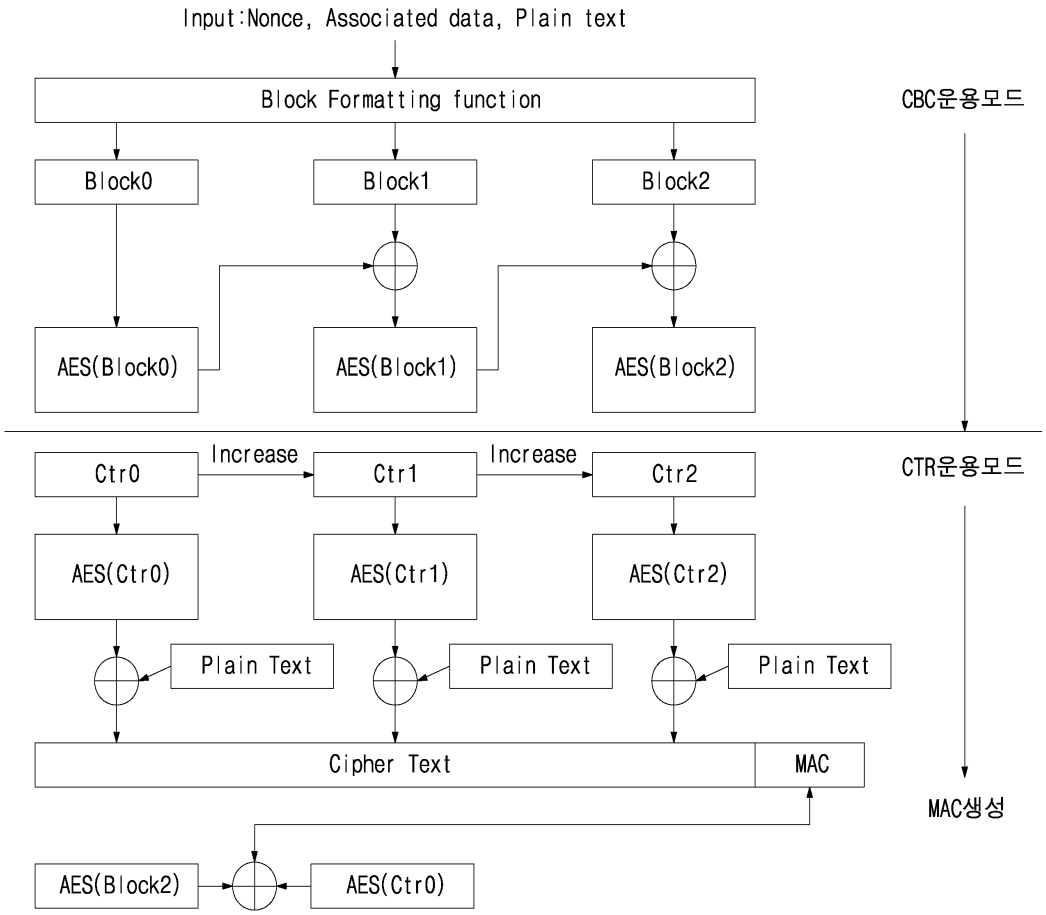
도면3


Nonce
Counter 1
KEY
Block Cipher Encryption
Plain Text
Cipher Text
Nonce
Counter 2
KEY
Block Cipher Encryption
Plain Text
Cipher Text
Nonce
Counter 3
KEY
Block Cipher Encryption
Plain Text
Cipher Text

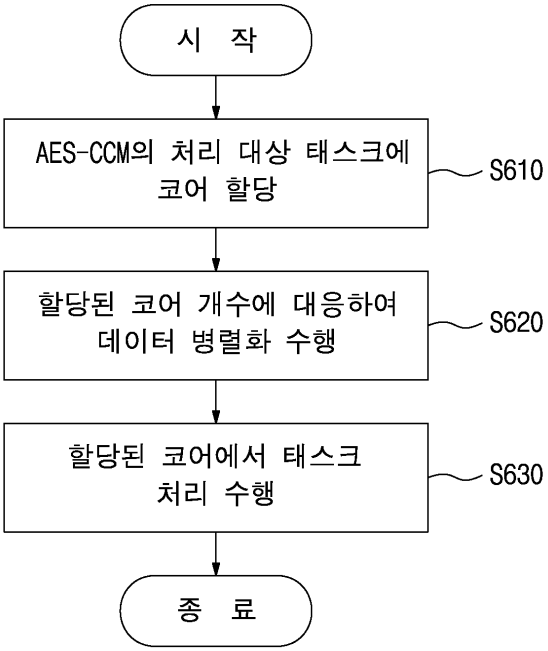
도면4


M 1
IV
Encryption
KEY
M 2
Encryption
KEY
M n
Encryption
KEY
Result

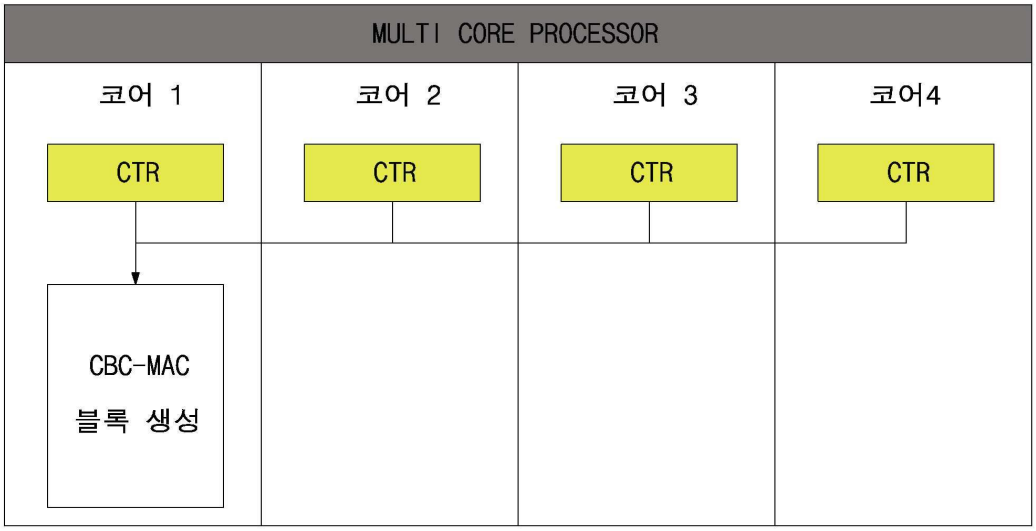
도면5


Input:Nonce, Associated data, Plain text
Block Formatting function
CBC운용모드
Block0
Block1
Block2
AES(Block0)
AES(Block1)
AES(Block2)
Ctr0
Increase
Ctr1
Increase
Ctr2
CTR운용모드
AES(Ctr0)
AES(Ctr1)
AES(Ctr2)
Plain Text
Plain Text
Plain Text
Cipher Text
MAC
MAC생성
AES(Block2)
AES(Ctr0)

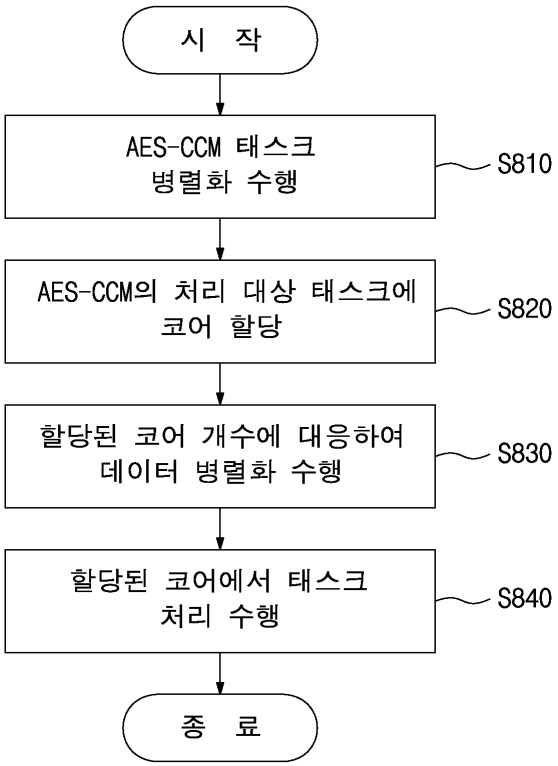
도면6


시 작
AES-CCM의 처리 대상 태스크에 코어 할당
S610
할당된 코어 개수에 대응하여 데이터 병렬화 수행
S620
할당된 코어에서 태스크 처리 수행
S630
종 료

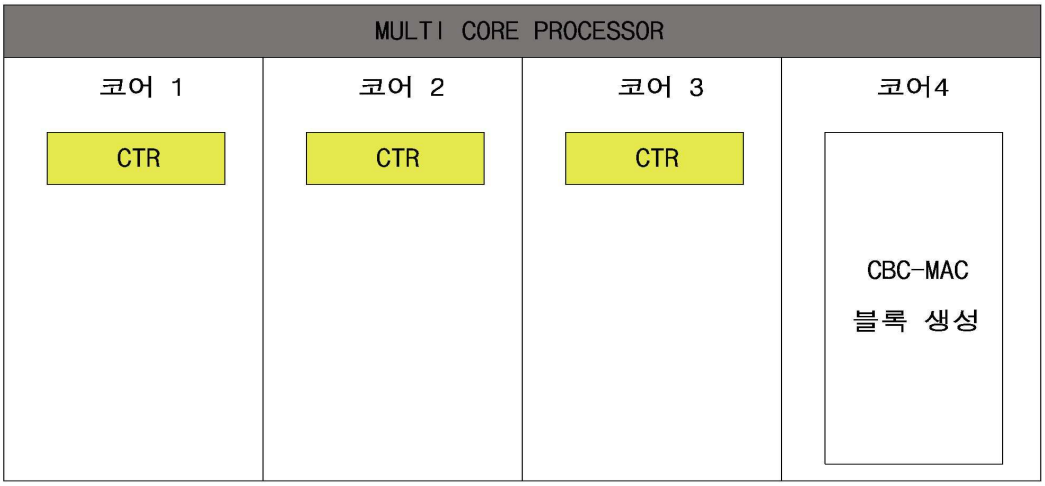
도면7


MULTI CORE PROCESSOR
코어 1
코어 2
코어 3
코어4
CTR
CTR
CTR
CTR
CBC-MAC
블록 생성

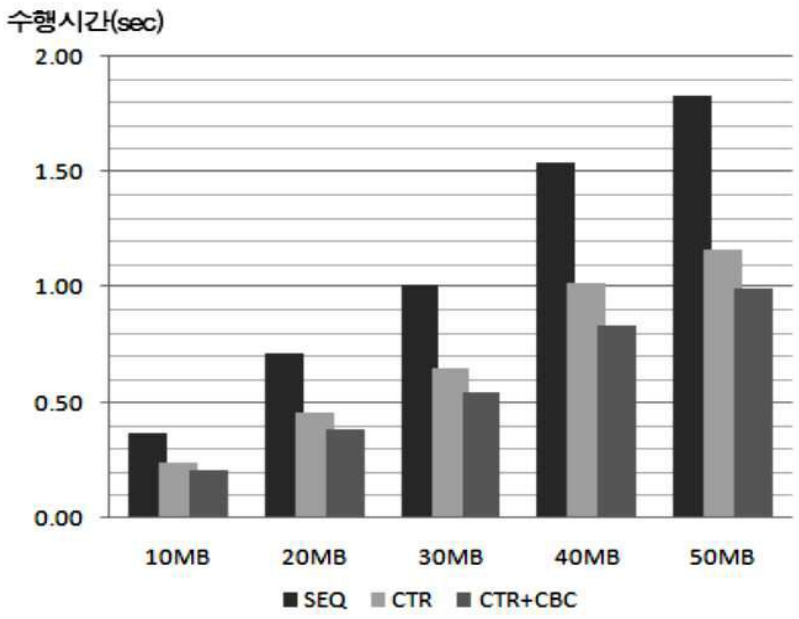
도면8


시 작
AES-CCM 태스크
병렬화 수행
S810
AES-CCM의 처리 대상 태스크에
코어 할당
S820
할당된 코어 개수에 대응하여
데이터 병렬화 수행
S830
할당된 코어에서 태스크
처리 수행
S840
종 료

도면9


MULTI CORE PROCESSOR
코어 1
CTR
코어 2
CTR
코어 3
CTR
코어4
CBC-MAC
블록 생성

도면10


수행시간(sec)
2.00
1.50
1.00
0.50
0.00
10MB
20MB
30MB
40MB
50MB
SEQ
CTR
CTR+CBC