(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0071844
(43) 공개일자 2012년07월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/28 (2006.01) *H04L 9/06* (2006.01)
(21) 출원번호 10-2010-0133553
(22) 출원일자 2010년12월23일
심사청구일자 없음
기술이전 희망 : 기술양도, 실시권허여, 기술지도

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
장구영
대전광역시 유성구 배울1로 35, 대덕테크노밸리아파트 407동 1002호 (관평동)
홍석희
서울특별시 도봉구 마들로 859-19, 한신아파트 103동 107호 (도봉동)
(뒷면에 계속)
(74) 대리인
김원준, 제일특허법인

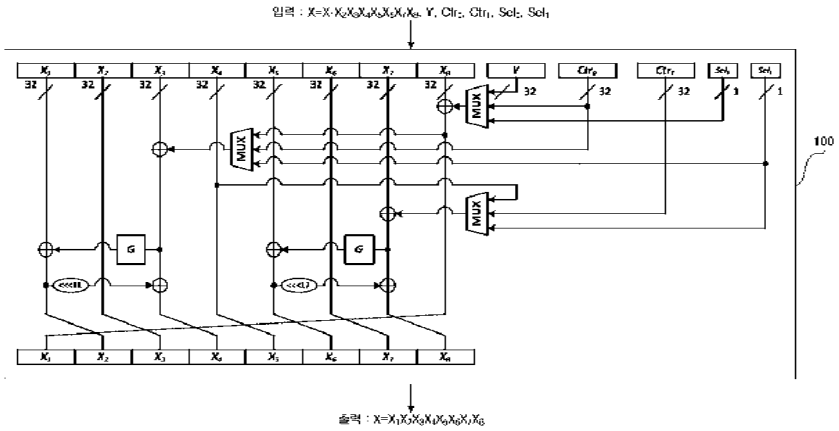
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **기밀성과 무결성을 제공하는 통합 암호화 장치 및 그 방법**

(57) 요 약

본 발명은 기밀성과 무결성을 제공하는 통합 암호화 기술에 관한 것으로, 유비쿼터스 컴퓨팅 환경과 같이 제약된 구현 환경에서 기밀성 및 무결성 기능을 보장할 수 있는 통합 암호 모듈 구성 방법을 제시하며, 무결성 기능을 제공하는 해쉬함수 H, 기밀성 기능을 제공하는 블록암호 BC를 포함한다. 통합 암호 모듈 ICM을 이용하여 대표적인 데이터 암호 알고리즘인 블록암호와 메시지 변조 여부를 파악할 수 있는 해쉬함수를 동시에 구성하는 것을 특징으로 한다. 본 발명에 의하면, 하나의 통합된 암호 모듈을 이용하여 두 개의 프리미티브 블록암호와 해쉬함수를 동작시킬 수 있기 때문에, 하드웨어 및 소프트웨어 환경에서 구현될 경우, 독립적인 두 개의 알고리즘을 구현해야 하는 기존의 암호 시스템보다 효율적으로 암호 시스템을 구성할 수 있다.

대 표 도 - 도1



(72) 발명자

이제상

서울특별시 도봉구 방학로11길 10, 한화아파트 102동 1408호 (방학동)

성재철

서울특별시 강북구 삼각산로 143-1, 벽산아파트 3동 1201호 (수유동)

강진건

서울특별시 양천구 목동서로 155, 107동 303호 (목동, 목동파라곤)

특허청구의 범위

청구항 1

기밀성 및 무결성 기능을 포함하는 통합 암호 모듈과,

상기 통합 암호 모듈을 토대로 메시지 변조 여부를 파악하는 해쉬함수와,

상기 통합 암호 모듈을 토대로 데이터 암호 알고리즘을 구성하는 블록암호

를 포함하는 기밀성과 무결성을 제공하는 기밀성과 무결성을 제공하는 통합 암호화 장치.

청구항 2

제 1항에 있어서,

상기 통합 암호 모듈은,

입력된 비트에 대해 S-박스, 순환이동, XOR 을 포함하는 연산으로 값을 출력하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 장치.

청구항 3

제 1항에 있어서,

상기 해쉬함수는,

입력된 임의 길이의 비트열을 32비트 워드열로 변환하는 메시지 사전 처리부와,

상기 32비트 워드열로 변환된 메시지를 압축하는 메시지 압축부와,

상기 메시지 압축부로부터 출력된 값으로 어느 한 해쉬 길이의 해쉬값을 출력하는 해쉬값 추출부

를 포함하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 장치.

청구항 4

제 3항에 있어서,

상기 메시지 사전 처리부는,

입력된 메시지에 대한 비트열이 32비트의 배수가 되도록 마지막 비트에 하나의 1과 적어도 하나의 0을 추가하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 장치.

청구항 5

제3항에 있어서,

상기 메시지 압축부는,

상기 32비트 워드열로 변환된 메시지를 상태 갱신 함수를 이용하여 순차적으로 압축하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 장치.

청구항 6

제4항에 있어서,

상기 상태 갱신 함수는,

입력된 값에 대해 상기 통합 암호 모듈을 반복 적용하여 상기 입력된 값을 갱신하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 장치.

청구항 7

제3항에 있어서,

상기 해쉬값 추출부는,

해쉬함수의 길이에 대응하는 상태 갱신 함수를 수행하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 장치.

청구항 8

제 1항에 있어서,

상기 블록암호는,

128비트 평문 및 128비트 키를 입력 받아 적어도 하나의 통합 암호 모듈의 반복을 통해 128비트 암호문을 출력하는 함수인 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 장치.

청구항 9

기밀성 및 무결성 기능을 포함하는 통합 암호 모듈을 토대로 메시지 변조 여부를 파악하는 해쉬함수를 생성하는 과정과,

상기 통합 암호 모듈을 토대로 데이터 암호 알고리즘을 구성하는 블록암호를 생성하는 과정

을 포함하는 기밀성과 무결성을 제공하는 통합 암호화 방법.

청구항 10

제 9항에 있어서,

상기 통합 암호 모듈은,

입력된 비트에 대해 S-박스, 순환이동, XOR 을 포함하는 연산으로 값을 출력하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 방법.

청구항 11

제 9항에 있어서,

상기 해쉬함수를 생성하는 과정은,

입력된 임의 길이의 비트열을 32비트 워드열로 변환하는 메시지 사전 처리 과정과,

상기 32비트 워드열로 변환된 메시지를 압축하는 메시지 압축 과정과,

상기 메시지 압축부로부터 출력된 값으로 어느 한 해쉬 길이의 해쉬값을 출력하는 해쉬값 추출 과정

을 포함하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 방법.

청구항 12

제 11항에 있어서,

상기 메시지 사전 처리 과정은,

입력된 메시지에 대한 비트열이 32비트의 배수가 되도록 마지막 비트에 하나의 1과 적어도 하나의 0을 추가하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 방법.

청구항 13

제11항에 있어서,

상기 메시지 압축 과정은,

상기 32비트 워드열로 변환된 메시지를 상태 갱신 함수를 이용하여 순차적으로 압축하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 방법.

청구항 14

제13항에 있어서,

상기 상태 갱신 함수는,

입력된 값에 대해 상기 통합 암호 모듈을 반복 적용하여 상기 입력된 값을 갱신하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 방법.

청구항 15

제11항에 있어서,

상기 해쉬값 추출 과정은,

해쉬함수의 길이에 대응하는 상태 갱신 함수를 수행하는 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 방법.

청구항 16

제 9항에 있어서,

상기 블록암호를 생성하는 과정은,

128비트 평문 및 128비트 키를 입력 받아 적어도 하나의 통합 암호 모듈의 반복을 통해 128비트 암호문을 출력하는 함수인 것을 특징으로 하는 기밀성과 무결성을 제공하는 통합 암호화 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 통합 암호화 기술에 관한 것으로서, 특히 유비쿼터스 컴퓨팅 환경에서의 RFID(Radio Frequency Identification)/USN(Ubiquitous Sensor Network) 등과 같이 자원이 제한된 구현 환경에서 기밀성을 제공하는 블록암호(BC)와 무결성을 보장하는 해쉬함수(H)를 동시에 사용할 수 있는 통합 암호 모듈(ICM)을 설계하는데 적

합한 기밀성과 무결성을 제공하는 통합 암호 모듈 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 암호학적 해쉬함수(Cryptographic Hash Function)는 임의의 길이의 스트링을 입력 받아 고정된 길이의 스트링을 출력하는 압축함수(Compression Function)로 해쉬함수를 사용하는 암호시스템의 안전성뿐만 아니라 효율성을 향상시키는데 사용 목적이 있다.

[0003] 암호학적 해쉬함수는 인터넷 뱅킹(Internet Banking), 전자서명(Digital Signature), 메시지 인증 코드(Message Authentication Code), 키 교환 알고리즘(Key Exchange Algorithm), 키 생성 알고리즘(Key Generation Algorithm), 의사 난수 생성기(Pseudo Random Number Generator) 뿐 아니라 다양한 암호시스템에서 사용되며 이들의 안전성은 해쉬함수의 안전성에 기반을 둔다는 점에 있어서 안전한 해쉬함수를 설계하는 것은 매우 중요하다.

[0004] 현재 미국 국립 기술 표준원(NIST, National Institute of Standards and Technology)에서는 2010년부터 가장 널리 사용되고 있는 MD5, SHA-1 해쉬함수 대신 출력 크기를 224, 256, 384, 512 비트로 갖는 SHA-224/256/384/512를 사용할 것을 권장하고 있으며, 미국 국립 기술 표준원은 신규 해쉬 알고리즘 SHA-3 개발을 목표로 2007년부터 2012년까지 6 개년 “SHA-3 개발 프로젝트 (Cryptographic Hash Project)” 계획을 수립하고 현재 진행 중에 있다. NIST의 6 개년 프로젝트를 진행하는 이유에서 볼 수 있듯이 안전하고 효율적인 새로운 해쉬함수의 개발은 매우 필요한 상황이다.

[0005] 한편, 대칭키 알고리즘(Symmetric Key Algorithm) 중 가장 널리 이용되는 블록암호(Block Cipher)는 송신자와 수신자간에 공유된 비밀키 정보를 이용하여 데이터를 암호화함으로써 기밀성을 보장하는 알고리즘이다. 뿐만 아니라, 해쉬함수와 마찬가지로 다양한 환경에 적용 가능하다.

[0006] 대표적인 블록암호로는 미연방 표준 암호인 AES(Advanced Encryption Standard)가 있다. AES는 미국의 연방 표준 알고리즘으로서 20년이 넘게 사용되어 온 DES(Data Encryption Standard)를 대신할 차세대 표준 알고리즘이다. DES는 1972년에 미국 상무성 산하 NIST의 전신인 NBS(National Bureau of Standards)에서 컴퓨터 데이터를 보호할 목적으로 표준 알고리즘을 공모하여 IBM사가 개발한 암호 알고리즘이다.

[0007] DES는 연방 표준으로 제정된 후에 5년마다 안정성을 인정받으면서 표준으로 존속되어 왔으나, 1997년 이후 안정성에 대한 논란이 대두되자 NIST가 DES를 대체할 차세대 표준 암호 알고리즘 제정을 위한 프로젝트로 추진한 것이 AES이다. 2001년 미 연방 표준 암호 알고리즘으로 제정되어, 전 세계적으로 널리 이용되고 있다.

[0008] 이처럼 안전한 암호시스템을 구성하기 위해서는 기밀성 및 무결성을 보장할 수 있는 블록암호와 해쉬함수가 반드시 필요하다. 하지만, 종래에 제안된 암호 시스템들의 경우는 블록암호와 해쉬함수가 독립적인 알고리즘으로 구성되었으며, 유비쿼터스 컴퓨팅 환경의 RFID/USN 등과 같은 자원이 제약된 구현 환경에서는 두 개의 프리미티브(Primitive)를 동시에 구현하기가 어렵다.

[0009] 예를 들어, 해쉬함수 SHA와 블록암호 AES는 비록 미 연방 표준 암호 알고리즘이지만, 그 설계 기법이 상이하여 두 개의 표준 알고리즘을 구성하기 위해서는 독립적으로 각각의 알고리즘이 구현되어야 한다는 문제점이 있었다.

발명의 내용

해결하려는 과제

[0010] 상기한 바와 같이 동작하는 종래 기술의 문제점을 해결하기 위한 본 발명의 실시예는 유비쿼터스 컴퓨팅 환경에서의 RFID/USN 등과 같이 자원이 제한된 구현 환경에서 기밀성을 제공하는 블록암호(BC)와 무결성을 보장하는 해쉬함수(H)를 동시에 사용할 수 있는 통합 암호 모듈(ICM: Integrated Cryptographic Module)을 설계할 수 있는 기밀성과 무결성을 제공하는 통합 암호화 장치 및 그 방법을 제공할 수 있다.

과제의 해결 수단

[0011] 본 발명의 일 실시예에 따른 기밀성과 무결성을 제공하는 통합 암호화 장치는, 기밀성 및 무결성 기능을 포함하

는 통합 암호 모듈과, 상기 통합 암호 모듈을 토대로 메시지 변조 여부를 파악하는 해쉬함수와, 상기 통합 암호 모듈을 토대로 데이터 암호 알고리즘을 구성하는 블록암호를 포함할 수 있다.

[0012] 그리고 상기 통합 암호 모듈은, 입력된 비트에 대해 S-박스, 순환이동, XOR 을 포함하는 연산으로 값을 출력할 수 있다.

[0013] 그리고 상기 해쉬함수는, 입력된 임의 길이의 비트열을 32비트 워드열로 변환하는 메시지 사전 처리부와, 상기 32비트 워드열로 변환된 메시지를 압축하는 메시지 압축부와, 상기 메시지 압축부로부터 출력된 값으로 어느 한 해쉬 길이의 해쉬값을 출력하는 해쉬값 추출부를 포함할 수 있다.

[0014] 그리고 상기 메시지 사전 처리부는, 입력된 메시지에 대한 비트열이 32비트의 배수가 되도록 마지막 비트에 하나의 1과 적어도 하나의 0을 추가할 수 있다.

[0015] 그리고 상기 메시지 압축부는, 상기 32비트 워드열로 변환된 메시지를 상태 갱신 함수를 이용하여 순차적으로 압축할 수 있다.

[0016] 그리고 상기 상태 갱신 함수는, 입력된 값에 대해 상기 통합 암호 모듈을 반복 적용하여 상기 입력된 값을 갱신할 수 있다.

[0017] 그리고 상기 해쉬값 추출부는, 해쉬함수의 길이에 대응하는 상태 갱신 함수를 수행할 수 있다.

[0018] 그리고 상기 블록암호는, 128비트 평문 및 128비트 키를 입력 받아 적어도 하나의 통합 암호 모듈의 반복을 통해 128비트 암호문을 출력하는 함수인 것을 특징으로 할 수 있다.

[0019] 본 발명의 일 실시예에 따른 기밀성과 무결성을 제공하는 통합 암호화 방법은, 기밀성 및 무결성 기능을 포함하는 통합 암호 모듈을 토대로 메시지 변조 여부를 파악하는 해쉬함수를 생성하는 과정과, 상기 통합 암호 모듈을 토대로 데이터 암호 알고리즘을 구성하는 블록암호를 생성하는 과정을 포함할 수 있다.

[0020] 그리고 상기 통합 암호 모듈은, 입력된 비트에 대해 S-박스, 순환이동, XOR 을 포함하는 연산으로 값을 출력할 수 있다.

[0021] 그리고 상기 해쉬함수를 생성하는 과정은, 입력된 임의 길이의 비트열을 32비트 워드열로 변환하는 메시지 사전 처리 과정과, 상기 32비트 워드열로 변환된 메시지를 압축하는 메시지 압축 과정과, 상기 메시지 압축부로부터 출력된 값으로 어느 한 해쉬 길이의 해쉬값을 출력하는 해쉬값 추출 과정을 포함할 수 있다.

[0022] 그리고 상기 메시지 사전 처리 과정은, 입력된 메시지에 대한 비트열이 32비트의 배수가 되도록 마지막 비트에 하나의 1과 적어도 하나의 0을 추가할 수 있다.

[0023] 그리고 상기 메시지 압축 과정은, 상기 32비트 워드열로 변환된 메시지를 상태 갱신 함수를 이용하여 순차적으로 압축할 수 있다.

[0024] 그리고 상기 상태 갱신 함수는, 입력된 값에 대해 상기 통합 암호 모듈을 반복 적용하여 상기 입력된 값을 갱신할 수 있다.

[0025] 그리고 상기 해쉬값 추출 과정은, 해쉬함수의 길이에 대응하는 상태 갱신 함수를 수행할 수 있다.

[0026] 그리고 상기 블록암호를 생성하는 과정은, 128비트 평문 및 128비트 키를 입력 받아 적어도 하나의 통합 암호 모듈의 반복을 통해 128비트 암호문을 출력하는 함수인 것을 특징으로 할 수 있다.

발명의 효과

[0027] 상기와 같은 본 발명의 실시예에 따른 기밀성과 무결성을 제공하는 통합 암호화 장치 및 그 방법에 따르면 다음과 같은 효과가 하나 혹은 그 이상이 있다.

[0028] 본 발명의 실시예에 따른 기밀성과 무결성을 제공하는 통합 암호화 장치 및 그 방법에 의하면, 유비쿼터스 컴퓨팅 환경에서의 RFID/USN 등과 같이 자원이 제한된 구현 환경에서 블록암호와 해쉬함수를 통합하여 구현함으로써 기밀성과 무결성을 동시에 제공할 수 있으며, 통합 암호 모듈을 필요에 따라 블록암호나 해쉬함수를 선택적으로 사용할 수 있는 유연성을 제공할 수 있는 효과가 있다.

도면의 간단한 설명

[0029] 도 1은 본 발명의 실시예에 따른 통합 암호 모듈 ICM의 기본 구조도,

도 2는 본 발명의 실시예에 따른 무결성 기능을 제공하는 해쉬함수 H (Hash Function)의 구조를 도시한 블록도,

도 3은 본 발명의 실시예에 따른 해쉬함수의 메시지 압축부 MCP(Message Compressing Process)를 도시한 도면,

도 4는 본 발명의 실시예에 따라 메시지 압축부 및 해쉬값 출력부에서 이용되는 상태 갱신 함수 f(State Update Function)를 도시한 도면,

도 5는 본 발명의 실시예에 따른 해쉬함수의 해쉬값 출력부 HOP(Hash Value Output Process)를 도시한 도면,

도 6은 본 발명의 실시예에 따라 기밀성 기능을 제공하는 블록암호 BC (Block Cipher)를 도시한 도면.

발명을 실시하기 위한 구체적인 내용

[0030] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0031] 본 발명의 실시예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명의 실시예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0032] 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0033] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들 또는 단계들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0034] 본 발명의 실시예는, 유비쿼터스 컴퓨팅 환경에서의 RFID/USN 등과 같이 자원이 제한된 구현 환경에서 기밀성을 제공하는 블록암호(BC)와 무결성을 보장하는 해쉬함수(H)를 동시에 사용할 수 있는 통합 암호 모듈(ICM)을 설계하는 것으로서, 설계된 통합 암호모듈(ICM)은 112비트 이상의 보안강도를 만족해야 하며, 하드웨어 및 소프트웨어에 대한 효율성이 탁월해야 한다.

[0035] 이에 통합 암호화 장치에서는 통합 암호 모듈을 필요에 따라 블록암호나 해쉬함수로 선택적으로 사용할 수 있으며, 두 개의 프리미티브 블록암호와 해쉬함수를 동작시킬 수 있기 때문에, 하드웨어 및 소프트웨어 환경에서 구현될 경우, 독립적인 두 개의 알고리즘을 구현해야 하는 기존의 암호시스템보다 효율적으로 암호시스템의 구성을 가능하게 할 수 있다.

[0036] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명하기로 한다.

[0037] 도 1은 본 발명의 실시예에 따른 통합 암호 모듈 ICM의 기본 구조도이다.

[0038] 도 1을 참조하면, 통합 암호 모듈 ICM(100)은 $X = X_1 \| X_2 \| \cdots \| X_8$, Y, Ctr_0, Ctr_1, Sel_0, Sel_1을 입력 받아 아래의 (표 1)과 같은 연산을 수행할 수 있다. 단, 여기서 X는 256비트, $X_i (1 \le i \le 8)$, Y, Ctr_0, Ctr_1은 32비트 워드, Sel_0, Sel_1은 1비트이며, $\|$는 연접연산이다.

표 1

[0039]

$$ICM(X, Y, Ctr_0, Ctr_1, Sel_0, Sel_1)$$

$$X_8 = X_8 \oplus MUX(Y, Ctr_0, Sel_0)\ X_3 = X_3 \oplus MUX(X_8, Ctr_0, Sel_1)$$

$$X_7 = X_7 \oplus MUX(X_4, Ctr_1, Sel_1);\ X_1 = X_1 \oplus G(X_3);\ X_5 = X_5 \oplus G(X_7);$$

$$X_3 = X_3 \oplus X_1^{\lll 11};\ X_7 = X_7 \oplus X_5^{\lll 17};$$

$$T = X_8;\ X_8 = X_7;\ X_7 = X_6;\ X_6 = X_5;$$

$$X_5 = X_4;\ X_4 = X_3;\ X_3 = X_2;\ X_1 = T;$$

[0040] (표 1)에서 T는 32비트 워드 임시 변수이며, $x^{\lll s}$는 x를 s비트만큼 왼쪽으로 순환 이동하는 연산, $\oplus$는 32비트 워드간의 비트별 XOR 연산이다.

[0041] $MUX(x, y, z)$는 z 가 0 이면 x 를 출력하고, z 가 1 이면 y 를 출력하는 함수이다. 그리고 함수 G는 32 비트 워드를 입력 받아 32 비트 워드를 출력하는 함수로 암호학적으로 혼돈(Confusion) 및 확산(Diffusion) 성질이 우수한 함수를 사용할 수 있다. 암호학적으로 혼돈 성질을 주기 위한 대표적인 대치함수인 S-박스와 확산 성질을 주기 위한 치환 함수를 결합하여 내부함수 G를 구성할 수 있다. (표 2)는 32 비트 워드 입력을 8개의 4 비트 블록으로 나누어 각각의 4 비트 블록에 대하여 4×4 S-박스 연산을 수행하는 실시예이다.

표 2

[0042]

$S-박스(x_0, x_1, x_2, x_3) = (x'_0, x'_1, x'_2, x'_3)$

입력	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
출력	8	4	2	d	1	f	7	a	5	9	b	e	6	c	0	3

[0043] (표 3)은 32비트 워드 입력을 8개의 4비트 블록으로 나누어 각각의 4비트 블록을 가지고 확산 효과를 주기 위한 치환 함수의 실시예이다.

표 3

[0044]

$$DL(w_0,w_1,w_2,w_3,w_4,w_5,w_6,w_7)=(w'_0,w'_1,w'_2,w'_3,w'_4,w'_5,w'_6,w'_7)$$

$$w'_0=w_1\oplus w_2\oplus w_3\oplus w_4\oplus w_7 \qquad w'_1=w_0\oplus w_2\oplus w_3\oplus w_4\oplus w_5$$

$$w'_2=w_0\oplus w_1\oplus w_3\oplus w_5\oplus w_6 \qquad w'_3=w_0\oplus w_1\oplus w_2\oplus w_6\oplus w_7$$

$$w'_4=w_1\oplus w_2\oplus w_3\oplus w_4\oplus w_5 \qquad w'_5=w_0\oplus w_2\oplus w_4\oplus w_5\oplus w_6\oplus w_7$$

$$w'_6=w_0\oplus w_1\oplus w_3\oplus w_4\oplus w_6\oplus w_7 \qquad w'_7=w_0\oplus w_1\oplus w_2\oplus w_4\oplus w_5\oplus w_7$$

[0045] 한편, (표 1)에서 왼쪽 순환이동 연산에 이용되는 순환 이동양은 각각 서로 다른 고정된 상수이며, (표 1)에서 주어진 특정 값으로 한정하지 않으며, 암호학적으로 확산(Diffusion) 성질이 우수한 값을 선택하여 사용할 수 있다.

[0046] 도 2는 본 발명의 실시예에 따른 무결성 기능을 제공하는 해쉬함수의 구조를 도시한 블록도이다.

[0047] 도 2를 참조하면, 무결성을 제공하는 해쉬함수 H(200)는 메시지 사전 처리부(210), 메시지 압축부(220) 및 해쉬 값 출력부(230) 등을 포함할 수 있다.

[0048] 무결성을 제공하는 해쉬함수(200)는 32 비트 워드 단위의 연산을 사용한다. 따라서, 첫번째 과정에서 메시지 사전 처리부(210)에서는 임의 길이의 비트열을 32 비트 워드열로 변환한다. 두 번째 과정에서 메시지 압축부(220)는 32 비트 워드 단위로 변환된 메시지를 압축한다. 그리고 마지막 과정에서는 해쉬값 추출부(230)에서 사용자에게 필요한 해쉬 길이만큼 해쉬 값으로 출력한다.

[0049] 구체적으로 메시지 사전 처리부(210)(MP: Message Preprocessing)에서는 임의 길이의 비트열을 32 비트 워드열로 변환한다. 32 비트 비트열을 4 바이트의 문자열로 보고 첫 바이트가 워드의 최상위 바이트가 된다.

[0050] 예를 들면, 비트열 10101101 01101011 11001001 10101110 은 32 비트 워드로 $W=ad6bc9ae$ 가 된다. 이는 위의 4 바이트 문자열을 빅엔디안(big-endian) 컴퓨터에서 unsigned long의 형태로 타입 캐스팅(type casting)한 것과 같다.

[0051] 임의의 길이의 비트열을 32 비트 워드열로 변환하고자 할 때는 이 비트열을 바이트 열로 보고 첫 4 바이트를 첫 워드로, 두 번째 4 바이트를 두 번째 워드로 변환하는 과정을 반복한다. 예를 들면, 비트열 10101101 01101011 11001001 10101110 00111111 01011001 01000110은 32 비트 워드열로 표현하면 $ad6bc9ae\ 3f594600$ 가 된다.

[0052] 만약 입력 메시지가 32 비트의 배수가 아닌 경우, 입력 메시지가 32 비트의 배수가 되도록 $10\cdots0$을 채운다. 예를 들어 입력 메시지가 다음과 같은 비트열로 주어진 경우, 10100010 00111101 11100101 01101011 11001001 10001010 10011101

[0053] 이 비트열의 길이는 56이므로 1 다음에 7 개의 0을 덧붙여 64 비트로 만들 수 있다. 따라서 64 비트의 32 비트 워드열은 다음과 같이 주어진다.

[0054] $a239e56b$ $c98a9d80$

[0055] 메시지 압축부(MCP)(220)는 도 3과 같으며, 메시지 사전 처리부(MP)(210) 를 통해 32 비트 워드 단위로 변환된 메시지 워드를 상태 갱신 함수 f(222)를 이용하여 순차적으로 압축한다. 메시지 사전 처리부(MP)(210)에 의하여 변환된 32 비트 메시지 워드열을 $M=M_1\|M_2\|\cdots\|M_t$ 라고 가정하면, 메시지 압축부(MCP)(220)는 (표 4)와 같이 정의할 수 있다. 단, $M_i(1\le i\le t)$ 는 32 비트 워드이다.

표 4

[0056]

$MCP(M)$

$X_1 = IV_1;\ X_2 = IV_2;\ X_3 = IV_3;\ X_4 = IV_4;$

$X_5 = IV_5;\ X_6 = IV_6;\ X_7 = IV_7;\ X_8 = IV_8;$

for from i=1 to i=t

$f(X, M_i);$

[0057] (표 4)에서 $IV_1, \cdots, IV_8$ 은 각각 32 비트 워드로 고정된 초기 상수이며, 특정 값으로 한정하지 않는다.

[0058] (표 4)에서 상태 갱신 함수 f(222)는 도 4와 같으며, 통합 암호 모듈 ICM (100)을 이용하여 구성할 수 있다. 256 비트인 $X = X_1 \| X_2 \| \cdots \| X_8$ (단, $X_i (1 \le i \le 8)$ 32 비트 워드)를 입력 받아 통합 암호 모듈 ICM(100)을 이용하여 입력값을 갱신하는 함수이다. 상태 갱신 함수 f(222)는 (표 5)와 같이 정의할 수 있다.

표 5

[0059]

$f(X, M_i)$

$ICM(X, M_i, Ctr_{0,1}, Ctr_{1,1}, 0, 0);$

for from i=2 to i=R_H

$ICM(X, M_i, Ctr_{0,i}, Ctr_{1,i}, 1, 0);$

[0060] 상태 갱신 함수 f(222)는 X와 M_i을 입력 받아 통합 암호 모듈 ICM(100)을 R_H번 반복하여 적용함으로써 X 값을 갱신할 수 있다. 단, $Ctr_{0,i}$, $Ctr_{1,i} (1 \le i \le R_H)$ 은 서로 다른 고정된 상수이며, 특정 값으로 한정하지 않는다. R_H는 무결성을 제공하는 해쉬함수 H (200)에 대한 안전성을 보장할 수 있는 범위에서 선택적으로 이용할 수 있다.

[0061] 해쉬값 출력부 HOP(230)는 도 5와 같으며, 메시지 압축부 MCP(220)를 마친 후, 출력하고자 하는 해쉬값의 길이만큼 해쉬값을 출력하는 함수이다. 출력하고자 하는 해쉬함수의 길이만큼 추가적으로 상태 갱신 함수 f(222)를 수행하면서, 32 비트 워드 $h_i (1 \le i \le 8)$를 출력한다. 해쉬값 출력부 HOP(220)는 (표 6)과 같이 정의할 수 있다.

표 6

[0062]

```
HOP(X)
    Out h1←X1;
    if i > 1
        for from i=2 to i=HLength
            f(X,0);
            Out hi←X1;
```

[0063] 해쉬값의 길이가 32 비트인 경우, 해쉬값으로 h_1이 비트열로 변환되어 출력되며, 해쉬값의 길이 64 비트인 경우 $h_1 \| h_2$가 비트열로 변환되어 출력된다. 이와 같은 방법으로 해쉬값을 출력하며, 만약 해쉬값의 길이가 224 비트인 경우, $h_1 \| h_2 \| h_3 \| h_4 \| h_5 \| h_6 \| h_7$가 비트열로 변환되어 출력된다. 예를 들어, 해쉬값의 길이가 224 비트인 경우, 각각의 출력변수 h_i가 $h_i = h_{i1} h_{i2} h_{i3} h_{i4}$ (h_{ij}는 1바이트)를 만족하면, 해쉬값은 다음과 같이 비트열로 변환된다.

[0064] $h_{11} h_{12} h_{13} h_{14} h_{21} h_{22} h_{23} h_{24} h_{31} h_{32} h_{33} h_{34} h_{41} h_{42} h_{43} h_{44} h_{51} h_{52} h_{53} h_{54} h_{61} h_{62} h_{63} h_{64} h_{71} h_{72} h_{73} h_{74}$

[0065] 이제 도 2에 주어진 입력 메시지에 대해 기밀성을 제공하는 블록암호 BC (300)를 단계별로 자세히 기술한다. 기밀성을 제공하는 블록암호 BC (300)는 도 6과 같으며, 128비트 평문 $P = P_1 \| P_2 \| P_3 \| P_4$와 128비트 키 $K = K_1 \| K_2 \| K_3 \| K_4$를 입력 받아 비트 암호문 $C = C_1 \| C_2 \| C_3 \| C_4$를 출력하는 함수이다. 기밀성을 제공하는 블록암호 BC (300)는 ICM 통합 암호 모듈 (100)을 이용하여 (표 7)과 같이 정의할 수 있다.

표 7

[0066]

```
BC(P, C, K)
    X1←P1;  X3←P2;  X5←P3;  X7←P4;
    X2←K1;  X4←K2;  X6←K3;  X8←K4;
    for from i=1 to i=RB
        ICM(X, 0, Ctr0,i, Ctr1,i, 0, 1);
        ICM(X, 0, Ctr0,i, Ctr1,i, 0, 0);
    C1←X3;  C2←X5;  C3←X7;  C4←X1;
```

[0067] (표 7)에서 $Ctr_i (1 \le i \le R_H)$ $Ctr_{0,i}$, $Ctr_{1,i} (1 \le i \le R_H)$은 서로 다른 고정된 상수이며, 특정 값으로 한정하지 않는다. R_B는 기밀성을 제공하는 블록암호 BC(300)에 대한 안전성을 보장할 수 있는 범위에서 선택적으로 이용할 수 있다.

[0068] 이상 설명한 바와 같이, 본 발명의 실시예에 따른 기밀성과 무결성을 제공하는 통합 암호화 장치 및 그 방법은 유비쿼터스 컴퓨팅 환경에서의 RFID/USN 등과 같이 자원이 제한된 구현 환경에서 기밀성을 제공하는 블록암호(BC)와 무결성을 보장하는 해쉬함수(H)를 동시에 사용할 수 있는 통합 암호 모듈(ICM)을 설계한다.

[0069] 이와 같이 통합된 암호 모듈을 이용하면 하드웨어 및 소프트웨어 환경에서 구현될 때 독립적인 두 개의 알고리즘을 구현해야 하는 기존의 암호시스템보다 효율적으로 암호시스템을 구성할 수 있다. 뿐만 아니라, 유비쿼터스 컴퓨팅 환경에서의 RFID/USN 등과 같이 자원이 제한된 구현 환경에서도 매우 간단한 연산을 통하여 효율적으로 구현될 수 있으며, 암호학적으로도 안전하게 구현할 수 있다.

[0070] 한편 본 발명의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시예에 국한되지 않으며, 후술되는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

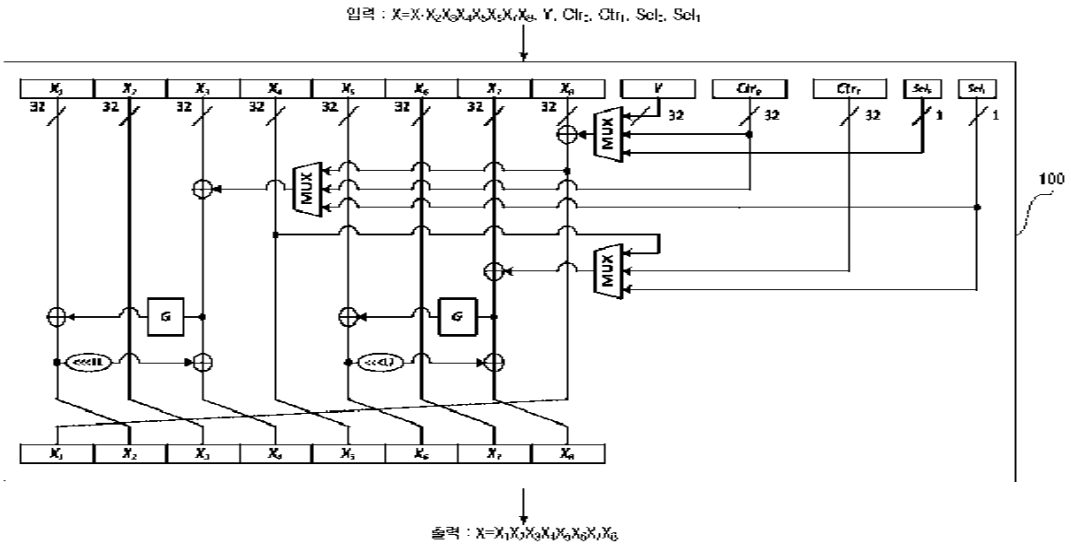
[0071] 100: 통합 암호화 장치 200: 해쉬함수

210: 메시지 사전 처리부 220: 메시지 압축부

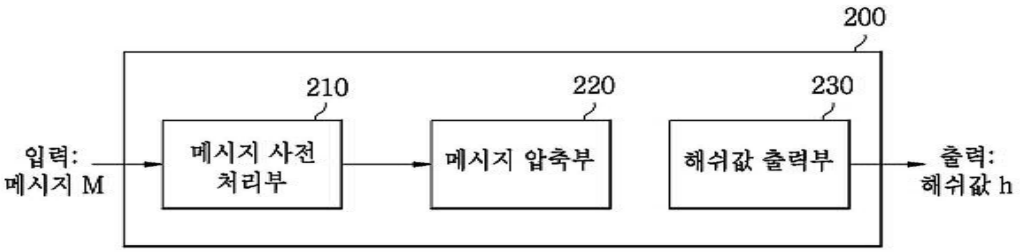
230: 해쉬값 출력부 300: 블록암호

도면

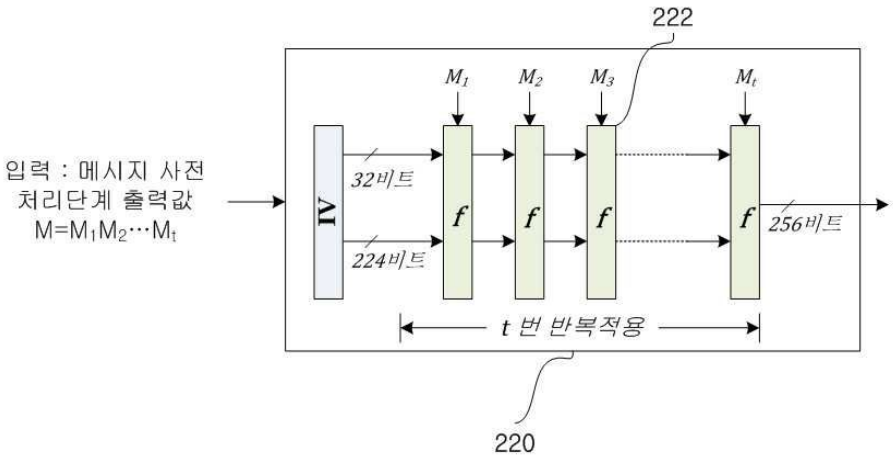
도면1



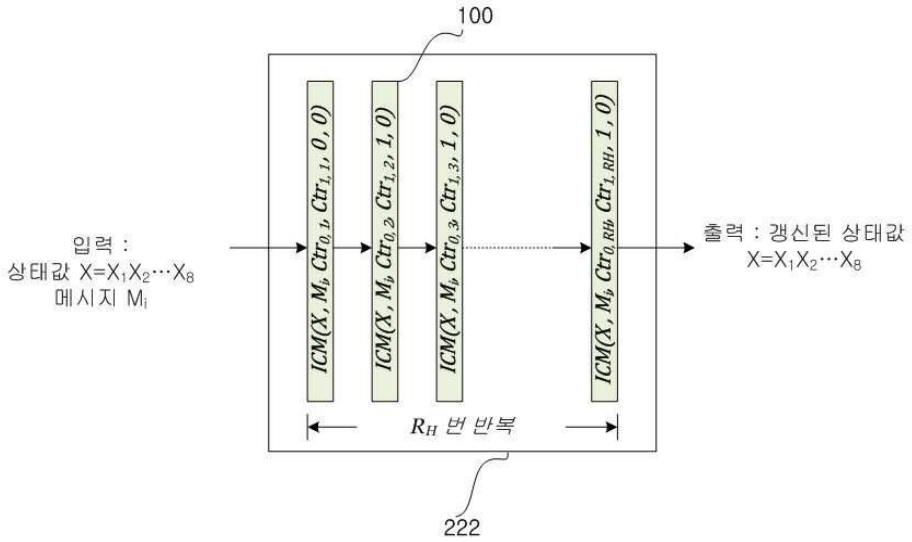
도면2



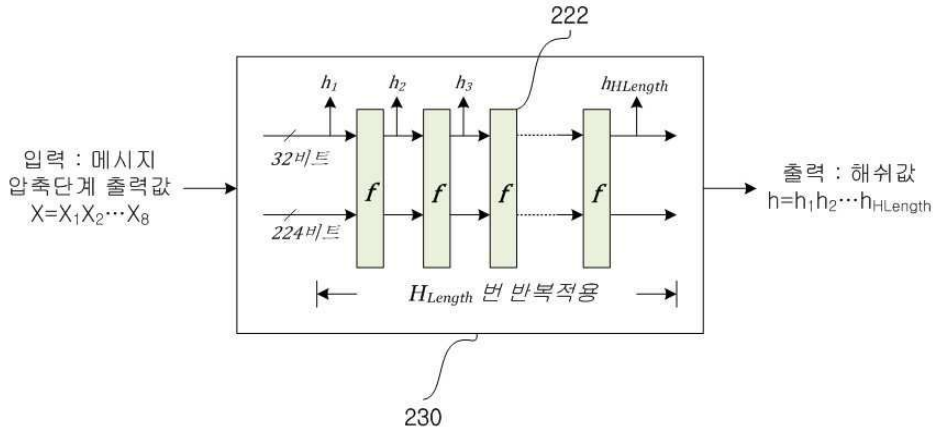
도면3


222
입력 : 메시지 사전
처리단계 출력값
M=M1M2…Mt
IV
32비트
224비트
f
256비트
t 번 반복적용
220

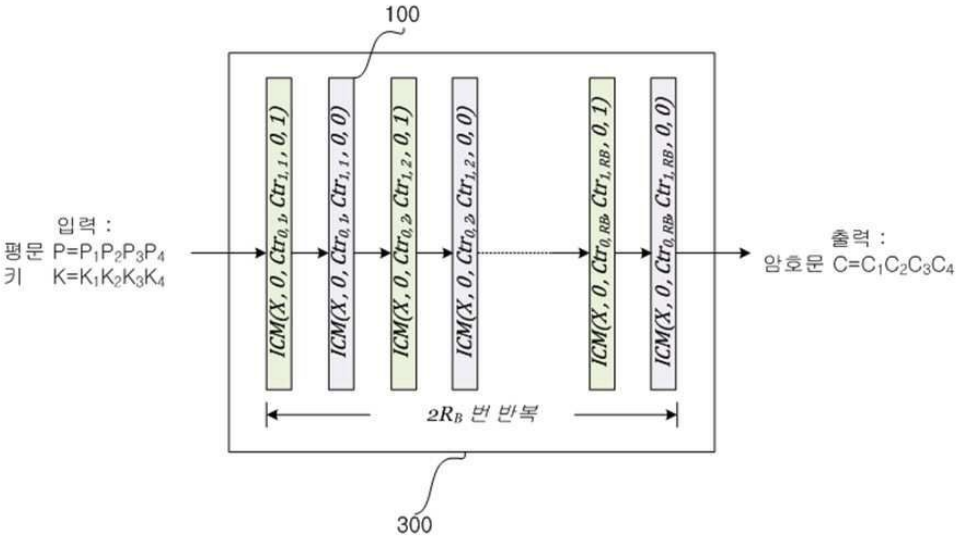
도면4


100
입력 :
상태값 X=X1X2…X8
메시지 Mi
출력 : 갱신된 상태값
X=X1X2…X8
RH 번 반복
222

도면5


222
입력 : 메시지
압축단계 출력값
X=X1X2…X8
32비트
224비트
f
출력 : 해쉬값
h=h1h2…hHLength
HLength 번 반복적용
230

도면6


100
입력 :
평문 P=P1P2P3P4
키 K=K1K2K3K4
ICM(X, 0, Ctr0,1, Ctr1,1, 0, 1)
ICM(X, 0, Ctr0,1, Ctr1,1, 0, 0)
ICM(X, 0, Ctr0,2, Ctr1,2, 0, 1)
ICM(X, 0, Ctr0,2, Ctr1,2, 0, 0)
ICM(X, 0, Ctr0,RB, Ctr1,RB, 0, 1)
ICM(X, 0, Ctr0,RB, Ctr1,RB, 0, 0)
2RB 번 반복
출력 :
암호문 C=C1C2C3C4
300