



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0028782
(43) 공개일자 2020년03월17일

(51) 국제특허분류(Int. Cl.)

H04L 9/06 (2006.01)

(52) CPC특허분류

H04L 9/0618 (2013.01)

H04L 9/0643 (2013.01)

(21) 출원번호 10-2018-0107373

(22) 출원일자 2018년09월07일

심사청구일자 없음

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

김황남

서울특별시 서초구 서운로 104, 205동 503호

오승환

성남시 분당구 양현로 138, 809동 1602호

박성준

서울특별시 강남구 삼성로4길 17, 502동 1203호

(74) 대리인

심경식, 홍성욱

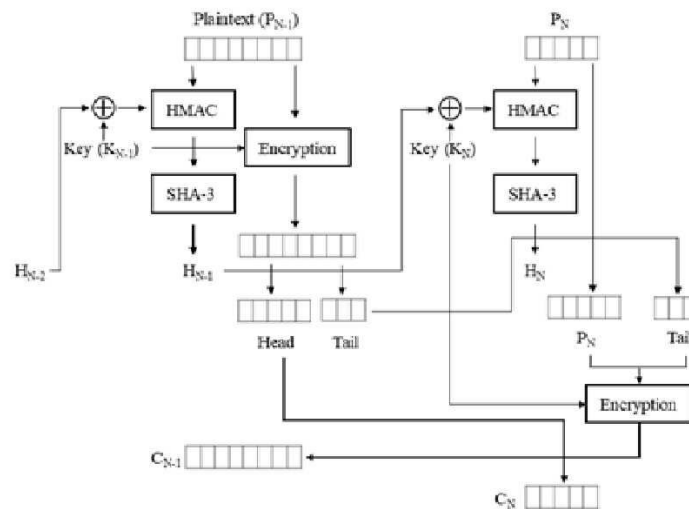
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 방법 및 장치

(57) 요약

본 발명은 리소스 제한과 계산량 한계를 가지는 IoT 디바이스, 무인 이동체, 차량 네트워크 환경에서 안전성과 실시간성을 제공하는 것이 가능하도록 하는 실시간 데이터 전송을 위한 패턴 암호 블록 모드를 사용하는 암호화 방법 및 장치에 관한 것이다.

대표도 - 도2



(52) CPC특허분류

H04L 2209/122 (2013.01)

H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 NRF-2016M1B3A1A01937599

부처명 과학기술정보통신부

연구관리전문기관 한국연구재단

연구사업명 거대과학연구개발사업

연구과제명 다중 무인 이동체 기반 사이버-물리 융합공격 대응 기술 및 자율복원 통신/보안기술 개발

기 여 율 1/1

주관기관 한국항공우주연구원

연구기간 2016.09.21 ~ 2019.03.31

명세서

청구범위

청구항 1

리소스 제한과 계산량 한계를 가지는 IoT 디바이스, 무인 이동체, 차량 네트워크 환경에서 안전성과 실시간성을 제공하는 것이 가능하도록 하는 실시간 데이터 전송을 위한 패턴 암호 블록 모드를 사용하는 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 방법.

발명의 설명

기술 분야

[0001] 본 발명은 실시간 데이터 전송을 위한 패턴 암호 블록 모드를 사용하는 암호화 방법 및 장치에 관한 것이다.

배경 기술

[0002] 암호화 기법은 그 자체로서는 큰 의미를 가지지는 못하지만 서로 간의 통신하는 상황에서 주고받는 메시지가 개인 정보를 담고 있는 중요한 데이터라면 데이터가 가지는 정보가 노출되지 않도록 하는 것이 중요하기 때문에 암호화 기법 기술이 필요하다. 이러한 암호화 기법에는 대칭키 암호화 기법과 비대칭키 암호화 기법이 있다. 일반적으로 대칭키 암호화 기법은 구조적인 복잡도에 기반으로 하며 키 길이가 비대칭키 암호화 기법의 키 길이보다 짧기 때문에 빠른 암호화/복호화 수행이 가능하다. 반면에 비대칭키 암호화 기법은 수학적인 복잡도(이산대수 문제)에 기반으로 하며 공개키와 개인키로 나뉘어 암호화와 복호화를 따로 수행한다. 즉, 대칭키 암호화 기법의 경우 하나의 키로 암호화 복호화를 수행하기 때문에 사전에 송수신자가 안전하게 대칭키를 공유해야하는 문제를 가지고 있는 반면 비대칭키 암호화 기법의 경우 공개키와 개인키로 나뉘어 있어서 따로 키를 교환할 필요 없이 송신자는 수신자의 공개키로 중요 메시지를 암호화하여 전송하면 수신자는 자신의 개인키로 암호문을 복호화하여 메시지 정보를 확인할 수 있는 장점을 가지고 있다. 이러한 비/대칭키 암호화 기법의 장단점을 SSL/TLS은 네트워크 통신환경에 잘 활용하였다.

[0003] SSL은 Secure Socket Layer의 약자로 웹 서버와 웹 브라우저 간의 안전한 암호화 통신을 위하여 응용계층과 TCP/IP 계층에서 동작하는 프로토콜로서, Netscape사에서 만들었으며 ISO표준 정식명칭은 TLS(Transport Layer Security)이다. TLS에서는 통신하기 전에 핸드 셰이킹 프로토콜을 통해서 서로 안전하게 대칭키를 공유하기 위한 작업을 수행하는데, 핸드 셰이킹 과정에서 사용가능한 비·대칭키 암호화 기법 및 해쉬 종류 등 필요한 정보들을 공유한 후에 송신자는 수신자에게 사전에 정한 비대칭키 암호화 기법으로 앞으로 통신에서 사용하게 될 대칭키를 수신자의 공개키로 암호화하여 수신자에게 보낸다. 송신자로부터 받은 암호문을 수신자는 자신의 비밀키로 복호화하여 대칭키를 안전하게 획득한다. 이로써 TLS에서는 비대칭 암호화 기법과 대칭키 암호화 기법의 단점을 보완하여 안전한 통신이 가능하다.

[0004] 그러나 TLS 프로토콜 안전성은 암호화 기법의 안전성에 의존할 뿐 사용하는 비·대칭키 암호화 기법의 안전성을 보완해 주진 않는다. 또한 TLS는 실시간성과 안전성을 네트워크 상황에 맞게 적절하게 조절하지 못하는 단점을 가지고 있다.

[0005] IoT와 웨어러블 디바이스 사용으로 안전성과 실시간성이 중요시 되고 있는 오늘날 현대 사회에서는 디바이스에 기존의 TLS와 같은 암호화 모듈을 적용하여 사용하는 경우 오버헤드와 딜레이가 발생하게 된다. 즉, 실시간성을 제공하는 것이 가능하게 하려할 경우 안전성이 위협을 받게 되는 반면, 안전성을 제공하는 것이 가능하게 하려할 경우 실시간성이 떨어지게 된다. 따라서 본 발명에선 계산량 한계와 리소스 제한을 가지는 디바이스 네트워크 환경에서도 안전성과 실시간성이 가능한 암호화 기법에 관한 내용을 담고 있다.

[0006] 네트워크 통신 환경에 안전성을 제공하기 위한 암호화 기법 기술에는 스트림 암호, 대칭키 암호화 기법, 비대칭키 암호화 기법이 있다. 비대칭키 암호화 기법은 기본적으로 키 길이가 길기 때문에 안전성은 제공하지만 실시간성을 제공하지는 못한다. 반면 스트림 암호는 간단한 XOR연산을 통해서 암호문을 생성하기 때문에 50% 확률로 평문을 예측하는 것이 가능해 실시간성은 제공하지만 안전성은 제공하지 못한다. 대칭키 암호화 기법의 경우 비

대칭키 암호화 기법보다 키 길이가 짧아 빠르며 스트림 암호보다 안전하기 때문에 일반적으로 다른 암호화 기법보다 안전성과 실시간성을 보장한다. 이러한 대칭키 암호화 기법에는 ARIA, SEED, AES등이 있는데 3가지의 키 길이를 가지고 있으며 키 길이가 길수록 높은 안전성을 제공하지만 암호화/복호화로 인한 딜레이가 발생하여 실시간성이 떨어지게 된다. 게다가, 기존의 대칭키 암호화 기법들은 양자 컴퓨터의 등장으로 더 이상 키 길이가 짧은 것은 안전성을 보장할 수 없게 되면서 키 길이가 가장 긴 것을 사용해야지만 안전성을 보장할 수 있게 되었다.

[0007] 이러한 문제를 다루기 위한 기존의 해결 방법으로는 안전성을 위해 키 길이가 긴 대칭키 암호화 기법을 사용하면서 동시에 실시간성을 제공하기 위해 사용자가 임의로 암호화 기법을 적용할 영역과 적용하지 않을 영역을 나누는 방법을 사용하였다. 그러나 기존의 이러한 방법은 암호화 기법을 적용을 하지 않은 영역의 경우 정보가 그대로 노출될 뿐 만 아니라 안전성과 실시간성을 요하는 네트워크 환경에서 근본적인 해결책이 되지 못한다. 오늘날 IoT, 무인 이동체, 차량이 널리 사용되면서 IoT, 무인 이동체, 차량과 같은 사양을 가지는 네트워크 환경에서 안전성과 동시에 실시간성을 제공할 수 있는 기술을 요하는 요구가 증가하고 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 리소스 제한과 계산량 한계를 가지는 IoT 디바이스, 무인 이동체, 차량 네트워크 환경에서 안전성과 실시간성을 제공하는 것이 가능하도록 하는 실시간 데이터 전송을 위한 패턴 암호 블록 모드를 사용하는 암호화 방법 및 장치를 제공하는데 그 목적이 있다.

과제의 해결 수단

[0009] 본 발명은 네트워크 환경에 맞게 대칭키 암호화 기법에서 요구하는 블록 단위로 나누어주는 운영 모드에 기술할 것이다. 일반적으로 네트워크 환경에서 주고받는 메시지 사이즈는 가변적이다. 따라서 대칭키 암호화 기법을 네트워크 환경에 적용하기 위해선 대칭키 암호화 기법에서 요구하는 메시지 단위로 나누어주어야 한다. 가변적인 메시지 단위를 일정 메시지 단위로 나누어 대칭키 암호화 기법이 적용 가능하도록 도와주는 것을 운영 모드라고 부른다.

[0010] 본 내용에서 제안하는 인증된 운영 모드 (Patterned Cipher Block (PCB))란 독립적인 구조로 서로 다른 길이의 대칭 키들을 임의로 순서를 정하여 암호화함으로써 패턴 형식을 가지는 기법임과 동시에 공격자가 송신자로부터 전송된 암호문을 교체하거나 위조하는 경우를 수신자가 검증가능하게 해주는 기술이다.

[0011] 일반적으로 대칭키 암호화 기법에서 키 길이가 짧을수록 실시간성은 높지만 안전성은 떨어진다. 반면에 키 길이가 길수록 안전성은 높지만 실시간성은 떨어진다. 그러나 본 내용에서 제안하는 운영 모드 기술은 서로 다른 길이의 대칭 키들을 동시에 사용하여 서로 다른 길이의 키 비율을 조절함으로써 안전성과 실시간성을 가능하게 한다. 사용자가 기존에 하나의 키를 사용하는 경우보다 서로 다른 길이의 키들을 동시에 사용할 경우가 더 안전하다. 즉, 공격자가 임의의 암호문을 해독하기 위해 공격을 시도해야하는 횟수가 증가할 뿐만 아니라 알아내야하는 키들이 늘어남으로써 높은 수준의 안전성을 제공하는 것이 가능하다. 이전보다 높은 안전성을 제공하는 것이 가능함을 다음 [도 1]와 같이 수학적 수식으로 나타 낼 수 있다.

[0012] 본 내용에서 운영 모드 기술과 함께 제안하는 기술은 무결성 검증 기술로서, 구조도는 [도 2]을 통해서 확인할 수 있다. 암호화하기 위해 사용되는 키들과 이전에 생성된 무결성 검증 값을 함께 XOR 연산한다. XOR 연산한 결과 값을 암호학 해쉬 알고리즘의 키의 입력 값으로 사용하여 알고리즘의 결과 값을 얻는다. 이렇게 생성된 결과 값을 한 번 더 암호학 해쉬 알고리즘의 입력 값으로 받음으로써 해당 평문에 대한 무결성 검증 결과 값을 생성할 수 있다.

발명의 효과

[0013] 이와 같이 서로 다른 암호학 해쉬 알고리즘을 두 번 사용함으로써 발생할지 모르는 암호학 해쉬 함수의 충돌을 방지할 수 있을 뿐만 아니라 암호학 해쉬 비가역성 특성으로 인해 공격자로부터 위조하는 것이 불가능하도록 한다.

[0014] 또한 본 내용에서 제안하는 운영 모드 기술은 독립된 구조적인 특성을 가지기 때문에 대칭키 암호화 기법을 통해서 생성되는 암호문마다 [도 3]과 같이 Counter 값을 제공하는 것이 가능하다. 즉, 네트워크 환경에서 TCP뿐

만 아니라 패킷 손실이 빈번하게 일어날 수 있는 UDP에서도 오류확산 없이 제대로 된 평문들을 얻을 수 있으며 중간에 패킷 손실이 일어나더라도 Counter 값을 통해 손실된 패킷을 재전송하는 것이 가능하다.

[0015] 본 발명에 의하면, 대칭키 암호화 기법을 네트워크 환경에 맞게 암호화할 수 있는 운영 모드를 제공할 뿐만 아니라 무결성 검증을 함께 제공함으로써 인증된 운영 모드 기술이라 할 수 있다.

[0016] 추가로 대칭키 암호화 기법에서 암호화하기 위해 사용되는 서로 다른 길이의 키들을 다음과 같은 방법으로 생성할 수 있다. 첫 번째 방법은 하나의 PW로 3가지 종류의 키들을 생성하는 것이다. 즉, PW를 hash 함수의 입력 값으로 하여 나오는 결과 값을 비트에 맞게 잘라 사용하는 방법이다. hash 함수를 사용하는 이유는 공격자가 하나의 해쉬 결과 값을 알아내더라도 hash 함수 성질인 역상저항성으로 나머지 해쉬 결과 값들을 알 수 없기 때문이다. 두 번째 방법은 서로 다른 3종류의 hash 함수를 사용하여 하나의 PW를 입력하였을 때 나오는 결과 값들을 비트에 맞게 잘라 사용하는 것이다. 3종류의 hash 함수를 사용하는 이유는 hash 함수는 기본적으로 충돌 저항성 성질을 만족한다고 하나 발생할지 모르는 충돌에 대해 대비하기 위해서이다. 세 번째 방법은 사용자가 임의로 서로 다른 3종류의 키를 각각 생성하는 것으로 가장 안전한 방법이라고 할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일 실시예에 따른 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 방법 및 장치를 사용한 경우 높은 안전성을 제공하는 것을 수치화한 수학적식이다.

도 2는 본 발명의 일 실시예에 따른 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 장치의 개략적인 구조도이다.

도 3은 본 발명의 일 실시예에 따른 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 방법 및 장치에 의해 생성되는 암호문마다 카운터값을 제공하는 것을 설명하기 위한 도면이다.

도 4는 본 발명의 일 실시예에 따른 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 방법 및 장치를 통해 CBC와 같이 동일한 평문에 대해 암호화를 수행한 암호문이다.

도 5는 본 발명의 일 실시예에 따른 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 방법 및 장치에 의해 패턴 형식을 가지는 독립적인 구조로 기존의 공격이 불가능함을 증명하는 도면이다.

도 6은 본 발명의 일 실시예에 따른 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 방법 및 장치에 의해 안전성과 실시간성을 함께 제공하는 것이 가능할 뿐만 아니라 패턴 형식에 사용되는 서로 다른 길이의 키를 생성하는 도면이다.

도 7은 본 발명의 일 실시예에 따른 실시간 데이터 전송을 위한 패턴 암호 블록 모드에 기초한 암호화 방법 및 장치에 의해 블록단위 암호화 중에서 가장 빠른 ECB보다 암호화 복호화를 수행하는 속도가 더 빠르다는 것을 확인하는 실험데이터이다.

발명을 실시하기 위한 구체적인 내용

[0018] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면을 참조하여 상세하게 설명하도록 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0019] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재 항목들의 조합 또는 복수의 관련된 기재 항목들 중의 어느 항목을 포함한다.

[0020] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급될 때에는 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급될 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0021] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가

아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0022] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0023] 명세서 및 청구범위 전체에서, 어떤 부분이 어떤 구성 요소를 포함한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있다는 것을 의미한다.

[0025] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0026] 블록 단위로 암호화하는 운영 모드에는 ECB, CBC, PCBC가 있다.

[0027] ECB는 독립적인 구조로 암호화/복호화를 수행하기 때문에 병렬처리 연산이 가능하며 오류확산이 없고 암호화 스티어링 기법이 적용이 가능하다. 즉, 별도의 패딩 연산을 필요로 하지 않아 일정 블록 단위로 암호화/복호화를 수행하는 다른 운영 모드들보다 빠르다. 하지만 인증된 블록 암호 모드가 아니며 독립적인 구조로 암호화 복호화를 수행하기 때문에 deterministic하여 공격자가 암호문 재사용이 가능하다는 치명적인 단점을 가지고 있다.

[0028] CBC와 PCBC는 기본적으로 IV를 필요로 하며 chain형태로 이전 암호문이 다음 암호문 생성에 영향을 주는 구조이기 때문에 전송 중에 비트에러가 발생할 경우 오류확산이 일어나 제대로 된 평문을 얻기 힘들다. 게다가 CBC와 PCBC는 추가 패딩 연산을 요구하기 때문에 ECB보다 암호화 복호화 속도가 느리다. 그러나 구조상 블록 패턴은 유지 되지 않지만 암호문 생성 시 병렬처리가 불가능하다.

[0029] 제안하는 암호화 기법 PCB는 ECB와 같이 독립적인 구조로 인해 오류확산이 일어나지 않으며 패딩과 같은 추가 연산을 필요로 하지 않아 빠르기 때문에 실시간성에 적합하다는 장점을 가진다. 또한 서로 다른 길이의 키에 따라 암호화를 수행하기 때문에 키들의 순서로 인한 패턴을 가진다. 패턴 형식을 가지는 구조적인 특성 [도 4]을 통해 CBC와 같이 동일한 평문에 대해 암호화를 수행하였을 때 서로 다른 암호문이 생성된다. 뿐만 아니라 네트워크 환경에서 공격자가 암호문의 위조 및 교체하는 것을 막기 위해 수신자가 무결성 검증이 가능하도록 하는 기술도 함께 제안함으로써 인증된 운영 모드라 할 수 있다. 또한 본 내용에서 제안하는 PCB는 TCP와 달리 UDP 프로토콜을 사용할 경우 발생하는 패킷 손실에 대해서 오류확산이 없음으로 TCP, UDP 모두 안전하게 사용 가능하다. 따라서 제안하는 암호화 기법은 패턴 형식을 가지는 독립적인 구조로 기존의 공격이 불가능함을 증명[도 5]함으로써, 높은 안전성과 실시간성을 함께 제공하는 것이 가능할 뿐만 아니라 패턴 형식에 사용되는 서로 다른 길이의 키를 [도 6]와 같은 방법으로 생성하는 것이 가능하다.

[0030] 본 발명에서 제안하는 운영 모드 PCB가 [도 7]을 통해 블록단위 암호화 중에서 가장 빠른 ECB보다 암호화 복호화를 수행하는 속도가 더 빠르다는 것을 확인할 수 있다. 기본적으로 PCB와 ECB는 독립적인 구조를 가진다. 그러나 PCB는 ECB와 달리 서로 다른 길이의 키를 동시에 사용함으로써 생기는 패턴 특성 때문에 높은 안전성을 제공하는 것이 가능하다. 즉, PCB는 기존의 대칭키 암호화 기법이 가지는 키 길이에 대한 안전성 문제를 보완하여 높은 수준의 안전성을 제공할 뿐만 아니라 동시에 암호화 복호화를 수행하는 속도가 블록단위 암호화 중에서 가장 빠르므로 실시간성을 제공하는 것이 가능하다.

[0031] PCB 운영모드는 독립적인 구조를 가짐으로써 패딩과 같은 추가적인 연산을 수행할 필요가 없기 때문에 실시간성이 가능하다. 또한, PCB는 서로 다른 길이의 키를 동시에 사용함으로써 생기는 패턴 특성을 통해서 기존의 대칭키 암호화 기법의 키 길이에 대한 안전성 문제를 보완할 수 있기 때문에 높은 수준의 안전성을 제공한다.

[0032] 발명 PCB는 리소스 제한과 계산량 한계를 가지는 IoT등과 같은 디바이스 네트워크 환경에 안전성과 실시간성을 제공하는 것이 가능하다. 뿐만 아니라 PCB는 이동성으로 인해 패킷 손실이 일어나기 쉬운 무인 이동체 및 차량 네트워크 환경에서도 오류확산 없이 복호화가 가능하다. 즉, 리소스 제한, 계산량 한계, 이동성으로 인한 패킷 손실이 일어나기 쉬운 특성 등 이러한 제한들을 가진 분야에 PCB 운영모드를 적용함으로써 안전성과 실시간성이 가능하다.

[0033] 참고 문헌들

[0034] [1] M. Y. Rhee, Cryptography and secure communications. McGraw-Hill, Inc. 1993.

[0035] [2] W. Abdallah, S. kyu Lee, H. Kim, and N. Boudriga, "Adaptive qos and security for video transmission over wireless networks: A cognitivebased approach," in International Conference on Algorithms and Architectures for Parallel Processing. Springer, 2014, pp. 138-151.

[0036] [3] M. Dworkin, "Recommendation for block cipher modes of operation. methods and techniques," NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV, Tech. Rep., 2001.

[0038] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 사람이라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

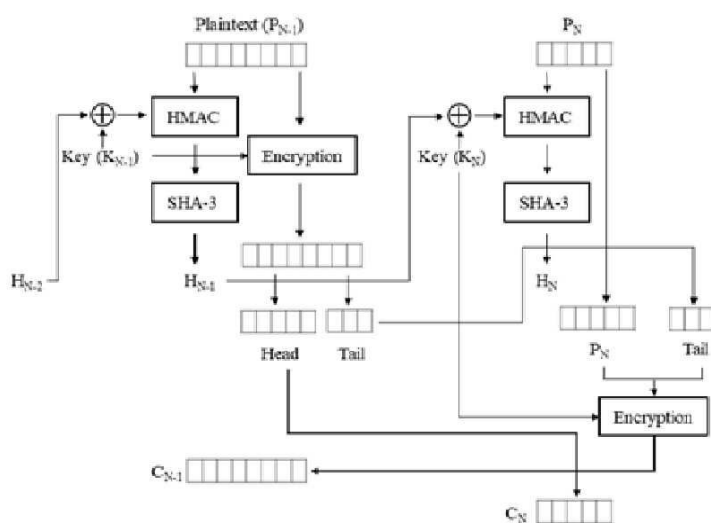
도면

도면1

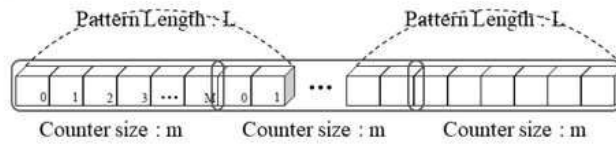
$$\left(\frac{1}{\frac{n_1 C_m}{n C_m}}\right) \times 2^{128} \left(\frac{1}{\frac{n_2 C_m}{n C_m}}\right) \times 2^{192} \left(\frac{1}{\frac{n_3 C_m}{n C_m}}\right) \times 2^{256}$$

(PCB의 암호를 해독하기 위한 수행횟수는 총)

도면2

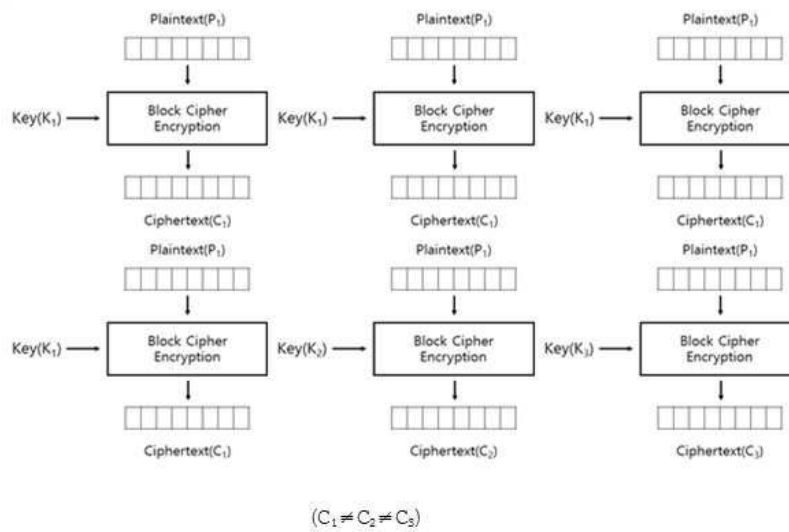


도면3



(단, $\gcd(n,m)=1$ 즉 n 와 m 은 서로소)

도면4



도면5

Adversary $A^{E_k(LR(...,b))}$

$M_0 \leftarrow 0^n \| 1^n;$

$M_1 \leftarrow 0^n \| 0^n;$

$C[1]C[2] \leftarrow E_k(LR(M_0, M_1, b))$

If $C[1] = C[2]$ then return 1 else return 0

$E_k(LR(M_0, M_1, b)) \begin{cases} E_k(M_1) & \text{if } b = 1 \\ E_k(M_0) & \text{if } b = 0 \end{cases}$

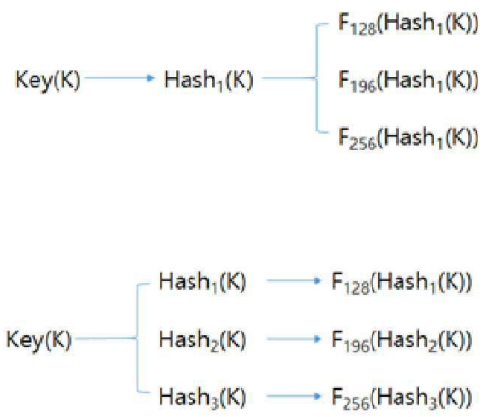
$C[i]$ denotes the i -th block of a string C .

In the right word, $C[1]C[2] = E_k(0^n) \| E_k(0^n)$ and $E_k(0^n)$ is not equal to $E_k(1^n)$

In the left word, $C[1]C[2] = E_k(0^n) \| E_k(1^n)$ and $E_k(0^n)$ is not equal to $E_k(1^n)$

$Adv_{SE}^{IND-CPA}(A) = 0 - 0 = 0$, Because of different key

도면6



도면7

