고려대학교 KOREA UNIVERSITY

김황남 교수 (고려대학교 스마트융합학과)

실시간 데이터 전송을 위한 블록 암호 장치 및 방법
(기술분류-보안-네트워크·클라우드 보안)

기술성 분석

기술 개요

- 서로 다른 길이를 갖는 키들의 순서에 따라 키를 선택하여 각 평문블록을 암호화함으로써 공격자가 송신자로부터 전송된 암호문을 교체하거나 위조하는 경우를 수신자가 검증가능하게 하는 실시간 데이터 전송을 위한 블록 암호 장치 및 방법에 관한 것임
- 본 기술은 리소스 제한과 계산량 한계를 가지는 IoT 디바이스, 무인 이동체, 차량 네트워크 환경에서 안전성과 실시간성을 제공함

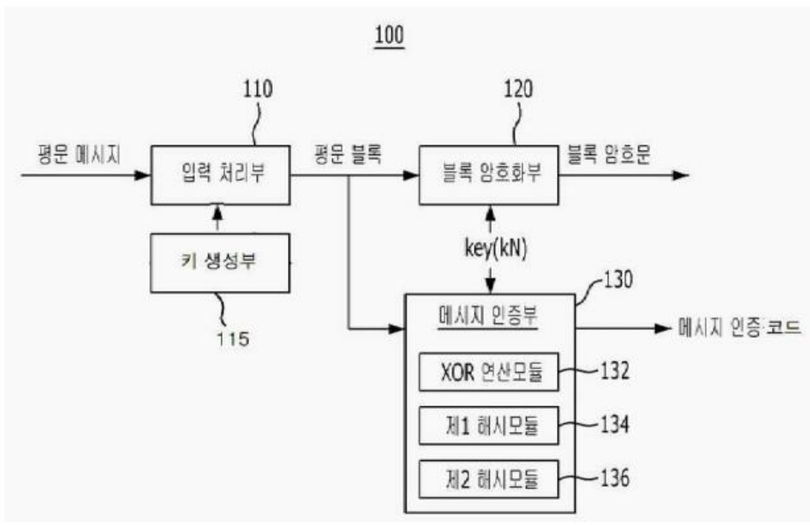
미해결 과제(Unmet needs)

- 기존 암호화 기법의 한계
  - TLS(Transport Layer Security)는 비대칭 암호화 기법과 대칭키 암호화 기법의 단점을 보완하여 안전한 통신이 가능하나, 디바이스에 기존의 TLS와 같은 암호화 모듈을 적용하여 사용하는 경우 키 길이에 따라 실시간성을 제공하는 것이 가능하게 할 경우 안전성이 위협받게 되는 반면, 안전성을 제공하는 것이 가능하게 할 경우 실시간성이 떨어지게 되는 문제가 있음
  - 이러한 문제를 해결하기 위한 기존의 방법은 암호화 기법을 적용하지 않은 영역의 경우 정보가 그대로 노출될 뿐만 아니라 안전성과 실시간성을 요하는 네트워크 환경에서 근본적인 해결책이 되지 못함
  - 따라서, 리소스 제한과 계산량 한계를 가지는 IoT 디바이스, 무인 이동체, 차량 네트워크 환경에서 안전성과 실시간성이 가능한 암호화 기법에 대한 기술 개발이 요구되는 실정임

기술적 해결수단(발명의 구성)

- 1) 본 발명에 따른 실시간 데이터 전송을 위한 블록 암호 장치의 구성
  - 본 발명의 블록 암호 장치(100)는 입력 처리부(110), 키 생성부(115), 블록 암호화부(120), 메시지 인증부(130)를 포함함
  - 입력 처리부는 입력받은 평문 메시지를 서로 다른 비트 길이를 갖는 복수의 순서화된 평문 블록으로 나누며, 이때 평문 블록은 암호문 메시지를 복호화하는 것을 목표로 하는 역 프로세스 중에 동일한 순서가 적용될 수 있도록 순차적인 방식으로 배열됨
  - 키 생성부는 블록 암호화부에서 평문 블록을 암호화하기 위해 사용되는 서로 다른 길이의 키들을 생성하고, 해당 키들의 순서를 정하여 네트워크 환경과 데이터 안정성을 고려하여 패턴을 설정함
  - 블록 암호화부는 서로 다른 길이를 갖는 키들의 순서에 따라 키를 선택하여 각 평문 블록을 암호화하여 암호화문 블록을 생성함
  - 메시지 인증부는 서로 다른 암호학 해시 알고리즘을 두 번 사용하여, 공격자로부터 메시지의 위조를 방지하기 위한 메시지 인증 코드를 생성함

본 발명의 실시간 데이터 전송을 위한 블록 암호 장치

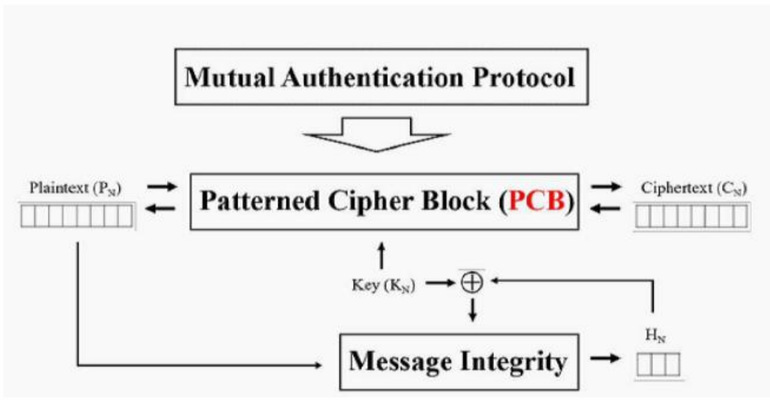


본 기술의 우수성 및 파급 효과

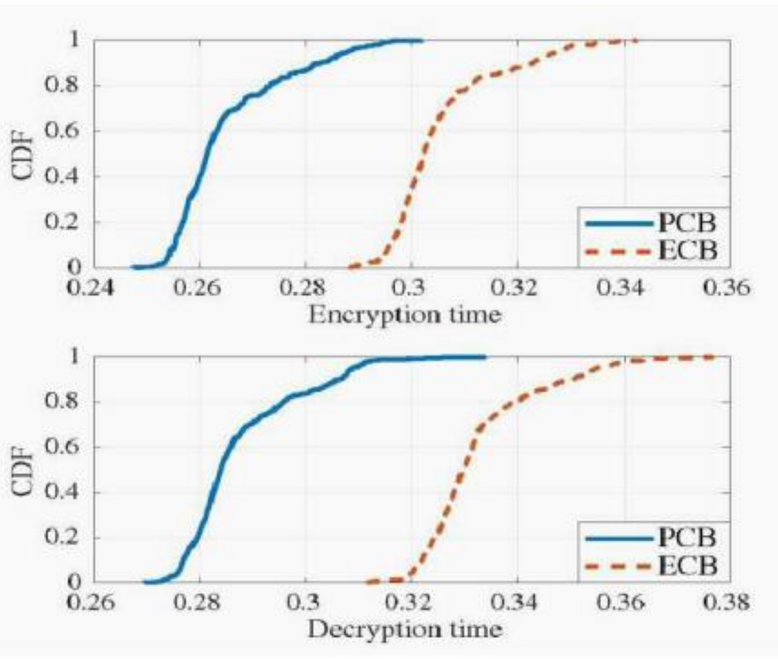
본 기술의 우수성(효과)

- 안전성 및 실시간성 확보
  - 대칭키 암호화 기법에서는 키 길이가 짧을수록 실시간성은 높지만 안전성은 떨어지고, 키 길이가 길수록 안전성은 높지만 실시간성은 떨어짐
  - 그러나, 본 기술의 PCB(Patterned Cipher Block)는 서로 다른 길이의 대칭키들을 동시에 사용하여 서로 다른 길이의 키 비율을 조절함으로써 실시간성을 가지며, 기존에 하나의 키를 사용하는 경우보다 공격자가 임의의 암호문을 해독하기 위해 공격을 시도해야 하는 횟수가 증가할 뿐만 아니라 알아내야 하는 키들이 늘어나 높은 수준의 안전성을 제공함
  - PCB는 패턴이라는 주어진 시퀀스의 순서로 블록당 여러 개의 암호 알고리즘을 번갈아 사용하는 운영 모드로, PCB 운영 모드에서 송신자와 수신자는 동일한 패턴을 가지며, 각 블록에 대해 동일한 알고리즘을 사용하여 암호화 또는 복호화를 수행함
  - 이때, 공격자가 암호문들을 획득하더라도 동일한 키로 암호화된 블록 집합을 알 수 없어 공유 키를 추출하기 어려우므로 보안이 개선되고, 상대적으로 빠른 암호화/복호화 방법을 이용하게 되어 시간 비용을 줄일 수 있음
  - 또한, 블록단위 암호화 중에서 가장 빠른 ECB 운영모드와 PCB 운영모드를 비교한 결과, PCB 운영모드가 ECB보다 암호화 복호화를 수행하는 속도가 더 빠른 것을 확인함

본 발명의 실시간 데이터 전송을 위한 블록 암호



PCB 운영모드와 ECB 운영모드의 성능 비교



적용 제품 및 파급 효과

- 보안 장치
- 본 기술의 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 가능함

지식재산권 현황

발명의 명칭	출원/등록번호	출원/등록일자
실시간 데이터 전송을 위한 블록 암호 장치 및 방법	10-2172181	2020.10.26.
패밀리 특허 현황	**패밀리 국가**	
US11115187	US	

문 의 | 고려대학교 산학협력단 기술사업화센터 권성진 02-3290-5832, giannie77@korea.ac.kr