(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0139875
(43) 공개일자 2024년09월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 2209/24 (2013.01)
(21) 출원번호 10-2023-0034086
(22) 출원일자 2023년03월15일
심사청구일자 2023년03월15일

(71) 출원인
국방과학연구소
대전광역시 유성구 북유성대로488번길 160 (수남동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이상진
서울특별시 성북구 안암로 145
홍득조
서울특별시 성북구 안암로 145
(뒷면에 계속)
(74) 대리인
특허법인 광장리앤고

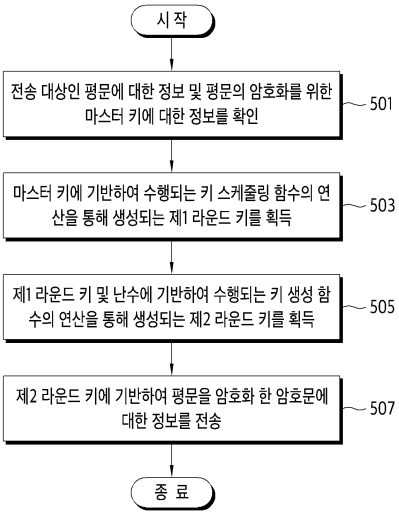
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **정보를 전송하는 전자 장치의 동작 방법 및 이를 지원하는 전자 장치**

(57) 요 약

본 개시에 따르면, 전자 장치가 정보를 전송하는 방법에 있어서, 전송 대상인 평문에 대한 정보 및 상기 평문의 암호화를 위한 마스터 키에 대한 정보를 확인하는 단계; 상기 마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득하는 단계; 상기 제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득하는 단계; 및 상기 제2 라운드 키에 기반하여 상기 평문을 암호화 한 암호문에 대한 정보를 전송하는 단계를 포함할 수 있다.

대 표 도 - 도5



(72) 발명자
김희석
서울특별시 성북구 안암로 145
권동근
서울특별시 성북구 안암로 145

명 세 서

청구범위

청구항 1

전자 장치가 정보를 전송하는 방법에 있어서,

전송 대상인 평문에 대한 정보 및 상기 평문의 암호화를 위한 마스터 키에 대한 정보를 확인하는 단계;

상기 마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득하는 단계;

상기 제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득하는 단계; 및

상기 제2 라운드 키에 기반하여 상기 평문을 암호화 한 암호문에 대한 정보를 전송하는 단계를 포함하는,

정보 전송 방법.

청구항 2

제 1 항에 있어서,

상기 암호문에 대한 정보의 전송 과정에서 상기 키 스케줄링 함수의 연산이 수행되는 횟수는 1회로 제한되도록 설정되는,

정보 전송 방법.

청구항 3

제 1 항에 있어서,

상기 키 생성 함수의 연산은, 상기 제1 라운드 키 및 상기 난수에 기반한 배타적 논리합(XOR) 연산을 포함하는,

정보 전송 방법.

청구항 4

제 3 항에 있어서,

상기 난수의 비트 크기(i+1)가 상기 제1 라운드 키의 비트 크기(j+1) 보다 큰 경우, 상기 난수의 k번째 비트와 상기 제1 라운드 키의 [k mod (j+1)]번째 비트에 대하여 상기 XOR 연산이 수행되도록 설정되는($0 \leq k \leq i$),

정보 전송 방법.

청구항 5

제 3 항에 있어서,

상기 난수의 비트 크기(i+1)가 상기 제1 라운드 키의 비트 크기(j+1) 보다 작은 경우, 상기 제1 라운드 키의 k번째 비트와 상기 난수의 [k mod (i+1)]번째 비트에 대하여 상기 XOR 연산이 수행되도록 설정되는($0 \leq k \leq j$),

정보 전송 방법.

청구항 6

제 1 항에 있어서,

상기 키 생성 함수의 연산은,

사전에 설정된 내부 상태 값 및 상기 난수에 기반하여 새로운 난수를 생성하는 연산, 및

상기 제1 라운드 키 및 상기 새로운 난수에 기반한 배타적 논리합(XOR) 연산을 포함하는,

정보 전송 방법.

청구항 7

제 1 항에 있어서,

상기 정보 전송 방법은,

상기 제2 라운드 키 및 상기 평문에 기반하여 수행되는 암호화 함수의 연산을 통해 상기 암호문을 획득하는 단계를 더 포함하는,

정보 전송 방법.

청구항 8

제 7 항에 있어서,

상기 정보 전송 방법은,

상기 평문의 비트 크기에 대한 정보를 확인하는 단계; 및

상기 평문의 비트 크기가 상기 암호화 함수의 입력 요구 비트 크기 보다 작은 경우, 상기 평문에 대한 패딩(padding)을 적용하는 단계를 더 포함하는,

정보 전송 방법.

청구항 9

정보 전송 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 비일시적 컴퓨터 판독 가능 저장 매체에 있어서,

상기 정보 전송 방법은:

전송 대상인 평문에 대한 정보 및 상기 평문의 암호화를 위한 마스터 키에 대한 정보를 확인하는 단계;

상기 마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득하는 단계;

상기 제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득하는 단계; 및

상기 제2 라운드 키에 기반하여 상기 평문을 암호화 한 암호문에 대한 정보를 전송하는 단계를 포함하는 것을 특징으로 하는,

비일시적 컴퓨터 판독 가능 저장 매체.

청구항 10

정보를 전송하는 전자 장치에 있어서,

프로세서 (processor); 및

하나 이상의 인스트럭션 (instruction)을 저장하는 하나 이상의 메모리 (memory)를 포함하고,

상기 하나 이상의 인스트럭션은, 실행 시에, 상기 프로세서가:

전송 대상인 평문에 대한 정보 및 상기 평문의 암호화를 위한 마스터 키에 대한 정보를 확인하는 단계;

상기 마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득하는 단계;

상기 제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득하는 단계; 및

상기 제2 라운드 키에 기반하여 상기 평문을 암호화 한 암호문에 대한 정보를 전송하는 단계를 수행하도록 상기 프로세서를 제어하는,

전자 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 정보를 전송하는 방법 및 장치에 관한 것으로서, 더욱 상세하게는 장치가 암호화와 관련된 다양한 함수의 연산에 기반하여 암호문에 대한 정보를 전송하는 방법 및 이의 전자 장치에 관한 것이다.

배 경 기 술

[0002] 부채널(side-channel) 공격은, 암호 기능을 탑재한 기기로부터 부채널에서 수집할 수 있는 모든 정보를 그룹화하여, 상관 계수 등에 따른 통계적인 기법을 이용해 암호 키와 같은 비밀 정보를 획득하는 물리적인 공격 중 하나이다. 대표적인 부채널 공격인 차분 전력 분석(Differential Power Analysis) 및 상관 전력 분석(Correlation Power Analysis)은 고정된 암호 키를 사용할 때 수집하는 부채널 정보와 그에 대한 평문 또는 암호문을 이용할 수 있다. 상기 분석 방법들에 따르면, 고정된 암호 키 중 일부를 임의로 추측하여 평문 또는 암호문과 결합해 암호 연산 중간 값을 계산한 후, 각 중간 값에 대한 소비 전력 값을 계산하여, 계산한 소비 전력 값과 실제 장비에서 획득된 소비 전력 값 사이의 유사성을 통계적인 분석 기법을 이용하여 획득하는 방식을 기반으로 부채널 공격을 수행할 수 있다.

[0003] 키 재생성(Fresh Re-keying) 대응 기법은 통계적인 부채널 공격에 대한 프로토콜 수준의 대응 기법이다. 전술한 차분 전력 분석 및 상관 전력 분석은 추측을 통해 중간 값을 예측하여 고정된 키가 연산하는 부채널 정보를 매칭시켜 분석하는데, 이에 대한 대표적인 대응 기법으로 마스킹 대응 기법과 키 재생성 대응 기법이 있다.

[0004] 마스킹 대응 기법은 난수를 암호화 연산 중간 값에 추가하는 방식으로 부채널 분석 공격자가 중간 값 추측을 통한 통계적인 공격 수행을 어렵게 하며, 키 재생성 대응 기법은 세션마다 새로운 암호화 키를 사용하여 라운드 키를 재생성 함으로써 부채널 분석 공격자가 중간 값 추측을 통한 통계적인 공격 수행을 어렵게 할 수 있다. 두 대응 기법은 모두 암호화 연산 중간 값에 난수를 추가함으로써 공격자가 중간 값을 추측하기 어렵게 하여 부채널 공격에 대응한다는 점을 공통으로 할 수 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명의 방법에 따르면, 전자 장치가 암호화와 관련된 다양한 함수의 연산에 기반하여 암호문에 대한 정보를 전송할 수 있다.

[0006] 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0007] 다양한 실시예들은, 정보 전송을 위한 전자 장치의 동작 방법 및 이를 지원하는 전자 장치를 제공할 수 있다.

[0008] 전자 장치가 정보를 전송하는 방법에 있어서, 전송 대상인 평문에 대한 정보 및 상기 평문의 암호화를 위한 마스터 키에 대한 정보를 확인하는 단계; 상기 마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득하는 단계; 상기 제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득하는 단계; 및 상기 제2 라운드 키에 기반하여 상기 평문을 암호화 한 암호문에 대한 정보를 전송하는 단계를 포함할 수 있다.

[0009] 예시적 실시예에서, 상기 암호문에 대한 정보의 전송 과정에서 상기 키 스케줄링 함수의 연산이 수행되는 횟수는 1회로 제한되도록 설정될 수 있다.

[0010] 예시적 실시예에서, 상기 키 생성 함수의 연산은, 상기 제1 라운드 키 및 상기 난수에 기반한 배타적 논리합

(XOR) 연산을 포함할 수 있다.

[0011] 예시적 실시예에서, 상기 난수의 비트 크기(i+1)가 상기 제1 라운드 키의 비트 크기(j+1) 보다 큰 경우, 상기 난수의 k번째 비트와 상기 제1 라운드 키의 [k mod (j+1)]번째 비트에 대하여 상기 XOR 연산이 수행되도록 설정될 수 있다.

[0012] 예시적 실시예에서, 상기 난수의 비트 크기(i+1)가 상기 제1 라운드 키의 비트 크기(j+1) 보다 작은 경우, 상기 제1 라운드 키의 k번째 비트와 상기 난수의 [k mod (i+1)]번째 비트에 대하여 상기 XOR 연산이 수행되도록 설정될 수 있다.

[0013] 예시적 실시예에서, 상기 키 생성 함수의 연산은, 사전에 설정된 내부 상태 값 및 상기 난수에 기반하여 새로운 난수를 생성하는 연산, 및 상기 제1 라운드 키 및 상기 새로운 난수에 기반한 배타적 논리합(XOR) 연산을 포함할 수 있다.

[0014] 예시적 실시예에서, 상기 정보 전송 방법은, 상기 제2 라운드 키 및 상기 평문에 기반하여 수행되는 암호화 함수의 연산을 통해 상기 암호문을 획득하는 단계를 더 포함할 수 있다.

[0015] 예시적 실시예에서, 상기 정보 전송 방법은, 상기 평문의 비트 크기에 대한 정보를 확인하는 단계; 및 상기 평문의 비트 크기가 상기 암호화 함수의 입력 요구 비트 크기 보다 작은 경우, 상기 평문에 대한 패딩(padding)을 적용하는 단계를 더 포함할 수 있다.

[0016] 다양한 실시예들에 따른 정보 전송 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 비일시적 컴퓨터 판독 가능 저장 매체에 있어서, 상기 정보 전송 방법은: 전송 대상인 평문에 대한 정보 및 상기 평문의 암호화를 위한 마스터 키에 대한 정보를 확인하는 단계; 상기 마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득하는 단계; 상기 제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득하는 단계; 및 상기 제2 라운드 키에 기반하여 상기 평문을 암호화 한 암호문에 대한 정보를 전송하는 단계를 포함할 수 있다.

[0017] 다양한 실시예들에 따른 정보를 전송하는 전자 장치에 있어서, 프로세서 (processor); 및 하나 이상의 인스트럭션 (instruction) 을 저장하는 하나 이상의 메모리 (memory) 를 포함하고, 상기 하나 이상의 인스트럭션은, 실행 시에, 상기 프로세서가: 전송 대상인 평문에 대한 정보 및 상기 평문의 암호화를 위한 마스터 키에 대한 정보를 확인하는 단계; 상기 마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득하는 단계; 상기 제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득하는 단계; 및 상기 제2 라운드 키에 기반하여 상기 평문을 암호화 한 암호문에 대한 정보를 전송하는 단계를 수행하도록 상기 프로세서를 제어할 수 있다.

[0018] 상술한 본 개시의 다양한 실시예들은 본 개시의 바람직한 실시예들 중 일부에 불과하며, 본 개시의 다양한 실시예들의 기술적 특징들이 반영된 여러 가지 실시예들이 당해 기술분야의 통상적인 지식을 가진 자에 의해 이하 상술할 상세한 설명을 기반으로 도출되고 이해될 수 있다.

발명의 효과

[0019] 본 발명은 전자 장치가 암호화와 관련된 다양한 함수의 연산에 기반하여 암호문에 대한 정보를 전송하는 방법을 제시하여, 효율적으로 평문에 대한 암호화를 수행할 수 있는 측면에서 기술적인 효과를 갖는다.

[0020] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0021] 도 1은 다양한 실시예들에 따른 정보 전송을 위한 전자 장치의 동작 방법이 구현될 수 있는 정보 전송 시스템을 설명하기 위한 도면이다.

도 2는 다양한 실시예들에 따른 통신 노드의 구성을 도시한 도면이다.

도 3은 종래의 키 재생성 대응 기법이 적용된 암호 알고리즘이 수행되는 모습을 도시한 도면이다.

도 4는 본 발명에서 제안하는 정보 전송 방법을 수행하는 전자 장치의 구조도를 도시한 도면이다.

도 5는 다양한 실시예들에 따른 정보 전송을 위한 전자 장치의 동작 방법을 도시한 도면이다.

도 6은 본 발명에서 제안하는 키 재사용 기법이 적용된 암호 알고리즘이 수행되는 모습을 도시한 도면이다.

도 7은 본 발명에서 제안하는 키 생성 함수에 대한 알고리즘의 일 예시를 도시한 도면이다.

도 8은 본 발명에서 제안하는 키 생성 함수에 대한 알고리즘의 다른 예시를 도시한 도면이다.

도 9는 다양한 실시예들에 따른 본 발명의 정보 전송 방법을 처리하는 알고리즘의 일 예시를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0022] 이하의 실시예들은 다양한 실시예들의 구성요소들과 특징들을 소정 형태로 결합한 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으로 고려될 수 있다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있다. 또한, 일부 구성요소들 및 특징들을 결합하여 다양한 실시예들을 구성할 수도 있다. 다양한 실시예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시예의 일부 구성이나 특징은 다른 실시예에 포함될 수 있고, 또는 다른 실시예의 대응하는 구성 또는 특징과 교체될 수 있다.

[0023] 도면에 대한 설명에서, 다양한 실시예들의 요지를 흐릴 수 있는 절차 또는 단계 등은 기술하지 않았으며, 당해 기술분야에서 통상의 지식을 가진 자의 수준에서 이해할 수 있을 정도의 절차 또는 단계는 또한 기술하지 아니하였다.

[0024] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함(comprising 또는 including)"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다. 또한, "일(a 또는 an)", "하나(one)", "그(the)" 및 유사 관련어는 다양한 실시예들을 기술하는 문맥에 있어서(특히, 이하의 청구항의 문맥에서) 본 명세서에 달리 지시되거나 문맥에 의해 분명하게 반박되지 않는 한, 단수 및 복수 모두를 포함하는 의미로 사용될 수 있다.

[0025] 이하, 다양한 실시예들에 따른 바람직한 실시 형태를 첨부된 도면을 참조하여 상세하게 설명한다. 첨부된 도면과 함께 이하에 개시될 상세한 설명은 다양한 실시예들의 예시적인 실시형태를 설명하고자 하는 것이며, 유일한 실시형태를 나타내고자 하는 것이 아니다.

[0026] 또한, 다양한 실시예들에서 사용되는 특정(特定) 용어들은 다양한 실시예들의 이해를 돕기 위해서 제공된 것이며, 이러한 특정 용어의 사용은 다양한 실시예들의 기술적 사상을 벗어나지 않는 범위에서 다른 형태로 변경될 수 있다.

[0028] 도 1은 다양한 실시예들에 따른 정보 전송을 위한 전자 장치의 동작 방법이 구현될 수 있는 정보 전송 시스템을 설명하기 위한 도면이다.

[0029] 도 1을 참조하면, 다양한 실시예들에 따른 정보 전송 시스템은 다양한 종류의 전자 장치들에 의해 구현될 수 있다. 예를 들어, 정보 전송 시스템은 서버(100)로 대표되는 통신 노드와 단말(200)로 대표되는 통신 노드 사이, 및/또는 단말(200)로 대표되는 통신 노드들 사이 등에서 구현될 수 있다. 여기서 서버(100)로 대표되는 통신 노드와 단말(200)로 대표되는 통신 노드는, 기지국(base station), 셀(cell), 송수신 포인트(Transmission and Reception Point; TRP), 네트워크 노드(Network Node), 사용자 장치(User Device) 등 통신 서비스를 제공하거나 사용할 수 있는 임의의 형태의 통신 노드 중 하나 또는 일부를 의미할 수 있다. 즉, 도 1의 정보 전송 시스템은 각종 통신 노드에 의해 구현될 수 있으며, 이하의 본 개시에서 정보 전송 시스템의 주체로서 기술하는 통신 노드는 통신 서비스를 제공하거나 사용할 수 있는 임의의 형태의 통신 노드를 포함하는 개념일 수 있다. 본 개시에서는 특히, 서버(100)로 대표되는 통신 노드들을 통해 정보 전송 방법이 수행되는 것을 중심으로 정보 전송 시스템이 구현될 수 있다.

[0030] 도 1에 따른 본 발명의 정보 전송 시스템에서, 서버(100) 또는 단말(200)로 대표되는 통신 노드는 본 개시의 다양한 실시예들에 따른 동작을 수행할 수 있다. 한편, 다양한 실시예들에 따른 정보 전송 시스템은, 상기 도 1에 도시된 바에 국한되지 않고, 더 다양한 전자 장치와 서버들에 구현될 수도 있을 것이다.

[0031] 다양한 실시예들에 따른 서버(100)로 대표되는 통신 노드는, 복수 개의 단말(200)로 대표되는 통신 노드와 무선 및 유선 통신을 수행하며, 대단위의 저장 용량을 갖는 스토리지를 포함하는 장치일 수 있다. 이외에도 유사한 기능을 수행하는 다른 전자 장치들이 서버(100)로 대표되는 통신 노드로 이용될 수 있다.

[0032] 다양한 실시예들에 따른 단말(200)로 대표되는 통신 노드는, 서버(100)로 대표되는 통신 노드 또는 단말(200)로 대표되는 다른 통신 노드와 무선 및 유선 통신을 수행하며, 일정한 저장 용량을 갖는 스토리지를 포함하는 장치일 수 있다. 또한 단말(200)로 대표되는 통신 노드는 데스크탑 피시, 태블릿 피시, 모바일 단말 등의 개인 사용자에 의해 이용될 수 있는 장치일 수 있다. 이외에도 유사한 기능을 수행하는 다른 전자 장치들이 단말(200)로 대표되는 통신 노드로 이용될 수 있다.

[0033] 다양한 실시예들에 따른 정보 전송 시스템은 그 동작을 위한 다양한 모듈들을 포함할 수 있다. 정보 전송 시스템에 포함된 모듈들은 정보 전송 시스템이 구현되는(또는, 물리적 장치에 포함되는) 물리적 장치(예: 서버(100) 또는 단말(200)를 포함한 통신 노드)가 지정된 동작을 수행할 수 있도록 구현된 컴퓨터 코드 내지는 하나 이상의 인스트럭션 (instruction) 일 수 있다. 다시 말해, 정보 전송 시스템이 구현되는 물리적 장치는 복수 개의 모듈들을 컴퓨터 코드 형태로 메모리에 저장하고, 메모리에 저장된 복수 개의 모듈들이 실행되는 경우 복수 개의 모듈들은 물리적 장치가 복수 개의 모듈들에 대응하는 지정된 동작들을 수행하도록 할 수 있다.

[0034] 또는 다양한 실시예들에 따른 정보 전송 시스템은 그 동작을 위한 컴퓨터가 읽을 수 있는 비일시적 컴퓨터 판독 가능 저장 매체 (또는 비일시적 기록 매체)에 의해 구현될 수 있다. 정보 전송을 위한 동작 방법은 소프트웨어 모듈 또는 알고리즘으로 구현될 수 있으며, 프로세서 상에서 실행 가능한 컴퓨터가 읽을 수 있는 코드들 또는 프로그램 명령들로서 컴퓨터가 읽을 수 있는 기록 매체 상에 저장될 수 있다. 여기서 컴퓨터가 읽을 수 있는 기록 매체로 마그네틱 저장 매체(예컨대, ROM(read-only memory), RAM(random-Access memory), 플로피 디스크, 하드 디스크 등) 및 광학적 판독 매체(예컨대, 시디롬(CD-ROM), 디브이디(DVD: Digital Versatile Disc)) 등이 있다. 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템들에 분산되어, 분산 방식으로 컴퓨터가 판독 가능한 코드가 저장되고 실행될 수 있다. 매체는 컴퓨터에 의해 판독 가능하며, 메모리에 저장되고, 프로세서에서 실행될 수 있다.

[0035] 도 2는 다양한 실시예들에 따른 통신 노드의 구성을 도시한 도면이다.

[0036] 도 2를 참조하면, 서버(100) 또는 단말(200)로 대표되는 통신 노드는 입/출력부(210), 통신부(220), 스토리지(230) 및 프로세서(240)를 포함할 수 있다.

[0037] 입/출력부(210)는 사용자 입력을 받거나 또는 사용자에게 정보를 출력하는 각종 인터페이스나 연결 포트 등일 수 있다. 입/출력부(210)는 입력 모듈과 출력 모듈을 포함할 수 있는데, 입력 모듈은 사용자로부터 사용자 입력을 수신한다. 사용자 입력은 키 입력, 터치 입력, 음성 입력을 비롯한 다양한 형태로 이루어질 수 있다. 이러한 사용자 입력을 받을 수 있는 입력 모듈의 예로는 전통적인 형태의 키패드나 키보드, 마우스는 물론, 사용자의 터치를 감지하는 터치 센서, 음성 신호를 입력받는 마이크, 영상 인식을 통해 제스처 등을 인식하는 카메라, 사용자 접근을 감지하는 조도 센서나 적외선 센서 중 적어도 하나를 포함하는 근접 센서, 가속도 센서나 자이로 센서 등을 통해 사용자 동작을 인식하는 모션 센서 및 그 외의 다양한 형태의 사용자 입력을 감지하거나 입력받는 다양한 형태의 입력 수단이 있으며, 본 개시의 실시예에 따른 입력 모듈은 위에 나열한 장치 중 적어도 하나를 포함할 수 있다. 여기서, 터치 센서는 디스플레이 패널에 부착되는 터치 패널이나 터치 필름을 통해 터치를 감지하는 압전식 또는 정전식 터치 센서, 광학적인 방식에 의해 터치를 감지하는 광학식 터치 센서 등으로 구현될 수 있다. 이외에도 입력 모듈은 자체적으로 사용자 입력을 감지하는 장치 대신 사용자 입력을 입력 받는 외부의 입력 장치를 연결시키는 입력 인터페이스(USB 포트, PS/2 포트 등)의 형태로 구현될 수도 있다. 또 출력 모듈은 각종 정보를 출력할 수 있다. 출력 모듈은 영상을 출력하는 디스플레이, 소리를 출력하는 스피커, 진동을 발생시키는 햅틱 장치 및 그 외의 다양한 형태의 출력 수단 중 적어도 하나를 포함할 수 있다. 이외에도 출력 모듈은 상술한 개별 출력 수단을 연결시키는 포트 타입의 출력 인터페이스의 형태로 구현될 수도 있다.

[0038] 일 예로, 디스플레이 형태의 출력 모듈은 텍스트, 정지 영상, 동영상을 디스플레이 할 수 있다. 디스플레이는 액정 디스플레이(LCD: Liquid Crystal Display), 발광 다이오드(LED: light emitting diode) 디스플레이, 유기 발광 다이오드(OLED: Organic Light Emitting Diode) 디스플레이, 평판 디스플레이(FPD: Flat Panel Display), 투명 디스플레이(transparent display), 곡면 디스플레이(Curved Display), 플렉시블 디스플레이(flexible display), 3차원 디스플레이(3D display), 홀로그래픽 디스플레이(holographic display), 프로젝터 및 그 외의 영상 출력 기능을 수행할 수 있는 다양한 형태의 장치 중 적어도 하나를 포함할 수 있다. 이러한 디스플레이는

입력 모듈의 터치 센서와 일체로 구성된 터치 디스플레이의 형태일 수도 있다.

[0039] 통신부(220)는 다른 장치와 통신할 수 있다. 따라서, 통신 노드(100 또는 200)는 통신부를 통해 다른 장치와 정보를 송수신할 수 있다. 예를 들어, 통신 노드(100 또는 200)는 통신부를 이용해 상호 간 통신을 수행하거나, 기타 다른 장치와 통신을 수행할 수 있다.

[0040] 여기서, 통신, 즉 데이터의 송수신은 유선 또는 무선으로 이루어질 수 있다. 이를 위해 통신부는 LAN(Local Area Network)를 통해 인터넷 등에 접속하는 유선 통신 모듈, 이동 통신 서버를 거쳐 이동 통신 네트워크에 접속하여 데이터를 송수신하는 이동 통신 모듈, 와이파이(Wi-Fi) 같은 WLAN(Wireless Local Area Network) 계열의 통신 방식이나 블루투스(Bluetooth), 직비(Zigbee)와 같은 WPAN(Wireless Personal Area Network) 계열의 통신 방식을 이용하는 근거리 통신 모듈, GPS(Global Positioning System)과 같은 GNSS(Global Navigation Satellite System)을 이용하는 위성 통신 모듈 또는 이들의 조합으로 구성될 수 있다.

[0041] 스토리지(230)는 각종 정보를 저장할 수 있다. 스토리지(230)는 데이터를 임시적으로 또는 반영구적으로 저장할 수 있다. 예를 들어, 통신 노드(100 또는 200)의 스토리지(230)에는 통신 노드(100 또는 200)를 구동하기 위한 운용 프로그램(OS: Operating System), 웹 사이트를 호스팅하기 위한 데이터나 점자 생성을 위한 프로그램 내지는 어플리케이션(예를 들어, 웹 어플리케이션)에 관한 데이터 등이 저장될 수 있다. 또, 스토리지(230)는 상술한 바와 같이 모듈들을 컴퓨터 코드 형태로 저장할 수 있다.

[0042] 스토리지(230)의 예로는 하드 디스크(HDD: Hard Disk Drive), SSD(Solid State Drive), 플래쉬 메모리(flash memory), 롬(ROM: Read-Only Memory), 램(RAM: Random Access Memory) 등이 있을 수 있다. 이러한 스토리지(230)는 내장 타입 또는 탈부착 가능한 타입으로 제공될 수 있다.

[0043] 프로세서(240)는 통신 노드(100 또는 200)의 전반적인 동작을 제어한다. 이를 위해 프로세서(240)는 각종 정보의 연산 및 처리를 수행하고 통신 노드(100 또는 200)의 구성요소들의 동작을 제어할 수 있다. 예를 들어, 프로세서(240)는 정보 전송을 위한 프로그램 내지 어플리케이션을 실행시킬 수 있을 것이다. 프로세서(240)는 하드웨어, 소프트웨어 또는 이들의 조합에 따라 컴퓨터나 이와 유사한 장치로 구현될 수 있다. 하드웨어적으로 프로세서(240)는 전기적인 신호를 처리하여 제어 기능을 수행하는 전자 회로 형태로 구현될 수 있으며, 소프트웨어적으로는 하드웨어적인 프로세서(240)를 구동시키는 프로그램 형태로 구현될 수 있다. 한편, 이하의 설명에서 특별한 언급이 없는 경우에는 통신 노드(100 또는 200)의 동작은 프로세서(240)의 제어에 의해 수행되는 것으로 해석될 수 있다. 즉, 상술한 정보 전송 시스템에 구현되는 모듈들이 실행되는 경우, 모듈들은 프로세서(240)가 통신 노드(100 또는 200)를 이하의 동작들을 수행하도록 제어하는 것으로 해석될 수 있다.

[0044] 요약하면, 다양한 실시예들은 다양한 수단을 통해 구현될 수 있다. 예를 들어, 다양한 실시예들은 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다.

[0045] 하드웨어에 의한 구현의 경우, 다양한 실시예들에 따른 방법은 하나 또는 그 이상의 ASICs(application specific integrated circuits), DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays), 프로세서, 콘트롤러, 마이크로 콘트롤러, 마이크로 프로세서 등에 의해 구현될 수 있다.

[0046] 펌웨어나 소프트웨어에 의한 구현의 경우, 다양한 실시예들에 따른 방법은 이하에서 설명된 기능 또는 동작들을 수행하는 모듈, 절차 또는 함수 등의 형태로 구현될 수 있다. 예를 들어, 소프트웨어 코드는 메모리에 저장되어 프로세서에 의해 구동될 수 있다. 상기 메모리는 상기 프로세서 내부 또는 외부에 위치할 수 있으며, 이미 공지된 다양한 수단에 의해 상기 프로세서와 데이터를 주고 받을 수 있다.

[0047] 이하에서는, 상기와 같은 기술적 사상에 기반하여 다양한 실시예들에 대해 보다 상세히 설명한다. 이하에서 설명되는 다양한 실시예들에 대해서는 앞서 설명한 내용들이 적용될 수 있다. 예를 들어, 이하에서 설명되는 다양한 실시예들에서 정의되지 않은 동작, 기능, 용어 등은 앞서 설명한 내용들에 기반하여 수행되고 설명될 수 있다.

[0048] 도 3은 종래의 키 재생성 대응 기법이 적용된 암호 알고리즘이 수행되는 모습을 도시한 도면이다.

[0049] 도 3의 키 재생성 기법에서 사용되는 함수는 e, s, g의 3개로, e는 암호화(encryption) 함수에 해당하고, s는 키 스케줄링(scheduling) 함수를, g는 키 생성 함수를 각각 의미할 수 있다.

[0050] 도 3에서 P, C는 각각 평문, 암호문을 나타내며, 암호화 함수 e는 R을 비밀 키로 하는 함수일 수 있다. 도 3의 키 재생성 대응 기법이 적용된 암호화 과정에 따르면, 마스터 키 K와 난수(또는 논스(Nonce)) N을 결합하여 키

재생성 함수 g를 통해 세션 키 K*를 생성한 후(301), 세션 키 K*를 기반으로 키 스케줄링 함수 s를 통해 라운드 키 R을 생성하며(303), 라운드 키 R을 이용해 평문 P를 암호화하여 암호문 C를 생성할 수 있다(305). 이후 P와 다른 평문 P' 에 대한 암호문 C' 을 생성하고자 한다면, 마스터 키 K는 동일하되 난수 N을 새로운 난수 N' 으로 변경해 새로운 세션 키 K*'를 생성하여 암호화 연산을 수행할 수 있다.

[0051] 도 3과 같은 키 재생성 대응 기법은 난수를 마스터 키에 추가함으로써 통계적인 부채널 공격에 대한 안전성을 가지며, 암호 알고리즘 별로 서로 다르게 적용될 필요가 없으므로 키 생성 함수에 대한 모듈화가 가능하여 기존 암호 알고리즘에 대한 적용이 용이할 수 있다. 또한 도 3의 키 재생성 대응 기법은, 암호 알고리즘의 비선형 연산 횟수에 따라 비용이 크게 증가하는 마스킹 대응 기법과는 달리 키 생성 함수만 추가적으로 연산하기에 비교적 연산 비용이 저렴하다는 장점을 가질 수 있다.

[0052] 그러나 키 재생성 대응 기법은 세션마다 발신자와 수신자가 난수를 교환하여 암호 키를 생성해야 하므로 키 스케줄링 연산을 자주, 반복적으로 수행해야 한다는 문제를 가진다. 공격자의 부채널 분석으로부터 안전하기 위해서는 매 암호화 연산 시마다 새로운 난수를 사용하여 암호화 연산 중간 값이 서로 다른 값을 가지도록 하는 것이 요구되는데, 도 3과 같은 기존의 키 재생성 대응 기법은 기본적으로 난수마다 새로운 라운드 키 생성이 필요하기에 암호화 시마다 키 스케줄링 연산이 필요하게 되며, 이는 연산의 과부하를 일으키는 문제를 발생시킬 수 있다.

[0053] 상기와 같은 문제점을 해결하기 위하여 이하의 본 발명에서는, 암호화 연산을 탑재한 장치에 구현된 암호 알고리즘의 부채널 정보가 노출될 수 있는 환경에서, 부채널 분석을 통한 공격을 방지하기 위한 키 재사용(Reuse-keying) 기법에 기반하여 효율적으로 암호화 키를 생성하고, 생성된 암호화 키를 바탕으로 평문을 암호화 한 암호문에 대한 정보를 전송하는 장치 및 방법을 제공한다. 본 발명에서 제공하는 장치와 방법에 따라, 부채널 대응 기법 중 하나인 키 재생성(Re-keying) 기법의 키 생성 과정을 개선한 키 재사용 기법을 활용할 수 있으며, 키 재사용 기법에 기반하여 부하의 부담이 경감된 효율적인 연산으로 부채널 분석 공격자가 암호화 연산 중간 값을 알 수 없도록 관리할 수 있다.

[0054] 도 4는 본 발명에서 제안하는 정보 전송 방법을 수행하는 전자 장치의 구조도를 도시한 도면이다.

[0055] 도 4에서 정보 전송 방법을 수행하는 전자 장치(400)는 통신 디바이스(401), 제어부(403) 및 메모리(405)를 포함할 수 있다. 도 4에 따른 전자 장치(400)에 포함된 각 구성 요소는 도 2에 따른 통신 노드의 구성에 대응하거나 또는 도 4에 따른 전자 장치(400)가 도 2에 따른 통신 노드의 구성을 포함할 수 있으며, 일 예로, 전자 장치(400)에 포함된 통신 디바이스(401)는 도 2의 통신부(220)에 대응하여 외부의 장치와 신호를 송수신할 수 있다.

[0056] 도 4에 따른 전자 장치(400)는 통신 디바이스(401)를 통해 다른 전자 장치와 연결될 수 있으며, 이를 기반으로 다른 전자 장치와 신호를 송수신할 수 있다.

[0057] 제어부(403)는 후술할 도 5 내지 도 9에 따른 다양한 실시예들을 포함하는 정보 전송 방법을 수행하도록 전자 장치(400)를 제어할 수 있다. 일 예로, 제어부(403)는 전자 장치(400)가 도 5의 동작 501 내지 507을 수행하도록 제어할 수 있으며, 전자 장치(400)가 도 5의 동작 501 내지 507을 수행하는데 필요한 다양한 정보를 저장하고 송수신하도록 제어할 수 있다.

[0058] 메모리(405)는 휘발성 메모리 또는 비휘발성 메모리일 수 있으며, 제어부(403)가 정보 전송 방법을 수행하기 위한 프로그램을 실행하는데 필요한 프로그램의 코드가 메모리(405)에 저장될 수 있다.

[0059] 본 발명에서 정보 전송 방법을 수행하는 전자 장치(400)가 도 4의 구성에 한정되는 것은 아니며, 도 4에 도시된 다양한 구성 요소들 외에 다른 범용적인 구성 요소들이 본 발명의 전자 장치(400)에 포함될 수 있다.

[0060] 도 5는 다양한 실시예들에 따른 정보 전송을 위한 전자 장치의 동작 방법을 도시한 도면이다.

[0061] 도 5에서 전자 장치는, 전송 대상인 평문에 대한 정보 및 평문의 암호화를 위한 마스터 키에 대한 정보를 확인하며(501), 마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득 하고(503), 제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득하며(505), 제2 라운드 키에 기반하여 평문을 암호화 한 암호문에 대한 정보를 전송할 수 있다(507).

[0062] 도 5에서 전자 장치가 암호문에 대한 정보를 전송하는 방법을 처리하기 위한 암호 알고리즘이 수행되는 예시는 도 6과 같을 수 있다.

[0063] 도 6은 본 발명에서 제안하는 키 재사용 기법이 적용된 암호 알고리즘이 수행되는 모습을 도시한 도면이다.

[0064] 도 6의 키 재사용 기법에서 사용되는 함수는 e, s, g의 3개로, e는 AES, DES, ARIA와 같은 블록 암호 알고리즘의 암호화(encryption) 함수에 해당하고, s는 키 스케줄링(scheduling) 함수를, g는 키 생성 함수를 각각 의미할 수 있다.

[0065] 도 6의 키 재사용 기법에서는 도 3의 키 재생성 대응 기법과 달리, 키 스케줄링 함수 s를 먼저 실행한 뒤 이후 키 생성 함수 g를 실행할 수 있다. 구체적으로, 도 6의 키 재사용 기법에서는 키 스케줄링 함수 s를 실행하여 마스터 키 K로부터 라운드 키 R을 생성하고(601), 이 때 난수 N의 변경 여부와 무관하게 라운드 키 R를 새롭게 생성하지 않고 변경 없이 그대로 사용한다. 대신 키 재생성 함수 g가 이전과 다르게 난수 N과 라운드 키 R을 입력으로 받아 새로운 라운드 키 R*를 생성할 수 있다(603). 이후, 새로운 라운드 키 R*를 이용해 평문 P를 암호화하여 암호문 C를 생성할 수 있다(605).

[0066] 도 3의 키 재생성 대응 기법에 따르면, 암호화 연산 수행 시마다 난수 N이 변경됨에 따라 새로운 세션 키 K*를 생성해야 하며, 암호화 연산에서 새로운 세션 키 K*에 따른 새로운 라운드 키 R을 생성하기 위해 새로운 세션 키 K*를 입력 값으로 하는 키 스케줄링 함수 s를 새롭게 수행해야 하므로, 키 스케줄링 연산이 반복적으로 요구될 수 있다. 반면, 도 6의 키 재사용 기법에서는 키 스케줄링 함수 s의 입력 값인 마스터 키 K가 변경되지 않음에 따라 키 스케줄링 함수 s의 연산이 통신 과정에서 1회만 수행될 수 있다. 또한, 도 6과 같은 암호 알고리즘을 통해 마스터 키 K가 고정되고 키 스케줄링 함수 s가 1회만 수행되는 점을 고려하여, 한 번의 정상적인 암호문의 통신 과정에서 1회의 키 스케줄링 함수의 연산만이 수행되도록 제한할 수도 있으며, 이를 통해 1회의 키 스케줄링 함수의 연산이 제대로 처리되지 않을 시 마스터 키 K에 대한 연산이 제대로 처리되지 않은 것으로 보아 암호문의 통신 과정에 문제가 있음을 확인할 수도 있다.

[0067] 도 6의 키 재사용 기법에 따르면, 난수마다 암호화 함수 e에 입력되는 라운드 키 R*이 달라지고 이에 따라 암호화 연산마다 서로 다른 암호화 연산 중간 값을 가지게 되어 부채널 공격으로부터의 안전성이 기존처럼 유지될 수 있는 동시에, 암호문을 전송 받는 사용자도 하나의 마스터 키에 대해 1회의 키 스케줄링 연산만을 수행하면 되므로 연산의 부담이 경감될 수 있다. 특히 암호문을 전송 받는 사용자는, 사전에 공유한 마스터 키 K를 기반으로 1회의 키 스케줄링 함수 s 연산을 통해 세션 키(라운드 키) R을 생성하여 저장할 수 있으며, 키 생성 함수 g를 통해 난수마다 라운드 키 R*를 확인하고 복호화 함수를 이용해 전달 받은 암호문 C와 라운드 키 R*를 통해 평문 P를 획득할 수 있다.

[0068] 이 때 키 생성 함수 g는 도 7 내지 도 8과 같은 구체적인 알고리즘에 기반하여 형성될 수 있다.

[0069] 도 7은 본 발명에서 제안하는 키 생성 함수에 대한 알고리즘의 일 예시를 도시한 도면이다.

[0070] 도 7의 키 생성 함수에 대한 알고리즘에서는 난수 N과 라운드 키 R를 입력 받아, 난수 N과 라운드 키 R에 대한 배타적 논리합(XOR) 연산을 수행할 수 있다. 도 7의 키 생성 함수에 대한 알고리즘은 난수 N의 크기와 라운드 키 R의 크기가 서로 다른 경우에도 적용 가능하도록 설정되므로, 도 7의 알고리즘에서는 우선 입력으로 받은 난수 N과 라운드 키 R의 크기를 비교하게 된다.

[0071] 이 때 크기가 i+1인 난수 N 및 크기가 j+1인 라운드 키 R에 대하여, 만약 난수 N의 크기가 라운드 키 R의 크기보다 크거나 같다면, k를 0부터 i까지 증가시키면서 난수 N의 k번째 비트와 라운드 키 R의 [k mod (j+1)] 번째 비트를 XOR 연산을 위한 비트로 대응시킬 수 있다. 이와 같은 대응 관계를 가지는 난수 N의 k번째 비트와 라운드 키 R의 [K mod (j+1)]번째 비트에 대해 XOR 연산을 수행하고, XOR 연산을 수행한 결과를 암호화 키에 해당하는 새로운 라운드 키 R*의 k번째 비트의 값으로 설정할 수 있다(701). 반대로 만약 난수 N의 크기가 라운드 키 R의 크기보다 작다면, k를 0부터 j까지 증가시키면서 난수 N의 [k mod (i+1)]번째 비트와 라운드 키 R의 k번째 비트를 XOR 연산을 위한 비트로 대응시킬 수 있다. 이와 같은 대응 관계를 가지는 난수 N의 [k mod (i+1)]번째 비트와 라운드 키 R의 k번째 비트에 대해 XOR 연산을 수행하고, XOR 연산을 수행한 결과를 암호화 키에 해당하는 새로운 라운드 키 R*의 k번째 비트의 값으로 설정할 수 있다(703).

[0072] 이 때, 위와 같은 도 7의 키 생성 함수에 대한 알고리즘에 더하여, 공격자가 하나의 난수를 획득하더라도 암호화 키에 사용된 난수를 알아낼 수 없도록 한층 더 강화된 보안을 도모하고자 하는 경우, 전자 장치는 도 8과 같이 난수의 설정에 이용 가능한 내부 상태 값을 추가한 알고리즘을 활용할 수도 있다.

[0073] 도 8은 본 발명에서 제안하는 키 생성 함수에 대한 알고리즘의 다른 예시를 도시한 도면이다.

[0074] 도 8의 키 생성 함수에 대한 알고리즘에서는, 도 7에서와 유사하게 난수 N과 라운드 키 R를 입력 받아 난수 N과 라운드 키 R를 기반으로 배타적 논리합(XOR) 연산을 수행할 수 있다. 다만 도 7과는 달리 도 8의 알고리즘은,

우선 내부 상태 값이 정의되어 있거나 사전에 설정되어 있는지 확인하여, 내부 상태 값이 정의되어 있거나 사전에 설정되어 있다면 해당 내부 상태 값과 난수를 이용해 내부 상태 값에 기반한 새로운 난수 S을 설정할 수 있다(801). 만약 내부 상태 값이 정의되지 않았다면 내부 상태 값은 0으로 설정될 수 있다. 도 8의 알고리즘에서는 내부 상태 값이 정의되어 있거나 사전에 설정되어 있는 경우에 생성되는 새로운 난수 S와 라운드 키 R에 대한 배타적 논리합(XOR) 연산을 수행할 수 있게 된다.

[0075] 도 8의 키 생성 함수에 대한 알고리즘 역시 입력 값인 난수 N의 크기와 라운드 키 R의 크기가 서로 다른 경우에도 적용 가능하도록 설정되므로, 도 8의 알고리즘에서는 입력으로 받은 난수 N과 라운드 키 R의 크기를 비교하게 되며, 이후 도 7과 유사한 연산을 수행할 수 있다.

[0076] 도 8의 알고리즘에서, 크기가 i+1인 난수 S 및 크기가 j+1인 라운드 키 R에 대하여, 만약 난수 S의 크기가 라운드 키 R의 크기보다 크거나 같다면, k를 0부터 i까지 증가시키면서 난수 S의 k번째 비트와 라운드 키 R의 [k mod (j+1)] 번째 비트를 XOR 연산을 위한 비트로 대응시킬 수 있다. 이와 같은 대응 관계를 가지는 난수 S의 k번째 비트와 라운드 키 R의 [K mod (j+1)]번째 비트에 대해 XOR 연산을 수행하고, XOR 연산을 수행한 결과를 암호화 키에 해당하는 새로운 라운드 키 R*의 k번째 비트의 값으로 설정할 수 있다(803). 반대로 만약 난수 S의 크기가 라운드 키 R의 크기보다 작다면, k를 0부터 j까지 증가시키면서 난수 S의 [k mod (i+1)]번째 비트와 라운드 키 R의 k번째 비트를 XOR 연산을 위한 비트로 대응시킬 수 있다. 이와 같은 대응 관계를 가지는 난수 S의 [k mod (i+1)]번째 비트와 라운드 키 R의 k번째 비트에 대해 XOR 연산을 수행하고, XOR 연산을 수행한 결과를 암호화 키에 해당하는 새로운 라운드 키 R*의 k번째 비트의 값으로 설정할 수 있다(805).

[0077] 물리적 공격 중 하나인 차분 전력 분석 및 상관 전력 분석과 같은 부채널 공격은, 고정된 암호 키 중 임의로 추측한 일부의 암호 키를 평문 또는 암호문과 결합하여 예측한 소비 전력과 실제 소비 전력에 대한 통계적인 유사성을 분석하는 방식에 따라 암호 키를 추출하기 때문에, 도 5 내지 도 8에 포함된 다양한 암호화 연산을 기반으로 암호화 연산 중간 값이 매번 달라지도록 관리하는 본 발명의 방법은 공격자의 부채널 분석으로부터 안전할 수 있다. 일 예로, 본 발명의 도 6에서 난수 N에 따라 암호화 연산에 사용되는 라운드 키 R*가 달라지므로, 전체 암호화 연산의 중간 값이 달라지게 되어 도 6의 방법이 외부의 부채널 공격으로부터 저항성을 가질 수 있다.

[0078] 도 5 내지 도 8에 따른 다양한 연산을 기반으로 한 본 발명의 정보 전송 방법을 처리하는 종합적인 알고리즘의 예시는 도 9와 같을 수 있다.

[0079] 도 9는 다양한 실시예들에 따른 본 발명의 정보 전송 방법을 처리하는 알고리즘의 일 예시를 도시한 도면이다.

[0080] 도 9에서 도시하는 알고리즘의 예시는, 국제 표준 블록 암호 중 하나인 AES를 적용한 알고리즘의 일 예시에 해당할 수 있다. 도 9에서는 128, 192 및 256 비트 중 하나의 크기를 가지는 마스터 키 K와 임의의 크기의 평문 P를 입력으로 받을 수 있으며, 입력된 마스터 키 K에 대한 AES 키 스케줄링 함수의 연산을 통해 마스터 키 K로부터 라운드 키 R을 생성할 수 있다(901).

[0081] 도 9의 알고리즘에서는, 평문 P에 대한 암호화를 수행함에 있어 암호화 함수의 입력 비트 크기가 128 비트임에도 평문 P의 마지막 블록의 크기가 128 비트 미만이라면, 평문 P의 비트 크기를 암호화 함수의 입력 요구 비트 크기에 맞추기 위해 평문 P에 패딩(padding)이 적용될 수 있으며(903), 이후 평문 블록의 개수만큼 후술하는 905 내지 909의 과정이 반복될 수 있다. 여기서 패딩이란, 요구되는 입력 비트의 크기를 맞추기 위해, 본래의 데이터 비트 뒤쪽에 요구되는 입력 비트의 크기를 맞출 수 있을 때까지 '0'의 비트를 추가하는 동작을 의미할 수 있다.

[0082] 도 9의 알고리즘은 우선 암호화 과정에 사용될 임의의 크기의 난수 N을 생성할 수 있으며(905), 생성한 난수 N과 사전에 계산한 라운드 키 R을 결합하여 전술한 도 7 내지 도 8의 알고리즘에 따른 키 생성 함수를 통해 암호화 키 R*를 생성할 수 있다(907). 이후 평문 블록과 암호화 키 R*를 입력으로 AES 암호화 함수의 연산을 통해 평문 P에 대응하는 암호문 C가 생성될 수 있다(909). 도 9의 알고리즘에서는 상기의 과정을 반복함으로써 임의의 평문에 대한 암호문을 생성할 수 있으며, 기존과 다르게 라운드 별 키 스케줄링을 블록마다 수행하지 않기 때문에 효율성이 증가하는 장점을 가질 수 있다.

[0083] 다른 암호 알고리즘에 대해 본 발명의 방식을 적용하고자 하는 경우, 도 9의 알고리즘에서 AES 암호화 함수의 연산에 대응하는 AESe를 해당 다른 암호 알고리즘의 암호화 함수로 변경하고, AES 키 스케줄링 함수의 연산에 대응하는 AESs를 해당 다른 암호 알고리즘의 키 스케줄링 함수로 변경하는 과정을 거쳐 다른 암호 알고리즘에 대해 본 발명의 방식을 유사하게 적용할 수 있다. 이와 같은 적용 방식을 통해 본 발명은 모든 블록 암호에 적용되는 범용성을 가질 수 있다.

[0084] 본 발명에서 제안하는 키 스케줄링 함수 및 키 생성 함수에 기반하여 평문을 암호화 한 암호문을 전송하는 방법을 통해, 복잡한 키 스케줄링 수행을 암호화 연산마다 수행해야 하는 기존의 알고리즘과 다르게, 한 번의 키 스케줄링 연산만을 수행하여 효율성을 높이면서도 부채널 분석에 대해 기존과 동일한 안전성을 도모할 수 있다.

[0086] 본 명세서와 도면에 개시된 본 발명의 실시예들은 본 발명의 기술 내용을 쉽게 설명하고 본 발명의 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 즉 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은 본 발명의 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명한 것이다. 또한 상기 각각의 실시 예는 필요에 따라 서로 조합되어 운용할 수 있다. 예컨대, 본 발명의 모든 실시 예는 일부분들이 서로 조합되어 시스템에 의해 구현될 수 있다.

[0087] 또한, 본 발명에 따른 시스템 등에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다.

[0088] 이와 같이, 본 발명의 다양한 실시예들은 특정 관점에서 컴퓨터 리드 가능 기록 매체(computer readable recording medium)에서 컴퓨터 리드 가능 코드(computer readable code)로서 구현될 수 있다. 컴퓨터 리드 가능 기록 매체는 컴퓨터 시스템에 의해 리드될 수 있는 데이터를 저장할 수 있는 임의의 데이터 저장 디바이스이다. 컴퓨터 리드 가능 기록 매체의 예들은 읽기 전용 메모리(read only memory: ROM)와, 랜덤-접속 메모리(random access memory: RAM)와, 컴팩트 디스크- 리드 온니 메모리(compact disk-read only memory: CD-ROM)들과, 마그네틱 테이프(magnetic tape)들과, 플로피 디스크(floppy disk)들과, 광 데이터 저장 디바이스들, 및 캐리어 웨이브(carrier wave)들(인터넷을 통한 데이터 송신 등)을 포함할 수 있다. 컴퓨터 리드 가능 기록 매체는 또한 네트워크 연결된 컴퓨터 시스템들을 통해 분산될 수 있고, 따라서 컴퓨터 리드 가능 코드는 분산 방식으로 저장 및 실행된다. 또한, 본 발명의 다양한 실시예들을 성취하기 위한 기능적 프로그램들, 코드, 및 코드 세그먼트(segment)들은 본 발명이 적용되는 분야에서 숙련된 프로그래머들에 의해 쉽게 해석될 수 있다.

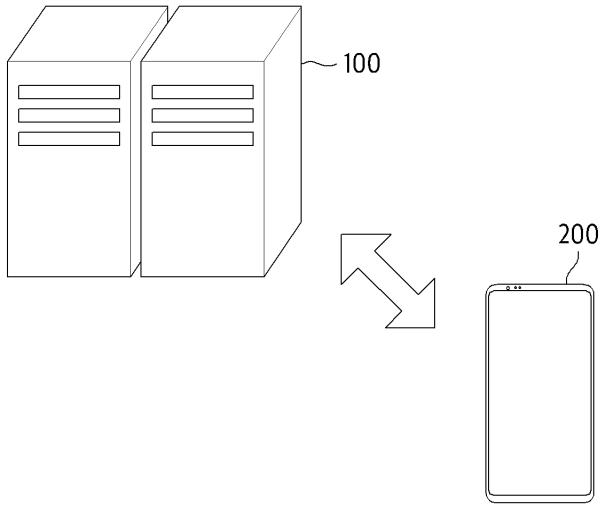
[0089] 또한 본 발명의 다양한 실시예들에 따른 장치 및 방법은 하드웨어, 소프트웨어 또는 하드웨어 및 소프트웨어의 조합의 형태로 실현 가능하다는 것을 알 수 있을 것이다. 이러한 소프트웨어는 예를 들어, 삭제 가능 또는 재기록 가능 여부와 상관없이, ROM 등의 저장 장치와 같은 휘발성 또는 비 휘발성 저장 장치, 또는 예를 들어, RAM, 메모리 칩, 장치 또는 집적 회로와 같은 메모리, 또는 예를 들어 콤팩트 디스크(compact disk: CD), DVD, 자기 디스크 또는 자기 테이프 등과 같은 광학 또는 자기적으로 기록 가능함과 동시에 기계(예를 들어, 컴퓨터)로 읽을 수 있는 저장 매체에 저장될 수 있다. 본 발명의 다양한 실시예들에 따른 방법은 제어부 및 메모리를 포함하는 컴퓨터 또는 이와 같은 메모리 또는 컴퓨터를 포함한 차량 등에 의해 구현될 수 있고, 이러한 메모리는 본 발명의 실시예들을 구현하는 명령들을 포함하는 프로그램 또는 프로그램들을 저장하기에 적합한 기계로 읽을 수 있는 저장 매체의 한 예임을 알 수 있을 것이다.

[0090] 따라서, 본 발명은 본 명세서의 청구항에 기재된 장치 또는 방법을 구현하기 위한 코드를 포함하는 프로그램 및 이러한 프로그램을 저장하는 기계(컴퓨터 등)로 읽을 수 있는 저장 매체를 포함한다. 또한, 이러한 프로그램은 유선 또는 무선 연결을 통해 전달되는 통신 신호와 같은 임의의 매체를 통해 전자적으로 이송될 수 있고, 본 발명은 이와 균등한 것을 적절하게 포함한다.

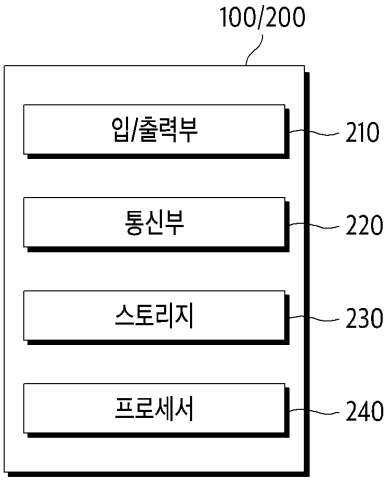
[0091] 상기에서는 본 발명의 실시예들을 참조하여 설명하였지만, 본 명세서와 도면에 개시된 본 발명의 실시예들은 본 발명의 기술 내용을 쉽게 설명하고 본 발명의 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며 본 발명의 범위를 한정하고자 하는 것은 아니다. 또한 앞서 설명된 본 발명에 따른 실시예들은 예시적인 것에 불과하며, 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 범위의 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 다음의 특허청구범위에 의해서 정해져야 할 것이다.

도면

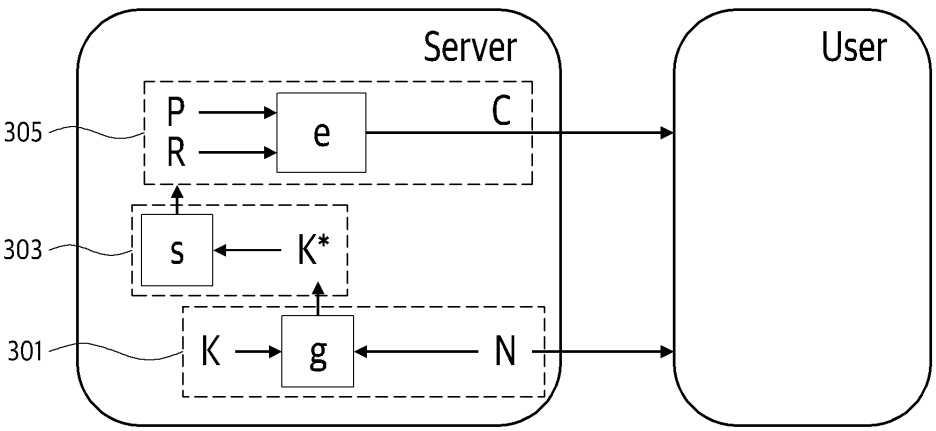
도면1



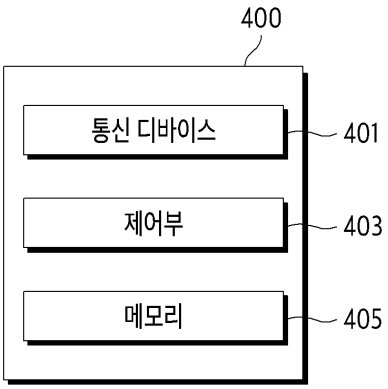
도면2



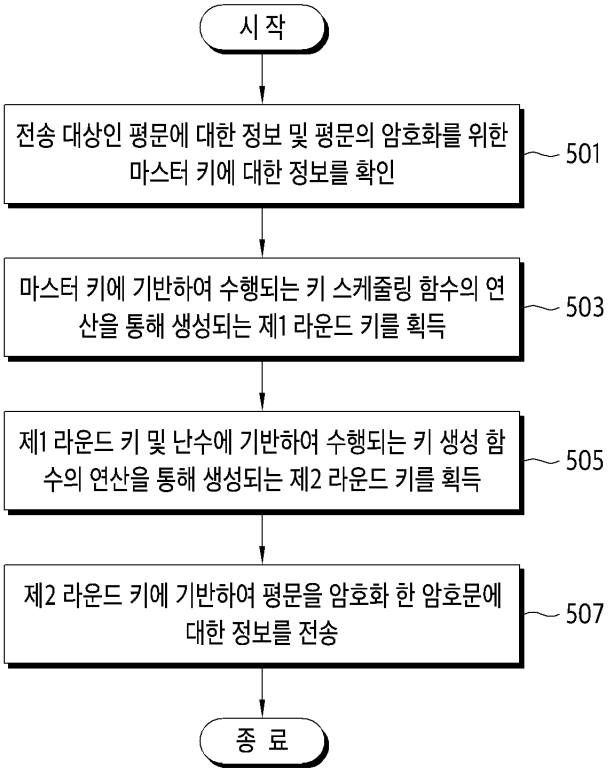
도면3



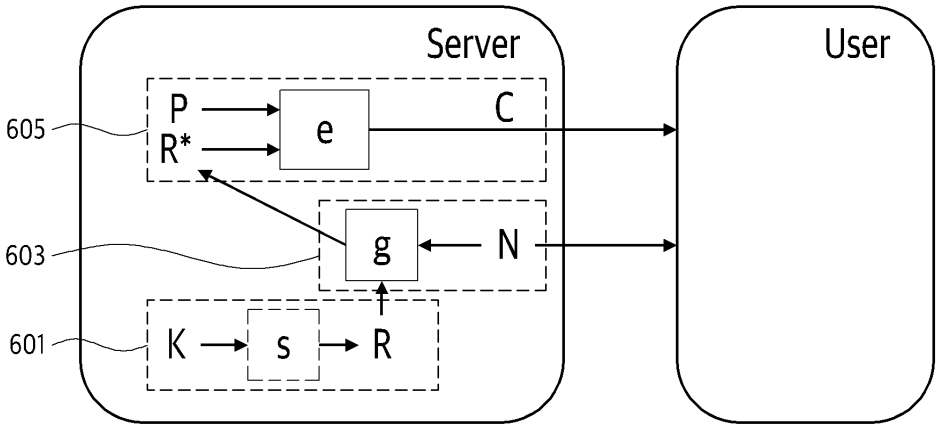
도면4


400
통신 디바이스
401
제어부
403
메모리
405

도면5


시 작
전송 대상인 평문에 대한 정보 및 평문의 암호화를 위한 마스터 키에 대한 정보를 확인
501
마스터 키에 기반하여 수행되는 키 스케줄링 함수의 연산을 통해 생성되는 제1 라운드 키를 획득
503
제1 라운드 키 및 난수에 기반하여 수행되는 키 생성 함수의 연산을 통해 생성되는 제2 라운드 키를 획득
505
제2 라운드 키에 기반하여 평문을 암호화 한 암호문에 대한 정보를 전송
507
종 료

도면6



도면7

알고리즘 1. 키 생성 함수 g

입력: 난수 $N=(N_0, N_1, ..., N_i)$, 라운드 키 $R=(R_0, R_1, ..., R_j) = s(K)$ (A_i 는 A의 i번째 비트)

출력: 암호화 키 R^*

```
1. if  i ≥ j                                  ┐
2.      for k = 0 to i                        │ 701
3.          R*_k = N_k ⊕ R_{kmod(j+1)}        │
4.      end for                               ┘
5. else ( i < j )                             ┐
6.      for k = 0 to j                        │ 703
7.          R*_k = N_{kmod(i+1)} ⊕ R_k        │
8.      end for                               ┘
9. end if
5. return R*
```

도면8

알고리즘 2. 내부 상태 값을 가지는 키 생성 함수 g

입력: 난수 $N=(N_0, N_1, ..., N_i)$, 라운드 키 $R=(R_0, R_1, ..., R_j) = s(K)$ (A_i 는 A의 i번째 비트)

출력: 암호화 키 R^*

```
//내부 상태 값 S                                                    ~ 801
 1. ifndef S
 2.     S = 0 // 내부 상태 값이 정의되지 않은 경우, 0으로 초기화.
 3. end ifndef
 4. S ← S ⊕ N
 5. if i ≥ j                                                       ~ 803
 6.     for k = 0 to i
 7.         R*_k = S_k ⊕ R_kmod(j+1)
 8.     end for
 8. else ( i < j )                                                 ~ 805
10.     for k = 0 to j
11.         R*_k = S_kmod(i+1) ⊕ R_k
12.     end for
13. end if
14. return R*
```

도면9

알고리즘 3. 키 재사용 기법 알고리즘 (Case: AES)

입력: 마스터키 K, 평문 $P = (P_0, P_1, ..., P_i)$. P_j는 P의 j 번째 블록이며,
$j = i$를 제외한 각 블록의 크기는 128비트.

출력: 암호문 $C = (C_0, C_1, ..., C_i)$

```
1. R ← AESs (K)                          //AES 키 스케줄링 함수 수행   ~ 901
2. if size(P_i) ≠ 128 - bit then P_i ← padding(P_i)                  ~ 903
3. for k = 0 to i
4.     N ← Rand( )                       //난수 생성                 ~ 905
5.     R* ← g(N, R)                      //키 생성 함수 수행         ~ 907
6.     C_k ← AESe (Pk, R*)               //AES 암호화 함수 수행      ~ 909
7. end for
8. return C
```