(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0115963
(43) 공개일자 2016년10월06일

(51) 국제특허분류(Int. Cl.)
G09C 1/00 (2006.01) *H04L 9/00* (2006.01)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
G09C 1/00 (2013.01)
H04L 9/003 (2013.01)
(21) 출원번호 10-2016-7023777
(22) 출원일자(국제) 2015년02월03일
심사청구일자 없음
(85) 번역문제출일자 2016년08월29일
(86) 국제출원번호 PCT/US2015/014294
(87) 국제공개번호 WO 2015/117144
국제공개일자 2015년08월06일
(30) 우선권주장
14/171,558 2014년02월03일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
구오, 시아오페이
미국 11218 뉴욕 브루클린 12 애비뉴 3543 에프엘 1
구오, 수
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
브럼리, 빌리 비.
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인 남앤드남

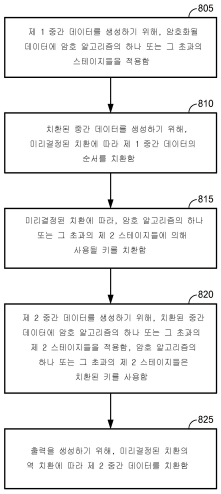
전체 청구항 수 : 총 28 항

(54) 발명의 명칭 **암호 알고리즘들 상의 사이드-채널 공격들에 대해 치환들을 사용하는 대책들**

(57) 요 약

암호 알고리즘들에 대한 사이드-채널 공격들을 방지하는 것을 돕기 위해 사용될 수 있는, 데이터를 암호화하기 위한 기술들이 제공된다. 이들 기술들에 따른 예시적인 방법은, 치환된 중간 데이터를 생성하기 위해, 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환시키는 단계를 포함한다. 제 1 중간 데이터는, 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력된다. 방법은 또한, 미리결정된 치환에 따라, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키를 치환시키는 단계, 제 2 중간 데이터를 생성하기 위해, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들을 치환된 중간 데이터에 적용하는 단계 – 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 –, 및 출력을 생성하기 위해, 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키는 단계를 포함한다.

대 표 도 - 도8



암호화 프로세스

(52) CPC특허분류
H04L 9/0631 (2013.01)
H04L 9/0869 (2013.01)
H04L 2209/08 (2013.01)
H04L 2209/12 (2013.01)
H04L 2209/24 (2013.01)

명 세 서

청구범위

청구항 1

데이터를 암호화하기 위한 방법으로서,

치환(permute)된 중간(intermediate) 데이터를 생성하기 위해 선택된 치환에 따라 제 1 중간 데이터의 순서를 치환시키는 단계 – 상기 제 1 중간 데이터는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력됨 –;

상기 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키(key)의 바이트들의 순서를 상기 선택된 치환에 따라 치환시키는 단계;

제 2 중간 데이터를 생성하기 위해 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들을 상기 치환된 중간 데이터에 적용하는 단계 - 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 -; 및

출력을 생성하기 위해 상기 선택된 치환의 역(inverse) 치환에 따라 상기 제 2 중간 데이터의 바이트들의 순서를 치환시키는 단계를 포함하는, 데이터를 암호화하기 위한 방법.

청구항 2

제 1 항에 있어서,

상기 제 1 중간 데이터를 생성하기 위해 암호화될 데이터에 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들을 적용하는 단계를 더 포함하는, 방법.

청구항 3

제 1 항에 있어서,

일 세트의 치환들로부터 치환을 선택하는 단계를 더 포함하며,

상기 치환된 중간 데이터를 생성하기 위해 선택된 치환에 따라 제 1 중간 데이터의 순서를 치환시키는 단계는, 상기 선택된 치환을 사용하여 상기 제 1 중간 데이터의 순서를 치환시키는 단계를 포함하는, 방법.

청구항 4

제 3 항에 있어서,

상기 일 세트의 치환들로부터 치환을 선택하는 단계는,

난수(random number) 시드(seed) 값을 생성하는 단계; 및

상기 난수 시드 값에 기초하여 상기 일 세트의 치환들로부터 상기 치환을 선택하는 단계를 포함하는, 방법.

청구항 5

제 3 항에 있어서,

상기 일 세트의 치환들로부터 치환을 선택하는 단계는, 선택된 패턴에 기초하여 상기 일 세트의 치환들로부터 상기 치환을 선택하는 단계를 포함하는, 방법.

청구항 6

제 3 항에 있어서,

상기 출력을 생성하기 위해 상기 선택된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키는 단계는, 상기 일 세트의 치환들로부터의 상기 선택된 치환에 기초하여 일 세트의 역 치환들로부터 상기 역 치환을 선택하는

단계를 포함하는, 방법.

청구항 7

제 1 항에 있어서,

상기 암호 알고리즘은 AES(Advanced Encryption Standard) 알고리즘이고,

상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들은 상기 AES 알고리즘의 제 1 라운드를 포함하고 그리고 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 상기 AES 알고리즘의 제 2 라운드를 포함하거나, 또는 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들은 상기 AES 알고리즘의 마지막 라운드 바로 앞의 라운드(next to last round)를 포함하고 그리고 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 상기 AES 알고리즘의 최종 라운드를 포함하는, 방법.

청구항 8

데이터를 암호화하기 위한 시스템으로서,

치환된 중간 데이터를 생성하기 위해 선택된 치환에 따라 제 1 중간 데이터의 순서를 치환시키기 위한 수단 - 상기 제 1 중간 데이터는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력됨 -;

상기 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키의 바이트들의 순서를 상기 선택된 치환에 따라 치환시키기 위한 수단;

제 2 중간 데이터를 생성하기 위해 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들을 상기 치환된 중간 데이터에 적용하기 위한 수단 - 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 -; 및

출력을 생성하기 위해 상기 선택된 치환의 역 치환에 따라 상기 제 2 중간 데이터의 바이트들의 순서를 치환시키기 위한 수단을 포함하는, 데이터를 암호화하기 위한 시스템.

청구항 9

제 8 항에 있어서,

상기 제 1 중간 데이터를 생성하기 위해 암호화될 데이터에 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들을 적용하기 위한 수단을 더 포함하는, 데이터를 암호화하기 위한 시스템.

청구항 10

제 8 항에 있어서,

일 세트의 치환들로부터 치환을 선택하기 위한 수단을 더 포함하며,

상기 치환된 중간 데이터를 생성하기 위해 선택된 치환에 따라 제 1 중간 데이터의 순서를 치환시키기 위한 수단은, 상기 선택된 치환을 사용하여 상기 제 1 중간 데이터의 순서를 치환시키기 위한 수단을 포함하는, 데이터를 암호화하기 위한 시스템.

청구항 11

제 10 항에 있어서,

상기 일 세트의 치환들로부터 치환을 선택하기 위한 수단은,

난수 시드 값을 생성하기 위한 수단; 및

상기 난수 시드 값에 기초하여 상기 일 세트의 치환들로부터 상기 치환을 선택하기 위한 수단을 포함하는, 데이터를 암호화하기 위한 시스템.

청구항 12

제 10 항에 있어서,

상기 일 세트의 치환들로부터 치환을 선택하기 위한 수단은,

난수 시드 값을 생성하기 위한 수단; 및

상기 난수 시드 값에 기초하여 상기 일 세트의 치환들로부터 상기 치환을 선택하기 위한 수단을 포함하는, 데이터를 암호화하기 위한 시스템.

청구항 13

제 10 항에 있어서,

상기 출력을 생성하기 위해 상기 선택된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키기 위한 수단은, 상기 일 세트의 치환들로부터의 상기 선택된 치환에 기초하여 일 세트의 역 치환들로부터 상기 역 치환을 선택하기 위한 수단을 포함하는, 데이터를 암호화하기 위한 시스템.

청구항 14

제 8 항에 있어서,

상기 암호 알고리즘은 AES(Advanced Encryption Standard) 알고리즘이고,

상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들은 상기 AES 알고리즘의 제 1 라운드를 포함하고 그리고 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 상기 AES 알고리즘의 제 2 라운드를 포함하거나, 또는 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들은 상기 AES 알고리즘의 마지막 라운드 바로 앞의 라운드를 포함하고 그리고 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 상기 AES 알고리즘의 최종 라운드를 포함하는, 데이터를 암호화하기 위한 시스템.

청구항 15

데이터를 암호화하기 위한 컴퓨터-판독가능 명령들이 저장된 비-일시적인 컴퓨터-판독가능 매체로서,

컴퓨터로 하여금, 치환된 중간 데이터를 생성하기 위해 선택된 치환에 따라 제 1 중간 데이터의 순서를 치환시키게 하도록 구성되는 명령들 – 상기 제 1 중간 데이터는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력됨 –;

상기 컴퓨터로 하여금, 상기 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키의 바이트들의 순서를 상기 선택된 치환에 따라 치환시키도록 구성되는 명령들;

상기 컴퓨터로 하여금, 제 2 중간 데이터를 생성하기 위해 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들을 상기 치환된 중간 데이터에 적용하게 하도록 구성되는 명령들 - 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 -; 및

상기 컴퓨터로 하여금, 출력을 생성하기 위해 상기 선택된 치환의 역 치환에 따라 상기 제 2 중간 데이터의 바이트들의 순서를 치환시키게 하도록 구성되는 명령들을 포함하는, 비-일시적인 컴퓨터-판독가능 매체.

청구항 16

제 15 항에 있어서,

상기 컴퓨터로 하여금, 상기 제 1 중간 데이터를 생성하기 위해 암호화될 데이터에 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들을 적용하게 하도록 구성되는 명령들을 더 포함하는, 비-일시적인 컴퓨터-판독가능 매체.

청구항 17

제 15 항에 있어서,

상기 컴퓨터로 하여금, 일 세트의 치환들로부터 치환을 선택하게 하도록 구성되는 명령들을 더 포함하며,

상기 컴퓨터로 하여금, 치환된 중간 데이터를 생성하기 위해 선택된 치환에 따라 제 1 중간 데이터의 순서를 치환시키게 하도록 구성되는 명령들은, 상기 컴퓨터로 하여금, 상기 선택된 치환을 사용하여 상기 제 1 중간 데이터의 순서를 치환시키게 하도록 구성되는 명령들을 포함하는, 비-일시적인 컴퓨터-판독가능 매체.

청구항 18

제 17 항에 있어서,

상기 컴퓨터로 하여금, 일 세트의 치환들로부터 치환을 선택하게 하도록 구성되는 명령들은,

상기 컴퓨터로 하여금, 난수 시드 값을 생성하게 하도록 구성되는 명령들; 및

상기 컴퓨터로 하여금, 상기 난수 시드 값에 기초하여 상기 일 세트의 치환들로부터 상기 치환을 선택하게 하도록 구성되는 명령들을 포함하는, 비-일시적인 컴퓨터-판독가능 매체.

청구항 19

제 17 항에 있어서,

상기 컴퓨터로 하여금, 일 세트의 치환들로부터 치환을 선택하게 하도록 구성되는 명령들은,

상기 컴퓨터로 하여금, 선택된 패턴에 기초하여 상기 일 세트의 치환들로부터 상기 치환을 선택하게 하도록 구성되는 명령들을 포함하는, 비-일시적인 컴퓨터-판독가능 매체.

청구항 20

제 17 항에 있어서,

상기 컴퓨터로 하여금, 출력을 생성하기 위해 상기 선택된 치환의 역 치환에 따라 상기 제 2 중간 데이터를 치환시키게 하도록 구성되는 명령들은, 상기 컴퓨터로 하여금, 상기 일 세트의 치환들로부터의 상기 선택된 치환에 기초하여 일 세트의 역 치환들로부터 상기 역 치환을 선택하게 하도록 구성되는 명령들을 포함하는, 비-일시적인 컴퓨터-판독가능 매체.

청구항 21

제 15 항에 있어서,

상기 암호 알고리즘은 AES(Advanced Encryption Standard) 알고리즘이고,

상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들은 상기 AES 알고리즘의 제 1 라운드를 포함하고 그리고 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 상기 AES 알고리즘의 제 2 라운드를 포함하거나, 또는 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들은 상기 AES 알고리즘의 마지막 라운드 바로 앞의 라운드를 포함하고 그리고 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 상기 AES 알고리즘의 최종 라운드를 포함하는, 비-일시적인 컴퓨터-판독가능 매체.

청구항 22

데이터를 암호화하기 위한 회로로서,

치환된 중간 데이터를 생성하기 위해 선택된 치환에 따라 제 1 중간 데이터의 순서를 치환시키도록 구성되는 제 1 세트의 컴포넌트들 – 상기 제 1 중간 데이터는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력됨 –;

상기 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키의 바이트들의 순서를 상기 선택된 치환에 따라 치환시키도록 구성되는 제 2 세트의 컴포넌트들;

제 2 중간 데이터를 생성하기 위해 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들을 상기 치환된 중간 데이터에 적용하도록 구성되는 제 3 세트의 컴포넌트들 - 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 -; 및

출력을 생성하기 위해 상기 선택된 치환의 역 치환에 따라 상기 제 2 중간 데이터의 바이트들의 순서를 치환시키도록 구성되는 제 4 세트의 컴포넌트들을 포함하는, 데이터를 암호화하기 위한 회로.

청구항 23

제 22 항에 있어서,

상기 제 1 중간 데이터를 생성하기 위해 암호화될 데이터에 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들을 적용하도록 구성되는 제 5 세트의 컴포넌트들을 더 포함하는, 데이터를 암호화하기 위한 회로.

청구항 24

제 22 항에 있어서,

일 세트의 치환들로부터 치환을 선택하도록 구성되는 제 6 세트의 컴포넌트들을 더 포함하며,

상기 치환된 중간 데이터를 생성하기 위해 상기 선택된 치환에 따라 상기 제 1 중간 데이터의 순서를 치환시키는 것은, 상기 선택된 치환을 사용하여 상기 제 1 중간 데이터의 순서를 치환시키는 것을 포함하는, 데이터를 암호화하기 위한 회로.

청구항 25

제 24 항에 있어서,

상기 제 6 세트의 컴포넌트들은 추가로,

난수 시드 값을 생성하고; 그리고

상기 난수 시드 값에 기초하여 상기 일 세트의 치환들로부터 상기 치환을 선택

하도록 구성되는, 데이터를 암호화하기 위한 회로.

청구항 26

제 24 항에 있어서,

상기 제 6 세트의 컴포넌트들은 추가로, 선택된 패턴에 기초하여 상기 일 세트의 치환들로부터 상기 치환을 선택하도록 구성되는, 데이터를 암호화하기 위한 회로.

청구항 27

제 24 항에 있어서,

상기 제 4 세트의 컴포넌트들은, 상기 선택된 치환에 기초하여 일 세트의 역 치환들로부터 상기 역 치환을 선택하도록 구성되는, 데이터를 암호화하기 위한 회로.

청구항 28

제 22 항에 있어서,

상기 암호 알고리즘은 AES(Advanced Encryption Standard) 알고리즘이고,

상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들은 상기 AES 알고리즘의 제 1 라운드를 포함하고 그리고 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 상기 AES 알고리즘의 제 2 라운드를 포함하거나, 또는 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 1 스테이지들은 상기 AES 알고리즘의 마지막 라운드 바로 앞의 라운드를 포함하고 그리고 상기 암호 알고리즘의 상기 하나 또는 그 초과의 제 2 스테이지들은 상기 AES 알고리즘의 최종 라운드를 포함하는, 데이터를 암호화하기 위한 회로.

발명의 설명

배 경 기 술

[0001] [0001] 보호된 데이터에 대한 비인가된 액세스 및/또는 수정을 방지하기 위해 다양한 암호화(encryption) 기술들이 사용될 수 있다. 그러나, 몇몇 암호화 기술들은 사이드-채널(side-channel) 공격들에 취약할 수 있다. 사이드-채널 공격들은, 암호 시스템의 물리적 구현으로부터 획득되는 정보에 기초하는 공격들이며, 통상적으로, 암호 알고리즘에 대한 브루트 포스(brute force) 공격 또는 알고리즘에 내재하는 이론적 취약점에 대한 공격이 아니다. 사이드-채널 공격들은, 암호 키들, 부분적 상태 정보, 및/또는 암호화되는 정보에 관한 완전한 또는 부분적 평문(plaintext) 정보를 비롯하여, 암호 알고리즘이 어떻게 동작하는지에 관한 정보를 수집하는데 사용될 수 있다.

[0002] [0002] 전력 분석 및 전자기(EM) 공격들은, 암호 알고리즘들을 손상시키는데 사용될 수 있는 사이드-채널 공격들의 2개의 타입들의 예들이다. 전력 분석 공격에서, 공격자는, 공격 받는 암호 알고리즘을 구현한 디바이스의 전력 소모를 모니터링한다. 전력 분석 공격들은 복잡도가 다양할 수 있다. 단순 전력 분석(SPA; simple power analysis) 공격들은, 암호 알고리즘에 관한 정보를 도출하기 위해, 공격 받는 암호 알고리즘을 구현하는 하드웨어에 의해 생성되는 전력 트레이스(trace)들(이들은 시간에 걸친 전기 활동도의 그래프들임)을 해석하는 것을 수반한다. 차동 전력 분석(DPA; Differential power analysis)은, 공격 받는 디바이스에 의해 수행되는 다수의 암호 동작들로부터 수집되는 데이터에 통계적 분석을 적용하는 더 진보된 전력 분석 공격 기술을 수반한다. 통계적은 분석은, 공격 받는 암호 알고리즘 내의 중간(intermediate) 값들을 결정하는데 사용될 수 있는 정보를 공격자에게 제공할 수 있다. EM 공격에서, 공격자는 암호 알고리즘을 구현한 하드웨어로부터의 전자기 방출(emanation)들을 모니터링한다. 공격자는, 이들 방출들을 분석함으로써, 하드웨어를 통해 흐르는 전류들에 관한 정보를 도출하고 그 정보를 사용하여 각각의 클록 사이클 동안 디바이스 내에서 발생하는 이벤트들을 식별할 수 있다. 다른 타입들의 사이드-채널 공격들은, 차동 장애 분석(differential fault analysis)(여기서, 암호 알고리즘에 관한 정보를 유출(reveal)시키려는 시도 시에 암호 연산(computation)들에서 장애들이 유발됨), 타이밍 공격들(여기서, 공격은, 암호 알고리즘이 실행되는 동안 특정 연산 태스크들을 수행는 것이 얼마나 오래 걸리는지를 측정하는 것에 기초함), 및 음향(acoustic) 공격들(여기서, 공격은, 암호 알고리즘이 실행되는 동안 공격 받는 암호 알고리즘을 구현하는 디바이스의 하드웨어로부터 방출되는 사운드들에 기초함)을 포함한다.

[0003] [0003] 모바일 폰들, 태블릿 컴퓨터들, 랩톱들, 및/또는 다른 그러한 디바이스들과 같은 많은 디바이스들은, 상보성 금속-산화물-반도체(CMOS) 기술에 기초하는 디지털 회로들을 사용하여 구성된다. CMOS 기술은 보통, 디지털 로직 회로들, 정적 랜덤 액세스 메모리(SRAM), 마이크로프로세서들, 및 마이크로제어기들에서 사용된다. CMOS 구현들은, 전력 분석 및 EM 공격들에 취약(susceptible)할 수 있다. CMOS 디지털 회로들의 정적 전력 소모는 통상적으로 매우 낮다. CMOS 디지털 회로들이 상이한 입력들로 클로킹(clock)되는 경우, 디지털 회로들은 상태들을 변경한다. 이러한 상태 변경들은, 내부 커패시터들의 충전(charging) 및 방전(discharging)을 유발한다. 결과적인 전압 요동들은 연산되는 데이터에 의존한다. 암호화 방식을 해독(break)하길 원하는 악의적인 파티(party)는, 디바이스의 전력 소모 및/또는 디바이스로부터의 EM 방출을 모니터링하여, 수신되고 있는 데이터와 전력 소모 및/또는 EM 방출들을 상관(correlate)시킬 수 있다. 그러한 테스팅의 결과들을 분석하는 것은, 암호화 방식에 의해 사용되는 키, 암호 알고리즘에 의해 생성되는 중간 값들, 및/또는 공격자가 암호화 알고리즘을 구성하는데 이용하는 것이 가능할 수 있는 다른 정보를 유출시킬 수 있다.

[0004] [0004] 도 1은, 암호 알고리즘에 대한 전력 분석 공격을 수행하는데 사용될 수 있는 예시적인 프로세스를 예시한다. 도 1에 예시된 전력 분석 공격은, 암호화 알고리즘에 의해 사용되는 키를 결정하려 시도하기 위해 브루트 포스 접근법을 활용한다. 도 1에 예시된 예시적인 프로세스는 AES(Advanced Encryption Standard) 알고리즘을 공격하는데 사용되지만, 다른 타입들의 암호화 기술들을 공격하기 위해 유사한 절차들이 사용될 수 있다. 전력 분석 공격이 성공적이게 하기 위해, 공격자는, 그러한 추정적(hypothetical) 전력 소모를 시뮬레이팅하기 위한 전력 모델이 생성될 수 있도록, 공격 받는 알고리즘을 알아야 하며, 공격자는, 연산되고 있는 데이터와 회로의 어느 전력 트레이스들이 상관되는지를 알아야 한다. 이러한 정보를 사용하여, 공격자는, 특정 디바이스에 의해 사용되는 암호 알고리즘에 대해 다음의 단계들을 사용함으로써 전력 분석 공격을 수행할 수 있다.

[0005] (1) 실행되는 암호 알고리즘의 중간 결과들이 선택될 수 있다. 예를 들어, 특정 디바이스가 AES(Advanced Encryption Standard) 알고리즘의 일 버전을 구현한다는 것을 공격자가 인지하면, 공격자는, 공격 포인트로서 디바이스 상에 구현되는 AES 알고리즘의 제 1 라운드(round)의 출력을 선택할 수 있다. 공격자는 AES 알고리즘의 다른 라운드들을 또한 선택할 수 있다. 예를 들어, AES 알고리즘의 마지막 라운드 바로 앞의 라운드(next to last round)가 또한 공격자들에 의해 타겟팅될 수 있다.

[0006] (2) 평문 입력 및 키 추정(hypothesis)들에 기초하는 추정적 중간 값들이 생성될 수 있다. 예를 들어, 추정적 중간 값들은, 알려진 평문 값 및 일 세트의 키 추정들을 암호화 알고리즘에 제공함으로써 생성될 수 있다. AES 예로 돌아가면, 추정 중간 값들은, AES 알고리즘의 제 1 라운드 또는 어느 라운드이든 간에 공격자가 타겟팅한 AES 알고리즘의 라운드의 출력일 수 있다.

[0007] (3) 추정적 중간 값들은 그 후, 추상적(abstract) 전력 소모 모델에 맵핑(map)될 수 있다. 추상적 전력 소모 모델은, 공격받고 있는 암호 알고리즘에 기초한다(스테이지 103). 암호 알고리즘에 타입에 의존하여 전력 소모는 변할 것이고, 암호 알고리즘의 다양한 스테이지들 또는 라운드들 에 대한 전력 소모가 추정될 수 있다.

[0008] (4) 암호 알고리즘의 타겟팅된 스테이지의 전력 트레이스들은 그 후, 공격받고 있는 암호 알고리즘을 사용하도

록 구성되는 실제 모바일 디바이스 상에서 측정될 수 있다(스테이지 104). 전력 트레이스들은 시간에 걸쳐 사용되는 전류의 그래프들이고, 전력 트레이스들은, 암호 알고리즘의 다양한 라운드들 또는 스테이지들의 속성들을 유출시킬 수 있고, 이는 공격자가 키들을 도출하는 것을 허용할 수 있다.

[0009] (5) 전력 트레이스들은 그 후, 암호 알고리즘과 연관된 키 또는 키의 적어도 일부를 식별하려 시도하기 위해, 추상적 소모 모델과 상관될 수 있다(스테이지 105).

발명의 내용

[0010] [0005] 본 개시내용에 따른, 데이터를 암호화하기 위한 예시적인 방법은, 치환(permute)된 중간 데이터를 생성하기 위해 미리결정된 치환(permutation)에 따라 제 1 중간 데이터의 순서를 치환시키는 단계를 포함하며, 제 1 중간 데이터는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력된다. 방법은 또한, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키를 미리결정된 치환에 따라 치환시키는 단계, 제 2 중간 데이터를 생성하기 위해, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들을 치환된 중간 데이터에 적용하는 단계 – 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 –, 및 출력을 생성하기 위해, 미리결정된 치환의 역 치환(inverse permutation)에 따라 제 2 중간 데이터를 치환시키는 단계를 포함한다.

[0011] [0006] 그러한 방법의 구현들은 다음의 특성들 중 하나 또는 그 초과를 포함할 수 있다. 제 1 중간 데이터를 생성하기 위해, 암호화될 데이터에 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들이 적용된다. 일 세트의 치환들로부터 치환이 선택되며, 여기서, 치환된 중간 데이터를 생성하기 위해 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환시키는 단계는, 선택된 치환을 사용하여 제 1 중간 데이터의 순서를 치환시키는 단계를 포함한다. 일 세트의 치환들로부터 치환을 선택하는 단계는, 난수(random number) 시드(seed) 값을 생성하는 단계, 및 난수 시드 값에 기초하여 일 세트의 치환들로부터 치환을 선택하는 단계를 포함한다. 일 세트의 치환들로부터 치환을 선택하는 단계는, 미리결정된 패턴에 기초하여 일 세트의 치환들로부터 치환을 선택하는 단계를 포함한다. 출력을 생성하기 위해 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키는 단계는, 선택된 치환에 기초하여 일 세트의 역 치환들로부터 역 치환을 선택하는 단계를 포함한다. 암호 알고리즘은 AES(Advanced Encryption Standard) 알고리즘이고, 여기서, 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은 AES 알고리즘의 제 1 라운드를 포함하고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 AES 알고리즘의 제 2 라운드를 포함하거나, 또는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은 AES 알고리즘의 마지막 라운드 바로 앞의 라운드를 포함하고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 AES 알고리즘의 최종 라운드를 포함한다.

[0012] [0007] 본 개시내용에 따른, 데이터를 암호화하기 위한 시스템은, 치환된 중간 데이터를 생성하기 위해 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환시키기 위한 수단 – 제 1 중간 데이터는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력됨 –, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키를 미리결정된 치환에 따라 치환시키기 위한 수단, 제 2 중간 데이터를 생성하기 위해 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들을 치환된 중간 데이터에 적용하기 위한 수단 - 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 -, 및 출력을 생성하기 위해, 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키기 위한 수단을 포함한다.

[0013] [0008] 그러한 시스템의 구현들은 다음의 특성들 중 하나 또는 그 초과를 포함할 수 있다. 제 1 중간 데이터를 생성하기 위해, 암호화될 데이터에 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들을 적용하기 위한 수단을 포함한다. 일 세트의 치환들로부터 치환을 선택하기 위한 수단을 포함하며, 치환된 중간 데이터를 생성하기 위해 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환시키기 위한 수단은, 선택된 치환을 사용하여 제 1 중간 데이터의 순서를 치환시키기 위한 수단을 포함한다. 일 세트의 치환들로부터 치환을 선택하기 위한 수단은, 난수 시드 값을 생성하기 위한 수단, 및 난수 시드 값에 기초하여 일 세트의 치환들로부터 치환을 선택하기 위한 수단을 포함한다. 일 세트의 치환들로부터 치환을 선택하기 위한 수단은, 난수 시드 값을 생성하기 위한 수단, 및 난수 시드 값에 기초하여 일 세트의 치환들로부터 치환을 선택하기 위한 수단을 포함한다. 출력을 생성하기 위해 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키기 위한 수단은, 선택된 치환에 기초하여 일 세트의 역 치환들로부터 역 치환을 선택하기 위한 수단을 포함한다. 암호 알고리즘은 AES(Advanced Encryption Standard) 알고리즘이고, 여기서, 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은 AES 알고리즘의 제 1 라운드를 포함하고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 AES 알고리즘의 제 2 라운드를 포함하거나, 또는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은

AES 알고리즘의 마지막 라운드 바로 앞의 라운드를 포함하고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 AES 알고리즘의 최종 라운드를 포함한다.

[0014] [0009] 본 개시내용에 따른 비-일시적인 컴퓨터 판독가능 매체에는, 데이터를 암호화하기 위한 컴퓨터-판독가능 명령들이 저장된다. 매체는, 컴퓨터로 하여금, 치환된 중간 데이터를 생성하기 위해 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환시키게 하도록 구성되는 명령들 - 제 1 중간 데이터는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력됨 -, 컴퓨터로 하여금, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키를 미리결정된 치환에 따라 치환시키게 하도록 구성되는 명령들, 컴퓨터로 하여금, 제 2 중간 데이터를 생성하기 위해 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들을 치환된 중간 데이터에 적용시키게 하도록 구성되는 명령들 - 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 -, 및 컴퓨터로 하여금, 출력을 생성하기 위해 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키게 하도록 구성되는 명령들을 포함한다.

[0015] [0010] 그러한 비-일시적인 컴퓨터 판독가능 매체의 구현들은 다음의 특성들 중 하나 또는 그 초과를 포함할 수 있다. 컴퓨터로 하여금, 제 1 중간 데이터를 생성하기 위해, 암호화될 데이터에 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들을 적용하게 하도록 구성되는 명령들을 포함한다. 컴퓨터로 하여금, 일 세트의 치환들로부터 치환을 선택하게 하도록 구성되는 명령들을 포함하며, 컴퓨터로 하여금, 치환된 중간 데이터를 생성하기 위해 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환시키게 하도록 구성되는 명령들은, 컴퓨터로 하여금, 선택된 치환을 사용하여 제 1 중간 데이터의 순서를 치환시키게 하도록 구성되는 명령들을 포함한다. 컴퓨터로 하여금, 일 세트의 치환들로부터 치환을 선택하게 하도록 구성되는 명령들은, 컴퓨터로 하여금, 난수 시드 값을 생성하게 하도록 구성되는 명령들, 및 컴퓨터로 하여금, 난수 시드 값에 기초하여 일 세트의 치환들로부터 치환을 선택하게 하도록 구성되는 명령들을 포함한다. 컴퓨터로 하여금, 일 세트의 치환들로부터 치환을 선택하게 하도록 구성되는 명령들은, 컴퓨터로 하여금, 미리결정된 패턴에 기초하여 일 세트의 치환들로부터 치환을 선택하게 하도록 구성되는 명령들을 포함한다. 컴퓨터로 하여금, 출력을 생성하기 위해 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키게 하도록 구성되는 명령들은, 컴퓨터로 하여금, 선택된 치환에 기초하여 일 세트의 역 치환들로부터 역 치환을 선택하게 하도록 구성되는 명령들을 포함한다. 암호 알고리즘은 AES(Advanced Encryption Standard) 알고리즘이고, 여기서, 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은 AES 알고리즘의 제 1 라운드를 포함하고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 AES 알고리즘의 제 2 라운드를 포함하거나, 또는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은 AES 알고리즘의 마지막 라운드 바로 앞의 라운드를 포함하고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 AES 알고리즘의 최종 라운드를 포함한다.

[0016] [0011] 본 개시내용에 따른, 데이터를 암호화하기 위한 회로는, 치환된 중간 데이터를 생성하기 위해 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환시키도록 구성되는 제 1 세트의 컴포넌트들 - 제 1 중간 데이터는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들에 의해 출력됨 -, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키를 미리결정된 치환에 따라 치환시키도록 구성되는 제 2 세트의 컴포넌트들, 제 2 중간 데이터를 생성하기 위해 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들을 치환된 중간 데이터에 적용하도록 구성되는 제 3 세트의 컴포넌트들 - 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함 -, 및 출력을 생성하기 위해, 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터를 치환시키도록 구성되는 제 4 세트의 컴포넌트들을 포함한다.

[0017] [0012] 그러한 회로의 구현들은 다음의 특성들 중 하나 또는 그 초과를 포함할 수 있다. 제 5 세트의 컴포넌트들은, 제 1 중간 데이터를 생성하기 위해, 암호화될 데이터에 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들을 적용하도록 구성된다. 제 6 세트의 컴포넌트들은, 일 세트의 치환들로부터 치환을 선택하도록 구성되며, 여기서, 치환된 중간 데이터를 생성하기 위해 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환시키는 것은, 선택된 치환을 사용하여 제 1 중간 데이터의 순서를 치환시키는 것을 포함한다. 제 6 세트의 컴포넌트들은 추가로, 난수 시드 값을 생성하고 그리고 난수 시드 값에 기초하여 일 세트의 치환들로부터 치환을 선택하도록 구성된다. 제 6 세트의 컴포넌트들은 추가로, 미리결정된 패턴에 기초하여 일 세트의 치환들로부터 치환을 선택하도록 구성된다. 제 4 세트의 컴포넌트들은, 선택된 치환에 기초하여 일 세트의 역 치환들로부터 역 치환을 선택하도록 구성된다. 암호 알고리즘은 AES(Advanced Encryption Standard) 알고리즘이고, 여기서, 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은 AES 알고리즘의 제 1 라운드를 포함하고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 AES 알고리즘의 제 2 라운드를 포함하거나, 또는 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은 AES 알고리즘의 마지막 라운드 바로 앞의 라운드를 포함하고 그

리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 AES 알고리즘의 최종 라운드를 포함한다.

도면의 간단한 설명

[0018] [0013] 도 1은, 암호 알고리즘에 대한 전력 분석 공격을 수행하는데 사용될 수 있는 예시적인 프로세스를 예시한다.

[0014] 도 2는, 암호 알고리즘에 대한 전력 분석 공격의 성공 가능성을 감소시키기 위해 사용될 수 있는 대책들의 비교를 제공하는 예시이다.

[0015] 도 3은, 본원에 개시되는 기술들에 따른 수정된 AES 암호 알고리즘과 종래의 AES 암호 알고리즘의 라운드의 비교를 제공하는 예시이다.

[0016] 도 4는, 본원에 개시되는 기술들을 이용하는 수정된 AES-192 구현과 종래의 AES-192 구현의 라운드들 간의 비교를 예시한다.

[0017] 도 5a는, 종래의 AES-128 알고리즘을 구현하는데 사용될 수 있는 회로의 기능적 도면이다.

[0018] 도 5b는, AES-128 알고리즘 내에 랜덤화를 도입시키기 위해 알고리즘 변환 기술을 사용하는 수정된 AES-128 알고리즘을 구현하기 위해 사용될 수 있는 회로의 기능적 도면이다.

[0019] 도 5c는, AES-128 알고리즘 내에 랜덤화를 도입시키기 위해 알고리즘 랜덤화 기술을 사용하는 수정된 AES-128 알고리즘을 구현하기 위해 사용될 수 있는 회로의 기능적 도면이다.

[0020] 도 6은, 본원에 개시되는 기술들을 구현하기 위해 사용될 수 있는 모바일 디바이스(600)의 블록도이다.

[0021] 도 7은, 도 6에 도시된 메모리의 기능 모듈들을 예시하는, 도 6에 예시된 모바일 디바이스의 기능 블록도이다.

[0022] 도 8은, 본원에 개시되는 암호화 기술들을 구현하기 위해 사용될 수 있는, 데이터를 암호화하기 위한 프로세스의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0019] [0023] 본원에 개시되는 기술들은, 암호 알고리즘들에 대한 사이드-채널 공격들을 방지하는 것을 돕기 위해 사용될 수 있다. 예를 들어, 본원에 개시되는 기술들은, 암호 알고리즘들에 대한 전력 분석 및/또는 EM 공격들을 방지하는 것을 도울 수 있고, 또한, 암호 알고리즘들에 대한 다른 타입들의 사이드-채널 공격들에 대해 보호들을 제공할 수 있다. 본원에 개시되는 기술들은, 암호 알고리즘들에 대한 사이드-채널 공격들을 훨씬 더 어렵게 만들 수 있는 랜덤화를 암호 알고리즘 내에 도입시키기 위해 사용될 수 있다. 본원에 개시되는 기술들의 예들은, AES(Advanced Encryption Standard) 알고리즘들을 사용하는 예들을 사용하여 예시되어 있다. 그러나, 본원에 개시되는 기술들은 또한, 다른 타입들의 암호 알고리즘들에도 또한 적용될 수 있다. 본원에서의 기술들은, 하드웨어-기반, 소프트웨어-기반, 또는 이들의 결합에 대한 암호 알고리즘 구현에 대해 사용될 수 있다.

[0020] [0024] 도 2는, 암호 알고리즘에 대한 전력 분석 공격의 성공 가능성을 감소시키기 위해 사용될 수 있는 대책들의 비교를 제공하는 예시이다. 대책들은 2개의 카테고리들, 즉 (1) 하이딩(hiding) 기술들, 및 (2) 마스킹(masking) 기술들로 분할될 수 있다. 하이딩 기술들에서, 암호 알고리즘들에 상이한 입력들이 제공되는 경우라 하더라도 암호 알고리즘을 구현하는 디지털 회로의 전력 소모를 대략적으로 동일하게 유지하기 위한 회로 레벨 설계 기술들이 적용될 수 있다. 마스킹 기술들에서, 암호 알고리즘들은, 데이터에 대해 알고리즘들이 동작하고 있는 동안 랜덤 마스크(random mask)를 사용하여 데이터를 마스킹함으로써 전력 소모를 랜덤화하고 그리고 연산이 완료된 이후 마스크를 제거하도록 설계된다. 본원에 개시되는 기술들은, 암호화 알고리즘이 실행되고 있는 동안 전력 소모를 랜덤화하여, 공격자가 암호화 알고리즘을 해독하기 위해 사이드-채널 공격을 통해 수집되는 데이터를 분석하는 것을 훨씬 더 어렵게 하는 것을 돕는 마스킹 기술들의 변형들이다.

[0021] [0025] 오리지널(original) 암호 알고리즘(205)의 흐름도는, 입력 값 a가 암호 함수 f에 제공되어 암호 함수가 암호화된 버전의 입력 값 a(도 1에서 f(a)로서 지칭됨)를 출력하는 것을 예시한다. 오리지널 암호 알고리즘(205)은 일반적인 암호 알고리즘을 표현하며, AES 또는 임의의 다른 특정한 암호 기술로 제한되지 않는다. 오리지널 암호 알고리즘(205)은, 전력 분석 공격들, EM 공격들, 또는 다른 타입들의 사이드-채널 공격들을 방지하기 위한 어떠한 단계들도 취하지 않는다. 따라서, 오리지널 암호 알고리즘(205)은, 암호 알고리즘과 연관된 중

간 데이터, 알고리즘과 연관된 키들, 및/또는 공격자가 암호 알고리즘을 해독하는데 사용할 수 있는 다른 정보를 유출시킬 수 있는 사이드-채널 공격들에 취약할 수 있다.

[0022] [0026] 마스킹 암호 알고리즘(210)에 의해 마스킹 기술이 예시된다. 마스킹 암호 알고리즘(210)은, 마스킹 및 언마스킹(unmasking) 단계들을 포함하는, 오리지널 암호 알고리즘(205)의 수정된 버전이다. 마스킹 암호 알고리즘(210)은, 암호 알고리즘에 의한 전력 소모를 랜덤화하여, 암호 알고리즘에 대한 전력 분석 및 EM 공격들을 저지(thwart)하려 시도할 수 있다. 마스킹 암호 알고리즘(210)에서, 마스크 값 m을 사용하는 마스킹 동작이 입력 값 a에 적용되어, 마스킹된 입력 값 a_m을 생성한다. 마스킹된 입력 값 a_m은 그 후, 마스킹된 버전의 암호 함수 fm에 제공된다. 마스킹된 버전의 암호 함수 f_m으로부터의 출력은 그 후, 오리지널 암호 알고리즘(205)에서 획득되는 f(a) 값을 획득하기 위해 언마스킹 동작을 이용하여 언마스킹된다. 마스킹 암호 알고리즘(210)은, 암호 프로세싱과 연관된 전력 소모가 랜덤화되게 하기 위해, 오리지널 암호 함수가 마스킹된 값들로 작업하도록 수정되는 것을 요구한다.

[0023] [0027] 도 2는 또한, 전력 분석 공격, EM 공격, 또는 암호 알고리즘에 대한 다른 타입들의 사이드-채널 공격을 훨씬 더 어렵게 하도록 암호 알고리즘 내에 랜덤화를 도입시키기 위해 사용될 수 있는, 본원에 개시되는 2개의 기술들을 예시한다. 제 1 기술은 알고리즘 변환 기술이고, 제 2 기술은 알고리즘 랜덤화 기술이다. 기술들 둘 모두는, 암호 함수가 마스킹 암호 알고리즘(210)에서와 같이 수정되는 것을 요구하지 않으면서 암호 알고리즘의 하나 또는 그 초과의 스테이지들에 랜덤화를 부가하기 위해 사용될 수 있다.

[0024] [0028] 변환 알고리즘(215)은, 입력 값이 암호 함수 f에 의해 동작되기 이전에, 입력 값을 치환시키는 변환 함수 P를 적용한다. 치환은, 암호 함수 f에 제공되는 입력 값의 바이트들을 재순서화(reorder)한다. 암호 함수는 라운드 레벨 또는 스테이지 레벨 불변성(invariance)을 나타내며, 이는, 입력의 바이트들의 순서가 변환 함수 P에 따라 치환될 수 있고, 암호 함수 f의 출력에 영향을 주지 않으면서 암호 함수 f에 입력될 수 있다는 것을 의미한다. 암호 함수 f의 출력의 바이트들의 순서는 변환 함수 P의 적용으로 인해 치환될 것이다. 그러나, 변환 함수 P의 역인 역 치환 함수 P^{-1}이, 암호 함수의 치환된 출력의 바이트들을 오리지널 암호 알고리즘(205)의 출력에 매칭하도록 재순서화한다.

[0025] [0029] 랜덤화 알고리즘(220)은, 암호 알고리즘이 실행될 때마다 입력 값에 동일한 치환 함수를 적용하는 것이 아니라 다수의 치환 함수들로부터 하나를 선택함으로써, 변환 알고리즘(215)에 비해 부가적인 보호를 제공한다. 랜덤화 알고리즘(220)은, 입력 값 a의 바이트들의 순서를 치환할 수 있는 2개 또는 그 초과의 변환 함수들로부터 선택하도록 구성된다. 도 2에 예시된 예에서, 어느 변환 함수를 입력 값 a에 적용할 것인지의 선택은, 랜덤 시드 값을 사용하여 결정된다. 랜덤 시드 값은 그 후, 복수의 역 치환 함수들로부터 치환 함수에 대응하는 역 치환 함수를 선택하기 위해 사용된다. 어느 변환 함수가 입력 값 a에 적용될 것인지를 선택하기 위해 다른 기술들이 또한 사용될 수 있다. 예를 들어, 어느 변환 함수가 입력 값 a에 적용될 것인지를 선택하기 위해 랜덤 시드 값 대신 라운드 로빈(round robin) 또는 다른 선택 방식이 사용될 수 있다. 몇몇 구현들에서, 어느 변환 함수가 적용될 것인지를 결정하기 위해, 하나 또는 그 초과의 고정 선택 패턴들이 구현될 수 있고, 랜덤 시드 대신 사용될 수 있다.

[0026] [0030] 도 3은, 본원에 개시되는 기술들에 따른 수정된 AES 암호 알고리즘과 종래의 AES 암호 알고리즘의 라운드의 비교를 제공하는 예시이다. AES 암호 알고리즘은 라운드 레벨 불변성을 나타내며, 이는, AES 알고리즘에 부가적인 랜덤화를 부가하기 위해 입력 데이터의 바이트들의 순서가 변환 함수를 사용하여 치환될 수 있다는 것을 의미한다. 도 3의 좌측 열은 종래의 AES 암호 알고리즘의 라운드의 입력들 및 출력들을 예시하고, 우측 열은 본 개시내용에 따른 수정된 AES 암호 알고리즘의 라운드의 입력들 및 출력들을 예시한다. 수정된 AES 기술은, 도 2에 예시된 변환 알고리즘 또는 랜덤화 알고리즘 기술들 중 어느 하나를 사용하여 구현될 수 있다. 변환 알고리즘 기술이 적용되는 변환에서, 입력 값들에 치환을 적용하는 변환 알고리즘은 미리결정될 것이고, 치환은 암호 알고리즘의 하나 또는 그 초과의 라운드들에 선택적으로 적용될 수 있다. 랜덤화 알고리즘 기술이 적용되면, 입력 값들에 치환을 적용하는 변환 알고리즘은, 각각이 상이한 패턴으로 입력 값들의 바이트들을 치환시키는 다수의 변환 알고리즘들 중의 하나로부터 선택될 것이거나, 몇몇 예시들에서는, 어떠한 치환도 적용되지 않을 수 있다. 또한, 상이한 변환 알고리즘이 암호 알고리즘의 상이한 라운드들에 적용될 수 있다.

[0027] [0031] 종래의 AES 암호 알고리즘을 표현하는 좌측 열에서, 종래의 AES 알고리즘에 대한 입력 값들은, 암호화 알고리즘이 적용될 16 바이트의 입력 데이터를 포함한다. 이러한 예에서 데이터는 4 x 4 매트릭스에 의해 표현된다. AES 암호화 알고리즘들은, 쇼트 키(short key)를 다수의 별개의 라운드 키(round key)들로 확장시키기

위해 사용될 수 있는 기술인 Rijndael의 키 스케줄을 사용하여 메인 암호 키(cipher key)로부터 도출되는 별개의 키를 각각의 라운드에 대해 요구한다. 따라서, 라운드에 대한 적절한 키는 AES 세션에 대해 사용되고 있는 메인 암호 키로부터 생성될 수 있거나, 또는 키는 이미 생성되었을 수 있고, 메모리로부터 액세스될 수 있다.

[0028] [0032] 본원에 개시된 기술들을 사용하는 수정된 AES 암호 알고리즘을 표현하는 우측 열에서, 라운드와 연관된 서브키(subkey) 및 입력 값들 둘 모두가 변환 함수에 따라 치환된다. 변환 함수는, 입력 데이터 내의 바이트들을 치환시키고, 또한, AES 암호 함수의 라운드를 수행하기에 앞서 도 3에 도시된 AES 라운드에서 적용될 키에 대해 등가의 치환을 수행한다. AES 암호 알고리즘은 적어도 이러한 라운드에 대해 불변이기 때문에, 치환 함수가 AES 암호 알고리즘과 함께 사용되게 하기 위해 AES 암호 알고리즘에 대해 어떠한 변경들도 행해질 필요가 없다. 우측 열에서 예시된, 변환 기술이 적용된 AES 라운드의 출력의 바이트들의 순서는, 도 3의 좌측 열에서 예시된 종래의 AES 암호화 라운드의 출력의 바이트들의 순서와 상이할 것이다. 그러나, 변환 기술이 적용된 AES 라운드의 출력의 바이트들은, AES 암호 알고리즘의 라운드가 수행되기 이전에 입력 데이터에 적용된 치환의 역 치환을 사용하여 재순서화될 수 있다. 변환 기술이 적용된 출력 데이터에 역 치환을 적용한 이후, 변환 기술이 적용된 출력 데이터는, 도 3의 좌측 열에서 예시된 종래의 AES 라운드의 라운드 출력에 매칭할 것이다. 라운드에 앞서 입력 데이터의 바이트들을 치환시키는 것은 라운드에 랜덤화를 도입시키며, 이는, 공격자가 암호화 알고리즘을 해독하기 위해 전력 분석 또는 EM 공격들을 사용하는 것을 더 어렵게 할 수 있다.

[0029] [0033] 도 4는, 본원에 개시되는 기술들을 이용하는 수정된 AES-192 구현과 종래의 AES-192 구현의 라운드들 간의 비교를 예시한다. 도 4에 예시된 예에서, 제 9 및 제 10 라운드들의 부분들은 제 10 AES 라운드를 보호하도록 수정된다. 그러나, 본원에 예시된 기술은, AES 알고리즘의 임의의 라운드를 보호하도록 사용될 수 있다. 더욱이, 본원에서 이용되는 변환 기술은, 다른 버전의 AES 알고리즘, 이를테면 AES-192 및 AES-256, 및/또는 다른 암호 기술들에 또한 적용될 수 있다. AES-128 알고리즘은 128 비트의 키 길이를 사용하고, AES-192 알고리즘은 192 비트의 키 길이를 사용하며, AES-256 알고리즘은 256 비트의 키 길이를 사용한다. 도 4에 예시된 예가 본원에서 개시되는 기술들을 AES-192 알고리즘에 적용하지만, 본원에서 설명되는 기술들은 또한, 상이한 사이즈의 비트 길이들을 갖는 키들을 사용하고 그리고/또는 알고리즘에 대한 다른 변동들을 갖는 다른 AES 알고리즘들에 적용될 수 있다.

[0030] [0034] 종래의 AES-192 구현 및 수정된 AES-192 구현 둘 모두에 대해, 라운드 8로부터의 출력은 A이고 그리고 라운드 9의 키 입력은 K9이다. 종래의 AES-192 구현에서, 라운드 9로부터의 출력은 값 B이고, 라운드 10의 키 입력은 키 K10이며, 라운드 10으로부터의 출력은 값 C이다. 수정된 AES-192 구현에서, 알고리즘의 처음 8개 라운드들은 종래의 AES-192 구현과 동일한 방식으로 수행된다. 그러나, 라운드 9 출력은 변환 함수를 사용하여 치환되며, 치환된 출력은 P(B)이다. 라운드 10의 키 K10은 또한 라운드 9의 출력에 적용되는 치환 함수와 동일한 치환 함수를 사용하여 치환된다. 라운드 10은, 치환된 데이터 입력 매트릭스 P(B) 및 치환된 키 P(K10)를 사용하여 수행된다. 라운드 10의 출력은 $P^{-1}(C)$이다. 출력은 그 후, 라운드 9의 출력에 적용되는 치환 함수의 역 치환을 사용하여 역 치환된다. 라운드 10의 출력에 역 치환을 적용하는 것의 결과는, 종래의 AES-192 구현의 라운드 10이 생성한 것과 동일한 암호문(ciphertext) 출력인 암호문 C를 생성한다.

[0031] **예시적인 하드웨어**

[0032] [0035] 도 5a, 도 5b, 및 도 5c는, 본원에 개시되는 기술을 구현하는데 사용될 수 있는 회로들을 예시하는 기능 블록도들이다. 도 5a는, 종래의 AES-128 알고리즘을 구현하는데 사용될 수 있는 회로의 기능적 도면이다. 도 5b는, AES-128 알고리즘 내에 랜덤화를 도입시키기 위한 알고리즘 변환 기술을 사용하는 수정된 AES-128 알고리즘을 구현하기 위해 사용될 수 있는 회로의 기능적 도면이다. 도 5c는, AES-128 알고리즘 내에 랜덤화를 도입시키기 위한 알고리즘 랜덤화 기술을 사용하는 수정된 AES-128 알고리즘을 구현하기 위해 사용될 수 있는 회로의 기능적 도면이다. 도 5b 및 도 5c에 예시되는 회로들은, 도 8에 예시되는 프로세스들을 구현하는데 사용될 수 있다. 도 5b 및 도 5c에 예시된 예시적인 실시예들이 수정된 버전의 AES-128 알고리즘에 관한 것이지만, 다른 버전의 AES 암호 알고리즘 및/또는 다른 암호 알고리즘들을 구현하는 회로들에 대해 유사한 수정들이 이루어질 수 있다.

[0033] [0036] 도 5a는, 종래의 AES-128 알고리즘의 라운드를 구현하는데 사용될 수 있는 회로를 예시한다. 회로는, 암호화될 평문 메시지 및 암호 키(이로부터, 각각의 라운드와 연관되는 라운드 키들이 도출될 수 있음)를 수신하도록 구성된다. 회로는, AES 암호 알고리즘의 각각의 라운드에 포함되는 SubBytes, ShiftRows, 및 MixColumns 단계들을 표현하는 기능 블록들을 포함한다. AES-128 알고리즘은 10개의 라운드들을 포함하고, 다음 라운드에 대한 적절한 키는, AES-128 알고리즘의 SubBytes, ShiftRows, 및 MixColumns 단계들을 표현하는

기능 블록들로 루프 백(loop back)되기 이전에 현재 라운드의 완료 시에 선택될 것이다.

[0034] [0037] 도 5b는, AES-128 알고리즘 내에 랜덤화를 도입시키기 위한 알고리즘 변환 기술을 사용하는 수정된 AES-128 알고리즘을 구현하기 위해 사용될 수 있는 회로의 기능적 도면이다. 도 5a에 예시된 예와 유사하게, 회로는, 암호화될 평문 메시지 및 암호 키(이로부터, 각각의 라운드와 연관되는 라운드 키들이 도출될 수 있음)를 수신하도록 구성된다. 그러나, 도 5b에 예시된 예시적인 회로는, AES 라운드의 단계들에 의해 사용되는 입력 데이터의 순서를 치환하는데 사용될 수 있는, 알고리즘 변환 기술을 지원하는 부가적인 컴포넌트들을 포함한다. 도 5b에 예시된 예에서, 회로는, 도 5a에 예시된 종래의 AES-128 라운드를 구현하는 회로에서 포함되지 않은 변환 함수 블록(505) 및 멀티플렉서(510)를 포함한다. 도 5b에 예시된 회로에서, 변환 함수가 적용되어 MixColumns 단계들 이전에 데이터의 바이트들의 순서가 치환된다. 그러나, 다른 구현들에서, 변환 함수는 AES 라운드의 SubBytes 단계 이전에 또는 ShiftRows 단계 이전에 적용될 수 있다. 더욱이, 변환 함수 블록(505) 및 멀티플렉서(510)의 배치는, 상이한 암호 알고리즘이 회로에 의해 구현되는 경우, 다를 수 있다. ShiftRows 단계 기능 블록으로부터의 출력은, 변환 함수에 의해 구현되는 미리결정된 치환에 따라 ShiftRows 단계 기능 블록으로부터의 출력을 치환시키는 변환 함수 블록(505)으로 공급된다. 변환 함수 블록(505)은 변환 함수 블록(505)에 의해 수신되는 입력 데이터의 바이트들의 순서를 변경하는 치환을 적용한다. 치환된 데이터는 그 후, 멀티플렉서(510)로 출력된다. 멀티플렉서(510)는 그 후, ShiftRows 단계 기능 블록으로부터의 오리지널 출력과 변환 함수 블록(505)에 의해 출력되는 치환된 데이터 사이에서 선택할 수 있다. 멀티플렉서(510)로 하여금 ShiftRows 단계 기능 블록으로부터의 오리지널 출력 또는 변환 함수 블록(505)에 의해 출력되는 치환된 데이터 중 어느 하나를 선택하게 하기 위한 선택 신호가 멀티플렉서(510)에 제공될 수 있다. 따라서, 회로는, 변환 함수가 특정 라운드에 적용되었는지 여부 또는 그 패턴이 특정 라운드에 적용된 것인지를 공격자가 인지하지 않을 것이기 때문에, 각각의 라운드에서의 변환 함수의 사용을 인에이블링(enable) 또는 디스에이블링(disable)하도록 구성됨으로써 변환 함수에 따라 전력 분석 또는 EM 공격을 더 어렵게 할 수 있다.

[0035] [0038] 회로는 또한, 역 변환 함수 블록(515) 및 멀티플렉서(520)를 포함한다. 역 변환 함수 블록(515)은, MixColumns 단계 기능 블록의 출력을 수신하고, MixColumns 단계 기능 블록의 출력에 역 치환을 적용한다. 역 변환 함수는, 역 변환 함수 블록(515)에 의해 수신되는 입력의 바이트들을 변환 함수 블록(505)에 의해 치환이 적용되기 이전의 바이트들의 순서로 재순서화하는 역 치환을 적용한다. 따라서, 도 5b에 예시된 회로로부터의 특정 라운드에서의 출력은, 도 5a에 예시된 종래의 AES-128 알고리즘 구현의 대응하는 라운드로부터 획득될 출력 값과 동일한 출력 값일 것이다. 라운드 동안 도입되는 랜덤화는, 암호화 알고리즘에 대해 어떠한 변경들도 요구하지 않으면서 사이드-채널 공격을 더 어렵게 할 수 있다.

[0036] [0039] 도 5c는, AES-128 알고리즘 내에 랜덤화를 도입시키기 위한 알고리즘 랜덤화 기술을 사용하는 수정된 AES-128 알고리즘을 구현하기 위해 사용될 수 있는 회로의 기능적 도면이다. 도 5a 및 도 5b에 예시된 예와 유사하게, 회로는, 암호화될 평문 메시지 및 암호 키(이로부터, 각각의 라운드와 연관되는 라운드 키들이 도출될 수 있음)를 수신하도록 구성된다. 도 5c에 예시된 회로는 알고리즘 랜덤화의 예를 제공한다. 회로는, ShiftRows 단계 기능 블록의 출력을 수신하도록 구성되는 다수의 변환 함수 블록들(555)을 포함한다. 변환 함수 블록들(555) 각각은, 그 변환 함수 블록에 의해 수신되는 입력 데이터의 바이트들의 순서에 상이한 치환을 적용한다. 치환된 데이터는 그 후, 멀티플렉서(560)로 출력된다. 멀티플렉서(560)는 그 후, ShiftRows 단계 기능 블록으로부터의 오리지널 출력과 변환 함수 블록들(555) 중 하나에 의해 출력되는 치환된 데이터 사이에서 선택할 수 있다. 몇몇 구현들에서, 랜덤 시드 값(575)이 생성되어, 어느 입력을 멀티플렉서(560)가 선택하는지를 결정하는 선택 값으로서 멀티플렉서(560)에 제공될 수 있다. 다른 기술들이 또한 선택 값을 결정하는데 사용될 수 있다. 예를 들어, 몇몇 구현들에서, 회로는, 어느 입력을 멀티플렉서(560)가 선택하는지를 결정하는 하나 또는 그 초과의 미리결정된 패턴들로부터 선택하도록 구성될 수 있다.

[0037] [0040] 도 5c에 예시된 회로는 또한, 다수의 역 변환 함수 블록들(565) 및 멀티플렉서(570)를 포함한다. 역 변환 함수 블록들(565)은, MixColumns 단계 기능 블록의 출력을 수신하고, MixColumns 단계 기능 블록의 출력에 역 치환을 적용한다. 역 변환 함수 블록들(565) 각각은 변환 함수 블록들(555) 중 하나에 대응하고, 대응하는 변환 함수 블록들(555)의 역 치환을 구현한다. 역 변환 함수는, 역 변환 함수 블록(565)에 의해 수신되는 입력의 바이트들을 변환 함수 블록(555)에 의해 치환이 적용되기 이전의 바이트들의 순서로 재순서화하는 역 치환을 적용한다. 따라서, 도 5c에 예시된 회로로부터의 특정 라운드에서의 출력은 또한, 도 5a에 예시된 종래의 AES-128 알고리즘 구현의 대응하는 라운드로부터 획득될 출력 값과 동일한 출력 값일 것이다. 라운드 동안 도입되는 랜덤화는, 암호화 알고리즘에 대해 어떠한 변경들도 요구하지 않으면서 성공적인 사이드-채널 공격을 더 어렵게 할 수 있다. 더욱이, 다수의 가능한 치환들의 부가는, 그 라운드에서 데이터에 적용된 임의의 치환이 있

는지를 잠재적 공격자가 인지하지 않을 것이므로, 부가적인 보호를 제공한다.

[0038] [0041] 도 6은, 본원에 개시되는 기술들을 구현하기 위해 사용될 수 있는 모바일 디바이스(600)의 블록도이다. 도 8에 예시된 프로세스를 적어도 부분적으로 구현하는데 모바일 디바이스(600)가 사용될 수 있다. 도 6에 예시된 예시적인 디바이스가 모바일 디바이스이지만, 도 8에 예시되는 프로세스는 또한, 다른 타입들의 컴퓨팅 디바이스들, 이를테면, 서버, 데스크톱 컴퓨터 시스템, 또는 프로세서-판독가능 프로세서-실행가능 소프트웨어 코드를 실행할 수 있는 프로세서를 포함하는 다른 디바이스에서 구현될 수 있다.

[0039] [0042] 모바일 디바이스(600)는, 버스(601)에 의해 서로 연결되는, 범용 프로세서(610), 디지털 신호 프로세서(DSP)(620), 무선 인터페이스(625), GNSS 인터페이스(665), 및 비-일시적인 메모리(660)를 포함하는 컴퓨터 시스템을 포함한다. 모바일 디바이스(600)의 다른 구현들은, 도 6의 예시적인 구현에 예시되지 않은 부가적인 엘리먼트들을 포함할 수 있고 그리고/또는 도 6에 예시된 예시적인 실시예에 예시된 엘리먼트들 전부를 포함하지는 않을 수 있다. 예를 들어, 모바일 디바이스(600)의 몇몇 구현들은 GNSS 인터페이스(665)를 포함하지 않을 수 있다.

[0040] [0043] 무선 인터페이스(625)는, 무선 수신기, 송신기, 트랜시버, 및/또는 모바일 디바이스(600)가 WWAN, WLAN, 및/또는 다른 무선 통신 프로토콜들을 사용하여 데이터를 전송 및/또는 수신하는 것을 가능하게 하는 다른 엘리먼트들을 포함할 수 있다. 무선 인터페이스(625)는, 다수의 무선 통신 표준들을 사용하여 무선 신호들을 송신 및 수신하는 것이 가능한 하나 또는 그 초과의 멀티-모드 모뎀들을 포함할 수 있다. 무선 인터페이스(625)는, 무선 통신 프로토콜들을 사용하여 통신하도록 구성되는 디바이스로/로부터 통신들을 전송 및 수신하기 위한 안테나(634)에 라인(632)에 의해 연결된다. 도 6에 예시된 모바일 디바이스(600)가 단일 무선 인터페이스(625) 및 단일 안테나(634)를 포함하지만, 모바일 디바이스(600)의 다른 구현들은 다수의 무선 인터페이스들(625) 및/또는 다수의 안테나들(634)을 포함할 수 있다.

[0041] [0044] 글로벌 내비게이션 위성 시스템(GNSS; Global Navigation Satellite System) 인터페이스(665)는, 무선 수신기 및/또는 모바일 디바이스(600)가 하나 또는 그 초과의 GNSS 시스템들과 연관된 송신기들로부터 신호들을 수신하는 것을 가능하게 하는 다른 엘리먼트들을 포함할 수 있다. GNSS 인터페이스(665)는, GNSS 송신기들로부터 신호들을 수신하기 위한 안테나(674)에 라인(672)에 의해 연결된다. 모바일 디바이스(600)는, 모바일 디바이스(600)의 포지션을 결정하기 위해, 위성들과 연관된 위성들 및 GNSS 시스템들과 연관된 다른 송신기들로부터 수신되는 신호들을 사용하도록 구성될 수 있다. 모바일 디바이스(600)는 또한, 모바일 디바이스(600)의 포지션을 결정하기 위해, 지상 무선 송신기들로부터 수신되는 신호들과 함께, GNSS 위성들 및 GNSS 시스템들과 연관된 다른 송신기들로부터 수신되는 신호들을 사용하도록 구성될 수 있다.

[0042] [0045] DSP(620)는, 무선 인터페이스(625) 및/또는 GNSS 인터페이스(665)로부터 수신되는 신호들을 프로세싱하도록 구성될 수 있고, 메모리(660)에 저장된 프로세서-판독가능, 프로세서-실행가능 소프트웨어 코드로서 구현되는 하나 또는 그 초과의 모듈들과 함께 또는 그들에 대한 신호들을 프로세싱하도록 구성될 수 있고 그리고/또는 프로세서(610)와 함께 신호들을 프로세싱하도록 구성될 수 있다.

[0043] [0046] 프로세서(610)는, 지능형 디바이스, 예컨대 Intel® Corporation 또는 AMD®에 의해 만들어진 것들과 같은 개인용 컴퓨터 중앙 프로세싱 유닛(CPU), 마이크로제어기, 주문형 집적회로(ASIC) 등일 수 있다. 메모리(660)는, 랜덤 액세스 메모리(RAM), 판독-전용 메모리(ROM), 또는 이들의 결합을 포함할 수 있는 비-일시적인 저장 디바이스이다. 메모리(660)는, (본 설명이 소프트웨어가 기능(들)을 수행하는 것으로 읽힐 수 있지만) 본원에 설명되는 기능들을 수행하도록 프로세서(610)를 제어하기 위한 명령들을 포함하는 프로세서-판독가능, 프로세서-실행가능 소프트웨어 코드를 저장할 수 있다. 소프트웨어는, 네트워크 연결을 통해 다운로드되고 디스크로부터 업로드되는 식에 의해 메모리(660) 상에 로딩될 수 있다. 추가로, 소프트웨어는 직접 실행가능하지 않을 수 있는데, 예를 들어, 실행 이전에 컴파일링(compiling)을 요구할 수 있다.

[0044] [0047] 메모리(660) 내의 소프트웨어는, 무선 송신기들, 무선 기지국들, 다른 모바일 디바이스들, 및/또는 무선 통신을 위해 구성되는 다른 디바이스로부터 데이터를 수신하고 그리고/또는 그들에 데이터를 전송하는 것을 구현하는 것을 비롯하여, 다양한 동작들을 프로세서(610)가 수행할 수 있게 하도록 구성된다.

[0045] [0048] 도 7은, 도 6에 도시된 메모리(660)의 기능 모듈들을 예시하는, 도 6에 예시된 모바일 디바이스(600)의 기능 블록도이다. 예를 들어, 모바일 디바이스(600)는, 암호화 모듈(762) 및 데이터 액세스 모듈(768)을 포함할 수 있다. 모바일 디바이스(600)는 또한, 모바일 디바이스(600)에 다른 기능성을 제공하는 하나 또는 그 초과의 부가적인 기능 모듈들을 포함할 수 있다. 도 6 및 도 7에 예시되는 모바일 디바이스(600)는, 도 8에 예시

되는 프로세스를 구현하는데 사용될 수 있다.

[0046] [0049] 암호화 모듈(762)은, 본원에 개시되는 알고리즘 변환 및/또는 알고리즘 랜덤화 기술들에 따라 구성 데이터를 암호화하도록 구성될 수 있다. 암호화 모듈(762)은, 데이터를 암호화하는데 사용될 수 있는 하나 또는 그 초과의 암호화 알고리즘들을 구현하도록 구성될 수 있다. 암호화 모듈(762)은, 모바일 디바이스(600) 상의 하나 또는 그 초과의 애플리케이션들에 대한 데이터를 암호화하도록 구성될 수 있다. 예를 들어, 암호화 모듈(762)은, 데이터에 대한 비인가된 액세스를 방지하기 위해, 모바일 디바이스(600) 상에서 동작하는 애플리케이션으로부터 수신되는 데이터를 암호화하도록 구성될 수 있다. 암호화 모듈(762)은, 데이터 액세스 모듈(768)에 암호화된 데이터를 제공함으로써 메모리(660)에 암호화된 데이터를 저장하도록 구성될 수 있다. 암호화 모듈(762)은 또한, 모바일 디바이스(600) 상에서 동작하는 애플리케이션들로부터 수신되는 데이터를 복호화(decrypt)하도록 구성될 수 있다. 예를 들어, 모바일 디바이스 상에서 구동하는 이메일 애플리케이션은, 암호화된 첨부물(attachment)을 갖는 이메일을 다운로드할 수 있고, 이메일 애플리케이션은, 첨부물을 복호화하는데 필요한 키 또는 키들이 암호화 모듈(762)에 대해 이용가능하면 암호화된 첨부물을 복호화하도록 구성될 수 있다.

[0047] [0050] 암호화 모듈(762)은, 암호화 모듈(762)에 의해 구현되는 암호화 알고리즘들의 하나 또는 그 초과의 스테이지에 의해 사용될 수 있는 하나 또는 그 초과의 키들에 액세스하도록 구성될 수 있다. 암호화 모듈(762)은, 모바일 디바이스(600)의 메모리(660)의 보호된 영역 또는 액세스가 제한되는 다른 메모리에 키들을 저장하도록 구성될 수 있다. 암호화 모듈(762)은, 데이터 액세스 모듈(768)을 통해 하나 또는 그 초과의 키들에 액세스하도록 구성될 수 있다. 암호화 모듈(762)은, 데이터를 암호화 및/또는 복호화하기 위해 키들을 사용하도록 구성될 수 있다.

[0048] [0051] 데이터 액세스 모듈(768)은, 메모리(660) 및/또는 모바일 디바이스(600)와 연관된 다른 데이터 저장 디바이스들에 데이터를 저장하도록 구성될 수 있다. 데이터 액세스 모듈(768)은 또한, 메모리(660) 및/또는 모바일 디바이스(600)와 연관된 다른 데이터 저장 디바이스들 내의 데이터에 액세스하도록 구성될 수 있다. 데이터 액세스 모듈(768)은, 모바일 디바이스(600)의 다른 모듈들 및/또는 컴포넌트들로부터 요청들을 수신하고, 메모리(660) 및/또는 모바일 디바이스(600)와 연관된 다른 데이터 자장 디바이스들에 데이터를 저장하고 그리고/또는 저장된 데이터에 액세스하도록 구성될 수 있다.

[0049] 예시적인 구현들

[0050] [0052] 도 8은, 본원에 개시되는 암호화 기술들을 구현하기 위해 사용될 수 있는, 데이터를 암호화하기 위한 프로세스의 흐름도이다. 도 8에 예시된 프로세스는, 하드웨어로, 소프트웨어로, 또는 이들의 결합으로 구현될 수 있다. 예를 들어, 도 8에 예시된 프로세스는, 도 6 및 도 7에 예시된 모바일 디바이스(600)에 의해 구현될 수 있다. 도 8에 예시된 프로세스는 또한, 도 5에 예시된 예시적인 회로와 같은 회로에서 구현될 수 있다.

[0051] [0053] 제 1 중간 데이터를 생성하기 위해, 암호화될 데이터에 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들이 적용될 수 있다(스테이지 805). 적용될 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은, 알고리즘의 어느 스테이지가 보호를 제공받는지, 그리고 암호 알고리즘의 특정 구현에 얼마나 많은 스테이지들이 포함되는지에 의존할 수 있다. 예를 들어, 암호 알고리즘이 AES 암호 알고리즘인 구현들에서, 수행되는 라운드들의 개수는 그 특정 구현에 의해 사용되는 키 길이에 의존한다. AES-128 알고리즘은 128 비트의 키 길이를 사용하고, AES-192 알고리즘은 192 비트의 키 길이를 사용하며, AES-256 알고리즘은 256 비트의 키 길이를 사용한다. 키 사이즈는, 실행될 라운드들의 개수에 영향을 미친다. 예를 들어, AES-128 구현들은 통상적으로 10개의 라운드들을 포함하고, AES-192 구현들은 통상적으로 12개의 라운드들을 포함하며, AES-256 구현들은 통상적으로 14개의 라운드들을 포함한다.

[0052] [0054] AES 알고리즘들에 대한 공격의 하나의 공통적인 포인트는 제 1 라운드와 제 2 라운드 사이이다. AES 알고리즘들에 대한 공격의 다른 공통적인 포인트는 알고리즘의 마지막 라운드 바로 앞의 라운드와 마지막 라운드 사이이다. 예를 들어, AES-128 알고리즘에 대한 공격의 공통 포인트는 제 9 및 제 10 라운드들에서이고, AES-192 알고리즘에 대한 공격의 공통 포인트는 제 11 및 제 12 라운드들에서이며, AES-256 알고리즘에 대한 공격의 공통 포인트는 제 13 및 제 14 라운드들에서이다. 따라서, 암호 알고리즘의 하나 또는 그 초과의 제 1 스테이지들은 AES 알고리즘들 중 하나의 제 1 라운드일 수 있다. 암호 알고리즘들의 하나 또는 그 초과의 제 1 스테이지들은 또한, AES 알고리즘 중 하나의 마지막 라운드 바로 앞의 라운드, 이를테면, AES-128 알고리즘의 제 9 라운드, AES-192 알고리즘의 제 10 라운드, 및 AES-256 알고리즘의 제 13 라운드를 지칭할 수 있다. 마지막 라운드 바로 앞의 라운드의 넘버는 다른 암호 알고리즘들에 대해 다를 수 있다.

[0053] [0055] 공격자는, 디바이스의 전기 활동을 관측하는 것으로 위에 설명된 것과 같은 전력 분석 공격을 사용할 수 있는데, 여기서, 암호 알고리즘은 전력 트레이스들을 현상(develop)하기 위한 일 시간 기간에 걸쳐 구현된다. 전력 트레이스들은, 알고리즘에 의해 사용되는 암호 키들을 추출하기 위해 사용될 수 있다.

[0054] [0056] 치환된 중간 데이터를 생성하기 위해, 제 1 중간 데이터의 순서가 미리결정된 치환에 따라 치환될 수 있다(스테이지 810). 제 1 중간 데이터의 바이트들의 순서는, 미리결정된 치환 패턴에 따라 치환되어 치환된 중간 데이터를 생성할 수 있다. 몇몇 구현들에서, 미리결정된 치환들은, 도 2에 예시된 알고리즘 변환 기술(214)의 것과 유사한 알고리즘 변환 기술에 따라 수행될 수 있다. 알고리즘 변환 기술에서, 변환 함수는, 암호화 알고리즘이 구현되는 하드웨어 및/또는 소프트웨어서 구현될 수 있다. 변환 함수는, 일단 암호 알고리즘의 다음 스테이지 또는 스테이지들이 입력 데이터에 적용되었으면, 역 치환 함수를 사용하여 반전(reverse)될 수 있는 미리결정된 패턴에 따라 입력 데이터의 바이트들을 재순서화할 수 있다. 도 3은, AES 암호화 알고리즘의 라운드의 입력 데이터에 적용되는 그러한 변환 함수의 예를 예시한다. 16 바이트의 입력 데이터는 4 x 4 매트릭스의 데이터로서 표현된다. 변환 함수는, 입력 데이터의 바이트들이 더 이상 이전 AES 라운드로부터의 출력될 때 그들이 있었던 순서와 동일한 순서로 로케이팅되지 않도록, 입력 데이터의 바이트들의 순서를 치환시킨다. 다른 구현들에서, 알고리즘 랜덤화 기술이 도 2에 예시된 랜덤화 알고리즘(220)의 기술과 유사하게 이용될 수 있다. 알고리즘 랜덤화 기술에서, 입력 데이터를 치환하기 위해 사용되는 변환 함수는 정적이 아니며, 다수의 미리결정된 치환 함수로부터 선택될 수 있다. 예를 들어, 알고리즘 랜덤화 기술을 특정 구현은, 각각이 입력 데이터를 상이한 패턴으로 치환시키는 5개의 변환 함수들의 세트를 포함할 수 있다. 알고리즘 랜덤화 기술은 또한, 5개의 미리결정된 변환 함수들 중 입력 데이터에 적용할 하나를 선택하기 위한 수단을 구현할 수 있다. 변환 알고리즘들 중 입력 데이터를 치환시키기 위한 하나를 랜덤으로 선택하는 것은, 암호 알고리즘에 대한 전력 분석 및 다른 타입들의 공격들의 사용되고 있는 키들을 알아내려 하는 시도를 훨씬 더 어렵게 할 수 있다. 몇몇 구현들에서, 랜덤 시드 값이 생성되어 입력 데이터에 적용하기 위한 변환 함수를 선택하는 멀티플렉서에 공급될 수 있다. 위에 논의된 알고리즘 변환 및 알고리즘 랜덤화 기술들 둘 모두에 대해, 사용되는 치환 패턴 또는 패턴들은 가급적 비밀로 유지되어야 한다. 어느 변환 함수가 적용될 것인지를 선택하기 위해 다른 기술들이 또한 사용될 수 있다. 예를 들어, 어느 변환 함수가 적용될 것인지를 선택하기 위해 랜덤 시드 값 대신 라운드 로빈 또는 다른 선택 방식이 사용될 수 있다. 몇몇 구현들에서, 어느 변환 함수가 적용될 것인지를 결정하기 위해, 하나 또는 그 초과의 고정 선택 패턴들이 구현될 수 있고, 랜덤 시드 대신 사용될 수 있다.

[0055] [0057] 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 사용될 키가 미리결정된 치환에 따라 치환될 수 있다(스테이지 815). 제 1 중간 데이터 상에서 동작하도록 암호 알고리즘에 의해 사용될 키는 또한, 입력 값들에 적용된 변환과 동일한 변환 알고리즘 따라 치환될 수 있다. 도 3에 예시된 예는, 입력 데이터와 동일한 변환 알고리즘을 사용하여 치환되는 키의 예를 제공한다. 키는 암호 알고리즘의 다수의 스테이지들에 의해 사용될 수 있거나, 또는 암호 알고리즘의 하나의 스테이지에 대해 특정적일 수 있다. 예를 들어, AES 알고리즘들은, 쇼트 키를 다수의 별개의 라운드 키들로 확장시키기 위해 사용될 수 있는 기술인 Rijndael의 키 스케줄을 사용하여 메인 암호 키로부터 도출되는 별개의 키를 각각의 라운드에 대해 요구한다.

[0056] [0058] 제 2 중간 데이터를 생성하기 위해, 치환된 중간 데이터에 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들이 적용될 수 있다(스테이지 820). 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 스테이지(815)에서 생성된 치환된 키를 사용할 수 있다. 도 3에 예시된 예는 AES 라운드의 단계들이 치환된 중간 데이터에 적용되는 예를 제공하며, 여기서, 도 3의 예는 AES 알고리즘의 이전 라운드에 의해 출력되는 입력 값들의 4 x 4 매트릭스이다. 스테이지(815)로부터의 치환된 키가 또한 AES 라운드에서 사용된다. 본원에 개시된 기술들이 다른 암호 알고리즘들에 적용되는 경우, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용되는 키의 타입 및/또는 입력 값들은 도 3에서 제공되는 AES 예에서 사용되는 것들과 상이할 수 있다.

[0057] [0059] 출력을 생성하기 위해, 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터가 치환될 수 있다(스테이지 825). 제 2 중간 데이터는, 수정되지 않은 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들의 출력이 생성했을 것과 동일한 출력을 생성하기 위해, 스테이지들(810 및 820)에 적용되는 치환의 역 치환을 사용하여 치환될 수 있다. 예를 들어, 다시 도 3의 예를 참조하면, 본원에 개시된 수정된 암호 기술 대신 종래의 AES 암호 알고리즘이 적용되게 했을 때 바이트들이 가졌을 순서와 동일한 순서로 바이트들이 있도록, 입력 데이터를 치환시키기 위해 적용된 변환 함수와 연관된 역 치환 및 그 라운드와 연관된 서브키가 치환된 중간 데이터에 적용되어, 치환된 중간 데이터의 바이트들을 재순서화한다. 따라서, 본원에 개시되는 기술들은, 스테이지 또는 라운드들 각각에서 암호 알고리즘에 의해 수행되는 동작들이 이들 기술들을 이용하여 동작하도록 수정되는 것을 요구하지 않는다. 본 기술들은, 전력 분석 공격들, EM 공격들, 및/또는 다른 타입들의 사이드-채널 공격들에 의

해 타겟팅될 수 있는, 암호 알고리즘의 하나 또는 그 초과의 스테이지들 또는 라운드들에서 적용될 수 있다.

[0058] [0060] 스테이지(825)로부터의 출력은 암호 알고리즘의 하나 또는 그 초과의 후속 스테이지들에 대한 입력으로서 사용될 수 있다. 예를 들어, 암호 알고리즘이 AES 알고리즘이고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들이 AES 알고리즘 중 하나의 라운드 2에 대응하는 경우, 라운드 2로부터의 출력은 암호문이 알고리즘에 의해 출력되기 이전에 수 개의 부가적인 라운드들에 의해 프로세싱될 것이다. 암호 알고리즘이 AES 알고리즘이고 그리고 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들이 AES 알고리즘 중 하나의 마지막 라운드에 대응하는 경우, 마지막 라운드로부터의 출력은, 암호문이 알고리즘에 의해 출력되기 이전에 수 개의 부가적인 라운드들에 의해 프로세싱될 것이다.

[0059] [0061] 본원에 설명된 방법들은 애플리케이션에 의존하여 다양한 수단에 의해 구현될 수 있다. 예를 들어, 이들 방법들은 하드웨어, 펌웨어, 소프트웨어, 또는 이들의 임의의 결합에서 구현될 수 있다. 하드웨어 구현에 대해, 프로세싱 유닛들은 하나 또는 그 초과의 주문형 집적 회로(ASIC)들, 디지털 신호 프로세서(DSP)들, 디지털 신호 프로세싱 디바이스(DSPD; digital signal processing device)들, 프로그래밍가능 로직 디바이스(PLD; programmable logic device)들, 필드 프로그래밍가능 게이트 어레이(FPGA; field programmable gate array)들, 프로세서들, 제어기들, 마이크로-제어기들, 마이크로프로세서들, 전자 디바이스들, 본원에 설명된 기능들을 수행하도록 설계된 다른 전자 유닛들, 또는 이들의 결합 내에 구현될 수 있다.

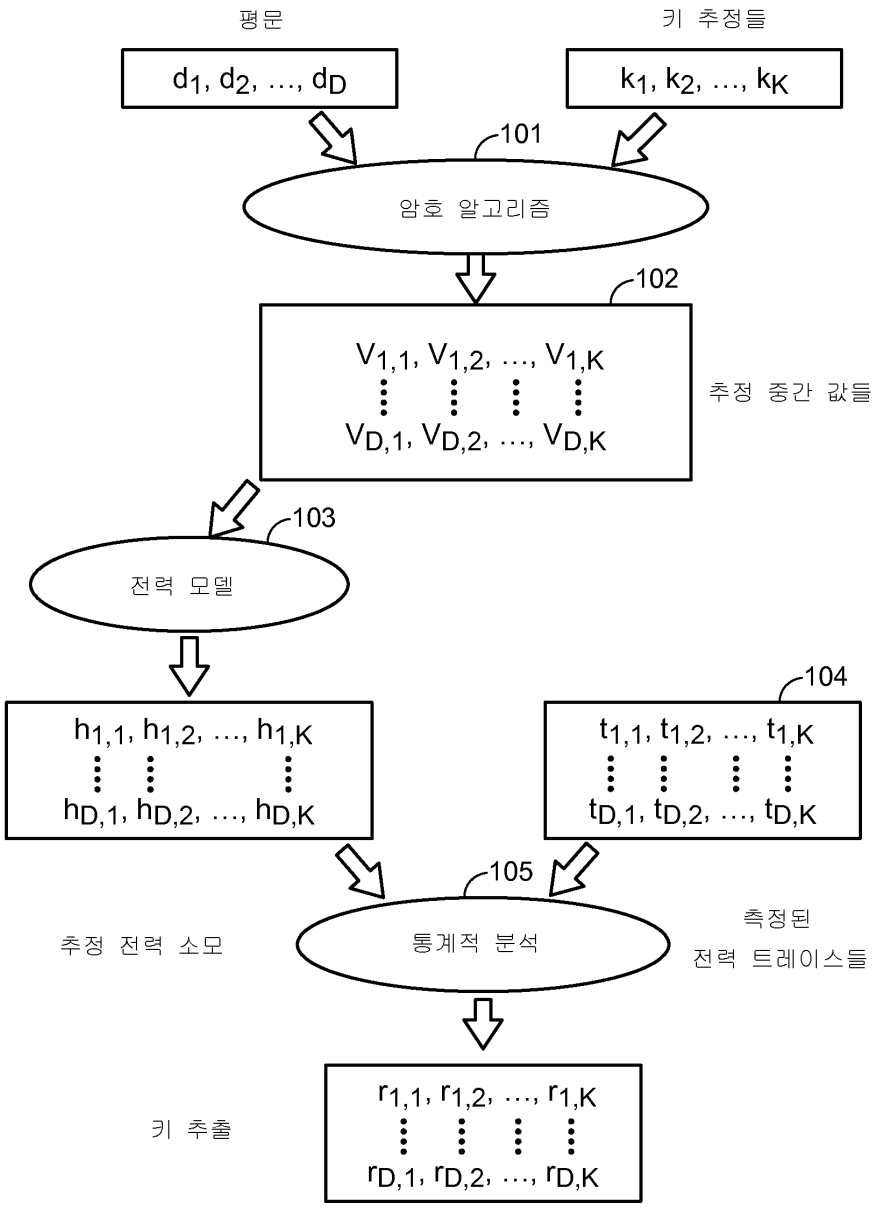
[0060] [0062] 펌웨어 및/또는 소프트웨어 구현에 대해, 방법들은 본원에 설명된 기능들을 수행하는 모듈들(예를 들어, 절차들, 함수들 등)을 이용하여 구현될 수 있다. 명령들을 유형적으로(tangibly) 구현하는 임의의 머신-판독가능 매체는, 본원에 설명된 방법들을 구현할 시에 사용될 수 있다. 예를 들어, 소프트웨어 코드들은 메모리에 저장되고 프로세서 유닛에 의해 실행될 수 있다. 메모리는 프로세서 유닛의 내부에 또는 프로세서 유닛의 외부에 구현될 수 있다. 본원에서 사용되는 바와 같이, 용어 “메모리”는, 장기, 단기, 휘발성, 비휘발성, 또는 다른 메모리 중 임의의 타입을 지칭하며, 임의의 특정한 메모리의 타입 또는 메모리들의 개수, 또는 매체들의 타입으로 제한되는 것은 아니다. 유형의 매체들은, 랜덤 액세스 메모리, 자기 저장부, 광학 저장 매체들 등과 같은 머신 판독가능 매체들의 하나 또는 그 초과의 물리적 물품(article)들을 포함한다.

[0061] [0063] 펌웨어 및/또는 소프트웨어로 구현되면, 기능들은 컴퓨터-판독가능 매체 상에 하나 또는 그 초과의 명령들 또는 코드로서 저장될 수 있다. 예들은, 데이터 구조로 인코딩된 컴퓨터-판독가능 매체들 및 컴퓨터 프로그램으로 인코딩된 컴퓨터-판독가능 매체들을 포함한다. 컴퓨터-판독가능 매체들은 물리적 컴퓨터 저장 매체들을 포함한다. 저장 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수 있다. 제한이 아닌 예로서, 그러한 컴퓨터-판독가능 매체들은 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장부, 자기 디스크 저장 또는 다른 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 저장하는데 사용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있고; 본원에 사용된 바와 같이, 디스크(disk) 및 디스크(disc)는 컴팩트 디스크(disc)(CD), 레이저 디스크(disc), 광학 디스크(disc), 디지털 다목적 디스크(disc)(DVD), 플로피 디스크(disk) 및 Blu-ray 디스크(disc)를 포함하며, 여기서, 디스크(disk)들은 일반적으로 데이터를 자기적으로 재생하지만, 디스크(disc)들은 레이저들을 이용하여 광학적으로 데이터를 재생한다. 또한, 상기의 것들의 결합들은 컴퓨터-판독가능 매체들의 범위 내에 포함되어야 한다. 그러한 매체들은 또한 머신 판독가능할 수 있는 비-일시적인 매체들의 예들을 제공하며, 여기서, 그러한 비-일시적인 매체들로부터 판독할 수 있는 머신의 일 예는 컴퓨터들이다.

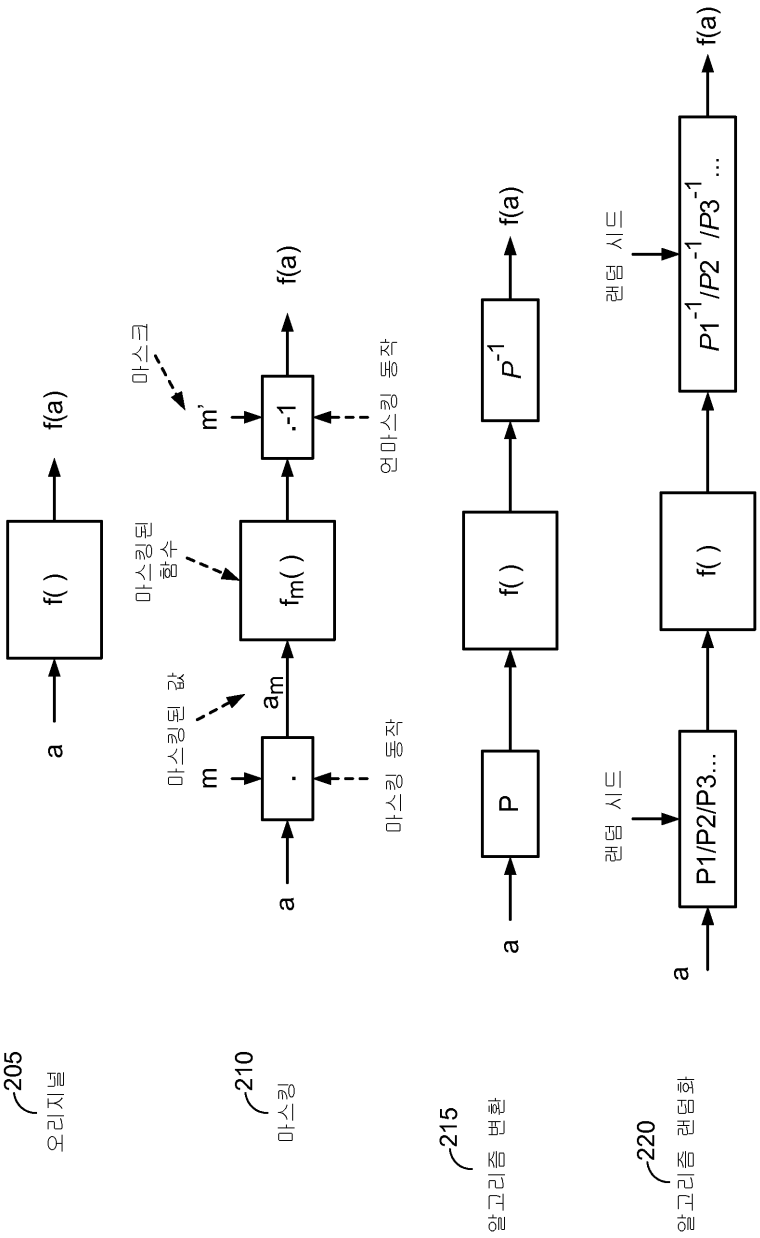
[0062] [0064] 본원에서 논의되는 일반적인 원리들은, 본 개시내용 또는 청구항들의 사상 또는 범위를 벗어나지 않으면서 다른 구현들에 적용될 수 있다.

도면

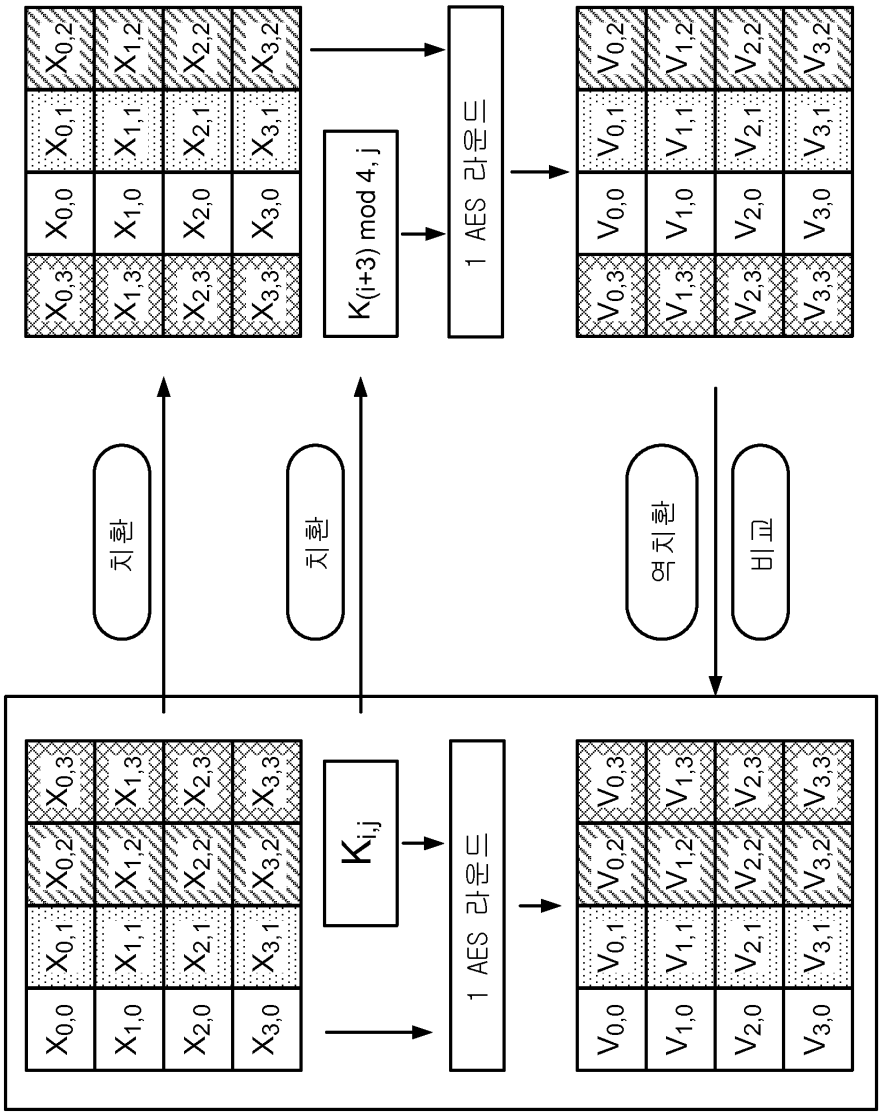
도면1


평문
키 추정들
$d_1, d_2, \ldots, d_D$
$k_1, k_2, \ldots, k_K$
101
암호 알고리즘
102
$V_{1,1}, V_{1,2}, \ldots, V_{1,K}$
$V_{D,1}, V_{D,2}, \ldots, V_{D,K}$
추정 중간 값들
103
전력 모델
$h_{1,1}, h_{1,2}, \ldots, h_{1,K}$
$h_{D,1}, h_{D,2}, \ldots, h_{D,K}$
104
$t_{1,1}, t_{1,2}, \ldots, t_{1,K}$
$t_{D,1}, t_{D,2}, \ldots, t_{D,K}$
105
추정 전력 소모
통계적 분석
측정된
전력 트레이스들
키 추출
$r_{1,1}, r_{1,2}, \ldots, r_{1,K}$
$r_{D,1}, r_{D,2}, \ldots, r_{D,K}$

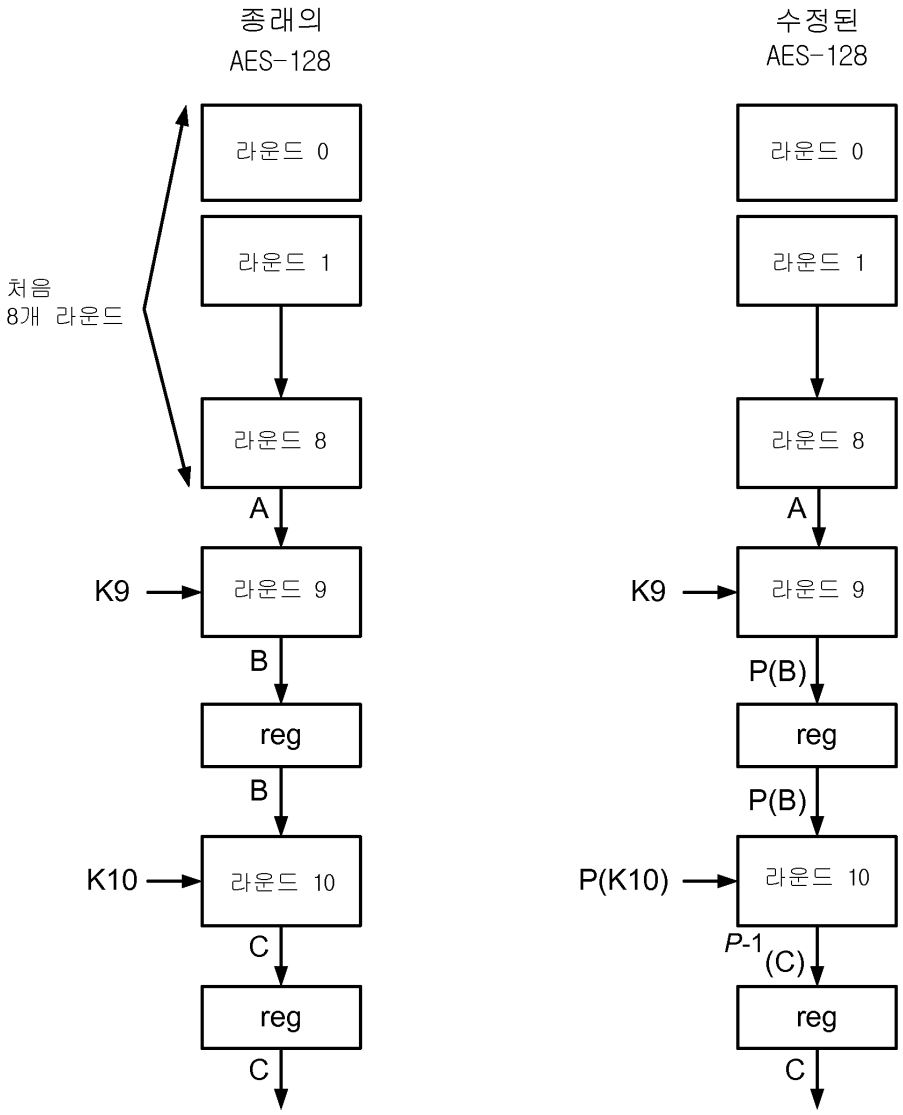
도면2


205
오리지널
a
f( )
f(a)
210
마스킹
a
m
마스킹된 값
마스킹 동작
am
fm( )
마스킹된 함수
m'
.-1
언마스킹 동작
마스크
f(a)
215
알고리즘 변환
a
P
f( )
P-1
f(a)
220
알고리즘 랜덤화
a
랜덤 시드
P1/P2/P3...
f( )
랜덤 시드
P1-1/P2-1/P3-1 ...
f(a)

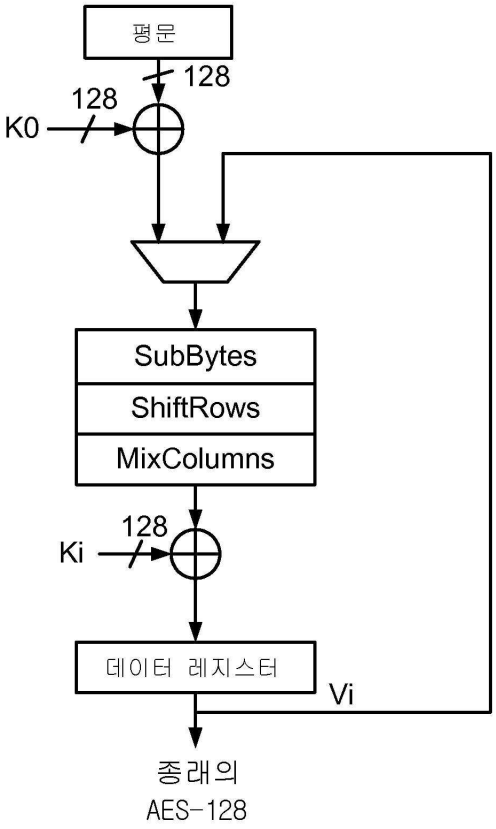
도면3



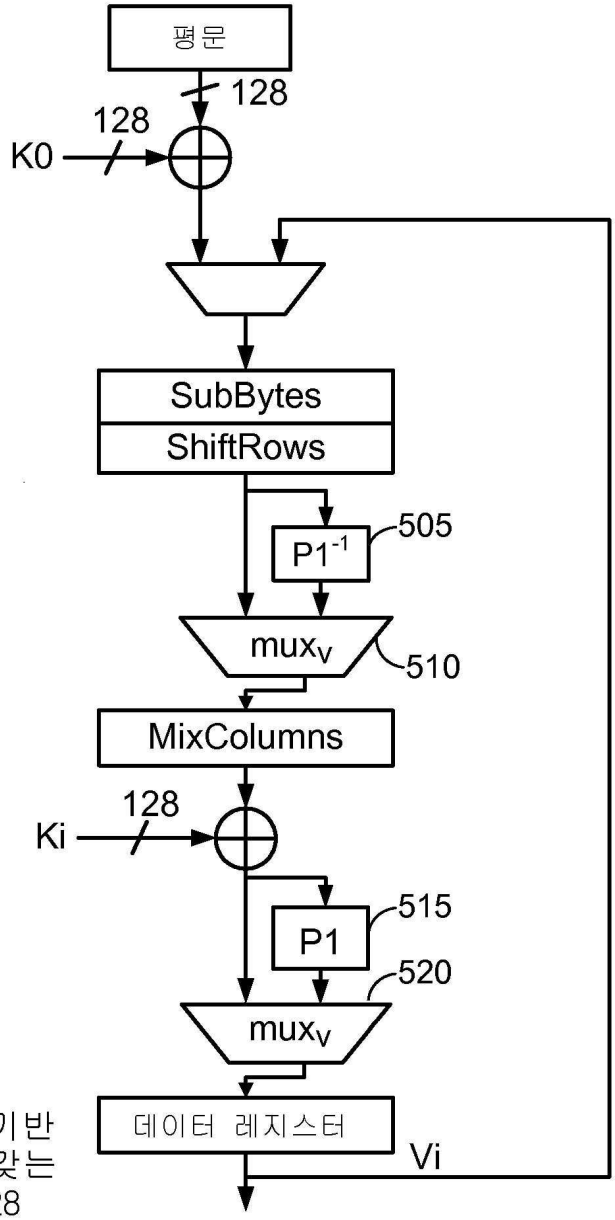
도면4


종래의
AES-128
수정된
AES-128
처음
8개 라운드
라운드 0
라운드 1
라운드 8
A
K9
라운드 9
B
reg
B
K10
라운드 10
C
reg
C
라운드 0
라운드 1
라운드 8
A
K9
라운드 9
P(B)
reg
P(B)
P(K10)
라운드 10
P-1(C)
reg
C

도면5a

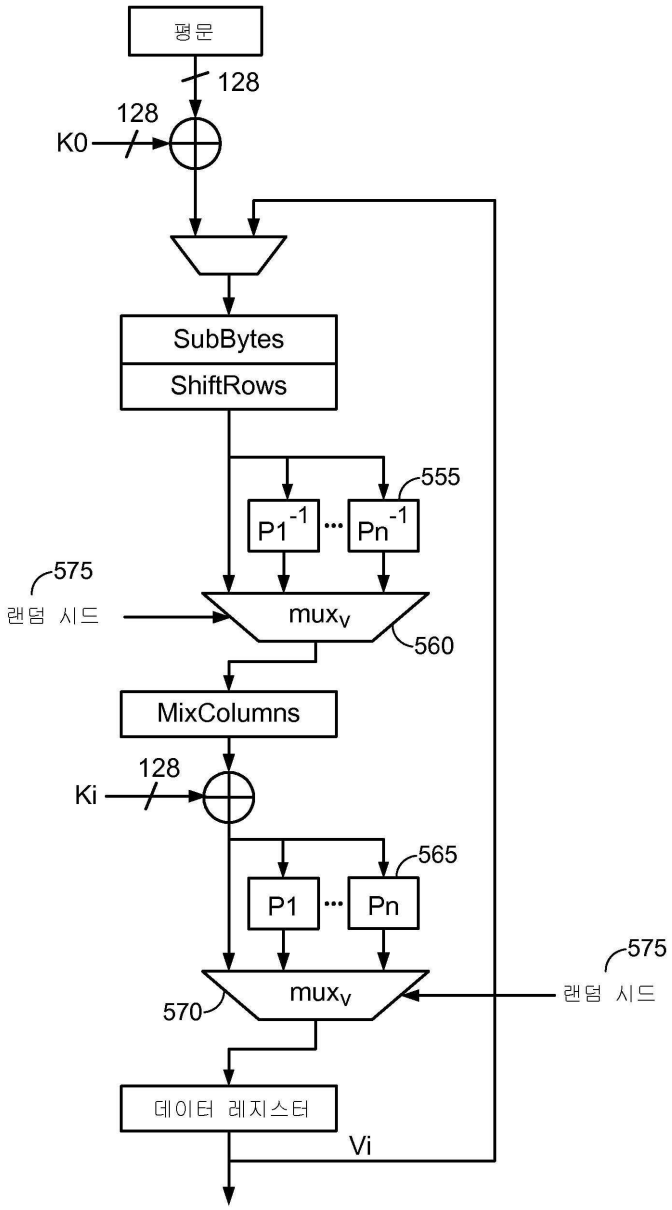

평문
128
128
K0
SubBytes
ShiftRows
MixColumns
128
Ki
데이터 레지스터
Vi
종래의
AES-128

도면5b

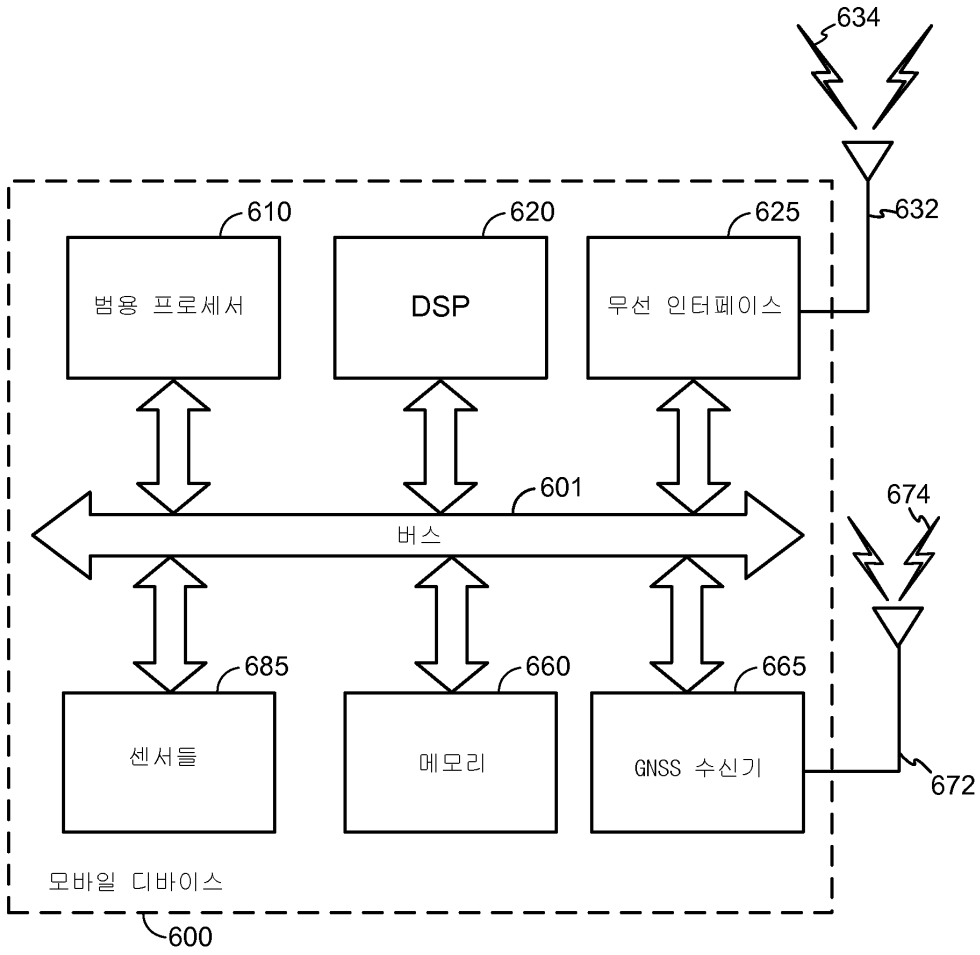


불변성-기반 대책을 갖는 AES-128

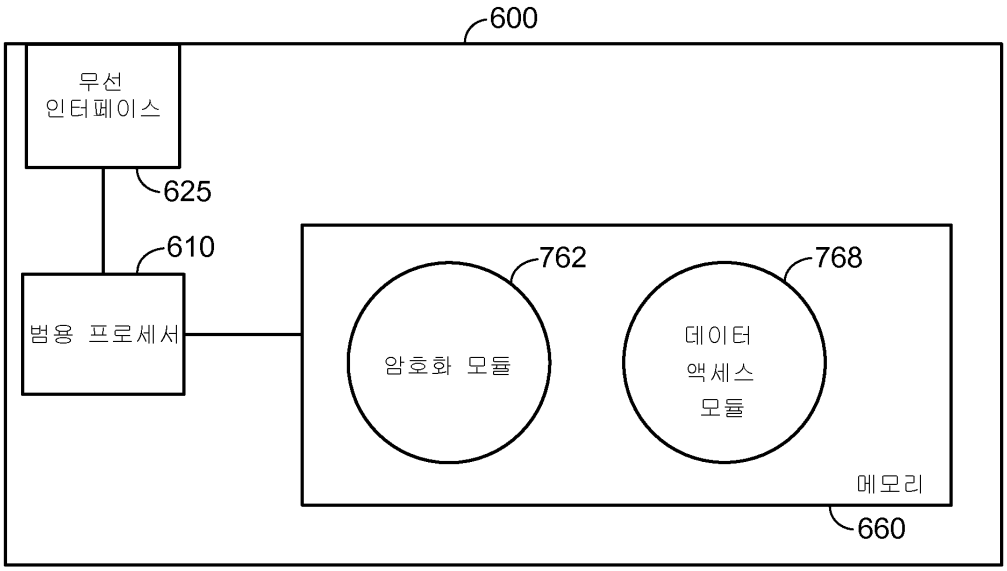
도면5c


평문
128
128
K0
SubBytes
ShiftRows
555
P1-1
Pn-1
575
랜덤 시드
muxV
560
MixColumns
128
Ki
565
P1
Pn
575
랜덤 시드
muxV
570
데이터 레지스터
Vi

도면6

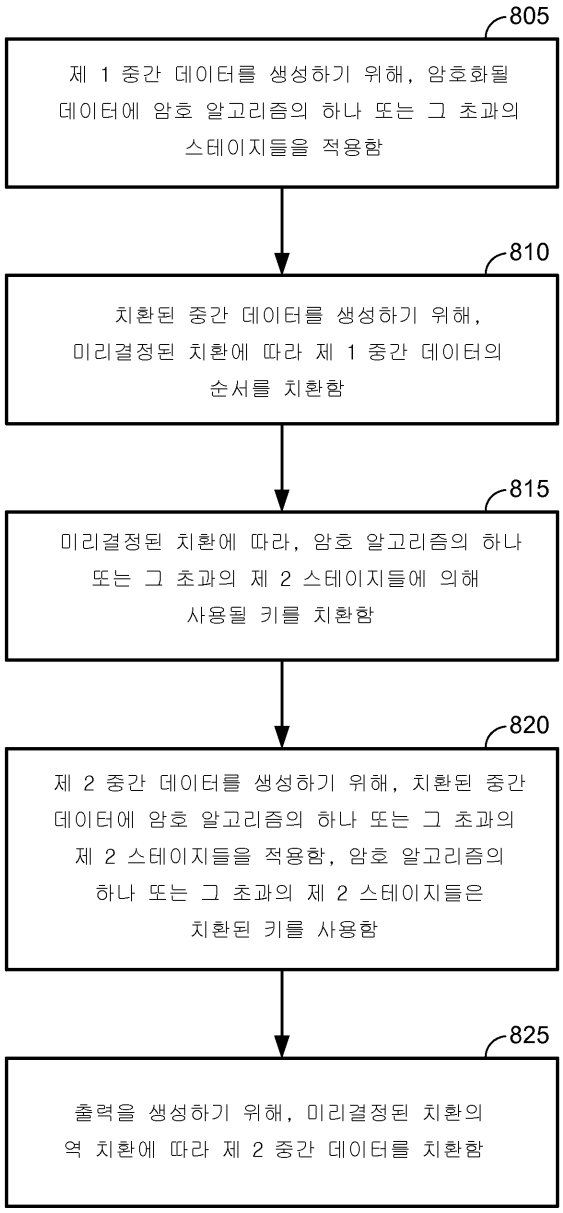


도면7



모바일 디바이스

도면8


805
제 1 중간 데이터를 생성하기 위해, 암호화될 데이터에 암호 알고리즘의 하나 또는 그 초과의 스테이지들을 적용함
810
치환된 중간 데이터를 생성하기 위해, 미리결정된 치환에 따라 제 1 중간 데이터의 순서를 치환함
815
미리결정된 치환에 따라, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들에 의해 사용될 키를 치환함
820
제 2 중간 데이터를 생성하기 위해, 치환된 중간 데이터에 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들을 적용함, 암호 알고리즘의 하나 또는 그 초과의 제 2 스테이지들은 치환된 키를 사용함
825
출력을 생성하기 위해, 미리결정된 치환의 역 치환에 따라 제 2 중간 데이터를 치환함

암호화 프로세스