(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년10월21일
(11) 등록번호 10-2168502
(24) 등록일자 2020년10월15일

(51) 국제특허분류(Int. Cl.)
*H04L 29/06* (2006.01) *G06F 7/58* (2006.01)
*H04L 9/32* (2006.01)
(52) CPC특허분류
*H04L 63/08* (2013.01)
*G06F 7/588* (2013.01)
(21) 출원번호 10-2016-7006993
(22) 출원일자(국제) 2014년08월19일
심사청구일자 2019년08월05일
(85) 번역문제출일자 2016년03월16일
(65) 공개번호 10-2016-0048114
(43) 공개일자 2016년05월03일
(86) 국제출원번호 PCT/US2014/051718
(87) 국제공개번호 WO 2015/026838
국제공개일자 2015년02월26일
(30) 우선권주장
13/975,082 2013년08월23일 미국(US)
(56) 선행기술조사문헌
JP2014002369 A

(73) 특허권자
**퀄컴 인코포레이티드**
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
**구오, 수**
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
**제이콥슨, 데이비드 엠.**
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
*(뒷면에 계속)*
(74) 대리인
**특허법인 남앤남**

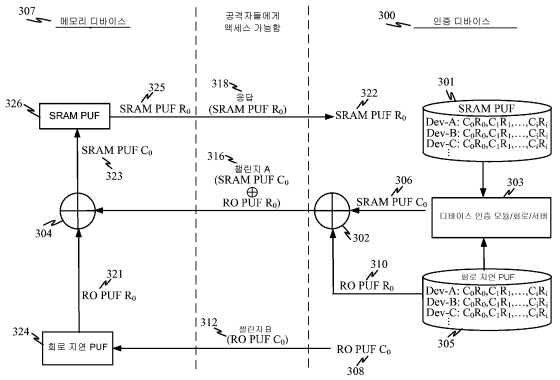
전체 청구항 수 : 총 54 항 심사관 : 문형섭

(54) 발명의 명칭 **침입 및 복제 공격들에 저항하기 위해 메모리 기반-PUF(PHYSICALLY UNCLONABLE FUNCTION)들의 동작을 마스킹하기 위한 회로 지연-기반 PUF들의 적용**

## (57) 요 약

하나의 피처는 정적 랜덤 액세스 메모리(SRAM) PUF들과 회로 지연 기반 PUF들(예를 들어, 링 오실레이터(RO) PUF들, 아비터 PUF들 등)을 결합함으로써 전자 디바이스에 대한 고유한 식별자를 생성하는 것에 관한 것이다. 회로 지연 기반 PUF들은 SRAM PUF들로의 챌린지(challenge)를 은폐하거나 및/또는 SRAM PUF로부터의 응답들을 은폐하는데 사용될 수 있고, 그에 의해, 공격자가 메모리 디바이스의 응답을 복제할 수 있게 되는 것을 막는다.

*대 표 도* - 도3



(52) CPC특허분류
*H04L 63/0884* (2013.01)
*H04L 9/3278* (2013.01)
(72) 발명자
**양, 야페이**
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
**드류, 아담 제이.**
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

**로젠베르크, 브라이언 마크**
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775

# 명 세 서

## 청구범위

### 청구항 1

전자 디바이스에 의해 동작가능한 방법으로서,

상기 전자 디바이스 내의 복수의 메모리 셀들을 이용하여 제 1 물리적 복제 불가능 기능(physically unclonable function)을 구현하는 단계;

상기 전자 디바이스 내의 복수의 회로 지연 기반 경로들을 이용하여 제 2 물리적 복제 불가능 기능을 구현하는 단계;

외부 서버로부터 챌린지(challenge)를 수신하는 단계;

(a) 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 1 챌린지를 마스킹/언마스킹(mask/unmask)하도록,

(b) 상기 챌린지와 상기 제 2 물리적 복제 불가능 기능으로부터의 제 1 응답을 결합함으로써, 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 2 챌린지를 생성하도록, 또는

(c) 상기 제 1 물리적 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록

상기 제 1 응답을 이용함으로써 상기 제 1 물리적 복제 불가능 기능에 상기 챌린지를 적용하는 단계; 및

상기 제 1 물리적 복제 불가능 기능으로부터의 제 2 응답을 상기 외부 서버에 송신하는 단계

를 포함하는,

전자 디바이스에 의해 동작가능한 방법.

### 청구항 2

제 1 항에 있어서,

상기 제 2 물리적 복제 불가능 기능으로부터의 상기 제 1 응답을 상기 외부 서버에 송신하는 단계

를 더 포함하는,

전자 디바이스에 의해 동작가능한 방법.

### 청구항 3

제 1 항에 있어서,

상기 제 1 물리적 복제 불가능 기능은 상기 챌린지에 대한 응답으로서 하나 이상의 메모리 셀들에 대한 초기화되지 않은 메모리 셀 상태들을 사용하는,

전자 디바이스에 의해 동작가능한 방법.

### 청구항 4

제 1 항에 있어서,

상기 복수의 회로 지연 기반 경로들은 링 오실레이터(ring oscillator)들이고, 그리고 상기 제 2 물리적 복제 불가능 기능은 복수의 링 오실레이터들로부터 2개의 링 오실레이터들을 선택하는 제 2 챌린지를 수신하고 그리고 상기 2개의 링 오실레이터들 사이의 주파수 차이(differential)로 응답하는,

전자 디바이스에 의해 동작가능한 방법.

### 청구항 5

삭제

**청구항 6**

제 1 항에 있어서,

상기 챌린지는 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하는,

전자 디바이스에 의해 동작가능한 방법.

**청구항 7**

제 6 항에 있어서,

상기 제 1 챌린지는 제 2 챌린지에 대해 예상된 응답에 의해 마스킹되는 챌린지인,

전자 디바이스에 의해 동작가능한 방법.

**청구항 8**

제 6 항에 있어서,

상기 제 1 챌린지는 상기 제 1 물리적 복제 불가능 기능에 의한 프로세싱 이전에, 상기 제 2 물리적 복제 불가능 기능으로부터의 상기 제 1 응답에 의해 수정되는,

전자 디바이스에 의해 동작가능한 방법.

**청구항 9**

제 1 항에 있어서,

상기 수신된 챌린지는 상기 제 1 응답을 생성하기 위해 상기 제 2 물리적 복제 불가능 기능에 의해 사용되고, 상기 제 1 응답은 그 후, 상기 제 2 응답을 생성하기 위해 상기 제 1 물리적 복제 불가능 기능에 의해 제 2 챌린지로서 사용되는,

전자 디바이스에 의해 동작가능한 방법.

**청구항 10**

제 1 항에 있어서,

상기 챌린지는 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 제 2 챌린지는 상기 제 1 물리적 복제 불가능 기능으로부터의 상기 제 2 응답을 마스킹하는데 사용되는 상기 제 1 응답을 생성하기 위해 상기 제 2 물리적 복제 불가능 기능에 의해 사용되는,

전자 디바이스에 의해 동작가능한 방법.

**청구항 11**

제 10 항에 있어서,

중간 응답을 획득하기 위해 상기 제 2 물리적 복제 불가능 기능으로부터의 상기 제 1 응답을 해싱(hashing)하는 단계;

상기 중간 응답을 사용하여 상기 제 2 응답을 마스킹하는 단계

를 더 포함하는,

전자 디바이스에 의해 동작가능한 방법.

**청구항 12**

제 1 항에 있어서,

상기 챌린지는 상기 전자 디바이스의 인증 프로세스, 상기 전자 디바이스의 식별 프로세스, 및/또는 상기 전자 디바이스 내의 키 생성 프로세스 중 적어도 하나의 부분으로서 수신되는,

전자 디바이스에 의해 동작가능한 방법.

**청구항 13**

제 1 항에 있어서,

상기 전자 디바이스는 배포 전(pre-deployment) 또는 제조 단계 동안 하나 이상의 챌린지들을 수신하고 그리고 하나 이상의 대응하는 응답들을 제공한,

전자 디바이스에 의해 동작가능한 방법.

**청구항 14**

제 1 항에 있어서,

(a) 상기 챌린지가 수신되기 이전에, 또는

(b) 상기 제 2 응답을 송신하는 것과 동시에

상기 전자 디바이스로부터 상기 외부 서버에 미리-저장된 디바이스 식별자를 송신하는 단계

를 더 포함하고,

상기 디바이스 식별자는 상기 전자 디바이스를 고유하게 식별하는,

전자 디바이스에 의해 동작가능한 방법.

**청구항 15**

전자 디바이스로서,

제 1 물리적 복제 불가능 기능으로서 역할하는 상기 전자 디바이스 내의 복수의 메모리 셀들;

제 2 물리적 복제 불가능 기능을 구현하는 상기 전자 디바이스 내의 복수의 회로 지연 기반 경로들;

외부 서버로부터 챌린지를 수신하기 위한 통신 인터페이스;

상기 통신 인터페이스, 상기 복수의 메모리 셀들, 및 상기 복수의 회로 지연 기반 경로들에 커플링되는 프로세싱 회로

를 포함하고,

상기 프로세싱 회로는:

(a) 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 1 챌린지를 마스킹/언마스킹하도록,

(b) 상기 챌린지와 상기 제 2 물리적 복제 불가능 기능으로부터의 제 1 응답을 결합함으로써, 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 2 챌린지를 생성하도록, 또는

(c) 상기 제 1 물리적 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록

상기 제 1 응답을 이용함으로써 상기 제 1 물리적 복제 불가능 기능에 상기 챌린지를 적용하도록 적응되고,

상기 통신 인터페이스는 상기 제 1 물리적 복제 불가능 기능으로부터의 제 2 응답을 상기 외부 서버에 송신하도록 적응되는,

전자 디바이스.

**청구항 16**

제 15 항에 있어서,

상기 제 2 물리적 복제 불가능 기능으로부터의 상기 제 1 응답을 상기 외부 서버에 송신하는 것

을 더 포함하는,

전자 디바이스.

**청구항 17**

제 15 항에 있어서,

상기 제 1 물리적 복제 불가능 기능은 상기 챌린지에 대한 응답으로서 하나 이상의 메모리 셀들에 대한 초기화되지 않은 메모리 셀 상태들을 사용하는,

전자 디바이스.

**청구항 18**

제 15 항에 있어서,

상기 복수의 회로 지연 기반 경로들은 링 오실레이터들이고, 그리고 상기 제 2 물리적 복제 불가능 기능은 복수의 링 오실레이터들로부터 2개의 링 오실레이터들을 선택하는 제 2 챌린지를 수신하고 그리고 상기 2개의 링 오실레이터들 사이의 주파수 차이로 응답하는,

전자 디바이스.

**청구항 19**

삭제

**청구항 20**

제 15 항에 있어서,

상기 챌린지는 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하는,

전자 디바이스.

**청구항 21**

제 20 항에 있어서,

상기 제 1 챌린지는 제 2 챌린지에 대해 예상된 응답에 의해 마스킹되는 챌린지인,

전자 디바이스.

**청구항 22**

제 20 항에 있어서,

상기 제 1 챌린지는 상기 제 1 물리적 복제 불가능 기능에 의한 프로세싱 이전에, 상기 제 2 물리적 복제 불가능 기능으로부터의 상기 제 1 응답에 의해 수정되는,

전자 디바이스.

**청구항 23**

제 15 항에 있어서,

상기 수신된 챌린지는 상기 제 1 응답을 생성하기 위해 상기 제 2 물리적 복제 불가능 기능에 의해 사용되고, 상기 제 1 응답은 그 후, 상기 제 2 응답을 생성하기 위해 상기 제 1 물리적 복제 불가능 기능에 의해 제 2 챌린지로서 사용되는,

전자 디바이스.

**청구항 24**

제 15 항에 있어서,

상기 챌린지는 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 제 2 챌린지는 상기 제 1 물리적 복제 불가능 기능으로부터의 상기 제 2 응답을 마스킹하는데 사용되는 상기 제 1 응답을 생성하기 위해 상기 제 2 물리적 복제 불가능 기능에 의해 사용되는,

전자 디바이스.

**청구항 25**

제 15 항에 있어서,

상기 프로세싱 회로는 추가로:

중간 응답을 획득하기 위해 상기 제 2 물리적 복제 불가능 기능으로부터의 상기 제 1 응답을 해싱하고; 그리고

상기 중간 응답을 사용하여 상기 제 2 응답을 마스킹하도록

적응되는,

전자 디바이스.

**청구항 26**

제 15 항에 있어서,

상기 챌린지는 상기 전자 디바이스의 인증 프로세스, 상기 전자 디바이스의 식별 프로세스, 및/또는 상기 전자 디바이스 내의 키 생성 프로세스 중 적어도 하나의 부분으로서 수신되는,

전자 디바이스.

**청구항 27**

제 15 항에 있어서,

상기 프로세싱 회로는 추가로:

(a) 상기 챌린지가 수신되기 이전에, 또는

(b) 상기 제 2 응답의 송신과 동시에

상기 전자 디바이스로부터 상기 외부 서버에 미리-저장된 디바이스 식별자를 송신하도록

적응되고,

상기 디바이스 식별자는 상기 전자 디바이스를 고유하게 식별하는,

전자 디바이스.

**청구항 28**

전자 디바이스로서,

상기 전자 디바이스 내의 복수의 메모리 셀들을 이용하여 제 1 물리적 복제 불가능 기능을 구현하기 위한 수단;

상기 전자 디바이스 내의 복수의 회로 지연 기반 경로들을 이용하여 제 2 물리적 복제 불가능 기능을 구현하기 위한 수단;

외부 서버로부터 챌린지를 수신하기 위한 수단;

(a) 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 1 챌린지를 마스킹/언마스킹하도록,

(b) 상기 챌린지와 상기 제 2 물리적 복제 불가능 기능으로부터의 제 1 응답을 결합함으로써, 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 2 챌린지를 생성하도록, 또는

(c) 상기 제 1 물리적 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록

상기 제 1 응답을 이용함으로써 상기 제 1 물리적 복제 불가능 기능에 상기 챌린지를 적용하기 위한 수단: 및

상기 제 1 물리적 복제 불가능 기능으로부터의 제 2 응답을 상기 외부 서버에 송신하기 위한 수단

을 포함하는,

전자 디바이스.

**청구항 29**

제 28 항에 있어서,

상기 챌린지는 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하는,

전자 디바이스.

**청구항 30**

제 29 항에 있어서,

상기 제 1 챌린지는 제 2 챌린지에 대해 예상된 응답에 의해 마스킹되는 챌린지인,

전자 디바이스.

**청구항 31**

제 29 항에 있어서,

상기 제 1 챌린지는 상기 제 1 물리적 복제 불가능 기능에 의한 프로세싱 이전에, 상기 제 2 물리적 복제 불가능 기능으로부터의 상기 제 1 응답에 의해 수정되는,

전자 디바이스.

**청구항 32**

제 29 항에 있어서,

상기 수신된 챌린지는 상기 제 1 응답을 생성하기 위해 상기 제 2 물리적 복제 불가능 기능에 의해 사용되고, 상기 제 1 응답은 그 후, 상기 제 2 응답을 생성하기 위해 상기 제 1 물리적 복제 불가능 기능에 의해 제 2 챌린지로서 사용되는,

전자 디바이스.

**청구항 33**

제 28 항에 있어서,

상기 챌린지는 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 제 2 챌린지는 상기 제 1 물리적 복제 불가능 기능으로부터의 상기 제 2 응답을 마스킹하는데 사용되는 상기 제 1 응답을 생성하기 위해 상기 제 2 물리적 복제 불가능 기능에 의해 사용되는,

전자 디바이스.

**청구항 34**

하나 이상의 명령들이 저장되어 있는 비-일시적 기계-판독가능 저장 매체로서, 상기 명령들은, 전자 디바이스의 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금:

제 1 물리적 복제 불가능 기능을 구현하도록 전자 디바이스 내의 복수의 메모리 셀들을 선택하게 하고;

제 2 물리적 복제 불가능 기능을 구현하도록 상기 전자 디바이스 내의 복수의 회로 지연 기반 경로들을 선택하

게 하고;

외부 서버로부터 챌린지를 수신하게 하고;

(a) 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 1 챌린지를 마스킹/언마스킹하도록,

(b) 상기 챌린지와 상기 제 2 물리적 복제 불가능 기능으로부터의 제 1 응답을 결합함으로써, 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 2 챌린지를 생성하도록, 또는

(c) 상기 제 1 물리적 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록

상기 제 1 응답을 이용함으로써 상기 제 1 물리적 복제 불가능 기능에 상기 챌린지를 적용하게 하고; 그리고

상기 제 1 물리적 복제 불가능 기능으로부터의 제 2 응답을 상기 외부 서버에 송신하게 하는,

비-일시적 기계-판독가능 저장 매체.

**청구항 35**

인증 디바이스에 의해 동작가능한 방법으로서,

전자 디바이스와 연관된 디바이스 식별자를 수신하는 단계;

상기 전자 디바이스에 하나 이상의 챌린지들을 송신하는 단계 - 상기 하나 이상의 챌린지들은:

(a) 상기 전자 디바이스에 대한 상기 하나 이상의 챌린지들 중 적어도 하나로부터 제 1 물리적 복제 불가능 기능에 입력되는 제 1 챌린지를 마스킹/언마스킹하도록,

(b) 상기 전자 디바이스에서 제 1 응답과 챌린지를 결합함으로써, 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 2 챌린지를 생성하도록, 또는

(c) 상기 전자 디바이스에 대한 상기 제 1 물리적 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록

상기 전자 디바이스의 상기 제 1 물리적 복제 불가능 기능 및 제 2 물리적 복제 불가능 기능에 적용되도록 구성됨 - ;

상기 전자 디바이스로부터 하나 이상의 응답들을 수신하는 단계 - 상기 하나 이상의 응답들은 상기 제 1 및 제 2 물리적 복제 불가능 기능들로부터의 특성 정보를 포함함 - ;

전자 디바이스 식별자를 사용하여 상기 전자 디바이스에 특정한 미리-저장된 응답들을 식별하는 단계; 및

상기 전자 디바이스에 대한 상기 수신된 하나 이상의 응답들과 상기 미리-저장된 응답들을 비교함으로써 상기 전자 디바이스를 인증하는 단계

를 포함하는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 36**

제 35 항에 있어서,

상기 챌린지들은, 응답들이 상기 전자 디바이스로부터 이전에 획득되었던 복수의 챌린지들로부터 선택되는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 37**

제 35 항에 있어서,

상기 미리-저장된 응답들은 상기 전자 디바이스의 배포 전 스테이지 또는 제조 스테이지에서 획득된,

인증 디바이스에 의해 동작가능한 방법.

**청구항 38**

제 35 항에 있어서,

상기 디바이스 식별자는 상기 하나 이상의 챌린지들을 송신하기 이전에 수신되는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 39**

제 35 항에 있어서,

상기 디바이스 식별자는 상기 하나 이상의 응답들을 수신하는 것과 함께 수신되는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 40**

제 35 항에 있어서,

상기 챌린지는 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 41**

제 40 항에 있어서,

상기 제 1 챌린지는 상기 제 2 챌린지에 대해 예상된 응답에 의해 마스킹되는 챌린지인,

인증 디바이스에 의해 동작가능한 방법.

**청구항 42**

제 40 항에 있어서,

상기 하나 이상의 챌린지들은 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 하나 이상의 응답들은 상기 제 1 물리적 복제 불가능 기능으로부터의 제 1 응답 및 상기 제 2 물리적 복제 불가능 기능으로부터의 제 2 응답을 포함하고, 상기 제 1 응답이 상기 제 1 챌린지에 대응하는 제 1 미리-저장된 응답과 매칭하고 그리고 상기 제 2 응답이 상기 제 2 챌린지에 대응하는 제 2 미리-저장된 응답과 매칭하는 경우, 상기 전자 디바이스는 성공적으로 인증되는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 43**

제 40 항에 있어서,

상기 하나 이상의 챌린지들은 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 하나 이상의 응답들은 상기 제 1 물리적 복제 불가능 기능으로부터의 제 1 응답 및 상기 제 2 물리적 복제 불가능 기능으로부터의 제 2 응답을 포함하고, 그리고

상기 방법은:

상기 제 2 응답으로 상기 제 1 챌린지를 언마스킹함으로써 중간 챌린지를 획득하는 단계, 및 수신된 제 1 응답을 상기 중간 챌린지와 연관된 미리-저장된 응답에 대해 비교하는 단계

를 더 포함하는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 44**

제 35 항에 있어서,

상기 하나 이상의 챌린지들은 상기 제 2 물리적 복제 불가능 기능에 대한 제 1 챌린지를 포함하고, 상기 하나

이상의 응답들은 상기 제 1 물리적 복제 불가능 기능으로부터의 제 1 응답을 포함하고, 그리고

상기 방법은:

상기 제 1 챌린지에 대응하는 미리-저장된 중간 응답을 리트리브(retrieve)함으로써 중간 챌린지를 획득하는 단계, 및 수신된 제 1 응답을 상기 중간 챌린지에 대응하는 미리-저장된 중간 응답에 대해 비교하는 단계

를 더 포함하는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 45**

제 35 항에 있어서,

상기 하나 이상의 챌린지들은 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 하나 이상의 응답들은 제 1 응답을 포함하고, 그리고

상기 방법은:

상기 제 2 챌린지에 대응하는 미리-저장된 제 2 응답으로 상기 제 1 응답을 언마스킹함으로써 중간 응답을 획득하는 단계, 및 상기 중간 응답을 상기 제 1 챌린지와 연관된 미리-저장된 응답에 대해 비교하는 단계

를 더 포함하는,

인증 디바이스에 의해 동작가능한 방법.

**청구항 46**

인증 디바이스로서,

전자 디바이스와 통신하기 위한 통신 인터페이스;

상기 통신 인터페이스에 커플링되는 프로세싱 회로

를 포함하고,

상기 프로세싱 회로는:

상기 전자 디바이스와 연관된 디바이스 식별자를 수신하고;

상기 전자 디바이스에 하나 이상의 챌린지들을 송신하고 - 상기 하나 이상의 챌린지들은:

(a) 상기 전자 디바이스에 대한 상기 하나 이상의 챌린지들 중 적어도 하나로부터 제 1 물리적 복제 불가능 기능에 입력되는 제 1 챌린지를 마스킹/언마스킹하도록,

(b) 상기 전자 디바이스에서 제 1 응답과 챌린지를 결합함으로써, 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 2 챌린지를 생성하도록, 또는

(c) 상기 전자 디바이스에 대한 상기 제 1 물리적 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록

상기 전자 디바이스의 상기 제 1 물리적 복제 불가능 기능 및 제 2 물리적 복제 불가능 기능에 적용되도록 구성됨 - ;

상기 전자 디바이스로부터 하나 이상의 응답들을 수신하고 - 상기 하나 이상의 응답들은 상기 제 1 및 제 2 물리적 복제 불가능 기능들로부터의 특성 정보를 포함함 - ;

전자 디바이스 식별자를 사용하여 상기 전자 디바이스에 특정한 미리-저장된 응답들을 식별하고; 그리고

상기 전자 디바이스에 대한 상기 수신된 하나 이상의 응답들과 상기 미리-저장된 응답들을 비교함으로써 상기 전자 디바이스를 인증하도록

적응되는,

인증 디바이스.

**청구항 47**

제 46 항에 있어서,

상기 챌린지들은, 응답들이 상기 전자 디바이스로부터 이전에 획득되었던 복수의 챌린지들로부터 선택되는,

인증 디바이스.

**청구항 48**

제 46 항에 있어서,

상기 챌린지는 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하는,

인증 디바이스.

**청구항 49**

제 48 항에 있어서,

상기 제 1 챌린지는 상기 제 2 챌린지에 대해 예상된 응답에 의해 마스킹되는 챌린지인,

인증 디바이스.

**청구항 50**

제 48 항에 있어서,

상기 하나 이상의 챌린지들은 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 하나 이상의 응답들은 상기 제 1 물리적 복제 불가능 기능으로부터의 제 1 응답 및 상기 제 2 물리적 복제 불가능 기능으로부터의 제 2 응답을 포함하고, 상기 제 1 응답이 상기 제 1 챌린지에 대응하는 제 1 미리-저장된 응답과 매칭하고 그리고 상기 제 2 응답이 상기 제 2 챌린지에 대응하는 제 2 미리-저장된 응답과 매칭하는 경우, 상기 전자 디바이스는 성공적으로 인증되는,

인증 디바이스.

**청구항 51**

제 46 항에 있어서,

상기 하나 이상의 챌린지들은 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 하나 이상의 응답들은 상기 제 1 물리적 복제 불가능 기능으로부터의 제 1 응답 및 상기 제 2 물리적 복제 불가능 기능으로부터의 제 2 응답을 포함하고, 그리고

상기 프로세싱 회로는 추가로:

상기 제 2 응답으로 상기 제 1 챌린지를 언마스킹함으로써 중간 챌린지를 획득하고, 그리고 수신된 제 1 응답을 상기 중간 챌린지와 연관된 미리-저장된 응답에 대해 비교하도록

적응되는,

인증 디바이스.

**청구항 52**

제 46 항에 있어서,

상기 하나 이상의 챌린지들은 상기 제 2 물리적 복제 불가능 기능에 대한 제 1 챌린지를 포함하고, 상기 하나 이상의 응답들은 상기 제 1 물리적 복제 불가능 기능으로부터의 제 1 응답을 포함하고, 그리고

상기 프로세싱 회로는 추가로:

상기 제 1 챌린지에 대응하는 미리-저장된 중간 응답을 리트리브함으로써 중간 챌린지를 획득하고, 그

리고 수신된 제 1 응답을 상기 중간 챌린지에 대응하는 미리-저장된 중간 응답에 대해 비교하도록

적응되는,

인증 디바이스.

**청구항 53**

제 46 항에 있어서,

상기 하나 이상의 챌린지들은 상기 제 1 물리적 복제 불가능 기능에 대한 제 1 챌린지 및 상기 제 2 물리적 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 상기 하나 이상의 응답들은 제 1 응답을 포함하고, 그리고

상기 프로세싱 회로는 추가로:

상기 제 2 챌린지에 대응하는 미리-저장된 제 2 응답으로 상기 제 1 응답을 언마스킹함으로써 중간 응답을 획득하고, 그리고 상기 중간 응답을 상기 제 1 챌린지와 연관된 미리-저장된 응답에 대해 비교하도록

적응되는,

인증 디바이스.

**청구항 54**

인증 디바이스로서,

전자 디바이스와 연관된 디바이스 식별자를 수신하기 위한 수단;

상기 전자 디바이스에 하나 이상의 챌린지들을 송신하기 위한 수단 - 상기 하나 이상의 챌린지들은:

(a) 상기 전자 디바이스에 대한 상기 하나 이상의 챌린지들 중 적어도 하나로부터 제 1 물리적 복제 불가능 기능에 입력되는 제 1 챌린지를 마스킹/언마스킹하도록,

(b) 상기 전자 디바이스에서 제 1 응답과 챌린지를 결합함으로써, 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 2 챌린지를 생성하도록, 또는

(c) 상기 전자 디바이스에 대한 상기 제 1 물리적 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록

상기 전자 디바이스의 상기 제 1 물리적 복제 불가능 기능 및 제 2 물리적 복제 불가능 기능에 적용되도록 구성됨 - ;

상기 전자 디바이스로부터 하나 이상의 응답들을 수신하기 위한 수단 - 상기 하나 이상의 응답들은 상기 제 1 및 제 2 물리적 복제 불가능 기능들로부터의 특성 정보를 포함함 - ;

전자 디바이스 식별자를 사용하여 상기 전자 디바이스에 특정한 미리-저장된 응답들을 식별하기 위한 수단; 및

상기 전자 디바이스에 대한 상기 수신된 하나 이상의 응답들과 상기 미리-저장된 응답들을 비교함으로써 상기 전자 디바이스를 인증하기 위한 수단

을 포함하는,

인증 디바이스.

**청구항 55**

하나 이상의 명령들이 저장되어 있는 비-일시적 기계-판독가능 저장 매체로서, 상기 명령들은, 인증 디바이스의 적어도 하나의 프로세서에 의해 실행될 때, 상기 적어도 하나의 프로세서로 하여금:

전자 디바이스와 연관된 디바이스 식별자를 수신하게 하고;

상기 전자 디바이스에 하나 이상의 챌린지들을 송신하게 하고 - 상기 하나 이상의 챌린지들은:

(a) 상기 전자 디바이스에 대한 상기 하나 이상의 챌린지들 중 적어도 하나로부터 제 1 물리적 복제 불가능 기능에 입력되는 제 1 챌린지를 마스킹/언마스킹하도록,

(b) 상기 전자 디바이스에서 제 1 응답과 챌린지를 결합함으로써, 상기 제 1 물리적 복제 불가능 기능에 입력되는 제 2 챌린지를 생성하도록, 또는

(c) 상기 전자 디바이스에 대한 상기 제 1 물리적 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록

상기 전자 디바이스의 상기 제 1 물리적 복제 불가능 기능 및 제 2 물리적 복제 불가능 기능에 적용되도록 구성됨 - ;

상기 전자 디바이스로부터 하나 이상의 응답들을 수신하게 하고 - 상기 하나 이상의 응답들은 상기 제 1 및 제 2 물리적 복제 불가능 기능들로부터의 특성 정보를 포함함 - ;

전자 디바이스 식별자를 사용하여 상기 전자 디바이스에 특정한 미리-저장된 응답들을 식별하게 하고; 그리고

상기 전자 디바이스에 대한 상기 수신된 하나 이상의 응답들과 상기 미리-저장된 응답들을 비교함으로써 상기 전자 디바이스를 인증하게 하는,

비-일시적 기계-판독가능 저장 매체.

**청구항 56**

제 46 항에 있어서,

상기 전자 디바이스와 연관되는 응답들 및 챌린지들의 데이터베이스를 저장하는 저장 디바이스

를 더 포함하고,

상기 인증 디바이스는 상기 데이터베이스의 응답들 중 적어도 일부에 기초하여 상기 전자 디바이스를 인증하거나 또는 식별하는,

인증 디바이스.

## *발명의 설명*

### *기 술 분 야*

[0001] [0001] 본 개시는 메모리 디바이스 또는 이러한 메모리 디바이스가 통합되는 디바이스를 고유하게 식별하도록 물리적 복제 불가능 기능(physically unclonable function; PUF)들의 이용에 관한 것이다.

### *배 경 기 술*

[0002] [0002] 물리적 복제 불가능 기능(Physical Unclonable function; PUF)들은 물리적 컴포넌트의 본질적인 변동들에 기초하여 하드웨어 디바이스를 고유하게 식별하기 위한 메커니즘을 제공한다. 다수의 칩들이 제조될 때, 복잡한 반도체 제조 프로세스는 설계자의 제어를 벗어난 약간의 변동들을 도입한다. 예를 들면, 두 개의 칩들이 동일한 실리콘 웨이퍼로부터 제조되더라도, 동일하게 되도록 설계된 전기적 경로는 아마 몇 나노미터들만큼 폭에서 차이가 날 것이고; 실리콘의 표면의 미세한 차이들은 라인의 곡률에 거의 하찮은 변동들을 유도할 것이다. 이러한 고유한 특성들은 제어 불가능하고 물리적 디바이스에 대해 고유하기 때문에, 이들을 정량화하는 것은 고유한 식별자를 생성할 수 있다. 링 오실레이터 기반 PUF들, 아비터 PUF들, 및 경로 지연 분석 기반 PUF들과 같은 PUF들의 몇 가지 다른 타입들은 회로 지연들에서 실리콘 변동들의 분석 및 조사에 기초하여 제안되었다.

[0003] [0003] 하나의 PUF는 식별 "지문"을 생성하도록 정적 랜덤 액세스 메모리(SRAM)의 초기화되지 않은 파워-업 상태를 이용한다. 그러나 SRAM PUF들은 복제 공격(cloning attack)들에 취약하다.

[0004] [0004] 결과적으로, 일반적으로 복제 공격들 및 침입 공격에 저항하기 위해 현재 SRAM PUF 설계들의 보안성을 개선할 필요가 있다.

### *발명의 내용*

[0005] [0005] 복제 공격들에 저항력이 있으면서 고유하게 식별될 수 있는 전자 디바이스(예들 들어, 프로세서, 프로세싱 회로, 메모리, 프로그래밍 가능 로직 어레이, 칩, 반도체, 메모리 등)가 제공된다. 전자 디바이스는 제 1 물리적으로 복제 불가능 기능(PUF)으로서 역할하는 전자 디바이스 내의 복수의 메모리 셀들을 포함할 수 있다.

일 예에서, 제 1 물리적으로 복제 불가능 기능은 챌린지(challenge)에 대한 응답으로서 하나 이상의 메모리 셀들에 대한 초기화되지 않은 메모리 셀 상태들을 사용할 수 있다. 부가적으로, 전자 디바이스 내의 복수의 회로 지연 기반 경로들은 제 2 물리적으로 복제 불가능 기능을 구현할 수 있다. 일 예에서, 복수의 회로 지연 기반 경로들은 링 오실레이터들일 수 있고, 제 2 물리적으로 복제 불가능 기능은, 복수의 링 오실레이터들로부터 2개의 링 오실레이터들을 선택하고 2개의 링 오실레이터들 사이의 주파수 차이로 응답하는 챌린지를 수신할 수 있다.

[0006] [0006] 통신 인터페이스는 외부 서버로부터 챌린지를 수신하도록 역할을 할 수 있다. 프로세싱 회로는 통신 인터페이스, 복수의 메모리 셀들 및 복수의 회로 지연 기반 경로들에 커플링될 수 있고, 프로세싱 회로는, (a) 제 1 물리적으로 복제 불가능 기능에 입력되는 챌린지를 마스킹/언마스킹하도록, (b) 제 1 물리적 복제 불가능 기능에 입력되는 챌린지를 생성하도록, 또는 (c) 제 1 물리적으로 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록 제 2 물리적으로 복제 불가능 기능으로부터의 제 1 응답을 이용함으로써 제 1 물리적 복제 불가능 기능에 챌린지를 적용하도록 적응된다. 통신 인터페이스는 제 1 물리적으로 복제 불가능 기능으로부터의 제 2 응답을 외부 서버에 송신하도록 적응될 수 있다. 부가적으로, 제 1 응답은 제 2 물리적으로 복제 불가능 기능으로부터 외부 서버에 송신될 수 있다. 일 예에서, 외부 서버는 제 1 물리적으로 복제 불가능 기능에 대한 챌린지들 및 응답들의 제 1 데이터베이스 및 제 2 물리적으로 복제 불가능 기능에 대한 챌린지들 및 응답들의 제 2 데이터베이스를 포함할 수 있고, 외부 서버는 전자 디바이스에 챌린지를 송신하고 제 2 응답에 기초하여 전자 디바이스를 인증 또는 식별한다.

[0007] [0007] 일 예에서, 챌린지는 제 1 물리적으로 복제 불가능 기능에 대한 제 1 챌린지 및 제 2 물리적으로 복제 불가능 기능에 대한 제 2 챌린지를 포함할 수 있다. 일 구현에서, 제 1 챌린지는 제 2 챌린지에 대해 예상된 응답에 의해 마스킹되는 챌린지일 수 있다. 다른 구현에서, 제 1 챌린지는 제 1 물리적으로 복제 불가능 기능에 의한 프로세싱 이전에, 제 2 물리적으로 복제 불가능 기능으로부터의 제 1 응답에 의해 수정될 수 있다.

[0008] [0008] 다른 예에서, 수신된 챌린지는 제 2 응답을 생성하기 위해 제 1 물리적으로 복제 불가능 기능에 의해 제 2 챌린지로서 추후에 사용되는 제 1 응답을 생성하도록 제 2 물리적으로 복제 불가능 기능에 의해 사용될 수 있다.

[0009] [0009] 또 다른 예에서, 챌린지는 제 1 물리적으로 복제 불가능 기능에 대한 제 1 챌린지 및 제 2 물리적으로 복제 불가능 기능에 대한 제 2 챌린지를 포함할 수 있고, 제 2 챌린지는 제 1 물리적으로 복제 불가능 기능으로부터 제 2 응답을 마스킹하는데 사용되는 제 1 응답을 생성하도록 제 2 물리적으로 복제 불가능 기능에 의해 사용된다. 제 2 물리적으로 복제 불가능 기능으로부터 제 1 응답은 중간 응답을 획득하기 위해 해싱될 수 있다. 제 2 응답은 그 후 중간 응답을 사용하여 마스킹될 수 있다.

[0010] [0010] 다른 인스턴스들에서, 챌린지는 전자 디바이스의 인증 프로세스, 전자 디바이스의 식별 프로세스, 및/또는 전자 디바이스 내의 키 생성 프로세스 중 적어도 하나의 부분으로서 수신될 수 있다.

[0011] [0011] 일부 구현들에서, 전자 디바이스는 배포 전 또는 제조 단계 동안 하나 이상의 챌린지들을 이전에 수신하고 하나 이상의 대응하는 응답들을 (예를 들어, 데이터 수집기에) 제공하였을 수 있다.

[0012] [0012] 부가적으로, (a) 챌린지가 수신되기 이전에, 또는 (b) 제 2 응답의 송신과 동시에, 미리-저장된 디바이스 식별자가 전자 디바이스로부터 외부 서버에 송신될 수 있고, 디바이스 식별자는 전자 디바이스를 고유하게 식별한다.

[0013] [0013] 전자 디바이스의 배포 전 또는 제조 스테이지 동안 전자 디바이스와 연관된 디바이스 식별자를 획득(예를 들어, 수신 또는 할당)하는 데이터 수집기 디바이스가 또한 제공된다. 데이터 수집기 디바이스는 그 후 하나 이상의 챌린지들을 생성하고 전자 디바이스에 송신할 수 있다. 그 결과, 데이터 수집기 디바이스는 전자 디바이스로부터 하나 이상의 응답들을 수신할 수 있고, 하나 이상의 응답들은 전자 디바이스에서 두 개 이상의 별개의 타입들의 물리적으로 복제 불가능 기능들로부터 생성된 특성 정보를 포함한다. 디바이스 식별자, 챌린지들, 및 대응하는 응답들은 전자 디바이스의 후속 인증을 위해 저장된다. 이 프로세스는 복수의 전자 디바이스들 각각에 대해 반복될 수 있다. 전자 디바이스들로 송신된 챌린지는 모든 디바이스들에 대해 동일할 수 있고, 각각의 전자 디바이스에 대해 랜덤으로 생성될 수 있으며, 및/또는 가능한 챌린지들의 서브세트일 수 있다는 것에 주의한다.

[0014] [0014] 마찬가지로, 별개의 타입들의 물리적 복제 불가능 기능들로부터의 응답에 기초하여 전자 디바이스를 인증하는 인증 디바이스가 제공된다. 인증 디바이스는 전자 디바이스와 연관된 디바이스 식별자를 수신한다. 인

증 디바이스는 그 후 전자 디바이스에 하나 이상의 챌린지들을 송신한다. 응답으로, 인증 디바이스는 전자 디바이스로부터 하나 이상의 응답들을 수신하고, 하나 이상의 응답들은 전자 디바이스에서 두 개 이상의 별개의 타입들의 물리적으로 복제 불가능 기능들로부터 생성된 특성 정보를 포함한다. 전자 디바이스 특유의 미리-저장된 응답은 전자 디바이스 식별자를 사용하여 식별될 수 있다. 전자 디바이스는 그 후 전자 디바이스에 대한 미리-저장된 응답들과 수신된 하나 이상의 응답들을 비교함으로써 인증될 수 있다. 챌린지들은 전자 디바이스로부터 이전에 응답들이 획득된 복수의 챌린지들로부터 선택될 수 있다. 미리-저장된 응답들은 전자 디바이스 배포 전 스테이지 또는 제조 스테이지에서 획득될 수 있다. 디바이스 식별자는 하나 이상의 챌린지들을 송신하기 이전에 수신될 수 있다. 디바이스 식별자는 하나 이상의 응답들을 수신하는 것과 함께 수신될 수 있다.

[0015] [0015] 챌린지는 제 1 물리적으로 복제 불가능 기능에 대한 제 1 챌린지 및 제 2 물리적으로 복제 불가능 기능에 대한 제 2 챌린지를 포함할 수 있다. 제 1 챌린지는 제 2 챌린지에 대해 예상된 응답에 의해 마스킹되는 챌린지일 수 있다. 하나 이상의 챌린지들은 제 1 물리적으로 복제 불가능 기능에 대한 제 1 챌린지 및 제 2 물리적으로 복제 불가능 기능에 대한 제 2 챌린지를 포함할 수 있고, 하나 이상의 응답들은 제 1 물리적으로 복제 불가능 기능으로부터의 제 1 응답 및 제 2 물리적으로 복제 불가능 기능으로부터의 제 2 응답을 포함하고, 제 1 응답이 제 1 챌린지에 대응하는 제 1 미리-저장된 응답과 매칭하고 제 2 응답이 제 2 챌린지에 대응하는 제 2 미리-저장된 응답과 매칭하는 경우, 전자 디바이스가 성공적으로 인증된다.

[0016] [0016] 하나 이상의 챌린지들은 제 1 물리적으로 복제 불가능 기능에 대한 제 1 챌린지 및 제 2 물리적으로 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 하나 이상의 응답들은 제 1 물리적으로 복제 불가능 기능으로부터의 제 1 응답 및 제 2 물리적으로 복제 불가능 기능으로부터의 제 2 응답을 포함한다. 부가적으로, 중간 챌린지는 제 2 응답으로 제 1 챌린지를 언마스킹함으로써 획득될 수 있다. 수신된 제 1 응답은 중간 챌린지와 연관된 미리-저장된 응답에 대해 비교될 수 있다.

[0017] [0017] 또 다른 예에서, 하나 이상의 챌린지들은 제 2 물리적으로 복제 불가능 기능에 대한 제 1 챌린지를 포함하고, 하나 이상의 응답들은 제 1 물리적으로 복제 불가능 기능으로부터의 제 1 응답을 포함한다. 중간 챌린지는 제 1 챌린지에 대응하는 미리-저장된 중간 응답을 리트리브(retrieve)함으로써 획득될 수 있다. 수신된 제 1 응답은 중간 챌린지에 대응하는 미리-저장된 중간 응답에 대해 비교될 수 있다.

[0018] [0018] 또 다른 예에서, 하나 이상의 챌린지들은 제 1 물리적으로 복제 불가능 기능에 대한 제 1 챌린지 및 제 2 물리적으로 복제 불가능 기능에 대한 제 2 챌린지를 포함하고, 하나 이상의 응답들은 제 1 응답을 포함한다. 중간 응답은 제 2 챌린지에 대응하는 미리-저장된 제 2 응답으로 제 1 응답을 언마스킹함으로써 획득될 수 있다. 중간 응답은 제 1 챌린지와 연관된 미리-저장된 응답에 대해 비교될 수 있다.

## *도면의 간단한 설명*

[0019] [0019] 도 1은 SRAM PUF 및 회로 지연 기반 PUF에 기초하여 메모리 디바이스에 대한 응답들의 고유 맵핑을 생성하는 예시적인 방식을 예시하는 블록도이다.

[0020] [0020] 도 2는 SRAM PUF와 회로 지연 기반 PUF를 결합하는 특정한 메모리 디바이스에 대해 이전에 획득한 특성 응답들을 사용하여 그 특정한 메모리 디바이스를 검증 또는 식별하는 예시적인 방식을 예시하는 블록도이다.

[0021] [0021] 도 3은 공격자가 메모리 디바이스를 복제할 수 있게 되는 것을 방지하기 위해 SRAM PUF와 회로 지연 PUF가 결합될 수 있는 방법의 제 1 예를 예시하는 블록도이다.

[0022] [0022] 도 4는 공격자가 메모리 디바이스를 복제할 수 있게 되는 것을 방지하기 위해 SRAM PUF와 회로 지연 PUF가 결합될 수 있는 방법의 제 2 예를 예시하는 블록도이다.

[0023] [0023] 도 5는 공격자가 메모리 디바이스를 복제할 수 있게 되는 것을 방지하기 위해 SRAM PUF와 회로 지연 PUF가 결합될 수 있는 방법의 제 3 예를 예시하는 블록도이다.

[0024] [0024] 도 6은 공격자가 메모리 디바이스를 복제할 수 있게 되는 것을 방지하기 위해 SRAM PUF와 RO PUF가 결합될 수 있는 방법의 제 4 예를 예시하는 블록도이다.

[0025] [0025] 도 7은 일 실시예에 따른 데이터 수집기 디바이스를 예시하는 블록도이다.

[0026] [0026] 도 8은 전자 디바이스로부터 특성 정보를 획득하기 위해 데이터 수집기 디바이스에서 동작하는 방법을 예시한다.

[0027] [0027] 도 9는 각각의 전자 디바이스 내의 다수의 물리적으로 복제 불가능 기능으로부터의 응답들에 기초하여

전자 디바이스를 인증하도록 적응된 예시적인 인증 디바이스를 예시하는 블록도이다.

[0028] 도 10은 복수의 물리적으로 복제 불가능 기능으로부터의 응답들에 기초하여 전자 디바이스를 인증하기 위해 인증 디바이스에서 동작하는 방법을 예시한다.

[0029] 도 11은 다수의 물리적으로 복제 불가능 기능을 갖는 예시적인 전자 디바이스를 예시하는 블록도이다.

[0030] 도 12는 복수의 물리적으로 복제 불가능 기능으로부터의 응답들에 기초하여 인증 디바이스를 통해 스스로를 인증하기 위해 전자 디바이스에서 동작하는 방법을 예시한다.

## *발명을 실시하기 위한 구체적인 내용*

[0020] [0031] 이하의 설명에서, 특정한 세부사항들은 본 개시의 다양한 양상들의 철저한 이해를 제공하기 위해 제공된다. 그러나 양상들은 이러한 특정한 세부사항들 없이 실시될 수 있다는 것이 당업자에 의해 이해될 것이다. 예를 들어, 회로들은 불필요한 세부사항들로 양상들을 모호하게 하는 것을 방지하기 위해 블록도들로 도시될 수 있다. 다른 인스턴스들에서, 잘 알려진 회로들, 구조들 및 기법들은 본 개시의 양상들을 모호하게 하지 않도록 상세히 도시되지 않을 수도 있다.

[0021] [0032] "예시적인"이라는 단어는 "예시, 실례 또는 예증으로서 역할하는 것"을 의미하는 것으로 여기서 사용된다. "예시"로서 본 명세서에 기술된 임의의 구현 또는 양상은, 반드시 본 개시의 다른 양상들에 비해 바람직하거나 유리한 것으로 해석되는 것은 아니다. 마찬가지로, "양상들"이라는 용어는 본 개시의 모든 양상들이 논의된 피처, 장점 또는 동작 모드를 포함할 것을 요구하진 않는다.

[0022] 개요

[0023] [0033] 하나의 피처는 정적 랜덤 액세스 메모리(SRAM) PUF들과 회로 지연 기반 PUF들(예를 들어, 링 오실레이터(RO) PUF들, 아비터 PUF들 등)을 결합함으로써 고유한 식별자를 생성하는 것을 제공한다. SRAM PUF들 그 자체들로만은 장애 분석 툴(예를 들어, FIB(Focused Ion Beam))을 이용하는 복제 공격들에 취약할 수 있다. 이에 따라, 회로 지연 기반 PUF들은 SRAM PUF들로의 챌린지(challenge)를 은폐하거나 및/또는 SRAM PUF로부터의 응답들을 은폐하는데 사용될 수 있고, 그에 의해, 공격자가 메모리 디바이스의 응답을 복제할 수 있게 되는 것을 막는다.

[0024] SRAM과 회로 지연 기반 PUF(Physically Unclonable Function)들의 결합

[0025] [0034] PUF(Physical Unclonable Function)는 고유한 식별자를 획득하기 위해 회로 내의 제조 프로세스 변동들을 이용하는 챌린지-응답 메커니즘(challenge-response mechanism)이다. 일 예에서, 챌린지와 대응하는 응답 사이의 관계는 회로(예를 들어, 집적 회로)에서 로직 컴포넌트들 및 상호연결들의 복잡한 통계적 변동들에 의해 결정된다. 2개의 타입들의 PUF들은 예를 들어, SRAM PUF 및 회로 지연 PUF(예를 들어, 링 오실레이터 PUF)를 포함한다.

[0026] [0035] SRAM PUF는 메모리 디바이스 또는 메모리 디바이스가 통합되는 전자 디바이스에 대한 식별 "지문"을 생성하기 위해 정적 랜덤 액세스 메모리(SRAM)의 초기화되지 않은 파워-업 상태를 이용한다. SRAM 셀 설계가 대칭적이지만, 제조 프로세스 편차들은 SRAM 셀들 사이의 작은 비대칭으로 이어지며, 이는 시동 동안 차등/바이어싱된 상태(0 또는 1)를 초래한다. 초기화되지 않은 SRAM 셀들의 이러한 차등 또는 바이어스는 메모리 디바이스를 고유하게 식별하는데 사용될 수 있다.

[0027] [0036] 그러나 FIB(Focused Ion Beam)를 사용한 장애 분석 공격의 최근의 진보들은 메모리-기반 PUF들의 보안성을 위협한다. 회로 편집 공격은 원래 디바이스와 동일한 SRAM PUF 응답을 갖는 하드웨어 복제(clone)를 생성할 수 있다.

[0028] [0037] 회로 지연 기반 PUF들은 제작/제조 결함들에 의해 야기되는 오실레이터 회로들 사이의 체계적인 변동들을 이용한다. 제작/제조 프로세스들이 회로 지연 기반 PUF들의 이러한 변동들을 방지하고자 하지만, 그들은 항상 어느 정도까지는 존재하고 실제로 디바이스들/칩들을 식별하는데 유용하다. 회로 지연 기반 PUF의 일 예에서, 복수의 링 오실레이터들이 동시에 사용될 수 있으며 적어도 2개의 링 오실레이터들의 출력들은 하나 이상의 스위치들(멀티플렉서들)로 송신된다. 챌린지는 링 오실레이터들에 대한 입력으로서 역할을 할 수 있고(예를 들어, 챌린지는 2개의 링 오실레이터들을 선택하도록 역할을 하고), 2개의 선택된 링 오실레이터들(204)로부터의 출력은 제 1 주파수 및 제 2 주파수로서 표현된다. 선택된 링 오실레이터들 사이의 차이들로 인해, 그들의 주

파수들은 상이하게 될 것이다(즉, 주파수 차이를 초래함). RO PUF 출력(응답)은 링 오실레이터 주파수들의 페어-와이즈 비교(pair-wise comparison)(예를 들어, 제 1 및 제 2 주파수 간의 차이)에 의해 생성된다.

[0029] [0038] 그러나 크기 조정 가능한 회로 지연 기반 PUF를 구현하는 것은 집적 회로에서 필요한 공간을 많이 차지한다.

[0030] [0039] 일 피처에 따라, SRAM PUF 및 회로 지연 기반 PUF는 SRAM PUF의 보안성을 강화하기 위해 전자 디바이스(예를 들어, 메모리 디바이스, 반도체 디바이스 등) 내에서 결합된다.

[0031] [0040] 도 1은 SRAM PUF 및 회로 지연 기반 PUF, 예를 들어 링 오실레이터(RO) PUF에 기초하여 메모리 디바이스에 대한 응답들의 고유 맵핑을 생성하는 예시적인 방식을 예시하는 블록도이다. 이 블록도는 SRAM PUF(105) 및 (예를 들어, 링 오실레이터 뱅크로서 구현되는) 회로 지연 PUF(122)를 포함하는 메모리 디바이스(102)(예를 들어, 칩, 반도체 디바이스 등) 에 대한 챌린지/응답 특성들을 질의하고 수집하는 프로세스를 예시한다.

[0032] [0041] 일 예에서, SRAM PUF는 메모리 디바이스(102)의 SRAM 셀들 모두 또는 부분들로부터 구현될 수 있다. 특히, SRAM PUF(105)는 SRAM(106)의 초기화되지 않은 메모리 셀들(104)에서의 바이어싱을 이용한다. 예를 들면, 제조 스테이지 동안, 초기화되지 않은 SRAM(106)는, 각각의 챌린지(110)(예를 들면, 메모리 어드레스)에 대해, 대응하는 응답(112)(예를 들어, 로직 0 또는 1)이 획득되도록 질의될 수 있다. 예를 들어, SRAM(106) 내의 각각의 메모리 어드레스에 대해, 그 메모리 어드레스와 연관되는 메모리 셀(104)에 대한 초기화되지 않은 값/상태가 획득된다. 복수의 챌린지들(110)에 대해, 복수의 응답들(112)이 획득된다. 다른 접근법들에서, 메모리 어드레스들의 서브세트만이 질의될 수 있다. 이러한 방식으로, 초기화되지 않은 값들과 어드레스들의 맵핑이 SRAM(106)에 대해 구축되고 (예를 들어, 챌린지들 및 대응하는 응답들로서) 데이터베이스(114)에 저장될 수 있다. 즉, SRAM PUF 챌린지들/응답들(114)의 데이터베이스가 예를 들어, 제조 또는 품질 제어 프로세스 동안 각각의 메모리 디바이스(칩)에 대해 구축될 수 있다. 예를 들면, 디바이스-A에 대해, 챌린지들/응답들의 제 1 세트[$C_0R_0$, $C_1R_1$,…, $C_iR_i$]가 획득되고, 디바이스-B에 대해, 챌린지들/응답들의 제 2 세트[$C_0R_0$, $C_1R_1$,…, $C_iR_i$]가 획득되고, 디바이스-C에 대해, 챌린지들/응답들의 제 3 세트[$C_0R_0$, $C_1R_1$,…, $C_iR_i$]가 획득된다. 일부 구현들에서, 모든 디바이스들에 대한 챌린지들[C0, C1,…, Ci]은 동일할 수 있지만, 응답은 상이할 것임에 주의한다. 다른 구현들에서, 각각의 디바이스 대한 챌린지들[C0, C1,…, Ci]이 랜덤으로 선택될 수 있고, 그래서 상이한 디바이스들은 상이한 챌린지들을 수신한다.

[0033] [0042] 일 예에서, 회로 지연 PUF(120)는 고유한 서명/응답을 생성하도록 복수의 링 오실레이터들(123) 및 그의 주파수 변동들을 이용하는 링 오실레이터(RO) PUF(122)로서 구현될 수 있다. 예를 들면, 주어진 챌린지(124)(예를 들어, 2개의 링 오실레이터 입력들/출력들의 선택)에 대해, 대응하는 응답(예를 들어, 2개의 선택된 링 오실레이터들 간의 주파수 차이)이 획득된다. 이러한 방식으로, 챌린지들 및 대응하는 응답들의 회로 지연 PUF 데이터베이스(128)가 획득될 수 있다.

[0034] [0043] SRAM(106)의 초기화되지 않은 메모리 셀 상태들이 FIB(focused ion beam) 공격에 의한 복제에 취약하기 때문에, 메모리 디바이스(102)에 대한 고유한 식별자를 제공하기 위해 SRAM PUF(105)만을 사용하는 것은 안전하지 않다. 그러나 SRAM PUF(105)와 달리, 회로 지연 PUF(120)(예를 들어, RO PUF(122))는 복제에 취약하지는 않지만, 매우 다수의 RO PUF들이 칩 상의 공간을 차지하기 때문에 이들을 사용하는 것은 바람직하지 않다. 결과적으로, 비교적 소수의 링 오실레이터들(123)은 SRAM PUF(102) 상의 복제 공격들을 저지하도록 메모리 디바이스(102)(예를 들어, 칩, 반도체 등) 상에서 SRAM PUF(105)와 결합될 수 있다.

[0035] [0044] 각각의 디바이스에 챌린지들/응답들을 연관시키기 위해, 디바이스 식별자(108)(예를 들어, 일련번호, ID 번호 등)은 디바이스(102)에 저장되고, 데이터베이스(114, 128)에게 알려지거나, 또는 거기에 저장될 수 있다. 즉, 각각의 메모리 디바이스(102)에 대한 디바이스 식별자(108)는 저장되고, 그 메모리 디바이스(102)에 대한 대응하는 챌린지들 및/또는 응답들과 연관될 수 있다.

[0036] [0045] 도 2는 SRAM PUF와 회로 지연 기반 PUF, 예를 들어 링 오실레이터(RO) PUF를 결합하는 특정한 메모리 디바이스에 대해 이전에 획득한 특성 응답들을 사용하여 그 특정한 메모리 디바이스를 검증 또는 식별하는 예시적인 방식을 예시하는 블록도이다. 동작 동안, (예를 들어, 검증기 또는 인증 디바이스/서버에 의해 구현되는) 디바이스 검증 모듈/회로(202)는 SRAM PUF 데이터베이스(114)와 회로 지연 PUF 데이터베이스(128)의 결합을 사용하여 검증될 수 있는 응답(206)을 획득하기 위해 챌린지(204)로 메모리 디바이스(102)에 질의할 수 있다. 응답(206)은 메모리 디바이스의 아이덴티티를 검증하거나 메모리 디바이스(102)를 인증하도록 역할을 할 수 있다. 이 기술은 또한 메모리 디바이스에 대한 고유한 식별자/서명을 생성하도록 역할을 할 수 있다는 것에 주의한다.

[0037] [0046] 일 예에서, 메모리 디바이스(102)는 디바이스 인증 모듈/회로/서버(202)에 그의 미리-저장된/미리-할당된 디바이스 식별자(108)를 제공할 수 있다는 것에 주의한다. 디바이스 인증 모듈/회로/서버(202)는 그 후 그 디바이스 식별자(108)에 대해 이전에 저장된 하나 이상의 챌린지들을 리트리브하고, 이들을 메모리 디바이스(102)에 송신(204)할 수 있다. 대안적으로, 디바이스 식별자(108)는 (예를 들어, 동일한 챌린지들이 모든 전자 디바이스들에 사용되는 경우) 챌린지에 대한 임의의 응답들과 함께 전자 디바이스에 의해 제공된다. 응답(206)을 수신 시에, 디바이스 인증 모듈/회로/서버(202)는 매칭이 존재하는지를 확인하기 위해 SRAM PUF(114) 및 회로 지연 PUF(128)의 대응하는 이전에 저장된 응답(들)에 대해 수신된 응답(206)를 비교한다.

[0038] [0047] 이 검증 스테이지 동안, 챌린지(204) 및 응답(206)은 공격자에 의해 액세스 가능하거나 액세스될 수 있다. 이에 따라, 다양한 피처들은 공격자가 메모리 디바이스(102)를 복제하는 것을 막기 위해 메모리 디바이스(102)로의/로부터의 챌린지(204) 및/또는 응답(206)의 보호를 제공된다.

[0039] [0048] 일 예에서, 회로 지연 PUF(120)(예를 들어, 지연-기반 PUF)는 변조-방지적(tamper-resistant)이다. FIB(focused ion beam) 공격이 SRAM PUF(105)의 메모리 셀들의 응답들을 노출할 수 있지만, 이것은 회로 지연 PUF(120)(예를 들어, 링 오실레이터들)에 대한 정보를 제공하지 않는다. 사실상, 메모리 디바이스(102)를 복제/공격하는데 사용되는 프로세스는 그것이, 공격에 노출되고 메모리 디바이스(102)의 인증/식별의 장애를 야기하도록 회로 지연 PUF(120)(예를 들어, 링 오실레이터들)의 응답을 변경할 수 있다는 점에서 충분히 침입적일 수 있다.

[0040] [0049] 챌린지들(204) 및 응답들(206)이 공격자에 의해 액세스 가능할 때조차도, 공격자가 메모리 디바이스(102)를 복제하는 것을 막기 위해 SRAM PUF(105)와 회로 지연 PUF(120)을 결합하는 다양한 방식들이 있다.

[0041] 챌린지들을 마스킹하기 위한 SRAM와 RO PUF(Physically Unclonable Function)들의 결합

[0042] [0050] 도 3은 공격자가 메모리 디바이스(307)를 복제할 수 있게 되는 것을 방지하기 위해 SRAM PUF(326)와 회로 지연 PUF(324)가 결합될 수 있는 방법의 제 1 예를 예시하는 블록도이다. 이 예에서, 인증 디바이스(300)는 디바이스 인증 모듈/회로/서버(303), SRAM PUF 데이터베이스(301) 및 회로 지연 PUF 데이터베이스(305)를 포함할 수 있다. SRAM PUF 데이터베이스(301)는 예를 들면, 메모리 디바이스(307)의 메모리 셀 지역에 복수의 챌린지들(예를 들면, 메모리 어드레스들)을 송신하고 대응하는 응답들(예를 들어, 초기화되지 않은 메모리 셀 상태들/값들)을 획득함으로써 제조 동안 그 메모리 셀 지역에 대해 생성될 수 있다. 유사하게, 회로 지연 PUF 데이터베이스(305)는 예를 들면, 메모리 디바이스(307) 내의 복수의 링 오실레이터들에 복수의 챌린지들(예를 들어, 2개의 링 오실레이터들의 선택)을 송신하고 대응하는 응답들(예를 들어, 2개의 선택된 링 오실레이터들 간의 주파수 차이)을 획득함으로써 제조 동안 그 링 오실레이터들에 대해 생성될 수 있다.

[0043] [0051] 이 예에서, 디바이스 인증 모듈/회로/서버(303)가 이어서 메모리 디바이스(307)를 인증하도록 시도할 때, 그것은 메모리 디바이스(307)에 챌린지(챌린지 A(316) 및 챌린지 B(312)를 포함함)를 송신한다. 챌린지 A(316)은 XOR 연산(302)에 의해 결합되는 SRAM PUF 챌린지 $C_0$(306) 및 RO PUF 응답 $R_0$(310)를 포함할 수 있다. 이 챌린지 A(316)가 공격자에 의해 액세스 가능하게 될 수 있기 때문에, 일 양상은 전송된(노출된) 챌린지 A(316)를 생성하도록 (회로 지연 PUF 데이터베이스(305)로부터 획득된) 대응하는 RO PUF 응답 $R_0$(310)으로 실제 SRAM PUF 챌린지 $C_0$(306)를 마스킹(예를 들어, XOR 연산)함으로써 그것을 모호하게 한다. 부가적으로, RO PUF 응답 $R_0$(310)에 대응하는, RO PUF 챌린지 $C_0$(308)를 포함하는 챌린지 B(312)는 또한 인증 디바이스(300)로부터 메모리 디바이스(307)로 송신된다.

[0044] [0052] 메모리 디바이스(307)에서, RO PUF 챌린지 $C_0$(312)는 회로 지연 PUF(324)로부터 RO PUF 응답 $R_0$(321)를 생성하는데 사용된다. 챌린지 A(316)는 그 후 SRAM PUF(326)에 대한 챌린지로서 사용될 수 있는 실제(평문(clear)) SRAM PUF 챌린지 $C_0$(323)을 획득하기 위해 RO PUF 응답 $R_0$(321)와 XOR 연산(304)된다. SRAM PUF(326)는 그 후 응답 SRAM PUF $R_0$(325)를 생성한다. 이러한 방식으로, 메모리 디바이스(307)로부터 인증 디바이스(300)로의 응답은 SRAM PUF 응답 $R_0$(318)를 포함할 수 있다.

[0045] [0053] 인증 디바이스(300)에서, 수신된 응답 SRAM PUF $R_0$(322)는 SRAM PUF 데이터베이스(301) 및 회로 지연 PUF(305)의 저장된 응답들에 대해 비교하고 이들이 매칭하는지를 확인하는데 이용될 수 있다. RO PUF 응답

$R_0$(310)이 이미 알려졌거나 회로 지연 PUF 데이터베이스(305)에 저장되어 있기 때문에, 인증 디바이스(300)는 RO PUF 응답 $R_0$(310)으로 SRAM PUF 챌린지 $C_0$(306)을 마스킹하도록 그것을 이용할 수 있다는 것에 주의한다.

[0046] [0054] 도 4는 공격자가 메모리 디바이스(407)를 복제할 수 있게 되는 것을 방지하기 위해 SRAM PUF(426)와 회로 지연 PUF(424)가 결합될 수 있는 방법의 제 2 예를 예시하는 블록도이다. 도 3의 예와는 달리, 이 예에서, SRAM PUF 챌린지 $C_0$(406) 및 RO PUF 챌린지 $C_0$(408)는 디바이스 인증 모듈/회로/서버(403)로부터 메모리 디바이스(407)로 평문으로 송신된다. 이 예에서, 인증 디바이스(400)는 디바이스 인증 모듈/회로/서버(403), SRAM PUF 데이터베이스(401) 및 회로 지연 PUF 데이터베이스(405)를 포함할 수 있다. SRAM PUF 데이터베이스(401)는 예를 들면, 메모리 디바이스(407)의 메모리 셀 지역에 복수의 챌린지들(예를 들면, 메모리 어드레스들)을 송신하고 대응하는 응답들(예를 들어, 초기화되지 않은 메모리 셀 상태들/값들)을 획득함으로써 제조 동안 그 메모리 셀 지역에 대해 생성될 수 있다. 유사하게, 회로 지연 PUF 데이터베이스(405)는 예를 들면, 메모리 디바이스(407) 내의 복수의 링 오실레이터들에 복수의 챌린지들(예를 들어, 2개의 링 오실레이터들의 선택)을 송신하고 대응하는 응답들(예를 들어, 2개의 선택된 링 오실레이터들 간의 주파수 차이)을 획득함으로써 제조 동안 그 링 오실레이터들에 대해 생성될 수 있다.

[0047] [0055] 이 예에서, 디바이스 인증 모듈/회로/서버(403)가 이어서 메모리 디바이스(407)를 인증하도록 시도할 때, 그것은 메모리 디바이스(407)에 챌린지(챌린지 A(416) 및 챌린지 B(412)를 포함함)를 송신한다. 챌린지 A(416)는 SRAM PUF 챌린지 $C_0$(406)를 포함할 수 있다. RO PUF 응답 $R_0$(410)에 대응하는, RO PUF 챌린지 $C_0$(408)를 포함하는 챌린지 B(412)는 또한 인증 디바이스(400)로부터 메모리 디바이스(407)로 송신된다.

[0048] [0056] 챌린지 A(416)가 공격자에 의해 액세스 가능하게 될 수 있지만, 일 양상은 메모리 디바이스(407)에서의 XOR 연산(404)에 의해 수정된 SRAM PUF 챌린지 $C_0$'(423)로 실제 SRAM PUF 챌린지 $C_0$(406)를 수정한다. 메모리 디바이스(407)에서, RO PUF 챌린지 $C_0$(412)는 회로 지연 PUF(424)로부터 RO PUF 응답 $R_0$(421)를 생성하는데 사용된다. 챌린지 A(416)(즉, SRAM PUF 챌린지 $C_0$(406))는 그 후 SRAM PUF(426)에 대한 챌린지로서 사용될 수 있는 수정된 SRAM PUF 챌린지 $C_0$'(423)를 획득하도록 RO PUF 응답 $R_0$(421)과 XOR 연산(404)된다. SRAM PUF(426)은 그 후 인증 디바이스(400)로 (응답 A(418)으로서) 리턴되는 SRAM PUF 응답 $R_0$'(425)을 생성한다. 이러한 방식으로, 메모리 디바이스(407)로부터 인증 디바이스(400)로의 응답은 SRAM PUF 응답 $R_0$(418)를 포함할 수 있다.

[0049] [0057] 이 접근법에서, RO PUF 응답 $R_0$(421)은 메모리 셀 지역(426)에 대한 실제 챌린지를 수정하는데 사용된다. 공격자가 RO PUF 응답 $R_0$(421)을 재생할 수 없기 때문에, 공격자는 응답 SRAM PUF 응답 $R_0$'(425)를 생성하는데 사용된 수정된 SRAM PUF 챌린지 $C_0$'(423)을 알 수 없다.

[0050] [0058] 인증 디바이스(400)에서, 디바이스 인증 모듈/회로/서버(403)는 SRAM PUF 응답 $R_0$'(422)를 검증할 수 있다. 이것은 수정된 SRAM PUF 챌린지 $C_0$'(427)의 로컬 버전을 획득하기 위해 예를 들어, (회로 지연 PUF 데이터베이스(405)로부터 획득되는) RO PUF 응답 $R_0$(420)와 SRAM PUF 챌린지 $C_0$(406)를 XOR 연산(402)함으로써 행해질 수 있다. 수정된 SRAM PUF 챌린지 $C_0$'(427)의 로컬 버전은 그 후 SRAM PUF 데이터베이스(401)에서 대응하는 응답을 룩업하고 수신된 응답 SRAM PUF 응답 $R_0$'(422)에 대해 그 응답을 비교하는데 사용할 수 있다.

[0051] [0059] 도 5는 공격자가 메모리 디바이스를 복제할 수 있게 되는 것을 방지하기 위해 SRAM PUF(526)와 회로 지연 PUF(524)가 결합될 수 있는 방법의 제 3 예를 예시하는 블록도이다. 이 예에서, 인증 디바이스(500)는 디바이스 인증 모듈/회로/서버(503), SRAM PUF 데이터베이스(501) 및 회로 지연 PUF 데이터베이스(505)를 포함할 수 있다. SRAM PUF 데이터베이스(501)는 예를 들면, 메모리 디바이스(507)의 메모리 셀 지역에 복수의 챌린지들(예를 들면, 메모리 어드레스들)을 송신하고 대응하는 응답들(예를 들어, 초기화되지 않은 메모리 셀 상태들/값들)을 획득함으로써 제조 동안 그 메모리 셀 지역에 대해 생성될 수 있다. 유사하게, 회로 지연 PUF 데이터베이스(505)는 예를 들면, 메모리 디바이스(507) 내의 복수의 링 오실레이터들에 복수의 챌린지들(예를 들어, 2개의 링 오실레이터들의 선택)을 송신하고 대응하는 응답들(예를 들어, 2개의 선택된 링 오실레이터들 간의 주파수 차이)을 획득함으로써 제조 동안 그 링 오실레이터들에 대해 생성될 수 있다.

[0052] [0060] 이 예에서, 디바이스 인증 모듈/회로/서버(503)가 이어서 메모리 디바이스(507)를 인증하도록 시도할

때, 그것은 대응하는 RO PUF 응답 $R_0$를 갖는 RO PUF 챌린지 $C_0$(508)을 포함하는 챌린지(512)를 송신한다.

[0053] [0061] RO PUF 챌린지 $C_0$(512)가 공격자에 의해 액세스 가능하게 될 수 있지만, 회로 지연 PUF(524)는 공격자에 의해 복제될 수 없다. 메모리 디바이스(507)에서, RO PUF 챌린지 $C_0$(512)는 회로 지연 PUF(524)로부터의 RO PUF 응답 $R_0$(521)를 생성하는데 사용된다. 이 RO PUF 응답 $R_0$(521)은 그 후 RO PUF 응답 $R_0$(525)을 획득하기 위해 SRAM PUF(526)로의 SRAM PUF 챌린지 $C_0$(523)으로서 사용된다. 대안적인 접근법에서, RO PUF 응답 $R_0$(521)은 (예를 들어, RO PUF 응답 $R_0$(521)를 메모리 어드레스에 맵핑하거나 변환함으로써) 챌린지 SRAM PUF $C_0$(523)을 생성하기 위해 사용될 수 있다. SRAM PUF 응답 $R_0$(518)는 인증 디바이스(500)에 송신된다.

[0054] [0062] 이 접근법에서, RO PUF 응답 $R_0$(521)은 SRAM PUF(526)에 대한 실제 챌린지를 수정하는데 사용된다. 공격자가 RO PUF 응답 $R_0$(521)을 재생할 수 없기 때문에, 공격자는 응답 SRAM PUF 응답 $R_0$(525)를 생성하는데 사용된 SRAM PUF 챌린지 $C_0$(523)을 알 수 없다.

[0055] [0063] 인증 디바이스(500)에서, 디바이스 인증 모듈/회로/서버(503)는 회로 지연 PUF(505)로부터, 송신된 RO PUF 챌린지 $C_0$(508)에 대응하는 RO PUF 응답 $R_0$(520)를 획득할 수 있다. 이 RO PUF 응답 $R_0$(520)는 SRAM PUF 챌린지 $C_0$(527)로서 역할을 할 수 있다. 디바이스 인증 모듈/회로/서버(503)는 SRAM PUF 응답 $R_0$(522)를 검증할 수 있다. SRAM PUF 챌린지 $C_0$(527)은 그 후 SRAM PUF 데이터베이스(501)에서 대응하는 응답을 룩업하고 수신된 응답 SRAM PUF 응답 $R_0$(522)에 대해 그 응답을 비교하는데 사용할 수 있다.

[0056] [0064] 도 3, 도 4, 및 도 5에서 예시된 접근법에서, 디바이스 인증 모듈/회로/서버(303, 403 및/또는 503)는 SRAM PUF 및 RO PUF 둘 다에 대한 챌린지 및 응답 쌍에 대한 액세스를 가질 수 있다. 이에 따라, 디바이스 인증 모듈/회로/서버(303, 403, 및/또는 503)는 메모리 디바이스(307, 407, 및 507)에 의해 수행된 동작들을 검증하고 응답(들)을 검증할 수 있다.

[0057] 응답들을 마스킹하기 위한 SRAM과 RO PUF(Physically Unclonable Function)들의 결합

[0058] [0065] 대안적으로, 접근법은 RO PUF의 이용에 의해 메모리 디바이스로부터의 SRAM PUF 응답을 보호한다.

[0059] [0066] 도 6은 공격자가 메모리 디바이스(607)를 복제할 수 있게 되는 것을 방지하기 위해 SRAM PUF(626)와 RO PUF(624)가 결합될 수 있는 방법의 제 4 예를 예시하는 블록도이다. 이 예에서, 인증 디바이스(600)는 디바이스 인증 모듈/회로/서버(603), SRAM PUF 데이터베이스(601) 및 RO PUF 데이터베이스(605)를 포함할 수 있다. SRAM PUF 데이터베이스(601)는 예를 들면, 메모리 디바이스(607)의 메모리 셀 지역에 복수의 챌린지들(예를 들면, 메모리 어드레스들)을 송신하고 대응하는 응답들(예를 들어, 초기화되지 않은 메모리 셀 상태들/값들)을 획득함으로써 제조 동안 그 메모리 셀 지역에 대해 생성될 수 있다. 유사하게, 회로 지연 PUF 데이터베이스(605)는 예를 들면, 메모리 디바이스(607) 내의 복수의 링 오실레이터들에 복수의 챌린지들(예를 들어, 2개의 링 오실레이터들의 선택)을 송신하고 대응하는 응답들(예를 들어, 2개의 선택된 링 오실레이터들 간의 주파수 차이)을 획득함으로써 제조 동안 그 링 오실레이터들에 대해 생성될 수 있다.

[0060] [0067] 이 예에서, 디바이스 인증 모듈/회로/서버(603)가 이어서 메모리 디바이스(607)를 인증하도록 시도할 때, 그것은 메모리 디바이스(607)에 챌린지(챌린지 A(616) 및 챌린지 B(612)를 포함함)를 송신한다. 챌린지 A(616)는 SRAM PUF 챌린지 $C_0$(606)를 포함할 수 있다. 챌린지 B(612)는 인증 디바이스(600)로부터 메모리 디바이스(607)로 또한 송신되는 RO PUF 챌린지 $C_0$(608)를 포함한다.

[0061] [0068] 메모리 디바이스(604)에서, RO PUF 챌린지 $C_0$(612)는 회로 지연 PUF(624)로부터 RO PUF 응답 $R_0$(621)를 생성하는데 사용된다. SRAM PUF 챌린지 $C_0$(616)는 SRAM PUF 응답 $R_0$(623)를 생성하도록 SRAM PUF(626)에 의해 프로세싱된다. RO PUF 응답 $R_0$(621)의 해시(619)는 그 후 RO PUF 응답 $R_0$'(625)로서 획득된다. RO PUF 응답 $R_0$'(625)는 그 후 디바이스 인증 모듈/회로/서버(603)로 역으로 전송되는 결합된 응답(618)(예를 들어, SRAM PUF $R_0$ XOR RO PUF 응답 $R_0$')을 획득하기 위해 SRAM PUF $R_0$(623)와 XOR 연산(604)된다. 이러한 방식으로, SRAM PUF(626)로부터 인증 디바이스(600)로의 SRAM PUF 응답 $R_0$(623)은 전송 동안 보호될 수 있다.

[0062] [0069] 인증 디바이스(600)에서, 디바이스 인증 모듈/회로/서버(603)는 응답(618)이 송신된 챌린지들(SRAM PUF

$C_0$(606) 및 RO PUF $C_0$(608))에 대응한다는 것을 검증할 수 있다. 예를 들면, 회로 지연 PUF 데이터베이스(605)를 사용하여, 송신된 RO PUF 챌린지 $C_0$(608)에 대응하는 RO PUF 응답 $R_0$(620)이 획득된다. 그 후, 디바이스 인증 모듈/회로/서버(603)는 SRAM PUF 응답 $R_0$(627)을 획득하기 위해 RO PUF 응답 $R_0$(620)을 해싱(617)하고 그 결과를 응답(618)과 XOR 연산(602)함으로써 SRAM PUF 응답 $R_0$(627)를 획득할 수 있다. SRAM PUF 응답 $R_0$(627)는 그 후 SRAM PUF 데이터베이스(601)에서 SRAM PUF 챌린지 $C_0$(606)에 대해 예상되는 대응하는 응답을 룩업하는데 이용될 수 있다. 응답들이 매칭하는 경우, 메모리 디바이스(607)는 성공적으로 인증 또는 식별된다.

[0063] 예시적인 데이터 수집기 디바이스 및 거기에서의 동작 방법

[0064] [0070] 도 7은 일 예에 따른 데이터 수집기 디바이스를 예시하는 블록도이다. 데이터 수집기 디바이스(702)는 전자 디바이스들(예를 들어, 칩들, 반도체들, 메모리 디바이스들 등)을 고유하게 특징화하는 정보를 수집하고 저장하도록 적응될 수 있다. 예를 들어, 제조 스테이지, 품질 제어 스테이지 및/또는 배포-전 스테이지 동안, 데이터 수집기 디바이스(702)는 각각의 전자 디바이스에 챌린지를 송신하고 응답을 수신하고, 각각의 전자 디바이스를 인증/식별하는데 있어 나중에 이용하기 위해 수신된 정보를 저장하도록 적응될 수 있다.

[0065] [0071] 데이터 수집기 디바이스(702)는 프로세싱 회로(704), 저장 디바이스(706), 통신 인터페이스(708) 및/또는 기계-판독 가능 매체(710)를 포함할 수 있다. 통신 인터페이스(708)는 데이터 수집기 디바이스(702)가 하나 이상의 전자 디바이스들과 (예를 들어, 유선 또는 무선으로) 통신하도록 허용하는 전송기/수신기 회로(718)를 포함할 수 있다.

[0066] [0072] 프로세싱 회로(704)는 각각의 전자 디바이스에 대한 고유한 식별자를 획득하고 저장 디바이스(706)의 디바이스 식별자 데이터베이스(716)에 이러한 고유한 식별자를 저장하도록 적응되는 디바이스 식별자 회로/모듈(722)을 포함할 수 있다. 프로세싱 회로(704)는 또한 하나 이상의 챌린지들을 생성하고 전자 디바이스에 송신하도록 적응된 챌린지 생성기 회로/모듈(720)을 포함할 수 있다. 예를 들면, 챌린지들은 (예를 들어, SRAM PUF에 대해) 메모리 어드레스 또는 (예를 들어, RO PUF에 대해) 링 오실레이터 쌍들일 수 있다. 프로세싱 회로(704)는 또한 송신된 하나 이상의 챌린지들에 응답하여 전자 디바이스의 SRAM PUF로부터 응답들을 수집하도록 적응되는 SRAM PUF 수집 회로/모듈(726)을 포함할 수 있다. 프로세싱 회로(704)는 또한 송신된 하나 이상의 챌린지들에 응답하여 전자 디바이스의 회로 지연 PUF로부터 응답들을 수집하도록 적응되는 회로 지연 PUF 수집 회로/모듈(726)을 포함할 수 있다.

[0067] [0073] 기계-판독 가능 매체(710)는 (예를 들어, 프로세싱 회로가 질의되고 있는 전자 디바이스로부터 디바이스 식별자를 획득하게 하는) 디바이스 식별자 명령들(730), (예를 들어, 프로세싱 회로가 질의되고 있는 전자 디바이스의 회로 지연 PUF 및/또는 SRAM PUF에 대한 랜덤 또는 미리-생성된 챌린지들을 생성/송신하게 하기 위한) 챌린지 생성기 명령들(728), (예를 들어, 프로세싱 회로가 질의되고 있는 전자 디바이스의 SRAM PUF로부터 응답들을 수집하게 하기 위한) SRAM PUF 수집 명령들(732), 및/또는 (예를 들어, 프로세싱 회로가 질의되고 있는 전자 디바이스의 회로 지연 PUF로부터 응답들을 수집하게 하기 위한) 회로 지연 PUF 수집 명령들(734)을 포함하거나 저장할 수 있다. 일 예에서, 회로 지연 PUF는 변조-방지 PUF일 수 있다는 것에 주의한다. 대조적으로, SRAM PUF는 다양한 공격들(예를 들어, FIB(Focused Ion Beam) 공격들, 회로 편집 공격들 등)에 취약한 것으로 확인되었다.

[0068] [0074] 데이터 수집기 디바이스(702)는 도 1 내지 도 6에서 예시된 단계들 또는 기능들 중 하나 이상을 수행하도록 적응될 수 있다.

[0069] [0075] 도 8은 전자 디바이스로부터 특성 정보를 획득하기 위한 데이터 수집기 디바이스에서 동작하는 방법을 예시한다. 데이터 수집기 디바이스는 배포 전 또는 제조 스테이지(802) 동안 전자 디바이스와 연관된 디바이스 식별자를 획득(예를 들어, 수신 또는 할당)할 수 있다. 데이터 수집기 디바이스는 그 후 하나 이상의 챌린지들을 생성하고 전자 디바이스(804)에 송신할 수 있다. 그 결과, 데이터 수집기 디바이스는 전자 디바이스로부터 하나 이상의 응답들을 수신할 수 있고, 하나 이상의 응답들은 전자 디바이스(806)의 두 개 이상의 별개의 타입들의 물리적으로 복제 불가능 기능들로부터 생성된 특성 정보를 포함한다. 디바이스 식별자, 챌린지들, 및 대응하는 응답들은 전자 디바이스(808)의 후속 인증을 위해 저장된다. 이 프로세스는 복수의 전자 디바이스들 각각에 대해 반복될 수 있다. 전자 디바이스들로 송신된 챌린지는 모든 디바이스들에 대해 동일할 수 있고, 각각의 전자 디바이스에 대해 랜덤으로 생성될 수 있으며, 및/또는 가능한 챌린지들의 서브세트일 수 있다는 것에 주의한다.

[0070] 예시적인 인증 디바이스 및 거기에서의 동작 방법

[0071] [0076] 도 9는 각각의 전자 디바이스 내의 다수의 물리적으로 복제 불가능 기능으로부터의 응답들에 기초하여 전자 디바이스를 인증하도록 적응된 예시적인 인증 디바이스를 예시하는 블록도이다. 인증 디바이스(902)는 전자 디바이스(예를 들어, 칩, 반도체, 메모리 디바이스 등)에 질의하고, (예를 들어, 전자 디바이스로부터 획득된) 디바이스 식별자에 기초하여 전자 디바이스를 식별하고 전자 디바이스의 SRAM PUF 및 회로 지연 PUF에 대한 챌린지들을 수반한 질의를 수행함으로써 전자 디바이스를 인증하도록 시도하게 적응될 수 있다. 인증 디바이스(902)는 프로세싱 회로(904), 저장 디바이스(906), 통신 인터페이스(908) 및/또는 기계-판독 가능 매체(910)를 포함할 수 있다. 통신 인터페이스(908)는 인증 디바이스(902)가 하나 이상의 전자 디바이스들과 (예를 들어, 유선 또는 무선으로) 통신하도록 허용하는 전송기/수신기 회로(918)를 포함할 수 있다.

[0072] [0077] 프로세싱 회로(904)는 전자 디바이스로부터 고유한 디바이스 식별자를 획득하도록 적응되는 디바이스 식별자 회로/모듈(922)을 포함할 수 있다. 획득된 디바이스 식별자를 사용하여, 인증 회로/모듈(936)은 그 디바이스 식별자와 연관된 대응하는 챌린지/응답 정보에 대해 (저장 디바이스(906)의) 디바이스 식별자 데이터베이스(916)를 검사할 수 있다. SRAM PUF 검증 회로/모듈(924) 및 회로 지연 PUF 검증 회로/모듈(926)과 협력하는 인증 회로/모듈(936)은 그 후 전자 디바이스에 대응하는 챌린지들 중 하나 이상을 송신하고 챌린지에 대한 하나 이상의 응답들을 획득할 수 있다. 일 예에서, 회로 지연 PUF는 변조-방지 PUF일 수 있다는 것에 주의한다. 대조적으로, SRAM PUF는 다양한 공격들(예를 들어, FIB(Focused Ion Beam) 공격들, 회로 편집 공격들 등)에 취약한 것으로 확인되었다.

[0073] [0078] 챌린지들과 함께 응답들은 (저장 디바이스(906))의 SRAM PUF 데이터베이스(914) 및 (저장 디바이스(906))의 회로 지연 PUF 데이터베이스(912)로부터, 그 응답들이 예상된 응답에 정확히 매칭하는지(즉, 데이터베이스들(914, 916)에서 챌린지에 대응하는 응답들에 매칭하는지)를 각각 확인하기 위해 SRAM PUF 검증 회로/모듈(924) 및 회로 지연 PUF 검증 회로/모듈(926)에 의해 사용될 수 있다. 수신된 응답들이 이전에 저장된 대응하는 응답들에 매칭하는 경우, 인증 회로/모듈(936)은 전자 디바이스가 성공적으로 인증되었다고 결론을 내릴 수 있다. 이러한 성공적인 인증은 확률론적 매칭일 수 있으며, 여기서, 응답들의 임계 퍼센티지 또는 수가 정확히 매칭하는 한, 성공적인 매칭이 결론으로 내려질 수 있다.

[0074] [0079] 기계-판독 가능 매체(910)는 (예를 들어, 프로세싱 회로가 검증되고 있는 전자 디바이스로부터 디바이스 식별자를 획득하게 하기 위한) 디바이스 식별자 명령들(930), (예를 들어, 프로세싱 회로가 검증되고 있는 전자 디바이스의 SRAM PUF로부터의 응답들을 검증하게 하기 위한) SRAM PUF 검증 명령들(932), (예를 들어, 프로세싱 회로가 검증되고 있는 전자 디바이스의 회로 지연 PUF로부터의 응답들을 검증하게 하기 위한) 회로 지연 PUF 검증 명령들(934) 및/또는 SRAM PUF 및 회로 지연 PUF 검증 둘 다가 성공적인지를 확인하기 위한 인증 명령들(938)을 포함하거나 저장할 수 있다.

[0075] [0080] 데이터 수집기 디바이스(902)는 도 1 내지 도 6에서 예시된 단계들 또는 기능들 중 하나 이상을 수행하도록 적응될 수 있다.

[0076] [0081] 도 10은 복수의 물리적으로 복제 불가능 기능으로부터의 응답들에 기초하여 전자 디바이스를 인증하기 위해 인증 디바이스에서 동작하는 방법을 예시한다. 인증 디바이스는 배포 후 스테이지 동안 전자 디바이스와 연관된 디바이스 식별자를 획득(예를 들어, 요청 또는 수신)할 수 있다(1002). 인증 디바이스는 하나 이상의 챌린지들을 획득하고 전자 디바이스에 송신할 수 있다(1004). 예를 들어, 챌린지들은 모든 전자 디바이스들에 대해 활용되는 챌린지들의 미리 정의된 세트일 수 있다. 대안적으로, 챌린지들은 디바이스 식별자를 사용하여 데이터베이스로부터 획득된 전자 디바이스에 대한 챌린지들의 특정한 서브세트일 수 있다. 하나 이상의 챌린지들을 송신하는 결과로서, 인증 디바이스는 전자 디바이스로부터 하나 이상의 응답들을 수신할 수 있고, 하나 이상의 응답들은 전자 디바이스에서 두 개 이상의 별개의 타입들의 물리적으로 복제 불가능 기능들로부터 생성된 특성 정보를 포함한다(1006). 다양한 구현들에서, 인증 디바이스는 도 1, 도 2, 도 3, 도 4, 도 5 및/또는 도 6을 참조하여 예시되고 설명된 바와 같이 동작할 수 있다.

[0077] [0082] 디바이스 식별자는 전자 디바이스 특유의 미리-저장된 챌린지들 및 대응하는 응답들을 식별하는데 사용될 수 있다(1008). 인증 디바이스는 그 후 전자 디바이스에 대한 미리-저장된 응답들 및 수신된 하나 이상의 응답들을 비교함으로써 전자 디바이스를 인증할 수 있다(1010). 성공적인 인증은, 수신된 하나 이상의 응답들이 전자 디바이스에 대한 미리-저장된 응답들과 매칭할 때 발생한다. 성공적인 인증은 확률론적 매칭일 수 있으며, 여기서, 응답들의 임계 퍼센티지 또는 수가 정확히 매칭하는 한, 성공적인 매칭이 결론으로 내려질 수 있다. 이 프로세스는 복수의 전자 디바이스들 각각에 대해 반복될 수 있다. 물리적으로 복제 불가능 기능들이

각각의 전자 디바이스에 의해 사용되기 때문에, 동일한 챌린지가 모든 디바이스들에 대해 사용되는 경우조차도, 하나 이상의 응답들은 별개일 것이다.

[0078] 예시적인 전자 디바이스 및 거기에서의 동작 방법

[0079] [0083] 도 11은 다수의 물리적으로 복제 불가능 기능을 갖는 예시적인 전자 디바이스를 예시하는 블록도이다. 전자 디바이스(1102)는 칩, 반도체, 메모리 디바이스 등일 수 있고, 디바이스 식별자를 제공하고 전자 디바이스의 SRAM PUF 및 회로 지연 PUF에 대한 챌린지에 응답하도록 적응된다. 전자 디바이스(1102)는 프로세싱 회로(1104), (저장 디바이스의) 디바이스 식별자(1116), 지연-기반 PUF 회로(1112)(예를 들어, 복수의 오실레이터 링 회로들), (SRAM PUF로서 사용될 수 있는) 정적 랜덤 액세스 메모리(1116), 통신 인터페이스(1108) 및/또는 기계-판독 가능 매체(1110)를 포함할 수 있다. 통신 인터페이스(1108)는 전자 디바이스(1102)가 하나 이상의 데이터 수집기 및/또는 인증 디바이스들과 (예를 들어, 유선 또는 무선으로) 통신하도록 허용하는 전송기/수신기 회로(1118)를 포함할 수 있다.

[0080] [0084] 프로세싱 회로(1104)는 자신의 고유한 디바이스 식별자(1116)를 데이터 수집기 및/또는 인증 디바이스에 제공하도록 적응되는 디바이스 식별자 회로/모듈(1122)을 포함할 수 있다. 프로세싱 회로는 또한 수신된 챌린지에 대한 응답들을 획득하고 응답들을 데이터 수집기 디바이스 및 인증 디바이스에 송신하도록 적응되는 SRAM PUF 응답 회로/모듈(1124) 및 회로 지연 PUF 응답 회로/모듈(1126)을 포함할 수 있다. 일 예에서, 회로 지연 PUF는 변조-방지 PUF일 수 있다는 것에 주의한다. 대조적으로, SRAM PUF는 다양한 공격들(예를 들어, FIB(Focused Ion Beam) 공격들, 회로 편집 공격들 등)에 취약한 것으로 확인되었다.

[0081] [0085] SRAM PUF 응답 회로/모듈(1124)은 응답들을 획득하기 위해 수신된 챌린지들을 정적 랜덤 액세스 메모리(1114)에 송신할 수 있다. 예를 들어, 응답들은 정적 랜덤 액세스 메모리(1114)의 하나 이상의 메모리 셀들의 초기화되지 않은 상태들일 수 있다. 유사하게, 회로 지연 PUF 응답 회로/모듈(1126)은 응답들을 획득하기 위해 수신된 챌린지들을 지연-기반 PUF 회로(1112)에 송신할 수 있다.

[0082] [0086] 기계-판독 가능 매체(1110)는 (예를 들면, 프로세싱 회로가 전자 디바이스에 대한 디바이스 식별자(1116)를 획득하게 하기 위한) 디바이스 식별자 명령들(1130), (예를 들면, 프로세싱 회로가 전자 디바이스의 정적 랜덤 액세스 메모리(1114)로부터 응답들을 획득하게 하기 위한) SRAM PUF 응답 명령들(1132), 및/또는 (예를 들어, 프로세싱 회로가 전자 디바이스의 회로 지연 PUF로부터 응답들을 획득하게 하기 위한) 회로 지연 PUF 응답 명령들(1134)을 포함하거나 저장할 수 있다.

[0083] [0087] 전자 디바이스(1102)는 도 1 내지 도 6에서 예시된 단계들 또는 기능들 중 하나 이상을 수행하도록 적응될 수 있다.

[0084] [0088] 도 12는 복수의 물리적으로 복제 불가능 기능으로부터의 응답들에 기초하여 인증 디바이스를 통해 스스로를 인증하기 위해 전자 디바이스에서 동작하는 방법을 예시한다. 전자 디바이스는 배포 전 또는 제조 단계 동안 하나 이상의 챌린지들을 수신하고 하나 이상의 대응하는 응답들을 제공하였을 수 있다.

[0085] [0089] 전자 디바이스는 전자 디바이스 내의 복수의 메모리 셀들을 사용하여 제 1 물리적으로 복제 불가능 기능을 구현한다(1204). 일 예에서, 제 1 물리적으로 복제 불가능 기능은 챌린지에 대한 응답으로서 하나 이상의 메모리 셀들에 대한 초기화되지 않은 메모리 셀 상태들을 사용할 수 있다.

[0086] [0090] 전자 디바이스는 또한 전자 디바이스 내의 복수의 회로 지연 기반 경로들을 사용하여 제 2 물리적으로 복제 불가능 기능을 구현할 수 있다(1206). 일 예에서, 복수의 회로 지연 기반 경로들은 변조-방지적이다. "변조-방지적(tamper-resistant)"이란 용어는, PUF 응답 또는 출력을 예측, 확인 및/또는 판독하기 위해 그것을 변조하기 위한 시도가 이루어질 때, 응답 및/또는 출력이 변경되게 하는 PUF의 구현 또는 타입을 지칭한다. 예를 들어, 링 오실레이터 또는 회로 지연 경로 타입 오실레이터를 물리적으로 변조하려는 시도는 링 오실레이터 또는 회로 지연 경로에 대한 응답이 변경(예를 들어, 출력 주파수 변경들)되게 할 것이다.

[0087] [0091] 챌린지는 외부 서버로부터 수신될 수 있다(1208). 챌린지는 (a) 제 1 물리적으로 복제 불가능 기능에 입력되는 챌린지를 마스킹/언마스킹하도록, (b) 제 1 물리적 복제 불가능 기능에 입력되는 챌린지를 생성하도록, 또는 (c) 제 1 물리적으로 복제 불가능 기능으로부터 출력되는 응답을 마스킹하도록 제 2 물리적으로 복제 불가능 기능으로부터의 제 1 응답을 이용함으로써 제 1 물리적 복제 불가능 기능에 적용될 수 있다(1210). 일 예에서, 제 1 챌린지는 복수의 메모리 셀들 내에서 메모리 어드레스들을 식별할 수 있다. 다른 예에서, 챌린지는 제 2 물리적으로 복제 불가능 기능의 복수의 링 오실레이터들로부터 2개의 링 오실레이터들을 선택할 수 있으며, 2개의 링 오실레이터들 사이의 주파수 차이로 응답한다. 챌린지는 전자 디바이스의 인증 프

로세스, 전자 디바이스의 식별 프로세스, 및/또는 전자 디바이스 내의 키 생성 프로세스 중 적어도 하나의 부분으로서 수신될 수 있다.

[0088] [0092] 제 2 물리적으로 복제 불가능 기능으로부터의 제 1 응답 및/또는 제 1 물리적으로 복제 불가능 기능으로부터의 제 2 응답이 그 후 외부 서버에 송신될 수 있다(1212). 외부 서버는 제 1 물리적으로 복제 불가능 기능에 대한 챌린지들 및 응답들의 제 1 데이터베이스 및 제 2 물리적으로 복제 불가능 기능에 대한 챌린지들 및 응답들의 제 2 데이터베이스를 포함할 수 있고, 외부 서버는 전자 디바이스에 챌린지를 송신하고 제 2 응답에 기초하여 전자 디바이스를 인증 또는 식별한다.

[0089] [0093] 응답이 외부 서버에 의해 성공적으로 검증되었다는 표시자가 수신될 수 있다(1214). 예를 들면, 성공적인 인증 시에, 전자 디바이스는 그것이 네트워크 및/또는 데이터에 대한 액세스를 얻었다는 표시자를 수신할 수 있다.

[0090] [0094] 일 예에서, 챌린지는 제 1 물리적으로 복제 불가능 기능에 대한 제 1 챌린지 및 제 2 물리적으로 복제 불가능 기능에 대한 제 2 챌린지를 포함할 수 있다. 예를 들면, 제 1 챌린지는 (도 3에서 예시된 바와 같이) 제 2 챌린지에 대한 예상된 응답에 의해 마스킹되는 챌린지일 수 있다. 다른 인스턴스에서, 제 1 챌린지는 (도 4에서 예시된 바와 같이) 제 1 물리적으로 복제 불가능 기능에 의한 프로세싱 이전에, 제 2 물리적으로 복제 불가능 기능으로부터의 제 1 응답에 의해 수정될 수 있다.

[0091] [0095] 또 다른 예에서, 수신된 챌린지는 (도 5에 예시된 바와 같이) 제 2 응답을 생성하기 위해 제 1 물리적으로 복제 불가능 기능에 의해 제 2 챌린지로서 추후에 사용되는 제 1 응답을 생성하도록 제 2 물리적으로 복제 불가능 기능에 의해 사용될 수 있다.

[0092] [0096] 다른 구현에서, 챌린지는 제 1 물리적으로 복제 불가능 기능에 대한 제 1 챌린지 및 제 2 물리적으로 복제 불가능 기능에 대한 제 2 챌린지를 포함할 수 있고, 제 2 챌린지는 (도 6에서 예시된 바와 같이) 제 1 물리적으로 복제 불가능 기능으로부터의 제 2 응답을 마스킹하는데 사용되는 제 1 응답을 생성하도록 제 2 물리적으로 복제 불가능 기능에 의해 사용될 수 있다. 이 방법은 추가로, (a) 중간 응답을 획득하기 위해 제 2 물리적으로 복제 불가능 기능으로부터의 제 1 응답을 해싱하는 단계; 및/또는 (b) 중간 응답을 사용하여 제 2 응답을 마스킹하는 단계를 포함할 수 있다.

[0093] [0097] 일 예에서, 미리-저장된 디바이스 식별자는 또한 전자 디바이스 내에서 미리 프로비저닝될 수 있다(1202). 그것은 (a) 챌린지가 수신되기 이전에, 또는 (b) 제 2 응답의 송신과 동시에, 전자 디바이스로부터 외부 서버에 미리-저장된 디바이스 식별자를 송신할 수 있다. 디바이스 식별자는 전자 디바이스를 고유하게 식별한다.

[0094] [0098] 도 1 내지 도 12에서 예시된 컴포넌트들, 단계들, 피처들 및/또는 기능들 중 하나 이상은 단일 컴포넌트, 단계, 피처 또는 기능 내로 재배열 및/또는 결합되거나 또는 여러 컴포넌트들, 단계들, 또는 기능들에서 실현될 수 있다. 부가적인 엘리먼트들, 컴포넌트들, 단계들, 및/또는 기능들은 또한 본 발명으로부터 벗어남 없이 부가될 수 있다. 도 1 내지 도 7, 도 9 및 도 11에서 예시된 장치, 디바이스들 및/또는 컴포넌트들은 도 8, 도 10, 및 도 12에서 설명된 방법들, 피처들 또는 단계들 중 하나 이상을 수행하도록 구성될 수 있다. 여기서 설명되는 알고리즘은 또한 효율적으로 소프트웨어에서 구현되고 및/또는 하드웨어에 임베딩될 수 있다.

[0095] [0099] 또한, 본 개시의 일 양상에서, 도 7, 도 9 및 도 11에서 예시된 프로세싱 회로(704, 904 및 1104)는 도 8, 도 10, 및 도 12에서 각각 설명된 알고리즘들, 방법들, 및/또는 단계들을 수행하도록 특별히 설계 및/또는 하드-와이어링되는 특수 프로세서들(예를 들어, 주문형 집적 회로(예를 들어, ASIC))일 수 있다. 따라서, 이러한 특수 프로세서(예를 들어, ASIC)는 도 8, 도 10 및 도 12에서 설명된 알고리즘들, 방법들 및/또는 단계들을 실행하는 수단의 일례일 수 있다.

[0096] [00100] 또한, 본 개시의 양상들은 흐름 차트, 흐름도, 구조도, 또는 블록도로서 도시되는 프로세스로서 설명될 수 있다는 것이 주의된다. 흐름 차트가 순차적 프로세스로서 동작들을 설명할 수 있지만, 동작들 대부분은 병렬로 또는 동시에 수행될 수 있다. 또한, 동작들의 순서는 재배열될 수 있다. 프로세스는 그의 동작들이 완료될 때, 종료된다. 프로세스는 방법, 함수, 프로시저, 서브루틴, 서브프로그램 등에 대응할 수 있다. 프로세스가 함수에 대응할 때, 그의 종료는 호출 함수 또는 메인 함수로의 함수의 복귀에 대응한다.

[0097] [00101] 또한, 저장 매체는 판독-전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 자기 디스크 저장 매체들, 광학 저장 매체들, 플래시 메모리 디바이스들을 포함하는, 데이터를 저장하기 위한 하나 이상의 디바이스들 및/또는

정보를 저장하기 위한 다른 기계-판독 가능 매체들 및 프로세서-판독 가능 매체들 및/또는 컴퓨터-판독 가능 매체들을 나타낼 수 있다. "기계-판독 가능 매체", "컴퓨터-판독 가능 매체" 및/또는 "프로세서-판독 가능 매체"란 용어들은 휴대식 또는 고정식 저장 디바이스들, 광학 저장 디바이스들, 및 명령(들) 및/또는 데이터를 저장, 포함 또는 전달할 수 있는 다양한 다른 매체들과 같은 비-일시적 매체들을 포함할 수 있지만, 이것으로 한정되지 않는다. 따라서 여기서 설명되는 다양한 방법들은 "기계-판독 가능 매체", "컴퓨터-판독 가능 매체" 및/또는 "프로세서-판독 가능 매체"에 저장되고 하나 이상의 프로세서들, 기계들 및/또는 디바이스들에 의해 실행될 수 있는 명령들 및/또는 데이터에 의해 완전히 또는 부분적으로 구현될 수 있다.

[0098] [00102] 또한, 본 개시의 양상들은 하드웨어, 소프트웨어, 펌웨어, 미들웨어, 마이크로코드, 또는 이들의 임의의 결합에 의해 구현될 수 있다. 소프트웨어, 펌웨어, 미들웨어 또는 마이크로코드로 구현될 때, 필요한 작업들을 수행하기 위한 프로그램 코드 또는 코드 세그먼트들은 저장 매체 또는 다른 저장소(들)과 같은 기계-판독 가능 매체에 저장될 수 있다. 프로세서는 필요한 작업들을 수행할 수 있다. 코드 세그먼트는, 프로시저, 함수, 서브프로그램, 프로그램, 루틴, 서브루틴, 모듈, 소프트웨어 패키지, 클래스, 또는 명령들, 데이터 구조들 또는 프로그램문들의 임의의 결합을 나타낼 수 있다. 코드 세그먼트는 정보, 데이터, 아규멘트들, 파라미터들 또는 메모리 콘텐츠들을 전달 및/또는 수신함으로써 다른 코드 세그먼트 또는 하드웨어 회로에 커플링될 수 있다. 정보, 아규멘트들, 파라미터들, 데이터 등은 메모리 공유, 메시지 전달, 토큰 전달, 네트워크 전송 등을 포함하는 임의의 적합한 수단을 통해 전달, 포워딩, 또는 전송될 수 있다.

[0099] [00103] 여기서 개시된 예들과 관련하여 설명된 다양한 예시적인 로직 블록, 모듈, 회로들, 엘리먼트들 및/또는 컴포넌트들은, 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적 회로(ASIC), 필드 프로그래밍 가능 게이트 어레이(FPGA), 또는 다른 프로그래밍 가능 로직 컴포넌트, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트, 또는 여기서 설명된 기능을 수행하도록 설계된 이들의 임의의 결합으로 구현 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로, 프로세서는 임의의 종래 프로세서, 제어기, 마이크로 제어기, 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 컴포넌트들의 조합, 예를 들어, DSP와 마이크로프로세서의 조합, 다수의 마이크로프로세서들, DSP 코어와 결합된 하나 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로 구현될 수 있다.

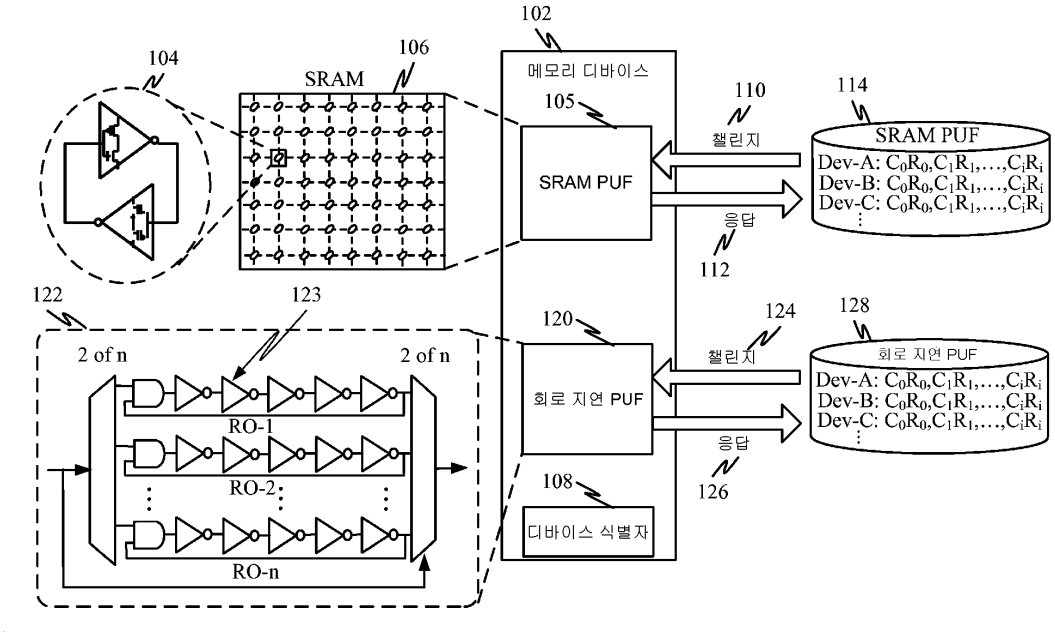
[0100] [00104] 여기에 개시된 예들과 관련하여 설명된 방법들 또는 알고리즘들은 프로세싱 유닛, 프로그래밍 명령들 또는 다른 지시들의 형태로, 직접 하드웨어로, 프로세서에 의해 실행 가능한 소프트웨어 모듈로 또는 둘 다의 결합으로 실현될 수 있고, 단일 디바이스에 포함되거나 또는 여러 디바이스들에 걸쳐 분산될 수 있다. 소프트웨어 모듈은, RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 착탈식 디스크, CD-ROM, 또는 당업계에 공지된 저장 매체의 임의의 다른 형태에 상주할 수 있다. 저장 매체는 프로세서와 결합될 수 있어서, 프로세서는 저장 매체로부터 정보를 판독하고, 그리고 저장 매체에 정보를 기록할 수 있다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다.

[0101] [00105] 여기서 개시된 양상들과 관련하여 설명된 다양한 예시적인 로직 블록, 모듈, 회로, 및 알고리즘 단계는, 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이 둘의 조합으로 구현될 수 있다는 것을 당업자는 추가로 이해할 것이다. 하드웨어와 소프트웨어의 이러한 상호 교환 가능성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들이 이들의 기능성의 관점에서 일반적으로 상술되었다. 이러한 기능성이 하드웨어 또는 소프트웨어로 구현되는지 여부는 전체 시스템에 부과된 설계 제약들 및 특정 애플리케이션에 의존한다.

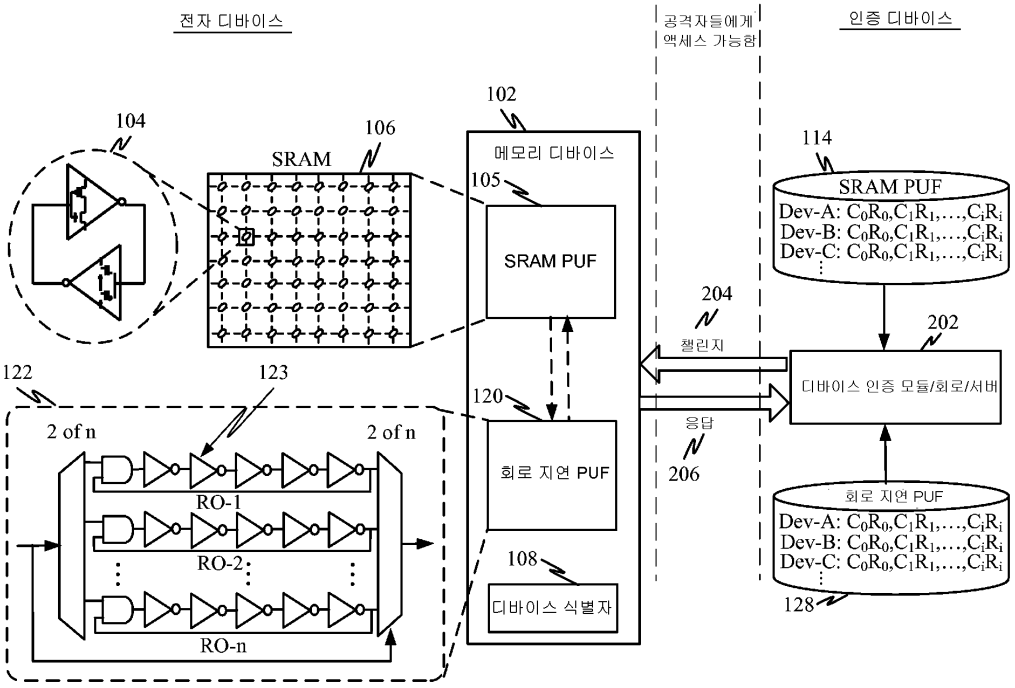
[0102] [00106] 여기서 설명되는 본 발명의 다양한 피처들은 본 발명으로부터 벗어남 없이 다른 시스템에서 구현될 수 있다. 본 개시의 전술한 양상들은 단지 예시이며 본 발명을 제한한 것으로서 해석되지 않는다는 것이 주의되어야 한다. 본 개시의 양상들의 설명은 예시하는 것으로 의도되며, 청구항들의 범위를 제한하지 않는다. 따라서, 본 교시들은 다른 타입들의 장치들에 쉽게 적용될 수 있고, 많은 대안들, 수정들 및 변동들이 당업자에게 명백하게 될 것이다.

## 도면

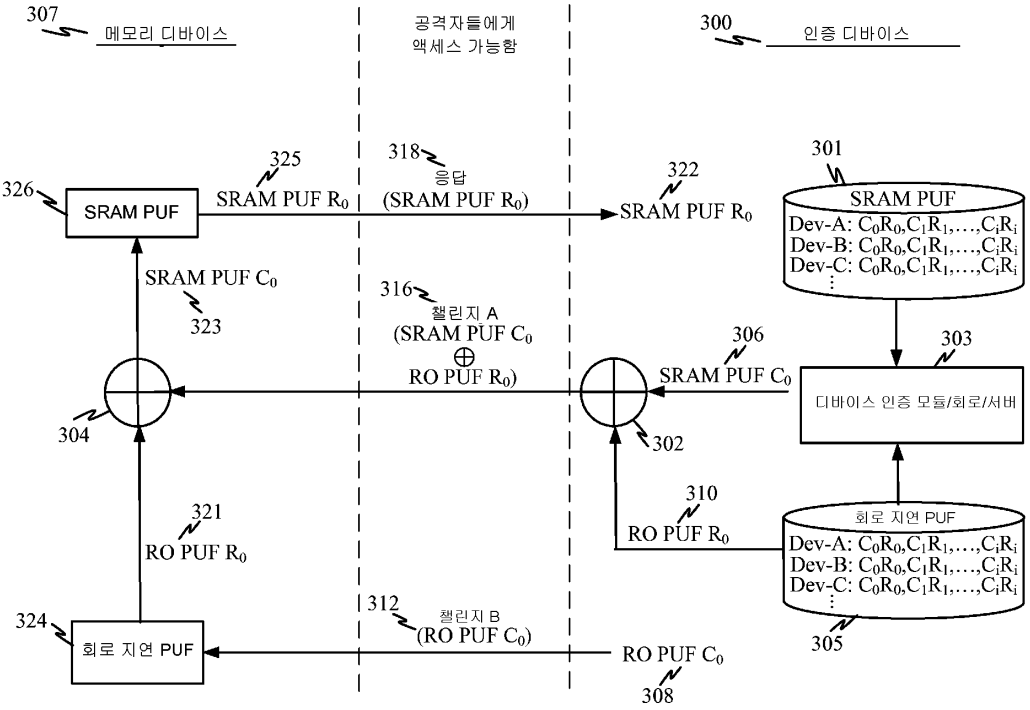
### 도면1


102
104
106
SRAM
메모리 디바이스
105
SRAM PUF
110
챌린지
114
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
응답
112
122
123
120
124
128
2 of n
2 of n
회로 지연 PUF
챌린지
회로 지연 PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
RO-1
RO-2
응답
126
108
디바이스 식별자
RO-n

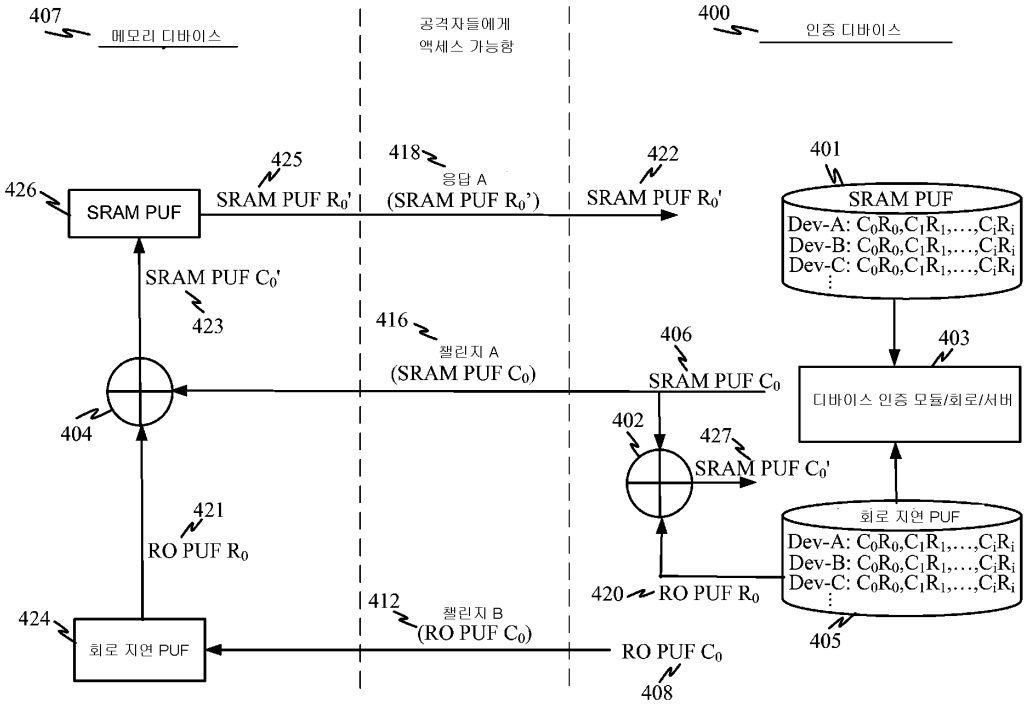
### 도면2


전자 디바이스
공격자들에게 액세스 가능함
인증 디바이스
102
104
106
SRAM
메모리 디바이스
105
SRAM PUF
114
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
204
챌린지
202
디바이스 인증 모듈/회로/서버
122
123
120
2 of n
2 of n
회로 지연 PUF
응답
206
RO-1
RO-2
회로 지연 PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
108
디바이스 식별자
128
RO-n

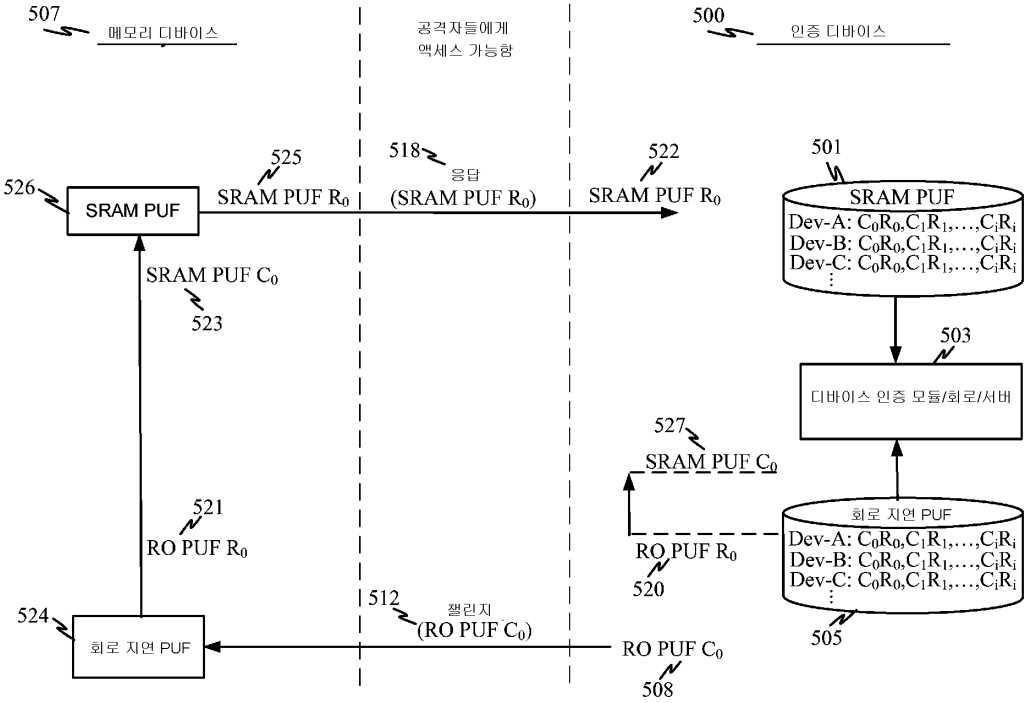
도면3


307
메모리 디바이스
공격자들에게
액세스 가능함
300
인증 디바이스
326
SRAM PUF
325
SRAM PUF $R_0$
318
응답
(SRAM PUF $R_0$)
322
SRAM PUF $R_0$
301
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
SRAM PUF $C_0$
323
316
챌린지 A
(SRAM PUF $C_0$ ⊕ RO PUF $R_0$)
306
SRAM PUF $C_0$
303
디바이스 인증 모듈/회로/서버
304
302
310
RO PUF $R_0$
회로 지연 PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
321
RO PUF $R_0$
312
챌린지 B
(RO PUF $C_0$)
324
회로 지연 PUF
RO PUF $C_0$
308
305

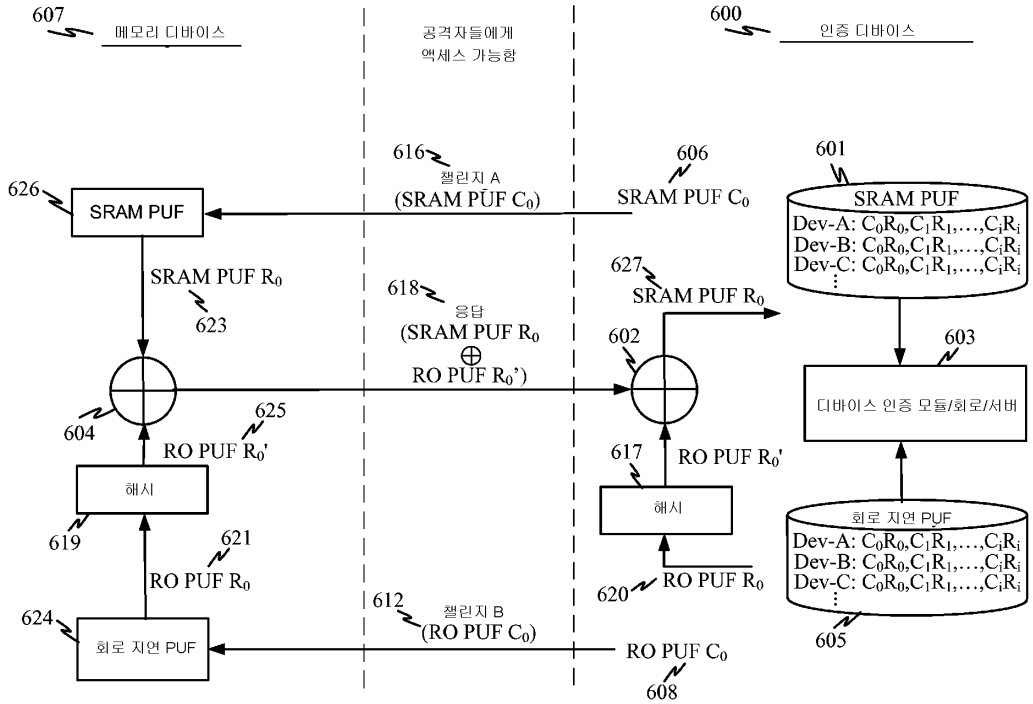
도면4


407
메모리 디바이스
공격자들에게
액세스 가능함
400
인증 디바이스
426
SRAM PUF
425
SRAM PUF $R_0$'
418
응답 A
(SRAM PUF $R_0$')
422
SRAM PUF $R_0$'
401
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
SRAM PUF $C_0$'
423
416
챌린지 A
(SRAM PUF $C_0$)
406
SRAM PUF $C_0$
403
디바이스 인증 모듈/회로/서버
404
402
427
SRAM PUF $C_0$'
421
RO PUF $R_0$
회로 지연 PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
420
RO PUF $R_0$
412
챌린지 B
(RO PUF $C_0$)
424
회로 지연 PUF
RO PUF $C_0$
408
405

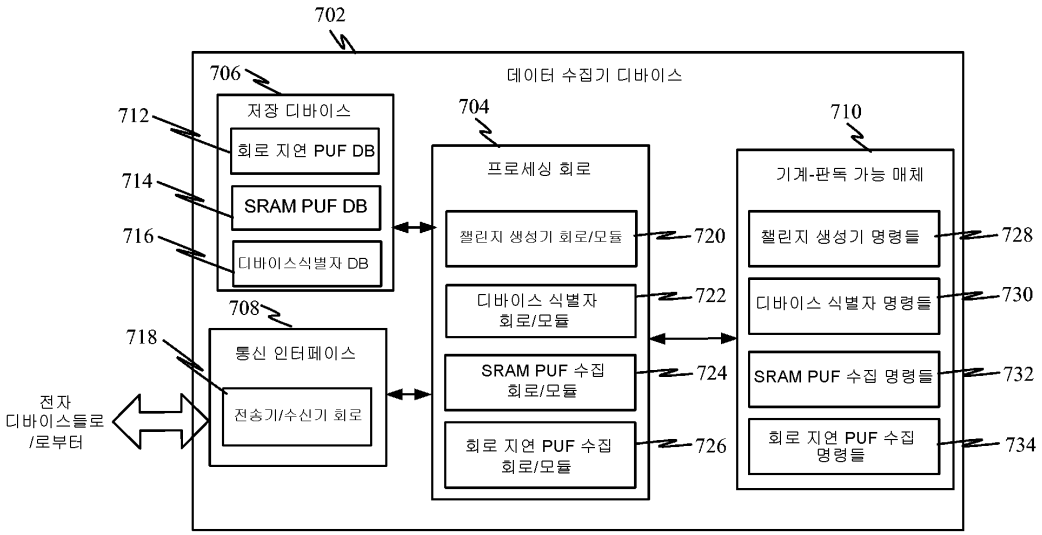
도면5


507
메모리 디바이스
공격자들에게
액세스 가능함
500
인증 디바이스
526
SRAM PUF
525
SRAM PUF $R_0$
518
응답
(SRAM PUF $R_0$)
522
SRAM PUF $R_0$
501
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
503
디바이스 인증 모듈/회로/서버
SRAM PUF $C_0$
523
527
SRAM PUF $C_0$
회로 지연 PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
521
RO PUF $R_0$
RO PUF $R_0$
520
524
회로 지연 PUF
512
챌린지
(RO PUF $C_0$)
505
RO PUF $C_0$
508

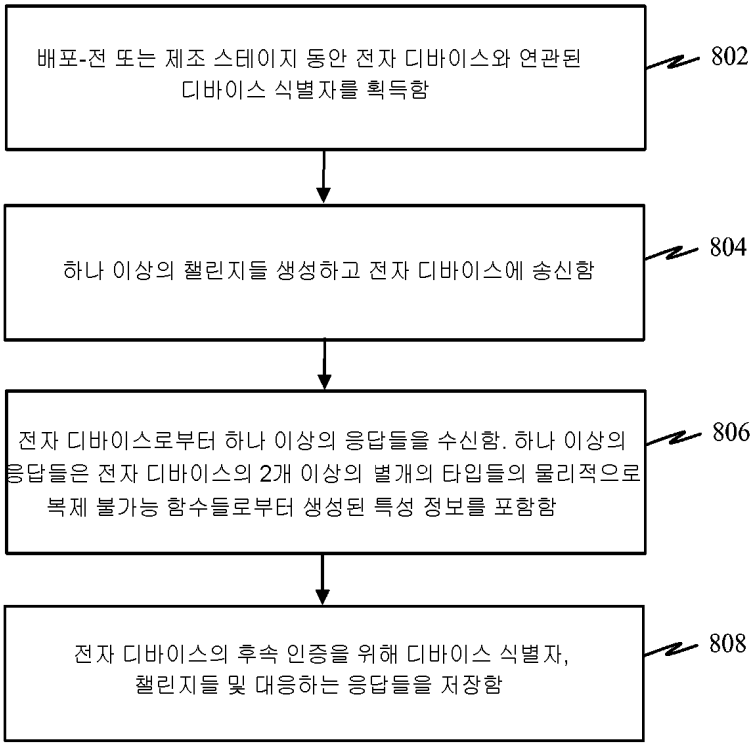
도면6


607
메모리 디바이스
공격자들에게
액세스 가능함
600
인증 디바이스
616
챌린지 A
(SRAM PUF $C_0$)
606
SRAM PUF $C_0$
601
SRAM PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
626
SRAM PUF
627
SRAM PUF $R_0$
SRAM PUF $R_0$
623
618
응답
(SRAM PUF $R_0$
⊕
RO PUF $R_0$')
602
603
디바이스 인증 모듈/회로/서버
604
625
RO PUF $R_0$'
617
RO PUF $R_0$'
해시
해시
619
621
회로 지연 PUF
Dev-A: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-B: $C_0R_0,C_1R_1,\ldots,C_iR_i$
Dev-C: $C_0R_0,C_1R_1,\ldots,C_iR_i$
RO PUF $R_0$
620
RO PUF $R_0$
624
회로 지연 PUF
612
챌린지 B
(RO PUF $C_0$)
605
RO PUF $C_0$
608

도면7

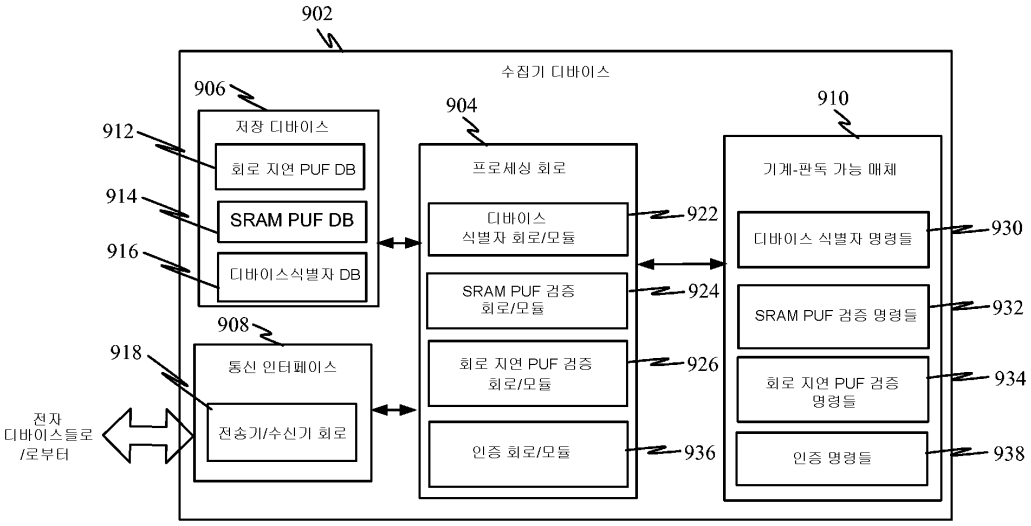



도면8

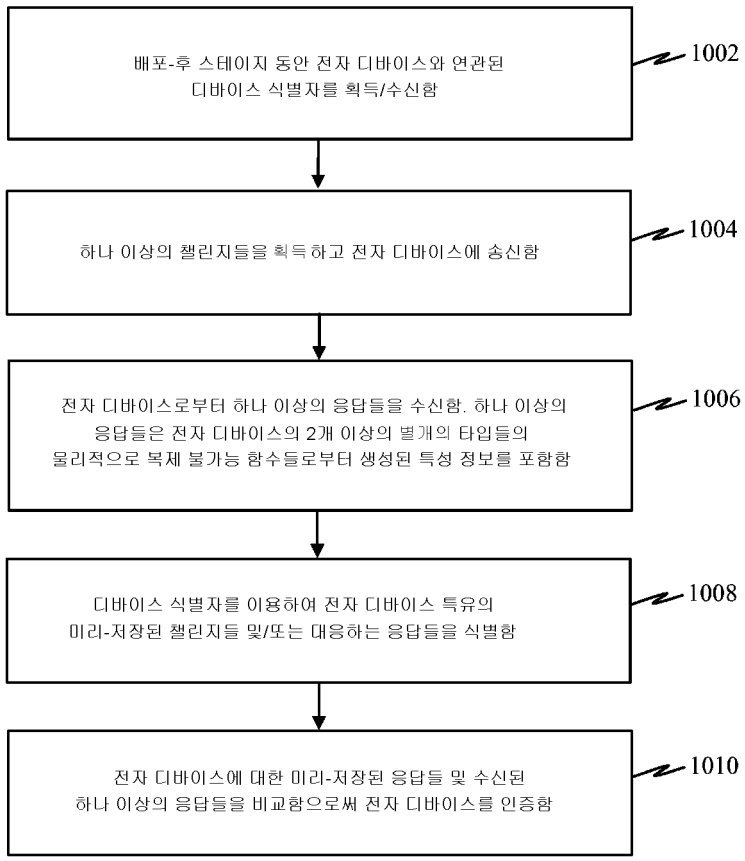



데이터 수집기 디바이스 상의 동작 방법

도면9

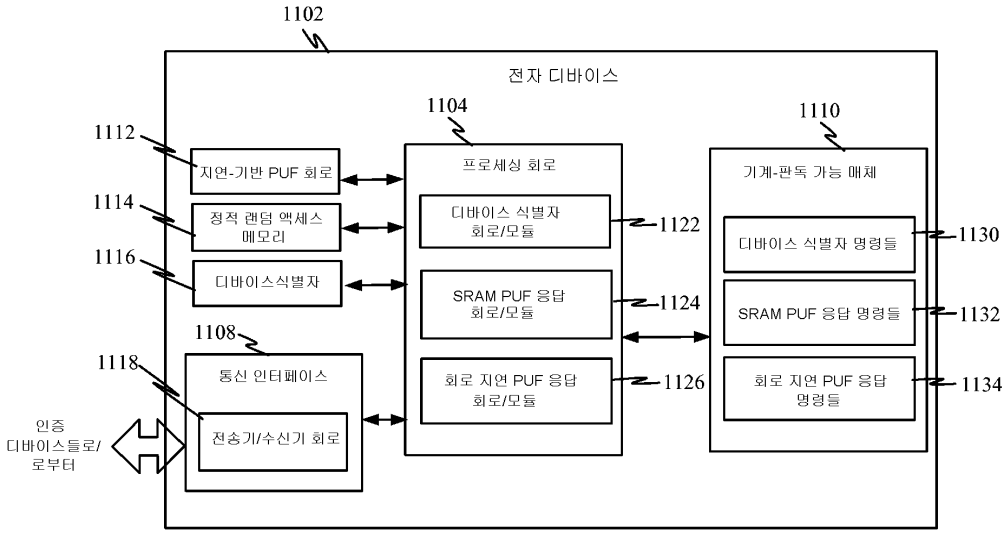



도면10

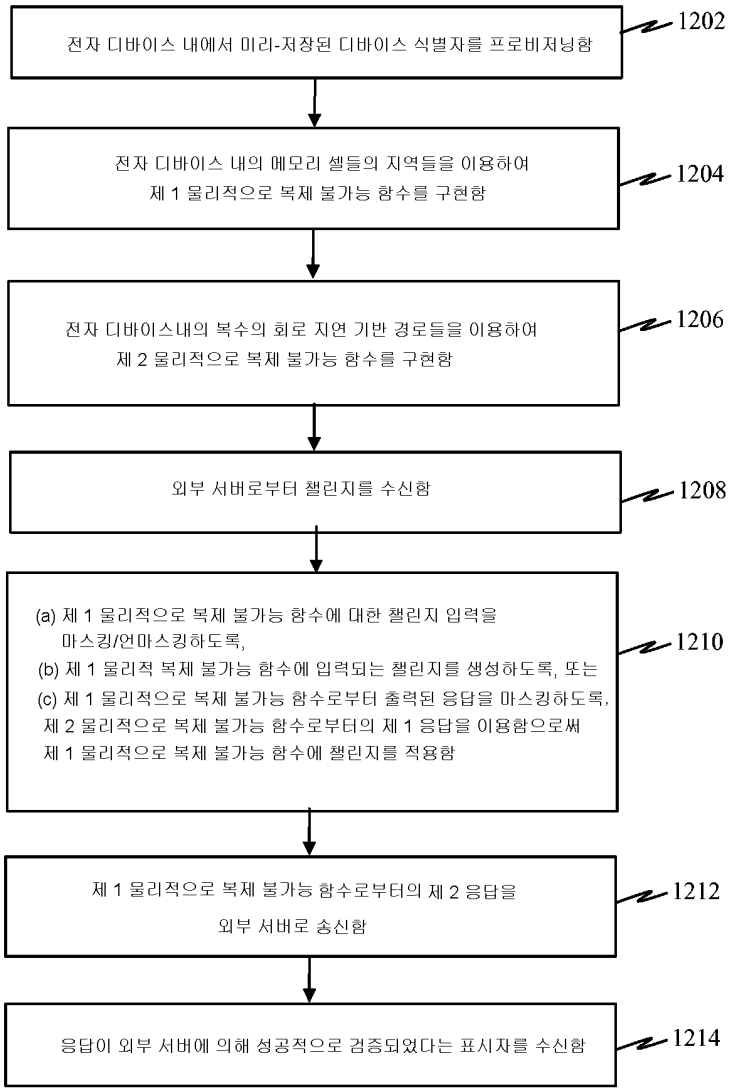



인증 디바이스 상의 동작 방법

도면11


1102
전자 디바이스
1104
1110
1112
지연-기반 PUF 회로
프로세싱 회로
기계-판독 가능 매체
1114
정적 랜덤 액세스 메모리
디바이스 식별자 회로/모듈
1122
디바이스 식별자 명령들
1130
1116
디바이스식별자
SRAM PUF 응답 회로/모듈
1124
SRAM PUF 응답 명령들
1132
1108
1118
통신 인터페이스
회로 지연 PUF 응답 회로/모듈
1126
회로 지연 PUF 응답 명령들
1134
인증 디바이스들로/로부터
전송기/수신기 회로

도면12




전자 디바이스에 의한 동작 방법