(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0152322
(43) 공개일자 2023년11월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3278 (2013.01)
H04L 9/0866 (2013.01)
(21) 출원번호 10-2022-0051917
(22) 출원일자 2022년04월27일
심사청구일자 2022년04월27일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
서울대학교산학협력단
서울특별시 관악구 관악로 1 (신림동)
(72) 발명자
신형순
서울특별시 서초구 반포대로5길 65, 102동 301호 (서초동, 아이파크빌)
최윤영
서울특별시 서대문구 봉원사길 38, 203호(대신동)
(뒷면에 계속)
(74) 대리인
특허법인 무한

전체 청구항 수 : 총 20 항

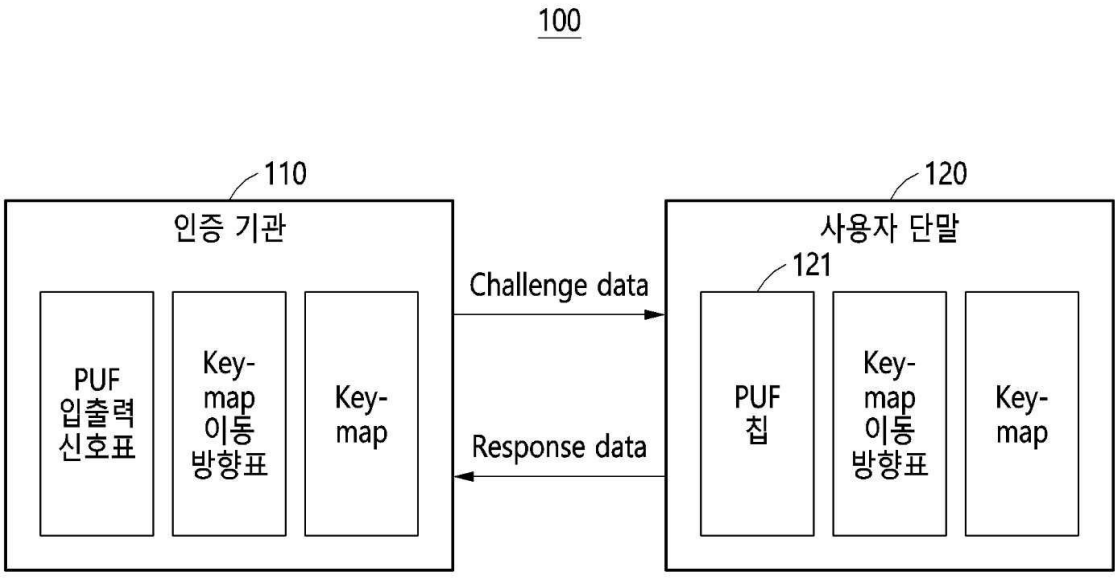
(54) 발명의 명칭 **물리적 복제 방지 기능을 이용한 사용자 단말의 인증 방법 및 인증 장치**

(57) 요 약

물리적 복제 방지 기능을 이용한 사용자 단말의 인증 방법 및 인증 장치가 개시된다. 서버가 수행하는 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법은 PUF 입출력 신호표에 기초하여 사용자 단말의 인증을 위한 첼린지(Challenge) 데이터를 상기 사용자 단말로 전송하는 단계; 상기 첼린

(뒷면에 계속)

대 표 도 - 도1



지 데이터에 대응하여 상기 PUF 입출력 신호표로부터 결정된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하는 단계; 상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 첼린지 데이터에 대응하는 리스폰스 데이터를 결정하는 단계; 및 상기 결정된 리스폰스 데이터와 상기 첼린지 데이터에 대응하여 상기 사용자 단말로부터 수신된 리스폰스 데이터를 비교하는 단계를 포함하고, 상기 사용자 단말로부터 수신된 리스폰스 데이터는 상기 첼린지 데이터를 상기 사용자 단말에 배치된 PUF 칩에 입력하여 도출된 PUF 출력 신호를 상기 서버가 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵에 적용함으로써 결정될 수 있다.

(52) CPC특허분류
H04L 2209/12 (2013.01)
H04L 2209/20 (2013.01)

(72) 발명자
선우경
서울특별시 서대문구 신촌역로 17(대현동)

이정원
인천광역시 부평구 부흥로 246(부평동, 동아아파트)

이 발명을 지원한 국가연구개발사업
과제고유번호 1345331993
과제번호 2020R1I1A1A01065622
부처명 교육부
과제관리(전문)기관명 한국연구재단
연구사업명 이공학학술연구기반구축(R&D)
연구과제명 재구성 가능한 3D 멤리스터 PUF 회로를 이용한 하드웨어 보안 시스템 개발
기 여 율 1/2
과제수행기관명 서울대학교
연구기간 2021.03.01 ~ 2022.02.28
이 발명을 지원한 국가연구개발사업
과제고유번호 1345332839
과제번호 2021R1I1A1A01042218
부처명 교육부
과제관리(전문)기관명 한국연구재단
연구사업명 이공학학술연구기반구축(R&D)
연구과제명 하드웨어 보안 향상을 위한 물리적 복제 방지 기술 기반 변형 블룸 필터 구조 개발에 관한 연구
기 여 율 1/2
과제수행기관명 서울대학교
연구기간 2021.06.01 ~ 2022.02.28

명 세 서

청구범위

청구항 1

서버가 수행하는 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법에 있어서,

PUF 입출력 신호표에 기초하여 사용자 단말의 인증을 위한 첼린지(Challenge) 데이터를 상기 사용자 단말로 전송하는 단계;

상기 첼린지 데이터에 대응하여 상기 PUF 입출력 신호표로부터 결정된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하는 단계;

상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 첼린지 데이터에 대응하는 리스폰스 데이터를 결정하는 단계; 및

상기 결정된 리스폰스 데이터와 상기 첼린지 데이터에 대응하여 상기 사용자 단말로부터 수신된 리스폰스 데이터를 비교하는 단계

를 포함하고,

상기 사용자 단말로부터 수신된 리스폰스 데이터는,

상기 첼린지 데이터를 상기 사용자 단말에 배치된 PUF 칩에 입력하여 도출된 PUF 출력 신호를 상기 서버가 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵에 적용함으로써 결정되는 사용자 단말의 인증 방법.

청구항 2

제1항에 있어서,

상기 이동 방향표는,

상기 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트(Bit) 수가 조정되는 사용자 단말의 인증 방법.

청구항 3

제2항에 있어서,

상기 키맵에서 키의 이동 횟수는,

상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 상기 단위 비트 수에 기초하여 제로 패딩(Zero padding)을 수행하거나 상기 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 조정되는 사용자 단말의 인증 방법.

청구항 4

제2항에 있어서,

상기 리스폰스 데이터를 결정하는 단계는,

상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 추가 정보를 조합함으로써 리스폰스 데이터를 결정하는 사용자 단말의 인증 방법.

청구항 5

제1항에 있어서,

상기 키맵에 포함된 키의 이동 경로를 추출하는 단계는,

상기 사용자 단말에 대한 이전 인증 정보, PUF 출력 신호 및 시간 정보 중 적어도 하나 이상의 정보에 대한 조합을 통해 결정된 키맵의 좌표를 상기 키의 이동 경로를 추출하기 위한 시작 위치로 결정하는 사용자 단말의 인증 방법.

청구항 6

제5항에 있어서,

상기 키맵에 포함된 키의 이동 경로를 추출하는 단계는,

상기 첼린지 데이터에 대응하는 PUF 출력 신호를 상기 키맵의 이동 방향표에 적용하여 결정된 키가 상기 키맵의 범위를 벗어나는 경우, 상기 시작 위치를 미리 설정된 규칙을 통해 재결정하거나, 상기 결정된 키가 위치한 방향으로 동일한 키맵을 복사하여 확장하는 사용자 단말의 인증 방법.

청구항 7

제1항에 있어서,

상기 리스폰스 데이터의 비트 수는,

상기 키맵에 포함된 키가 나타낼 수 있는 단위 정보의 비트 수 및 상기 키맵에서 키의 이동 횟수에 따라 조절되는 사용자 단말의 인증 방법.

청구항 8

제1항에 있어서,

상기 사용자 단말의 인증에 대한 보안 강화를 위해 상기 키맵의 이동 방향표 또는 키맵을 상기 사용자 단말과 동일한 방법에 따라 업데이트 하는 단계

를 더 포함하는 사용자 단말의 인증 방법.

청구항 9

사용자 단말이 수행하는 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법에 있어서,

서버로부터 수신된 첼린지 데이터를 PUF 칩에 입력함으로써 PUF 출력 신호를 식별하는 단계;

상기 식별된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하는 단계; 및

상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 첼린지 데이터에 대응하는 리스폰스 데이터를 결정하는 단계

를 포함하고,

상기 결정된 리스폰스 데이터는,

상기 서버가 첼린지 데이터에 대응하는 PUF 출력 신호를 이용하여 결정한 리스폰스 데이터와의 비교를 통해 상기 사용자 단말의 인증 결과를 도출하는데 이용되고,

상기 서버를 통해 결정되는 리스폰스 데이터는,

상기 사용자 단말이 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵을 통해 결정되는 사용자 단말의 인증 방법.

청구항 10

제9항에 있어서,

상기 이동 방향표는,

상기 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트(Bit) 수가 조정되는 사용자 단말의 인증 방법.

청구항 11

제10항에 있어서,

상기 키맵에서 키의 이동 횟수는,

상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 상기 단위 비트 수에 기초하여 제로 패딩(Zero padding)을 수행하거나 상기 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 조정되는 사용자 단말의 인증 방법.

청구항 12

제10항에 있어서,

상기 리스폰스 데이터를 결정하는 단계는,

상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 추가 정보를 조합함으로써 리스폰스 데이터를 결정하는 사용자 단말의 인증 방법.

청구항 13

제9항에 있어서,

상기 키맵에 포함된 키의 이동 경로를 추출하는 단계는,

상기 사용자 단말에 대한 이전 인증 정보, PUF 출력 신호 및 시간 정보 중 적어도 하나 이상의 정보에 대한 조합을 통해 결정된 키맵의 좌표를 상기 키의 이동 경로를 추출하기 위한 시작 위치로 결정하는 사용자 단말의 인증 방법.

청구항 14

제13항에 있어서,

상기 키맵에 포함된 키의 이동 경로를 추출하는 단계는,

상기 첼린지 데이터에 대응하는 PUF 출력 신호를 상기 키맵의 이동 방향표에 적용하여 결정된 키가 상기 키맵의 범위를 벗어나는 경우, 상기 시작 위치를 미리 설정된 규칙을 통해 재결정하거나, 상기 결정된 키가 위치한 방향으로 동일한 키맵을 복사하여 확장하는 사용자 단말의 인증 방법.

청구항 15

제9항에 있어서,

상기 리스폰스 데이터의 비트 수는,

상기 키맵에 포함된 키가 나타낼 수 있는 단위 정보의 비트 수 및 상기 키맵에서 키의 이동 횟수에 따라 조절되는 사용자 단말의 인증 방법.

청구항 16

제9항에 있어서,

상기 사용자 단말의 인증에 대한 보안 강화를 위해 상기 키맵의 이동 방향표 또는 키맵을 상기 서버와 동일한 방법에 따라 업데이트 하는 단계

를 더 포함하는 사용자 단말의 인증 방법.

청구항 17

물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법을 수행하는 인증 장치인 서버에 있어서,

프로세서를 포함하고,

상기 프로세서는,

PUF 입출력 신호표에 기초하여 사용자 단말의 인증을 위한 첼린지(Challenge) 데이터를 상기 사용자 단말로 전송하고, 상기 첼린지 데이터에 대응하여 상기 PUF 입출력 신호표로부터 결정된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하며,상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 첼린지 데이터에 대응하는 리스폰스 데이터를 결정하고, 상기 결정된 리스폰스 데이터와 상기 첼린지 데이터에 대응하여 상기 사용자 단말로부터 수신된 리스폰스 데이터를 비교하며,

상기 사용자 단말로부터 수신된 리스폰스 데이터는,

상기 첼린지 데이터를 상기 사용자 단말에 배치된 PUF 칩에 입력하여 도출된 PUF 출력 신호를 상기 서버가 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵에 적용함으로써 결정되는 사용자 단말의 인증 장치.

청구항 18

제17항에 있어서,

상기 이동 방향표는,

상기 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트(Bit) 수가 조정되고,

상기 키맵에서 키의 이동 횟수는,

상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 상기 단위 비트 수에 기초하여 제로 패딩(Zero padding)을 수행하거나 상기 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 조정되는 사용자 단말의 인증 장치.

청구항 19

물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법을 수행하는 인증 장치인 사용자 단말에 있어서,

프로세서를 포함하고,

상기 프로세서는,

서버로부터 수신된 첼린지 데이터를 PUF 칩에 입력함으로써 PUF 출력 신호를 식별하고, 상기 식별된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하며,상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 첼린지 데이터에 대응하는 리스폰스 데이터를 결정하고,

상기 결정된 리스폰스 데이터는,

상기 서버가 첼린지 데이터에 대응하는 PUF 출력 신호를 이용하여 결정한 리스폰스 데이터와의 비교를 통해 상기 사용자 단말의 인증 결과를 도출하는데 이용되며,

상기 서버를 통해 결정되는 리스폰스 데이터는,

상기 사용자 단말이 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵을 통해 결정되는 사용자

단말의 인증 장치.

청구항 20

제19항에 있어서,

상기 이동 방향표는,

상기 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트(Bit) 수가 조정되고,

상기 키맵에서 키의 이동 횟수는,

상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 상기 단위 비트 수에 기초하여 제로 패딩(Zero padding)을 수행하거나 상기 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 조정되는 사용자 단말의 인증 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법 및 인증 장치에 관한 것으로, 보다 구체적으로는 첼린지 데이터에 대응하는 리스폰스 데이터를 결정하기 위한 키맵과 키맵의 이동 방향표를 이용하여 PUF 출력 신호를 암호화 함으로써 보안 성능을 향상시키는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 기존의 소프트웨어 기반 보안은 키(key)를 비휘발성 메모리(Non-Volatile Memory, NVM)에 저장해 두는 방식이다. 이러한 NVM에 저장된 디지털 키는 알고리즘 해킹 속도가 가속화됨에 따라 보안에 취약하다. 이를 극복하기 위해 고유 휘발성 디지털 키(unique volatile digital keys)를 생성하는 하드웨어 기반 보안 방식의 일종인 물리적 복제 방지 기술(Physical Unclonable Function, PUF)이 고안되었다.

[0003] 물리적 복제 방지 기술을 이용한 PUF 칩은 하드웨어 제작 중 발생하는 예측 불가능, 조절 불가능한 공정 편차를 활용하여 복제 불가한 고유한 특성을 가지도록 만든 하드웨어 칩이다. PUF 칩의 고유한 특성을 활용하여 생성한 난수를 디지털 키 생성 및 인증 등 보안 기능에 활용 가능하다.

[0004] 종래의 PUF 칩은 다음의 문제점을 가지고 있다. 첫 번째로, 인증기관이 해킹을 당하는 상황에 대응할 수 없다. 기존의 PUF 기반 인증 방식은 인증 기관에 저장된 CRP(Challenge-Response Pair) 테이블은 유출되는 상황은 없다고 가정한다. 하지만 은행 등 인증기관이 해킹을 당하는 경우 메모리에 저장된 CRP 테이블이 유출될 수 있다. 또한, 머신러닝 기법 등으로 일부 노출된 CRP를 통해 전체 CRP를 일정 확률로 추정할 수도 있다. 이 경우 한 번 만들어진 PUF 칩의 고유 특성은 바꿀 수 없기 때문에 PUF 칩을 폐기해야 한다.

[0005] 두 번째로, 모든 인증은 이전 인증 정보에 무관하다. 때문에 이전에 인증에 참여한 유저와 동일한 유저가 인증을 요청하는 것 인지 확인할 수 없다.

[0006] 세 번째로, PUF 칩의 리스폰스 비트(response bit) 수가 확정적이다. 하드웨어는 배선 등 구조가 정해져 있기 때문에 제작 이후 출력 신호의 비트 수를 조정할 수 없다. 때문에 보안 인증에 요구되는 리스폰스 비트 수가 바뀌면 호환이 불가하다.

[0007] 네 번째로, CRP 개수가 제한적이다. 기존의 인증 방식은 PUF 칩의 특정 입력에 대한 출력 신호를 인증 키의 한 단위인 CRP로 사용한다. 특정 입력 신호에 대한 PUF 칩의 출력 신호는 항상 동일하므로 CRP는 통상적으로 재사용하지 않는다. 인증기관이 보유한 CRP 소진 시 사용자는 PUF 칩을 폐기해야 한다. 때문에 인증기관은 사용 기한 대비 충분히 많은 CRP를 저장하기 위해서 비용을 소모해야 한다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 챌린지 데이터에 대응하는 리스폰스 데이터를 결정하기 위한 키맵과 키맵의 이동 방향표를 이용하여 PUF 출력 신호를 암호화 함으로써 인증 정보의 네트워크 노출을 감소시킬 수 있는 방법 및 장치를 제공한다.

[0009] 또한, 본 발명은 키맵과 키맵의 이동 방향표의 업데이트를 통해 CRP에 PUF 칩의 고유 특성에 대한 정보가 누적되는 것을 방지함으로써 보안성을 강화할 뿐만 아니라 적은 시간과 비용으로 해킹 상황에 대처할 수 있는 방법 및 장치를 제공한다.

[0010] 또한, 본 발명은 인증 히스토리(history) 정보를 포함하는 인증 정보를 생성하여 활용함으로써 사용자와 해커를 판별할 수 있는 방법 및 장치를 제공한다.

과제의 해결 수단

[0011] 본 발명의 일실시예에 따른 서버가 수행하는 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법은 PUF 입출력 신호표에 기초하여 사용자 단말의 인증을 위한 챌린지(Challenge) 데이터를 상기 사용자 단말로 전송하는 단계; 상기 챌린지 데이터에 대응하여 상기 PUF 입출력 신호표로부터 결정된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하는 단계; 상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 챌린지 데이터에 대응하는 리스폰스 데이터를 결정하는 단계; 및 상기 결정된 리스폰스 데이터와 상기 챌린지 데이터에 대응하여 상기 사용자 단말로부터 수신된 리스폰스 데이터를 비교하는 단계를 포함하고, 상기 사용자 단말로부터 수신된 리스폰스 데이터는 상기 챌린지 데이터를 상기 사용자 단말에 배치된 PUF 칩에 입력하여 도출된 PUF 출력 신호를 상기 서버가 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵에 적용함으로써 결정될 수 있다.

[0012] 상기 이동 방향표는 상기 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트(Bit) 수가 조정될 수 있다.

[0013] 상기 키맵에서 키의 이동 횟수는 상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 상기 단위 비트 수에 기초하여 제로 패딩(Zero padding)을 수행하거나 상기 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 조정될 수 있다.

[0014] 상기 리스폰스 데이터를 결정하는 단계는 상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 추가 정보를 조합함으로써 리스폰스 데이터를 결정할 수 있다.

[0015] 상기 키맵에 포함된 키의 이동 경로를 추출하는 단계는 상기 사용자 단말에 대한 이전 인증 정보, PUF 출력 신호 및 시간 정보 중 적어도 하나 이상의 정보에 대한 조합을 통해 결정된 키맵의 좌표를 상기 키의 이동 경로를 추출하기 위한 시작 위치로 결정할 수 있다.

[0016] 상기 키맵에 포함된 키의 이동 경로를 추출하는 단계는 상기 챌린지 데이터에 대응하는 PUF 출력 신호를 상기 키맵의 이동 방향표에 적용하여 결정된 키가 상기 키맵의 범위를 벗어나는 경우, 상기 시작 위치를 미리 설정된 규칙을 통해 재결정하거나, 상기 결정된 키가 위치한 방향으로 동일한 키맵을 복사하여 확장할 수 있다.

[0017] 상기 리스폰스 데이터의 비트 수는 상기 키맵에 포함된 키가 나타낼 수 있는 단위 정보의 비트 수 및 상기 키맵에서 키의 이동 횟수에 따라 조절될 수 있다.

[0018] 상기 사용자 단말의 인증에 대한 보안 강화를 위해 상기 키맵의 이동 방향표 또는 키맵을 상기 사용자 단말과 동일한 방법에 따라 업데이트 하는 단계를 더 포함할 수 있다.

[0019] 본 발명의 일실시예에 따른 사용자 단말이 수행하는 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법은 서버로부터 수신된 챌린지 데이터를 PUF 칩에 입력함으로써 PUF 출력 신호를 식별하는 단계; 상기 식별된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하는 단계; 및 상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 챌린지 데이터에 대응하는 리스폰스 데이터를 결정하는 단계를 포함하고, 상기 결정된 리스폰스 데이터는 상기 서버가 챌린지 데이터에 대응하는 PUF 출력 신호를 이용하여 결정한 리스폰스

데이터와의 비교를 통해 상기 사용자 단말의 인증 결과를 도출하는데 이용되고, 상기 서버를 통해 결정되는 리스폰스 데이터는 상기 사용자 단말이 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵을 통해 결정될 수 있다.

[0020] 상기 이동 방향표는 상기 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트(Bit) 수가 조정될 수 있다.

[0021] 상기 키맵에서 키의 이동 횟수는 상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 상기 단위 비트 수에 기초하여 제로 패딩(Zero padding)을 수행하거나 상기 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 조정될 수 있다.

[0022] 상기 리스폰스 데이터를 결정하는 단계는 상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 추가 정보를 조합함으로써 리스폰스 데이터를 결정할 수 있다.

[0023] 상기 키맵에 포함된 키의 이동 경로를 추출하는 단계는 상기 사용자 단말에 대한 이전 인증 정보, PUF 출력 신호 및 시간 정보 중 적어도 하나 이상의 정보에 대한 조합을 통해 결정된 키맵의 좌표를 상기 키의 이동 경로를 추출하기 위한 시작 위치로 결정할 수 있다.

[0024] 상기 키맵에 포함된 키의 이동 경로를 추출하는 단계는 상기 첼린지 데이터에 대응하는 PUF 출력 신호를 상기 키맵의 이동 방향표에 적용하여 결정된 키가 상기 키맵의 범위를 벗어나는 경우, 상기 시작 위치를 미리 설정된 규칙을 통해 재결정하거나, 상기 결정된 키가 위치한 방향으로 동일한 키맵을 복사하여 확장할 수 있다.

[0025] 상기 리스폰스 데이터의 비트 수는 상기 키맵에 포함된 키가 나타낼 수 있는 단위 정보의 비트 수 및 상기 키맵에서 키의 이동 횟수에 따라 조절될 수 있다.

[0026] 상기 사용자 단말의 인증에 대한 보안 강화를 위해 상기 키맵의 이동 방향표 또는 키맵을 상기 서버와 동일한 방법에 따라 업데이트 하는 단계를 더 포함할 수 있다.

[0027] 본 발명의 일실시예에 따른 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법을 수행하는 인증 장치인 서버는 프로세서를 포함하고, 상기 프로세서는 PUF 입출력 신호표에 기초하여 사용자 단말의 인증을 위한 첼린지(Challenge) 데이터를 상기 사용자 단말로 전송하고, 상기 첼린지 데이터에 대응하여 상기 PUF 입출력 신호표로부터 결정된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하며,상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 첼린지 데이터에 대응하는 리스폰스 데이터를 결정하고, 상기 결정된 리스폰스 데이터와 상기 첼린지 데이터에 대응하여 상기 사용자 단말로부터 수신된 리스폰스 데이터를 비교하며, 상기 사용자 단말로부터 수신된 리스폰스 데이터는 상기 첼린지 데이터를 상기 사용자 단말에 배치된 PUF 칩에 입력하여 도출된 PUF 출력 신호를 상기 서버가 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵에 적용함으로써 결정될 수 있다.

[0028] 상기 이동 방향표는 상기 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트(Bit) 수가 조정되고, 상기 키맵에서 키의 이동 횟수는 상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 상기 단위 비트 수에 기초하여 제로 패딩(Zero padding)을 수행하거나 상기 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 조정될 수 있다.

[0029] 본 발명의 일실시예에 따른 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법을 수행하는 인증 장치인 사용자 단말은 프로세서를 포함하고, 상기 프로세서는 서버로부터 수신된 첼린지 데이터를 PUF 칩에 입력함으로써 PUF 출력 신호를 식별하고, 상기 식별된 PUF 출력 신호를 리스폰스(Response) 데이터를 결정하기 위한 키맵(key-map)의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출하며,상기 추출된 이동 경로에 대응하는 키를 이용하여 상기 첼린지 데이터에 대응하는 리스폰스 데이터를 결정하고, 상기 결정된 리스폰스 데이터는 상기 서버가 첼린지 데이터에 대응하는 PUF 출력 신호를 이용하여 결정한 리스폰스 데이터와의 비교를 통해 상기 사용자 단말의 인증 결과를 도출하는데 이용되며, 상기 서버를 통해 결정되는 리스폰스 데이터는 상기 사용자 단말이 리스폰스 데이터를 결정하는데 활용한 키맵의 이동 방향표 및 키맵을 통해 결정될 수 있다.

[0030] 상기 이동 방향표는 상기 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트(Bit) 수가 조정되고, 상기 키맵에서 키의 이동 횟수는 상기 PUF 출력 신호의 비트 수가 상기 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 상기 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 상기 단위 비트 수에 기초하여 제로 패딩(Zero padding)을 수행하거나 상기 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 조정될 수 있다 .

발명의 효과

[0031] 본 발명의 일실시예에 의하면, 챌린지 데이터에 대응하는 리스폰스 데이터를 결정하기 위한 키맵과 키맵의 이동 방향표를 이용하여 PUF 출력 신호를 암호화 함으로써 인증 정보의 네트워크 노출을 감소시킬 수 있다.

[0032] 또한, 본 발명의 일실시예에 의하면, 키맵과 키맵의 이동 방향표의 업데이트를 통해 CRP에 PUF 칩의 고유 특성에 대한 정보가 누적되는 것을 방지함으로써 보안성을 강화할 뿐만 아니라 적은 시간과 비용으로 해킹 상황에 대처할 수 있다.

[0033] 또한, 본 발명의 일실시예에 의하면, 인증 히스토리(history) 정보를 포함하는 인증 정보를 생성하여 활용함으로써 사용자와 해커를 판별할 수 있다.

도면의 간단한 설명

[0034] 도 1은 본 발명의 일실시예에 따른 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 인증 시스템을 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 키맵과 키맵의 방향 이동표를 이용하여 암호화된 리스폰스 데이터를 결정함으로써 인증을 수행하는 구체적인 예를 나타낸 도면이다.

도 3은 본 발명의 일실시예에 따른 키맵을 변경하여 PUF 출력 신호를 암호화 하는 방법을 나타낸 도면이다.

도 4는 본 발명의 일실시예에 따른 키맵의 이동 방향표를 변경하여 PUF 출력 신호를 암호화 하는 방법을 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0035] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0036] 도 1은 본 발명의 일실시예에 따른 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 인증 시스템을 도시한 도면이다.

[0037] 물리적 복제 방지 기능을 이용한 인증 시스템(100)은 공정 편차에 따라 각기 다르게 형성된 PUF 칩(회로)에 특정 입력 신호를 넣었을 때 나오는 특정 출력 신호를 보안 인증 절차에서 활용함으로써 보안성을 강화할 수 있다. 이때, PUF 칩의 특정 입력 신호와 특정 출력 신호의 쌍을 CRP(Challenge-Response Pair)로 나타낼 수 있으며, 하나의 PUF 칩을 통해 생성 가능한 CRP들의 모음을 CRP 테이블이라고 칭할 수 있다. 여기서 CRP 테이블은 본 발명에서 제공하는 PUF 입출력 신호표와 동일할 수 있다.

[0038] 일례로, 도 1을 참고하면, 본 발명의 물리적 복제 방지 기능을 이용한 인증 시스템(100)은 인증기관(110)과 사용자 단말(120) 사이의 인증 방법을 제공할 수 있다. 이때, 인증기관(110)은 일례로, 서버일 수 있으며, 사용자 단말(120)은 PUF 칩(121)을 포함하는 다양한 종류의 인증장치일 수 있다.

[0039] 본 발명의 물리적 복제 방지 기능을 이용한 인증 시스템(100)은 PUF 출력 신호를 암호화하는 인증 방식을 제공함으로써 종래의 PUF 인증 방식이 가지는 보안 취약성 및 자원 한계의 문제를 해결할 수 있다.

[0040] 보다 구체적으로 인증 시스템(100)을 구성하는 인증기관(110)과 사용자 단말(120)은 PUF 출력 신호를 암호화 하기 위하여 동일한 키맵(key-map)과 키맵의 이동 방향표를 공유할 수 있다. 이때, 키맵은 챌린지 데이터에 대응하는 리스폰스 데이터를 결정하기 위한 키가 매트릭스 형태로 배열된 데이터 집합을 나타내고, 키맵의 이동 방향표는 PUF 출력 신호에 따라 키맵에 포함된 키의 이동 방향을 결정하기 위한 데이터 집합을 나타낼 수 있다.

[0041] 먼저, 사용자 단말(120)로부터 인증 요청이 수신된 경우, 인증기관(110)은 사용자 단말(120)의 인증을 위해 PUF 입출력신호표에서 특정한 챌린지 데이터를 선택하여 사용자 단말(120)로 전송할 수 있다. 이때, PUF 입출력신호표는 사용자 단말(120)에 포함된 PUF 칩(121)에 챌린지 데이터라는 특정 입력 신호를 넣었을 때 나오는 출력 신

호를 나타내는 데이터 집합일 수 있다.

[0042] 이후 인증기관(110)은 PUF 입출력신호표에 기초하여 선택된 첼린지 데이터에 대응하는 PUF 출력 신호를 식별할 수 있다. 인증기관(110)은 이와 같이 식별된 PUF 출력 신호를 사용자 단말(120)과 공유된 키맵의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출할 수 있다.

[0043] 인증기관(110)은 이와 같이 추출된 이동 경로에 대응하는 키를 이용하여 선택된 첼린지 데이터에 대응하는 리스폰스 데이터를 결정할 수 있다. 이때, 인증기관(110)은 사용자 단말(120)과 공유하는 리스폰스 데이터 결정 방법에 따라 추출된 이동 경로에 대응하는 모든 키를 이용하거나, 일부 키를 이용함으로써 리스폰스 데이터를 결정할 수 있다.

[0044] 예를 들어, 인증기관(110)은 추출된 이동 경로에 대응하는 모든 키를 순서대로 식별하여 리스폰스 데이터를 결정할 수 있다. 이와는 달리 인증기관(110)은 추출된 이동 경로에 대응하는 키 중 이동 경로 상의 첫 번째 키 및 마지막 키를 추출하여 리스폰스 데이터를 결정할 수 있다. 이러한 리스폰스 데이터의 결정 방법은 하나의 예시일 뿐 상기의 예에 한정되지 않고, 다양한 방법이 제공될 수 있다.

[0045] 한편, 사용자 단말(120)은 인증기관(110)으로부터 수신된 첼린지 데이터를 입력 신호로 하여 PUF 칩(121)에 사용자 단말(120)은 이와 같이 획득된 PUF 출력 신호를 인증기관(110)과 공유된 키맵의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출할 수 있다.

[0046] 사용자 단말(120)은 이와 같이 추출된 이동 경로에 대응하는 키를 이용하여 선택된 첼린지 데이터에 대응하는 리스폰스 데이터를 결정한 후 결정된 리스폰스 데이터를 인증기관(110)으로 전송할 수 있다. 이때, 사용자 단말(120)은 인증기관(110)과 공유하는 리스폰스 데이터 결정 방법에 따라 추출된 이동 경로에 대응하는 모든 키를 이용하거나, 일부 키를 이용함으로써 리스폰스 데이터를 결정할 수 있다.

[0047] 인증기관(110)은 사용자 단말(120)로부터 전송된 리스폰스 데이터와 자체적으로 결정된 리스폰스 데이터를 비교함으로써 사용자 단말(120)에 대한 인증 결과를 도출할 수 있다. 만약 사용자 단말(120)로부터 전송된 리스폰스 데이터와 자체적으로 결정된 리스폰스 데이터가 동일하다면, 인증기관(110)은 인증이 성공한 것으로 판단하여 사용자 단말(120)로 인증 성공을 나타내는 인증 결과 메시지를 전송할 수 있다. 이와는 달리 사용자 단말(120)로부터 전송된 리스폰스 데이터와 자체적으로 결정된 리스폰스 데이터가 동일하지 않으면, 인증기관(110)은 인증이 실패한 것으로 판단하여 사용자 단말(120)로 인증 실패를 나타내는 인증 결과 메시지를 전송할 수 있다.

[0048] 본 발명의 물리적 복제 방지 기능을 이용한 인증 시스템(100)은 아래의 네 가지 측면에서 PUF 칩(121)을 사용한 인증 방법의 보안성을 향상시킬 수 있다. 첫 번째로, 인증 정보의 네트워크 노출을 감소시킴으로써 보안성을 강화할 수 있다. 기존의 PUF 칩(121)을 이용한 인증 방법은 인증기관(110)과 사용자 단말(120)이 인증 정보를 주고받는 동안 CRP가 네트워크에 노출된다.

[0049] 그러나 본 발명의 구성 요소 중 키맵과 키맵의 이동 방향표는 인증기관(110)과 사용자 단말(120)이 리스폰스 데이터를 생성하는데 활용할 뿐 네트워크 상에 노출되지 않으므로 해커가 인증 정보를 탈취한 경우 첼린지 데이터에 대한 정보는 얻을 수 있어도 PUF 출력 신호는 물론 키맵과 키맵의 이동 방향표에 대해서는 알 수 없다는 장점이 있다.

[0050] 두 번째로, PUF 칩(121)의 고유 특성에 대한 정보가 CRP에 누적되는 것을 방지함으로써 보안성을 강화시킬 수 있다. 기존의 PUF 칩(121)을 이용한 인증 방법은 첼린지 데이터에 대한 PUF 출력 신호 자체를 리스폰스 데이터로 출력하기 때문에 첼린지 데이터와 리스폰스 데이터에 PUF 칩(121) 고유의 특성에 대한 정보가 누적된다. 혹은 PUF 출력 신호를 특정 방법으로 암호화하더라도 그 방법이 일정하다면 CRP는 규칙성을 가지게 되며, 이는 머신 러닝 기법 등 해킹 기술의 향상에 따라 일부 CRP를 통해 전체 CRP를 일정 확률로 예측할 수 있는 등 잠재적인 해킹 위험을 가지고 있다.

[0051] 본 발명의 인증 시스템(100)은 PUF 출력 신호를 암호화 할 수 있는 키맵과 키맵의 이동 방향표를 업데이트 함으로써 리스폰스 데이터의 생성 알고리즘을 다양하게 변환할 수 있다. 이를 통해 본 발명의 인증 시스템(100)은 CRP에 PUF 칩(121)의 고유 특성에 대한 정보가 누적되지 않게 하고 CRP의 규칙성을 교란해 향상된 해킹 기법에 대응할 수 있다.

[0052] 세 번째로, 인증기관(110)이 해킹되는 상황에 대응할 수 있다. 기존의 PUF 칩(121)을 이용한 인증 방법은 인증기관(110)이 저장하고 있는 CRP 테이블이 유출될 시, 모든 사용자 단말(120)의 PUF 칩(121)을 전량 폐기해야 한다. 본 발명의 인증 시스템(110)은 키맵 및 키맵의 이동 방향표를 업데이트 함으로써 동일한 PUF 출력 신호를

사용해도 전혀 다른 리스폰스 데이터를 출력할 수 있으므로 정보 유출 시 키맵 또는 키맵의 이동 방향표만 업데이트하는 등의 방법을 활용해 적은 시간과 비용으로 해킹 상황에 대처할 수 있다.

[0053] 네 번째로, 인증 히스토리 정보를 포함하는 인증 정보 생성하기 때문에 이를 활용한 심화된 인증 방식이 가능할 수 있다. 기존의 PUF 칩(121)을 이용한 인증 방법에서 CRP는 이전 인증 정보와 무관하기 때문에 CRP만 알고 있으면 그 동안 인증을 수행한 사용자 단말(120)이 정상 사용자인지 또는 해커인지를 구분할 수 없다. 본 발명의 인증 시스템(100)은 키맵의 시작 위치에 따라 리스폰스 데이터가 달라지기 때문에 이전 인증에 사용된 키맵의 좌표 및 키의 이동 경로를 다음 인증에 활용할 수 있다. 이는 PUF 입출력 신호, 키맵 및 키맵의 이동 방향표를 알고 있다고 해도 이전 인증 정보를 모르면 정확한 리스폰스 데이터를 생성할 수 없어 인증을 요청한 사용자 단말(120)이 정상 사용자인지 또는 해커인지를 판별하는 데 활용할 수 있다.

[0054] 본 발명의 인증 시스템(100)은 이외에도 두 가지 부가적인 이점을 가질 수 있다. 첫 번째로, 다양한 보안 시스템에 대한 호환성이 증대될 수 있다. 본 발명의 인증 방식은 키맵에 포함된 키가 나타낼 수 있는 단위 정보의 비트 수 및 키맵에서 키의 이동 횟수를 조절하여 리스폰스 데이터의 비트 수를 변경할 수 있다. 이를 통해 동일한 하드웨어를 사용하여 다양한 보안 시스템의 동작 조건에 맞춰 유연하게 구동 방식을 조정할 수 있다.

[0055] 두 번째로, PUF를 이용한 인증 시스템(100)의 유지비용을 감소시킬 수 있다. 기존의 PUF 칩(121)을 이용한 인증 방법은 인증기관(110)이 저장할 수 있는 CRP 테이블의 용량이 PUF 칩(121)의 사용 기한에 직결되기 때문에 인증기관(110)은 수많은 사용자의 CRP 테이블을 대량으로 저장하고 유지해야 하는 부담이 있다. 본 발명은 같은 첼린지 데이터에 대한 리스폰스 데이터가 다양하기 때문에 인증기관(110)이 대량의 CRP 테이블을 저장하지 않아도 되므로 인증기관(110)이 소모하는 유지비용을 줄일 수 있다.

[0056] 도 2는 본 발명의 일실시예에 따른 키맵과 키맵의 방향 이동표를 이용하여 암호화된 리스폰스 데이터를 결정함으로써 인증을 수행하는 구체적인 예를 나타낸 도면이다.

[0057] 도 2를 참고하면, 본 발명의 인증기관(110)과 사용자 단말(120)은 주어진 첼린지 데이터에 대한 PUF 출력 신호를 아래와 같은 방법을 통해 암호화 하여 리스폰스 데이터를 결정할 수 있다.

[0058] 먼저, 인증기관(110)은 사용자 단말(120)에 전송할 첼린지 데이터로 "1"이 선택된 경우, 선택된 첼린지 데이터 "1"을 사용자 단말(120)로 전송할 수 있다.

[0059] 이후 인증기관(110)은 인증기관(110)은 PUF 입출력신호표에 기초하여 첼린지 데이터 "1"에 대응하는 PUF 출력 신호 "00 00 00 00"을 식별할 수 있다.

[0060] 인증기관(110)은 식별된 PUF 출력 신호 "00 00 00 00"을 사용자 단말(120)과 공유된 키맵의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로를 추출할 수 있다. 이때, 키맵의 이동 방향표는 키맵에 포함된 키의 이동 가능한 방향의 개수에 따라 이동 방향 결정에 필요한 단위 비트의 수가 조정될 수 있다. 일례로, 도 2와 같이 키의 이동 가능한 방향의 개수가 상하좌우의 4방향인 경우, 이동 방향 결정에 필요한 단위 비트의 수는 2비트일 수 있다.

[0061] 따라서, 인증기관(110)은 첼린지 데이터 "1"에 대응하는 PUF 출력 신호가 "00 00 00 00"이므로 PUF 출력 신호 "00 00 00 00"를 2비트 단위로 구분하여 키맵의 이동 방향표에 적용함으로써 "상 상 상 상"에 대응하는 키의 이동 경로를 추출할 수 있다.

[0062] 추출된 이동 경로가 "상 상 상 상"이므로 인증기관(110)은 미리 설정된 기준에 따라 결정된 키맵의 시작 위치에서 "상 상 상 상"에 대응하는 이동 경로 상에 존재하는 키 "0 1 0 1"을 이용함으로써 첼린지 데이터 "1"에 대응하는 리스폰스 데이터 "0 1 0 1"을 결정할 수 있다. 상기의 예에서는 추출된 이동 경로에 대응하는 모든 키를 순서대로 식별하여 리스폰스 데이터를 결정하였으나 이는 하나의 예시일 뿐 인증기관(110)은 사용자 단말(120)과 공유된 다양한 방법을 통해 리스폰스 데이터를 결정할 수 있다.

[0063] 한편, 사용자 단말(120)은 인증기관(110)으로부터 수신된 첼린지 데이터 "1"을 입력 신호로 하여 PUF 칩(121)에 인가함으로써 PUF 출력 신호 "00 00 00 00"을 획득할 수 있다.

[0064] 사용자 단말(120)은 이와 같이 획득된 PUF 출력 신호 "00 00 00 00"을 인증기관(110)과 공유된 키맵의 이동 방향표에 적용함으로써 키맵에 포함된 키의 이동 경로 "상 상 상 상"을 추출할 수 있다.

[0065] 사용자 단말(120)은 이와 같이 추출된 이동 경로 "상 상 상 상"에 대응하는 키를 이용하여 선택된 첼린지 데이터 "1"에 대응하는 리스폰스 데이터 "0 1 0 1"을 결정한 후 결정된 리스폰스 데이터 "0 1 0 1"을 인증기관(11

0)으로 전송할 수 있다.

[0066] 인증기관(110)은 사용자 단말(120)로부터 전송된 리스폰스 데이터 "0 1 0 1"와 자체적으로 결정된 리스폰스 데이터 "0 1 0 1"을 비교함으로써 사용자 단말(120)에 대한 인증 결과를 도출할 수 있다.

[0067] 즉, 사용자 단말(120)로부터 전송된 리스폰스 데이터 "0 1 0 1"와 자체적으로 결정된 리스폰스 데이터 "0 1 0 1"가 동일하므로 인증기관(110)은 인증이 성공한 것으로 판단하여 사용자 단말(120)로 인증 성공을 나타내는 인증 결과 메시지를 전송할 수 있다.

[0068] 한편, 키맵의 시작 위치에 대한 좌표 정보는 인증기관(110)이 결정하여 사용자 단말(120)에 전송하거나, 인증기관(110)과 사용자 단말(120) 간의 미리 설정된 규칙에 따라 자동으로 결정될 수 있다. 이때, 키맵의 시작 위치를 결정하기 위한 규칙은 사용자 단말에 대한 이전 인증 정보, PUF 출력 신호 및 시간 정보 중 적어도 하나 이상의 정보에 대한 조합을 통해 결정될 수 있다.

[0069] 예를 들어, 사용자 단말(120)에 대한 이전 인증 정보에 기초하여 이전 인증 경로의 마지막 좌표 (3,7)인 경우, 인증기관(110) 또는 사용자 단말(120)은 키맵의 좌표 (3,7)을 다음 인증의 시작 위치로 결정할 수 있다.

[0070] 다른 일례로, 인증기관(110) 또는 사용자 단말(120)은 이전 인증 경로의 마지막 좌표 (3,7)로부터 일정 방향으로 이동(ex. 좌로 3칸)한 좌표(3,4)를 다음 인증의 시작 위치로 결정할 수 있다.

[0071] 다른 일례로, 인증기관(110) 또는 사용자 단말(120)은 이전 인증 경로의 마지막 좌표 (3,7)로부터 PUF 출력 신호에 따른 마지막 이동 방향인 "상"이 적용된 좌표(2,7)를 다음 인증의 시작 위치로 결정할 수 있다.

[0072] 다른 일례로, 인증기관(110) 또는 사용자 단말(120)은 인증 요청 시간을 활용하여 다음 인증의 시작 위치를 결정할 수 있는데 만약 인증 요청 시간이 '17시 31분 54초' 인 경우, 초 단위 정보를 활용해 좌표 (5,4)를 다음 인증의 시작 위치로 결정할 수 있다.

[0073] 도 3은 본 발명의 일실시예에 따른 키맵을 변경하여 PUF 출력 신호를 암호화 하는 방법을 나타낸 도면이다.

[0074] 본 발명의 물리적 복제 방지 기능을 이용한 인증 시스템(100)은 키맵을 변경, 즉 업데이트하여 동일한 PUF 출력 신호를 사용하더라도 새로운 리스폰스 데이터를 결정할 수 있다. 이를 통해 인증 시스템(100)은 CRP에 PUF 칩의 고유 특성에 대한 정보가 누적되는 것을 방지함으로써 보안성을 강화할 뿐만 아니라 적은 시간과 비용으로 해킹 상황에 대처할 수 있다.

[0075] 인증 시스템(100)은 키맵에 포함된 키가 나타낼 수 있는 단위 정보의 비트 수 및 키맵에서 키의 이동 횟수를 조절하여 리스폰스 데이터의 비트 수를 변경할 수 있다. 일례로 도 3의 (a)에 제시된 키맵은 1bit의 키로 구성되어 있으며, 각각의 키는 0 또는 1의 값을 가질 수 있다. 인증 시스템(100)을 구성하는 인증기관(110) 또는 사용자 단말(120)은 8 단위의 PUF 출력 신호 "01 11 11 00 11 00 10 00"를 키맵의 이동 방향표에 적용함으로써 8bits의 리스폰스 데이터 "0 0 1 0 0 1 0 0"를 결정할 수 있다.

[0076] 이와는 달리 도 3의 (b)에 제시된 키맵은 4bit의 키로 구성되어 있으며, 각각의 키는 0 내지 9 및 A 내지 F까지 총 16개의 값을 가질 수 있다. 인증 시스템(100)을 구성하는 인증기관(110) 또는 사용자 단말(120)은 8 단위의 PUF 출력 신호 "01 11 11 00 11 00 10 00"를 키맵의 이동 방향표에 적용함으로써 32bits의 리스폰스 데이터 "0110 1000 0100 0000 1010 0101 0001 1101"를 결정할 수 있다.

[0077] 한편, 도 3에서 키맵은 2차원 행렬로 표현되었으나, 이는 하나의 예시일 뿐 이에 한정되지 않으며, N(N=1, 2, 3, …) 차원 행렬로 구현될 수 있다. 따라서, 이동 방향표는 복수의 키가 N 차원 행렬로 구현된 데이터 집합인 키맵에서 데이터 주소를 변경하기 위한 일련의 규칙을 의미할 수 있다.

[0078] 만약 챌린지 데이터에 대응하는 PUF 출력 신호를 키맵의 이동 방향표에 적용하여 결정된 키가 키맵의 범위를 벗어나는 경우, 인증 시스템(100)을 구성하는 인증기관(110) 또는 사용자 단말(120)은 시작 위치를 공유된 규칙을 통해 재결정하거나, 이동 방향표를 적용하여 결정된 키가 위치한 방향으로 동일한 키맵을 복사하여 확장할 수 있다.

[0079] 일례로, 키맵의 좌표 (5,1)의 위치에서 이동 방향표를 적용하여 결정된 키의 이동 방향이 "좌"로 결정된 경우, 인증 시스템(100)을 구성하는 인증기관(110) 또는 사용자 단말(120)은 현재의 키맵 좌측으로 동일한 키맵을 복사하여 확장할 수 있으며, 최종 결정된 키의 좌표는 (5,9)가 될 수 있다.

[0080] 도 4는 본 발명의 일실시예에 따른 키맵의 이동 방향표를 변경하여 PUF 출력 신호를 암호화 하는 방법을 나타낸

도면이다.

[0081] 본 발명의 물리적 복제 방지 기능을 이용한 인증 시스템(100)은 키맵의 이동 방향표를 변경, 즉 업데이트하여 동일한 PUF 출력 신호를 사용하더라도 새로운 리스폰스 데이터를 결정할 수 있다. 이를 통해 인증 시스템(100)은 CRP에 PUF 칩의 고유 특성에 대한 정보가 누적되는 것을 방지함으로써 보안성을 강화할 뿐만 아니라 적은 시간과 비용으로 해킹 상황에 대처할 수 있다.

[0082] 인증 시스템(100)은 키맵에 포함된 키의 이동 방향 결정에 필요한 단위 비트 수 및 키의 이동 횟수를 조절하여 리스폰스 데이터의 비트 수를 변경할 수 있다. 일례로, 도 4의 (a)에 제시된 키맵의 이동 방향표는 상하좌우의 4 방향으로의 이동이 가능하며, 각각의 방향은 2비트로 구성된 서로 다른 PUF 출력 신호에 대응될 수 있다. 즉, PUF 출력 신호 "00"은 상 방향(0,1)으로의 키 이동을 나타내고, PUF 출력 신호 "01"은 하 방향(0,-1)으로의 키 이동을 나타내며, PUF 출력 신호 "10"은 좌 방향(-1,0)으로의 키 이동을 나타내고, PUF 출력 신호 "11"은 우 방향(1,0)으로의 키 이동을 나타낼 수 있다.

[0083] 이와는 달리 도 4의 (b)에 제시된 키맵의 이동 방향표는 상하좌우 및 대각선 방향을 포함하여 총 8방향으로의 이동이 가능하며, 각각의 방향은 3비트로 구성된 서로 다른 PUF 출력 신호에 대응할 수 있다. 즉, PUF 출력 신호 "000"은 상 방향(0,1)으로의 키 이동을 나타내고, PUF 출력 신호 "001"은 하 방향(0,-1)으로의 키 이동을 나타내며, PUF 출력 신호 "010"은 좌 방향(-1,0)으로의 키 이동을 나타내고, PUF 출력 신호 "011"은 우 방향(1,0)으로의 키 이동을 나타낼 수 있다. 또한, 즉, PUF 출력 신호 "100"은 좌상단 방향(-1,1)으로의 키 이동을 나타내고, PUF 출력 신호 "101"은 우상단 방향(1,1)으로의 키 이동을 나타내며, PUF 출력 신호 "110"은 좌하단 방향(-1,-1)으로의 키 이동을 나타내고, PUF 출력 신호 "111"은 우하단 방향(1,-1)으로의 키 이동을 나타낼 수 있다.

[0084] 한편, PUF 출력 신호의 비트 수가 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 인증 시스템(100)을 구성하는 인증기관(110) 또는 사용자 단말(120)은 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 이동 방향 결정에 필요한 단위 비트 수 만큼 추가하여 제로 패딩(Zero padding)을 수행하거나 이동 방향 결정에 사용된 PUF 출력 신호의 일부 비트를 재사용함으로써 키맵에서 키의 이동 횟수를 조절할 수 있다.

[0085] 일례로, 도 4의 (b)를 참고하면, 이동 방향 결정에 필요한 단위 비트 수는 3비트이고 PUF 출력 신호는 16비트이다. 이 경우 인증 시스템(100)을 구성하는 인증기관(110) 또는 사용자 단말(120)은 PUF 출력 신호를 15비트만 사용하여 키의 이동 횟수를 5회로 결정할 수 있다.

[0086] 이와는 달리 인증 시스템(100)을 구성하는 인증기관(110) 또는 사용자 단말(120)은 이동 방향 결정에 사용되고 남은 1비트 "0"의 PUF 출력 신호에 2비트 만큼 제로 패딩을 수행하거나, 이동 방향 결정에 사용된 PUF 출력 신호 중 일부 비트(2비트)를 재사용하여 총 18비트를 생성함으로써 키의 이동 횟수를 6회로 증가시킬 수 있다. 조절bits로 만들어 사용할 수 있다. 추가를 위해 zero padding을 하거나 PUF 출력신호의 일부를 재사용할 수 있다.

[0087] 한편, 인증 시스템(100)을 구성하는 인증기관(110) 또는 사용자 단말(120)은 PUF 출력 신호의 비트 수가 이동 방향 결정에 필요한 단위 비트 수의 배수가 아닌 경우, 이동 방향 결정에 사용되고 남은 PUF 출력 신호의 비트에 추가 정보를 조합함으로써 리스폰스 데이터를 결정할 수도 있다.

[0088] 한편, 본 발명에 따른 방법은 컴퓨터에서 실행될 수 있는 프로그램으로 작성되어 마그네틱 저장매체, 광학적 판독매체, 디지털 저장매체 등 다양한 기록 매체로도 구현될 수 있다.

[0089] 본 명세서에 설명된 각종 기술들의 구현들은 디지털 전자 회로조직으로, 또는 컴퓨터 하드웨어, 펌웨어, 소프트웨어로, 또는 그들의 조합들로 구현될 수 있다. 구현들은 데이터 처리 장치, 예를 들어 프로그램가능 프로세서, 컴퓨터, 또는 다수의 컴퓨터들의 동작에 의한 처리를 위해, 또는 이 동작을 제어하기 위해, 컴퓨터 프로그램 제품, 즉 정보 캐리어, 예를 들어 기계 판독가능 저장 장치(컴퓨터 판독가능 매체) 또는 전파 신호에서 유형적으로 구체화된 컴퓨터 프로그램으로서 구현될 수 있다. 상술한 컴퓨터 프로그램(들)과 같은 컴퓨터 프로그램은 컴파일된 또는 인터프리트된 언어들을 포함하는 임의의 형태의 프로그래밍 언어로 기록될 수 있고, 독립형 프로그램으로서 또는 모듈, 구성요소, 서브루틴, 또는 컴퓨팅 환경에서의 사용에 적절한 다른 유닛으로서 포함하는 임의의 형태로 전개될 수 있다. 컴퓨터 프로그램은 하나의 사이트에서 하나의 컴퓨터 또는 다수의 컴퓨터들 상에서 처리되도록 또는 다수의 사이트들에 걸쳐 분배되고 통신 네트워크에 의해 상호 연결되도록 전개될 수 있다.

[0090] 컴퓨터 프로그램의 처리에 적절한 프로세서들은 예로서, 범용 및 특수 목적 마이크로프로세서들 둘 다, 및 임의의 종류의 디지털 컴퓨터의 임의의 하나 이상의 프로세서들을 포함한다. 일반적으로, 프로세서는 판독 전용 메

모리 또는 랜덤 액세스 메모리 또는 둘 다로부터 명령어들 및 데이터를 수신할 것이다. 컴퓨터의 요소들은 명령어들을 실행하는 적어도 하나의 프로세서 및 명령어들 및 데이터를 저장하는 하나 이상의 메모리 장치들을 포함할 수 있다. 일반적으로, 컴퓨터는 데이터를 저장하는 하나 이상의 대량 저장 장치들, 예를 들어 자기, 자기-광 디스크들, 또는 광 디스크들을 포함할 수 있거나, 이것들로부터 데이터를 수신하거나 이것들에 데이터를 송신하거나 또는 양쪽으로 되도록 결합될 수도 있다. 컴퓨터 프로그램 명령어들 및 데이터를 구체화하는데 적절한 정보 캐리어들은 예로서 반도체 메모리 장치들, 예를 들어, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM(Compact Disk Read Only Memory), DVD(Digital Video Disk)와 같은 광 기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 롬(ROM, Read Only Memory), 램(RAM, Random Access Memory), 플래시 메모리, EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM) 등을 포함한다. 프로세서 및 메모리는 특수 목적 논리 회로조직에 의해 보충되거나, 이에 포함될 수 있다.

[0091] 또한, 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용매체일 수 있고, 컴퓨터 저장매체 및 전송매체를 모두 포함할 수 있다.

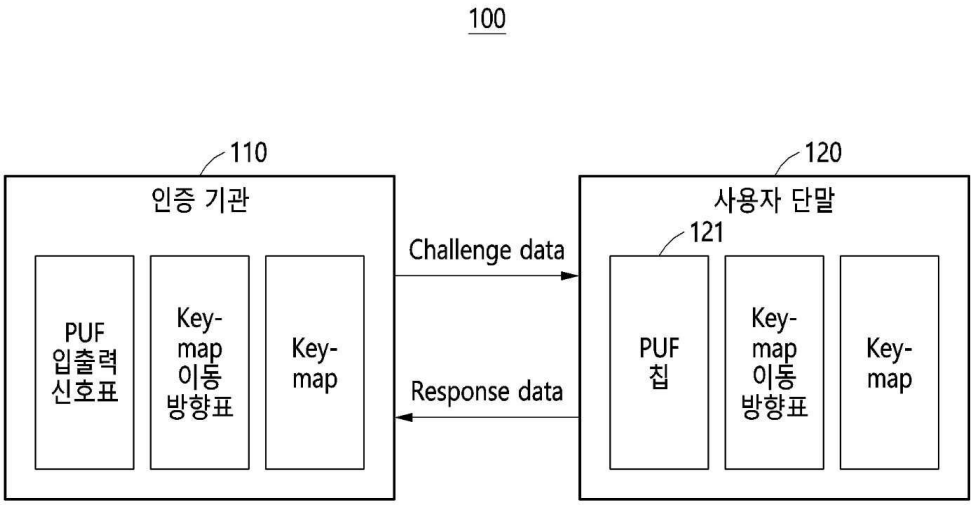
[0092] 본 명세서는 다수의 특정한 구현물의 세부사항들을 포함하지만, 이들은 어떠한 발명이나 청구 가능한 것의 범위에 대해서도 제한적인 것으로서 이해되어서는 안되며, 오히려 특정한 발명의 특정한 실시형태에 특유할 수 있는 특징들에 대한 설명으로서 이해되어야 한다. 개별적인 실시형태의 문맥에서 본 명세서에 기술된 특정한 특징들은 단일 실시형태에서 조합하여 구현될 수도 있다. 반대로, 단일 실시형태의 문맥에서 기술한 다양한 특징들 역시 개별적으로 혹은 어떠한 적절한 하위 조합으로도 복수의 실시형태에서 구현 가능하다. 나아가, 특징들이 특정한 조합으로 동작하고 초기에 그와 같이 청구된 바와 같이 묘사될 수 있지만, 청구된 조합으로부터의 하나 이상의 특징들은 일부 경우에 그 조합으로부터 배제될 수 있으며, 그 청구된 조합은 하위 조합이나 하위 조합의 변형물로 변경될 수 있다.

[0093] 마찬가지로, 특정한 순서로 도면에서 동작들을 묘사하고 있지만, 이는 바람직한 결과를 얻기 위하여 도시된 그 특정한 순서나 순차적인 순서대로 그러한 동작들을 수행하여야 한다거나 모든 도시된 동작들이 수행되어야 하는 것으로 이해되어서는 안 된다. 특정한 경우, 멀티태스킹과 병렬 프로세싱이 유리할 수 있다. 또한, 상술한 실시형태의 다양한 장치 컴포넌트의 분리는 그러한 분리를 모든 실시형태에서 요구하는 것으로 이해되어서는 안되며, 설명한 프로그램 컴포넌트와 장치들은 일반적으로 단일의 소프트웨어 제품으로 함께 통합되거나 다중 소프트웨어 제품에 패키징 될 수 있다는 점을 이해하여야 한다.

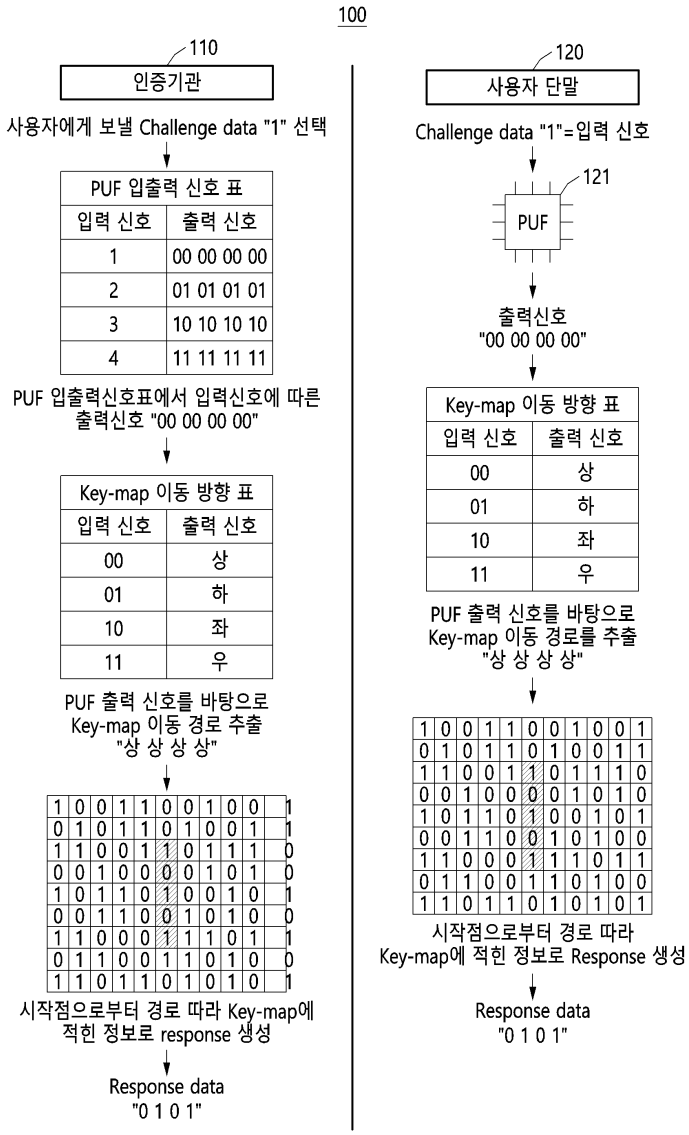
[0094] 한편, 본 명세서와 도면에 개시된 본 발명의 실시 예들은 이해를 돕기 위해 특정 예를 제시한 것에 지나지 않으며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 개시된 실시 예들 이외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형 예들이 실시 가능하다는 것은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 자명한 것이다.

도면

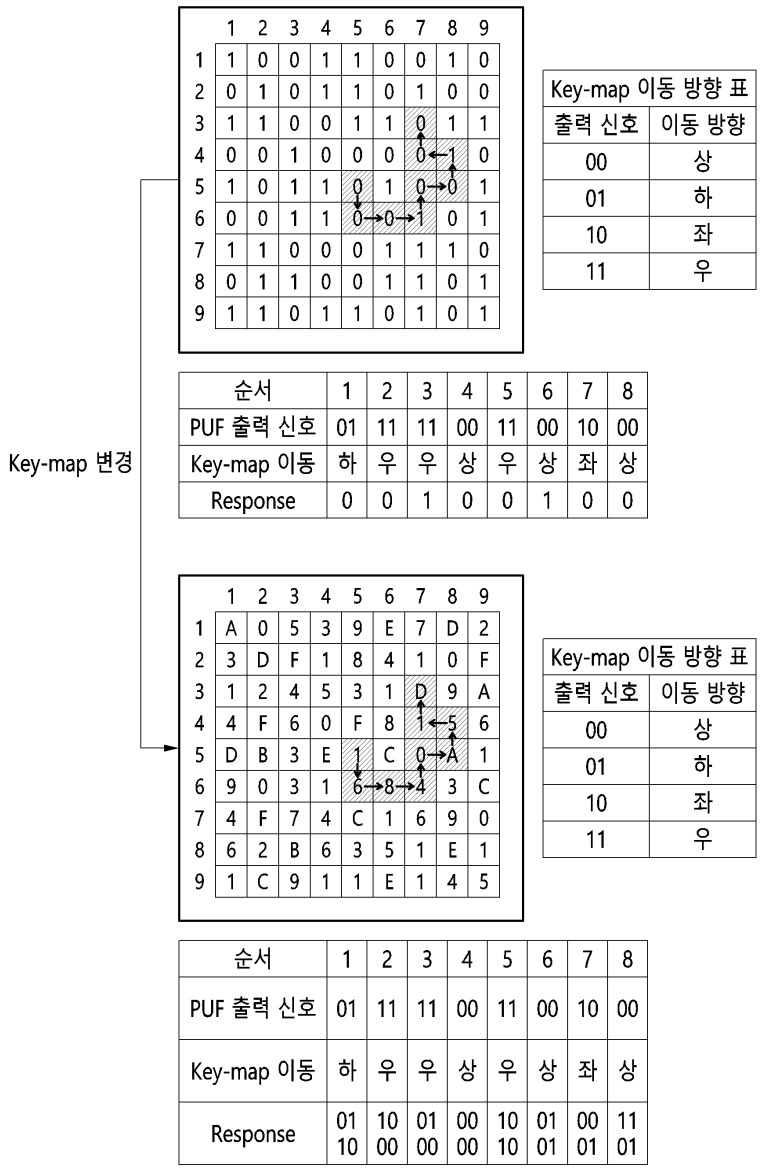
도면1


100
110
인증 기관
PUF 입출력 신호표
Key-map 이동 방향표
Key-map
Challenge data
Response data
120
사용자 단말
121
PUF 칩
Key-map 이동 방향표
Key-map

도면2


100
110
인증기관
사용자에게 보낼 Challenge data "1" 선택
PUF 입출력 신호 표
입력 신호 | 출력 신호
1 | 00 00 00 00
2 | 01 01 01 01
3 | 10 10 10 10
4 | 11 11 11 11
PUF 입출력신호표에서 입력신호에 따른 출력신호 "00 00 00 00"
Key-map 이동 방향 표
입력 신호 | 출력 신호
00 | 상
01 | 하
10 | 좌
11 | 우
PUF 출력 신호를 바탕으로 Key-map 이동 경로 추출 "상 상 상 상"
시작점으로부터 경로 따라 Key-map에 적힌 정보로 response 생성
Response data "0 1 0 1"
120
사용자 단말
Challenge data "1"=입력 신호
121
PUF
출력신호 "00 00 00 00"
Key-map 이동 방향 표
입력 신호 | 출력 신호
00 | 상
01 | 하
10 | 좌
11 | 우
PUF 출력 신호를 바탕으로 Key-map 이동 경로를 추출 "상 상 상 상"
시작점으로부터 경로 따라 Key-map에 적힌 정보로 Response 생성
Response data "0 1 0 1"

도면3



	1	2	3	4	5	6	7	8	9
1	1	0	0	1	1	0	0	1	0
2	0	1	0	1	1	0	1	0	0
3	1	1	0	0	1	1	0	1	1
4	0	0	1	0	0	0	0	1	0
5	1	0	1	1	0	1	0	0	1
6	0	0	1	1	0	0	1	0	1
7	1	1	0	0	0	1	1	1	0
8	0	1	1	0	0	1	1	0	1
9	1	1	0	1	1	0	1	0	1

Key-map 이동 방향 표	
출력 신호	이동 방향
00	상
01	하
10	좌
11	우

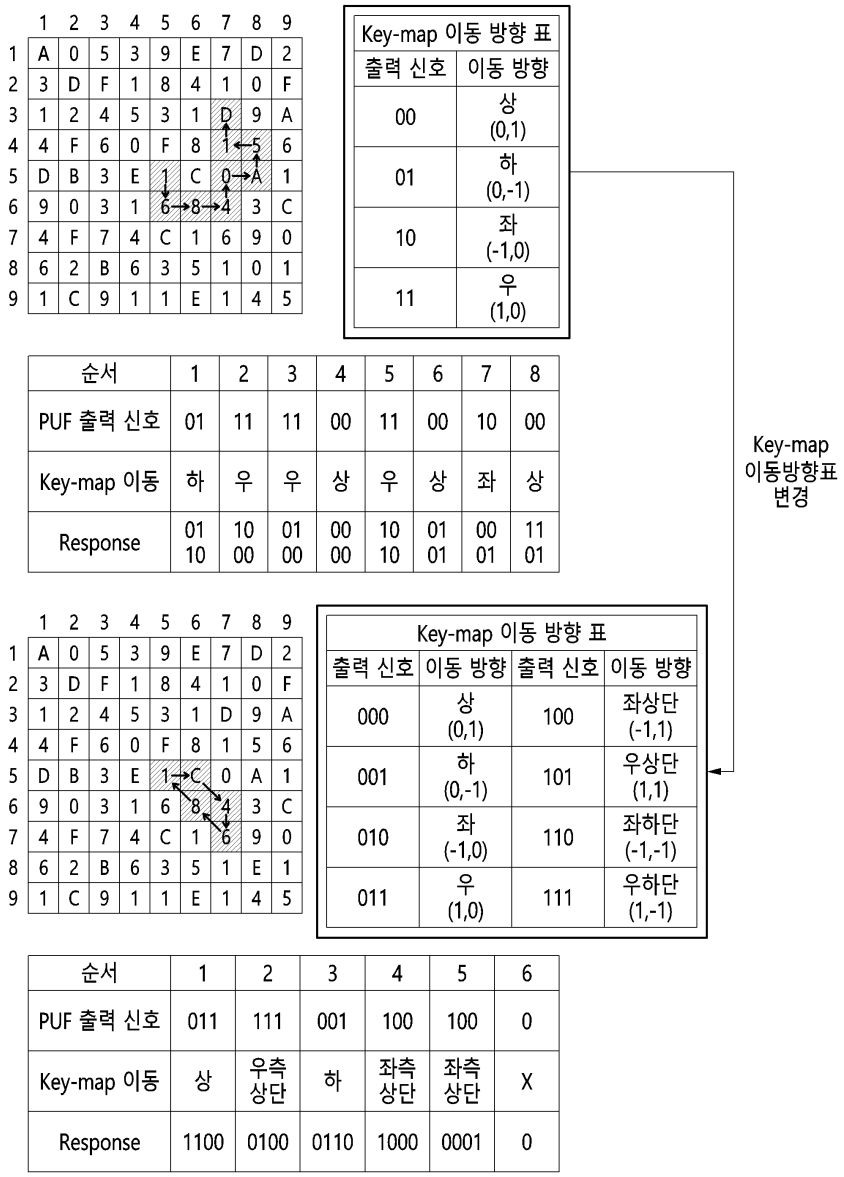
순서	1	2	3	4	5	6	7	8
PUF 출력 신호	01	11	11	00	11	00	10	00
Key-map 이동	하	우	우	상	우	상	좌	상
Response	0	0	1	0	0	1	0	0

	1	2	3	4	5	6	7	8	9
1	A	0	5	3	9	E	7	D	2
2	3	D	F	1	8	4	1	0	F
3	1	2	4	5	3	1	D	9	A
4	4	F	6	0	F	8	1	5	6
5	D	B	3	E	1	C	0	A	1
6	9	0	3	1	6	8	4	3	C
7	4	F	7	4	C	1	6	9	0
8	6	2	B	6	3	5	1	E	1
9	1	C	9	1	1	E	1	4	5

Key-map 이동 방향 표	
출력 신호	이동 방향
00	상
01	하
10	좌
11	우

순서	1	2	3	4	5	6	7	8
PUF 출력 신호	01	11	11	00	11	00	10	00
Key-map 이동	하	우	우	상	우	상	좌	상
Response	01 10	10 00	01 00	00 00	10 10	01 01	00 01	11 01

도면4



	1	2	3	4	5	6	7	8	9
1	A	0	5	3	9	E	7	D	2
2	3	D	F	1	8	4	1	0	F
3	1	2	4	5	3	1	D	9	A
4	4	F	6	0	F	8	1	5	6
5	D	B	3	E	1	C	0	A	1
6	9	0	3	1	6	8	4	3	C
7	4	F	7	4	C	1	6	9	0
8	6	2	B	6	3	5	1	0	1
9	1	C	9	1	1	E	1	4	5

순서	1	2	3	4	5	6	7	8
PUF 출력 신호	01	11	11	00	11	00	10	00
Key-map 이동	하	우	우	상	우	상	좌	상
Response	01 10	10 00	01 00	00 00	10 10	01 01	00 01	11 01

	1	2	3	4	5	6	7	8	9
1	A	0	5	3	9	E	7	D	2
2	3	D	F	1	8	4	1	0	F
3	1	2	4	5	3	1	D	9	A
4	4	F	6	0	F	8	1	5	6
5	D	B	3	E	1	C	0	A	1
6	9	0	3	1	6	8	4	3	C
7	4	F	7	4	C	1	6	9	0
8	6	2	B	6	3	5	1	E	1
9	1	C	9	1	1	E	1	4	5

순서	1	2	3	4	5	6
PUF 출력 신호	011	111	001	100	100	0
Key-map 이동	상	우측 상단	하	좌측 상단	좌측 상단	X
Response	1100	0100	0110	1000	0001	0