



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0109947
(43) 공개일자 2021년09월07일

- (51) 국제특허분류(Int. Cl.)
G06F 21/34 (2013.01) G06F 21/44 (2013.01)
G06F 21/73 (2013.01)
(52) CPC특허분류
G06F 21/34 (2013.01)
G06F 21/44 (2013.01)
(21) 출원번호 10-2020-0025236
(22) 출원일자 2020년02월28일
심사청구일자 2020년02월28일

- (71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
신형순
서울특별시 서초구 반포대로5길 65, 102동 301호 (서초동, 아이파크빌)
김다영
서울특별시 서대문구 이화여대1길 33, 유씨유 1608호(대현동)
(뒷면에 계속)
(74) 대리인
특허법인 무한

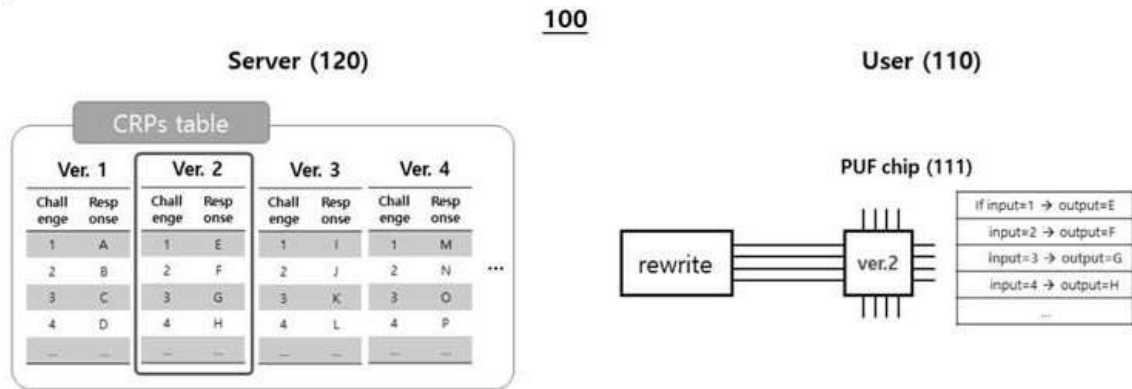
전체 청구항 수 : 총 20 항

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

(57) 요약

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 사용자 단말로부터 인증 요청 메시지를 수신한 경우, 복수의 보안 테이블들 중 어느 하나의 선택된 보안 테이블에 기초하여 인증을 위
(뒷면에 계속)

대표도



한 챌린지(Challenge) 데이터를 결정하여 상기 사용자 단말로 전송하는 단계; 상기 사용자 단말로부터 상기 챌린지 데이터에 대응하는 반응(Response) 데이터를 수신하는 단계; 상기 선택된 보안 테이블에 기초하여 상기 챌린지 데이터와 반응 데이터 간의 매칭 여부에 따라 인증 결과를 도출하는 단계; 및 상기 도출된 인증 결과를 상기 사용자 단말로 전송하는 단계를 포함하고, 상기 복수의 보안 테이블들은 재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 회로를 이용하여 상기 메모리 소자에 대해 서로 다른 기록(Write) 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정될 수 있다.

(52) CPC특허분류

G06F 21/73 (2013.01)

H04L 9/3278 (2013.01)

최서연

경기도 수원시 영통구 애플타운로 65, 5203동 1304호(이의동, 자연앤자이)

(72) 발명자

선우경

서울특별시 서대문구 북아현로4마길 18-6, 2층(북아현동)

이정원

서울특별시 광진구 용마산로1길 78, 1동 603호(중곡동, 대영아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711098989

부처명 과학기술정보통신부

과제관리(전문)기관명 한국연구재단

연구사업명 개인기초연구(과기정통부)(R&D)

연구과제명 CRP(Challenge-Response Pair) 극대화를 위한 멀티비트 맵리스트 기반 PUF(Physical Unclonable Function) 아키텍처 개발

기 여 율 1/1

과제수행기관명 이화여자대학교

연구기간 2019.09.01 ~ 2020.02.29

명세서

청구범위

청구항 1

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

사용자 단말로부터 인증 요청 메시지를 수신한 경우, 복수의 보안 테이블들 중 어느 하나의 선택된 보안 테이블에 기초하여 인증을 위한 챌린지(Challenge) 데이터를 결정하여 상기 사용자 단말로 전송하는 단계;

상기 사용자 단말로부터 상기 챌린지 데이터에 대응하는 반응(Response) 데이터를 수신하는 단계; 및

상기 선택된 보안 테이블에 기초하여 상기 챌린지 데이터와 반응 데이터 간의 매칭 여부에 따라 인증 결과를 도출하는 단계; 및

상기 도출된 인증 결과를 상기 사용자 단말로 전송하는 단계

를 포함하고,

상기 복수의 보안 테이블들은,

재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 회로를 이용하여 상기 메모리 소자에 대해 서로 다른 기록(Write) 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정되는 인증 방법.

청구항 2

제1항에 있어서,

상기 기록 방식은,

상기 메모리 소자가 멤리스터(Memristor)인 경우, 상기 PUF 회로에 인가되는 기록 전압이 변경되는 인증 방법.

청구항 3

제1항에 있어서,

상기 사용자 단말의 인증에 대한 보안성을 향상시키기 위하여 상기 인증에 필요한 보안 테이블을 변경하는 단계를 더 포함하는 인증 방법.

청구항 4

제3항에 있어서,

상기 변경하는 단계는,

특정 시간 주기 마다 일정 조건에 따라 상기 복수의 보안 테이블들 중 선택되는 보안 테이블이 변경되는 인증 방법.

청구항 5

제3항에 있어서,

상기 변경하는 단계는,

상기 사용자 단말의 인증 시점마다 보안 테이블에 대한 서로 다른 선택 규칙에 기초하여 복수의 보안 테이블들 중 선택되는 보안 테이블이 변경되는 인증 방법.

청구항 6

제5항에 있어서,
 상기 변경하는 단계는,
 상기 사용자 단말로 전송되는 챌린지 데이터를 상기 보안 테이블에 대한 선택 규칙으로 재활용하는 인증 방법.

청구항 7

제5항에 있어서,
 상기 변경하는 단계는,
 상기 챌린지 데이터와 함께 상기 사용자 단말로 전송되는 재기록(Rewrite) 데이터를 상기 보안 테이블에 대한 선택 규칙으로 활용하고,
 상기 재기록 데이터는 상기 복수의 보안 테이블들 중 상기 선택 규칙에 의해 선택되는 보안 테이블에 대한 정보가 포함되는 인증 방법.

청구항 8

제5항에 있어서,
 상기 변경하는 단계는,
 상기 인증 결과가 도출된 인증 완료 시점의 시간 정보를 상기 보안 테이블에 대한 선택 규칙으로 활용하는 인증 방법.

청구항 9

제3항에 있어서,
 상기 변경하는 단계는,
 임의의 시간에 상기 사용자 단말로 전송되는 재기록 데이터에 기초하여 상기 복수의 보안 테이블들 중 선택되는 보안 테이블이 변경되는 인증 방법.

청구항 10

사용자 단말이 수행하는 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 인증 방법에 있어서,
 사용자로부터 인증 요청 명령을 수신한 경우, 서버로 인증 요청 메시지를 전송하는 단계;
 상기 서버와 동일한 보안 테이블에 대응하는 기록(Write) 방식을 결정하는 단계;
 상기 결정된 기록 방식이 제공된 PUF 회로를 이용하여 상기 서버로부터 수신된 챌린지(Challenge) 데이터에 대응하는 반응(Response) 데이터를 출력하는 단계; 및
 상기 출력된 반응 데이터를 상기 서버로 전송하는 단계를 포함하고,
 상기 복수의 보안 테이블들은,
 재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 회로를 이용하여 상기 메모리 소자에 대해 서로 다른 기록 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정되는 인증 방법.

청구항 11

제10항에 있어서,
 상기 기록 방식은,
 상기 메모리 소자가 멤리스터(Memristor)인 경우, 상기 PUF 회로에 인가되는 기록 전압이 변경되는 인증 방법.

청구항 12

제10항에 있어서,

상기 서버는,

상기 사용자 단말의 인증에 대한 보안성을 향상시키기 위하여 상기 인증에 필요한 보안 테이블을 변경하는 인증 방법.

청구항 13

제12항에 있어서,

상기 서버는,

특정 시간 주기 마다 일정 조건에 따라 상기 복수의 보안 테이블들 중 선택되는 보안 테이블을 변경하는 인증 방법.

청구항 14

제12항에 있어서,

상기 서버는,

상기 사용자 단말의 인증 시점마다 보안 테이블에 대한 서로 다른 선택 규칙에 기초하여 복수의 보안 테이블들 중 선택되는 보안 테이블을 변경하는 인증 방법.

청구항 15

제14항에 있어서,

상기 서버는,

상기 사용자 단말로 전송되는 챌린지 데이터를 상기 보안 테이블에 대한 선택 규칙으로 재활용하는 인증 방법.

청구항 16

제14항에 있어서,

상기 서버는,

상기 챌린지 데이터와 함께 상기 사용자 단말로 전송되는 재기록(Rewrite) 데이터를 상기 보안 테이블에 대한 선택 규칙으로 활용하고,

상기 재기록 데이터는 상기 복수의 보안 테이블들 중 상기 선택 규칙에 의해 선택되는 보안 테이블에 대한 정보가 포함되는 인증 방법.

청구항 17

제14항에 있어서,

상기 서버는,

상기 인증 결과가 도출된 인증 완료 시점의 시간 정보를 상기 보안 테이블에 대한 선택 규칙으로 활용하는 인증 방법.

청구항 18

제12항에 있어서,

상기 서버는,

임의의 시간에 상기 사용자 단말로 전송되는 재기록 데이터에 기초하여 상기 복수의 보안 테이블들 중 선택되는 보안 테이블을 변경하는 인증 방법.

청구항 19

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

프로세서

를 포함하고,

상기 프로세서는

사용자 단말로부터 인증 요청 메시지를 수신한 경우, 복수의 보안 테이블들 중 어느 하나의 선택된 보안 테이블에 기초하여 인증을 위한 챌린지(Challenge) 데이터를 결정하여 상기 사용자 단말로 전송하며, 상기 사용자 단말로부터 상기 챌린지 데이터에 대응하는 반응(Response) 데이터를 수신하고, 상기 선택된 보안 테이블에 기초하여 상기 챌린지 데이터와 반응 데이터 간의 매칭 여부에 따라 인증 결과를 도출하며, 상기 도출된 인증 결과를 상기 사용자 단말로 전송하고, 상기 사용자 단말의 인증에 대한 보안성을 향상시키기 위하여 상기 인증에 필요한 보안 테이블을 변경하며,

상기 복수의 보안 테이블들은,

재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 회로를 이용하여 상기 메모리 소자에 대해 서로 다른 기록(Write) 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정되는 인증 장치.

청구항 20

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

프로세서

를 포함하고,

상기 프로세서는,

사용자로부터 인증 요청 명령을 수신한 경우, 서버로 인증 요청 메시지를 전송하고, 상기 서버와 동일한 보안 테이블에 대응하는 기록(Write) 방식을 결정하며, 상기 결정된 기록 방식이 제공된 PUF 회로를 이용하여 상기 서버로부터 수신된 챌린지(Challenge) 데이터에 대응하는 반응(Response) 데이터를 출력하며, 상기 출력된 반응 데이터를 상기 서버로 전송하고, 상기 사용자 단말의 인증에 대한 보안성을 향상시키기 위하여 상기 인증에 필요한 보안 테이블을 변경하며,

상기 복수의 보안 테이블들은,

재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 회로를 이용하여 상기 메모리 소자에 대해 서로 다른 기록 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정되는 인증 장치.

발명의 설명

기술 분야

[0001]

본 발명은 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법 및 인증 장치에 관한 것으로, 보다 구체적으로는 재기록(Rewrite)이 가능한 메모리 소자를 기반으로 한 PUF 회로를 이용하여 보안 테이블의 개수를 증가시키는 방법 및 장치에 관한 것이다.

배경 기술

[0002]

기존의 소프트웨어 기반 보안은 키(key)를 비휘발성 메모리(Non-Volatile Memory, NVM)에 저장해 두는 방식으로 진행되지만, NVM에 저장된 디지털 키는 물리적 공격을 이용한 알고리즘 해킹 속도가 가속화되면서 보안에 취약하다는 단점이 있다. 이를 극복하기 위해 고유의 휘발성 디지털 키를 생성하는 하드웨어 기반 보안 방식의 일종

인 물리적 복제 방지 기능 기술이 고안되었다.

[0003] 물리적 복제 방지 기능 기술은 하드웨어 장비에서 나타나는 예측 불가능하고 조절 불가능한 공정 편차를 키 생성에 활용함으로써, 간단한 하드웨어 칩으로 소프트웨어 보안 방식의 단점을 보완할 수 있는 강력한 키 관리가 가능하다는 장점이 있다.

[0004] 그러나 이와 같은 물리적 복제 방지 기능 기술은 하나의 PUF 칩(회로) 당 하나의 보안 테이블을 가지므로 CRP 개수만큼만 인증 키로 활용할 수 있다는 보안 성능의 한계가 존재하며, 인증 과정에서 하나의 CRP가 유출되었을 시 해당 CRP를 다시는 사용할 수 없는 등 해킹의 위험성이 높아지는 문제가 존재한다.

발명의 내용

해결하려는 과제

[0005] 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법 및 인증 장치에 관한 것으로, 보다 구체적으로는 재기록(Rewrite)이 가능한 메모리 소자를 기반으로 한 PUF 칩을 이용하여 보안 테이블의 개수를 증가시키는 방법 및 장치를 제공한다.

과제의 해결 수단

[0006] 본 발명의 일실시예에 따른 서버가 수행하는 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법은 사용자 단말로부터 인증 요청 메시지를 수신한 경우, 복수의 보안 테이블들 중 어느 하나의 선택된 보안 테이블에 기초하여 인증을 위한 챌린지(Challenge) 데이터를 결정하여 상기 사용자 단말로 전송하는 단계; 상기 사용자 단말로부터 상기 챌린지 데이터에 대응하는 반응(Response) 데이터를 수신하는 단계; 상기 선택된 보안 테이블에 기초하여 상기 챌린지 데이터와 반응 데이터 간의 매칭 여부에 따라 인증 결과를 도출하는 단계; 및 상기 도출된 인증 결과를 상기 사용자 단말로 전송하는 단계를 포함하고, 상기 복수의 보안 테이블들은 재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 칩을 이용하여 상기 메모리 소자에 대해 서로 다른 기록(Write) 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정될 수 있다.

[0007] 상기 기록 방식은 상기 메모리 소자가 메모리스터인 경우, 상기 PUF 칩에 인가되는 기록 전압이 변경될 수 있다.

[0008] 상기 사용자 단말의 인증에 대한 보안성을 향상시키기 위하여 상기 인증에 필요한 보안 테이블을 변경하는 단계를 더 포함할 수 있다.

[0009] 상기 변경하는 단계는 특정 시간 주기마다 일정 조건에 따라 상기 복수의 보안 테이블들 중 선택되는 보안 테이블이 변경될 수 있다.

[0010] 상기 변경하는 단계는 상기 사용자 단말의 인증 시점마다 보안 테이블에 대한 서로 다른 선택 규칙에 기초하여 복수의 보안 테이블들 중 선택되는 보안 테이블이 변경될 수 있다.

[0011] 상기 변경하는 단계는 상기 사용자 단말로 전송되는 챌린지 데이터를 상기 보안 테이블에 대한 선택 규칙으로 재활용할 수 있다.

[0012] 상기 변경하는 단계는 상기 챌린지 데이터와 함께 상기 사용자 단말로 전송되는 재기록(Rewrite) 데이터를 상기 보안 테이블에 대한 선택 규칙으로 활용하고, 상기 재기록 데이터는 상기 복수의 보안 테이블들 중 상기 선택 규칙에 의해 선택되는 보안 테이블에 대한 정보가 포함될 수 있다.

[0013] 상기 변경하는 단계는 상기 인증 결과가 도출된 인증 완료 시점의 시간 정보를 상기 보안 테이블에 대한 선택 규칙으로 활용할 수 있다.

[0014] 상기 변경하는 단계는 임의의 시간에 상기 사용자 단말로 전송되는 재기록 데이터에 기초하여 상기 복수의 보안 테이블들 중 선택되는 보안 테이블이 변경될 수 있다.

[0015] 본 발명의 일실시예에 따른 사용자 단말이 수행하는 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 인증 방법은 사용자로부터 인증 요청 명령을 수신한 경우, 서버로 인증 요청 메시지를 전송하는 단계; 상기 서버와 동일한 보안 테이블에 대응하는 기록(Write) 방식을 결정하는 단계; 상기 결정된 기록 방식이 제공된 PUF 회로를 이용하여 상기 서버로부터 수신된 챌린지(Challenge) 데이터에 대응하는 반응(Response) 데이터를 출력하는 단계; 및 상기 출력된 반응 데이터를 상기 서버로 전송하는 단계를 포함하고, 상기 복수의

보안 테이블들은 재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 회로를 이용하여 상기 메모리 소자에 대해 서로 다른 기록 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정될 수 있다.

- [0016] 상기 기록 방식은 상기 메모리 소자가 멤리스터(Memristor)인 경우, 상기 PUF 회로에 인가되는 기록 전압이 변경될 수 있다.
- [0017] 상기 서버는 상기 사용자 단말의 인증에 대한 보안성을 향상시키기 위하여 상기 인증에 필요한 보안 테이블을 변경할 수 있다.
- [0018] 상기 서버는 특정 시간 주기 마다 일정 조건에 따라 상기 복수의 보안 테이블들 중 선택되는 보안 테이블을 변경할 수 있다.
- [0019] 상기 서버는 상기 사용자 단말의 인증 시점마다 보안 테이블에 대한 서로 다른 선택 규칙에 기초하여 복수의 보안 테이블들 중 선택되는 보안 테이블을 변경할 수 있다.
- [0020] 상기 서버는 상기 사용자 단말로 전송되는 챌린지 데이터를 상기 보안 테이블에 대한 선택 규칙으로 재활용할 수 있다.
- [0021] 상기 서버는 상기 챌린지 데이터와 함께 상기 사용자 단말로 전송되는 재기록(Rewrite) 데이터를 상기 보안 테이블에 대한 선택 규칙으로 활용하고, 상기 재기록 데이터는 상기 복수의 보안 테이블들 중 상기 선택 규칙에 의해 선택되는 보안 테이블에 대한 정보가 포함될 수 있다.
- [0022] 상기 서버는 상기 인증 결과가 도출된 인증 완료 시점의 시간 정보를 상기 보안 테이블에 대한 선택 규칙으로 활용할 수 있다.
- [0023] 상기 서버는 임의의 시간에 상기 사용자 단말로 전송되는 재기록 데이터에 기초하여 상기 복수의 보안 테이블들 중 선택되는 보안 테이블을 변경할 수 있다.
- [0024] 본 발명의 일실시예에 따른 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 인증 방법을 수행하는 인증 장치인 서버는 프로세서를 포함하고, 상기 프로세서는 사용자 단말로부터 인증 요청 메시지를 수신한 경우, 복수의 보안 테이블들 중 어느 하나의 선택된 보안 테이블에 기초하여 인증을 위한 챌린지(Challenge) 데이터를 결정하여 상기 사용자 단말로 전송하며, 상기 사용자 단말로부터 상기 챌린지 데이터에 대응하는 반응(Response) 데이터를 수신하고, 상기 선택된 보안 테이블에 기초하여 상기 챌린지 데이터와 반응 데이터 간의 매칭 여부에 따라 인증 결과를 도출하며, 상기 도출된 인증 결과를 상기 사용자 단말로 전송하고, 상기 사용자 단말의 인증에 대한 보안성을 향상시키기 위하여 상기 인증에 필요한 보안 테이블을 변경하며, 상기 복수의 보안 테이블들은 재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 회로를 이용하여 상기 메모리 소자에 대해 서로 다른 기록(Write) 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정될 수 있다.
- [0025] 본 발명의 일실시예에 따른 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 인증 방법을 수행하는 인증 장치인 사용자 단말은 프로세서를 포함하고, 상기 프로세서는 사용자로부터 인증 요청 명령을 수신한 경우, 서버로 인증 요청 메시지를 전송하고, 상기 서버와 동일한 보안 테이블에 대응하는 기록(Write) 방식을 결정하며, 상기 결정된 기록 방식이 제공된 PUF 회로를 이용하여 상기 서버로부터 수신된 챌린지(Challenge) 데이터에 대응하는 반응(Response) 데이터를 출력하며, 상기 출력된 반응 데이터를 상기 서버로 전송하고, 상기 사용자 단말의 인증에 대한 보안성을 향상시키기 위하여 상기 인증에 필요한 보안 테이블을 변경하며, 상기 복수의 보안 테이블들은 재기록(Rewrite)이 가능한 메모리 소자로 구성된 PUF 회로를 이용하여 상기 메모리 소자에 대해 서로 다른 기록 방식을 제공함에 따라 생성되는 복수의 챌린지 데이터들 및 반응 데이터들의 쌍으로 결정될 수 있다.

발명의 효과

- [0026] 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 사용자 단말의 인증 방법 및 인증 장치에 관한 것으로, 보다 구체적으로는 재기록(Rewrite)이 가능한 메모리 소자를 기반으로 한 PUF 칩을 이용하여 보안 테이블의 개수를 증가시킬 수 있다.

도면의 간단한 설명

- [0027] 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 보안 테이블의 선택 방법의 제1 예를 도시한 도면이다.
- 도 3은 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제2 예를 도시한 도면이다.
- 도 4는 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제2 예를 구체화하여 나타낸 도면이다.
- 도 5는 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제3 예를 도시한 도면이다.
- 도 6은 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제4 예를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0028] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0029] 도 1은 본 발명의 일실시예에 따른 물리적 복제 방지 기능(Physical Unclonable Function, PUF)을 이용한 인증 시스템을 도시한 도면이다.
- [0030] 물리적 복제 방지 기능 기술은 공정 편차에 따라 각기 다르게 형성된 PUF 칩(회로)에 챌린지 데이터(Challenge data)라는 특정 입력 신호를 넣었을 때 나오는 출력 신호를 반응 데이터(Response data)라고 하며, 이와 같은 챌린지 데이터-반응 데이터 쌍(Challenge-Response Pair, CRP)을 보안 인증 절차에서 활용할 수 있다. 여기서 하나의 PUF 칩에서 사용할 수 있는 CRP들의 모음을 보안 테이블(CRPs Table)이라고 칭할 수 있다.
- [0031] 일례로, 도 1을 참고하면, 본 발명의 물리적 복제 방지 기능을 이용한 인증 시스템(100)은 사용자 단말(110)과 서버(120)로 구성될 수 있다. 이때, 사용자 단말(110)은 재기록이 가능한 모든 종류의 메모리 소자를 기반으로 하는 PUF 칩(111)이 사용될 수 있다. 이를 통해, 본 발명의 사용자 단말(110)은 PUF 칩(111)의 재기록 특성을 이용하여 기존의 PUF 칩이 하나의 보안 테이블을 가지는 한계를 극복하도록 복수의 보안 테이블을 활용할 수 있으며, 이와 같은 복수의 보안 테이블을 통해 인증 시스템(100)의 보안성을 향상시킬 수 있다.
- [0032] 일례로, 멤리스터(Memristor) 소자의 경우 어떤 기록 전압이 가해지는지에 따라서 각 소자의 저항(Resistance)이 다르게 결정될 수 있다. 이 경우, 본 발명의 사용자 단말(110)의 재기록 블록은 PUF 칩(111)에 서로 다른 기록 전압을 제공하는 기능을 수행할 수 있다. 그리고, PUF 칩(111)은 재기록 블록을 통해 가해지는 기록 전압에 따라 동일한 챌린지 데이터들에 대해 서로 다른 반응 데이터들이 결과로 출력되는 재구성 가능한(Reconfigurable) 특성을 가질 수 있다.
- [0033] 즉, 사용자 단말(110)은 재기록이 가능한 모든 종류의 메모리 소자를 기반으로 하는 하나의 PUF 칩(111)을 통해 재기록 블록을 통한 기록 방식에 따라 서로 다른 보안 테이블을 생성할 수 있으며, 이와 같이 생성된 서로 다른 보안 테이블들은 서버(120)에 기록될 수 있다.
- [0034] 만약 서버(120)가 복수의 보안 테이블들 중 어느 하나의 보안 테이블을 선택한 후 선택된 제1 보안 테이블의 특정 챌린지 데이터를 사용자 단말(110)로 전송하면, 사용자 단말(110)의 재기록 블록은 제1 보안 테이블에 대응하는 기록 방식을 PUF 칩(111)에 제공할 수 있다. 일례로, 재기록 블록은 제1 보안 테이블에 대응하는 기록 전압을 PUF 칩(111)에 인가할 수 있다. 이후 제1 보안 테이블에 대응하는 기록 방식이 제공된 PUF 칩(111)은 서버(120)로부터 수신된 특정 챌린지 데이터에 대한 반응 데이터를 출력할 수 있다.
- [0035] 사용자 단말(110)이 PUF 칩(111)을 통해 출력된 반응 데이터를 서버(120)로 전송하면, 서버(120)는 사전에 기록되어 있는 복수의 보안 테이블들 중 제1 보안 테이블을 이용하여 챌린지 데이터-반응 데이터 쌍의 일치 여부를 판단할 수 있다.
- [0036] 만약 챌린지 데이터-반응 데이터 쌍이 일치하여 인증이 성공한 것으로 판단되면, 서버(120)는 사용자 단말(110)로 인증 성공을 나타내는 인증 결과 메시지를 전송하고, 일치하지 않아 인증이 실패한 것으로 판단되면, 인증 실패를 나타내는 인증 결과 메시지를 전송할 수 있다.
- [0037] 일례로, 도 1을 참고하면, 서버(120)는 복수의 보안 테이블들 중 Ver.2에 대응하는 제1 보안 테이블을 선택한 후 챌린지 데이터로 '3'을 사용자 단말(110)로 전송할 수 있다. 그러면, 사용자 단말(110)의 재기록 블록은 제1 보안 테이블 즉, Ver.2에 대응하는 기록 방식을 PUF 칩(111)에 제공할 수 있다.
- [0038] 이후 제1 보안 테이블에 대응하는 기록 방식이 제공된 PUF 칩(111)은 서버(120)로부터 수신된 챌린지 데이터

'3'에 대한 반응 데이터인 'G'를 출력할 수 있다.

- [0039] 사용자 단말(110)이 출력된 반응 데이터인 'G'를 서버(120)로 전송하면, 서버(120)는 사전에 기록되어 있는 복수의 보안 테이블들 중 제1 보안 테이블을 이용하여 챌린지 데이터-반응 데이터 쌍의 일치 여부를 판단할 수 있다.
- [0040] 제1 보안 테이블의 챌린지 데이터-반응 데이터 쌍을 참고하면, 챌린지 데이터 '3'에 대한 반응 데이터는 'G'이므로 서버(120)는 인증이 성공한 것으로 판단하여 사용자 단말(110)로 인증 성공을 나타내는 인증 결과 메시지를 전송할 수 있다.
- [0041] 이후 물리적 복제 방지 기능을 이용한 인증 시스템(100)에서 서버(120)는 사용자 단말(110)의 인증에 대한 보안성을 향상 시키기 위하여 인증에 필요한 보안 테이블을 제1 보안 테이블에서 제2 보안 테이블로 변경하여 선택할 수 있다. 보다 자세한 보안 테이블 선택 방법은 이후의 도면을 통해 자세히 설명하도록 한다.
- [0042] 도 2는 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제1 예를 도시한 도면이다.
- [0043] 위에서 언급한 바와 같이 물리적 복제 방지 기능을 이용한 인증 시스템(100)에서 서버(120)는 사용자 단말(110)의 인증에 대한 보안성을 향상 시키기 위하여 인증에 필요한 보안 테이블을 변경할 수 있다. 구체적으로 서버(120)는 사용자 단말(110)과 동일한 선택 규칙을 공유하여 보안 테이블을 변경할 수 있다. 이때, 사용자 단말(110)과 서버(120)는 특정 시간 주기마다 일정 조건에 따라 복수의 보안 테이블들 중 어느 하나의 보안 테이블을 선택하는 선택 규칙을 통해 인증에 필요한 보안 테이블을 변경할 수 있다.
- [0044] 일례로, 도 2를 참고하면, 사용자 단말(110)과 서버(120)는 Ver.2에 대응하는 보안 테이블을 이용하여 인증을 수행하고 있다. 이때, 사용자 단말(110)과 서버(120)는 특정 시간 주기(ex. 1시간)마다 일정 조건(ex. Ver.(x+1))에 대응하는 선택 규칙을 통해 보안 테이블을 선택함으로써 인증을 수행할 수 있다. 예를 들어, 현재 Ver.2의 보안 테이블을 사용하고 있으므로, 사용자 단말(110)과 서버(120)는 1시간 뒤에 Ver.3의 보안 테이블로 변경하고, 2시간 뒤에 Ver.4의 보안 테이블로 변경함으로써 인증의 보안성을 증가시킬 수 있다. 이와 같은 선택 규칙은 상기의 예에 한정되지 않고 다양하게 적용될 수 있다.
- [0045] 도 3은 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제2 예를 도시한 도면이다.
- [0046] 도 3을 참고하면, 물리적 복제 방지 기능을 이용한 인증 시스템(100)에서 서버(120)는 인증 전 또는 인증 후에 즉시 보안 테이블을 변경할 수 있다. 구체적으로 서버(120)는 인증 단계에서 사용자 단말(110)로 전송하는 챌린지 데이터를 보안 테이블에 대한 선택 규칙으로 재활용할 수 있다.
- [0047] 일례로, 도 3을 참고하면, 서버(120)는 기존의 ver.2에 대응하는 보안 테이블을 이용하여 '3'에 대응하는 챌린지 데이터를 사용자 단말(110)로 전송할 수 있다. 이때, 서버(120)는 챌린지 데이터 '3'을 이후에 선택되는 보안 테이블의 선택 규칙으로 활용할 수 있다.
- [0048] 구체적으로 사용자 단말(110)의 재기록 블록은 기존의 보안 테이블인 ver.2에 대응하는 기록 방식을 PUF 칩(111)에 제공하므로, PUF 칩(111)은 재기록 블록으로부터 제공받은 기록 방식에 기초하여 챌린지 데이터 '3'에 대한 반응 데이터 'G'를 획득할 수 있다. 이후 사용자 단말(110)이 획득된 반응 데이터 'G'를 서버(120)로 전송하면, 서버(120)는 수신된 반응 데이터 'G'와 보안 테이블 Ver.2를 이용하여 인증 결과를 도출할 수 있다.
- [0049] 이와 같이 인증 결과도 도출되어 인증이 수행된 이후 사용자 단말(110)과 서버(120)는 보안 테이블의 선택 규칙에 의해 기존의 보안 테이블 ver.2를 다른 보안 테이블로 변경할 수 있다. 이때, 사용자 단말(110)과 서버(120)는 위에서 언급한 바와 같이 챌린지 데이터를 보안 테이블에 대한 선택 규칙으로 재활용할 수 있다.
- [0050] 즉, 사용자 단말(110)은 챌린지 데이터 '3'에 대응하여 Ver.3에 대한 기록 방식을 PUF 칩(111)에 제공함으로써 다음 챌린지 데이터에 대한 반응 데이터를 획득할 수 있다. 마찬가지로, 서버(120)는 챌린지 데이터 '3'에 대응하여 보안 테이블 Ver.3을 선택하고, 사용자 단말(110)로부터 수신되는 반응 데이터를 보안 테이블 Ver.3에 적용함으로써 인증 결과를 도출할 수 있다.
- [0051] 도 4는 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제2 예를 구체화하여 나타낸 도면이다.
- [0052] 도 3의 예에서는 챌린지 데이터를 그대로 보안 테이블의 선택 규칙으로 이용하는 구성을 제시하였으나, 실제로 물리적 복제 방지 기능을 이용한 인증 시스템(100)의 사용자 단말(110)과 서버(120) 각각은 챌린지 데이터의 일부를 활용함으로써 이후 사용될 보안 테이블을 선택할 수 있다.

- [0053] 일반적으로 멀티비트(Multi-bit)의 챌린지 데이터를 통해 1비트의 반응 데이터가 출력될 수 있으므로, 길이가 긴 반응 데이터를 활용하기 위해서는 서버(120)가 사용자 단말(110)로 여러 개의 챌린지 데이터를 송신하게 됩니다. 이 경우 본 발명의 인증 시스템(100)은 이와 같은 여러 개의 챌린지 데이터가 합쳐진 챌린지 비트(Challenge bit) 중 일부분, 일례로, 가장 앞의 n 비트 혹은 가장 뒤의 n 비트를 후속하는 보안 테이블의 선택 규칙으로 활용할 수 있다.
- [0054] 이때, 챌린지 데이터의 개수는 어떤 회로에서 어떤 규칙을 적용하는지 또는 소자 어레이(array)의 크기가 얼마나 큰 지에 따라서 결정될 수 있으며, 보안 테이블의 개수는 서버(120)와 사용자가 정의함에 따라 달라질 수 있다.
- [0055] 예를 들어, 도 4는 ① 4 비트의 챌린지 데이터 한 개에서 1비트의 반응 데이터가 출력되고, ② 반응 데이터로 5 비트를 활용하고 싶으며, ③ 보안 테이블 맵(CRPs Map)은 총 4개(2 비트)로 구분하고 싶은 경우를 보여준다. 이 경우 챌린지 데이터의 5개의 합, 총 20 비트의 챌린지 데이터로 1개의 5 비트 반응 데이터가 결정될 수 있다. 만일 보안을 위해 보안 테이블 맵의 개수를 늘리고 싶다면, 선택 규칙으로 활용되는 챌린지 데이터의 앞 또는 뒤의 비트를 늘려 사용할 수 있다. 만약 챌린지 데이터의 앞 또는 뒤의 3 비트를 선택 규칙으로 활용한다면, 총 8개의 보안 테이블 중 하나가 선택될 수 있다.
- [0056] 도 5는 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제3 예를 도시한 도면이다.
- [0057] 도 5를 참고하면, 물리적 복제 방지 기능을 이용한 인증 시스템(100)에서 서버(120)는 인증 전 또는 인증 후에 즉시 보안 테이블을 변경할 수 있다. 구체적으로 서버(120)는 인증 단계에서 사용자 단말(110)의 재기록 블록이 어떤 기록 방식을 PUF 칩(111)에 제공할지를 알려주는 재기록 데이터를 사용자 단말(110)로 전송함으로써 보안 테이블에 대한 선택 규칙으로 활용할 수 있다.
- [0058] 일례로, 도 5와 같이 서버(120)는 기존의 ver.2에 대응하는 보안 테이블의 챌린지 데이터와 변경하고자 하는 보안 테이블에 대한 정보인 재기록 데이터 '4'를 함께 사용자 단말(110)로 전송할 수 있다.
- [0059] 그러면, 사용자 단말(110)의 재기록 블록은 기존의 ver.2에 대응하는 기록 방식을 PUF 칩(111)에 제공하고, PUF 칩(111)은 ver.2에 대응하는 기록 방식에 기초하여 서버(120)로부터 수신된 챌린지 데이터 '3'에 대한 반응 데이터 'G'를 출력할 수 있다.
- [0060] 인증이 완료된 이후 사용자 단말(110)의 재기록 블록은 서버(120)로부터 수신된 재기록 데이터 '4'에 기초하여 기존의 보안 테이블 Ver.2를 보안 테이블 Ver.4로 변경하고, 보안 테이블 Ver.4에 대응하는 기록 방식을 PUF 칩(111)에 제공할 수 있다.
- [0061] 한편, 도 5의 예에서는 인증 시스템(100)에서 서버(120)가 인증 전 또는 인증 후에 재기록 데이터를 이용하여 즉시 보안 테이블을 변경하는 구성을 제공하지만, 이와는 달리 서버(120)가 임의의 시간에 재기록 데이터를 사용자 단말(110)로 전송하여 사용자 단말(110)의 재기록 블록이 기록 방식을 변경하도록 할 수도 있다.
- [0062] 도 6은 본 발명의 일실시예에 따른 보안 테이블의 선택 방법의 제4 예를 도시한 도면이다.
- [0063] 도 6을 참고하면, 물리적 복제 방지 기능을 이용한 인증 시스템(100)에서 서버(120)는 인증 전 또는 인증 후에 즉시 보안 테이블을 변경할 수 있다. 구체적으로 사용자 단말(110)과 서버(120)는 인증 단계에서 인증 완료 시점의 시간 정보를 보안 테이블에 대한 선택 규칙으로 활용할 수 있다.
- [0064] 일례로, 도 6을 참고하면, 서버(120)는 기존의 Ver.2에 대응하는 보안 테이블을 이용하여 사용자 단말(110)에 대한 인증을 수행한 경우, 인증 완료 시점의 시간 정보인 "1시"를 이용하여 이후의 보안 테이블을 Ver.1로 변경할 수 있다.
- [0065] 마찬가지로, 사용자 단말(110)의 재기록 블록 역시 인증이 완료되면, 인증이 완료된 시간 정보 "1시"에 기초하여 Ver.1에 대응하는 기록 방식을 PUF 칩(111)에 제공할 수 있다. 그러면 PUF 칩(111)은 Ver.1에 대응하는 기록 방식에 기초하여 이후에 서버(120)로부터 수신되는 챌린지 데이터에 대한 반응 데이터를 출력할 수 있다.
- [0066] 한편, 본 발명에 따른 방법은 컴퓨터에서 실행될 수 있는 프로그램으로 작성되어 마그네틱 저장매체, 광학적 판독매체, 디지털 저장매체 등 다양한 기록 매체로도 구현될 수 있다.
- [0067] 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 제

품, 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.

[0068] 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 메모리 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.

[0069] 또한, 컴퓨터 판독가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용매체일 수 있고, 컴퓨터 저장매체 및 전송매체를 모두 포함할 수 있다.

[0070] 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.

[0071] 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.

[0072] 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.

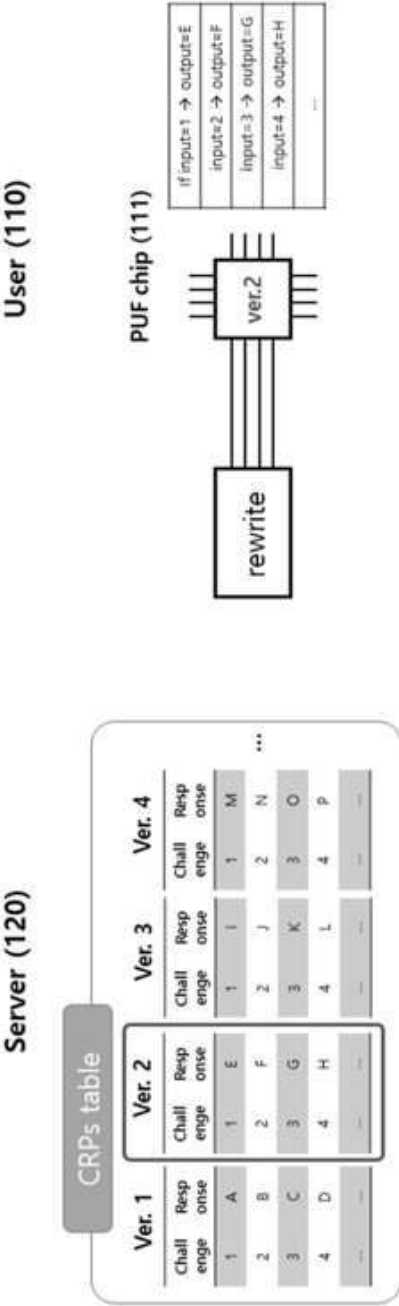
부호의 설명

[0073] 100 : 인증 시스템
110 : 사용자 단말
111 : PUF 칩
120 : 서버

도면

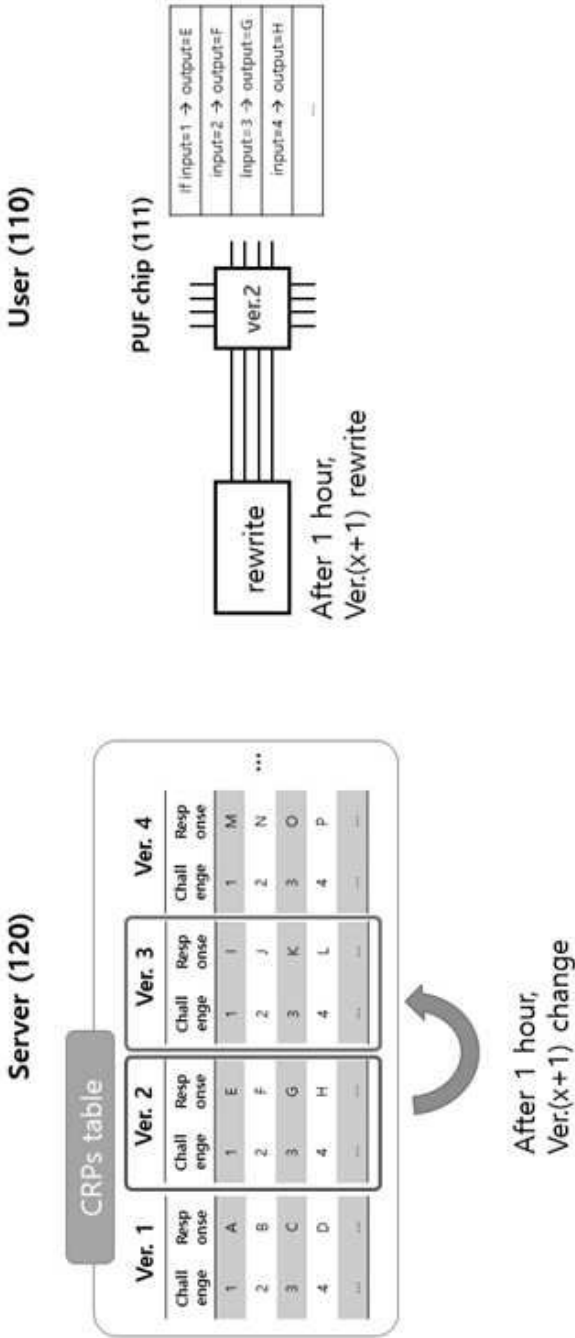
도면1

100



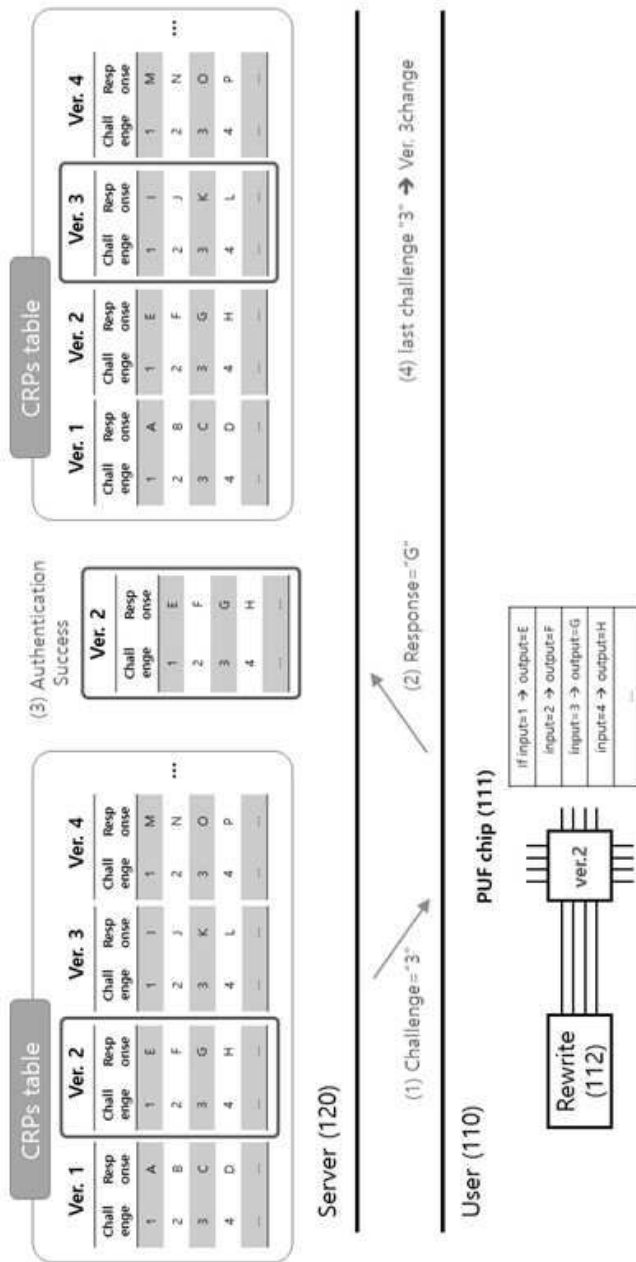
도면2

100

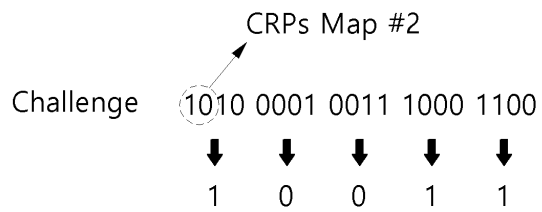


도면3

100



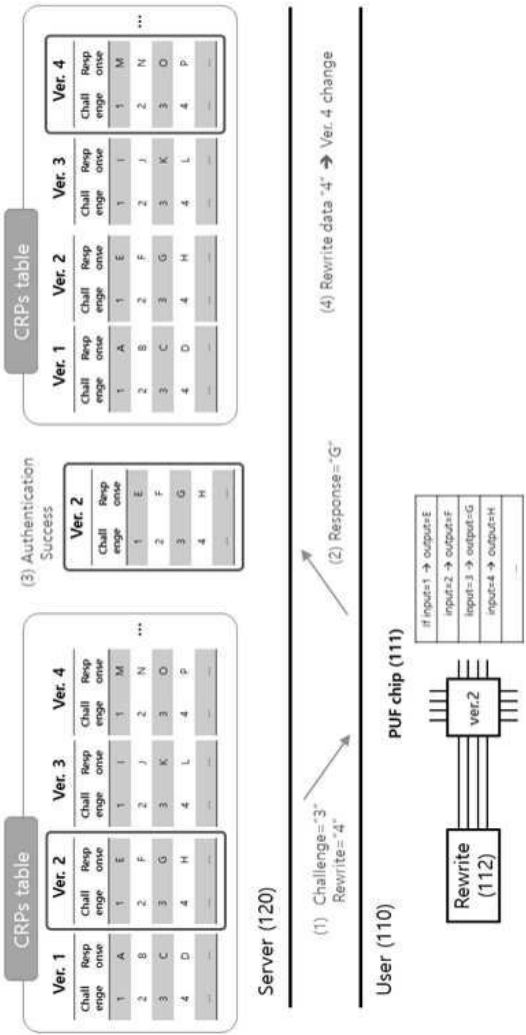
도면4



Challenge	Response			
	Map#0	#1	#2	#3
0000	0	0	1	1
0001	0	1	0	1
0010	0	0	1	0
0011	0	1	0	0
0100	0	0	1	1
0101	0	1	0	1
0110	0	0	1	0
0111	0	1	0	0
1000	1	0	1	1
1001	1	1	0	1
1010	1	0	1	0
1011	1	1	0	0
1100	1	0	1	1
1101	1	1	0	1
1110	1	0	1	0
1111	1	1	0	0

도면5

100



도면6

100

