(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0000485
(43) 공개일자 2021년01월05일

(51) 국제특허분류(Int. Cl.)
*H04L 9/32* (2006.01) *G06F 21/73* (2013.01)
(52) CPC특허분류
*H04L 9/3278* (2013.01)
*G06F 21/73* (2013.01)
(21) 출원번호 10-2019-0075668
(22) 출원일자 2019년06월25일
심사청구일자 2019년06월25일

(71) 출원인
**이화여자대학교 산학협력단**
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
**이정원**
서울특별시 광진구 용마산로1길 78, 1동 603호(중곡동, 대영아파트)
**권효진**
부산광역시 연제구 월드컵대로243번길 19, 101동 1303호(거제동, 거제동원타워)
*(뒷면에 계속)*
(74) 대리인
**특허법인 무한**

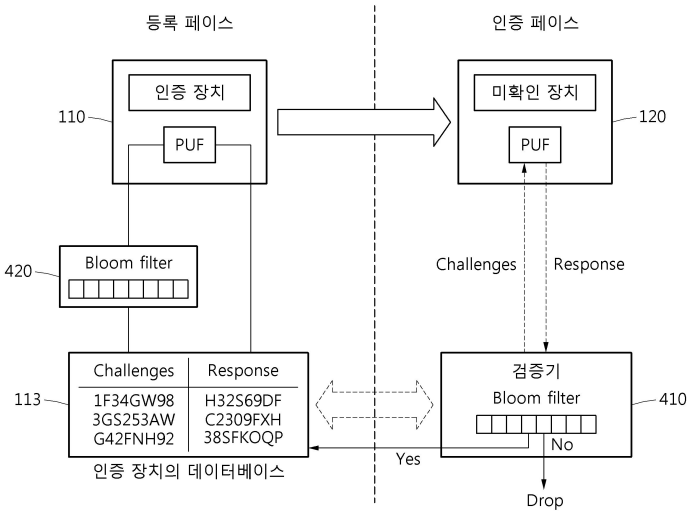
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **블룸 필터를 이용한 물리적 복제 방지 기술 인증 시스템 및 그 방법**

## (57) 요 약

블룸 필터를 이용한 물리적 복제 방지 기술 인증 시스템 및 그 방법이 개시된다. 물리적 복제 방지 기술 인증 방법은 미확인 장치로 챌린지(Challenge)를 전송하는 단계; 상기 미확인 장치로부터 상기 챌린지에 대한 리스폰스(response)를 수신하는 단계; 블룸 필터를 이용하여 상기 리스폰스가 인증 장치의 데이터베이스에 포함되어 있는지 여부를 확인하는 단계; 상기 리스폰스가 데이터베이스에 포함된 것으로 확인된 경우, 상기 데이터베이스에서 상기 리스폰스를 검색하는 단계; 및 상기 리스폰스의 검색 결과에 따라 상기 미확인 장치를 인증하는 단계를 포함하고, 상기 블룸 필터는 상기 데이터베이스에 저장된 리스폰스들을 이용하여 생성될 수 있다.

## 대 표 도



(72) 발명자

**김다영**

서울특별시 중랑구 사가정로42길 90, 502동 301호 (면목동, 면목두산아파트)

**선우경**

서울특별시 서대문구 북아현로4마길 18-6, 2층(북아현동)

이 발명을 지원한 국가연구개발사업

| | |
|---|---|
| 과제고유번호 | 1345292767 |
| 부처명 | 교육부 |
| 과제관리(전문)기관명 | 한국연구재단 |
| 연구사업명 | 이공학학술연구기반구축(R&D) |
| 연구과제명 | 변형된 블룸필터를 적용한 블록체인 시스템 성능 향상에 관한 연구 |
| 기 여 율 | 1/1 |
| 과제수행기관명 | 이화여자대학교 산학협력단 |
| 연구기간 | 2019.03.01 ~ 2020.02.29 |

# 명 세 서

## 청구범위

### 청구항 1

미확인 장치로 챌린지(Challenge)를 전송하는 단계;

상기 미확인 장치로부터 상기 챌린지에 대한 리스폰스(response)를 수신하는 단계;

블룸 필터를 이용하여 상기 리스폰스가 인증 장치의 데이터베이스에 포함되어 있는지 여부를 확인하는 단계;

상기 리스폰스가 데이터베이스에 포함된 것으로 확인된 경우, 상기 데이터베이스에서 상기 리스폰스를 검색하는 단계; 및

상기 리스폰스의 검색 결과에 따라 상기 미확인 장치를 인증하는 단계

를 포함하고,

상기 블룸 필터는

상기 데이터베이스에 저장된 리스폰스들을 이용하여 생성되는 물리적 복제 방지 기술 인증 방법.

### 청구항 2

제1항에 있어서,

상기 리스폰스가 데이터베이스에 포함되지 않은 것으로 확인된 경우, 상기 리스폰스를 제거하고, 상기 미확인 장치를 인증하지 않는 단계

를 더 포함하는 물리적 복제 방지 기술 인증 방법.

### 청구항 3

제1항에 있어서,

상기 미확인 장치는,

블룸 필터를 이용하여 상기 챌린지가 인증 장치로부터 전송된 정보인지 여부를 확인하고, 상기 챌린지가 인증 장치로부터 전송된 정보인 경우, 상기 챌린지를 이용하여 상기 리스폰스를 생성하는 물리적 복제 방지 기술 인증 방법.

### 청구항 4

제1항에 있어서,

상기 미확인 장치를 인증하는 단계는,

상기 데이터베이스에서 상기 리스폰스에 매칭된 챌린지가 상기 미확인 장치에 전송한 챌린지와 동일한 경우, 상기 미확인 장치를 인증하는 단계; 및

상기 데이터베이스에서 상기 리스폰스에 매칭된 챌린지가 상기 미확인 장치에 전송한 챌린지와 서로 다른 경우, 상기 미확인 장치를 인증하지 않는 단계

를 포함하는 물리적 복제 방지 기술 인증 방법.

### 청구항 5

제1항에 있어서,

상기 챌린지에 대한 블룸 필터를 생성하는 단계;

상기 미확인 장치와 서로 다른 미확인 장치로 전송할 챌린지를 상기 챌린지에 대한 블룸 필터에 입력하는 단계;

상기 전송할 챌린지가 상기 챌린지에 대한 블룸 필터에서 양성으로 판단되는 경우, 상기 전송할 챌린지를 삭제하는 단계; 및

상기 전송할 챌린지가 상기 챌린지에 대한 블룸 필터에서 음성으로 판단되는 경우, 상기 전송할 챌린지를 상기 서로 다른 미확인 장치로 전송하는 단계

를 더 포함하는 물리적 복제 방지 기술 인증 방법.

**청구항 6**

외부로부터 챌린지(Challenge)를 수신하는 단계;

블룸 필터를 이용하여 상기 챌린지가 기 등록된 인증 장치로부터 전송된 정보인지 여부를 확인하는 단계;

상기 챌린지가 인증 장치로부터 전송된 정보인 경우, 상기 챌린지를 이용하여 상기 리스폰스를 생성하는 단계; 및

상기 챌린지를 전송한 인증 장치로 상기 리스폰스를 전송하는 단계

를 포함하고,

상기 블룸 필터는,

상기 인증 장치로부터 수신 가능한 챌린지들을 이용하여 생성되는 물리적 복제 방지 기술 인증 방법.

**청구항 7**

제6항에 있어서,

상기 챌린지가 인증 장치로부터 전송된 정보가 아닌 경우, 상기 챌린지를 삭제하는 단계

를 더 포함하는 물리적 복제 방지 기술 인증 방법.

**청구항 8**

제6항에 있어서,

상기 인증 장치는,

블룸 필터를 이용하여 미확인 장치로부터 수신한 상기 리스폰스가 데이터베이스에 포함되어 있는지 여부를 확인하고, 상기 리스폰스가 데이터베이스에 포함된 것으로 확인된 경우, 상기 데이터베이스에서 상기 리스폰스를 검색하여 상기 미확인 장치를 인증하는 물리적 복제 방지 기술 인증 방법.

**청구항 9**

제8항에 있어서,

상기 인증 장치는,

상기 리스폰스가 데이터베이스에 포함되지 않은 것으로 확인된 경우, 상기 리스폰스를 제거하고, 상기 미확인 장치를 인증하지 않는 물리적 복제 방지 기술 인증 방법.

**청구항 10**

미확인 장치로 챌린지를 전송하는 단계;

전송한 챌린지에 대한 블룸 필터를 생성하는 단계;

상기 미확인 장치와 서로 다른 미확인 장치로 전송할 챌린지를 상기 블룸 필터에 입력하는 단계;

상기 전송할 챌린지가 상기 블룸 필터에서 양성으로 판단되는 경우, 상기 전송할 챌린지를 삭제하는 단계; 및

상기 전송할 챌린지가 상기 블룸 필터에서 음성으로 판단되는 경우, 상기 전송할 챌린지를 상기 서로 다른 미확인 장치로 전송하는 단계

를 포함하는 물리적 복제 방지 기술 인증 방법.

**청구항 11**

인증된 장치 별로 적어도 하나의 챌린지와 리스폰스가 매칭하여 저장된 데이터베이스;

미확인 장치로 데이터베이스에 저장된 챌린지들 중 하나를 전송하고, 상기 미확인 장치로부터 상기 챌린지에 대한 리스폰스를 수신하는 통신기; 및

블룸 필터를 이용하여 상기 수신한 리스폰스가 데이터베이스에 포함되어 있는지 여부를 확인하고, 상기 수신한 리스폰스가 데이터베이스에 포함된 것으로 확인된 경우, 상기 데이터베이스에서 상기 리스폰스를 검색하여 상기 미확인 장치를 인증하는 프로세서

를 포함하고,

상기 블룸 필터는

상기 데이터베이스에 저장된 리스폰스들을 이용하여 생성되는 물리적 복제 방지 기술 인증 시스템의 인증 장치.

**청구항 12**

제11항에 있어서,

상기 프로세서는,

상기 리스폰스가 데이터베이스에 포함되지 않은 것으로 확인된 경우, 상기 리스폰스를 제거하고, 상기 미확인 장치를 인증하지 않는 물리적 복제 방지 기술 인증 시스템의 인증 장치.

**청구항 13**

제11항에 있어서,

상기 챌린지에 대한 블룸 필터를 생성하고, 상기 미확인 장치와 서로 다른 미확인 장치로 전송할 챌린지가 상기 챌린지에 대한 블룸 필터에서 양성으로 판단되는 경우, 상기 전송할 챌린지를 삭제하며, 상기 전송할 챌린지가 상기 챌린지에 대한 블룸 필터에서 음성으로 판단되는 경우, 상기 통신기에게 상기 전송할 챌린지를 상기 서로 다른 미확인 장치로 전송하도록 요청하는 물리적 복제 방지 기술 인증 시스템의 인증 장치.

**청구항 14**

외부로부터 챌린지(Challenge)를 수신하는 통신기; 및

블룸 필터를 이용하여 상기 챌린지가 기 등록된 인증 장치로부터 전송된 정보인지 여부를 확인하고, 상기 챌린지가 인증 장치로부터 전송된 정보인 경우, 상기 챌린지를 이용하여 상기 리스폰스를 생성하는 프로세서

를 포함하고,

상기 통신기는,

상기 챌린지를 전송한 인증 장치로 상기 리스폰스를 전송하며,

상기 블룸 필터는,

상기 인증 장치로부터 수신 가능한 챌린지들을 이용하여 생성되는 물리적 복제 방지 기술 인증 시스템의 미확인 장치.

**청구항 15**

제14항에 있어서,

상기 프로세서는,

상기 챌린지가 인증 장치로부터 전송된 정보가 아닌 경우, 상기 챌린지를 삭제하는 물리적 복제 방지 기술 인증 시스템의 미확인 장치.

**청구항 16**

미확인 장치로 챌린지를 전송하는 통신기; 및

전송한 챌린지에 대한 블룸 필터를 생성하고, 상기 미확인 장치와 서로 다른 미확인 장치로 전송할 챌린지가 상기 블룸 필터에서 양성으로 판단되는 경우, 상기 전송할 챌린지를 삭제하며, 상기 전송할 챌린지가 상기 블룸 필터에서 음성으로 판단되는 경우, 상기 전송할 챌린지를 상기 서로 다른 미확인 장치로 전송하도록 상기 통신기에게 요청하는 프로세서

를 포함하는 물리적 복제 방지 기술 인증 시스템의 인증 장치.

## 발명의 설명

### 기 술 분 야

[0001] 본 발명은 블룸 필터를 이용한 물리적 복제 방지 기술 인증 시스템 및 방법에 관한 것이다.

### 배 경 기 술

[0002] 물리적 복제 방지 기술(PUF : Physical Unclonable Functions)을 이용한 인증 시스템은 프로세서의 공정 과정에서 발생하는 편차를 이용하여 암호키를 생성하는 하드웨어 기반의 보안 기술이다.

[0003] 종래의 물리적 복제 방지 기술 인증 시스템은 인증 장치에 챌린지와 리스폰스의 쌍(CRP: Challenge-response pair)을 저장하고, 인증하고자 하는 미확인 장치에 챌린지를 전송하며, 미확인 장치가 챌린지에 따라 생성한 리스폰스를 CRP과 비교하여 미확인 장치를 인증하였다.

[0004] 그러나, 인증 장치는 복수의 CRP들을 저장 및 관리하고 있으므로, 미확인 장치가 생성한 리스폰스의 검색에 시간이 소요되는 실정이다. 또한, 미확인 장치가 생성한 리스폰스가 인증 장치의 데이터베이스에 저장된 CRP에 포함되지 않은 경우, 미확인 장치가 생성한 리스폰스가 인증 장치의 데이터베이스에 저장된 CRP에 포함되지 않았다는 것을 확인하기 위하여 인증 장치의 데이터베이스에 저장된 모든 CRP를 검색해야 하므로, 해당 미확인 장치가 인증되지 않는다는 것을 확인하기 위한 자원 및 시간이 많이 소요된다는 문제점이 있었다.

[0005] 그리고, 물리적 복제 방지 기술 인증 시스템을 공격하는 공격자가 미확인 장치에 임의의 챌린지를 전송하고, 미확인 장치가 그에 대응하여 생성한 리스폰스를 수신하면 미확인 장치의 CRP를 생성할 수도 있다는 문제점도 있었다.

[0006] 따라서, 물리적 복제 방지 기술 인증 시스템의 인증 속도를 향상시키고, 미확인 장치의 CRP가 누출되는 것을 방지할 수 있는 방법이 요청되고 있다.

## 발명의 내용

### 해결하려는 과제

[0007] 본 발명은 인증 장치가 미확인 장치로부터 수신한 리스폰스를 블룸 필터로 필터링하여 인증 장치의 데이터베이스에 저장되어 있지 않은 리스폰스를 삭제함으로써, 인증 장치의 데이터베이스에 저장되어 있지 않은 리스폰스를 인증 장치의 데이터베이스에서 검색하기 위한 자원 낭비를 방지하는 장치 및 방법을 제공할 수 있다.

[0008] 또한, 본 발명은 물리적 복제 방지 기술 인증 시스템이 Strong-PUF인 경우, 전송한 이력이 있는 챌린지에 대한 블룸 필터를 생성하고, 전송할 챌린지가 전송한 이력이 있는 챌린지인지 여부를 블룸 필터로 확인하여 전송한 이력이 있는 챌린지인 경우, 삭제함으로써, CRP의 재사용을 방지하는 장치 및 방법을 제공할 수 있다

[0009] 그리고, 본 발명은 미확인 장치가 인증 장치로부터 수신할 가능성이 있는 챌린지에 대한 블룸 필터를 생성하고, 수신한 챌린지가 인증 장치에서 전송한 챌린지인지 여부를 블룸 필터로 확인하며, 수신한 챌린지가 인증 장치에서 전송하지 않은 챌린지인 경우, 수신한 챌린지를 삭제함으로써, 외부의 공격자가 전송하는 챌린지를 차단하는 장치 및 방법을 제공할 수 있다.

### 과제의 해결 수단

[0010] 본 발명의 일실시예에 따른 인증 장치의 물리적 복제 방지 기술 인증 방법은 미확인 장치로 챌린지(Challenge)

를 전송하는 단계; 상기 미확인 장치로부터 상기 챌린지에 대한 리스폰스(response)를 수신하는 단계; 블룸 필터를 이용하여 상기 리스폰스가 인증 장치의 데이터베이스에 포함되어 있는지 여부를 확인하는 단계; 상기 리스폰스가 데이터베이스에 포함된 것으로 확인된 경우, 상기 데이터베이스에서 상기 리스폰스를 검색하는 단계; 및 상기 리스폰스의 검색 결과에 따라 상기 미확인 장치를 인증하는 단계를 포함하고, 상기 블룸 필터는 상기 데이터베이스에 저장된 리스폰스들을 이용하여 생성될 수 있다.

[0011] 본 발명의 일실시예에 따른 인증 장치의 물리적 복제 방지 기술 인증 방법은 상기 리스폰스가 데이터베이스에 포함되지 않은 것으로 확인된 경우, 상기 리스폰스를 제거하고, 상기 미확인 장치를 인증하지 않는 단계를 더 포함할 수 있다.

[0012] 본 발명의 일실시예에 따른 인증 장치의 물리적 복제 방지 기술 인증 방법의 미확인 장치는, 블룸 필터를 이용하여 상기 챌린지가 인증 장치로부터 전송된 정보인지 여부를 확인하고, 상기 챌린지가 인증 장치로부터 전송된 정보인 경우, 상기 챌린지를 이용하여 상기 리스폰스를 생성할 수 있다.

[0013] 본 발명의 일실시예에 따른 인증 장치의 물리적 복제 방지 기술 인증 방법의 미확인 장치를 인증하는 단계는, 상기 데이터베이스에서 상기 리스폰스에 매칭된 챌린지가 상기 미확인 장치에 전송한 챌린지와 동일한 경우, 상기 미확인 장치를 인증하는 단계; 및 상기 데이터베이스에서 상기 리스폰스에 매칭된 챌린지가 상기 미확인 장치에 전송한 챌린지와 서로 다른 경우, 상기 미확인 장치를 인증하지 않는 단계를 포함할 수 있다.

[0014] 본 발명의 일실시예에 따른 인증 장치의 물리적 복제 방지 기술 인증 방법은 상기 챌린지에 대한 블룸 필터를 생성하는 단계; 상기 미확인 장치와 서로 다른 미확인 장치로 전송할 챌린지를 상기 챌린지에 대한 블룸 필터에 입력하는 단계; 상기 전송할 챌린지가 상기 챌린지에 대한 블룸 필터에서 양성으로 판단되는 경우, 상기 전송할 챌린지를 삭제하는 단계; 및 상기 전송할 챌린지가 상기 챌린지에 대한 블룸 필터에서 음성으로 판단되는 경우, 상기 전송할 챌린지를 상기 서로 다른 미확인 장치로 전송하는 단계를 더 포함할 수 있다.

[0015] 본 발명의 일실시예에 따른 미확인 장치의 물리적 복제 방지 기술 인증 방법은 외부로부터 챌린지(Challenge)를 수신하는 단계; 블룸 필터를 이용하여 상기 챌린지가 기 등록된 인증 장치로부터 전송된 정보인지 여부를 확인하는 단계; 상기 챌린지가 인증 장치로부터 전송된 정보인 경우, 상기 챌린지를 이용하여 상기 리스폰스를 생성하는 단계; 및 상기 챌린지를 전송한 인증 장치로 상기 리스폰스를 전송하는 단계를 포함하고, 상기 블룸 필터는, 상기 인증 장치로부터 수신 가능한 챌린지들을 이용하여 생성될 수 있다.

[0016] 본 발명의 일실시예에 따른 미확인 장치의 물리적 복제 방지 기술 인증 방법은 상기 챌린지가 인증 장치로부터 전송된 정보가 아닌 경우, 상기 챌린지를 삭제하는 단계를 더 포함할 수 있다.

[0017] 본 발명의 일실시예에 따른 미확인 장치의 물리적 복제 방지 기술 인증 방법의 인증 장치는, 블룸 필터를 이용하여 미확인 장치로부터 수신한 상기 리스폰스가 데이터베이스에 포함되어 있는지 여부를 확인하고, 상기 리스폰스가 데이터베이스에 포함된 것으로 확인된 경우, 상기 데이터베이스에서 상기 리스폰스를 검색하여 상기 미확인 장치를 인증할 수 있다.

[0018] 본 발명의 일실시예에 따른 미확인 장치의 물리적 복제 방지 기술 인증 방법의 인증 장치는, 상기 리스폰스가 데이터베이스에 포함되지 않은 것으로 확인된 경우, 상기 리스폰스를 제거하고, 상기 미확인 장치를 인증하지 않을 수 있다.

[0019] 본 발명의 일실시예에 따른 인증 장치의 물리적 복제 방지 기술 인증 방법은 미확인 장치로 챌린지를 전송하는 단계; 전송한 챌린지에 대한 블룸 필터를 생성하는 단계; 상기 미확인 장치와 서로 다른 미확인 장치로 전송할 챌린지를 상기 블룸 필터에 입력하는 단계; 상기 전송할 챌린지가 상기 블룸 필터에서 양성으로 판단되는 경우, 상기 전송할 챌린지를 삭제하는 단계; 및 상기 전송할 챌린지가 상기 블룸 필터에서 음성으로 판단되는 경우, 상기 전송할 챌린지를 상기 서로 다른 미확인 장치로 전송하는 단계를 포함할 수 있다.

[0020] 본 발명의 일실시예에 따른 생성되는 물리적 복제 방지 기술 인증 시스템의 인증 장치는 인증된 장치 별로 적어도 하나의 챌린지와 리스폰스가 매칭하여 저장된 데이터베이스; 미확인 장치로 데이터베이스에 저장된 챌린지들 중 하나를 전송하고, 상기 미확인 장치로부터 상기 챌린지에 대한 리스폰스를 수신하는 통신기; 및 블룸 필터를 이용하여 상기 수신한 리스폰스가 데이터베이스에 포함되어 있는지 여부를 확인하고, 상기 수신한 리스폰스가 데이터베이스에 포함된 것으로 확인된 경우, 상기 데이터베이스에서 상기 리스폰스를 검색하여 상기 미확인 장치를 인증하는 프로세서를 포함하고, 상기 블룸 필터는, 상기 데이터베이스에 저장된 리스폰스들을 이용하여 생성될 수 있다.

[0021] 본 발명의 일실시예에 따른 생성되는 물리적 복제 방지 기술 인증 시스템의 인증 장치의 프로세서는, 상기 리스폰스가 데이터베이스에 포함되지 않은 것으로 확인된 경우, 상기 리스폰스를 제거하고, 상기 미확인 장치를 인증하지 않을 수 있다.

[0022] 본 발명의 일실시예에 따른 생성되는 물리적 복제 방지 기술 인증 시스템의 인증 장치의 프로세서는, 상기 챌린지에 대한 블룸 필터를 생성하고, 상기 미확인 장치와 서로 다른 미확인 장치로 전송할 챌린지가 상기 챌린지에 대한 블룸 필터에서 양성으로 판단되는 경우, 상기 전송할 챌린지를 삭제하며, 상기 전송할 챌린지가 상기 챌린지에 대한 블룸 필터에서 음성으로 판단되는 경우, 상기 통신기에게 상기 전송할 챌린지를 상기 서로 다른 미확인 장치로 전송하도록 요청할 수 있다.

[0023] 본 발명의 일실시예에 따른 생성되는 물리적 복제 방지 기술 인증 시스템의 미확인 장치는 외부로부터 챌린지(Challenge)를 수신하는 통신기; 및 블룸 필터를 이용하여 상기 챌린지가 기 등록된 인증 장치로부터 전송된 정보인지 여부를 확인하고, 상기 챌린지가 인증 장치로부터 전송된 정보인 경우, 상기 챌린지를 이용하여 상기 리스폰스를 생성하는 프로세서를 포함하고, 상기 통신기는, 상기 챌린지를 전송한 인증 장치로 상기 리스폰스를 전송하며, 상기 블룸 필터는, 상기 인증 장치로부터 수신 가능한 챌린지들을 이용하여 생성될 수 있다.

[0024] 본 발명의 일실시예에 따른 생성되는 물리적 복제 방지 기술 인증 시스템의 미확인 장치의 프로세서는, 상기 챌린지가 인증 장치로부터 전송된 정보가 아닌 경우, 상기 챌린지를 삭제할 수 있다.

[0025] 본 발명의 일실시예에 따른 생성되는 물리적 복제 방지 기술 인증 시스템의 인증 장치는 미확인 장치로 챌린지를 전송하는 통신기; 및 전송한 챌린지에 대한 블룸 필터를 생성하고, 상기 미확인 장치와 서로 다른 미확인 장치로 전송할 챌린지가 상기 블룸 필터에서 양성으로 판단되는 경우, 상기 전송할 챌린지를 삭제하며, 상기 전송할 챌린지가 상기 블룸 필터에서 음성으로 판단되는 경우, 상기 전송할 챌린지를 상기 서로 다른 미확인 장치로 전송하도록 상기 통신기에게 요청하는 프로세서를 포함할 수 있다.

## *발명의 효과*

[0026] 본 발명의 일실시예에 의하면, 인증 장치가 미확인 장치로부터 수신한 리스폰스를 블룸 필터로 필터링하여 인증 장치의 데이터베이스에 저장되어 있지 않은 리스폰스를 삭제함으로써, 인증 장치의 데이터베이스에 저장되어 있지 않은 리스폰스를 인증 장치의 데이터베이스에서 검색하기 위한 자원 낭비를 방지할 수 있다.

[0027] 또한, 본 발명의 일실시예에 의하면, 물리적 복제 방지 기술 인증 시스템이 Strong-PUF인 경우, 전송한 이력이 있는 챌린지에 대한 블룸 필터를 생성하고, 전송할 챌린지가 전송한 이력이 있는 챌린지인지 여부를 블룸 필터로 확인하여 전송한 이력이 있는 챌린지인 경우, 삭제함으로써, CRP의 재사용을 방지할 수 있다.

[0028] 그리고, 본 발명의 일실시예에 의하면, 미확인 장치가 인증 장치로부터 수신할 가능성이 있는 챌린지에 대한 블룸 필터를 생성하고, 수신한 첼린지가 인증 장치에서 전송한 챌린지인지 여부를 블룸 필터로 확인하며, 수신한 챌린지가 인증 장치에서 전송하지 않은 챌린지인 경우, 수신한 챌린지를 삭제함으로써, 외부의 공격자가 전송하는 챌린지를 차단할 수 있다.

## *도면의 간단한 설명*

[0029] 도 1은 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 시스템을 나타내는 도면이다.

도 2는 본 발명의 일실시예에 따른 블룸 필터 생성 과정의 일례이다.

도 3은 본 발명의 일실시예에 따른 블룸 필터 쿼리 과정의 일례이다.

도 4는 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 방법의 동작이다.

도 5는 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 방법을 도시한 도면이다.

도 6은 본 발명의 다른 일실시예에 따른 물리적 복제 방지 기술 인증 방법을 도시한 도면이다.

도 7은 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 방법을 도시한 플로우차트이다.

## *발명을 실시하기 위한 구체적인 내용*

[0030] 이하에서, 첨부된 도면을 참조하여 실시예들을 상세하게 설명한다. 그러나, 실시예들에는 다양한 변경이 가해질 수 있어서 특허출원의 권리 범위가 이러한 실시예들에 의해 제한되거나 한정되는 것은 아니다. 실시예들에

대한 모든 변경, 균등물 내지 대체물이 권리 범위에 포함되는 것으로 이해되어야 한다.

[0031] 실시예에서 사용한 용어는 단지 설명을 목적으로 사용된 것으로, 한정하려는 의도로 해석되어서는 안된다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서 상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0033] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0034] 또한, 첨부 도면을 참조하여 설명함에 있어, 도면 부호에 관계없이 동일한 구성 요소는 동일한 참조부호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 실시예의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0035] 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 방법은 물리적 복제 방지 기술 인증 시스템에 의해 수행될 수 있다.

[0036] 도 1은 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 시스템을 나타내는 도면이다.

[0037] 물리적 복제 방지 기술 인증 시스템은 도 1에 도시된 바와 같이 인증 장치(110)와 인증 장치(110)에 인증을 요청하는 미확인 장치(120)로 구성될 수 있다.

[0038] 인증 장치(110)는 블룸 필터를 이용하여 미확인 장치(120)로부터 수신한 리스폰스 중에서 데이터베이스(113)에 저장되어 있지 않은 리스폰스를 데이터베이스(113) 검색 없이 삭제할 수 있다. 예를 들어, 인증 장치(110)는 인증 서버일 수도 있고, 인증 서버에 포함된 하드웨어 장치일 수도 있다.

[0039] 인증 장치(110)의 데이터베이스(113)는 물리적 복제 방지 기술 인증 시스템에 인증된 장치 별로 적어도 하나의 챌린지와 리스폰스를 매칭하여 저장하고 관리할 수 있다.

[0040] 이때, 챌린지(Challenge)는 물리적 복제 방지(PUF: Physical Unclonable Functions) 기술에서 인증된 장치에 입력되는 정보이고, 리스폰스(response)는 챌린지를 입력받은 장치가 출력하는 정보이며, 장치의 공정 과정에서 발생하는 편차에 따라 동일한 챌린지에 대하여 장치별로 서로 다른 리스폰스가 생성될 수 있다. 따라서, 데이터베이스(113)에는 챌린지와 해당 장치에서 출력된 리스폰스를 매칭하여 생성한 챌린지와 리스폰스의 쌍(CRP: Challenge-response pair)들이 저장될 수 있다.

[0041] 인증 장치(110)의 통신기(111)는 미확인 장치(120)로 데이터베이스(113)에 저장된 챌린지들 중 하나를 전송하고, 미확인 장치(120)로부터 챌린지에 대한 리스폰스를 수신할 수 있다.

[0042] 인증 장치(110)의 프로세서(112)는 블룸 필터를 이용하여 통신기(111)가 수신한 리스폰스가 데이터베이스(113)에 포함되어 있는지 여부를 확인할 수 있다. 이때, 블룸 필터는 데이터베이스(113)에 저장된 리스폰스들, 또는 CRP들을 이용하여 생성된 블룸 필터일 수 있다.

[0043] 이때, 프로세서(112)는 통신기(111)가 수신한 리스폰스를 블룸 필터에 입력할 수 있다. 그리고, 블룸 필터의 값이 음성인 경우, 프로세서(112)는 통신기(111)가 수신한 리스폰스가 데이터베이스(113)에 포함되어 있지 않은 것으로 확인할 수 있다. 이때, 데이터베이스(113)에 포함되어 있지 않은 것으로 확인된 리스폰스를 검색할 필요가 없으므로, 프로세서(112)는 통신기(111)가 수신한 리스폰스를 제거하고, 미확인 장치(120)를 인증하지 않을 수 있다.

[0044] 즉, 프로세서(112)는 미확인 장치(120)로부터 수신한 리스폰스를 블룸 필터로 필터링하여 데이터베이스(113)에 저장되어 있지 않은 리스폰스를 삭제함으로써, 데이터베이스(113)에 저장되어 있지 않은 리스폰스를 데이터베이스(113)에서 검색하기 위한 자원 낭비를 방지할 수 있다.

[0045] 또한, 블룸 필터의 값이 양성인 경우, 통신기(111)가 수신한 리스폰스가 데이터베이스(113)에 포함되어 있는 것

으로 확인할 수 있다. 이때, 프로세서(112)는 데이터베이스(113)에서 리스폰스를 검색하여 미확인 장치(120)를 인증할 수 있다.

[0046] 구체적으로, 프로세서(112)는 데이터베이스(113)에서 통신기(111)가 수신한 리스폰스를 검색할 수 있다. 다음으로, 프로세서(112)는 데이터베이스(113)에서 통신기(111)가 수신한 리스폰스에 매칭된 챌린지가 통신기(111)를 통하여 미확인 장치(120)에 전송한 챌린지와 동일한지 여부를 식별할 수 있다.

[0047] 통신기(111)가 수신한 리스폰스에 매칭된 챌린지가 통신기(111)를 통하여 미확인 장치(120)에 전송한 챌린지와 동일한 경우, 프로세서(112)는 미확인 장치(120)를 인증할 수 있다. 반면, 통신기(111)가 수신한 리스폰스에 매칭된 챌린지가 통신기(111)를 통하여 미확인 장치(120)에 전송한 챌린지와 서로 다른 경우, 프로세서(112)는 미확인 장치(120)를 인증하지 않을 수 있다.

[0048] 또한, 인증 장치(110)는 물리적 복제 방지 기술 인증 시스템이 Strong-PUF인 경우, 블룸 필터를 이용하여 CRP의 재사용을 방지할 수 있다.

[0049] 구체적으로, 프로세서(112)는 통신기(111)를 통하여 미확인 장치(120)에 전송한 챌린지에 대한 블룸 필터를 생성할 수 있다.

[0050] 그리고, 미확인 장치(120)와 서로 다른 미확인 장치로 챌린지를 전송해야 하는 경우, 프로세서(112)는 서로 다른 미확인 장치로 전송할 챌린지를 챌린지에 대한 블룸 필터에 입력할 수 있다.

[0051] 이때, 서로 다른 미확인 장치로 전송할 챌린지가 챌린지에 대한 블룸 필터에서 양성으로 판단된다는 것은 서로 다른 미확인 장치로 전송할 챌린지와 미확인 장치(120)에 전송한 챌린지가 동일하다는 것을 의미할 수 있다. 따라서, 서로 다른 미확인 장치로 전송할 챌린지가 챌린지에 대한 블룸 필터에서 양성으로 판단되는 경우, 프로세서(112)는 서로 다른 미확인 장치로 전송할 챌린지를 삭제함으로써, 미확인 장치(120)에 전송한 챌린지가 재사용되는 것을 방지할 수 있다.

[0052] 또한, 서로 다른 미확인 장치로 전송할 챌린지가 챌린지에 대한 블룸 필터에서 음성으로 판단된다는 것은 서로 다른 미확인 장치로 전송할 챌린지와 미확인 장치(120)에 전송한 챌린지가 서로 다르다는 것을 의미할 수 있다. 따라서, 서로 다른 미확인 장치로 전송할 챌린지가 챌린지에 대한 블룸 필터에서 음성으로 판단되는 경우, 프로세서(112)는 서로 다른 미확인 장치로 전송할 챌린지를 예정대로 서로 다른 미확인 장치에 전송할 수 있다.

[0053] 즉, 프로세서(112)는 전송한 이력이 있는 챌린지에 대한 블룸 필터를 생성하고, 전송할 챌린지가 전송한 이력이 있는 챌린지인지 여부를 블룸 필터로 확인하여 전송한 이력이 있는 챌린지인 경우, 삭제함으로써, CRP의 재사용을 방지할 수 있다.

[0054] 인증 장치(110)의 데이터베이스(113)는 물리적 복제 방지 기술 인증 시스템에 인증된 장치 별로 적어도 하나의 챌린지와 리스폰스를 매칭하여 저장하고 관리할 수 있다.

[0055] 미확인 장치(120)는 인증 장치(110)에게 인증을 요청하는 장치이며, 사용자 단말과 같은 휴대형 장치일 수도 있고, 카트리지와 같이 다른 장치에 탈착 가능한 장치일 수도 있다.

[0056] 미확인 장치(120)의 통신기(121)는 인증 장치(110)로부터 챌린지를 수신할 수 있다. 이때, 미확인 장치(120)의 프로세서(122)는 통신기(121)가 수신한 챌린지를 이용하여 리스폰스를 생성할 수 있다. 그리고, 통신기(121)는 프로세서(122)가 생성한 리스폰스를 챌린지를 전송한 인증 장치(110)로 전송할 수 있다.

[0057] 또한, 프로세서(122)는 데이터베이스(123)에 저장된 블룸 필터를 이용하여 통신기(121)가 수신한 챌린지가 기 등록된 인증 장치(110)로부터 전송된 정보인지 여부를 확인할 수도 있다. 이때, 블룸 필터는 기 등록된 적어도 하나의 인증 장치(110)로부터 수신 가능한 챌린지들을 이용하여 생성될 수 있다.

[0058] 구체적으로, 통신기(121)는 사용자로부터의 입력, 오프라인에서의 입력, 또는 인증된 경로에 따른 입력을 통하여 인증 장치(110)가 전송할 수 있는 챌린지들을 획득할 수 있다. 그리고, 프로세서(122)는 인증 장치(110)가 전송할 수 있는 챌린지들에 대한 블룸 필터를 생성하여 데이터베이스(123)에 저장할 수 있다.

[0059] 또한, 프로세서(122)는 통신기(121)가 수신한 챌린지를 블룸 필터에 입력할 수 있다. 그리고, 블룸 필터의 값이 음성인 경우, 프로세서(122)는 통신기(121)가 수신한 챌린지가 인증 장치(110)가 아닌 다른 외부에서 전송된 챌린지인 것으로 식별할 수 있다. 통신기(121)가 수신한 챌린지가 인증 장치(110)가 아닌 다른 외부에서 전송된 챌린지라는 것은 통신기(121)가 수신한 챌린지가 해킹과 같은 외부의 공격자에 의하여 생성된 챌린지라는 것을 의미할 수 있다. 따라서, 프로세서(122)는 통신기(121)가 수신한 챌린지를 삭제함으로써, 공격자가 미확인

장치(120)의 리스폰스를 획득하는 것을 방지할 수 있다.

[0060] 또한, 블룸 필터의 값이 양성인 경우, 프로세서(122)는 통신기(121)가 수신한 챌린지가 인증 장치(110)에서 전송된 챌린지인 것으로 식별할 수 있다. 이때, 프로세서(122)는 통신기(121)가 수신한 챌린지를 이용하여 리스폰스를 생성할 수 있다.

[0061] 즉, 프로세서(122)는 인증 장치(110)가 전송할 가능성이 있는 챌린지에 대한 블룸 필터를 생성하고, 수신한 챌린지가 인증 장치(110)에서 전송한 챌린지인지 여부를 블룸 필터로 확인하며, 수신한 챌린지가 인증 장치(110)에서 전송하지 않은 챌린지인 경우, 수신한 챌린지를 삭제함으로써, 외부의 공격자가 전송하는 챌린지를 차단할 수 있다.

[0062] 도 2는 본 발명의 일실시예에 따른 블룸 필터 생성 과정의 일례이다.

[0063] 단계(210)에서 프로세서(112), 또는 프로세서(122)는 블룸 필터의 모든 셀을0으로 초기화할 수 있다.

[0064] 단계(220)에서 프로세서(112), 또는 프로세서(122)는 집합의 원소를 해시 함수(Hash Function)에 입력하여 해시 인덱스(hash index)를 획득할 수 있다. 그리고, 프로세서(112), 또는 프로세서(122)는 블룸 필터에서 해시 인덱스에 해당되는 값을 1로 변경할 수 있다. 이때, 집합은 데이터베이스(113)에 저장된 리스폰스들의 집합, 데이터베이스(113)에 저장된 CRP들의 집합, 통신기(111)가 전송한 챌린지들의 집합, 또는 인증 장치(110)가 전송할 수 있는 챌린지들의 집합 중 하나일 수 있다.

[0065] 도 3은 본 발명의 일실시예에 따른 블룸 필터 쿼리 과정의 일례이다.

[0066] 프로세서(112), 또는 프로세서(122)는 정보를 해시 함수에 입력하여 획득한 해시 인덱스를 이용하여 블룸 필터의 셀을 확인할 수 있다. 이때, 프로세서(112)가 해시 함수에 입력하는 정보는 미확인 장치(120)로부터 수신한 리스폰스, 또는 미확인 장치로 전송할 챌린지 중 하나이고, 프로세서(112)가 해시 함수에 입력하는 정보는 인증 장치(110)로부터 수신한 챌린지일 수 있다.

[0067] 이때, 케이스 1(Case 1)에 도시된 바와 같이 해시 인덱스가 1,3,5 이고, 블룸 필터에서 1,3,5 셀의 값이 모두 1인 경우, 프로세서(112), 또는 프로세서(122)는 블룸 필터의 값을 양성(positive)으로 판단할 수 있다.

[0068] 또한, 케이스 2(Case 2)에 도시된 바와 같이 해시 인덱스가 0,3,5 이고, 블룸 필터에서 0,3,5 셀의 값들 중 0이 존재하는 경우, 프로세서(112), 또는 프로세서(122)는 블룸 필터의 값을 음성(negative)로 판단할 수 있다.

[0069] 다만, 케이스 3(Case 3)에 도시된 바와 같이 해시 인덱스가 1,5,6 이고, 블룸 필터에서 1,5,6 셀의 값이 모두 1인 경우, 프로세서(112), 또는 프로세서(122)가 집합의 해시 인덱스인 1,3,5와 서로 다른 해시 인덱스를 가진 정보를 양성으로 판단하는 거짓 양성(False positive)가 존재할 가능성도 있다. 이때, 거짓 양성은 블룸 필터의 사이즈를 증가시키거나 변형된 블룸 필터를 적용하면 0에 수렴하게 줄일 수 있다.

[0070] 도 4는 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 방법의 동작이다.

[0071] 인증 페이스에서 미확인 장치(120)는 인증 장치(110)로부터 수신한 챌린지(challenge)를 검증기(410)의 블룸 필터에 입력할 수 있다. 이때, 검증기(410)는 챌린지에 대한 블룸 필터의 값이 음성인 경우, 챌린지를 삭제, 또는 드랍(drop)할 수 있다. 또한, 검증기(410)는 챌린지에 대한 블룸 필터의 값이 양성인 경우, 챌린지를 미확인 장치(120)의 프로세서에 입력할 수 있다. 그리고, 검증기(410)는 미확인 장치(120)의 프로세서가 챌린지에 대한 응답으로 생성한 리스폰스(response)를 인증 장치(110)로 전송할 수 있다.

[0072] 인증 장치(110)는 미확인 장치(120)로부터 수신한 리스폰스를 블룸 필터로 필터링하여 데이터베이스(113)에 저장되어 있지 않은 리스폰스를 삭제할 수 있다.

[0073] 또한, 인증 장치(110)는 미확인 장치(120)로 전송한 챌린지에 대한 블룸 필터(420)를 생성할 수 있다. 그리고, 미확인 장치(120)로 챌린지를 재전송하거나, 다른 미확인 장치로 챌린지를 전송하고자 하는 경우, 인증 장치(110)는 전송할 챌린지를 블룸 필터(420)로 필터링하여 전송할 챌린지가 전송한 이력이 있는 챌린지인지 여부를 확인하고, 전송한 이력이 있는 챌린지인 경우, 삭제함으로써, CRP의 재사용을 방지할 수 있다.

[0074] 도 5는 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 방법을 도시한 도면이다.

[0075] 단계(510)에서 인증 장치(110)는 미확인 장치(120)로 챌린지(Challenge)를 전송할 수 있다.

[0076] 단계(520)에서 미확인 장치(120)는 단계(510)에서 수신한 챌린지를 이용하여 리스폰스를 생성할 수 있다. 그리

고, 미확인 장치(120)는 생성한 리스폰스를 인증 장치(110)로 전송할 수 있다.

[0077] 단계(530)에서 인증 장치(110)는 단계(520)에서 수신한 리스폰스를 블룸 필터에 입력할 수 있다.

[0078] 단계(540)에서 인증 장치(110)는 블룸 필터의 값이 양성인지 여부를 확인할 수 있다. 블룸 필터의 값이 양성인 경우, 리스폰스가 인증 장치(110)의 데이터베이스(113)에 포함되어 있는 것을 의미하므로, 인증 장치(110)는 단계(550)를 수행할 수 있다. 블룸 필터의 값이 음성인 경우, 리스폰스가 인증 장치(110)의 데이터베이스(113)에 포함되어 있지 않다는 것을 의미하므로, 인증 장치(110)는 리스폰스를 제거하고, 인증을 종료할 수 있다.

[0079] 단계(550)에서 인증 장치(110)는 데이터베이스(111)에서 리스폰스를 검색할 수 있다. 이때, 인증 장치(110)는 단계(520)에서 수신한 리스폰스를 블룸 필터에 입력하는 과정에서 단계(520)에서 수신한 리스폰스에 해시 함수를 적용하여 획득한 해시 인덱스를 이용하여 데이터베이스(111)에서 리스폰스를 검색할 수 있다.

[0080] 단계(560)에서 인증 장치(110)는 단계(550)의 검색 결과에 따라 미확인 장치(120)를 인증할 수 있다. 이때, 데이터베이스(113)에서 단계(520)에서 수신한 리스폰스에 매칭된 챌린지가 단계(510)에서 전송한 챌린지와 동일한 경우, 인증 장치(110)는 미확인 장치(120)를 인증할 수 있다. 또한, 데이터베이스(113)에서 단계(520)에서 수신한 리스폰스에 매칭된 챌린지가 단계(510)에서 전송한 챌린지와 서로 다른 경우, 인증 장치(110)는 미확인 장치(120)를 인증하지 않을 수 있다.

[0081] 도 6은 본 발명의 다른 일실시예에 따른 물리적 복제 방지 기술 인증 방법을 도시한 도면이다.

[0082] 단계(610)에서 인증 장치(110)는 미확인 장치(120)로 챌린지(Challenge)를 전송할 수 있다.

[0083] 단계(620)에서 미확인 장치(120)는 단계(610)에서 수신한 챌린지가 기 등록된 인증 장치(110)로부터 전송된 정보인지 여부를 블룸 필터로 확인할 수 있다.

[0084] 단계(630)에서 미확인 장치(120)는 챌린지가 인증 장치(110)로부터 전송된 정보인 경우, 챌린지를 이용하여 리스폰스를 생성할 수 있다. 반면, 챌린지가 인증 장치(110)로부터 전송된 정보가 아닌 경우, 인증 장치(110)는 챌린지를 제거하고, 인증을 종료할 수 있다.

[0085] 단계(640)에서 미확인 장치(120)는 단계(630)에서 생성한 리스폰스를 인증 장치(110)로 전송할 수 있다.

[0086] 단계(650)에서 인증 장치(110)는 단계(640)에서 수신한 리스폰스를 블룸 필터에 입력하고, 블룸 필터의 값이 양성인지 여부를 확인할 수 있다. 블룸 필터의 값이 양성인 경우, 리스폰스가 인증 장치(110)의 데이터베이스(113)에 포함되어 있는 것을 의미하므로, 인증 장치(110)는 단계(660)를 수행할 수 있다. 블룸 필터의 값이 음성인 경우, 리스폰스가 인증 장치(110)의 데이터베이스(113)에 포함되어 있지 않다는 것을 의미하므로, 인증 장치(110)는 리스폰스를 제거하고, 인증을 종료할 수 있다.

[0087] 단계(660)에서 인증 장치(110)는 데이터베이스(111)에서 리스폰스를 검색할 수 있다. 이때, 인증 장치(110)는 단계(620)에서 수신한 리스폰스를 블룸 필터에 입력하는 과정에서 단계(620)에서 수신한 리스폰스에 해시 함수를 적용하여 획득한 해시 인덱스를 이용하여 데이터베이스(111)에서 리스폰스를 검색할 수 있다.

[0088] 단계(670)에서 인증 장치(110)는 단계(660)의 검색 결과에 따라 미확인 장치(120)를 인증할 수 있다. 이때, 데이터베이스(113)에서 단계(620)에서 수신한 리스폰스에 매칭된 챌린지가 단계(610)에서 전송한 챌린지와 동일한 경우, 인증 장치(110)는 미확인 장치(120)를 인증할 수 있다. 또한, 데이터베이스(113)에서 단계(620)에서 수신한 리스폰스에 매칭된 챌린지가 단계(610)에서 전송한 챌린지와 서로 다른 경우, 인증 장치(110)는 미확인 장치(120)를 인증하지 않을 수 있다.

[0089] 도 7은 본 발명의 일실시예에 따른 물리적 복제 방지 기술 인증 방법을 도시한 플로우차트이다.

[0090] 단계(710)에서 인증 장치(110)는 미확인 장치(120)로 챌린지를 전송하고, 전송한 챌린지에 대한 블룸 필터를 생성할 수 있다.

[0091] 단계(720)에서 인증 장치(110)는 미확인 장치(120)와 서로 다른 미확인 장치로 전송할 챌린지, 또는 미확인 장치(120)로 재전송할 챌린지를 단계(710)에서 생성한 블룸 필터에 입력할 수 있다.

[0092] 단계(730)에서 인증 장치(110)는 블룸 필터의 값이 양성인지 여부를 확인할 수 있다. 블룸 필터의 값이 양성인 경우, 서로 다른 미확인 장치로 전송할 챌린지, 또는 미확인 장치(120)로 재전송할 챌린지가 이미 전송된 이력이 있는 챌린지이므로 사용할 수 없다는 것을 의미하므로, 인증 장치(110)는 단계(740)를 수행할 수 있다. 블룸 필터의 값이 음성인 경우, 서로 다른 미확인 장치로 전송할 챌린지, 또는 미확인 장치(120)로 재전송할 챌린

지가 전송된 이력이 없는 챌린지이므로 사용 가능하다는 것을 의미하므로, 인증 장치(110)는 단계(750)를 수행할 수 있다.

[0093] 단계(740)에서 인증 장치(110)는 서로 다른 미확인 장치로 전송할 챌린지, 또는 미확인 장치(120)로 재전송할 챌린지를 삭제하고, 데이터베이스(113)에 저장된 챌린지 중 하나를 재선택하며, 재선택한 챌린지를 전송할 챌린지로 설정하여 단계(720)를 수행할 수 있다.

[0094] 단계(750)에서 인증 장치(110)는 서로 다른 미확인 장치로 전송할 챌린지를 서로 다른 미확인 장치로 전송하거나, 미확인 장치(120)로 재전송할 챌린지를 미확인 장치(120)로 재전송할 수 있다.

[0095] 본 발명은 인증 장치가 미확인 장치로부터 수신한 리스폰스를 블룸 필터로 필터링하여 인증 장치의 데이터베이스에 저장되어 있지 않은 리스폰스를 삭제함으로써, 인증 장치의 데이터베이스에 저장되어 있지 않은 리스폰스를 인증 장치의 데이터베이스에서 검색하기 위한 자원 낭비를 방지할 수 있다.

[0096] 또한, 본 발명은 물리적 복제 방지 기술 인증 시스템이 Strong-PUF인 경우, 전송한 이력이 있는 챌린지에 대한 블룸 필터를 생성하고, 전송할 챌린지가 전송한 이력이 있는 챌린지인지 여부를 블룸 필터로 확인하여 전송한 이력이 있는 챌린지인 경우, 삭제함으로써, CRP의 재사용을 방지할 수 있다.

[0097] 그리고, 본 발명은 미확인 장치가 인증 장치로부터 수신할 가능성이 있는 챌린지에 대한 블룸 필터를 생성하고, 수신한 챌린지가 인증 장치에서 전송한 챌린지인지 여부를 블룸 필터로 확인하며, 수신한 챌린지가 인증 장치에서 전송하지 않은 챌린지인 경우, 수신한 챌린지를 삭제함으로써, 외부의 공격자가 전송하는 챌린지를 차단할 수 있다.

[0098] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0099] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0100] 이상과 같이 실시예들이 비록 한정된 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기를 기초로 다양한 기술적 수정 및 변형을 적용할 수 있다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0101] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 청구범위의 범위에 속한다.

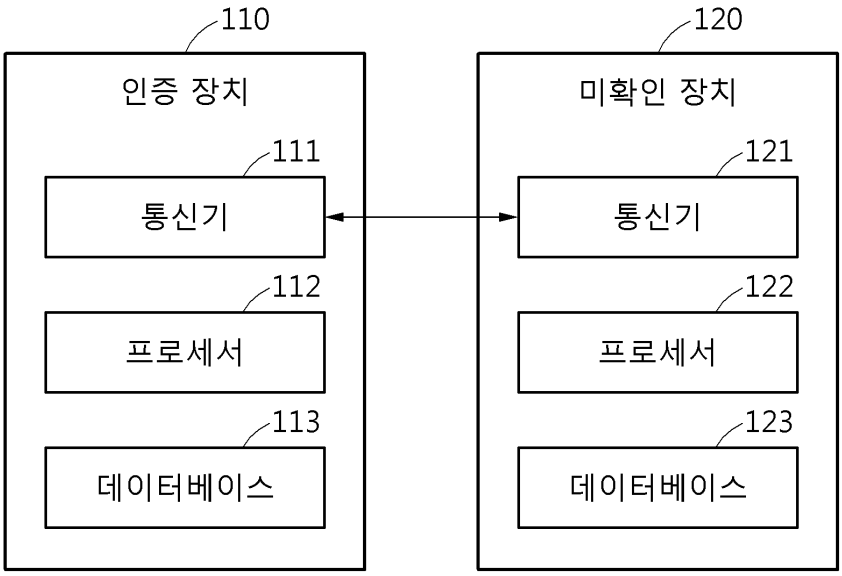
## *부호의 설명*

[0102] 110: 인증 장치

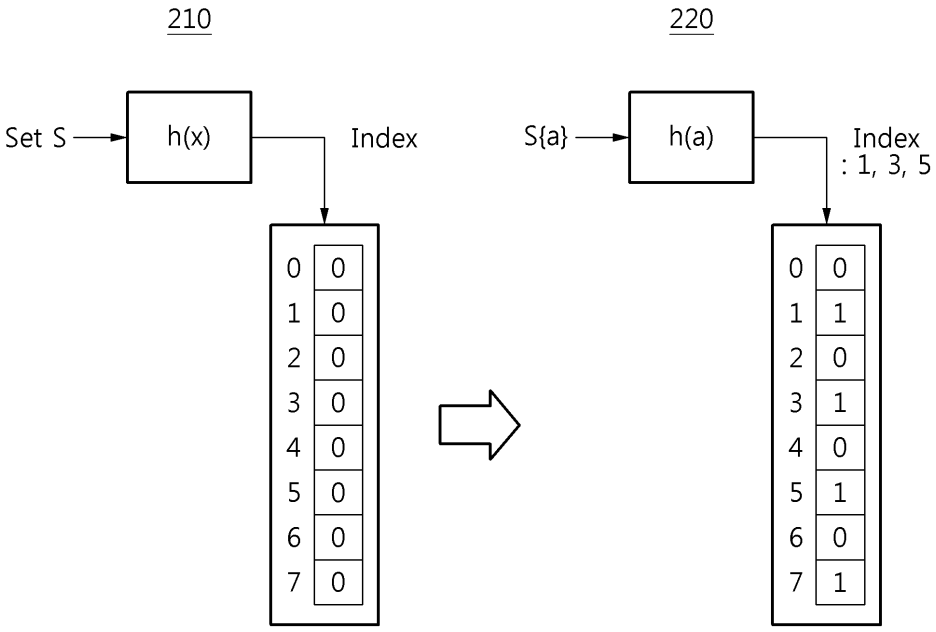
120: 미확인 장치

도면

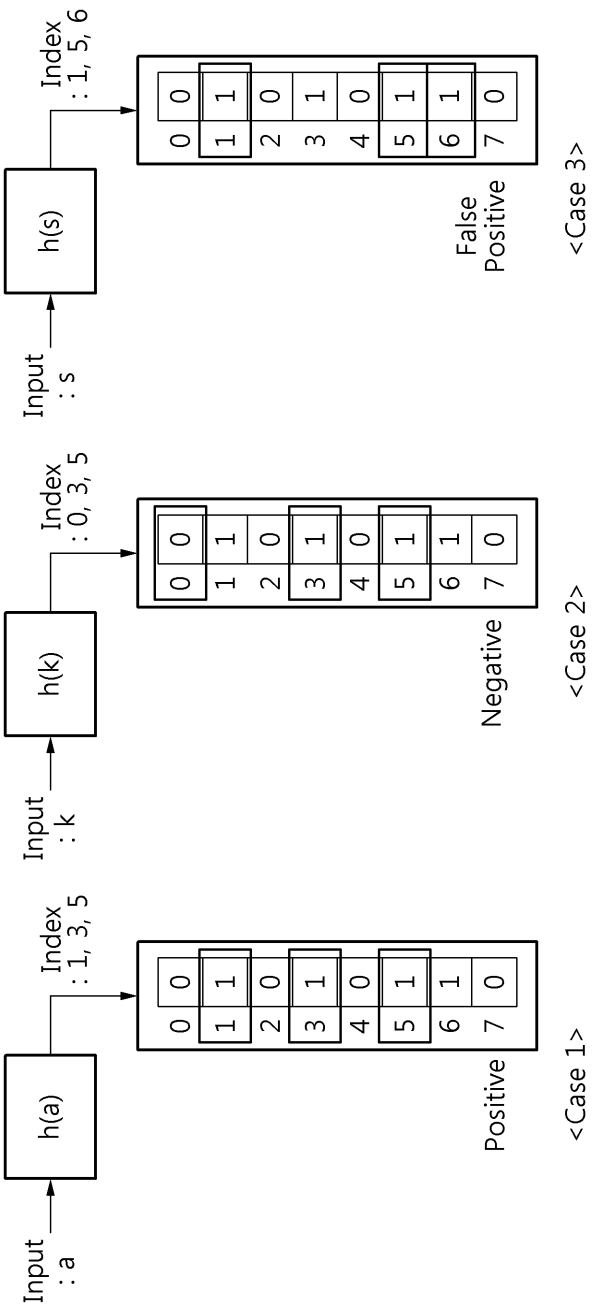
도면1


110
인증 장치
111
통신기
112
프로세서
113
데이터베이스
120
미확인 장치
121
통신기
122
프로세서
123
데이터베이스

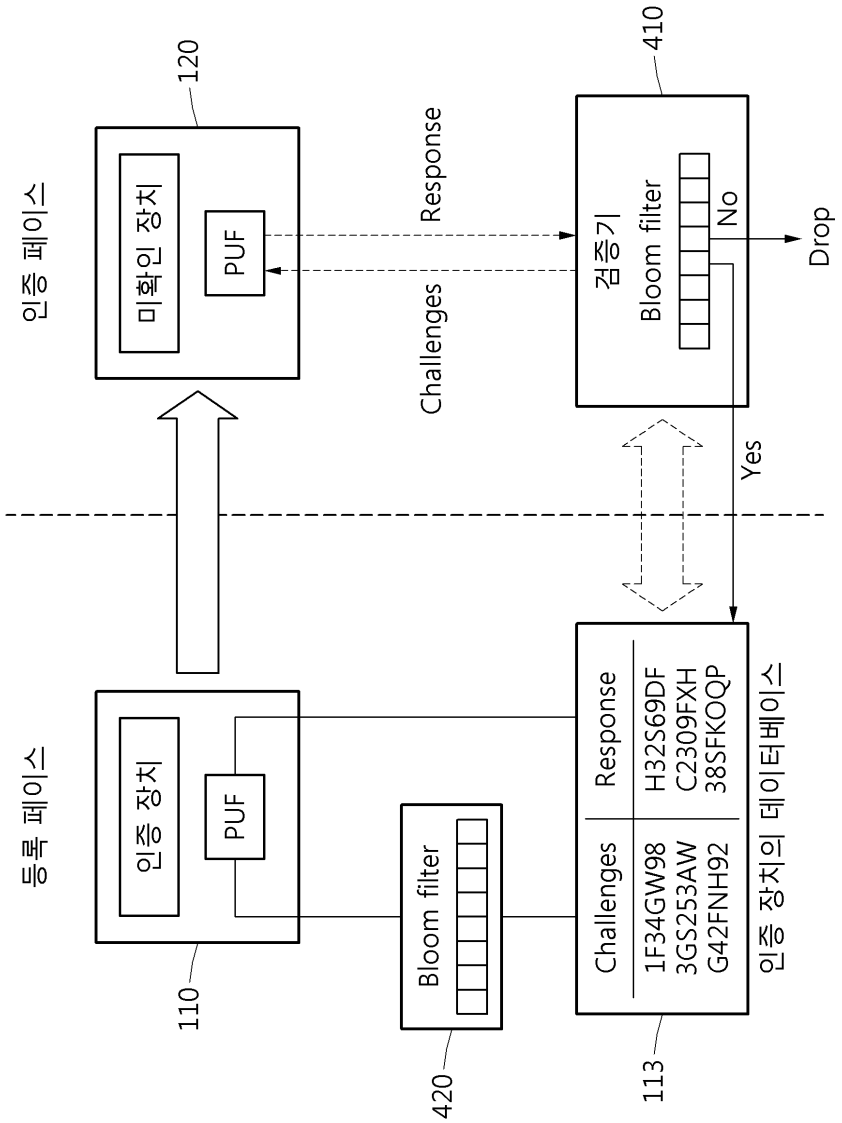
도면2


210
Set S
h(x)
Index
0 0
1 0
2 0
3 0
4 0
5 0
6 0
7 0
220
S{a}
h(a)
Index
: 1, 3, 5
0 0
1 1
2 0
3 1
4 0
5 1
6 0
7 1

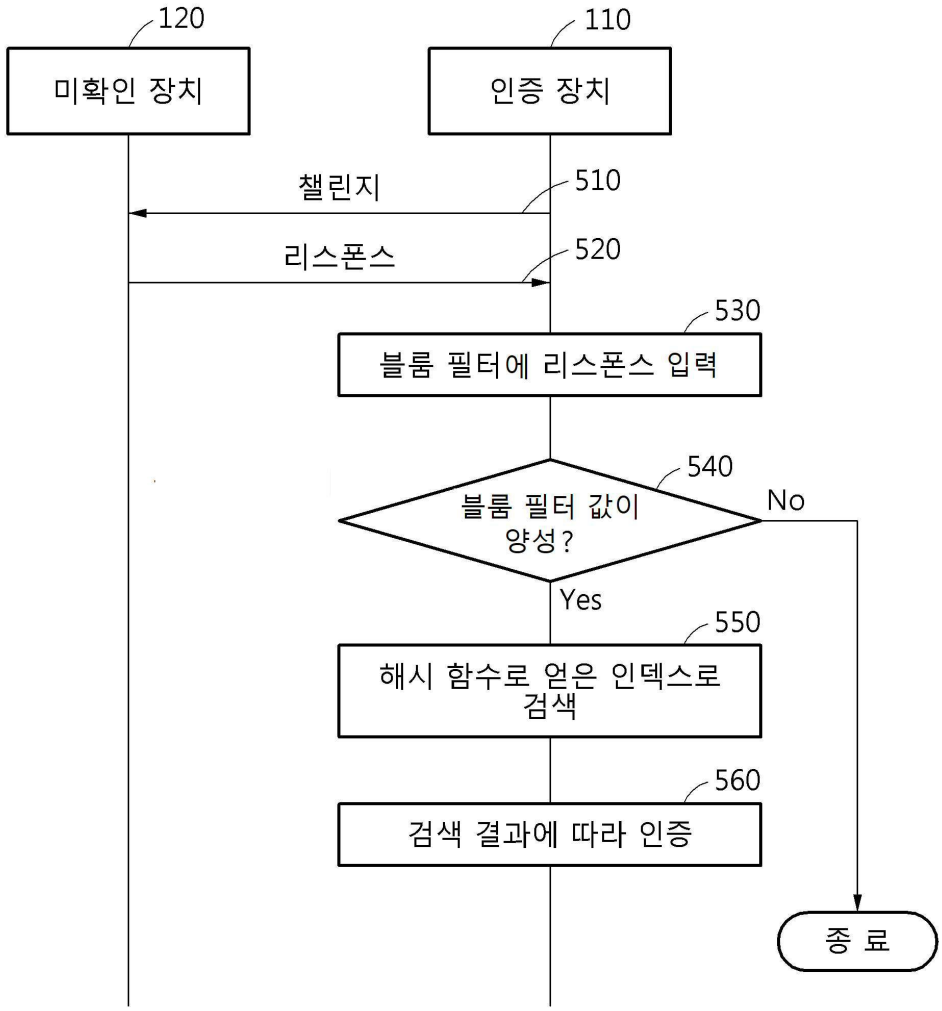
도면3


Input : a
h(a)
Index : 1, 3, 5
Positive
<Case 1>
Input : k
h(k)
Index : 0, 3, 5
Negative
<Case 2>
Input : s
h(s)
Index : 1, 5, 6
False Positive
<Case 3>

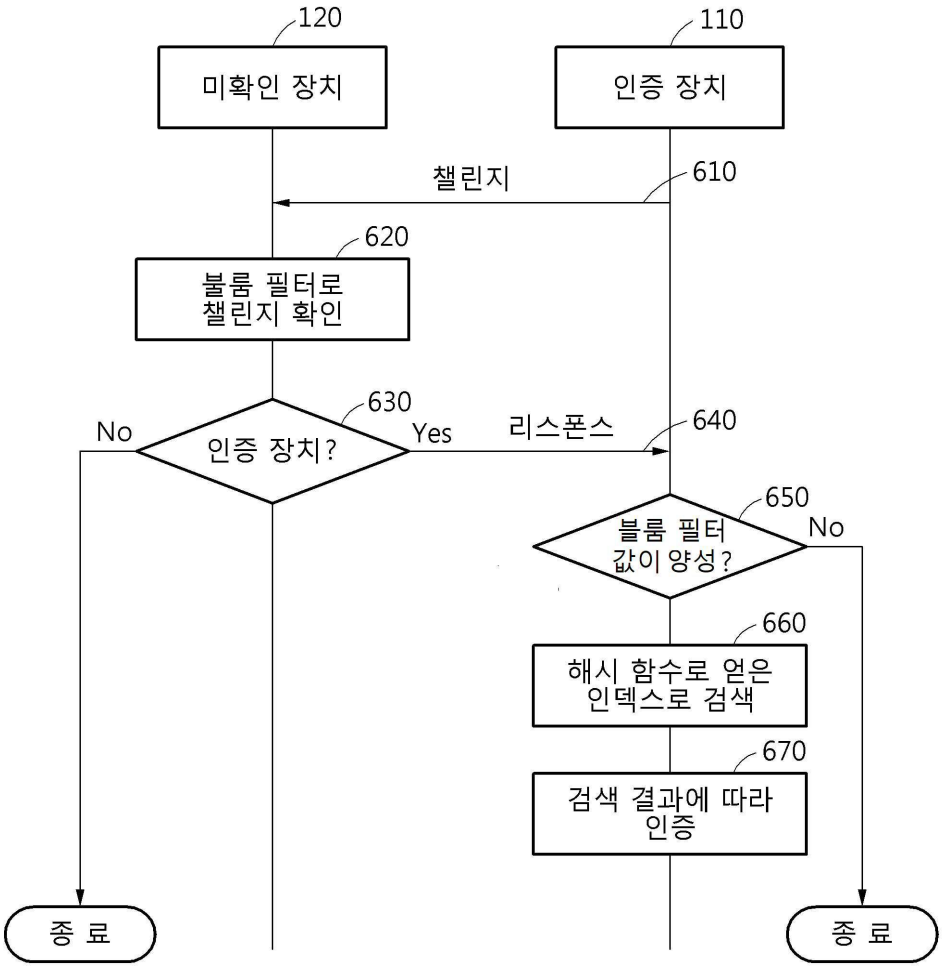
도면4


인증 페이스
미확인 장치
PUF
120
Response
Challenges
410
검증기
Bloom filter
No
Drop
Yes
등록 페이스
인증 장치
PUF
110
Bloom filter
420
Challenges
Response
1F34GW98
3GS253AW
G42FNH92
H32S69DF
C2309FXH
38SFKOQP
113
인증 장치의 데이터베이스

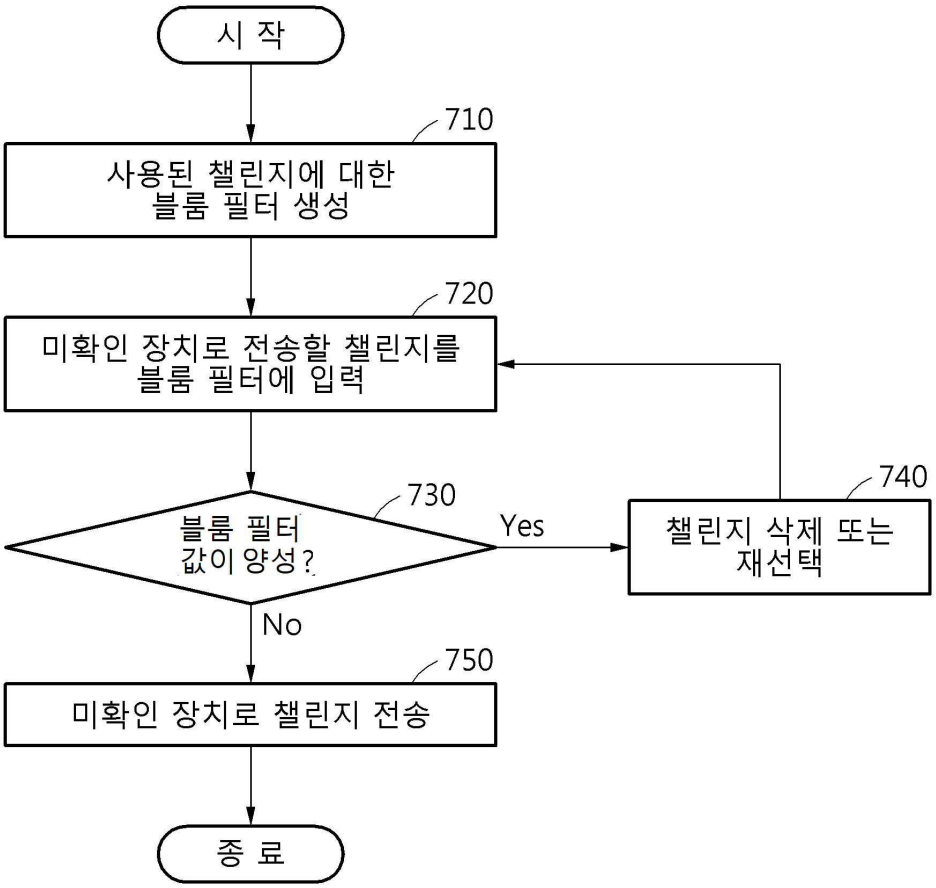
도면5


120
미확인 장치
110
인증 장치
챌린지
510
리스폰스
520
530
블룸 필터에 리스폰스 입력
540
블룸 필터 값이
양성?
No
Yes
550
해시 함수로 얻은 인덱스로
검색
560
검색 결과에 따라 인증
종 료

도면6


120
미확인 장치
110
인증 장치
챌린지
610
620
불룸 필터로
챌린지 확인
630
No
인증 장치?
Yes
리스폰스
640
650
블룸 필터
값이 양성?
No
660
해시 함수로 얻은
인덱스로 검색
670
검색 결과에 따라
인증
종 료
종 료

도면7


시 작
710
사용된 챌린지에 대한
블룸 필터 생성
720
미확인 장치로 전송할 챌린지를
블룸 필터에 입력
730
블룸 필터
값이 양성?
Yes
740
챌린지 삭제 또는
재선택
No
750
미확인 장치로 챌린지 전송
종 료