(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년04월07일
(11) 등록번호 10-1508521
(24) 등록일자 2015년03월30일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2014-0000874
(22) 출원일자 2014년01월03일
심사청구일자 2014년01월03일
(56) 선행기술조사문헌
KR1020050088085 A

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
정익래
서울특별시 광진구 긴고랑로4길 53 203호(중곡1동, 호동아파트)
노건태
서울특별시 강남구 개포로 516 707동 1304호 (개포동, 주공아파트)
천지영
서울특별시 성북구 오패산로 46 118동 104호 (하월곡동, 월곡두산위브아파트)
(74) 대리인
심경식, 홍성욱, 한승범, 유병욱

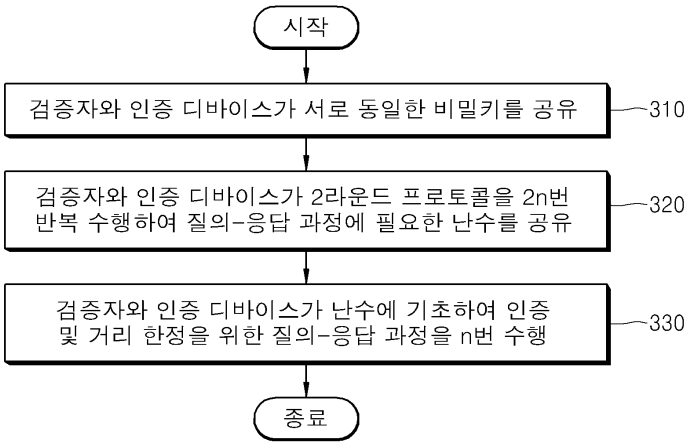
전체 청구항 수 : 총 14 항 심사관 : 문형섭

(54) 발명의 명칭 **LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템 및 방법**

(57) 요 약

본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법은 검증자와 인증 디바이스가 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유하는 단계; 및 상기 검증자와 상기 인증 디바이스가 상기 난수에 기초하여 인증 및 거리 한정을 위한 상기 질의-응답 과정을 n번 수행하는 단계를 포함한다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업
과제고유번호 2013026726
부처명 미래부
연구관리전문기관 한국연구재단
연구사업명 (이공)일반연구자-여성과학자
연구과제명 래티스 기반의 효율적인 서명 및 인증 기법 연구
기 여 율 1/1
주관기관 고려대학교산학협력단
연구기간 2013.05.01 ~ 2014.04.30

명 세 서

청구범위

청구항 1

검증자와 인증 디바이스가 대칭키 기반의 설계 구조에 따라 서로 동일한 비밀키를 공유하는 단계;

상기 검증자와 상기 인증 디바이스가 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유하는 단계; 및

상기 검증자와 상기 인증 디바이스가 상기 난수에 기초하여 인증 및 거리 한정을 위한 상기 질의-응답 과정을 n번 수행하는 단계

를 포함하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 비밀키를 공유하는 단계는

상기 검증자와 상기 인증 디바이스가 k비트열 난수 2개(x, y)와 실수값 $\eta \in \{0,1/2\}$를 상기 비밀키로서 공유하는 단계

를 포함하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법.

청구항 4

제1항에 있어서,

상기 비밀키는

보안 통신 채널을 통한 상기 검증자와 상기 인증 디바이스 간의 교환 방식으로 공유되는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법.

청구항 5

검증자와 인증 디바이스가 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유하는 단계; 및

상기 검증자와 상기 인증 디바이스가 상기 난수에 기초하여 인증 및 거리 한정을 위한 상기 질의-응답 과정을 n번 수행하는 단계

를 포함하고,

상기 인증 및 거리 한정에 사용할 난수를 공유하는 단계는

상기 검증자와 상기 인증 디바이스 간에 상기 난수를 교환하는 단계; 및

상기 난수 및 상기 검증자와 상기 인증 디바이스의 비밀키를 이용하여, 상기 인증 및 거리 한정의 판단에 필요한 값을 계산하여 저장하는 단계

를 포함하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법.

청구항 6

제5항에 있어서,

상기 인증 및 거리 한정에 사용할 난수를 공유하는 단계는

상기 인증 디바이스가 k비트열 난수 b_i를 생성하여 상기 검증자에게 전송하는 제1 단계;

상기 검증자가 k비트열 난수 a_i를 생성하여 상기 인증 디바이스에 전송하는 제2 단계; 및

상기 인증 디바이스가 z_i=(a_i*x)+(b_i*y)+v_i를 계산하여 저장하는 제3 단계

를 포함하고,

상기 제1 내지 제3 단계를 2n 라운드(1≤i≤2n) 동안 반복 수행하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법.

여기서, 상기 v_i∈{0,1|Pr[v_i=1]=η} 이고, 상기 x, y, η는 상기 인증 디바이스와 상기 검증자가 서로 공유하고 있는 비밀키임.

청구항 7

제6항에 있어서,

상기 질의-응답 과정을 n번 수행하는 단계는

n 라운드(1≤i≤n) 동안 시간을 측정하는 단계;

상기 검증자가 C_i∈{0,1|Pr[C_i=1]=η}를 생성하여 상기 인증 디바이스에 전송하는 단계;

상기 인증 디바이스가 상기 C_i의 값에 따라 상기 검증자에게 z_i 또는 z_n+i를 전송하는 단계;

상기 z_i의 값이 (a_i*x)+(b_i*y)와 다른 경우의 발생 횟수를 카운트하는 단계; 및

상기 카운트 된 발생 횟수와 n · η 유사도 및 유효 시간 내에 상기 n번의 질의-응답 과정이 이루어졌는지에 근거하여, 상기 검증자가 상기 인증 디바이스에 대한 인증 및 거리 한정 내 위치에 존재하는지 여부를 판단하는 단계

를 포함하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법.

청구항 8

제7항에 있어서,

상기 인증 디바이스가 상기 C_i의 값에 따라 상기 검증자에게 z_i 또는 z_n+i를 전송하는 단계는

상기 C_i의 값이 0인 경우, 상기 인증 디바이스가 상기 검증자에게 z_i를 전송하는 단계; 및

상기 C_i의 값이 1인 경우, 상기 인증 디바이스가 상기 검증자에게 z_n+i를 전송하는 단계

를 포함하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법.

청구항 9

검증자와 인증 디바이스가 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유하도록 제어하는 난수 공유부; 및

상기 검증자와 상기 인증 디바이스가 상기 난수에 기초하여 인증 및 거리 한정을 위한 상기 질의-응답 과정을 n번 수행하도록 제어하는 질의-응답부

를 포함하고,

상기 검증자와 상기 인증 디바이스는

대칭키 기반의 설계 구조에 따라 서로 동일한 비밀키를 공유하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템.

청구항 10

검증자와 인증 디바이스가 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유하도록 제어하는 난수 공유부; 및

상기 검증자와 상기 인증 디바이스가 상기 난수에 기초하여 인증 및 거리 한정을 위한 상기 질의-응답 과정을 n번 수행하도록 제어하는 질의-응답부

를 포함하고,

상기 난수 공유부는

상기 검증자와 상기 인증 디바이스 간에 상기 난수를 교환하고, 상기 난수 및 상기 검증자와 상기 인증 디바이스의 비밀키를 이용하여, 상기 인증 및 거리 한정의 판단에 필요한 값을 계산하여 저장하는 과정을 상기 2n번 반복 수행하도록 제어하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템.

청구항 11

제10항에 있어서,

상기 난수 공유부는

상기 인증 디바이스가 k비트열 난수 b_i를 생성하여 상기 검증자에게 전송하고, 상기 검증자가 k비트열 난수 a_i를 생성하여 상기 인증 디바이스에 전송하며, 상기 인증 디바이스가 $z_i=(a_i*x)+(b_i*y)+v_i$를 계산하여 저장하는 과정을 2n 라운드($1 \le i \le 2n$) 동안 반복 수행하도록 제어하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템.

여기서, 상기 $v_i \in \{0,1|Pr[v_i=1]=\eta\}$ 이고, 상기 x, y, η는 상기 인증 디바이스와 상기 검증자가 서로 공유하고 있는 비밀키임.

청구항 12

제11항에 있어서,

상기 질의-응답부는

상기 검증자가 n 라운드($1 \le i \le n$) 동안 시간을 측정하고, 상기 검증자가 $C_i \in \{0,1|Pr[C_i=1]=\eta\}$를 생성하여 상기 인증 디바이스에 전송하며, 상기 인증 디바이스가 상기 C_i의 값에 따라 상기 검증자에게 z_i 또는 z_{n+i}를 전송하고, 상기 검증자가 상기 z_i의 값이 $(a_i*x)+(b_i*y)$와 다른 경우의 발생 횟수를 카운트하며, 상기 카운트 된 발생 횟수와 $n \cdot \eta$ 유사도 및 유효 시간 내에 상기 n번의 질의-응답 과정이 이루어졌는지에 근거하여, 상기 검증자가 상기 인증 디바이스에 대한 인증 및 거리 한정 내 위치에 존재하는지 여부를 판단하도록 제어하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템.

청구항 13

제12항에 있어서,

상기 질의-응답부는

상기 C_i의 값이 0인 경우, 상기 인증 디바이스가 상기 검증자에게 z_i를 전송하고, 상기 C_i의 값이 1인 경우, 상기 인증 디바이스가 상기 검증자에게 z_n+i를 전송하도록 제어하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템.

청구항 14

삭제

청구항 15

제9항에 있어서,

상기 검증자와 상기 인증 디바이스는

k비트열 난수 2개(x, y)와 실수값 $\eta \in \{0,1/2\}$를 상기 비밀키로서 공유하는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템.

청구항 16

제9항에 있어서,

상기 비밀키는

보안 통신 채널을 통한 상기 검증자와 상기 인증 디바이스 간의 교환 방식으로 공유되는 것을 특징으로 하는 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 효율적인 경량 인증 및 거리 한정 프로토콜에 관한 것으로서, 더욱 상세하게는 경량 디바이스에 대한 인증을 수행하면서 동시에 거리 한정도 함께 수행하는 방법을 LPN 문제의 어려움에 기반을 두고 설계한 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 경량 디바이스에서 증명이 가능한 인증 프로토콜은 2001년, Hopper와 Blum에 의해서 처음으로 제안되었다. 이 기법은 흔히 HB 프로토콜로 불리며, 2라운드 프로토콜을 n번 반복 수행하여 경량 디바이스에 대한 인증을 수행한다.

[0003] 상기 HB 프로토콜은 수동적인 공격(도청 공격)에 안전하도록 설계되었으며, 이는 LPN 문제의 어려움에 기반을 두고 분석이 가능하다. 2005년, Juels와 Weis는 HB 프로토콜의 안전성을 높인 HB+ 프로토콜을 제안하였다.

[0004] 상기 HB+ 프로토콜은 3라운드 프로토콜을 n번 반복 수행하도록 구성되며, 수동적인 공격뿐만 아니라 적극적인 공격에도 안전하도록 설계되었으며, 이 역시 LPN 문제의 어려움에 기반을 두고 분석이 가능하다.

[0005] 상기 HB 프로토콜과 상기 HB+ 프로토콜 이후, 다수의 인증 프로토콜들이 제안되었으나, LPN 문제에 기반을 두고 설계되지 않거나, 추가적인 연산들, 예를 들면 해시값 계산을 요구하는 등, 경량 디바이스에 적합하지는 않다.

[0006] 한편, 지금까지 거리 한정 프로토콜은 인증 프로토콜이 수행된 이후, 인증과는 별도로 추가적인 과정을 수행하도록 구성되어 왔다. 경량 디바이스에서의 거리 한정이란, 인증받고자 하는 대상인 디바이스(인증 디바이스)가 실제로 그 위치에 존재하는지에 대한 검사를 수행하는 것이다.

[0007] 이에 대한 대표적인 예제는 차량용 무선 키이다. 차량용 무선 키는 실제로는 차와 근접해있는 경우에만 인증이 통과해야 함에도 불구하고, 중계 공격을 통해 근접하지 않은 상황에서도 인증에 통과할 수 있다.

[0008] 이러한 허점을 해결하기 위해서 실제로 인증받으려고 하는 디바이스가 원하는 위치에 존재하는지를 검사할 수 있는 거리 한정 프로토콜이 제안되었으며, 이는 위와 같은 중계 공격을 막을 수 있는 방법이다. 거리 한정 프로토콜은 일반적으로 질의-응답 과정을 n번 수행하여 유효한 시간에 올바른 대답을 하는지를 검사함으로써 중계 공격을 차단하도록 구성된다.

[0009] 지금까지 제안된 증명 가능한 경량 인증 프로토콜은 상기 HB 프로토콜과 상기 HB+ 프로토콜이 대표적이다. 반면, 거리 한정 프로토콜들은 어려운 문제에 기반을 두고 설계되기보다는 확률적인 분석을 통해 기법의 안전성을 분석해왔다. 즉, 아직까지는 거리 한정 프로토콜이 증명 가능한 형태로 설계되지 못하였으며, 이러한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0010] 본 발명의 일 실시예는 경량 디바이스에 대한 인증을 수행하면서 동시에 거리 한정도 함께 수행하는 방법을 LPN 문제의 어려움에 기반을 두고 설계한 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템 및 방법을 제공한다.

[0011] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0012] 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법은 검증자와 인증 디바이스가 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유하는 단계; 및 상기 검증자와 상기 인증 디바이스가 상기 난수에 기초하여 인증 및 거리 한정을 위한 상기 질의-응답 과정을 n번 수행하는 단계를 포함한다.

[0013] 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법은 상기 검증자와 상기 인증 디바이스가 대칭키 기반의 설계 구조에 따라 서로 동일한 비밀키를 공유하는 단계를 더 포함할 수 있다.

[0014] 상기 비밀키를 공유하는 단계는 상기 검증자와 상기 인증 디바이스가 k비트열 난수 2개(x, y)와 실수값 $\eta \in \{0,1/2\}$를 상기 비밀키로서 공유하는 단계를 포함할 수 있다.

[0015] 상기 비밀키는 보안 통신 채널을 통한 상기 검증자와 상기 인증 디바이스 간의 교환 방식으로 공유될 수 있다.

[0016] 상기 인증 및 거리 한정에 사용할 난수를 공유하는 단계는 상기 검증자와 상기 인증 디바이스 간에 상기 난수를 교환하는 단계; 및 상기 난수 및 상기 검증자와 상기 인증 디바이스의 비밀키를 이용하여, 상기 인증 및 거리 한정의 판단에 필요한 값을 계산하여 저장하는 단계를 포함할 수 있다.

[0017] 상기 인증 및 거리 한정에 사용할 난수를 공유하는 단계는 상기 인증 디바이스가 k비트열 난수 b_i를 생성하여 상기 검증자에게 전송하는 제1 단계; 상기 검증자가 k비트열 난수 a_i를 생성하여 상기 인증 디바이스에 전송하는 제2 단계; 및 상기 인증 디바이스가 $z_i=(a_i*x)+(b_i*y)+v_i$를 계산하여 저장하는 제3 단계를 포함하고, 상기 제1 내지 제3 단계를 2n 라운드($1 \le i \le 2n$) 동안 반복 수행할 수 있다. 여기서, 상기 $v_i \in \{0,1|Pr[v_i=1]=\eta\}$ 이고, 상기 x, y, η는 상기 인증 디바이스와 상기 검증자가 서로 공유하고 있는 비밀키일 수 있다.

[0018] 상기 질의-응답 과정을 n번 수행하는 단계는 n 라운드($1 \le i \le n$) 동안 시간을 측정하는 단계; 상기 검증자가 $C_i \in \{0,1|Pr[C_i=1]=\eta\}$를 생성하여 상기 인증 디바이스에 전송하는 단계; 상기 인증 디바이스가 상기 C_i의 값에 따라 상기 검증자에게 z_i 또는 z_{n+i}를 전송하는 단계; 상기 z_i의 값이 $(a_i*x)+(b_i*y)$와 다른 경우의 발생

횟수를 카운트하는 단계; 및 상기 카운트 된 발생 횟수와 $n \cdot \eta$ 유사도 및 유효 시간 내에 상기 n번의 질의-응답 과정이 이루어졌는지에 근거하여, 상기 검증자가 상기 인증 디바이스에 대한 인증 및 거리 한정 내 위치에 존재하는지 여부를 판단하는 단계를 포함할 수 있다.

[0019] 상기 인증 디바이스가 상기 C_i의 값에 따라 상기 검증자에게 z_i 또는 z_n+i를 전송하는 단계는 상기 C_i의 값이 0인 경우, 상기 인증 디바이스가 상기 검증자에게 z_i를 전송하는 단계; 및 상기 C_i의 값이 1인 경우, 상기 인증 디바이스가 상기 검증자에게 z_n+i를 전송하는 단계를 포함할 수 있다.

[0020] 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템은 상기 검증자와 상기 인증 디바이스가 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유하도록 제어하는 난수 공유부; 및 상기 검증자와 상기 인증 디바이스가 상기 난수에 기초하여 인증 및 거리 한정을 위한 상기 질의-응답 과정을 n번 수행하도록 제어하는 질의-응답부를 포함할 수 있다.

[0021] 상기 난수 공유부는 상기 검증자와 상기 인증 디바이스 간에 상기 난수를 교환하고, 상기 난수 및 상기 검증자와 상기 인증 디바이스의 비밀키를 이용하여, 상기 인증 및 거리 한정의 판단에 필요한 값을 계산하여 저장하는 과정을 상기 2n번 반복 수행하도록 제어할 수 있다.

[0022] 상기 난수 공유부는 상기 인증 디바이스가 k비트열 난수 b_i를 생성하여 상기 검증자에게 전송하고, 상기 검증자가 k비트열 난수 a_i를 생성하여 상기 인증 디바이스에 전송하며, 상기 인증 디바이스가 $z_i=(a_i*x)+(b_i*y)+v_i$를 계산하여 저장하는 과정을 2n 라운드($1 \le i \le 2n$) 동안 반복 수행하도록 제어할 수 있다. 여기서, 상기 $v_i \in \{0,1|Pr[v_i=1]=\eta\}$ 이고, 상기 x, y, η는 상기 인증 디바이스와 상기 검증자가 서로 공유하고 있는 비밀키일 수 있다.

[0023] 상기 질의-응답부는 상기 검증자가 n 라운드($1 \le i \le n$) 동안 시간을 측정하고, 상기 검증자가 $C_i \in \{0,1|Pr[C_i=1]=\eta\}$를 생성하여 상기 인증 디바이스에 전송하며, 상기 인증 디바이스가 상기 C_i의 값에 따라 상기 검증자에게 z_i 또는 z_n+i를 전송하고, 상기 검증자가 상기 z_i의 값이 $(a_i*x)+(b_i*y)$와 다른 경우의 발생 횟수를 카운트하며, 상기 카운트 된 발생 횟수와 $n \cdot \eta$ 유사도 및 유효 시간 내에 상기 n번의 질의-응답 과정이 이루어졌는지에 근거하여, 상기 검증자가 상기 인증 디바이스에 대한 인증 및 거리 한정 내 위치에 존재하는지 여부를 판단하도록 제어할 수 있다.

[0024] 상기 질의-응답부는 상기 C_i의 값이 0인 경우, 상기 인증 디바이스가 상기 검증자에게 z_i를 전송하고, 상기 C_i의 값이 1인 경우, 상기 인증 디바이스가 상기 검증자에게 z_n+i를 전송하도록 제어할 수 있다.

[0025] 상기 검증자와 상기 인증 디바이스는 대칭키 기반의 설계 구조에 따라 서로 동일한 비밀키를 공유할 수 있다.

[0026] 상기 검증자와 상기 인증 디바이스는 k비트열 난수 2개(x, y)와 실수값 $\eta \in \{0,1/2\}$를 상기 비밀키로서 공유할 수 있다.

[0027] 상기 비밀키는 보안 통신 채널을 통한 상기 검증자와 상기 인증 디바이스 간의 교환 방식으로 공유될 수 있다.

[0028] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 첨부 도면들에 포함되어 있다.

발명의 효과

[0029] 본 발명의 일 실시예에 따르면, 검증자와 인증 디바이스 간에 난수를 공유하고 그 난수를 이용하여 질의-응답 과정을 일정 횟수 반복 수행함으로써 경량 디바이스에 대한 인증 및 거리 한정을 동시에 수행할 수 있다.

[0030] 따라서, 인증을 원하는 디바이스가 원하는 위치에 존재하는지를 효율적으로 확인할 수 있으며, 특히 차량용 무선 키 인증 환경에서 유용하게 사용될 수 있다. 또한, 인증과 거리 한정을 수행하는 과정에 대한 안전성이 우수하며, 이에 따라 다른 인증과 거리 한정 프로토콜을 각각 사용해서 원하는 결과를 얻는 기존의 방법에 비해 안전성 측면에서 우수한 효과가 있다.

도면의 간단한 설명

[0031] 도 1은 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템의 네트워크 구성을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템을 설명하기 위해 도시한 블록도이다.

도 3은 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법을 설명하기 위해 도시한 흐름도이다.

도 4는 본 발명의 일 실시예에 따라 검증자와 인증 디바이스 간에 난수를 공유하는 과정을 도시한 흐름도이다.

도 5 및 도 6은 본 발명의 일 실시예에 따라 검증자와 인증 디바이스 간에 난수를 공유하는 과정을 보다 구체적으로 설명하기 위해 도시한 도면이다.

도 7 및 도 8은 본 발명의 일 실시예에 따라 검증자와 인증 디바이스 간에 질의-응답을 수행하는 과정을 보다 구체적으로 설명하기 위해 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0032] 본 발명의 이점 및/또는 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성요소를 지칭한다.

[0033] 이하에서는 첨부된 도면을 참조하여 본 발명의 실시예들을 상세히 설명하기로 한다.

[0034] 본 발명에서 제안하는 프로토콜은 대칭키 기반으로 설계된다. 즉, 검증자와 인증 디바이스는 동일한 비밀키를 서로 공유한다. 또한, 본 발명의 질의-응답 과정에서 사용되는 난수는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 사용이 가능하다.

[0035] 본 발명의 일 실시예에서 제안하는 프로토콜의 기능을 도 1을 참조하여 설명하면 다음과 같다. 도 1은 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템의 네트워크 구성을 도시한 도면이다.

[0036] 상기 프로토콜은 대칭키 기반이며, 따라서 검증자(110)와 인증 디바이스(120)가 k비트열 난수 2개 (x, y)와 실수값 $\eta \in \{0, 1/2\}$를 공유한다고 가정한다.

[0037] 2n 라운드($1 \le i \le 2n$)동안, 상기 인증 디바이스(120)는 k비트열 난수 b_i를 생성해서 상기 검증자(110)에게 전송하며, 상기 검증자(110)도 k비트열 난수 a_i를 생성하여 상기 인증 디바이스(120)에게 전송하고, 상기 인증 디바이스(120)는 $z_i=(a_i \cdot x)+(b_i \cdot y)+v_i$를 계산하여 저장한다. 여기서 $v_i \in \{0,1|Pr[v_i=1]=\eta\}$이다.

[0038] 즉, 2n 라운드($1 \le i \le 2n$) 동안, 상기 검증자(110)와 상기 인증 디바이스(120)는 난수 a_i와 b_i를 서로 주고받으며, 이때 상기 인증 디바이스(120)는 z_i를 계산하여 저장한다. 이후, n라운드($1 \le i \le n$)동안 시간을 측정하며 다음과 같이 n 라운드($1 \le i \le n$) 질의-응답 과정을 진행한다.

[0039] 즉, 상기 검증자(110)는 $C_i \in \{0,1|Pr[C_i=1]=\eta\}$를 생성하여 이를 상기 인증 디바이스(120)에 전송하고, 상기 인증 디바이스(120)는 만약 C_i의 값이 0이라면 z_i를 상기 검증자(110)에게 전송하고, C_i의 값이 1이라면 z_{n+i}를 상기 검증자(110)에게 전송한다.

[0040] 결과적으로, 상기 검증자(110)는 상기 인증 디바이스(120)와의 n 라운드 질의-응답 과정이 유효한 시간 내에 이루어졌는지를 검사하며, 이와 동시에 z_i의 값이 $(a_i \cdot x)+(b_i \cdot y)$와 다른 경우가 몇 번 발생하는지를 확인한다. 이때, 다른 경우의 수가 $n \cdot \eta$와 근사하면서 유효한 시간 내에 질의-응답 과정이 이루어졌다면, 상기 검증자(110)는 상기 인증 디바이스(120)가 정당하며 올바른 위치에 존재한다고 판단한다.

[0041] 도 2는 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템을 설명하기

위해 도시한 블록도이다. 여기서, 상기 프로토콜 제공 시스템은 도 1의 검증자(110) 내에 모듈 형태로 탑재되어 구현될 수 있으며, 적용 환경에 따라 다른 형태로 구현될 수 있는 등 다양한 변형이 가능하다.

[0042] 도 1 및 도 2를 참조하면, 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 시스템(200)은 난수 공유부(210), 질의-응답부(220) 및 제어부(230)를 포함할 수 있다.

[0043] 상기 난수 공유부(210)는 상기 검증자(110)와 상기 인증 디바이스(120)가 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유하도록 제어한다.

[0044] 이를 위해, 상기 난수 공유부(210)는 상기 난수 공유를 위한 제어 신호를 발생하여 상기 검증자(110)와 상기 인증 디바이스(120) 간에 상기 난수를 교환하고, 상기 난수 및 비밀키를 이용하여 상기 인증 및 거리 한정의 판단에 필요한 값을 계산하여 저장하는 과정을 2n번 반복 수행하도록 제어할 수 있다.

[0045] 즉, 상기 난수 공유부(210)는 상기 인증 디바이스(120)가 k비트열 난수 b_i를 생성하여 상기 검증자(110)에게 전송하고, 상기 검증자(110)가 k비트열 난수 a_i를 생성하여 상기 인증 디바이스(120)에 전송하며, 상기 인증 디바이스(120)가 z_i=(a_i*x)+(b_i*y)+v_i를 계산하여 저장하는 과정을 2n 라운드($1 \le i \le 2n$) 동안 반복 수행하도록 제어할 수 있다.

[0046] 여기서, 상기 $v_i \in \{0,1|Pr[v_i=1]=\eta\}$ 이고, 상기 x, y, η는 상기 인증 디바이스(120)와 상기 검증자(110)가 서로 안전한 보안 채널을 통해 공유하고 있는 비밀키를 나타낼 수 있다.

[0047] 상기 질의-응답부(220)는 상기 검증자(110)와 상기 인증 디바이스(120)가 상기 난수에 기초하여 인증 및 거리 한정을 위한 질의-응답 과정을 n번 수행하도록 제어한다.

[0048] 구체적으로, 상기 질의-응답부(220)는 상기 질의-응답 과정을 위한 제어신호를 발생하여, 상기 검증자(110)가 n 라운드($1 \le i \le n$) 동안 시간을 측정하고, 상기 검증자(110)가 $C_i \in \{0,1|Pr[C_i=1]=\eta\}$를 생성하여 상기 인증 디바이스(120)에 전송하며, 상기 인증 디바이스(120)가 상기 C_i의 값에 따라 상기 검증자(110)에게 z_i 또는 z_n+i를 전송하도록 제어할 수 있다.

[0049] 계속해서, 상기 질의-응답부(220)는 상기 검증자(110)가 상기 z_i의 값이 (a_i*x)+(b_i*y)와 다른 경우의 발생 횟수를 카운트하며, 상기 카운트 된 발생 횟수와 $n \cdot \eta$ 유사도 및 유효 시간 내에 상기 n번의 질의-응답 과정이 이루어졌는지에 근거하여, 상기 검증자(110)가 상기 인증 디바이스(120)에 대한 인증 및 거리 한정 내 위치에 존재하는지 여부를 판단하도록 제어할 수 있다.

[0050] 이때, 상기 질의-응답부(220)는 상기 C_i의 값이 0인 경우, 상기 인증 디바이스(120)가 상기 검증자(110)에게 z_i를 전송하고, 상기 C_i의 값이 1인 경우, 상기 인증 디바이스(120)가 상기 검증자(110)에게 z_n+i를 전송하도록 제어할 수 있다.

[0051] 도 3은 본 발명의 일 실시예에 따른 LPN 문제 기반의 경량 인증 및 거리 한정 프로토콜 제공 방법을 설명하기 위해 도시한 흐름도이다.

[0052] 도 1 및 도 3을 참조하면, 단계(310)에서 상기 검증자(110)와 상기 인증 디바이스(120)는 대칭키 기반의 설계 구조에 따라 서로 동일한 비밀키를 공유한다.

[0053] 이때, 상기 검증자(110)와 상기 인증 디바이스(120)는 k비트열 난수 2개(x, y)와 실수값 $\eta \in \{0,1/2\}$를 상기 비밀키로서 공유할 수 있다. 또한, 상기 비밀키는 보안 통신 채널을 통한 상기 검증자(110)와 상기 인증 디바이스(120) 간의 교환 방식으로 공유될 수 있다.

[0054] 다음으로, 단계(320)에서 상기 검증자(110)와 상기 인증 디바이스(120)는 2라운드 프로토콜을 2n(상기 n은 자연수)번 반복 수행하여 질의-응답 과정에 필요한 난수를 공유한다.

[0055] 다음으로, 단계(330)에서 상기 검증자(110)와 상기 인증 디바이스(120)는 상기 난수에 기초하여 인증 및 거리 한정을 위한 질의-응답 과정을 n번 수행한다.

[0056] 도 4는 본 발명의 일 실시예에 따라 검증자와 인증 디바이스 간에 난수를 공유하는 과정(도 3의 "320")을 도시한 흐름도이다.

[0057] 도 1 및 도 4를 참조하면, 단계(410)에서 상기 검증자(110)와 상기 인증 디바이스(120) 간에는 서로 난수를 교환한다. 여기서, 상기 난수는 k비트열의 랜덤한 숫자값을 가리킨다.

[0058] 다음으로, 단계(420)에서 상기 인증 디바이스(120)는 상기 난수 및 상기 검증자(110)와 상기 인증 디바이스(120)의 비밀키를 이용하여, 상기 인증 및 거리 한정의 판단에 필요한 값을 계산하여 저장한다.

[0059] 아래에서는 상기 검증자(110)와 상기 인증 디바이스(120) 간에 난수를 공유하는 과정에 대해 보다 구체적으로 설명하기로 한다.

[0060] 도 5 및 도 6은 본 발명의 일 실시예에 따라 검증자와 인증 디바이스 간에 난수를 공유하는 과정(도 3의 "320")을 보다 구체적으로 설명하기 위해 도시한 도면이다.

[0061] 도 1, 도 5 및 도 6을 참조하면, 단계(610)에서 상기 인증 디바이스(prover)(120)는 k비트열 난수 b_i를 생성하여 상기 검증자(verifier)(110)에게 전송한다.

[0062] 다음으로, 단계(620)에서 상기 검증자(110)는 k비트열 난수 a_i를 생성하여 상기 인증 디바이스(120)에 전송한다. 즉, 상기 검증자(110)는 상기 검증자(110)로부터 전송받은 k비트열 난수 b_i에 응답하여, 상기 k비트열 난수 a_i를 생성하여 상기 인증 디바이스(120)에 전송할 수 있다.

[0063] 다음으로, 단계(630)에서 상기 인증 디바이스(120)는 $z_i=(a_i*x)+(b_i*y)+v_i$를 계산하여 저장한다.

[0064] 다음으로, 단계(640)에서 상기 검증자(110)와 상기 인증 디바이스(120)는 상기 단계(610) 내지 단계(630)이 2n 라운드($1\leq i\leq 2n$)) 동안 반복 수행되었는지를 판단한다.

[0065] 상기 판단 결과, 2n 라운드 동안 반복 수행되었다면(640의 "예" 방향), 상기 검증자(110)와 상기 인증 디바이스(120)는 서로 간에 난수를 공유하는 과정을 종료한다.

[0066] 하지만, 상기 판단 결과, 2n 라운드 동안 반복 수행되지 않았다면(640의 "아니오" 방향), 상기 단계(610)으로 리턴(return)한다. 즉, 상기 검증자(110)와 상기 인증 디바이스(120)는 2n 라운드가 완료될 때까지 상기 단계(610) 내지 단계(630)를 반복 수행한다.

[0067] 도 7 및 도 8은 본 발명의 일 실시예에 따라 검증자와 인증 디바이스 간에 질의-응답을 수행하는 과정(도 3의 "330")을 보다 구체적으로 설명하기 위해 도시한 도면이다.

[0068] 도 1, 도 7 및 도 8을 참조하면, 단계(810)에서 상기 검증자(110)는 n 라운드($1\leq i\leq n$) 동안 시간을 측정한다.

[0069] 다음으로, 단계(820)에서 상기 검증자(820)는 $C_i\in\{0,1|Pr[C_i=1]=\eta\}$를 생성하여 상기 인증 디바이스(120)에 전송한다. 여기서, 상기 C_i는 0과 1 중에서 1이 나올 확률 η에 따른 값을 나타낼 수 있다. 상기 C_i는 상기 n 라운드 동안 상기 검증자(820)로부터 상기 인증 디바이스(120)로 전송될 수 있다.

[0070] 다음으로, 단계(830)에서 상기 인증 디바이스(120)는 상기 C_i의 값에 따라 상기 검증자(110)에게 z_i 또는 z_n+i를 전송한다. 즉, 상기 C_i의 값이 0인 경우, 상기 인증 디바이스(120)는 상기 검증자(110)에게 z_i를 R_i 값으로서 전송하고, 상기 C_i의 값이 1인 경우 z_n+i를 R_i 값으로서 전송할 수 있다.

[0071] 다음으로, 단계(840)에서 상기 검증자(110)는 상기 z_i의 값이 $(a_i*x)+(b_i*y)$와 다른 경우의 발생 횟수를 카운트한다.

[0072] 다음으로, 상기 검증자(110)는 단계(850)에서 상기 카운트 된 발생 횟수와 $n\cdot\eta$이 유사한가를 판단하고, 단계(860)에서 유효 시간 내에 상기 n번의 질의-응답 과정이 이루어졌는가를 판단한다.

[0073] 상기 판단 결과, 상기 카운트 된 발생 횟수와 $n\cdot\eta$이 유사하고(850의 "예" 방향), 유효 시간 내에 상기 n번의 질의-응답 과정이 이루어지는 경우(860의 "예" 방향), 상기 검증자(110)는 상기 인증 디바이스(120)가 정당하며 올바른 위치에 존재한다고 판단한다.

[0074] 하지만, 상기의 조건을 만족하지 못하는 경우, 다시 말해 단계(850) 및 단계(860) 중 적어도 하나가 "아니오"인 경우, 상기 검증자(110)는 상기 인증 디바이스(120)가 정당하지 않으며 올바른 위치에 존재하지도 않는 것으로 판단하고 본 과정을 종료한다.

[0075] 즉, 상기 검증자(110)는 상기 카운트 된 발생 횟수와 $n \cdot \eta$ 유사도 및 유효 시간 내에 상기 n번의 질의-응답 과정이 이루어졌는지에 근거하여, 상기 검증자가 상기 인증 디바이스에 대한 인증 및 거리 한정 내 위치에 존재하는지 여부를 판단할 수 있다.

[0076] 이와 같이, 본 발명의 일 실시예에서는 경량 디바이스에서의 인증과 동시에 거리 한정까지 함께 수행하는 프로토콜을 제공하며, 이러한 프로토콜은 LPN 문제의 어려움에 기반을 두고 설계되며, 양자 컴퓨팅 공격에 대해서도 안전하다. 기존에는 인증과 동시에 거리 한정까지 수행하는 프로토콜은 존재하지 않았는데, 본 발명의 일 실시예에서는 증명 가능한 경량 인증 프로토콜 중에서 HB+ 프로토콜을 확장 및 변형하여 거리 한정까지 가능한 방법을 제공한다. 이렇게 설계된 방법은 LPN 문제의 어려움에 기반을 두고 있으면서, 인증과 동시에 거리 한정을 수행하는 것이 가능하다.

[0077] 따라서, 본 발명의 일 실시예에 의하면, 인증을 원하는 디바이스가 원하는 위치에 존재하는지를 효율적으로 확인할 수 있으며, 특히 차량용 무선 키 인증 환경에서 유용하게 사용될 수 있다. 또한, 인증과 거리 한정을 수행하는 과정에 대한 안전성이 우수하며, 이에 따라 다른 인증과 거리 한정 프로토콜을 각각 사용해서 원하는 결과를 얻는 기존의 방법에 비해 안전성 측면에서 우수한 효과가 있다.

[0078] 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 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, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 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.

[0079] 지금까지 본 발명에 따른 구체적인 실시예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서는 여러 가지 변형이 가능함은 물론이다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허 청구의 범위뿐 아니라 이 특허 청구의 범위와 균등한 것들에 의해 정해져야 한다.

[0080] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0081] 110: 검증자

120: 인증 디바이스

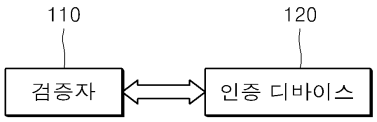
210: 난수 공유부

220: 질의-응답부

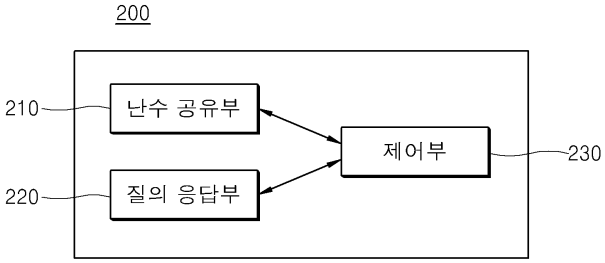
230: 제어부

도면

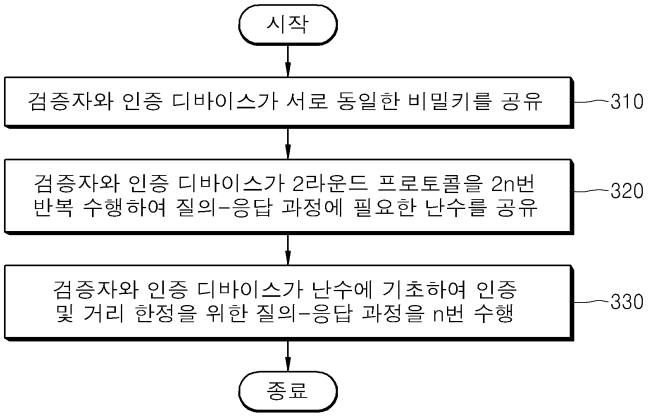
도면1



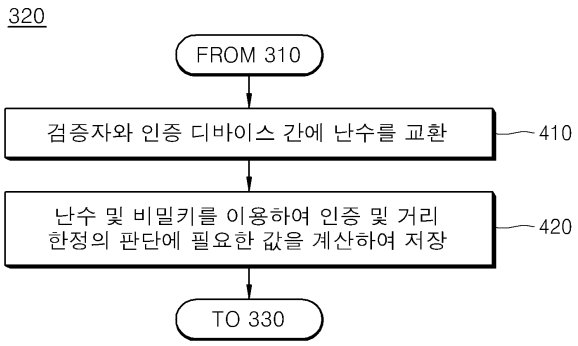
도면2



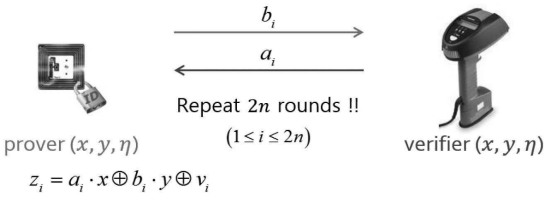
도면3



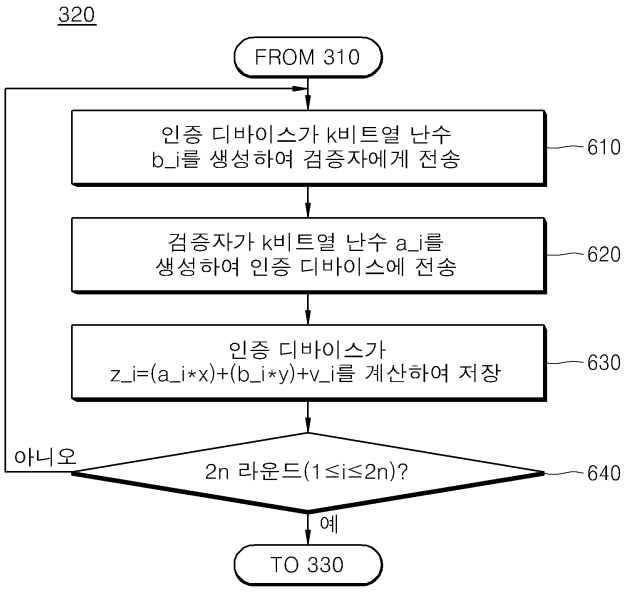
도면4


320
FROM 310
검증자와 인증 디바이스 간에 난수를 교환
410
난수 및 비밀키를 이용하여 인증 및 거리 한정의 판단에 필요한 값을 계산하여 저장
420
TO 330

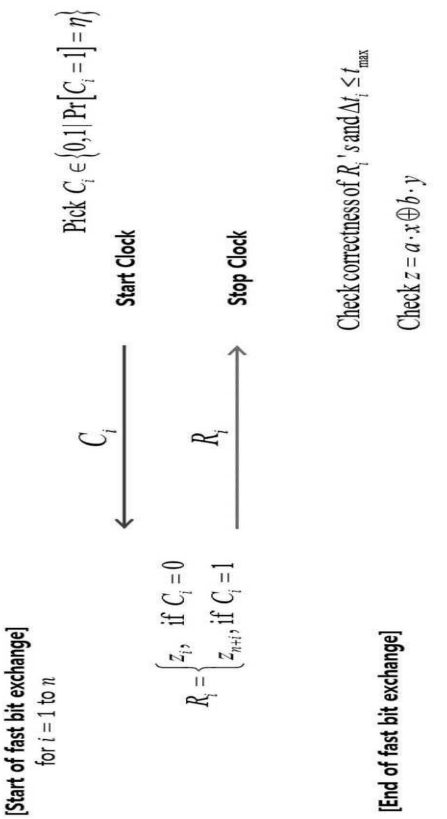
도면5


b_i
a_i
Repeat $2n$ rounds !!
$(1 \le i \le 2n)$
prover (x, y, η)
verifier (x, y, η)
$z_i = a_i \cdot x \oplus b_i \cdot y \oplus v_i$

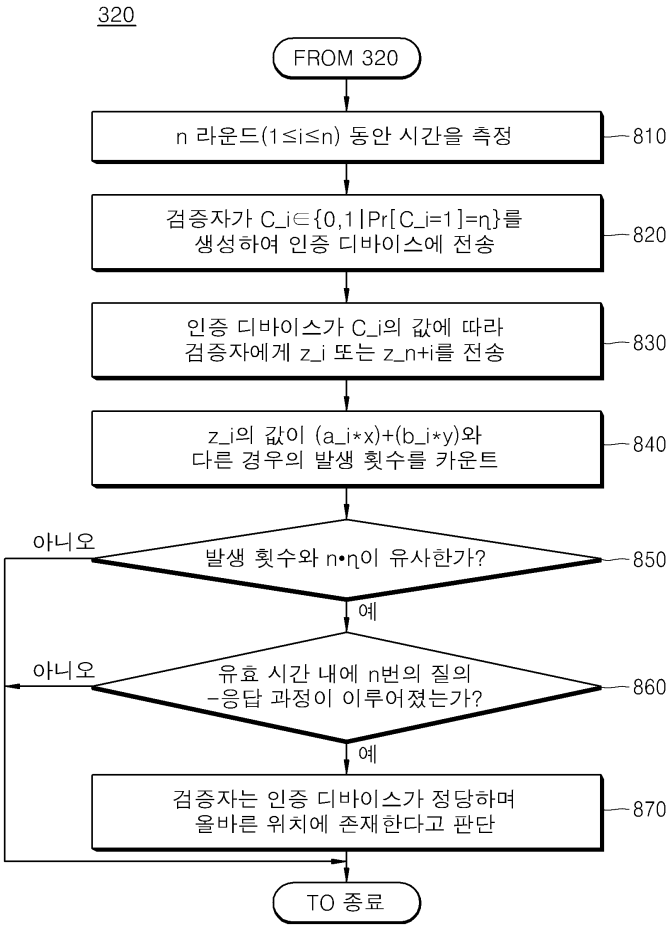
도면6


320
FROM 310
인증 디바이스가 k비트열 난수 b_i를 생성하여 검증자에게 전송
610
검증자가 k비트열 난수 a_i를 생성하여 인증 디바이스에 전송
620
인증 디바이스가 z_i=(a_i*x)+(b_i*y)+v_i를 계산하여 저장
630
아니오
2n 라운드(1≤i≤2n)?
640
예
TO 330

도면7


[Start of fast bit exchange]
for $i = 1$ to n
Pick $C_i \in \{0,1 | \Pr[C_i = 1] = \eta\}$
C_i
Start Clock
$R_i = \begin{cases} z_i, & \text{if } C_i = 0 \\ z_{(n+i)}, & \text{if } C_i = 1 \end{cases}$
R_i
Stop Clock
Check correctness of R_i's and $\Delta t_i \leq t_{max}$
[End of fast bit exchange]
Check $z = a \cdot x \oplus b \cdot y$

도면8


320
FROM 320
n 라운드(1≤i≤n) 동안 시간을 측정
810
검증자가 C_i∈{0,1|Pr[C_i=1]=η}를
생성하여 인증 디바이스에 전송
820
인증 디바이스가 C_i의 값에 따라
검증자에게 z_i 또는 z_n+i를 전송
830
z_i의 값이 (a_i*x)+(b_i*y)와
다른 경우의 발생 횟수를 카운트
840
아니오
발생 횟수와 n•η이 유사한가?
850
예
아니오
유효 시간 내에 n번의 질의
-응답 과정이 이루어졌는가?
860
예
검증자는 인증 디바이스가 정당하며
올바른 위치에 존재한다고 판단
870
TO 종료