(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0121429
(43) 공개일자 2012년11월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 9/28* (2006.01)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2011-0038900
(22) 출원일자 2011년04월26일
심사청구일자 2011년04월26일
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

전체 청구항 수 : 총 18 항

(71) 출원인
숭실대학교산학협력단
서울특별시 동작구 상도로 369 (상도동)
(72) 발명자
이정현
경기도 성남시 분당구 수내동 푸른마을쌍용아파트 610동 602호
마건일
서울특별시 동작구 사당로9가길 82, 201동 1705호 (사당동, 대아아파트)
이형찬
서울특별시 동작구 사당로2가길 27, 삼보빌라 202호 (사당동)
(74) 대리인
특허법인태백

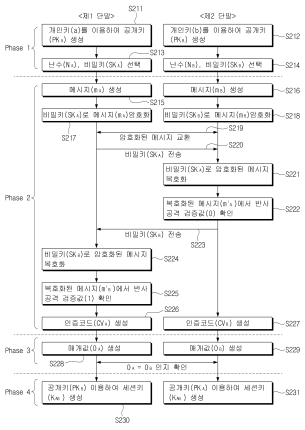
(54) 발명의 명칭 **가변길이 인증코드를 사용하는 무선 통신 단말간 세션키 공유 방법**

(57) 요 약

본 발명은 가변길이 인증코드를 사용하는 무선 통신 단말간 세션키 공유 방법에 관한 것이다. 본 발명에 따르면 DH(Diffie-Hellman) 프로토콜 기반에서 무선 통신 단말간 세션키를 공유하는 방법에 있어서, 자신의 개인키를 이용하여 공개키를 생성하는 단계, 상기 공개키 및 제1 난수를 포함하는 메시지를 생성하고, 상기 메시지를 자신의 비밀키로 암호화하여 상기 상대 단말의 암호화된 메시지와 교환하는 단계, 상기 상대 단말의 비밀키를 수신하여 상기 상대 단말의 암호화된 메시지를 복호화하는 단계, 상기 제1 난수와 상기 복호화된 메시지에 포함된 제2 난수를 연산하여 인증코드를 생성하는 단계, 상기 인증코드로부터 매개 값을 획득하는 단계, 및 상기 복호화된 메시지에 포함된 상대 단말의 공개키를 이용하여 세션키를 생성하는 단계를 포함한다.

이와 같이 본 발명에 따르면, 짧은 길이의 인증코드를 사용하므로 OOB 채널을 통한 인증 기법 사용 시 높은 사용성 증대를 기대할 수 있다. 또한 인증코드 길이의 조절이 유연하므로 어플리케이션의 보안 요구 수준에 따라 인증코드의 길이를 조절하여 사용성과 보안성의 절충을 꾀할 수 있다. 또한 컬러 그리드는 기존 흑백 그리드에 비해 절반 크기 또는 개수로 표현이 가능하므로 직접적인 세션키 인증을 훨씬 수월하게 할 수 있다.

대 표 도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호	20100011057
부처명	교육과학기술부
연구사업명	기초연구사업-일반연구자지원사업-기본연구지원사업
연구과제명	개방형 스마트폰 플랫폼 보안 기술 연구
주관기관	숭실대학교 산학협력단
연구기간	2010.05.01 ~ 2013.04.30이 발명을 지원한 국가연구개발사업
과제고유번호	10035219-2011-02
부처명	지식경제부
연구사업명	SW컴퓨팅 산업원천기술개발사업(정보보안)
연구과제명	모바일 ID 보안 및 프라이버시를 위한 스마트지갑 기술 개발
주관기관	숭실대학교 산학협력단
연구기간	2010.03.01 ~ 2013.02.28

특허청구의 범위

청구항 1

DH(Diffie-Hellman) 프로토콜 기반에서 무선 통신 단말간 세션키를 공유하는 방법에 있어서,

자신의 개인키를 이용하여 공개키를 생성하는 단계,

상기 공개키 및 제1 난수를 포함하는 메시지를 생성하고, 상기 메시지를 자신의 비밀키로 암호화하여 상대 단말의 암호화된 메시지와 교환하는 단계,

상기 상대 단말의 비밀키를 수신하여 상기 상대 단말의 암호화된 메시지를 복호화하는 단계,

상기 제1 난수와 상기 복호화된 메시지에 포함된 제2 난수를 연산하여 인증코드를 생성하는 단계,

상기 인증코드로부터 매개 값을 산출하는 단계, 그리고

상기 복호화된 메시지에 포함된 상대 단말의 공개키를 이용하여 세션키를 생성하는 단계를 포함하는 무선 통신 단말간 세션키 공유 방법.

청구항 2

제1항에 있어서,

상기 메시지는,

식별자 및 반사 공격 검증 값을 더 포함하는 무선 통신 단말간 세션키 공유 방법.

청구항 3

제2항에 있어서,

상기 복호화된 메시지에 포함된 상기 상대 단말의 반사 공격 검증 값을 확인하는 단계를 더 포함하는 무선 통신 단말간 세션키 공유 방법.

청구항 4

제3항에 있어서,

상기 비밀키는 일회용 키이며,

상기 제1 및 제2 난수는 0 또는 1로 이루어진 비트열로 구성되는 무선 통신 단말간 세션키 공유 방법.

청구항 5

제4항에 있어서,

상기 인증코드를 생성하는 단계는,

상기 제1 난수와 상기 제2 난수를 배타적 논리 합 연산을 수행하여 인증코드를 생성하는 무선 통신 단말간 세션키 공유 방법.

청구항 6

제5항에 있어서,

상기 인증 코드는 n(n은 2이상의 자연수)개 비트 단위로 분할되며, 상기 분할된 인증 코드는 1개의 그리드에 대응되며, 각각의 그리드는 1개의 색상으로 표시되는 무선 통신 단말간 세션키 공유 방법.

청구항 7

제6항에 있어서,

상기 인증코드로부터 매개 값을 산출하는 단계는,

상기 인증코드를 2개 이상의 비트로 분할하여 OOB 함수에 입력하여 상기 매개 값을 획득하는 단계, 그리고

상기 매개 값을 복수의 그리드로 이루어진 화면 상에 표시하는 단계를 포함하는 무선 통신 단말간 세션키 공유 방법.

청구항 8

제7항에 있어서,

상기 매개 값을 표시하기 위하여 필요한 그리드의 개수(S')는 다음의 수학식과 같이 나타내는 무선 통신 단말간 세션키 공유 방법:

$S' = S / \log_2 k$

여기서, S는 상기 매개 값을 표시하는 색상의 종류가 2개일 때 필요한 그리드의 개수를 나타내며, k는 상기 매개 값을 표시하는데 사용하는 색상 종류의 개수로서 2^m이며, m은 분할된 상기 인증코드의 비트 개수이다.

청구항 9

제6항에 있어서,

상기 인증코드로부터 매개 값을 산출하는 단계는,

상기 인증코드를 OOB 함수에 입력하여 상기 매개 값을 획득하는 단계, 그리고

상기 매개 값에 대응하여 복수의 LED가 점등 또는 소등하도록 제어하는 단계를 포함하는 무선 통신 단말간 세션키 공유 방법.

청구항 10

제6항에 있어서,

상기 인증코드로부터 매개 값을 산출하는 단계는,

상기 인증코드를 OOB 함수에 입력하여 상기 매개 값을 획득하는 단계, 그리고

상기 매개 값에 대응하여 저장된 음원 파일을 재생하는 단계를 포함하는 무선 통신 단말간 세션키 공유 방법.

청구항 11

DH(Diffie-Hellman) 프로토콜 기반에서 상대 단말과 세션키를 공유하기 위한 무선 통신 단말에 있어서,

자신의 개인키를 이용하여 생성된 공개키를 포함하는 저장부,

상기 공개키 및 제1 난수를 포함하는 메시지를 생성하고, 상기 메시지를 자신의 비밀키로 암호화하여 상기 상대 단말의 암호화된 메시지와 교환하는 암호화부,

상기 상대 단말의 비밀키를 수신하여 상기 상대 단말의 암호화된 메시지를 복호화하는 복호화부,

상기 제1 난수와 상기 복호화된 메시지에 포함된 제2 난수를 연산하여 인증코드를 생성하는 인증코드 생성부,

상기 인증코드로부터 매개 값을 산출하는 OOB 변환부, 그리고

상기 복호화된 메시지에 포함된 상대 단말의 공개키를 이용하여 세션키를 생성하는 세션키 생성부를 포함하는 무선 통신 단말.

청구항 12

제11항에 있어서,

상기 메시지는,

식별자 및 반사 공격 검증 값을 더 포함하는 무선 통신 단말.

청구항 13

제12항에 있어서,

상기 복호화부는,

상기 복호화된 메시지에 포함된 상기 상대 단말의 반사 공격 검증 값을 확인하는 무선 통신 단말.

청구항 14

제13항에 있어서,

상기 비밀키는 일회용 키이며,

상기 제1 및 제2 난수는 0 또는 1로 이루어진 비트열로 구성되는 무선 통신 단말.

청구항 15

제14항에 있어서,

상기 인증코드 생성부는,

상기 제1 난수와 상기 제2 난수를 배타적 논리 합 연산을 수행하여 인증코드를 생성하는 무선 통신 단말.

청구항 16

제15항에 있어서,

상기 인증 코드는 n(n은 2이상의 자연수)개 비트 단위로 분할되며, 상기 분할된 인증 코드는 1개의 그리드에 대응되며, 각각의 그리드는 1개의 색상으로 표시되는 무선 통신 단말.

청구항 17

제16항에 있어서,

상기 OOB 변환부는,

2개 이상의 비트로 분할된 상기 인증코드를 입력받아 상기 매개 값을 획득하고, 상기 매개 값을 복수의 그리드로 이루어진 화면 상에 표시하는 무선 통신 단말.

청구항 18

제16항에 있어서,

상기 매개 값을 표시하기 위하여 필요한 그리드의 개수(S')는 다음의 수학식과 같이 나타내는 무선 통신 단말:

$S' = S / \log_2 k$

여기서, S는 상기 매개 값을 표시하는 색상의 종류가 2개일 때 필요한 그리드의 개수를 나타내며, k는 상기 매개 값을 표시하는데 사용하는 색상 종류의 개수로서 2^m이며, m은 분할된 상기 인증코드의 비트 개수이다.

명 세 서

기 술 분 야

[0001] 본 발명은 가변길이 인증코드를 사용하는 무선 통신 단말간 세션키 공유 방법에 관한 것으로서, 보다 상세하게는 근거리에 있는 무선 통신 단말 간에 높은 보안성을 유지한 상태에서 세션키를 공유할 수 있는 가변길이 인증코드를 사용하는 무선 통신 단말간 세션키 공유 방법에 관한 것이다.

배 경 기 술

[0002] 스마트 폰의 대중화는 스마트 폰의 이동성과 컴퓨팅 능력을 활용하는 어플리케이션의 양적 질적 팽창을 가져왔

다. 많은 모바일 어플리케이션 중에서도 모바일을 이용한 지불 결제 서비스는 사용자들에게 큰 편의를 가져다 줄 수 있는 서비스로 주목받고 있다. 모바일 지갑과 같은 다양한 지불 수단을 하나의 어플리케이션 안으로 통합시켜 사용자에게 스마트 폰을 통해 다양한 지불 결제 서비스를 간편하게 제공할 수 있다. 스마트 폰을 통한 지불 결제 방법에는 여러 가지 방법이 존재하지만, 모바일 지갑의 지불 결제 서비스는 가까운 거리에 있는 다양한 무선 단말간의 무선 통신을 통해 이루어진다. 하지만 무선통신은 근본적으로 공격자에게 쉽게 노출될 수 있는 취약점을 갖는다. 따라서 이러한 모바일 단말을 이용한 다양한 서비스가 실제 이루어지기 위해서는 근거리에서 이루어지는 단말 사이에 안전한 세션 관리 기술이 반드시 필요하다.

[0003] 안전한 세션 관리를 위해서는 양 통신 단말이 안전하게 비밀 키를 공유하는 기술이 필요하다. 비밀 키를 공유하는 가장 잘 알려진 방법은 DH(Diffie-Hellman) 프로토콜이지만 중간자 공격에 취약하다는 단점이 있다. 중간자 공격 취약점을 보완하기 위해 STS(Station-to-Station) 프로토콜을 비롯한 많은 키 교환 기술들이 제안되었으나 사전 공유 값을 필요로 한다거나 TTP(Trusted Third Party)를 요구하기 때문에 모바일 결제 서비스에 사용되기에 적합하지 않다. 모바일을 이용한 결제 서비스는 항상 다양한 각 통신 단말과 사전 공유 값을 갖거나 PKI(Public Key Infrastructure)와 같은 공통의 TTP를 가지는 것이 어렵기 때문이다.

[0004] 또한 DH 프로토콜을 통해 확립된 공유 키(세션키)에 대한 해쉬 값을 인증코드로 사용할 경우 인증코드의 크기는 OOB 채널에 사용되기에 그 값이 너무 크며, 해쉬 값은 pre-image 공격에 취약하다는 문제점이 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 근거리에 있는 무선 통신 단말 간에 높은 보안성을 유지한 상태에서 세션키를 공유할 수 있는 가변길이 인증코드를 사용하는 무선 통신 단말간 세션키 공유 방법을 제공하는데 목적이 있다.

과제의 해결 수단

[0006] 본 발명의 실시예에 따르면 DH(Diffie-Hellman) 프로토콜 기반에서 상대 단말과 세션키를 공유하는 방법에 있어서, 자신의 개인키를 이용하여 공개키를 생성하는 단계, 상기 공개키 및 제1 난수를 포함하는 메시지를 생성하고, 상기 메시지를 자신의 비밀키로 암호화하여 상기 상대 단말의 암호화된 메시지와 교환하는 단계, 상기 상대 단말의 비밀키를 수신하여 상기 상대 단말의 암호화된 메시지를 복호화하는 단계, 상기 제1 난수와 상기 복호화된 메시지에 포함된 제2 난수를 연산하여 인증코드를 생성하는 단계, 상기 인증코드로부터 매개 값을 산출하는 단계, 그리고 상기 복호화된 메시지에 포함된 상대 단말의 공개키를 이용하여 세션키를 생성하는 단계를 포함한다.

[0007] 상기 메시지는, 식별자 및 반사 공격 검증 값을 더 포함할 수 있다.

[0008] 상기 복호화된 메시지에 포함된 상기 상대 단말의 반사 공격 검증 값을 확인하는 단계를 더 포함할 수 있다.

[0009] 상기 비밀키는 일회용 키이며, 상기 제1 및 제2 난수는 0 또는 1로 이루어진 비트열로 구성될 수 있다.

[0010] 상기 인증코드를 생성하는 단계는, 상기 제1 난수와 상기 제2 난수를 배타적 논리 합 연산을 수행하여 인증코드를 생성할 수 있다.

[0011] 상기 인증 코드는 n(n은 2이상의 자연수)개 비트 단위로 분할되며, 상기 분할된 인증 코드는 1개의 그리드에 대응되며, 각각의 그리드는 1개의 색상으로 표시될 수 있다.

[0012] 상기 인증코드를 OOB 함수에 적용하여 매개 값을 산출하는 단계는, 상기 인증코드를 2개 이상의 비트로 분할하여 상기 OOB 함수에 입력하여 상기 매개 값을 획득하는 단계, 그리고 상기 매개 값을 복수의 그리드로 이루어진 화면 상에 표시하는 단계를 포함할 수 있다.

[0013] 상기 매개 값을 표시하기 위하여 필요한 그리드의 개수(S')는 다음의 수학식과 같이 나타낼 수 있다.

[0014] $S' = S / \log_2 k$

[0015] 여기서, S는 상기 매개 값을 표시하는 색상의 종류가 2개일 때 필요한 그리드의 개수를 나타내며, k는 상기 매개 값을 표시하는데 사용하는 색상 종류의 개수로서 2^m이며, m은 분할된 상기 인증코드의 비트 개수이다.

[0016] 상기 인증코드로부터 매개 값을 산출하는 단계는, 상기 인증코드를 OOB 함수에 입력하여 상기 매개 값을 획득하는 단계, 그리고 상기 매개 값에 대응하여 복수의 LED가 점등 또는 소등하도록 제어하는 단계를 포함할 수 있다.

[0017] 상기 인증코드로부터 매개 값을 산출하는 단계는, 상기 인증코드를 OOB 함수에 입력하여 상기 매개 값을 획득하는 단계, 그리고 상기 매개 값에 대응하여 저장된 음원 파일을 재생하는 단계를 포함할 수 있다.

[0018] 본 발명의 다른 실시예에 따르면, DH(Diffie-Hellman) 프로토콜 기반에서 상대 단말과 세션키를 공유하기 위한 무선 통신 단말에 있어서, 자신의 개인키를 이용하여 생성된 공개키를 포함하는 저장부, 상기 공개키 및 제1 난수를 포함하는 메시지를 생성하고, 상기 메시지를 자신의 비밀키로 암호화하여 상기 상대 단말의 암호화된 메시지와 교환하는 암호화부, 상기 상대 단말의 비밀키를 수신하여 상기 상대 단말의 암호화된 메시지를 복호화하는 복호화부, 상기 제1 난수와 상기 복호화된 메시지에 포함된 제2 난수를 연산하여 인증코드를 생성하는 인증코드 생성부, 상기 인증코드를 OOB 함수에 적용하여 매개 값을 산출하는 OOB 변환부, 그리고 상기 복호화된 메시지에 포함된 상대 단말의 공개키를 이용하여 세션키를 생성하는 세션키 생성부를 포함한다.

발명의 효과

[0019] 이와 같이 본 발명에 따르면, 짧은 길이의 인증코드를 사용하므로 OOB 채널을 통한 인증 기법 사용 시 높은 사용성 증대를 기대할 수 있다. 또한 인증코드 길이의 조절이 유연하므로 어플리케이션의 보안 요구 수준에 따라 인증코드의 길이를 조절하여 사용성과 보안성의 절충을 꾀할 수 있다. 또한 무선통신 단말의 다양한 사용환경에 따라 다양한 인증방법으로써 CCB(Comparing Color Barcode), CML(Comparing Multi LEDs), CM(Comparing Music) 방법을 제공함으로써 직접적인 세션키 인증을 훨씬 수월하게 할 수 있다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 실시예에 따른 무선 통신 단말의 구성도이다.

도 2는 본 발명의 실시예에 따른 무선 통신 단말간 가변 크기 세션키 설정 방법을 나타내는 흐름도이다.

도 3은 도 2에 따른 세션키 설정 방법을 더욱 상세하게 나타낸 흐름도이다.

도 4a는 본 발명의 실시예에 따른 OOB 변환부가 CCB 방법을 이용하여 매개 값을 산출하는 과정을 설명하기 위한 도면이다.

도 4b는 도 4a에 따른 OOB 함수의 매개 값이 화면 상에 표시되는 것을 도시한 예시도이다.

도 5a는 본 발명의 실시예에 따른 OOB 변환부가 CML 방법을 이용하여 매개 값을 산출하는 과정을 설명하기 위한 도면이다.

도 5b는 도 5a에 따른 OOB 함수의 매개 값이 LED를 통하여 표시되는 것을 도시한 예시도이다.

도 6a는 본 발명의 실시예에 따른 OOB 변환부가 CM 방법을 이용하여 매개 값을 산출하는 과정을 설명하기 위한 도면이다.

도 6b는 도 6a에 따른 OOB 함수의 매개 값에 따라 음악 파일이 재생되는 화면을 도시한 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 그러면 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다.

[0022] 도 1은 본 발명의 실시예에 따른 무선 통신 단말의 구성도이다. 도 1에 따른 무선 통신 단말(100)은 근거리에 있는 다른 무선 통신 단말과 세션키를 공유하기 위한 장치로서, 이동국(Mobile Station, MS), 이동 단말(Mobile Terminal, MT), 가입자국(Subscriber Station, SS), 휴대 가입자국(Portable Subscriber Station, PSS), 사용자 장치(User Equipment, UE), 접근 단말(Access Terminal, AT) 등을 지칭할 수도 있고, 이동 단말, 가입자국, 휴대 가입자 국, 사용자 장치 등의 전부 또는 일부의 기능을 포함할 수도 있다.

[0023] 본 발명의 실시예에 따른 무선 통신 단말(100)은 저장부(110), 암호화부(120), 복호화부(130), 인증코드 생성부(140), OOB 변환부(150) 및 세션키 생성부(160)를 포함한다.

[0024] 저장부(110)는 무선 통신 단말(100) 자신의 개인키를 이용하여 생성된 공개키, 식별자 ID, 난수, 비밀키를 저장

하고, 랜덤(random)하게 선택된 난수와 비밀키를 저장한다.

[0025] 암호화부(120)는 공격 검증 값, 식별자 ID, 공개키 및 난수를 포함하는 메시지를 생성하고, 생성된 메시지를 자신의 비밀키로 암호화하여 상대 단말의 암호화된 메시지와 교환되도록 한다. 이때 난수 및 공개키 값의 전송은 대칭키 암호화 알고리즘을 사용한다.

[0026] 복호화부(130)는 수신된 상대 단말의 비밀키를 이용하여 상대 단말의 암호화된 메시지를 복호화하고, 복호화된 메시지에서 공격 검증 값을 인증한다. 인증코드 생성부(140)는 복호화된 메시지에 포함된 상대 단말의 난수와 자신의 난수를 연산하여 인증코드를 생성한다.

[0027] 여기서, 인증코드 생성부(140)는 공유 키(세션키)에 대한 해쉬 값 대신 난수의 배타적 논리합 값을 인증코드로 사용한다.

[0028] OOB 변환부(150)는 인증코드를 OOB 함수에 적용하여 매개 값을 획득한다. 여기서, 양 단말간 매개 값의 인증방법은 컬러 바코드를 사용하며, 기존의 흑백 바코드와 같이 카메라 모듈을 통해 인식되는 것이 아니라 사람이 직접 간단한 컬러 바코드의 동일 여부를 비교하는 과정을 통해 세션키를 인증할 수 있도록 한다.

[0029] 세션키 생성부(160)는 복호화된 메시지에 포함된 상대 단말의 공개키를 이용하여 세션키를 생성한다.

[0030] 도 2는 본 발명의 실시예에 따른 무선 통신 단말간 가변 크기 세션키 설정 방법을 나타내는 흐름도이고 도 3은 도 2에 따른 세션키 설정 방법을 더욱 상세하게 나타낸 흐름도이다. 설명의 편의상 도 2 및 도 3에서는 본 발명의 실시예에 따른 무선 통신 단말을 제1 단말과 제2 단말로 나타내었으며, 제1 단말과 제2 단말은 DH 프로토콜 기반에서 지그비, RFID, 블루투스 방식을 통하여 근거리 무선 통신(Near Field Communication, NFC)을 수행하는 단말들이다.

[0031] 먼저 초기화 단계(Phase 1)에서는 제1 단말과 제2 단말은 사람이 식별 가능한 식별자 ID(예: E-Mail 주소)와 각각의 DH 공개키 값(PK_A, PK_B)을 설정받는다(S211, S212). 여기서, 제1 단말과 제2 단말에 설정되는 ID는 각각 도 3와 같이 ID_A, ID_B로 표시할 수 있다. 또한, 제1 단말이 설정받는 DH 공개키 값(PK_A)은 제1 단말의 개인키(a)를 이용하여 생성되며($g^a \bmod p$), 제2 단말이 설정받는 DH 공개키 값 PK_B는 제2 단말의 개인키(b)를 이용하여 생성된다($g^b \bmod p$).

[0032] 또한 제1 단말과 제2 단말은 각각 k 비트의 난수(N_A, N_B)와 t 비트의 일회용 비밀키(SK_A, SK_B)를 랜덤하게 선택한다(S213, S214). 여기서, 난수 N_A, N_B는 0 또는 1의 비트 값으로 이루어진 k 개의 비트열로 이루어져 있으므로, k 값을 조절함으로써 다양한 비트열로 이루어진 난수 N_A, N_B를 생성할 수 있다. 또한 일회용 비밀키 SK_A, SK_B는 0 또는 1의 비트 값으로 이루어진 t개의 비트열로 이루어지며, 수시로 그 값은 변경될 수 있다.

[0033] 다음으로 공개키 교환 단계(Phase 2)에서는 제1 단말과 제2 단말은 공개키 값 PK_A, PK_B을 서로 교환하기 위하여 메시지 m_A와 m_B를 각각 생성한다(S215, S216).

[0034] 여기서, 메시지(m_A, m_B)는 반사(reflection) 공격을 검증하기 위한 공격 검증 값(0 또는 1), 자신의 ID(ID_A, ID_B), 자신의 공개키 값(PK_A, PK_B), 자신의 난수(N_A, N_B)를 포함한다. 제1 단말이 생성하는 메시지(m_A)는 $0 \| ID_A \| PK_A \| N_A$로 나타낼 수 있으며, 제2 단말이 생성하는 메시지(m_B)는 $1 \| ID_B \| PK_B \| N_B$로 나타낼 수 있다. 여기서, 반사 공격 검증 값 0은 송신단말 측임을 의미하고, 1은 수신단말 측임을 의미한다.

[0035] 다음으로 제1 단말과 제2 단말은 생성된 메시지 m_A와 m_B를 각각 자신의 비밀키 SK_A, SK_B를 이용하여 암호화 한다(S217, S218). 그리고 제1 단말과 제2 단말은 비밀키 SK_A, SK_B에 의해 암호화된 메시지 $E(SK_A, m_A)$와 $E(SK_B, m_B)$를 서로 교환한다(S219).

[0036] 그리고 제1 단말은 제2 단말로부터 암호화된 메시지인 $E(SK_B, m_B)$를 수신하면, 자신의 비밀키 SK_A를 제2 단말로 전송한다(S220). 제1 단말의 비밀키(SK_A)를 수신한 제2 단말은 비밀키(SK_A)를 이용하여 암호화된 메시지 $E(SK_A, m_A)$를 복호화 한다($D(SK_A, E(SK_A, m_A))$(S221).

[0037] 그리고 제2 단말은 복호화된 메시지 m'_A에 반사 공격 검증 값 0이 있는지 여부를 확인한 후(S222), 반사 공격 검증 값 0의 존재를 확인하면 자신의 비밀키(SK_B)를 제1 단말로 전송한다(S223).

[0038] 제2 단말의 비밀키(SK_B)를 수신한 제1 단말은 비밀키(SK_B)를 이용하여 암호화된 메시지 $E(SK_B, m_B)$를 복호화 한다($D(SK_B, E(SK_B, m_B)$(S224). 그리고 제1 단말은 복호화된 메시지 m'_B에 반사 공격 검증 값 1이 있는지 여부를 확인한다(S225).

[0039] 이와 같이 제1 단말과 제2 단말이 서로 반사 공격 검증을 성공하면, 각각 자신의 난수 값과 전송 받은 난수 값을 연산하여 인증코드를 생성한다(S226, S227). 즉, 제2 단말은 자신의 난수 값(N_B)과 제1 단말로부터 수신한 난수 값(N'_A)을 연산처리하여 인증코드(CV_B)를 생성하고, 제1 단말은 자신의 난수 값(N_A)과 제2 단말로부터 수신한 난수 값(N'_B)을 연산처리하여 인증코드(CV_A)를 생성한다. 본 발명의 실시예에 따르면 인증코드 생성부(140)는 배타적 논리합(exclusive OR)을 이용하여 난수 값들을 연산한다.

[0040] 그리고, OOB 채널 인증 단계(Phase 3)에서는 제1 단말과 제2 단말은 각각 인증코드(CV_A, CV_B)를 OOB 함수에 적용하여, 사용자가 시각적 또는 청각적으로 직접 인식할 수 있는 OOB 채널의 매개 값(O_A, O_B)을 생성한다(S228, S229). 즉, 제1 단말에서는 OOB 함수에 인증코드(CV_A)를 적용하여 출력된 매개 값(O_A)을 획득하고, 제2 단말에서는 OOB 함수에 인증코드(CV_B)를 적용하여 출력된 매개 값(O_B)을 획득하게 된다.

[0041] 그러면 제1 단말의 사용자와 제2 단말의 사용자는 출력된 OOB 채널의 매개 값(O_A)과 매개 값(O_B)을 직접 비교하여 동일한지를 판단하고, 동일한 경우에는 서로 공개키가 정상적으로 교환된 것으로 인증한다. 여기서 OOB(Out-of-Band) 채널은 사람의 시각과 청각을 이용하는 시각(visual) 채널과 청각(auditory) 채널을 포함한다. OOB 채널이 청각 채널인 경우에는 매개 값은 멜로디, 음악, 효과음 등으로 표현되고, 시각 채널인 경우에는 매개 값은 바코드, 색상 등으로 표현된다.

[0042] 본 발명의 실시예와 같이, OOB 채널을 이용하는 페어링 기술에 따르면 사람이 직접 대상 단말인 제1 단말, 제2 단말을 선택하고, 선택한 대상 단말들의 인증 정보를 검증할 수 있으므로, 공격자가 메시지를 변조하거나 인증 대상의 디바이스를 가장하는 것을 TTP 없이 식별할 수 있도록 한다.

[0043] 마지막으로 세션키 설치 단계(Phase 4)에 따르면, 제1 단말과 제2 단말 사이에 공개키 교환에 대한 인증이 성공하면 제1 단말과 제2 단말은 각각 제1 단말과 제2 단말 사이의 세션키(K_{AB})를 생성하고, 전송받은 상대 단말의 ID와 함께 한 쌍으로 저장하게 된다(S230, S231).

[0044] 즉, 제1 단말은 수신된 제2 단말의 공개키(PK_B)를 이용하여 공유 세션키($K_{AB} = (PK_B)^a \bmod p$)를 생성하고, 제2 단말은 수신된 제1 단말의 공개키(PK_A)를 이용하여 공유 세션키($K_{AB} = (PK_A)^b \bmod p$)를 생성한다.

[0045] 이와 같이 본 발명의 실시예에 따르면 해쉬를 대신하여 DH 프로토콜에 기반한 대칭키 암호화 알고리즘을 사용함으로써 제1 단말과 제2 단말이 세션키(K_{AB})를 공유할 수 있다.

[0046] 특히, 본 발명의 실시예에 따르면 OOB 채널 인증 단계(Phase 3)에서 컬러 바코드 비교(CCB, Comparing Color Barcode), CML(Comparing Multi LEDs), CM(Comparing Music) 방법 중 어느 하나를 활용할 수 있는바, 이하에서는 도 4a 내지 도 6c를 통하여 OOB 채널을 인증하는 방법에 대하여 설명한다.

[0047] 도 4a는 본 발명의 실시예에 따른 OOB 변환부가 CCB 방법을 이용하여 매개 값을 산출하는 과정을 설명하기 위한 도면이다. 더욱 상세하게는 도 4a의 좌측 도면은 인증코드(CV)를 OOB 함수에 적용하는 과정을 나타낸 것이고, 우측 도면은 OOB 시각 채널을 통하여 단말기의 화면에 시각적으로 매개 값(O)이 표시되는 것을 나타낸 것이다. 여기서 OOB(Out-of-Band) 함수는 입력된 값을 시각적 또는 청각적 형태의 매개 값으로 변환시키기 위한 함수이다.

[0048] 즉, 도 4a의 좌측 하단에 나타낸 것처럼, 인증코드(CV)는 k+1개의 비트(0~k)로 이루어진 것으로 가정한다. 그러면 인증코드(CV)는 OOB 변환부(150)에 2비트씩 분할되어 입력되며(C_{00}, C_{01}, C_{02}, … C_{ij}), OOB 변환부(150)는 OOB 함수의 출력 매개 값을 i×j 그리드에 미리 지정된 4가지 색상을 통하여 표현한다. 예를 들어, OOB 변환부(150)는 00 비트를 빨간색, 01 비트를 흰색, 10 비트를 파란색, 11 비트를 검은색으로 설정할 수 있으며, 2비트

씩 분할되어 입력된 인증코드(CV)에 대응되는 색상을 해당되는 그리드 화면에 표시한다. 이때 색상의 선택은 서로 보색관계로 하여 색상 구분을 좋게 하는 것이 바람직하다.

[0049] 여기서 인증코드(CV)는 2개 이상의 비트로 분할되며, m개의 비트로 분할되는 경우 2^m개의 색상으로 나타낼 수 있다. 또한 m값이 클수록 화면에 나타내는 그리드의 개수 또는 크기를 줄일 수 있다. 그리고, 분할된 인증코드(CV)는 1개의 그리드에 표현되며, 각각의 그리드는 1개의 색상으로 표시된다.

[0050] 따라서 종래 기술에 따르면 인증코드(CV)를 분할하지 않으므로 2가지 색상인 흑백 그리드(또는 바코드)만으로 매개 값을 표시할 수 있는데 반하여, 본 발명의 실시예에 따르면 인증코드(CV)를 2개 이상의 비트로 분할하므로 다양한 색상으로 나타낼 수 있어 그리드의 개수 또는 크기를 크게 줄일 수 있다.

[0051] 즉, 흑백 그리드를 사용할 경우 0 비트는 검은색, 1 비트는 하얀색으로 나타내는 반면, 본 발명의 실시예와 같이 다양한 색상을 이용하는 경우에는 여러 비트를 하나의 색으로 나타낼 수 있으므로, 그리드의 개수 또는 크기를 현격하게 줄일 수 있다.

[0052] 종래 기술과 같이 매개 값을 흑백 그리드로 나타낼 때 필요로 하는 그리드의 개수를 S라고 하면, 매개 값을 표시하기 위하여 필요한 그리드의 개수(S')는 다음의 수학식 1에 나타낸 것과 같이 감소된다.

수학식 1

[0053] $$S' = S / \log_2 k$$

[0054] 여기서, k는 매개 값을 표시하는데 사용하는 색상 종류의 개수로서 2^m이며, m은 분할된 인증코드(CV)의 비트 개수로서 2이상의 값을 가진다.

[0055] 다만, 컬러 그리드(또는 바코드)의 개수 또는 크기를 줄이기 위하여 너무 많은 색상을 이용하면 사용자로 하여금 인증 과정 수행에 어려움을 줄 수 있기 때문에, 사용자는 그리드의 개수와 색상 개수를 적절하게 조절함으로써, 공개키 교환 인증 과정을 편의성을 도모할 수 있다.

[0056] 도 4b는 도 4a에 따른 OOB 함수의 매개 값이 화면 상에 표시되는 것을 도시한 예시도이다. 도 4b에서는 인증코드(CV)로 128비트 길이의 난수를 사용했을 경우의 동작화면으로서, 4가지 색상을 이용하여 표시하는 것으로 설정한 것이다.

[0057] 따라서, 종래의 흑백 그리드의 경우 128개의 그리드가 필요한 반면, 본 발명의 실시예에 다른 컬러 그리드를 사용하는 경우에는 수학식 1을 통해서 확인할 수 있듯이, 절반 크기인 64개의 그리드만으로도 인증 코드의 표현이 가능하다.

[0058] 이와 같이 본 발명의 실시예에 따르면 짧은 길이의 인증코드를 사용하므로 OOB 채널을 통한 인증 기법 사용 시 높은 사용성 증대를 기대할 수 있다. 또한 인증코드 길이의 조절이 유연하므로 어플리케이션의 보안 요구 수준에 따라 인증코드의 길이를 조절하여 사용성과 보안성의 절충을 꾀할 수 있다. 또한 컬러 그리드는 기존 흑백 그리드에 비해 절반 크기 또는 개수로 표현이 가능하므로 사용자가 직접적인 세션키 인증을 훨씬 수월하게 할 수 있게 한다.

[0059] 도 5a는 본 발명의 실시예에 따른 OOB 변환부가 CML 방법을 이용하여 매개 값을 산출하는 과정을 설명하기 위한 도면이다. 더욱 상세하게는 도 5a의 좌측 도면은 인증코드(CV)를 OOB 함수에 적용하는 과정을 나타낸 것이고, 우측 도면은 OOB 시각 채널을 통하여 생성된 매개 값(O)이 LED에 점멸되어 표시되는 것을 나타낸 것이다.

[0060] 즉, CML 방법에 따르면, 디스플레이 화면이 구비되지 않은 무선 통신 단말이 외부의 LED 표시 장치와 통신하여, 인증코드(CV)의 값을 LED의 점등 또는 소등으로 표현하도록 한다.

[0061] 인증코드(CV)는 OOB 변환부(150)에 입력되면, OOB 변환부(150)는 k비트의 인증코드를 최하위 비트부터 1비트씩 추출하여 LED의 점등 및 소등 상태 값으로 할당한다. 예를 들어, OOB 변환부(150)는 비트열의 1은 점등 값으로, 0은 소등 값으로 설정한다.

[0062] 도 5b는 도 5a에 따른 OOB 함수의 매개 값이 LED를 통하여 표시되는 것을 도시한 예시도이다. 도 5b에서 점등은 빨간색으로, 소등은 흰색으로 표시하였다. OOB 변환부(150)는 LED의 점등/소등 여부를 결정하는 매개 값

(LD_0, LD_1, … LD_K)을 생성하고, 생성된 매개 값을 시리얼 통신 등을 통하여 LED 표시 장치로 전달한다. 그리고, LED 표시 장치는 대응되는 매개 값에 따라 LED의 점등 또는 소등하도록 한다. 따라서 사용자는 LED의 점등 및 소등 상태 만으로 편리하게 세션키 교환 여부를 확인할 수 있다.

[0063] 도 6a는 본 발명의 실시예에 따른 OOB 변환부가 CM 방법을 이용하여 매개 값을 산출하는 과정을 설명하기 위한 도면이다. 더욱 상세하게는 도 6a의 좌측 도면은 인증코드(CV)를 OOB 함수에 적용하는 과정을 나타낸 것이고, 우측 도면은 OOB 청각 채널을 통하여 음악 파일의 인덱스 형태로 매개 값(O)이 생성되는 것을 나타낸 것이다. 도 6b는 도 6a에 따른 OOB 함수의 매개 값에 따라 음악 파일이 재생되는 화면을 도시한 예시도이다.

[0064] CM 방법에 따르면 인증코드(CV)가 OOB 변환부(150)에 입력되면, OOB 변환부(150)는 k비트의 인증코드를 음악 파일의 인덱스 형태로 매개 값(O)을 생성한다. 그러면 인덱스 값에 따라서 무선 통신 단말에 저장된 음악 파일(wav)이 재생된다. 여기서 인증코드가 k 비트인 경우 2^k개의 음악 파일이 저장된다. 예를 들어, 인증코드(CV)가 0011인 경우, 인증코드의 10진수 값에 해당하는 3번 인덱스에 해당하는 음악파일이 재생되도록 한다. 따라서 사용자는 짧은 멜로디 만으로도 편리하게 세션키 교환 여부를 확인할 수 있다.

[0065] 본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 다른 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의하여 정해져야 할 것이다.

부호의 설명

[0066] 100: 무선 통신 단말, 110: 저장부,

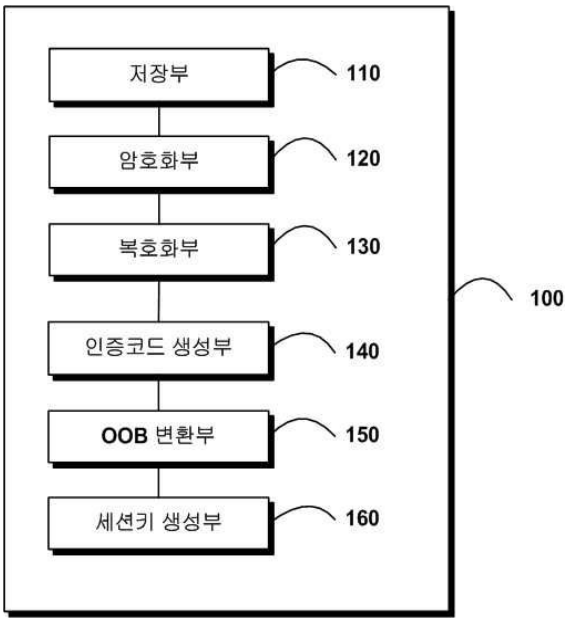
120: 암호화부, 130: 복호화부,

140: 인증코드 생성부, 150: OOB 변환부,

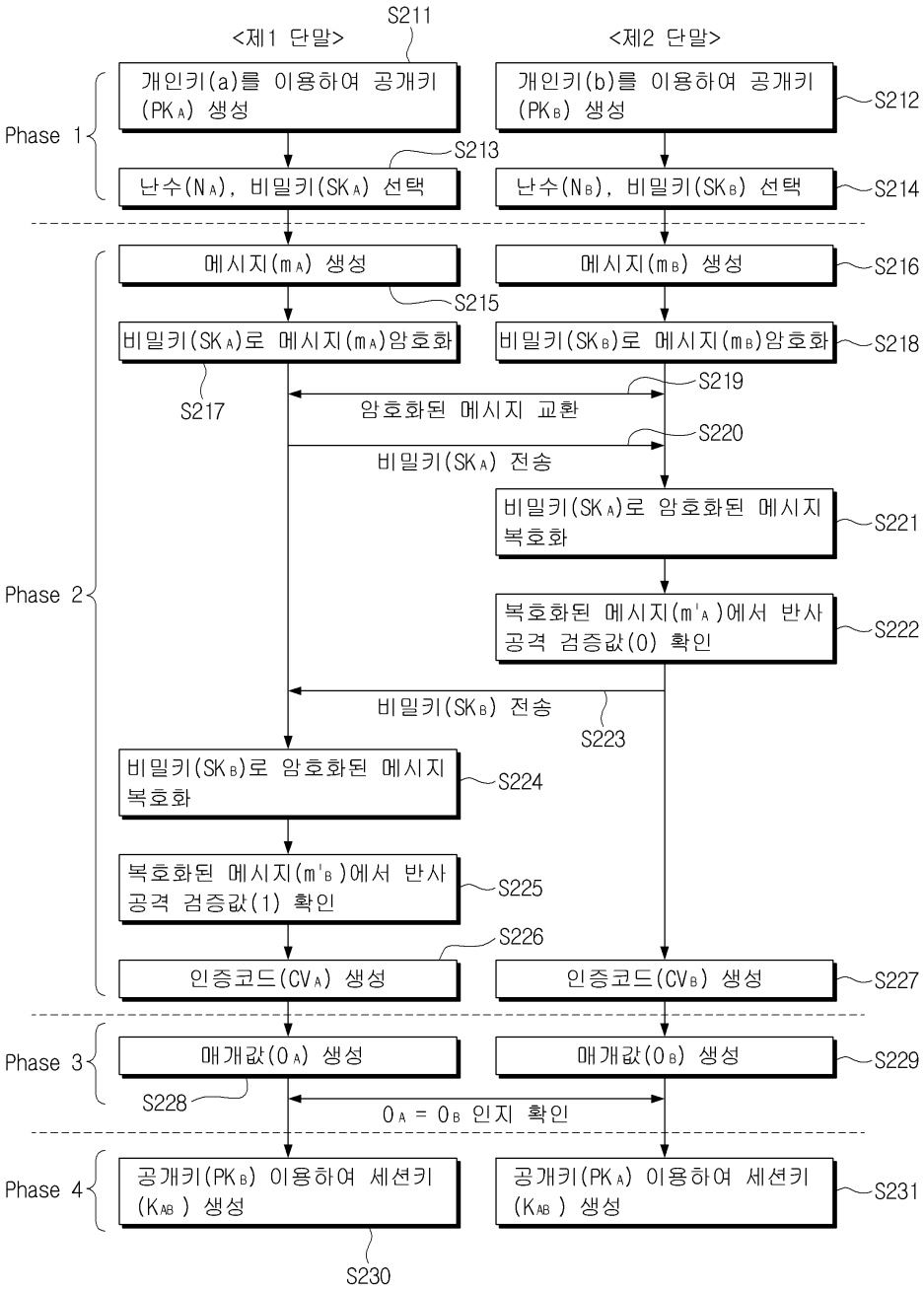
160: 세션키 생성부

도면

도면1



도면2


S211
<제1 단말>
<제2 단말>
Phase 1
개인키(a)를 이용하여 공개키 (PKA) 생성
개인키(b)를 이용하여 공개키 (PKB) 생성
S212
S213
난수(NA), 비밀키(SKA) 선택
난수(NB), 비밀키(SKB) 선택
S214
Phase 2
메시지(mA) 생성
메시지(mB) 생성
S216
S215
비밀키(SKA)로 메시지(mA)암호화
비밀키(SKB)로 메시지(mB)암호화
S218
S217
S219
암호화된 메시지 교환
S220
비밀키(SKA) 전송
비밀키(SKA)로 암호화된 메시지 복호화
S221
복호화된 메시지(m'A)에서 반사 공격 검증값(0) 확인
S222
비밀키(SKB) 전송
S223
비밀키(SKB)로 암호화된 메시지 복호화
S224
복호화된 메시지(m'B)에서 반사 공격 검증값(1) 확인
S225
S226
인증코드(CVA) 생성
인증코드(CVB) 생성
S227
Phase 3
매개값(0A) 생성
매개값(0B) 생성
S229
S228
0A = 0B 인지 확인
Phase 4
공개키(PKB) 이용하여 세션키 (KAB) 생성
공개키(PKA) 이용하여 세션키 (KAB) 생성
S231
S230

도면3

<제1 단말> <제2 단말>

Phase 1 : Setup

Given : $ID_A, PK_A = g^a \bmod p$ Given : $ID_B, PK_B = g^b \bmod p$

Pick : $N_A \in \{0,1\}^k, SK_A \in \{0,1\}^t$ Pick : $N_B \in \{0,1\}^k, SK_B \in \{0,1\}^t$

Phase 2 : PK Exchange

$m_A \leftarrow 0 \| ID_A \| PK_A \| N_A$ $m_B \leftarrow 1 \| ID_B \| PK_B \| N_B$

$E(SK_A, m_A)$ →

$E(SK_B, m_B)$ ←

SK_A → $m'_A \leftarrow D(SK_A, E(SK_A, m_A))$

SK_B ← Verify 0 in m'_A

$m'_B \leftarrow D(SK_B, E(SK_B, m_B))$ $CV_B \leftarrow N_B \oplus N'_A$

Verify 1 in m'_B

$CV_A \leftarrow N_A \oplus N'_B$

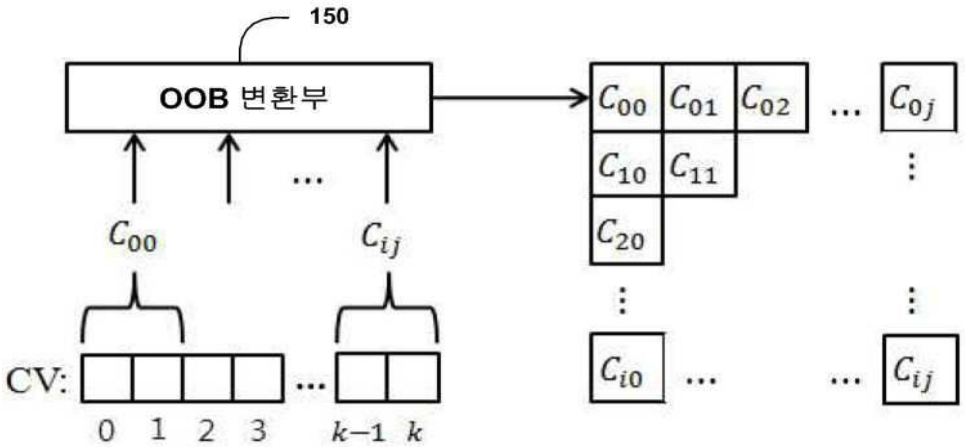
Phase 3: OOB channel Authentication

$O_A \leftarrow OOB(CV_A)$ $\xleftrightarrow{O_A = O_B}$ $O_B \leftarrow OOB(CV_B)$

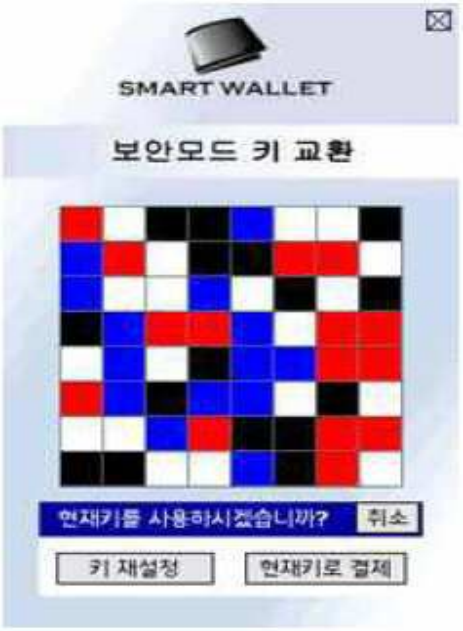
Phase 4: Session Key Establishment

$K_{AB} = (PK_B)^a \bmod p$ $K_{AB} = (PK_A)^b \bmod p$

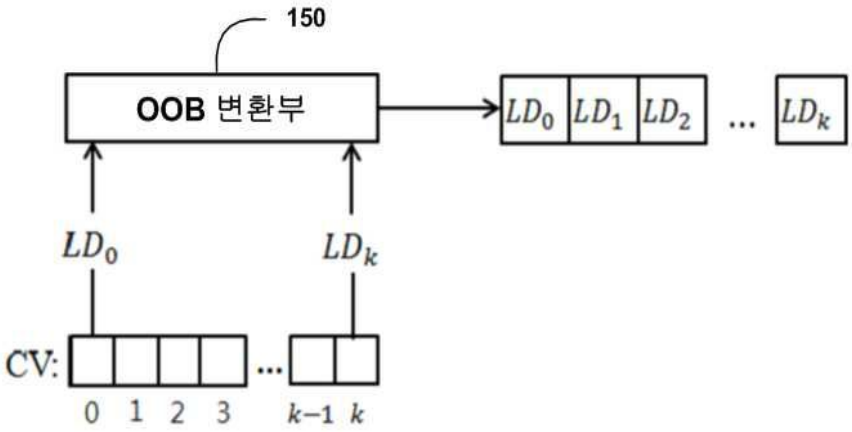
도면4a



도면4b


SMART WALLET
보안모드 키 교환
현재키를 사용하시겠습니까?
취소
키 재설정
현재키로 결제

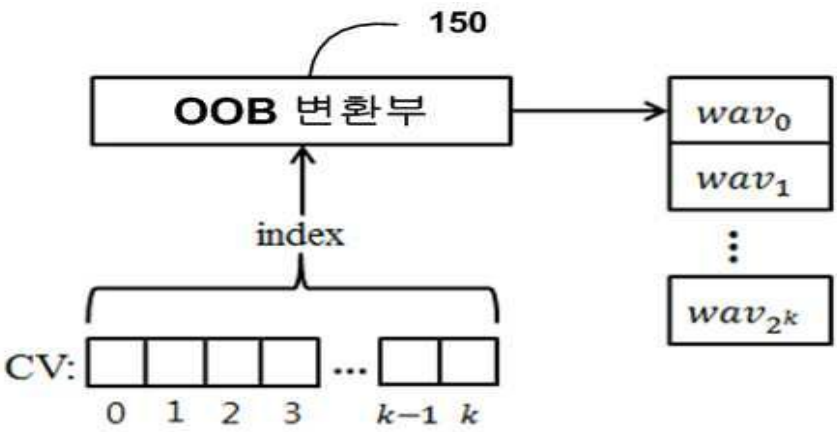
도면5a


150
OOB 변환부
LD_0
LD_1
LD_2
...
LD_k
LD_0
LD_k
CV:
0 1 2 3
k−1 k

도면5b


SMART WALLET
보안모드 키 교환
현재키를 사용하시겠습니까?
취소
키 재설정
현재키로 결제

도면6a


150
OOB 변환부
wav_0
wav_1
wav_{2^k}
index
CV:
0 1 2 3 ... k−1 k

도면6b