(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년03월04일
(11) 등록번호 10-1599994
(24) 등록일자 2016년02월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01)
(21) 출원번호 10-2014-0157220
(22) 출원일자 2014년11월12일
심사청구일자 2014년11월12일
(56) 선행기술조사문헌
US20050044356 A1
KR1020140057134 A
Xiaobing He 외 2인, Journal of Network and Computer Applications, "Dynamic Key Management in Wireless Sensor Networks: A Servey" (2013.04.26. 공개)

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이영경
서울특별시 동대문구 안암로22길 9 302호
엄지은
서울특별시 서대문구 가재울로 45 현대아파트 102-102
이동훈
서울특별시 종로구 사직로8길 34 경희궁의아침3단지 1404호
(74) 대리인
김등용, 김홍석

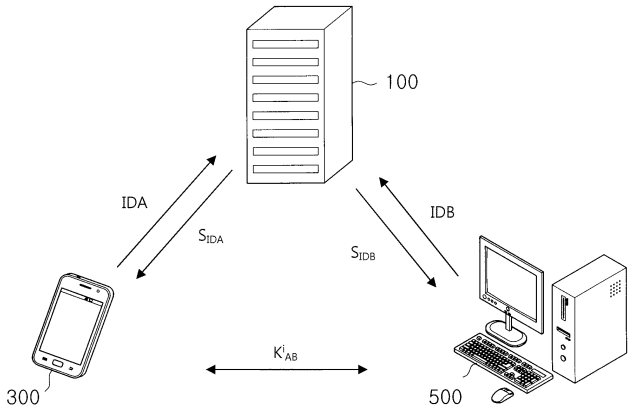
전체 청구항 수 : 총 6 항 심사관 : 문형섭

(54) 발명의 명칭 **신원기반 키교환 방법 및 시스템**

(57) 요 약

키교환 방법이 개시된다. 상기 키교환 방법은 (a) 제1 단말기가 상기 제1 단말기의 아이디(IDA)를 서버로 송신하는 단계, (b) 상기 제1 단말기가 상기 서버로부터 상기 제1 단말기의 개인키(S_{IDA}^{i})를 수신하는 단계, (c) 상기 제1 단말기가 상기 제1 단말기와 제2 단말기 사이의 세션키(K_{AB}^{i})를 생성하는 단계, 및 (d) 상기 제1 단말기가 상기 개인키(S_{IDA}^{i})를 업데이트하는 단계를 포함하고, 상기 (c) 단계와 상기 (d) 단계는 적어도 1회 이상 주기적으로 수행되되, 상기 (c) 단계는 업데이트된 개인키를 기초로 상기 제1 단말기와 상기 제2 단말기 사이의 세션키를 생성하는 것을 특징으로 한다.

대 표 도 - 도1



10

이 발명을 지원한 국가연구개발사업
과제고유번호 NIPA-2014-H0301-14-1004
부처명 미래창조과학부
연구관리전문기관 정보통신산업진흥원
연구사업명 ITRC
연구과제명 제어시스템 보안 연구
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2014.01.01 ~ 2014.12.31

명 세 서

청구범위

청구항 1

(a) 제1 단말기가 상기 제1 단말기의 아이디(IDA)를 서버로 송신하는 단계;

(b) 상기 제1 단말기가 상기 서버로부터 상기 아이디(IDA)에 대응하는, 상기 제1 단말기의 개인키(S_{IDA}^{i})를 수신하는 단계;

(c) 상기 제1 단말기가 상기 개인키(S_{IDA}^{i})와 제2 단말기의 아이디(IDB)를 이용하여 상기 제1 단말기와 상기 제2 단말기 사이의 세션키(K_{AB}^{i})를 생성하는 단계; 및

(d) 상기 제1 단말기가 상기 개인키(S_{IDA}^{i})를 업데이트하는 단계를 포함하고,

상기 (c) 단계와 상기 (d) 단계는 적어도 1회 이상 주기적으로 수행되되, 상기 (c) 단계는 업데이트된 개인키를 기초로 상기 제1 단말기와 상기 제2 단말기 사이의 세션키를 생성하는,

키교환 방법.

청구항 2

제1항에 있어서,

상기 (d) 단계는 상기 개인키(S_{IDA}^{i})와 다음 주기에 대응하는 공개변수(h_{i+1})를 입력으로 하는 다선형 함수($S_{IDA}^{i+1} = e(S_{IDA}^{i}, h_{i+1})$)를 연산하여 상기 개인키를 업데이트하는, 키교환 방법.

청구항 3

제1항에 있어서,

상기 (c) 단계는 상기 개인키(S_{IDA}^{i}), 공개변수($u_{i+1}, \cdots, u_{n}$) 및 상기 상기 아이디(IDB)의 해쉬값($H_1(IDB)$)을 입력으로 하는 다선형 함수를 연산하여 상기 세션키를 생성하는, 키교환 방법.

청구항 4

서버와 제1 단말기를 포함하는 키교환 시스템에 있어서,

상기 서버는,

제1 공개변수들, 제2 공개변수들 및 초기 마스터키를 생성하는 셋업 모듈;

상기 초기 마스터키를 주기적으로 업데이트하는 마스터키 업데이트 모듈; 및

상기 제1 단말기로부터 수신된 아이디에 대응하는 개인키를 생성하고, 생성된 개인키를 상기 제1 단말기로 송신하는 비밀키 생성 모듈을 포함하고,

상기 제1 단말기는,

상기 서버로 상기 아이디를 송신하고, 상기 서버로부터 상기 개인키를 수신하는 송수신 모듈;

상기 개인키를 주기적으로 업데이트하는 업데이트 모듈; 및

제2 단말기의 아이디와 상기 개인키를 이용하여 해당 주기에서 상기 제1 단말기와 상기 제2 단말기 간의 세션키를 생성하는 키교환 모듈을 포함하는,

키교환 시스템.

청구항 5

제4항에 있어서,

상기 업데이트 모듈은 상기 개인키를 입력으로 하는 다선형 함수를 연산하여 상기 개인키를 업데이트하는, 키교환 시스템.

청구항 6

제4항에 있어서,

상기 키교환 모듈은 상기 제2 단말기의 아이디의 해쉬값과 상기 개인키를 입력으로 하는 다선형 함수를 연산하여 상기 세션키를 생성하는, 키교환 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 신원기반 키교환 방법에 관한 것으로, 특히 개인키와 마스터키의 주기적인 업데이트를 통해 세션키의 안전성을 보장할 수 있는 전방향 안전성을 갖는 신원기반 키교환 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 키교환 프로토콜(key exchange protocol)은 안전한 통신을 위한 기술로써, 안전하지 않은 채널에서 키를 공유하기 위한 암호학적 도구이다. 신원기반(identity-based) 구조에서는 사용자의 공개키를 인증해 주어야 하는 PKI(Public Key Infrastructure) 구조와 다르게 시스템 내에서의 아이디 자체가 공개키 역할을 수행하므로 인증서 관리의 문제점을 해결할 수 있다. 최근 이러한 신원기반 구조에서 사전전송이 필요없는(non-interactive) 키교환 기법에 관한 연구가 제안되고 있다. 기존의 키교환 기법들은 1~2회의 정보 교환을 통하여 안전한 키를 생성하였는데, 사전전송이 필요없는 키교환 기법에서는 주고받는 사전정보 없이 자신의 비밀키와 상대방의 공개키만을 가지고 키 교환을 실행할 수 있다. 사전전송이 필요없는 키교환 기법은 사전전송으로 소요되는 시간과 전송 비용을 없애기 때문에 효율적인 키 교환 기법으로 볼 수 있다. 또한 상대방이 키교환을 시행할 준비가 안되어있어도 키교환을 시행할 수 있기 때문에 통신 상태가 불안정한 객체와의 키 교환에서 효율적으로 사용될 수 있다. 기존의 키교환 기법에서는 세션키(session key)의 안전성을 높이기 위해 사전에 주고받는 임시키(ephemeral key)가 세션키 생성에 관여하는 방식이었다.

선행기술문헌

특허문헌

[0003] (특허문헌 0001) 대한민국 등록특허 제10-1125481호

(특허문헌 0002) 대한민국 등록특허 제10-1373577호

발명의 내용

해결하려는 과제

[0004] 본 발명이 이루고자 하는 기술적인 과제는 사용자의 개인키와 마스터키를 주기적으로 업데이트하여 사용자의 개인키가 노출되더라도 이전에 생성된 세션키의 안전성을 보장할 수 있는 신원기반 키교환 방법 및 시스템을 제공하는 것이다.

과제의 해결 수단

[0005] 본 발명의 실시 예에 따른 키교환 방법은, (a) 제1 단말기가 상기 제1 단말기의 아이디(IDA)를 서버로 송신하는 단계, (b) 상기 제1 단말기가 상기 서버로부터 상기 제1 단말기의 개인키(S_{IDA}^{i})를 수신하는 단계, (c) 상기 제1 단말기가 상기 제1 단말기와 제2 단말기 사이의 세션키(K_{AB}^{i})를 생성하는 단계, 및 (d) 상기 제1 단말기가 상기 개인키(S_{IDA}^{i})를 업데이트하는 단계를 포함하고, 상기 (c) 단계와 상기 (d) 단계는 적어도 1회 이상 주기적으로 수행되되, 상기 (c) 단계는 업데이트된 개인키를 기초로 상기 제1 단말기와 상기 제2 단말기 사이의 세션키를 생성한다.

[0006] 본 발명의 실시 예에 따른 키교환 시스템은 서버와 제1 단말기를 포함하고, 상기 서버는, 제1 공개변수들, 제2 공개변수들 및 초기 마스터키를 생성하는 셋업 모듈; 상기 초기 마스터키를 주기적으로 업데이트하는 마스터키 업데이트 모듈, 및 상기 제1 단말기로부터 수신된 아이디에 대응하는 개인키를 생성하고, 생성된 개인키를 상기 제1 단말기로 송신하는 비밀키 생성 모듈을 포함하고, 상기 제1 단말기는, 상기 서버로 상기 아이디를 송신하고, 상기 서버로부터 상기 개인키를 수신하는 송수신 모듈, 상기 개인키를 주기적으로 업데이트하는 업데이트 모듈, 및 해당 주기에서 상기 제1 단말기와 제2 단말기 간의 세션키를 생성하는 키교환 모듈을 포함한다.

발명의 효과

[0007] 본 발명의 실시 예에 따른 신원기반 키교환 방법 및 시스템은 사용자의 개인키가 노출되어도 개인키의 업데이트 이전에 생성된 세션키의 안전성을 보장할 수 있는 효과가 있다.

[0008] 또한, 상기 신원기반 키교환 방법 및 시스템은 PKI(public key infrastructure)없이 구현이 가능하며 두 객체가 사전전송없이 안전한 키교환을 수행할 수 있는 효과가 있다.

[0009] 또한, 상기 신원기반 키교환 방법 및 시스템은 통신 상태가 불안정한 객체를 상대방으로하여 즉각적인 키교환을 수행할 수 있는 효과가 있다.

도면의 간단한 설명

[0010] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 실시 예에 의한 키교환 시스템을 도시한다.

도 2는 도 1에 도시된 서버의 기능 블럭도이다.

도 3은 도 1에 도시된 제1 단말기의 기능 블럭도이다.

도 4는 도 1에 도시된 키교환 시스템을 이용한 키교환 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0011] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0012] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0013] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0014] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소

에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0015] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0016] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0017] 우선, 본 발명에 대한 구체적인 설명에 앞서 기초적인 개념과 알고리즘을 설명하면 다음과 같다.

[0018] 전방향 안전성(forward secrecy)이란 사용자의 개인키가 노출되어도 이전에 맺었던 세션키의 안전성이 보장됨을 의미한다. 즉, 기존의 키교환 기법에서는 전방향 안전성을 만족시키기 위해 사용자들이 키교환을 시행하기 전에 각각 임시키(임시 공개키와 임시 개인키)를 생성하여 임시 공개키(ephemeral public key)를 교환하고 교환된 임시키 정보를 세션키 생성 과정에 관여시킨다. 그러므로 사용자의 개인키가 노출되어도 공격자가 이전에 맺은 세션키에서 사용된 임시 개인키(ephemeral private key)를 모르면 세션키의 정보를 유추해낼 수 없다.

[0019] 본 발명은 사전전송이 필요없는 키교환 기법에 관한 것으로서, 전방향 안전성을 만족시키기 위해 개인키를 주기적으로 업데이트한다. 업데이트 이후의 개인키가 노출되어도 이전에 맺은 세션키에 대해 당시의 개인키를 알지 못하면 세션키의 정보를 유추해낼 수 없다.

[0020] 다선형 함수(leveled multilinear map)란 n(n은 자연수) 개의 순환군(cyclic group; $G_1, \cdots, G_n$으로 이루어져 있으며 위수(order)는 모두 소수 p로 동일하다. 이때, 겹선형 함수(bilinear map) $e_{i,j} : G_i \times G_j \rightarrow G_{i+j} (i,j \geq 1, i+j \leq n)$가 모든 $g_i \in G_i, g_j \in G_j$와 $a, b \in Z_p$에 대해서 $e_{i,j}(g_i^a, g_j^b) = e_{i,j}(g_i, g_j)^{a \cdot b}$를 만족할 때, 다선형 함수라 한다. 이하에서는 표기의 간략함을 위하여, i와 j가 명확하다면 $e_{i,j}$를 e로 표기하고 $e(g_1, e(g_2, \cdots, g_n) \cdots)$을 $e(g_1, g_2, \cdots, g_n)$로 표기하기로 한다.

[0021] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0022] 도 1은 본 발명의 실시 예에 의한 키교환 시스템을 도시한다.

[0023] 도 1을 참조하면, 키교환 시스템(10)은 서버(100), 제1 단말기(300) 및 제2 단말기(500)를 포함한다. 도 1에는 2 개의 단말기들만이 도시되어 있으나, 본 발명이 이에 제한되는 것은 아니며, 키교환 시스템(10)에는 2 이상의 단말기들이 포함될 수 있다. 또한, 키교환 시스템(10) 내에서 동기화된 주기 개념이 적용되기 위해서, 서버(100), 제1 단말기(300) 및 제2 단말기(500) 각각은 동기화된 타이머 또는 동기화된 카운터를 포함할 수 있다.

[0024] 키생성 기관(Key Generation Center; KGC) 또는 키생성 서버라고도 불릴 수 있는 서버(100)는 소정의 알고리즘을 이용하여 공개변수, 마스터키 등을 생성할 수 있다. 또한, 서버(100)는 생성된 마스터키를 주기적으로 업데이트하여 새로운 마스터키를 생성할 수 있다.

[0025] 서버(100)는 제1 단말기(300) 또는 제2 단말기(500)로부터 아이디(ID)를 수신하고, 수신된 아이디에 대응하는

개인키를 생성하고, 생성된 개인키를 아이디(ID)를 송신한 단말기로 송신할 수 있다. 구체적으로, 서버(100)는 제1 단말기(300)로부터 제1 단말기(300)의 아이디(IDA)를 수신하고, 제1 단말기(300)의 개인키(S_{IDA})를 생성하여 생성된 개인키(S_{IDA})를 제1 단말기(300)로 송신한다. 또한, 서버(100)는 제2 단말기(500)로부터 제2 단말기(500)의 아이디(IDB)를 수신하고, 제2 단말기(500)의 개인키(S_{IDB})를 생성하여 생성된 개인키(S_{IDB})를 제2 단말기(500)로 송신한다.

[0026] 제1 단말기(300)와 제2 단말기(500)는 서버(100)로부터 수신한 개인키를 주기적으로 업데이트하여 새로운 개인키를 생성하고, 각각의 주기에 대응하는 세션키를 생성할 수 있다. 구체적으로, 제1 단말기(300)는 제1 단말기(300)의 아이디(IDA)를 서버(100)로 송신하고, i번째 주기에 대응하는 개인키(S_{IDA}^{i})를 서버(100)로부터 수신한다. 제1 단말기(300)는 주기적으로 개인키를 업데이트할 수 있다. 또한, 제1 단말기(300)는 각각의 주기에 대응하는 개인키를 이용하여 각각의 주기에 대응하는 세션키를 생성할 수 있다. 실시 예에 따라, 상기 개인키는 비밀키로 불릴 수도 있다.

[0027] 제2 단말기(500)의 기능 및 구성은 제1 단말기(300)의 기능 및 구성과 동일할 수 있으므로 이에 관한 상세한 설명은 생략하기로 한다.

[0028] 도 2는 도 1에 도시된 서버의 기능 블럭도이다.

[0029] 도 1과 도 2를 참조하면, 서버(100)는 셋업 모듈(110), 마스터키 업데이트 모듈(130) 및 비밀키 생성 모듈(150)을 포함한다.

[0030] 셋업 모듈(110)은 셋업 알고리즘($Setup(1^k, n)$)을 이용하여 공개변수, 마스터키 등을 생성할 수 있다. 구체적으로, 셋업 모듈(110)은 보안 상수(1^k)와 공개변수의 갯수(n, n은 자연수)를 입력받아 다선형 함수(e), 생성원($g \in G_1$), 제1 공개변수들($(u_1, \cdots, u_n) \in G_1^n$), 제2 공개변수들 ($(h_0, \cdots, h_n) \in G_1^{n+1}$), 해쉬함수($H_1 : \{0,1\}^* \rightarrow G_1^*$), 및 초기 마스터키($mk_0 = h_0^s$)를 생성한다. 이때, 상기 s 는 셋업 모듈(110)에 의해 생성된 비밀값으로, 초기 마스터키의 생성이 완료된 후 셋업 모듈(110)에 의해 삭제되어야 한다. 상기 s가 노출되는 경우, 전방향 안전성을 만족시키지 못하기 때문이다.

[0031] 마스터키 업데이트 모듈(130)은 마스터키 업데이트 알고리즘($MasterKeyUpdate(mk_{i-1})$)을 이용하여 i번째 주기의 마스터키를 생성할 수 있다. 구체적으로 마스터키 업데이트 모듈(130)은 아래의 수학식 1을 이용하여 i-1번째 주기의 마스터키(mk_{i-1})와 제2 공개변수(h_i)를 입력으로 하는 다선형 함수(e)를 연산함으로써 i번째 주기의 마스터키(mk_i)를 생성할 수 있다.

수학식 1

[0032] $$mk_i = e(mk_{i-1}, h_i) = e(h_0, \cdots, h_i)^s$$

[0033] 비밀키 생성 모듈(150)은 키추출 알고리즘($KeyExtract(mk_i, ID)$)을 이용하여 사용자의 개인키를 생성할 수 있다. 구체적으로 비밀키 생성 모듈(150)은 아래의 수학식 2를 이용하여 사용자의 아이디(ID)를 해쉬연산한 값과 마스터키를 입력으로 하는 다선형 함수(e)를 연산함으로써 상기 사용자의 개인키(S_{ID}^{i})를 생성할 수 있다. 이때, 상기 사용자의 아이디(ID)는 상기 사용자의 단말기로부터 수신될 수 있다.

수학식 2

[0034] $$S_{ID}^{i} = e(mk_i, H_1(ID))$$

[0035] 또한, 비밀키 생성 모듈(150)은 생성된 개인키(S_{ID}^{i})를 사용자에게 송신할 수 있다.

[0036] 도 3은 도 1에 도시된 제1 단말기의 기능 블럭도이다.

[0037] 도 1과 도 3을 참조하면, 제1 단말기(300)는 송수신 모듈(310), 업데이트 모듈(330) 및 키교환 모듈(350)을 포함한다.

[0038] 송수신 모듈(310)은 제1 단말기(300)의 아이디(IDA)를 서버(100)로 송신하고, 서버(100)로부터 제1 단말기(300)의 개인키(S_{IDA}^{i})를 수신할 수 있다. 예컨대, 송수신 모듈(310)이 i번째 주기 동안에 아이디(IDA)를 서버(100)로 송신한 경우, 송수신 모듈(310)은 i번째 주기 동안의 개인키(S_{IDA}^{i})를 서버(100)로부터 수신할 수 있다.

[0039] 업데이트 모듈(330)은 키 업데이트 알고리즘($KeyUpdate(S_{IDA}^{i})$)을 수행하여 개인키를 주기적으로 업데이트할 수 있다. 구체적으로, 업데이트 모듈(330)은 아래의 수학식 3을 이용하여 수신된 개인키(S_{IDA}^{i})를 주기적으로 업데이트할 수 있다. 예컨대, 업데이트 모듈(330)은 i번째 주기의 개인키(S_{IDA}^{i})와 공개변수(h_{i+1})를 입력으로 하는 다선형 함수(e)를 연산함으로써 i+1번째 주기의 개인키(S_{IDA}^{i+1})를 생성할 수 있다.

수학식 3

[0040] $$KeyUpdate(S_{IDA}^{i}) \rightarrow S_{IDA}^{i+1} = e(S_{IDA}^{i}, h_{i+1})$$

[0041] 키교환 모듈(350)은 주기적으로 공유키 생성 알고리즘($SharedKey(S_{IDA}^{i}, IDB)$)을 수행하여 각각의 주기에서 제1 단말기(300)와 제2 단말기(500) 간의 세션키를 생성한다. 구체적으로 키교환 모듈(350)은 아래의 수학식 4를 이용하여 i번째 주기에서의 제1 단말기(300)의 개인키(S_{IDA}^{i}), 공개변수($u_{i+1}, \cdots, u_n$), 및 제2 단말기(500)의 아이디(IDB)의 해쉬값($H_1(IDB)$)을 입력으로 하는 다선형 함수(e)를 연산함으로써, i번째 주기에서의 제1 단말기(300)와 제2 단말기(500) 간의 세션키(K_{AB}^{i})를 생성할 수 있다.

수학식 4

[0042] $$SharedKey(S_{IDA}^{i}, IDB) \rightarrow K_{A,B}^{i} = e(S_{IDA}^{i}, u_{i+1}, \cdots, u_n, H_1(IDB))$$

[0043] 도 1에 도시된 제2 단말기(500)의 기능 및 구성은 제1 단말기(300)의 기능 및 구성과 동일할 수 있으므로, 이에 관한 상세한 설명은 생략하기로 한다.

[0044] 다만, 제1 단말기(300)에 의해 생성된 세션키(K_{AB}^{i})와 제2 단말기(500)에 의해 생성된 세션키(K_{BA}^{i})의 동일성은 아래의 수학식 5를 통하여 증명될 수 있다.

수학식 5

[0045]
$$
\begin{aligned}
K_{AB}^{i} &= e(S_{IDA}^{i}, u_{i+1}, \cdots, u_n, H_1(IDB)) \\
&= e(e(H_1(IDA), h_0, \cdots, h_i)^s), u_{i+1}, \cdots, u_n, H_1(IDB)) \\
&= e(H_1(IDA), h_0, \cdots, h_i, u_{i+1}, \cdots, u_n, H_1(IDB))^s \\
&= e(H_1(IDB), h_0, \cdots, h_i, u_{i+1}, \cdots, u_n, H_1(IDA))^s \\
&= e(e(H_1(IDB), h_0, \cdots, h_i)^s, u_{i+1}, \cdots, u_n, H_1(IDA)) \\
&= e(S_{IDB}^{i}, u_{i+1}, \cdots, u_n, H_1(IDA)) \\
&= K_{BA}^{i}
\end{aligned}
$$

[0046] 따라서, 제1 단말기(300)와 제2 단말기(500)는 각 주기별로 동일한 세션키를 생성함으로써, 세션키 교환을 수행할 수 있다. 또한, 상대방 단말기의 통신 상태가 불안정하더라도 즉각적인 세션키 교환을 수행할 수 있다.

[0047] 도 2에 도시된 서버(100) 및 도 3에 도시된 제1 단말기(300) 구성들 각각은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것이 아님을 본 발명의 기술분야의 평균적 전문가는 용이하게 추론할 수 있을 것이다.

[0048] 또한, 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

[0049] 도 4는 도 1에 도시된 키 교환 시스템을 이용한 키 교환 방법을 설명하기 위한 흐름도이다.

[0050] 도 1 내지 도 4를 참조하면, 서버(100)의 셋업 모듈(110)은 셋업 알고리즘을 수행하여 초기 마스터키(mk_0)를 생성한다(S100).

[0051] 초기 마스터키(mk_0)는 서버(100)의 마스터키 업데이트 모듈(130)에 의해 주기적으로 업데이트될 수 있다(S200). 예컨대, i-1 번째 주기에서 서버(100)의 마스터키 업데이트 모듈(130)은 마스터키 업데이트 알고리즘을 이용하여 i 번째 주기의 마스터키(mk_i)를 생성할 수 있다(S200).

[0052] i 번째 주기에서, 서버(100)의 비밀키 생성 모듈(150)은 제1 단말기(300)의 송수신 모듈(310)로부터 제1 단말기(300)의 아이디(IDA)를 수신할 수 있다(S310). 비밀키 생성 모듈(150)은 아이디(IDA)의 수신에 대한 응답으로 i 번째 주기에서의 제1 단말기(300)의 개인키(S_{IDA}^{i})를 생성하고, 생성된 개인키(S_{IDA}^{i})를 제1 단말기(300)의 송수신 모듈(310)로 송신할 수 있다(S320).

[0053] i 번째 주기에서, 서버(100)의 비밀키 생성 모듈(150)은 제2 단말기(500)의 송수신 모듈로부터 제2 단말기(500)의 아이디(IDB)를 수신할 수 있다(S340). 비밀키 생성 모듈(150)은 아이디(IDB)의 수신에 대한 응답으로 i 번째 주기에서의 제2 단말기(500)의 개인키(S_{IDB}^{i})를 생성하고, 생성된 개인키(S_{IDB}^{i})를 제2 단말기(500)의 상기 송수신 모듈로 송신할 수 있다(S350).

[0054] i 번째 주기 동안에, 서버(100)의 마스터키 업데이트 모듈(130)은 i+1 번째 주기에서의 마스터키(mk_{i+1})를 생

성한다(S370). 제1 단말기(300)의 업데이트 모듈(330)은 i+1 번째 주기의 제1 단말기(300)의 개인키(S_{IDA}^{i+1})와 i 번째 주기의 세션키(K_{AB}^{i})를 생성할 수 있다(S380). 마찬가지로, 제2 단말기(500)의 업데이트 모듈(330)은 i+1 번째 주기의 제2 단말기(500)의 개인키(S_{IDB}^{i+1})와 i 번째 주기의 세션키(K_{BA}^{i})를 생성할 수 있다(S390).

[0055] i+1 번째 주기 동안에, 서버(100)의 마스터키 업데이트 모듈(130)은 i+2 번째 주기에서의 마스터키(mk_{i+2})를 생성한다(S410). 제1 단말기(300)의 업데이트 모듈(330)은 i+2 번째 주기의 제1 단말기(300)의 개인키(S_{IDA}^{i+2})와 i+1 번째 주기의 세션키(K_{AB}^{i+1})를 생성할 수 있다(S430). 마찬가지로, 제2 단말기(500)의 업데이트 모듈(330)은 i+2 번째 주기의 제2 단말기(500)의 개인키(S_{IDB}^{i+2})와 i+1 번째 주기의 세션키(K_{BA}^{i+1})를 생성할 수 있다(S450).

[0056] 이상에서, 각각의 주기에 대응하는 세션키는 각 주기 내에서 생성되는 것으로 설명되었으나, 실시 예에 따라, 각각의 주기에 대응하는 세션키는 이전 주기 동안에 생성될 수도 있다. 예컨대, i+1 번째 주기의 세션키는 i 번째 주기 동안에 생성될 수도 있다.

[0057] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0058] 10 : 키교환 시스템

100 : 서버

110 : 셋업 모듈

130 : 마스터키 업데이트 모듈

150 : 비밀키 생성 모듈

300 : 제1 단말기

310 : 송수신 모듈

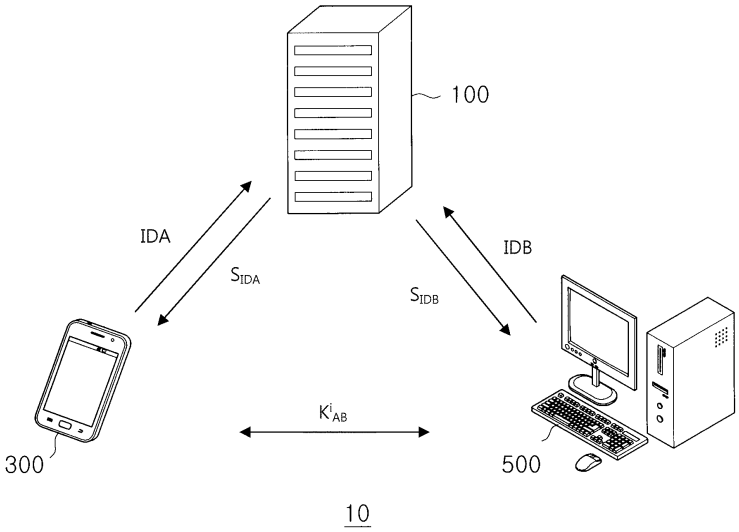
330 : 업데이트 모듈

350 : 키교환 모듈

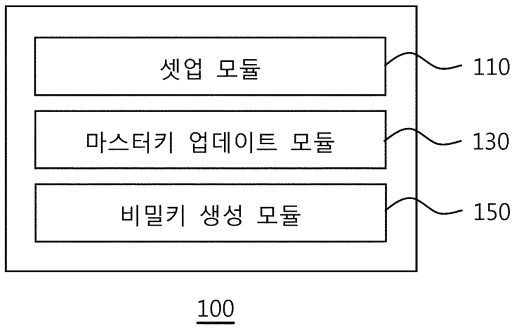
500 : 제2 단말기

도면

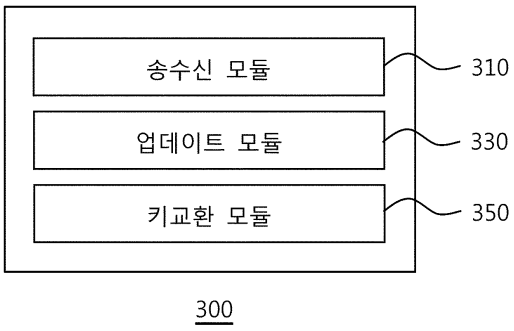
도면1



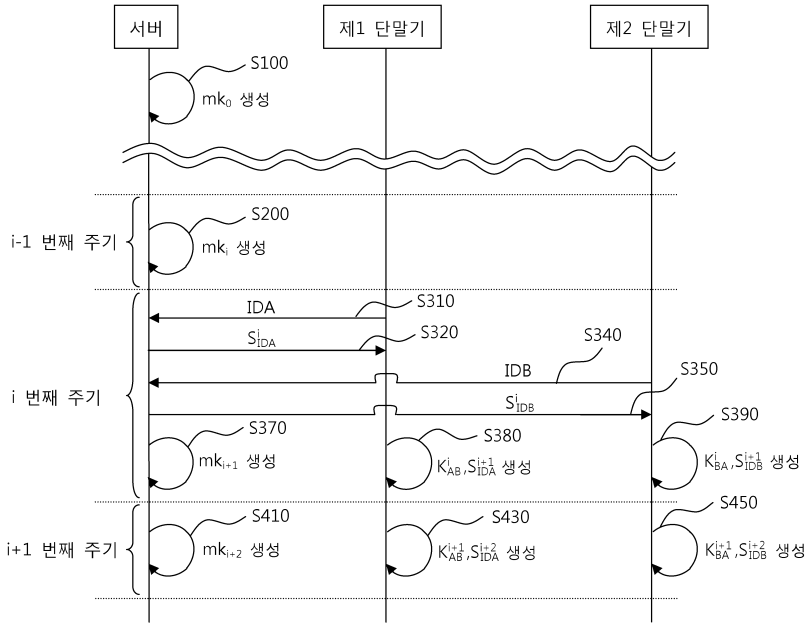
도면2



도면3



도면4


서버
제1 단말기
제2 단말기
S100
mk_0 생성
i-1 번째 주기
S200
mk_i 생성
i 번째 주기
IDA
S310
S^i_{IDA}
S320
S340
IDB
S350
S^i_{IDB}
S390
S370
mk_{i+1} 생성
S380
K^i_{AB}, S^{i+1}_{IDA} 생성
K^i_{BA}, S^{i+1}_{IDB} 생성
i+1 번째 주기
S410
mk_{i+2} 생성
S430
$K^{i+1}_{AB}, S^{i+2}_{IDA}$ 생성
S450
$K^{i+1}_{BA}, S^{i+2}_{IDB}$ 생성