(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0073001
(43) 공개일자 2017년06월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
H04W 12/04 (2009.01) *H04W 12/06* (2009.01)
(52) CPC특허분류
H04L 9/3228 (2013.01)
H04L 9/0819 (2013.01)
(21) 출원번호 10-2015-0181126
(22) 출원일자 2015년12월17일
심사청구일자 2015년12월17일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
정익래
서울특별시 광진구 아차산로 503-23, 103동 1701호 (광장동, 청구아파트)
김동민
서울특별시 동대문구 약령시로 154 1동 505호 (청량리동,미주아파트)
(뒷면에 계속)
(74) 대리인
김등용, 김홍석

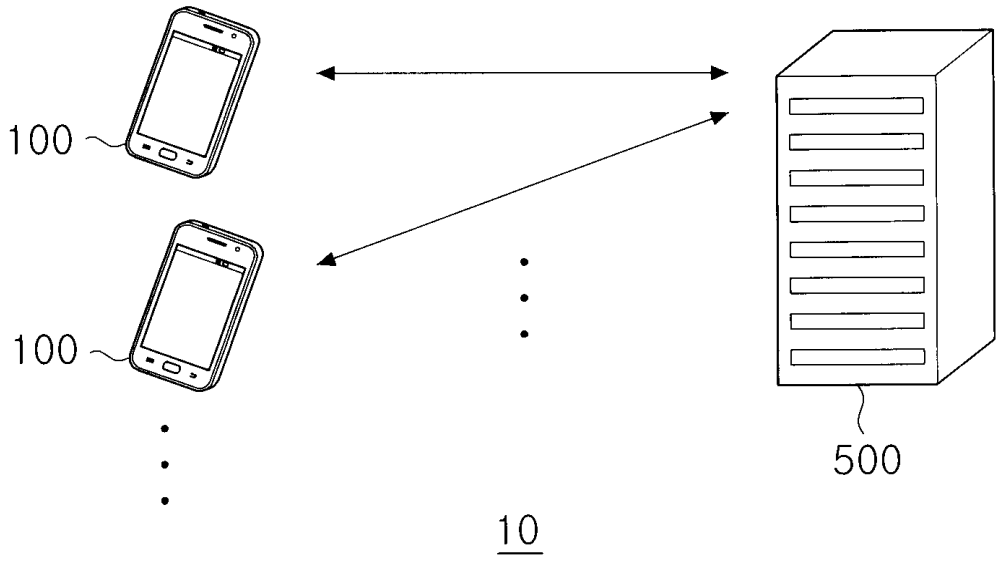
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **인증 및 키 공유 서버, 방법 및 시스템**

(57) 요 약

인증 및 키 공유 방법이 개시된다. 상기 인증 및 키 공유 방법은 서버에서 수행되고, 단말기로부터 등록 요청 메시지를 수신하는 단계, 상기 단말기의 사용자를 등록하는 단계, 상기 단말기로부터 인증 요청 메시지를 수신하는 단계, 상기 사용자를 인증하고 세션 키를 생성하는 단계, 및 상기 단말기로 응답값을 송신하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 9/3271 (2013.01)
H04L 9/3297 (2013.01)
H04W 12/04 (2013.01)
H04W 12/06 (2013.01)
(72) 발명자
백목련
경기도 안양시 동안구 동편로 4단지 405동 1702호

정원석
경기도 안양시 만안구 박달로560번길 46-21 501호 (안양동,초원맨션)

이 발명을 지원한 국가연구개발사업
과제고유번호 H8501151003000 1002
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학ICT연구센터지원사업
연구과제명 제어시스템 보안 기술 개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2015.01.01 ~ 2015.12.31

명 세 서

청구범위

청구항 1

서버에서 수행되는 인증 및 키 공유 방법에 있어서,

단말기로부터 등록 요청 메시지를 수신하는 단계;

상기 단말기의 사용자를 등록하는 단계;

상기 단말기로부터 인증 요청 메시지를 수신하는 단계;

상기 사용자를 인증하고 세션 키를 생성하는 단계; 및

상기 단말기로 응답값을 송신하는 단계를 포함하는,

인증 및 키 공유 방법.

청구항 2

제1항에 있어서,

상기 등록 요청 메시지는 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)를 포함하고,

상기 사용자를 등록하는 단계는,

상기 난수화된 아이디(RID_i), 상기 난수화된 패스워드(RPW_i), 상기 서버의 비밀값(x)을 이용하여 등록값(A_i , B_i)을 생성하는 단계; 및

상기 등록값(A_i , B_i)과 공개 파라미터(P , Y)를 상기 단말기로 송신하는 단계를 포함하는,

인증 및 키 공유 방법.

청구항 3

제2항에 있어서,

상기 인증 요청 메시지는 질의값(EID_i , K_u , V_u , T_1)을 포함하고,

상기 EID_i 는 수학식 1에 의해 정의되고,

상기 수학식 1은 $EID_i = RID_i \oplus h(z_a P)$ 이고,

상기 z_a 는 상기 단말기에 의해 선택된 임의의 난수이고,

상기 K_u 는 수학식 2에 의해 정의되고,

상기 수학식 2는 $K_u = z_a Y$ 이고,

상기 V_u 는 수학식 3에 의해 정의되고,

상기 수학식 3은 $V_u = h(RID_i \| EID_i \| K_u \| h(RID_i \| x) \| T_1)$ 이고,

상기 T_1 은 타임스탬프인,

인증 및 키 공유 방법.

청구항 4

제3항에 있어서,

상기 사용자를 인증하고 세션 키를 생성하는 단계는,

수학식 4를 이용하여 V_u^* 를 생성하는 단계;

상기 V_u^* 와 상기 단말기로부터 수신된 V_u 를 비교하여 상기 사용자를 인증하는 단계; 및

수학식 5를 이용하여 세션 키(SK)를 생성하는 단계를 포함하고,

상기 수학식 4는 $V_u^* = h(RID_i \| EID_i \| K_u \| h(RID_i \| x) \| T_1)$ 이고,

상기 수학식 5는 $SK = h(RID_i \| h(RID_i \| x) \| K_u \| K_s \| K_{su} \| Y)$ 이고,

상기 K_s 는 수학식 6에 의해 정의되고,

상기 수학식 6은 $K_s = z_b Y$ 이고,

상기 z_b 는 상기 서버에 의해 선택된 임의의 난수이고,

상기 K_{su} 는 수학식 7에 의해 정의되고,

상기 수학식 7은 $K_{su} = z_b K_u$ 인,

인증 및 키 공유 방법.

청구항 5

제4항에 있어서,

상기 단말기로 응답값을 송신하는 단계는 상기 응답값(K_s , V_s , T_2)을 생성하는 단계를 포함하고,

상기 V_s 는 수학식 8에 의해 정의되고,

상기 수학식 8은 $V_s = h(SK \| K_s \| T_2)$ 이고,

상기 T_2 는 타임스탬프인,

인증 및 키 공유 방법.

청구항 6

제2항에 있어서,

상기 A_i는 수학식 9에 의해 정의되고,

상기 수학식 9는 $A_i = h(RID_i \| x) \oplus RPW_i$ 이고,

상기 B_i는 수학식 10에 의해 정의되고,

상기 수학식 10은 $B_i = h(h(RID_i \| x) \| RPW_i)$ 인,

인증 및 키 교환 방법.

청구항 7

단말기로부터 등록 요청 메시지를 수신하고, 상기 단말기의 사용자를 등록하는 등록부; 및

상기 단말기로부터 인증 요청 메시지를 수신하고, 상기 사용자를 인증하고 세션 키를 생성하고, 상기 단말기로 응답값을 송신하는 인증부를 포함하는,

인증 및 키 공유 서버.

청구항 8

제7항에 기재된 인증 및 키 공유 서버; 및

상기 단말기를 포함하는,

인증 및 키 공유 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 인증 및 키 공유 서버, 방법 및 시스템에 관한 것으로, 특히 난수화된 아이디와 패스워드를 이용하여 사용자를 등록하고, 질의-응답 과정을 통하여 서버와 단말기가 상호 인증을 수행함과 동시에 세션 키를 공유할 수 있는 인증 및 키 공유 서버, 방법 및 시스템에 관한 것이다.

배 경 기 술

[0003] 최근 클라우드 시스템, 제어 시스템, IoT(Internet of Things), 스마트 카드(smart card) 등 다양한 환경에서 사용자 인증 및 키 공유에 관한 연구가 활발하게 진행되고 있다. 그러나, 대부분의 연구들의 경우 사용자 인증 과정에서 사용자의 ID가 드러난다거나, 통신 값이나 서버에 저장된 값을 통해 사용자의 ID나 패스워드가 추측가능하다는 취약점이 존재한다. 그리고, 전방향 안전성(forward secrecy)을 고려할 경우 안전하지 않는 프로토콜도 존재한다. 본 발명에서는 ID, 패스워드 추측 공격에 안전하고 전방향 안전성을 제공하며, 사용자의 ID가 인증과정에서 드러나지 않는 프로토콜을 제안한다.

[0004] 본 발명의 배경이 되는 기술은 다음과 같다.

[0006] 암호학적 해시함수(hash function)

[0007] 해시함수 h는 임의의 길이의 데이터를 고정된 길이의 데이터로 변환해주는 함수이다. 동일한 입력값에 대해서

는 동일한 출력값을 가지며, 특히 암호학적 해시함수 h는 아래의 세 가지 성질을 만족한다.

[0008] ① 역상 저항성(pre-image resistance) : 주어진 y에 대해서, $y=h(x)$를 만족하는 x를 찾기 어렵다.

[0009] ② 제2 역상 저항성(2nd preimage resistance) : 주어진 x_1에 대해서, $h(x_1)=h(x_2)$를 만족하는 x_2를 찾기 어렵다.

[0010] ③ 충돌 저항성(collision resistance) : $h(x_1)=h(x_2)$를 만족하는 x_1와 x_2를 찾기 어렵다.

[0012] 타원곡선암호(Elliptic curve cryptography)

[0013] 타원곡선 암호는 타원곡선 이론에 기반한 공개 키 암호 방식의 하나로서 RSA(Rivest Shamir Adleman)나 Elgamal보다 짧은 키를 사용하면서도 그와 비슷한 수준의 안전성을 제공한다는 장점을 가지고 있다. 이러한 장점을 바탕으로 무선 환경과 같이 전송량과 연산량이 제약적인 환경에서 주로 사용되고 있다. 타원곡선 암호에서는 주로 타원곡선 이산대수 문제에 기반해서 암호를 설계한다.

[0014] 타원곡선 이산대수 문제: 소수 p에 대해서 $GF(p)$를 p 개의 원소를 가지는 유한체(finite field)라고 하면, 타원곡선 위의 점 P의 위수(order) t는 $tP=O$를 만족하는 가장 작은 정수로 정의된다. $GF(p)$ 상에 정의된 타원곡선, 타원곡선 상에 정의된 점 P, 그리고 임의의 점 Q가 주어졌을 때, $Q=xP$를 만족하는 정수 $x\in[0,t-1]$를 찾는 문제를 타원곡선 이산대수 문제라 하고, 이 문제는 인수분해 문제나 이산대수 문제보다 더 어려운 문제로 인식되고 있다.

[0016] 바이오 해시함수(Biohash)

[0017] 바이오 해시함수 H는 지문과 같은 생체정보를 입력으로 받아 임의의 길이를 출력하는 함수이며, 암호학적 해시함수와 유사한 안전성을 가진다. 같은 사람임에도 불구하고 생체정보는 입력할 때마다 값이 조금씩 다르기 때문에, 정확한 값을 요구하는 일반적인 해시함수나 암호학적 해시함수를 사용할 수가 없다. 바이오 해시함수는 생체정보의 이러한 유사성(fuzzyness)을 해결하기 위한 함수로서, 유사한 입력에 대해서 높은 확률로 동일한 값을 출력해주는 성질을 지닌다.

선행기술문헌

비특허문헌

[0019] (비특허문헌 0001) A.T.B. Jin, D.N.C. Ling, and A. Goh, Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern recognition, 2004.

(비특허문헌 0002) R. Amin and G.P. Biswas, A Secure Three-Factor User Authentication and Key Agreement Protocol for TMIS With User Anonymity, J. Med. Syst., June 2015.

(비특허문헌 0003) R. Amin and G.P. Biswas, An Improved RSA Based User Authentication and Session Key Agreement Protocol Usable in TMIS, J. Med. Syst., June 2015.

(비특허문헌 0004) S.A. Chaudhry, H. Naqvi, T. Shon, M. Sher, and M.S. Farash, Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems, J. Med. Syst., April 2015.

(비특허문헌 0005) H. Arshad, V. Teymoori, M. Nikooghadam, and H. Abbassi, On the Security of a Two-Factor Authentication and Key Agreement Scheme for Telecare Medicine Information Systems, J. Med.

Syst., June 2015.

발명의 내용

해결하려는 과제

[0020] 본 발명이 이루고자 하는 기술적인 과제는 난수화된 아이디와 패스워드를 이용하여 사용자를 등록하고, 질의-응답 과정을 통하여 서버와 단말기가 상호 인증을 수행함과 동시에 세션 키를 공유할 수 있는 인증 및 키 공유 서버, 방법 및 시스템을 제공하는 것이다.

과제의 해결 수단

[0022] 본 발명의 일 실시 예에 따른 인증 및 키 공유 방법은 서버에서 수행되고, 단말기로부터 등록 요청 메시지를 수신하는 단계, 상기 단말기의 사용자를 등록하는 단계, 상기 단말기로부터 인증 요청 메시지를 수신하는 단계, 상기 사용자를 인증하고 세션 키를 생성하는 단계, 및 상기 단말기로 응답값을 송신하는 단계를 포함한다.

[0023] 또한, 본 발명의 일 실시 예에 따른 인증 및 키 공유 서버는 단말기로부터 등록 요청 메시지를 수신하고, 상기 단말기의 사용자를 등록하는 등록부 및 상기 단말기로부터 인증 요청 메시지를 수신하고, 상기 사용자를 인증하고 세션 키를 생성하고, 상기 단말기로 응답값을 송신하는 인증부를 포함한다.

[0024] 또한, 본 발명의 일 실시 예에 따른 인증 및 키 공유 시스템은 상기 인증 및 키 공유 서버 및 상기 단말기를 포함한다.

발명의 효과

[0026] 본 발명의 실시 예에 따른 인증 및 키 공유 서버, 방법 및 시스템에 의할 경우, ID, 패스워트 추측 공격에 안전하고 전방향 안전성을 만족하는 다중 인증 및 키 공유 프로토콜 설계가 가능하며, 인증 과정에서 사용자의 ID가 노출되지 않도록 함으로써 사용자의 프라이버시를 보호할 수 있는 효과가 있다.

도면의 간단한 설명

[0028] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 인증 및 키 공유 시스템을 도시한다.

도 2는 도 1에 도시된 단말기의 기능 블럭도이다.

도 3은 도 1에 도시된 서버의 기능 블럭도이다.

도 4는 도 1에 도시된 인증 및 키 공유 시스템에서 수행되는 인증 및 키 공유 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 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.

[0030] 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.

[0031] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어

들에 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.

[0032] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 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.

[0033] 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.

[0034] 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.

[0036] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다. 우선, 본 발명에서는 사용자와 서버를 포함하는 2명의 파티를 가정한다. 상기 서버에 사용자를 등록하기 위해 난수화된 ID와 패스워드를 전송하는 단계, 서버가 사용자를 등록하고 등록된 값을 전송하는 단계, 사용자가 ID, 패스워드, 생체정보를 입력하고 서버에 인증받기 위해 값을 생성하고 전송하는 단계, 서버가 사용자를 인증하고 세션키를 생성하는 단계, 사용자가 서버를 인증하고 세션키를 인증하는 단계, 총 5단계로 이루어진다. 최초 2단계는 서버에 사용자를 등록하는 단계로써, 안전한 채널을 이용한 통신을 가정한다.

[0037] 또한, 본 명세서에서 $h(\bullet):\{0,1\}^{*}\rightarrow\{0,1\}^{n}$ 를 암호학적 해시함수, $H(\bullet):\{0,1\}^{*}\times\{0,1\}^{k}\rightarrow\{0,1\}^{n}$ 를 바이오 해시함수라고 하자. 여기서 n은 해시함수 출력값의 길이, k는 바이오 해시함수에서 사용하는 랜덤 토큰(random token)의 길이를 의미한다. 그리고 $\oplus$은 비트별 XOR(Exclusive OR ; 배타적 논리합)을 의미한다. P는 타원곡선 암호에서 사용되는 타원곡선 상의 점, x는 서버의 비밀값, 그리고 $Y=xP$는 서버의 공개값을 의미한다.

[0039] 도 1은 본 발명의 일 실시 예에 따른 인증 및 키 공유 시스템을 도시한다.

[0040] 인증 시스템, 다중 인증 및 키 공유 시스템 등으로 불릴 수도 있는 인증 및 키 공유 시스템(10)은 적어도 하나의 단말기(100)와 서버(300)를 포함한다.

[0041] 단말기(100)는 등록 요청 메시지를 서버(300)로 송신하고, 서버(300)는 상기 등록 요청 메시지에 응답하여, 단말기(100)의 사용자를 등록한다.

[0042] 또한, 서버(300)는 단말기(100)의 인증 요청에 응답하여, 단말기(100) 또는 사용자를 인증하고, 응답값을 단말기(100)로 송신하며, 단말기(100)는 상기 응답값을 이용하여 서버(300)를 인증함으로써, 상호 인증을 완료할 수 있으며, 안전하게 세션 키를 공유할 수 있다.

[0043] 단말기(100)는 PC(personal computer), 태블릿 PC, 노트북(notebook), 넷-북(net-book), e-리더(e-reader), PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 또는 MP4 플레이어와 같

은 데이터 처리 장치로 구현되거나, 모바일폰(mobile phone), 스마트폰(smart phone) 등과 같은 핸드헬드 장치(handheld device)로 구현될 수 있다.

[0044] 서버(300)와 단말기(100)의 구체적인 구성 및 동작에 관하여는 도 2와 도 3을 통하여 상세하게 설명하기로 한다.

[0046] 도 2는 도 1에 도시된 단말기의 기능 블럭도이다. 도 2에 도시된 단말기(100)는 인증 및 키 공유 시스템(10)에 포함된 i 번째 사용자(u_i)의 단말기임을 가정한다.

[0047] 도 1과 도 2를 참조하면, 단말기(100)는 등록 요청부(110), 인증 요청부(130), 및 인증부(150)을 포함한다.

[0048] 등록 요청부(110)는 사용자 등록을 위한 등록 요청 메시지를 서버(300)로 송신한다. 상기 등록 요청 메시지는 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)를 포함할 수 있다. 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)를 생성하기 위해 등록 요청부(110)는 다음과 같은 과정을 수행한다.

[0049] 우선, 등록 요청부(110)는 임의의 난수들(r_{i0}, r_{i1})를 선택(또는 생성)한다.

[0050] 이후, 등록 요청부(110)는 아래와 같이 선택된 임의의 난수들(r_{i0}, r_{i1}), 아이디(ID_i), 및 패스워드(PW_i)를 입력으로 하는 암호학적 해시함수를 이용하여 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)를 생성할 수 있다.

[0051] $$RPW_i = h(PW_i \| r_{i0}),\ RID_i = h(ID_i \| r_{i1})$$

[0052] 상술한 바와 같이, 아이디(ID_i)와 패스워드(PW_i)를 직접 송신하는 경우에 발생할 수 있는 개인 정보 누출의 위험이 제거될 수 있다. 선택된 임의의 난수들(r_{i0}, r_{i1})은 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)가 생성된 후 단말기(100) 내에서 삭제될 수 있다.

[0053] 또한, 등록 요청부(110)는 서버(300)로부터 등록값(A_i, B_i)과 공개 파라미터(P, Y)를 수신하고, 아래와 같이 등록값(A_i, B_i), 공개 파라미터(P, Y), 및 사용자(u_i)의 생체정보(BIO)를 이용하여 계산값(F_{i0}, F_{i1})을 생성할 수 있다. 생체정보(BIO)의 일 예로 지문 정보, 홍채 정보 등이 될 수 있다.

[0054] $$F_{i0} = r_{i0} \oplus H(BIO \| 0)$$

[0055] $$F_{i1} = r_{i1} \oplus H(BIO \| 1)$$

[0056] 서버(300)로부터 수신된 등록값(A_i, B_i), 공개 파라미터(P, Y), 생성된 계산값(F_{i0}, F_{i1}), 암호학적 해시함수($h(\cdot)$), 및 바이오 해시함수($H(\cdot)$)는 등록 요청부(110)에 의해 단말기(100) 내에 포함될 수 있는 소정의 저장 수단에 저장될 수 있다.

[0058] 서버(300)와 통신을 위해 인증이 필요한 경우, 단말기(100)의 인증 요청부(130)는 아이디(ID_i), 패스워드(PW_i), 생체 정보(BIO), 및 단말기(100) 내에 저장된 값(A_i, F_{i0}, F_{i1}, Y, P, $h(\cdot)$, 및 $H(\cdot)$)을 이용하여 다음과 같은 연산을 수행한다.

[0059] 우선, 인증 요청부(130)는 아래 수학식을 이용하여 사용자 등록 단계에서 선택한 난수(r_{i0}, r_{i1})를 생성(또는

계산)한다.

[0060] $$F_{i0} \oplus H(BIO \| 0) = r_{i0}$$

[0061] $$F_{i1} \oplus H(BIO \| 1) = r_{i1}$$

[0062] 또한, 인증 요청부(130)는 아래 수학식을 이용하여 사용자 등록 단계에서 생성된 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)를 생성(또는 계산)한다.

[0063] $$RPW_i = h(PW_i \| r_{i0})$$

[0064] $$RID_i = h(ID_i \| r_{i1})$$

[0065] 또한, 인증 요청부(130)는 아래 수학식을 이용하여 $h(RID_i \| x)$ 를 계산한다.

[0066] $$RPW_i \oplus A_i = h(RID_i \| x)$$

[0067] 또한, 인증 요청부(130)는 아래 수학식을 이용하여 $B_i^{'}$ 를 계산하고, 계산된 $B_i^{'}$ 와 단말기(100) 내에 저장되어 있는 B_i 가 상이한 경우 프로토콜을 중단한다.

[0068] $$B_i^{'} = h(h(RID_i \| x) \| RPW_i)$$

[0069] 또한, 인증 요청부(130)는 아래 수학식을 이용하여 EID_i 를 계산한다.

[0070] $$EID_i = RID_i \oplus h(z_a P)$$

[0071] 여기서, z_a 는 단말기(100)의 인증 요청부(130)에 의해 선택된 임의의 난수일 수 있다.

[0072] 또한, 인증 요청부(130)는 아래 수학식과 같이 난수(z_a)와 공개 파라미터(Y)를 이용하여 K_u 를 계산한다.

[0073] $$K_u = z_a Y$$

[0074] 또한, 인증 요청부(130)는 아래 수학식을 이용하여 V_u 를 계산한다.

[0075] $$V_u = h(RID_i \| EID_i \| K_u \| h(RID_i \| x) \| T_1)$$

[0076] 여기서, T_1 은 현재의 타임스탬프일 수 있다.

[0077] 인증 요청부(130)는 상술한 과정을 통하여 생성된 값(EID_i , K_u , V_u , T_1)을 포함하는 인증 요청 메시지를 서버(300)로 송신할 수 있다. 상기 생성된 값(EID_i , K_u , V_u , T_1)은 질의값이라 명명될 수 있다.

[0079] 단말기(100)의 인증부(150)는 서버(300)로부터 응답값(K_s , V_s , T_2)를 수신하고, 수신된 응답값(K_s , V_s , T_2)과 단말기(100) 내에 저장되어 있는 값들을 이용하여 아래와 같이 V_s^* 를 계산한다.

[0080] $$K_{su} = z_a K_s$$

[0081] $$SK = h(RID_i \| h(RID_i \| x) \| K_u \| K_s \| K_{su} \| Y)$$

[0082] $$V_s^* = h(SK \| K_s \| T_2)$$

[0083] 인증부(150)는 서버(300)로부터 수신된 V_s와 생성된 V_s^*가 상이한 경우 프로토콜을 중단하고, 동일한 경우 서버(300)를 인증하고, 생성된 SK를 세션 키로 사용한다.

[0085] 도 3은 도 1에 도시된 서버의 기능 블럭도이다.

[0086] 도 1 내지 도 3을 참조하면, 인증 서버, 키 공유 서버, 또는 인증 및 키 공유 서버 등으로 명명될 수 있는 서버(300)는 등록부(310)와 인증부(330)를 포함한다.

[0088] 등록부(310)는 단말기(100)의 등록 요청부(110)로부터 등록 요청 메시지를 수신하고, 사용자 등록을 수행할 수 있다.

[0089] 구체적으로 등록부(310)는 아래와 같이 단말기(100)로부터 수신된 난수화된 아이디(RID_i), 난수화된 패스워드(RPW_i), 및 미리 설정된 서버(300)의 비밀값(x)을 이용하여 등록값(A_i, B_i)을 생성한다.

[0090] $$F_{i0} = r_{i0} \oplus H(BIO \| 0)$$

[0091] $$F_{i1} = r_{i1} \oplus H(BIO \| 1)$$

[0092] 또한, 등록부(310)는 생성된 등록값(A_i, B_i)과 공개 파라미터(P, Y)를 단말기(100)로 송신한다. 여기서, 공개 파라미터(P, Y)는 타원곡선암호에서 사용되는 공개 파라미터일 수 있다.

[0094] 인증부(330)는 단말기(100)로부터 수신된 인증 요청 메시지 또는 질의값(EID_i, K_u, V_u, T_1)과 자신의 비밀값(x)을 이용하여 다음과 같이 계산한다.

[0095] $$x^{-1} K_u = z_a P$$

[0096] $$EID_i \oplus h(z_a P) = RID_i$$

[0097] $$V_u^* = h(RID_i \| EID_i \| K_u \| h(RID_i \| x) \| T_1)$$

[0098] 인증부(330)는 상기와 같은 수학식을 이용하여 생성된 V_u^*와 단말기(100)로부터 수신된 V_u의 동일 여부에 따라, 사용자 인증을 수행한다. 즉, 인증부(330)는 V_u^*와 V_u이 상이한 경우 프로토콜을 중단하고, 동일한 경우에는 정당한 사용자임을 인증한다. 또한, 인증부(330)는 사용자 인증이 완료된 경우 응답값(K_s, V_s, T_2)을 아래와 같이 계산(또는 생성)한 뒤 단말기(100)로 송신한다.

[0099] $$K_s = z_b Y$$

[0100] $$K_{su} = z_b K_u$$

[0101] $$SK = h(RID_i \| h(RID_i \| x) \| K_u \| K_s \| K_{su} \| Y)$$

[0102] $$V_s = h(SK \| K_s \| T_2)$$

[0103] 상기 수학식에서 z_b는 서버(300) 또는 인증부(330)에 의해 선택된 임의의 난수일 수 있으며, T_2는 현재의 타임스탬프일 수 있다. 또한, SK는 서버(300)와 단말기(100) 사이의 통신에 이용되는 세션 키를 의미할 수 있다.

[0105] 도 2와 도 3에 도시된 단말기(100)와 서버(300)의 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.

[0106] 또한, 본 명세서에서 "~부"라 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.

[0108] 도 4는 도 1에 도시된 인증 및 키 공유 시스템에서 수행되는 인증 및 키 공유 방법을 설명하기 위한 흐름도이다. 상기 인증 및 키 공유 방법을 설명함에 있어 상술된 내용과 중복되는 내용에 관하여는 구체적인 기술을 생략하기로 한다.

[0109] 도 1 내지 도 4를 참조하면, 단말기(100)의 등록 요청부(110)는 사용자 등록을 위하여 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)를 생성하고(S100), 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)를 서버(300)로 송신한다(S200).

[0110] 난수화된 아이디(RID_i)와 난수화된 패스워드(RPW_i)를 수신한 서버(300)의 등록부(310)는 사용자 등록을 위한 등록값(A_i, B_i)을 생성하고(S300), 생성된 등록값(A_i, B_i)과 공개 파라미터(P, Y)를 단말기(100)로 송신할 수 있다(S400). 이때, 생성된 등록값(A_i, B_i) 등록부(310)에 의해 서버(300) 내의 소정의 저장 공간에 저장될 수 있다.

[0111] 서버(300)로부터 등록값(A_i, B_i)과 공개 파라미터(P, Y)를 수신한 등록 요청부(110)는 계산값(F_{i0}, F_{i1})을 생성하고, 등록값(A_i, B_i), 계산값(F_{i0}, F_{i1}), 공개 파라미터(P, Y), 암호학적 해시함수($h(\bullet)$), 및 바이오 해시함수($H(\bullet)$)를 단말기(100) 내의 저장 공간에 저장할 수 있다(S500).

[0112] 서버(300)와의 통신을 위해 인증이 필요한 경우, 단말기(100)의 인증 요청부(130)는 사용자 인증을 위한 질의값(EID_i, K_u, V_u, T_1)을 생성하고 생성된 질의값(EID_i, K_u, V_u, T_1)을 서버(300)로 송신할 수 있다(S600).

[0113] 서버(300)의 인증부(330)는 수신된 질의값(EID_i, K_u, V_u, T_1)을 이용하여 단말기(100)의 사용자를 인증하고(S700), 상기 질의값(EID_i, K_u, V_u, T_1)에 대응하는 응답값(K_s, V_s, T_2)을 생성하여 단말기(100)로 송신한다(S800).

[0114] 단말기(100)의 인증부(150)는 서버(300)로부터 수신된 응답값(K_s, V_s, T_2)을 이용하여 서버(300)를 인증할 수 있다(S900).

[0115] 상술한 과정을 통하여, 서버(300)와 단말기(100)는 동일한 세션 키(SK)를 공유할 수 있으며, 본 발명은 클라우드 시스템, 제어 시스템, 스마트 카드 등 다양한 환경에 적용 가능하다.

[0117] 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

[0118] 10 : 인증 및 키 공유 시스템

100 : 단말기

110 : 등록 요청부

130 : 인증 요청부

150 : 인증부

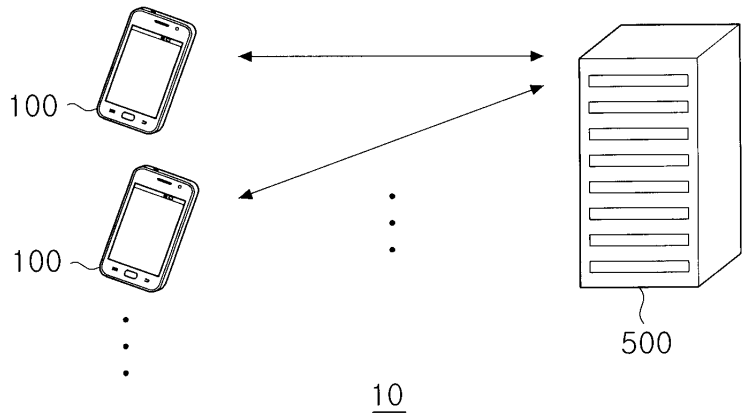
300 : 서버

310 : 등록부

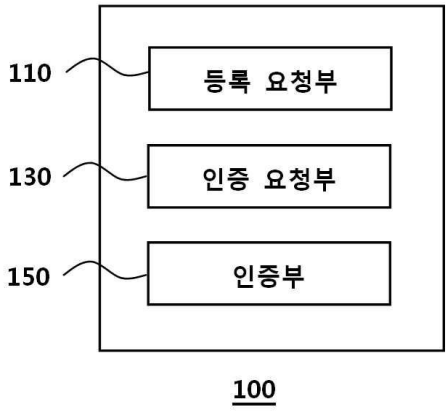
330 : 인증부

도면

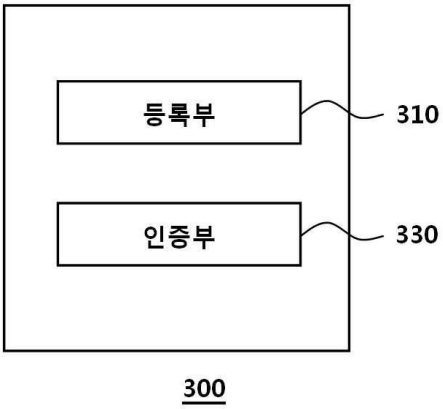
도면1



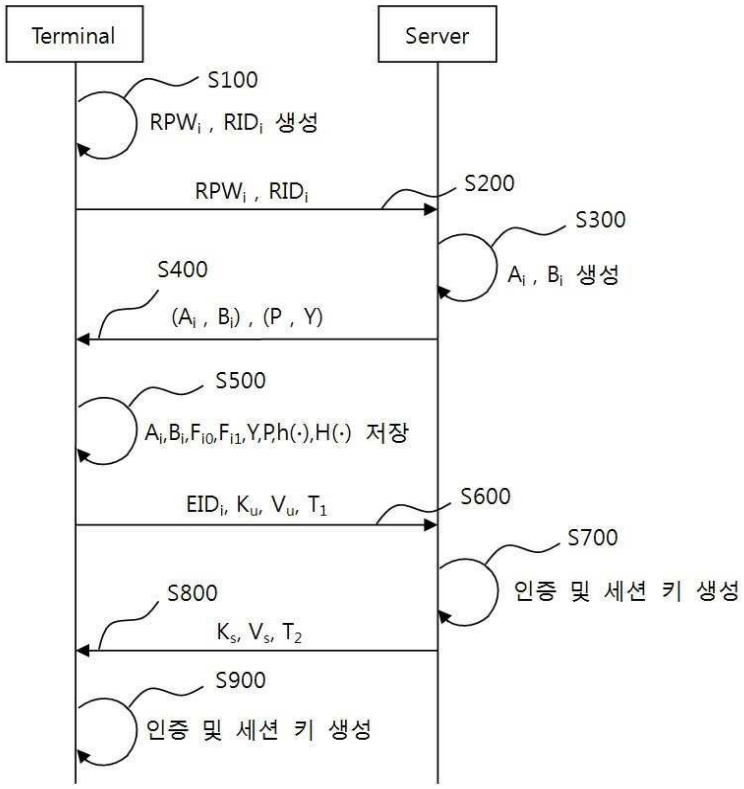
도면2



도면3



도면4


Terminal
Server
S100
RPW$_i$, RID$_i$ 생성
RPW$_i$, RID$_i$
S200
S300
A$_i$, B$_i$ 생성
S400
(A$_i$, B$_i$) , (P , Y)
S500
A$_i$,B$_i$,F$_{i0}$,F$_{i1}$,Y,P,h(·),H(·) 저장
EID$_i$, K$_u$, V$_u$, T$_1$
S600
S700
인증 및 세션 키 생성
S800
K$_s$, V$_s$, T$_2$
S900
인증 및 세션 키 생성