



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0074576
(43) 공개일자 2009년07월07일

(51) Int. Cl.

H04L 9/32 (2006.01) H04L 9/08 (2006.01)
G06K 19/07 (2006.01)

(21) 출원번호 10-2008-0000399
(22) 출원일자 2008년01월02일
심사청구일자 2008년01월02일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

김용훈

서울 종로구 익선동 비즈웰오피스텔 526호

윤택영

경기 성남시 중원구 성남동 3020번지

(뒷면에 계속)

(74) 대리인

현중철

전체 청구항 수 : 총 20 항

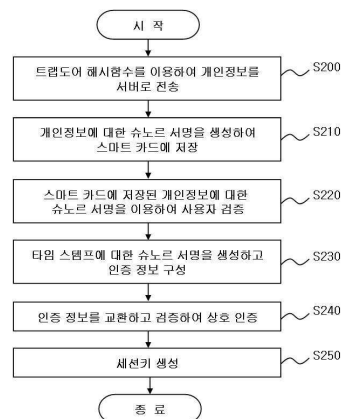
(54) 스마트카드 기반의 3자간 키 교환 방법 및 시스템과 이에사용되는 스마트카드 및 마이크로프로세서

(57) 요약

본 발명은 스마트카드를 사용하여 서버의 개입 없이 안전한 키 교환을 수행하기 위한 3자간 키 교환 방법 및 시스템과 이에 사용되는 스마트카드 및 마이크로프로세서에 관한 것이다.

본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법은 사용자 단말기에서 트랩도어 해시함수에 의해 변환된 개인정보를 포함하는 사용자 개인정보 및 서버의 비밀키를 통해, 서버에서 사용자 개인정보에 대한 슈노르(schnorr) 서명을 생성하고, 상기 개인정보에 대한 슈노르 서명을 포함하는 등록정보를 스마트카드에 저장하는 사용자 등록 단계; 상기 스마트카드와 인터페이싱(interfacing)할 수 있는 단말기를 통해 사용자의 개인정보가 입력되면, 상기 스마트카드에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 상기 사용자 등록 단계에 의한 등록 사용자인지를 검증하는 사용자 검증 단계; 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계; 네트워크를 통해 등록 사용자 간에 인증정보를 교환하고 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및 상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 포함한다.

대표도 - 도2



(72) 발명자

박영호

서울 마포구 성산2동 월드타운 대림아파트
104-2101

김창한

서울 강남구 대치동 은마아파트 21동 507호

홍석희

서울 은평구 응암2동 451-12번지 202호

특허청구의 범위

청구항 1

스마트카드를 기반으로 3자간 키 교환을 수행하는 방법에 있어서,

사용자 단말기에서 트랩도어 해시함수에 의해 변환된 개인정보를 포함하는 사용자 개인정보 및 서버의 비밀키를 통해, 서버에서 사용자 개인정보에 대한 슈노르(schnorr) 서명을 생성하고, 상기 개인정보에 대한 슈노르 서명을 포함하는 등록정보를 스마트카드에 저장하는 사용자 등록 단계;

상기 스마트카드와 인터페이싱(interfacing)할 수 있는 단말기를 통해 사용자의 개인정보가 입력되면, 상기 스마트카드에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 상기 사용자 등록 단계에 의한 등록 사용자인지를 검증하는 사용자 검증 단계;

등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계;

네트워크를 통해 등록 사용자 간에 인증정보를 교환하고 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및

상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 포함하는 스마트카드 기반의 3자간 키 교환 방법.

청구항 2

제1항에 있어서,

상기 사용자 등록 단계는, 상기 사용자 단말기에서 임의의 제1 난수를 이용하여 상기 트랩도어 해시함수로 변환된 개인정보를 생성하는 단계;

상기 사용자 단말기에서 네트워크를 통해 상기 트랩도어 해시함수에 의해 변환된 개인정보를 포함하는 사용자 개인정보를 상기 서버로 전송하는 단계; 및

상기 서버에서 임의의 제2 난수를 이용하여 상기 개인정보에 대한 슈노르 서명을 생성하고, 상기 개인정보에 대한 슈노르 서명을 포함하는 상기 등록정보를 상기 스마트카드에 저장하는 단계를 포함하는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법.

청구항 3

제2항에 있어서,

상기 사용자 등록 단계는, 상기 스마트카드와 인터페이싱할 수 있는 단말기를 통해 상기 제1 난수, 상기 트랩도어 해시함수의 해시값을 계산하기 위한 해시키, 및 상기 해시값의 중동쌍을 찾기 위한 트랩도어 키를 상기 스마트카드에 저장하는 단계를 더 포함하는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법.

청구항 4

제3항에 있어서,

상기 트랩도어 해시함수로 변환된 개인정보는, 패스워드(PW)를 트랩도어 해시함수로 변환한 개인정보인 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법.

청구항 5

제4항에 있어서,

상기 사용자 개인정보는 사용자 아이디(ID)를 포함하고, 그리고 상기 개인정보에 대한 슈노르 서명은 상기 사용자 아이디(ID)에 대한 슈노르 서명인 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법.

청구항 6

제5항에 있어서,

상기 등록정보는, 유한 순환 곱셈군의 생성자로서 상기 제2 난수를 승수로 하는 상기 생성자 및 상기 서버의 공개키를 포함하는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법.

청구항 7

제6항에 있어서,

상기 사용자 검증 단계에서 입력되는 상기 개인정보는 아이디 및 패스워드를 포함하고, 그리고 상기 사용자 검증 단계는 입력된 아이디 및 패스워드가 상기 사용자 등록 단계에서 사용된 상기 사용자 아이디(ID) 및 패스워드(PW)와 동일한지를 검증하는 단계인 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법.

청구항 8

제7항에 있어서,

상기 사용자 검증 단계는, 상기 개인정보에 대한 슈노르 서명(ω , t)이 하기 수학식 1과 같이 표현될 때, 하기 수학식 2에 나타난 등식이 성립하면 상기 입력된 패스워드와 상기 사용자 등록 단계에서 사용된 상기 패스워드가 동일한 것으로 검증하는 단계인 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법:

<수학식 1>

$$\begin{aligned} w &= g^{H_{HK}(PW,n)} g^s, \\ t &= H_{HK}(PW,n) + s + xH(ID,w) \end{aligned}$$

<수학식 2>

$$g^{H_{HK}(PW,n)} g^s = g^{H_{HK}(PW_{input},n)} g^s$$

상기 수학식 1 및 상기 수학식 2에서, g 는 유한 순환 곱셈군의 생성자, $H_{HK}()$ 는 트랩도어 해시함수, PW 는 상기 사용자 등록 단계에서 사용된 상기 패스워드, n 은 상기 제1 난수, s 는 상기 제2 난수, x 는 상기 서버의 비밀키, $H()$ 는 해시함수, ID 는 상기 사용자 아이디, 그리고 PW_{input} 는 상기 입력된 패스워드를 나타낸다.

청구항 9

제8항에 있어서,

상기 인증정보 구성 단계에서 생성되는 상기 타임스탬프에 대한 슈노르 서명(R , A)은, 상기 스마트카드에서 임의의 제3 난수를 이용하여 생성되며 하기 수학식 3과 같이 표현되는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법:

<수학식 3>

$$\begin{aligned} R &= g^r, \\ A &= r + tH(T,R) \end{aligned}$$

상기 수학식 3에서, r 은 상기 제3 난수, t 는 상기 개인정보에 대한 슈노르 서명, $H()$ 는 해시함수, 그리고 T 는 타임스탬프를 나타낸다.

청구항 10

제9항에 있어서,

상기 인증정보 구성 단계에서 구성되는 상기 인증정보는 상기 개인정보에 대한 슈노르 서명(ω), 상기 타임스탬프(T), 및 상기 사용자 아이디(ID)를 포함하는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법.

청구항 11

제10항에 있어서,

상기 상호 인증 단계는, 키 교환의 상대방 사용자로부터 전송받은 상기 인증정보를 이용하여 하기 수학식 4에

나타난 등식이 성립하는 경우 상기 상대방 사용자를 인증하는 단계인 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법:

<수학식 4>

$$R_2(w_2y^{H(ID_2, w_2)})^{H(T_2, R_2)} = g^{A_2}$$

상기 수학식 4에서, 아래첨자 2는 상대방 사용자로부터 전송받은 인증정보임을 나타내고, 그리고 y 는 상기 서버의 상기 공개키를 나타낸다.

청구항 12

제11항에 있어서,

상기 키 교환 단계에서 생성되는 상기 세션키(key)는, 하기 수학식 5에 의해 생성되는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법:

<수학식 5>

$$key = H(R_2^r) = H(g^{rr_2})^{\frac{1}{r_2}}$$

상기 수학식 5에서, R_2 는 상기 상대방 사용자의 상기 타임스탬프에 대한 슈노르 서명(R), r_2 는 상기 상대방 사용자의 상기 제3 난수를 나타낸다.

청구항 13

제8항에 있어서,

상기 사용자 검증 단계에 의해 상기 사용자가 등록 사용자임이 검증된 후에 상기 패스워드(PW)를 변경하여 키 교환을 수행하는 경우, 상기 스마트카드와 인터페이싱할 수 있는 상기 단말기를 통해 새로운 패스워드(PW_{new})를 입력하고 하기 수학식 6을 만족하는 새로운 난수(n_{new})를 상기 제1 난수(n)로서 상기 스마트 카드에 저장하는 패스워드 변경 단계를 더 포함하는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 방법:

<수학식 6>

$$H_{HK}(PW, n) = H_{HK}(PW_{new}, n_{new})$$

상기 수학식 6에서, $H_{HK}()$ 는 트랩도어 해시함수, n 은 상기 제1 난수, PW 는 상기 패스워드(PW), PW_{new} 는 새로운 패스워드, 그리고 n_{new} 는 새로운 난수를 나타낸다.

청구항 14

스마트카드의 제어, 데이터 처리 및 연산을 수행하는 마이크로프로세서 및 데이터를 저장하는 기억장치를 포함하는 스마트카드를 기반으로 3자간 키 교환을 수행하는 시스템에 있어서,

상기 스마트카드 기반의 3자간 키 교환 시스템은, 임의의 제1 난수를 이용하여 트랩도어 해시함수에 의해 변환된 개인정보를 생성하고, 네트워크를 통해 상기 트랩도어 해시함수에 의해 변환된 개인정보를 포함하는 사용자 개인정보를 서버로 전송하는 사용자 단말기;

임의의 제2 난수, 상기 사용자 개인정보, 및 비밀키를 이용하여 사용자 개인정보에 대한 슈노르 서명을 생성하고, 상기 개인정보에 대한 슈노르 서명을 포함하는 등록정보를 상기 스마트카드의 상기 기억장치에 저장함으로써 사용자 등록을 수행하는 상기 서버; 및

상기 스마트카드와 인터페이싱(interfacing)할 수 있는 단말기로서 상기 스마트카드에 데이터를 입력할 수 있는 상기 단말기를 포함하고,

상기 스마트카드의 상기 마이크로프로세서는, 상기 스마트카드와 인터페이싱(interfacing)할 수 있는 상기 단말기를 통해 사용자의 개인정보가 입력되면 상기 스마트카드의 상기 기억장치에 저장된 상기 개인정보에 대한 슈

노르 서명을 이용하여 상기 사용자가 등록 사용자인지를 검증하는 사용자 검증 단계;

상기 사용자가 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고, 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계;

네트워크를 통해 등록 사용자 간에 인증정보를 교환하고, 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및

상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 실행시키는 스마트카드 기반의 3자간 키 교환 시스템.

청구항 15

제14항에 있어서,

상기 사용자 단말기가 생성하는 상기 트랩도어 해시함수로 변환된 개인정보는, 패스워드(PW)를 트랩도어 해시함수로 변환한 개인정보인 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 시스템.

청구항 16

제15항에 있어서,

상기 사용자 단말기가 상기 서버로 전송하는 상기 사용자 개인정보는 사용자 아이디(ID)를 포함하고, 그리고 상기 서버가 생성하는 상기 개인정보에 대한 슈노르 서명은 상기 사용자 아이디(ID)에 대한 슈노르 서명인 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 시스템.

청구항 17

제16항에 있어서,

상기 스마트카드와 인터페이싱 할 수 있는 상기 단말기를 통해 입력되는 사용자의 개인정보는 아이디 및 패스워드를 포함하고, 그리고 상기 마스터카드의 상기 마이크로프로세서는 상기 사용자 검증 단계에서 상기 입력된 아이디 및 패스워드가 상기 서버에 의한 사용자 등록시 사용된 상기 사용자 아이디(ID) 및 패스워드(PW)와 동일한지를 검증하는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 시스템.

청구항 18

제17항에 있어서,

상기 마스터카드의 상기 마이크로프로세서는, 상기 사용자 검증 단계에 의해 상기 사용자가 등록 사용자임이 검증된 후에 상기 패스워드(PW)를 변경하여 키 교환을 수행하는 경우, 상기 스마트카드와 인터페이싱할 수 있는 상기 단말기를 통해 새로운 패스워드(PW_{new})를 입력받아 상기 새로운 패스워드를 상기 패스워드(PW)로서 상기 마스터카드의 상기 기억장치에 저장하는 패스워드 변경 단계를 더 수행하는 것을 특징으로 하는 스마트카드 기반의 3자간 키 교환 시스템.

청구항 19

제14항 내지 제18항 중 어느 한 항에 따른 스마트카드 기반의 3자간 키 교환 시스템에 사용되는 스마트카드에 있어서,

상기 스마트카드는, 상기 스마트카드의 제어, 데이터 처리 및 연산을 수행하는 마이크로프로세서; 및

상기 서버에 의해 생성되는 상기 개인정보에 대한 슈노르 서명을 포함하는 데이터를 저장하는 기억장치를 포함하고,

상기 스마트카드의 상기 마이크로프로세서는, 상기 스마트카드와 인터페이싱할 수 있는 상기 단말기를 통해 사용자의 개인정보가 입력되면 상기 스마트카드의 상기 기억장치에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 등록 사용자인지를 검증하는 사용자 검증 단계;

상기 사용자가 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고, 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계;

네트워크를 통해 등록 사용자 간에 인증정보를 교환하고, 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및

상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 실행시키는 스마트카드.

청구항 20

제14항 내지 제18항 중 어느 한 항에 따른 스마트카드 기반의 3자간 키 교환 시스템에 사용되는 스마트카드를 제어하고, 데이터 처리 및 연산을 수행하는 마이크로프로세서에 있어서,

상기 스마트카드는, 상기 서버에 의해 생성된 상기 개인정보에 대한 슈노르 서명을 포함하는 데이터를 저장하는 기억장치를 포함하고,

상기 마이크로프로세서는, 상기 스마트카드와 인터페이싱할 수 있는 상기 단말기를 통해 사용자의 개인정보가 입력되면 상기 스마트카드의 상기 기억장치에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 등록 사용자임을 검증하는 사용자 검증 단계;

상기 사용자가 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고, 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계;

네트워크를 통해 등록 사용자 간에 인증정보를 교환하고, 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및

상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 실행시키는 마이크로프로세서.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 스마트카드를 기반으로 3자간 키 교환을 수행하는 방법 및 시스템과 이에 사용되는 스마트카드 및 마이크로프로세서에 관한 것이며, 더 상세하게는 스마트카드를 사용하여 서버의 개입 없이 안전한 키 교환을 수행하기 위한 3자간 키 교환 방법 및 시스템과 이에 사용되는 스마트카드 및 마이크로프로세서에 관한 것이다.

배경 기술

- <2> 키 교환 프로토콜(key exchange protocol)은 안전한 통신을 위한 중요한 기술 중 하나로서 안전하지 않은 채널에서 키를 공유하기 위한 암호학적 도구이다. 키 교환 프로토콜은 1976년 Diffie와 Hellman(W.Diffie, M.E.Hellman, "New directions in cryptography", IEEE Trans., vol.IT-22, no.6, pp.644-654, 1976.)에 의해 처음으로 제시되었다. 그러나 Diffie와 Hellman이 제시한 방법은 상대방에 대한 인증이 고려되지 않았기 때문에 많은 약점이 발견되었다. 그 후 사용자 인증을 제공하는 키 교환 프로토콜에 대한 많은 연구가 진행되었다. 키 교환 프로토콜에서 사용자 인증을 위한 방법은 다음과 같이 크게 3가지로 분류할 수 있다. 공개 키 암호 시스템을 이용하는 방법, 사전에 공유된 키를 사용하여 대칭키 암호 시스템을 이용하는 방법, 및 패스워드를 사용하는 방법이 있다. 공개키 암호 시스템을 이용하는 방법은 신뢰할 수 있는 기관인 인증서 발급 기관이 발급한 인증서로써 상호 간의 인증을 수행한 후 인증받은 공개키를 기반으로 키를 설정하는 방법이다. 대칭키 암호 시스템을 이용하는 방법은 프로토콜 수행 전에 상호 간에 공유된 키를 사용해 사용자 인증과 키 설정을 하는 방법이다. 암호 시스템에서 사용할 수 있는 키는 보통 길이가 긴 난수이므로 사람이 기억하기 힘들다. 따라서, 두 방법 모두 사용자는 암호 시스템용 키를 저장할 수 있는 저장매체를 필요로 한다.
- <3> 키 교환 프로토콜에서 사용자 인증을 위한 또 다른 방법은 패스워드를 이용한 방법이다. 인증을 위해 사용되는 패스워드는 사람이 기억하기 쉬운 비교적 짧은 문자열이므로 패스워드를 저장할 특별한 저장매체나 컴퓨터의 메모리가 필요 없다. 패스워드를 이용한 방법은 공개키나 사전에 공유된 키를 사용하는 방법과 비교할 때, 사용자의 측면에서 편리하게 사용할 수 있는 방법이므로 많은 연구가 진행되고 있다.
- <4> 가장 기본적인 패스워드 기반의 키 교환 프로토콜은 Bellovin과 Merritt(SM.Bellovin, M.Merritt, "Encrypted

key exchange: password-based protocols secure against dictionary attacks”, Proceedings of the IEEE Symposium on Research in Research in Security and Privacy, pp.72-84, 1992.)가 처음 제안하고 그 이후로도 많은 연구가 되어온 2자간 키 교환 프로토콜이 있다. 2자간 키 교환 프로토콜은 서로 공유하고 있는 패스워드를 사용해 상대방을 인증하고 키를 교환하는 방법이다. 2자간 키 교환 프로토콜은 키를 공유하고자 하는 사용자끼리 패스워드를 공유하고 있어야 하므로 키 교환 프로토콜을 수행하기 전에 상대방과 패스워드를 교환해야 하고 또한 다수의 사용자와 키를 교환할 경우 사용자 개인이 다수의 패스워드를 기억하고 있어야 한다. 일반적으로 사람이 기억할 수 있는 패스워드의 개수는 한정되기 때문에 다수의 사용자와 키를 교환할 경우 상기 방법은 비효율적이다.

<5> Gong 외 다수(L.Gong, M.Lomas, R.Needham, J.Saltzer, “Protecting poorly chosen secrets from guessing attacks”, IEEE Journal on Selected Areas in Communications, vol.11, no.5, pp.648-656, 1993.), 또는 Halevi와 Krawczyk (S.Halevi, H.Krawczyk, “Public-key cryptography and password protocols”, ACM Transactions on Information and System Security, vol.2, no.3, pp.230-268, 1999.) 등에 의해 제안된 3자간 키 교환 프로토콜은, 각 사용자들이 서버와 패스워드를 공유하고 키 교환 수행시 공유한 패스워드를 사용해 각 사용자들이 서버에 의해 인증을 받은 후 인증정보로 상호 간의 키를 공유하는 방법이다. 따라서 사용자들은 서버와 공유한 자신의 패스워드 하나만 기억하고 있으면 서버로부터 인증을 받을 수 있으므로 자신의 패스워드 하나로 다수의 사용자와 키 교환이 가능하다. 따라서, 3자간 키 교환 프로토콜은 2자간 키 교환 프로토콜에 있어서의 다수의 사용자와 키 교환을 수행하기 위해 많은 패스워드를 기억해야 하는 단점을 개선하였다.

<6> 그러나, 기존의 3자간 키 교환 프로토콜에 있어서 서버는 각 사용자들이 키 교환 프로토콜 수행할 때마다 사용자 인증을 위해 매번 개입하여 연산을 수행하여야 한다. 따라서 다수의 사용자가 동시에 키 교환 프로토콜을 수행하는 경우 서버에게 부담이 된다. 이러한 경우 서버는 많은 연산량 및 통신량으로 인해 과부하가 걸리게 되므로 서비스를 받기 위한 사용자 대기 시간이 길어지는 단점이 있다.

발명의 내용

해결 하고자하는 과제

<7> 따라서, 본 발명이 이루고자 하는 첫 번째 기술적 과제는, 스마트카드를 기반으로 하여 서버의 개입 없이 키 교환을 안전하게 수행하는 방법을 제공하는 것이다.

<8> 본 발명이 이루고자 하는 두 번째 기술적 과제는, 스마트카드를 기반으로 하여 서버의 개입 없이 키 교환을 안전하게 수행하는 시스템을 제공하는 것이다.

<9> 본 발명이 이루고자 하는 세 번째 기술적 과제는, 본 발명에 따른 키 교환 방법 및 시스템에 사용되는 스마트카드를 제공하는 것이다.

<10> 본 발명이 이루고자 하는 네 번째 기술적 과제는, 본 발명에 따른 키 교환 방법 및 시스템에 사용되는 스마트카드를 제어하는 마이크로프로세서를 제공하는 것이다.

과제 해결수단

<11> 상기와 같은 첫 번째 기술적 과제를 해결하기 위하여, 스마트카드를 기반으로 3자간 키 교환을 수행하는 방법으로서, 사용자 단말기에서 트랩도어 해시함수에 의해 변환된 개인정보를 포함하는 사용자 개인정보 및 서버의 비밀키를 통해, 서버에서 사용자 개인정보에 대한 슈노르(schnorr) 서명을 생성하고, 상기 개인정보에 대한 슈노르 서명을 포함하는 등록정보를 스마트카드에 저장하는 사용자 등록 단계; 상기 스마트카드와 인터페이싱(interfacing)할 수 있는 단말기를 통해 사용자의 개인정보가 입력되면, 상기 스마트카드에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 상기 사용자 등록 단계에 의한 등록 사용자인지를 검증하는 사용자 검증 단계; 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계; 네트워크를 통해 등록 사용자 간에 인증정보를 교환하고 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및 상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 포함하는 스마트카드 기반의 3자간 키 교환 방법을 제공한다.

<12> 본 발명의 일 실시예에 따르면, 상기 사용자 등록 단계는 상기 사용자 단말기에서 임의의 제1 난수를 이용하여 상기 트랩도어 해시함수로 변환된 개인정보를 생성하는 단계; 상기 사용자 단말기에서 네트워크를 통해 상기 트

래도어 해시함수에 의해 변환된 개인정보를 포함하는 사용자 개인정보를 상기 서버로 전송하는 단계; 및 상기 서버에서 임의의 제2 난수를 이용하여 상기 개인정보에 대한 슈노르 서명을 생성하고, 상기 개인정보에 대한 슈노르 서명을 포함하는 상기 등록정보를 상기 스마트카드에 저장하는 단계를 포함할 수 있다.

- <13> 본 발명의 일 실시예에 따르면, 상기 사용자 등록 단계는 상기 스마트카드와 인터페이싱할 수 있는 단말기를 통해 상기 제1 난수, 상기 트랩도어 해시함수의 해시값을 계산하기 위한 해시키, 및 상기 해시값의 충돌쌍을 찾기 위한 트랩도어 키를 상기 스마트카드에 저장하는 단계를 더 포함할 수 있다.
- <14> 본 발명의 일 실시예에 따르면, 상기 트랩도어 해시함수로 변환된 개인정보는 패스워드(PW)를 트랩도어 해시함수로 변환한 개인정보일 수 있다.
- <15> 본 발명의 일 실시예에 따르면, 상기 사용자 개인정보는 사용자 아이디(ID)를 포함하고, 그리고 상기 개인정보에 대한 슈노르 서명은 상기 사용자 아이디(ID)에 대한 슈노르 서명일 수 있다.
- <16> 본 발명의 일 실시예에 따르면, 상기 등록정보는 유한 순환 곱셈군의 생성자로서 상기 제2 난수를 승수로 하는 상기 생성자 및 상기 서버의 공개키를 포함할 수 있다.
- <17> 본 발명의 일 실시예에 따르면, 상기 사용자 검증 단계에서 입력되는 상기 개인정보는 아이디 및 패스워드를 포함하고, 그리고 상기 사용자 검증 단계는 입력된 아이디 및 패스워드가 상기 사용자 등록 단계에서 사용된 상기 사용자 아이디(ID) 및 패스워드(PW)와 동일한지를 검증하는 단계일 수 있다.
- <18> 상기와 같은 두 번째 기술적 과제를 해결하기 위하여, 스마트카드의 제어, 데이터 처리 및 연산을 수행하는 마이크로프로세서 및 데이터를 저장하는 기억장치를 포함하는 스마트카드를 기반으로 3자간 키 교환을 수행하는 시스템으로서, 상기 스마트카드 기반의 3자간 키 교환 시스템은, 임의의 제1 난수를 이용하여 트랩도어 해시함수에 의해 변환된 개인정보를 생성하고, 네트워크를 통해 상기 트랩도어 해시함수에 의해 변환된 개인정보를 포함하는 사용자 개인정보를 서버로 전송하는 사용자 단말기; 임의의 제2 난수, 상기 사용자 개인정보, 및 비밀키를 이용하여 사용자 개인정보에 대한 슈노르 서명을 생성하고, 상기 개인정보에 대한 슈노르 서명을 포함하는 등록정보를 상기 스마트카드의 상기 기억장치에 저장함으로써 사용자 등록을 수행하는 상기 서버; 및 상기 스마트카드와 인터페이싱(interfacing)할 수 있는 단말기로서 상기 스마트카드에 데이터를 입력할 수 있는 상기 단말기를 포함하고, 상기 스마트카드의 상기 마이크로프로세서는, 상기 스마트카드와 인터페이싱(interfacing)할 수 있는 상기 단말기를 통해 사용자의 개인정보가 입력되면 상기 스마트카드의 상기 기억장치에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 등록 사용자인지를 검증하는 사용자 검증 단계; 상기 사용자가 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고, 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계; 네트워크를 통해 등록 사용자 간에 인증정보를 교환하고, 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및 상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 실행시키는 스마트카드 기반의 3자간 키 교환 시스템을 제공한다.
- <19> 본 발명의 일 실시예에 따르면, 상기 마스터카드의 상기 마이크로프로세서는 상기 사용자 검증 단계에 의해 상기 사용자가 등록 사용자임이 검증된 후에 상기 패스워드(PW)를 변경하여 키 교환을 수행하는 경우, 상기 스마트카드와 인터페이싱할 수 있는 상기 단말기를 통해 새로운 패스워드(PW_{new})를 입력받아 상기 새로운 패스워드를 상기 패스워드(PW)로서 상기 마스터카드의 상기 기억장치에 저장하는 패스워드 변경 단계를 더 수행할 수 있다.
- <20> 상기와 같은 세 번째 기술적 과제를 해결하기 위하여, 본 발명에 따른 스마트카드 기반의 3자간 키 교환 시스템에 사용되는 스마트카드로서, 상기 스마트카드는 상기 스마트카드의 제어, 데이터 처리 및 연산을 수행하는 마이크로프로세서; 및 상기 서버에 의해 생성되는 상기 개인정보에 대한 슈노르 서명을 포함하는 데이터를 저장하는 기억장치를 포함하고, 상기 스마트카드의 상기 마이크로프로세서는, 상기 스마트카드와 인터페이싱할 수 있는 상기 단말기를 통해 사용자의 개인정보가 입력되면 상기 스마트카드의 상기 기억장치에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 등록 사용자인지를 검증하는 사용자 검증 단계; 상기 사용자가 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고, 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계; 네트워크를 통해 등록 사용자 간에 인증정보를 교환하고, 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및 상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 실행시키는 스마트카드를 제공한다.
- <21> 상기와 같은 네 번째 기술적 과제를 해결하기 위하여, 본 발명에 따른 스마트카드 기반의 3자간 키 교환 시스템에 사용되는 스마트카드를 제어하고, 데이터 처리 및 연산을 수행하는 마이크로프로세서로서, 상기 스마트카드

는, 상기 서버에 의해 생성된 상기 개인정보에 대한 슈노르 서명을 포함하는 데이터를 저장하는 기억장치를 포함하고, 상기 마이크로프로세서는, 상기 스마트카드와 인터페이싱할 수 있는 상기 단말기를 통해 사용자의 개인정보가 입력되면 상기 스마트카드의 상기 기억장치에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 등록 사용자인지를 검증하는 사용자 검증 단계; 상기 사용자가 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고, 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성하는 인증정보 구성 단계; 네트워크를 통해 등록 사용자 간에 인증정보를 교환하고, 상기 교환된 인증정보를 이용하여 상호 인증하는 상호 인증 단계; 및 상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명을 이용하여 세션키를 생성하는 키 교환 단계를 실행시키는 마이크로프로세서를 제공한다.

효 과

- <22> 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법 및 시스템과 이에 사용되는 스마트카드 및 프로세서는, 서버의 연산 로드를 감소시키면서 안전하게 키 교환을 수행할 수 있다는 이점을 제공한다.

발명의 실시를 위한 구체적인 내용

- <23> 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 사용하는 트랩도어 해시함수(trapdoor hash function)의 개요를 설명한다.

- <24> 트랩도어 해시함수는 키를 사용하는 해시함수로서 함수와 해시키(HK), 트랩도어 키(TK)로 구성되어 있다. 해시키는 공개키로서 해시값을 계산하는데 사용되고, 트랩도어 키는 비밀키로서 충돌쌍을 찾기 위해 사용된다. 그러므로 일반적인 해시함수와 같이 해시값은 누구든지 계산할 수 있으나 정해진 해시값에 대한 충돌쌍은 트랩도어 키를 소유하고 있는 사람만이 찾을 수 있다. 트랩도어 해시함수는 여러 종류가 있지만 본 발명에서 사용하는 시스템변수와 동일한 것은 이산대수 가정(discrete log assumption)에 기반한 트랩도어 해시함수이다(H. Krawczyk, T. Rabin, "Chameleon Signatures", In Symposium on Network and Distributed Systems Security (NDSS '00), pp.143-154, 2000, Internet Society. 참조).

- <25> **키 생성 알고리즘**

- <26> 안전한 소수 $p(p=2q+1$ 이 되는 소수 q 가 존재하는 소수, $p \in \{0,1\}^k$)와 위수가 q 인 생성자 $g(g \in \mathbb{Z}_p^*)$ 를 선택한다. 또한 랜덤값 $a(a \in \mathbb{Z}_p^*)$ 를 선택하고 $y=g^a \pmod{p}$ 를 계산한다. 공개되는 해시키는 (p,g,y) 이고 비밀키인 트랩도어 키는 a 이다.

- <27> **해시함수**

- <28> 해시키 $HK=(p,g,y)$ 에 대하여 해시함수 $h_{HK}: \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p^*$ 를 하기 수학적 1과 같이 정의한다.

수학적 1

- <29>
$$h_{HK}(m,r) = g^m y^r \pmod{p}$$

- <30> 상기 수학적 1에서, m 은 해시를 취할 메시지이고 r 은 랜덤하게 선택되는 값이다. 상기 트랩도어 해시함수는 트랩도어 키 $TK=a$ 를 사용하면 선택한 메시지 m' 에 대하여 하기 수학적 2에 나타난 등식을 만족하는 r' 를 찾을 수 있다.

수학적 2

- <31>
$$h_{HK}(m,r) = h_{HK}(m',r')$$

- <32> 즉, 상기 r' 의 값은 상기 수학적 3과 같이 찾을 수 있다.

수학적 3

- <33>
$$r' = \alpha^{-1}(m - m') + r \pmod{q}$$

- <34> 이하, 본 발명의 기술적 과제의 해결 방안을 명확화하기 위해 첨부한 도면을 참조하여 본 발명의 바람직한 실시

예를 상세하게 설명한다. 다만, 본 발명을 설명함에 있어서 관련된 공지기술 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불명료하게 할 수 있다고 판단되는 경우에는 그 상세한 설명은 생략할 것이다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자 등의 의도 또는 관례 등에 따라 달라질 수 있을 것이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

<35> 도 1에는 본 발명에 따른 스마트카드 기반의 3자간 키 교환 시스템 환경이 개략적으로 도시되어 있으며, 도 2에는 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법의 일례가 흐름도로 도시되어 있다.

<36> 도 1 및 도 2를 참조하면, 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법은 사용자 단말기(110, 120)에서 서버(100)로 사용자 개인정보를 전송하여(S200) 상기 서버(100)에서 상기 전송된 사용자 개인정보를 이용하여 사용자 등록을 수행하는 사용자 등록 단계(S210), 스마트카드(112, 122)를 이용한 사용자 검증 단계(S220), 스마트카드(112, 122)를 이용한 인증정보 구성 단계(S230), 인증정보를 통한 상호 인증 단계(S240), 및 세션키를 생성하는 키 교환 단계(S250)를 포함한다.

<37> 더 구체적으로 설명하자면, 우선 시스템 변수를 정의한다.

<38> 안전한 소수 $p(p=2q+1$ 이 되는 소수 q 가 존재하는 소수, $p \in \{0, 1\}^k$)를 선택한 후, 위수가 q 인 유한한 순환 곱셈군 G 를 생성하고 상기 G 의 생성자 $g(g \in Z_p^*)$ 를 선택한다. 그리고 램덤(random)한 길이의 임의의 문자열을 Z_q 로 보내는 암호학적 해시함수 $H: \{0, 1\}^* \rightarrow Z_q$ 를 생성한다. 또한, 서버(100)는 자신의 비밀키(개인키) $x(x \in Z_q^*)$ 를 선택하고 공개키 $y=g^x \pmod{p}$ 를 계산한다.

<39> 사용자 등록 단계

<40> 사용자 등록 단계(S200, S210)에서는, 사용자 단말기(110, 120)에서 트랩도어 해시함수 H_{HK} 에 의해 변환된 개인정보를 포함하는 사용자 개인정보 및 서버의 비밀키를 통해, 서버에서 사용자 개인정보에 대한 슈노르(schnorr) 서명을 생성하고, 상기 개인정보에 대한 슈노르 서명을 포함하는 등록정보를 스마트카드(112, 122)에 저장한다.

<41> 예컨대, 제1 사용자가 서버(100)에 등록을 원한다고 가정하자. 상기 제1 사용자는 사용자 단말기(110)를 통해 자신의 아이디(ID), 패스워드(PW), 및 제1 난수(n)를 선택하고 트랩도어 해시함수 H_{HK} 를 생성하여 $H_{HK}(PW, n)$ 를 계산한다. 그리고 트랩도어 해시함수에 의해 변환된 패스워드 $H_{HK}(PW, n)$ 와 아이디(ID)를 상기 서버(100)로 보낸다(S200).

<42> 상기 서버(100)는 제2 난수(s)를 선택하여 하기 수식 4와 같이 표현되는 상기 아이디(ID)에 대한 슈노르(schnorr) 서명 쌍을 계산한다(C.Schnorr, "Efficient identification and signatures for smart cards", Crypto'89, pp.239-252, 1990. 참조).

수식 4

$$\begin{aligned} w &= g^{H_{HK}(PW, n)} g^s, \\ t &= H_{HK}(PW, n) + s + xH(ID, w) \end{aligned}$$

<44> 그리고 상기 서버(100)는 등록정보로서 상기 아이디(ID)에 대한 슈노르(schnorr) 서명 쌍 w 및 t 와 상기 제2 난수 s 를 승수로 하는 생성자 g^s , 및 상기 서버(100)의 공개키 y 를 스마트카드(112)에 입력한다. 상기 스마트카드(112)는 상기 스마트카드(112)를 제어하고 데이터 처리 및 연산을 수행하는 마이크로프로세서(미도시) 및 데이터를 저장하는 기억장치(미도시)를 포함하여 상기 등록정보들을 저장할 수 있다. 상기 스마트카드(112)의 사용자인 상기 제1 사용자는 상기 스마트카드(112)와 인터페이싱(interfacing) 할 수 있는 단말기(110)를 통해 자신이 처음 선택했던 상기 제1 난수 n , 상기 트랩도어 해시함수의 해시키 HK 및 트랩도어 키 TK 를 상기 스마트카드(112)에 입력하여 저장한다(S210). 본 발명의 일 실시예에 있어서, 상기 사용자 단말기(110)와 상기 스마트카드(112)와 인터페이싱 할 수 있는 상기 단말기(110)는 개별적일 수 있다.

<45> 상기 사용자 등록 단계는 키 교환을 수행할 상대방 사용자인 제2 사용자에게도 동일하게 적용될 수 있다.

<46> 사용자 검증 단계

<47> 사용자 검증 단계(S220)에서는, 상기 스마트카드와 인터페이싱(interfacing)할 수 있는 단말기를 통해 사용자의

개인정보가 입력되면, 상기 스마트카드에 저장된 상기 개인정보에 대한 슈노르 서명을 이용하여 상기 사용자가 상기 사용자 등록 단계에 의한 등록 사용자인지를 검증한다.

<48> 예컨대, 제1 사용자 및 제2 사용자가 안전한 통신을 위해 키를 교환하기 원한다고 가정하자. 상기 제1 사용자는 자신의 스마트카드(112)를 카드 리더기에 넣고 상기 스마트카드(112)와 인터페이싱할 수 있는 단말기(110)를 통해 아이디 ID₁'와 패스워드 PW₁'를 입력한다. 상기 스마트카드(112)는 하기 수학식 5와 같이 입력된 패스워드 PW₁'로 w₁'를 계산한다.

수학식 5

<49>
$$w_1' = g^{H_{HK_1}(PW_1', n_1)} g^{s_1}$$

<50> 그리고 아이디 동일성 확인과 상기 스마트카드(112)의 상기 기억장치에 저장된 w₁와 상기 수학식 5와 같이 계산된 w₁'를 비교해 상기 제1 사용자가 상기 사용자 등록 단계에 의한 등록 사용자인지를 검증한다(S220).

<51> 상기 사용자 검증 단계는 키 교환을 수행할 상대방 사용자인 상기 제2 사용자에게도 동일하게 적용될 수 있다.

<52> 인증정보 구성 단계

<53> 인증정보 구성 단계(S230)에서는, 상기 제1 사용자가 등록 사용자로 검증되면 타임스탬프에 대한 슈노르 서명을 생성하고 상기 타임스탬프에 대한 슈노르 서명을 포함하는 인증정보를 구성한다.

<54> 예컨대, 상기 제1 사용자의 상기 스마트카드(112)는 제3 난수 r₁을 선택하고 상기 선택한 제3 난수 r₁ 및 타임스탬프 T₁을 이용하여 하기 수학식 6과 같이 타임스탬프에 대한 슈노르 서명 쌍을 계산한다.

수학식 6

<55>
$$R_1 = g^{r_1},$$

<56>
$$A_1 = r_1 + t_1 H(T_1, R_1)$$

<57> 그리고 상기 타임스탬프에 대한 슈노르 서명 쌍 R₁ 및 A₁, 상기 타임스탬프 T₁, 상기 제1 사용자의 아이디(ID₁), 및 상기 아이디(ID₁)에 대한 슈노르 서명 w₁을 포함하는 인증정보를 구성한다.

<58> 상기 사용자 검증 단계는 키 교환을 수행할 상대방 사용자인 상기 제2 사용자에게도 동일하게 적용될 수 있으며, 상기 제2 사용자의 인증정보는 R₂, A₂, T₂, ID₂, 및 w₂을 포함한다.

<59> 상호 인증 단계

<60> 상호 인증 단계(S240)에서는, 네트워크를 통해 등록 사용자 간에 인증정보를 교환하고 상기 교환된 인증정보를 이용하여 상호 인증한다.

<61> 예컨대, 상기 제1 사용자의 스마트카드(112)는 유무선 네트워크를 통해 상기 제2 사용자의 상기 인증정보를 전송받아 하기 수학식 7에 나타난 등식이 성립하는 경우 상기 제2 사용자를 인증한다.

수학식 7

<62>
$$R_2(w_2 y^{H(ID_2, w_2)})^{H(T_2, R_2)} = g^{A_2}$$

<63> 상기 제2 사용자 측에서도 동일하다.

<64> 키 교환 단계

<65> 키 교환 단계(250)에서는, 상기 교환된 인증정보에 포함된 상기 타임스탬프에 대한 슈노르 서명(R)을 이용하여 세션키를 생성한다.

<66> 예컨대, 상기 제1 사용자의 스마트카드(112)는 하기 수학식 8에 의해 세션키 값(key)을 계산한다.

수학식 8

$$key = H(R_2^{r_1}) = H(g^{r_1 r_2})$$

<67>

<68>

상기 수학식 8에서, R_2 는 상기 제2 사용자의 상기 타임스탬프에 대한 슈노르 서명이고, r_1 은 상기 제1 사용자의 스마트카드(112)가 선택한 제3 난수이고, 그리고 r_2 는 상기 제2 사용자의 스마트카드(122)가 선택한 제3 난수를 나타낸다.

<69>

본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법 및 시스템은 트랩도어 해시함수를 사용함으로써 서버의 개입 없이 패스워드를 변경하여 변경된 패스워드를 통해 키 교환을 수행할 수 있다.

<70>

도 3에는 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법의 패스워드 변경 단계의 일례가 흐름도로 도시되어 있다.

<71>

패스워드 변경 단계

<72>

패스워드 변경 단계에서는, 상기 사용자 검증 단계(S220)에 의해 상기 사용자가 등록 사용자임이 검증된 후에 상기 패스워드(PW_1)를 변경하여 키 교환을 수행하는 경우, 상기 스마트카드와 인터페이싱할 수 있는 상기 단말기(110)를 통해 새로운 패스워드(PW_{new})를 입력받아 상기 새로운 패스워드를 상기 패스워드(PW_1)로서 상기 마스터카드(112)의 상기 기억장치에 저장한다.

<73>

예컨대, 상기 제1 사용자가 자신의 패스워드 PW_1 을 변경하여 새로운 패스워드 PW_{new} 로 키 교환을 수행하고자 한다면, 상기 제1 사용자는 자신의 스마트카드(112)를 카드 리더기에 넣고 상기 스마트카드(112)와 인터페이싱할 수 있는 단말기(110)를 통해 아이디 ID_1 '와 패스워드 PW_1 '를 입력한다(S300).

<74>

상기 스마트카드(112)는 상기 수학식 5와 같이 입력된 패스워드 PW_1 '로 w_1 '를 계산한다. 그리고 아이디 동일성 확인과 상기 스마트카드(112)의 상기 기억장치에 저장된 w_1 와 상기 수학식 5와 같이 계산된 w_1 '를 비교해 상기 제1 사용자가 상기 사용자 등록 단계에 의한 등록 사용자인지를 검증한다(S310).

<75>

상기 제1 사용자가 등록 사용자로 검증되면 자신이 사용할 새로운 패스워드 PW_{new} 를 입력한다(S320). 상기 스마트카드(112)는 상기 트랩도어 키 TK 를 사용해서 하기 수학식 9에 나타난 등식을 만족하는 새로운 난수 n_{new} 를 찾아 상기 제1 난수 n_1 을 삭제하고 새로운 난수 n_{new} 를 상기 제1 난수 n_1 대신 상기 기억장치에 저장한다(S330).

수학식 9

$$H_{HK_1}(PW_1, n_1) = H_{HK_1}(PW_{new}, n_{new})$$

<76>

<77>

상술한 바와 같이 패스워드가 변경된 스마트카드(112)는 새로운 패스워드 PW_{new} 로서 사용자 검증이 가능해 진다. 하지만 상기 아이디(ID_1)에 대한 슈노르 서명값 w_1 는 변하지 않으므로 키 교환 수행시 상기 스마트카드(112) 내의 정보를 정상적으로 사용할 수 있다.

<78>

본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법 및 시스템에 사용되는 스마트카드는, 상기 스마트카드를 제어하는 마이크로프로세서로서 데이터 처리 및 연산을 수행하는 상기 마이크로프로세서에 의해 상기 단계들을 수행할 수 있다.

<79>

상술한 바와 같이, 기존의 3자간 키 교환 프로토콜에서 서버는 사용자 등록 과정과 사용자들 각각의 키 교환 과정에 참여하여 연산과 통신을 수행하였다. 두 과정 중에서 사용자 등록 과정보다는 키 교환 과정이 더욱 빈번하게 발생할 것이고, 따라서 키 교환시의 서버의 개입을 줄일 수 있다면 서버의 부담은 많이 줄어들게 될 것이다.

<80>

본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법 및 시스템은 키 교환 과정에서 서버의 개입이 없이 키 교환 프로토콜을 수행하므로 기존의 프로토콜에 비해 서버의 부담을 대폭 감소시키는 이점을 제공한다. 서버의 개입 없이 키 교환을 수행한다는 점은 다수의 사용자가 동시에 키 교환을 수행하는 경우에도 서비스를 받기 위한 사용자 대기 시간이 없어진다는 이점을 제공한다. 또한, 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법 및 시스템은, 서버가 각 사용자들의 인증을 위한 정보(ex. 패스워드)를 저장할 필요가 없도록 구성하였다.

이러한 점은 기존의 프로토콜과 비교해 서버의 저장 부담도 줄여주는 이점을 제공한다.

<81> 나아가, 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법 및 시스템은 다양한 공격에 대한 안전성을 제공한다. 이하, 각각의 공격에 대한 안전성을 분석한다.

<82> 사전 공격(Dictionary attack)에 대한 안전성

<83> 온라인(On-line) 사전 공격(Dictionary attack)은 패스워드 입력 횟수를 제한하는 등의 방법으로 간단히 막을 수 있으므로 오프라인(Off-line) 사전 공격에 대한 안전성에 대해서만 분석한다. 사전 공격을 하기 위해 필요한 정보는 상호인증 및 키 교환 단계에서 얻을 수 있다. 상기 상호 인증 단계에서 공격자는 m_1 를 얻을 수 있지만 공격자가 패스워드를 추측해 확인을 하려면 $H_{HK1}(PW_1, n_1)$ 의 내부값인 n_1 과 s_1 를 알아야 한다. 하지만 n_1 과 s_1 는 랜덤한 값이기 때문에 공격자는 두 값을 알 수 없다. 따라서, 본 발명은 사전 공격에 안전하다.

<84> 내부자 공격(Insider attack)에 대한 안전성

<85> 내부 공격자가 정상적인 프로토콜의 수행 중 상대방의 패스워드를 알아내려면 상기 상호 인증 단계에서 전송되는 m_1 를 이용해서 패스워드를 추측하는 방법밖에 없다. 이것은 상기 사전 공격에서와 같은 이유로 불가능하다. 또한 상대방 스마트카드의 t_1 값을 알아내는 것은 e_{T_1} 대한 슈노르(schnorr) 서명인 A_1 , R_1 을 가지고 비밀키를 알아내는 것과 같다. 따라서 t_1 값을 알아내는 것 또한 불가능하다. 그러므로 내부 공격자가 다른 올바른 사용자의 어떠한 개인 비밀값도 알아내지 못한다. 이제 내부 공격자가 서버의 개인키를 알아내려고 한다고 가정하자. 서버의 개인키는 내부 공격자의 스마트카드에 있는 정보인 t_1 를 이용해야 알 수가 있는데 스마트카드에 저장되어 있는 정보는 볼 수 없으므로 불가능하다. 공격자가 t_1 를 알아낸다고 해도 s_1 는 랜덤한 값이기 때문에 자신의 패스워드, n_1 , 및 t_1 만으로 서버의 개인키를 계산하는 것은 불가능하다. 내부 공격자는 일반적인 공격자와 다르게 올바른 자신의 패스워드와 스마트카드를 소지하고 있지만 위에서 살펴본 바와 같이 서버의 어떠한 정보도 알아낼 수 없고 또한 다른 사용자들의 비밀정보도 알아낼 수 없다. 또한 다른 올바른 사용자와의 프로토콜 수행시에도 공격자가 얻는 정보 이외의 어떠한 정보도 얻을 수 없다. 따라서 내부 공격자는 추가적으로 패스워드와 스마트카드를 소지하고 있지만 공격 능력은 일반적인 공격자와 다르지 않다. 따라서, 본 발명은 내부자 공격에 안전하다.

<86> 위장 공격(Impersonation attack)에 대한 안전성

<87> 제1 사용자를 가장하는 경우를 살펴보자. 공격자가 제1 사용자를 가장하여 제2 사용자와 정상적인 키 교환 프로토콜을 수행하기 위해서는 상대방에게 올바른 R_1 , A_1 및 m_1 를 전송해야 한다. 하지만 서버에게 받아야 하는 t_1 없이 올바른 R_1 과 A_1 를 생성하는 것은 불가능하고 또한 m_1 도 알 수 없으므로 올바른 값을 전송할 수 없다. 따라서, 본 발명은 위장 공격에 안전하다.

<88> 재전송 공격(Replay attack)에 대한 안전성

<89> 본 발명에서는 타임스탬프 T_1 를 사용하여 이전의 통신 정보를 사용할 수 없으므로 재전송 공격이 불가능하다. 공격자가 타임스탬프만 바꿔서 올바른 정보를 생성해 전송하기 위해서는 공격 시점의 타임스탬프에 대한 서명인 R_1 과 A_1 를 생성해야 한다. t_1 없이 올바른 R_1 및 A_1 의 생성은 불가능하다. 따라서 본 발명은 재전송 공격에 안전하다.

<90> 알려진 키 비밀성(Known Key Security)

<91> 본 발명의 교환된 키는 $H(g^{r_1 r_2})$ 이다. 여기서 r_1 및 r_2 는 키를 교환할 때마다 랜덤하게 선택되는 값이다. 따라서 공격자가 다른 어떠한 세션의 키를 알고 있다고 하더라도 공격을 하고자 하는 세션에서 사용되는 랜덤값 r_1 및 r_2 와는 관련성이 없다. 따라서 내부 공격자의 공격에서 보았듯이 공격자가 키를 알아내려면 CDH문제를 풀어야만 한다. 따라서, 본 발명은 알려진 키 안전성을 만족한다.

<92> 완전 순방향 비밀성(Perfect Forward Security)

<93> 공격자가 각 사용자의 패스워드를 알아내고 스마트카드를 획득했다고 해도 각 세션의 키를 생성할 경우에는 랜

값 r_1 및 r_2 를 사용하게 되므로 이전의 어떠한 세션에 대해서도 사용된 키의 정보를 얻을 수 없다. 이전 세션에서 사용된 키를 알아내려면 공격자는 CDH문제를 풀어야 한다. 따라서, 본 발명은 완전 순방향 비밀성을 만족한다.

<94> **알려지지 않은 키 분배 공격(Unknown Key Share attack)**

<95> 제1 사용자와 제2 사용자가 프로토콜을 수행할 때, 두 사용자는 각각 R_1 및 A_1 와 R_2 및 A_2 를 사용해 상대방에 대한 인증을 하게 된다. 이때 제2 사용자가 자신이 계산한 키가 제1 사용자가 아닌 제3 사용자와 설정된 키라고 믿으려면 제2 사용자는 상호 인증 단계에서 받는 정보가 제3 사용자의 아이디인 ID_3 로 검증되어야 한다. 하지만 공격자는 t_3 를 알 수 없으므로 제3 사용자의 아이디인 ID_3 로 검증이 성공하는 값인 R_3 및 A_3 를 생성할 수 없다. 마찬가지로 이유로 제1 사용자도 자신과 키를 교환한 사람이 제2 사용자가 아닌 다른 사용자라고 믿을 가능성은 없다. 따라서, 본 발명은 알려지지 않은 키 분배 공격에 안전하다.

<96> **키 제어(Key Control)**

<97> 본 발명의 교환된 키는 두 사용자가 각각 랜덤값 r_1 및 r_2 를 선택한 후, $H(g^{r_1 r_2})$ 를 계산해 키로 사용하게 된다. 프로토콜 중에 두 사용자는 한 번씩의 통신을 한 후 키를 계산하게 되고, 또한 상대방이 선택한 랜덤값은 알지 못한다. 따라서 각 사용자는 설정된 키의 어떠한 부분도 미리 결정할 수 없다.

<98> 상술한 바와 같이, 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법 및 시스템은 다양한 공격에 대한 안전성을 보장하는 이점을 아울러 제공한다.

<99> 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 본 발명이 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 상술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면의 간단한 설명

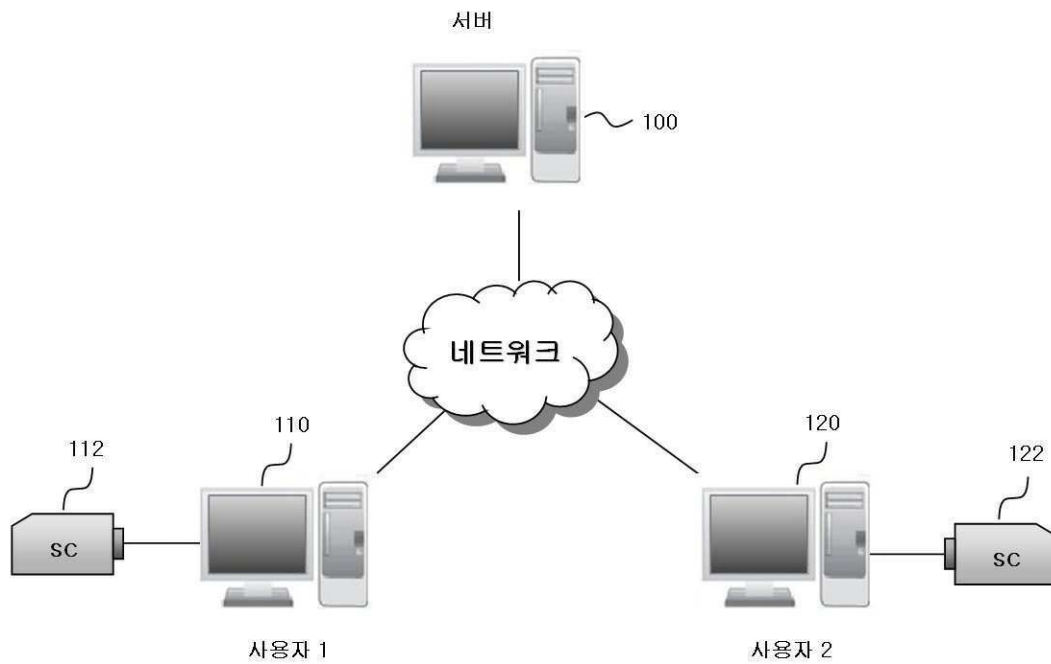
<100> 도 1은 본 발명에 따른 스마트카드 기반의 3자간 키 교환 시스템 환경을 개략적으로 나타낸 도면.

<101> 도 2는 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법의 일례를 나타낸 흐름도.

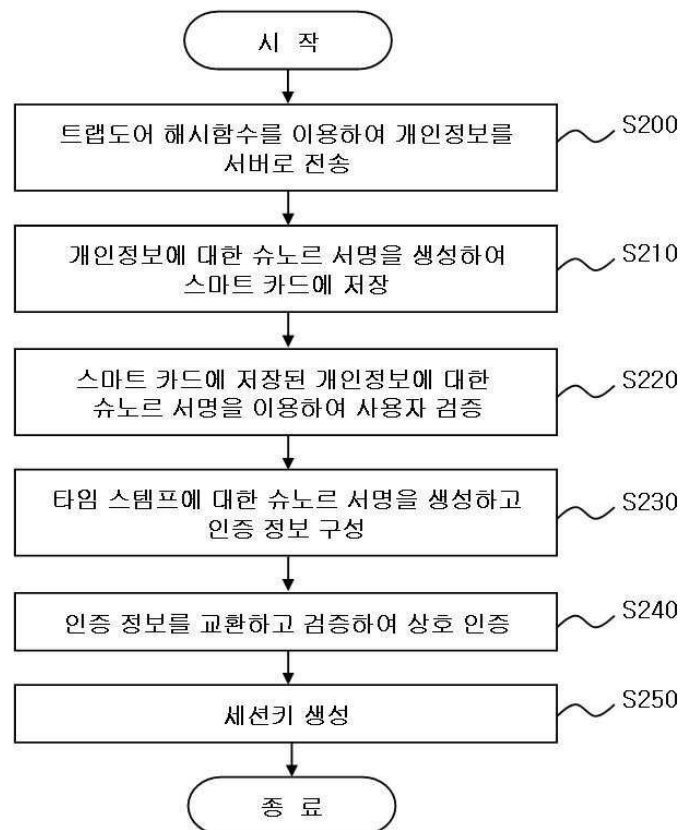
<102> 도 3은 본 발명에 따른 스마트카드 기반의 3자간 키 교환 방법의 패스워드 변경 단계를 나타낸 흐름도.

도면

도면1



도면2



도면3

