



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0067550
(43) 공개일자 2008년07월21일

(51) Int. Cl.

H04L 9/08 (2006.01) H04B 5/00 (2006.01)

(21) 출원번호 10-2007-0004984

(22) 출원일자 2007년01월16일

심사청구일자 2007년01월16일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

임종인

서울 종로구 내수동 95 삼성파크팰리스 101- 901

이동훈

경기 고양시 일산서구 일산3동 후곡동신아파트
808동 804호

(뒷면에 계속)

(74) 대리인

현종철

전체 청구항 수 : 총 10 항

(54) 스마트 카드를 이용한 삼자간 키 교환 방법, 그 기록 매체 및 스마트 카드를 이용한 삼자간 키 교환 시스템

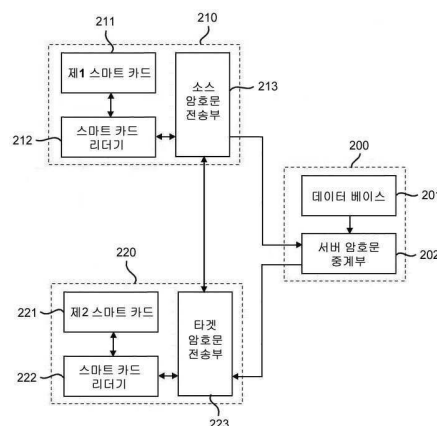
(57) 요약

스마트 카드를 이용한 삼자간 키 교환 방법, 그 기록 매체 및 스마트 카드를 이용한 삼자간 키 교환 시스템이 개시된다.

본 발명은 서버, 상기 서버로부터 스마트 카드를 발급받은 소스 클라이언트 및 타겟 클라이언트를 포함하는 시스템의 키 교환 방법에 있어서, 상기 소스 클라이언트의 스마트카드에서 임의의 난수인 제1난수 및 제2난수를 선택한 후, 상기 제2난수를 포함하는 암호문을 상기 서버에 전송하고, 상기 제1난수를 포함하는 암호문을 상기 타겟 클라이언트에 전송하는 단계, 상기 서버에서 상기 타겟 클라이언트에 상기 제2난수를 포함하는 암호문을 전송하는 단계, 상기 타겟 클라이언트의 스마트 카드에서 임의의 난수인 제3난수 및 제4난수를 선택한 후, 상기 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출하고, 상기 제2난수 및 제4난수를 이용하여 세션키를 연산하고, 상기 제3난수 및 제4난수를 포함하는 암호문을 상기 소스 클라이언트에 전송하는 단계 및 상기 소스 클라이언트의 스마트카드에서 상기 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 상기 제2난수 및 상기 제4난수를 이용한 세션키를 연산하여 세션키를 공유하는 단계를 포함한다.

본 발명에 의하면, 클라이언트-클라이언트 간 인증 및 키 교환을 가능하게 하고, 서버가 클라이언트들 간에 교환된 세션 키 정보를 알 수 없도록 하여 보안성을 향상시킬 수 있으며, 키 교환을 위한 데이터의 교환 횟수를 3번 이하로 제한할 수 있고, 스마트 카드를 이용하면서도 고속의 인증이 가능하며, 키 교환을 하는 클라이언트 간에 서로가 동일한 세션 키를 연산하였는지에 대한 여부도 확인할 수 있다.

대표도 - 도2



(72) 발명자

권정욱

서울 광진구 중곡1동 234-12번지

정익래

광주 북구 오치2동 로얄아파트 102동 101호

특허청구의 범위

청구항 1

서버, 상기 서버로부터 스마트 카드를 발급받은 소스 클라이언트 및 타겟 클라이언트를 포함하는 시스템의 키 교환 방법에 있어서,

상기 소스 클라이언트의 스마트카드에서 임의의 난수인 제1난수 및 제2난수를 선택한 후, 상기 제2난수를 포함하는 암호문을 상기 서버에 전송하고, 상기 제1난수를 포함하는 암호문을 상기 타겟 클라이언트에 전송하는 단계;

상기 서버에서 상기 타겟 클라이언트에 상기 제2난수를 포함하는 암호문을 전송하는 단계;

상기 타겟 클라이언트의 스마트 카드에서 임의의 난수인 제3난수 및 제4난수를 선택한 후, 상기 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출하고, 상기 제2난수 및 제4난수를 이용하여 세션키를 연산하고, 상기 제3난수 및 제4난수를 포함하는 암호문을 상기 소스 클라이언트에 전송하는 단계; 및

상기 소스 클라이언트의 스마트카드에서 상기 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 상기 제2난수 및 상기 제4난수를 이용한 세션키를 연산하여 세션키를 공유하는 단계를 포함하는 스마트 카드를 이용한 삼자간 키 교환 방법.

청구항 2

제 1 항에 있어서,

상기 제2난수를 포함하는 암호문은

상기 소스 클라이언트의 아이디, 상기 타겟 클라이언트의 아이디를 포함하고,

상기 제1난수를 포함하는 암호문은

상기 소스 클라이언트의 아이디를 포함하는 것을 특징으로 하는 스마트 카드를 이용한 삼자간 키 교환 방법.

청구항 3

제 2 항에 있어서,

상기 제1난수를 포함하는 암호문을 상기 타겟 클라이언트에 전송하는 단계는

상기 소스 클라이언트가 상기 서버로부터 상기 소스 클라이언트의 아이디 및 상기 서버의 마스터키를 해쉬함수에 적용한 제1검증자가 저장된 스마트 카드를 발급받고, 상기 타겟 클라이언트가 상기 서버로부터 상기 타겟 클라이언트의 아이디 및 상기 서버의 마스터키를 해쉬함수에 적용한 제2검증자가 저장된 스마트 카드를 발급받는 단계를 포함하는 것을 특징으로 하는 스마트 카드를 이용한 삼자간 키 교환 방법.

청구항 4

제 3 항에 있어서,

상기 타겟 클라이언트에 상기 제2난수를 포함하는 암호문을 전송하는 단계는

상기 서버에서 상기 제1검증자를 이용하여 상기 제2난수를 포함하는 암호문을 복호화하여 상기 소스 클라이언트의 아이디 및 상기 타겟 클라이언트의 아이디를 산출하는 단계; 및

상기 서버에서 상기 제2검증자로 상기 제2난수를 암호화한 암호문을 상기 타겟 클라이언트에 전송하는 단계를 포함하는 것을 특징으로 하는 스마트 카드를 이용한 삼자간 키 교환 방법.

청구항 5

제 1 항에 있어서,

상기 제3난수 및 제4난수를 포함하는 암호문은

상기 타겟 클라이언트에서 연산된 세션키로 상기 제1난수를 암호화한 암호문을 포함하고,

상기 제2난수 및 상기 제4난수를 이용한 세션키를 연산하여 세션키를 공유하는 단계는

상기 소스 클라이언트에서 연산된 세션키로 상기 제1난수를 암호화한 암호문을 복호화한 결과가 상기 제1난수와 일치하지 않으면, 상기 타겟 클라이언트와의 프로토콜을 종료하는 단계를 포함하는 것을 특징으로 하는 스마트 카드를 이용한 삼자간 키 교환 방법.

청구항 6

제 1 항에 있어서,

상기 소스 클라이언트에서 상기 제3난수 및 제4난수를 포함하는 암호문을 복호화하여 산출된 상기 제3난수를 상기 소스 클라이언트에서 연산된 세션키로 암호화한 암호문을 상기 타겟 클라이언트에 전송하는 단계; 및

상기 제3난수를 암호화한 암호문을 상기 타겟 클라이언트에서 연산된 세션키로 복호화한 결과가 상기 제3난수와 일치하지 않으면, 상기 타겟 클라이언트에서 연산된 세션키를 삭제하는 단계를 더 포함하는 것을 특징으로 하는 스마트 카드를 이용한 삼자간 키 교환 방법.

청구항 7

제 1 항 내지 제 6 항 중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 8

타겟 클라이언트, 상기 타겟 클라이언트와 인증하려는 소스 클라이언트 및 상기 소스 클라이언트 및 타겟 클라이언트에 각각 제1 스마트 카드 및 제2 스마트 카드를 발급하는 서버를 포함하는 시스템에 있어서,

상기 소스 클라이언트는

임의의 난수인 제1난수 및 제2난수를 선택하고, 상기 제2난수를 포함하는 암호문 및 상기 제1난수를 포함하는 암호문을 생성하며, 상기 타겟 클라이언트에서 선택된 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 상기 제2난수 및 상기 제4난수를 이용한 세션키를 연산하여 세션키를 공유하는 제1 스마트 카드; 및

상기 제2난수를 포함하는 암호문을 상기 서버에 전송하고, 상기 제1난수를 포함하는 암호문을 상기 타겟 클라이언트에 전송하는 소스 암호문 전송부를 포함하고,

상기 타겟 클라이언트는

상기 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출하고, 임의의 난수인 제3난수 및 제4난수를 선택하며, 상기 제2난수 및 제4난수를 이용하여 세션키를 연산하고, 상기 제3난수 및 제4난수를 포함하는 암호문을 생성하는 제2 스마트 카드; 및

상기 제3난수 및 제4난수를 포함하는 암호문을 상기 소스 클라이언트에 전송하는 타겟 암호문 전송부를 포함하고,

상기 서버는

상기 타겟 클라이언트에 상기 제2난수를 포함하는 암호문을 전송하는 서버 암호문 중계부를 포함하는 스마트 카드를 이용한 삼자간 키 교환 시스템.

청구항 9

제 8 항에 있어서,

상기 제1 스마트 카드는

상기 소스 클라이언트의 아이디 및 상기 서버의 마스터키를 해쉬함수에 적용한 제1검증자를 저장하고,

상기 제2 스마트 카드는

상기 타겟 클라이언트의 아이디 및 상기 서버의 마스터키를 해쉬함수에 적용한 제2검증자를 저장하고,

상기 서버는

상기 제1검증자 및 제2검증자를 저장하는 데이터베이스를 포함하고,

상기 서버 암호문 중계부는

상기 제1검증자를 이용하여 상기 제2난수를 포함하는 암호문을 복호화하여 상기 소스 클라이언트의 아이디 및 상기 타겟 클라이언트의 아이디를 산출하고, 상기 제2검증자로 상기 제2난수를 암호화한 암호문을 상기 타겟 클라이언트에 전송하는 것을 특징으로 하는 스마트 카드를 이용한 삼자간 키 교환 시스템.

청구항 10

제 8 항에 있어서,

상기 소스 클라이언트 및 타겟 클라이언트는

상기 제1 스마트카드 및 상기 제2 스마트카드에 저장된 정보를 독출하는 스마트 카드 리더기를 포함하는 것을 특징으로 하는 스마트 카드를 이용한 삼자간 키 교환 시스템.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <8> 본 발명은 인증 및 키 교환에 관한 것으로, 특히, 스마트 카드를 이용한 삼자간 키 교환 방법, 그 기록 매체 및 스마트 카드를 이용한 삼자간 키 교환 시스템에 관한 것이다.
- <9> 유·무선통신 및 인터넷의 발달은 여러 가지 정보보호 서비스들의 필요성을 대두시켰다. 따라서 정보보호 서비스들을 실질적으로 구현시키기 위한 여러 가지 기술 개발의 필요성이 제기되었으며 이러한 기술에 대한 많은 연구가 다양한 목적에 의하여 세분화되어 실행되고 있다.
- <10> 본 연구의 주제인 개체 간 (세션) 키 교환은 정보보호 분야에 해당하는 기술로 정보보호에 있어서 가장 기본적인 핵심적인 기술이다. 공개 네트워크 (예를 들어, Ad-hoc 네트워크, 모바일 네트워크, 홈 네트워크) 상에서 개체 간에 비밀 통신을 하거나 무결성이 보장된 통신 또는 서로를 인증해야 하는 경우에 통신하는 개체들끼리 하나의 암호학적으로 안전한 키만 공유할 수만 있다면 문제는 쉽게 해결될 수 있다. 즉, 공유된 키로 통신문을 비밀키 암호 알고리즘 (예를 들어 DES, AES, SEED 등)을 이용해서 암호화함으로써 비밀통신을 구현할 수 있으며, 또한 통신문에 대한 무결성은 이 키를 MAC (Message Authentication Code) 알고리즘의 키로 사용함으로써 구현될 수 있다. 그리고 서로에 대한 인증은 서로 공유한 비밀정보 (보통 키 값)에 대한 정보를 알고 있음을 증명하여 실현될 수 있다. 즉, 안전한 통신을 구현하기 위해서는 개체 간 키 교환이 우선적으로 선행되어야 한다. 따라서 키 교환은 정보보호기술에 있어서 필요불가결한 요소이다.
- <11> 도 1은 종래의 관용암호계를 이용한 스마트카드/단말간의 상호 인증 방법 예시도로서, 먼저 사용자 A가 스마트 카드를 이용하여 인증을 요청할 경우, 단말은 난수 R1을 생성하고 이를 스마트카드에 전달하고(1), 스마트카드는 이를 받아 자신이 보관하고 있는 키 KSA를 이용하여 암호화한 결과와 자신이 발생한 난수 R2를 함께 단말에 전달한다(2). 그러면 단말은 자신이 보관하고 있는 사용자 A의 비밀키KSA를 이용하여 R1을 암호화하고 이를 스마트카드가 전달한 결과와 비교하여 같으면 정당한 A의 스마트카드로 인식한 후(3), 스마트카드가 전달한 난수 R2를 KSA로 암호화하여 스마트카드에 전달하고(4), 스마트카드는 마찬가지로의 과정을 거쳐 단말을 인증한다(5).
- <12> 그러나 상기와 같은 관용 암호계를 이용한 사용자인증의 경우 단말기에서 각 사용자의 키를 모두 보관해야 하고 새로운 사용자가 가입했을 경우 모든 단말에 새로운 키를 등록해야 하는 관리상의 어려움 뿐만 아니라 안정성에도 문제가 있었다.
- <13> 최근에는 관용암호계 및 스마트카드를 이용한 사용자인증 시스템의 구현에 있어 사용자 ID개념을 이용하여 컴퓨터 단말기에서 관리하는 키의 수를 한개로 줄이고 카드와 단말간의 상호인증을 가능하게 하는 스마트카드를 이용한 사용자 인증방법이 제시되었다.
- <14> 즉, 종래의 스마트카드를 이용한 인증방법은 카드발급센터에서 임의의 사용자의 인증비밀키를 생성하여 스마트 카드에 공개된 정보인 ID와 비밀정보인 패스워드 및 인증비밀키를 담아 발급하고, 스마트카드에 저장된 정보를

이용하여 사용자인증을 수행하는 것이다. 이때, ID, 패스워드 및 인증비밀키를 담아 발급하는 단계는 사용자가 자신이 사용할 ID를 결정하여 패스워드와 함께 카드발급센터에 등록요청을 하는 단계와, 카드발급센터는 ID를 이용하여 인증비밀키를 연산하는 단계와, 공개된 정보의 ID와 비밀정보의 패스워드 및 인증비밀키를 스마트카드에 담아 발급하는 단계를 포함한다.

- <15> 이때, 두 개체 (클라이언트-서버) 간 인증 및 키 교환을 위해서는 클라이언트가 서버로부터 발급받은 스마트카드를 이용하여 이를 수행하게 된다. 이러한 기법으로는 클라이언트와 클라이언트 간의 인증 및 키 교환이 불가능하다.
- <16> 종래의 키 교환 방법에서는 두 클라이언트가 인증 및 키 교환을 수행하기 위해서 5번의 데이터 교환이 필요하다. 즉, 5라운드 가 소요된다.
- <17> 또한, 종래의 키 교환 방법은 두 개체 (클라이언트-서버) 간 인증 및 키 교환을 위해서는 클라이언트가 서버로부터 발급받은 스마트카드를 이용하여 이를 수행하게 된다. 하지만 이러한 기법으로는 클라이언트와 클라이언트 간의 인증 및 키 교환이 불가능하다.
- <18> 따라서, 종래의 스마트 카드를 이용한 키 교환 방법은 클라이언트 간의 인증을 위해 많은 횟수의 데이터 교환이 필요하고, 빠른 인증이 불가능하며, 클라이언트 간의 인증 및 키 교환이 용이하지 않은 문제점이 있다.

발명이 이루고자 하는 기술적 과제

- <19> 따라서, 본 발명이 이루고자 하는 첫번째 기술적 과제는 클라이언트-클라이언트 간 인증 및 키 교환을 가능하게 하고, 서버가 클라이언트들 간에 교환된 세션 키 정보를 알 수 없도록 하여 보안성을 향상시킬 수 있으며, 키 교환을 위한 데이터의 교환 횟수를 3번 이하로 제한할 수 있고, 스마트 카드를 이용하면서도 고속의 인증이 가능한 스마트 카드를 이용한 삼자간 키 교환 방법을 제공하는 데 있다.
- <20> 본 발명이 이루고자 하는 두번째 기술적 과제는 상기의 스마트 카드를 이용한 삼자간 키 교환 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 데 있다.
- <21> 본 발명이 이루고자 하는 세번째 기술적 과제는 상기의 스마트 카드를 이용한 삼자간 키 교환 방법이 적용된 스마트 카드를 이용한 삼자간 키 교환 시스템을 제공하는 데 있다.

발명의 구성 및 작용

- <22> 상기의 첫번째 기술적 과제를 이루기 위하여, 본 발명은 서버, 상기 서버로부터 스마트 카드를 발급받은 소스 클라이언트 및 타겟 클라이언트를 포함하는 시스템의 키 교환 방법에 있어서, 상기 소스 클라이언트의 스마트카드에서 임의의 난수인 제1난수 및 제2난수를 선택한 후, 상기 제2난수를 포함하는 암호문을 상기 서버에 전송하고, 상기 제1난수를 포함하는 암호문을 상기 타겟 클라이언트에 전송하는 단계, 상기 서버에서 상기 타겟 클라이언트에 상기 제2난수를 포함하는 암호문을 전송하는 단계, 상기 타겟 클라이언트의 스마트 카드에서 임의의 난수인 제3난수 및 제4난수를 선택한 후, 상기 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출하고, 상기 제2난수 및 제4난수를 이용하여 세션키를 연산하고, 상기 제3난수 및 제4난수를 포함하는 암호문을 상기 소스 클라이언트에 전송하는 단계 및 상기 소스 클라이언트의 스마트카드에서 상기 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 상기 제2난수 및 상기 제4난수를 이용한 세션키를 연산하여 세션키를 공유하는 단계를 포함하는 스마트 카드를 이용한 삼자간 키 교환 방법을 제공한다.
- <23> 상기의 두번째 기술적 과제를 이루기 위하여, 본 발명은 상기의 스마트 카드를 이용한 삼자간 키 교환 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.
- <24> 상기의 세번째 기술적 과제를 이루기 위하여, 본 발명은 타겟 클라이언트, 상기 타겟 클라이언트와 인증하려는 소스 클라이언트 및 상기 소스 클라이언트 및 타겟 클라이언트에 각각 제1 스마트 카드 및 제2 스마트 카드를 발급하는 서버를 포함하는 시스템에 있어서, 상기 소스 클라이언트는 임의의 난수인 제1난수 및 제2난수를 선택하고, 상기 제2난수를 포함하는 암호문 및 상기 제1난수를 포함하는 암호문을 생성하며, 상기 타겟 클라이언트에서 선택된 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 상기 제2난수 및 상기 제4난수를 이용한 세션키를 연산하여 세션키를 공유하는 제1 스마트 카드 및 상기 제2난수를 포함하는 암호문을 상기 서버에 전송하고, 상기 제1난수를 포함하는 암호문을 상기 타겟 클라이언트에 전송하는 소스 암호문 전송부를 포함하고, 상기 타겟 클라이언트는 상기 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출하고, 임의의 난수인 제3난수 및 제4난수를 선택하며, 상기 제2난수 및 제4난수를 이용하여 세션키를 연산하고, 상기 제3난수 및 제4난수를

포함하는 암호문을 생성하는 제2 스마트 카드 및 상기 제3난수 및 제4난수를 포함하는 암호문을 상기 소스 클라이언트에 전송하는 타겟 암호문 전송부를 포함하고, 상기 서버는 상기 타겟 클라이언트에 상기 제2난수를 포함하는 암호문을 전송하는 서버 암호문 중계부를 포함하는 스마트 카드를 이용한 삼자간 키 교환 시스템을 제공한다.

- <25> 본 발명은 스마트카드를 소지한 두 개체 (클라이언트-클라이언트)가 스마트카드 발급자인 서버의 도움으로 간접적으로 상호 인증하고, 암호학적으로 안전한 세션 키를 교환할 수 있는 방법에 관한 것이다.
- <26> 본 발명은 클라이언트-클라이언트 간 인증 및 키 교환을 위한 기술제안을 목적으로 한다. 본 발명은 서버가 클라이언트들 간에 교환된 세션 키 정보를 알 수 없도록 한다. 본 발명은 데이터의 교환 횟수를 3번 이하로 제한하는 것을 목적으로 한다.
- <27> 이하에서는 도면을 참조하여 본 발명의 바람직한 실시예를 설명하기로 한다. 그러나, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시예에 한정되는 것은 아니다.
- <28> 도 2는 본 발명의 일 실시 예에 따른 스마트 카드를 이용한 삼자간 키 교환 시스템의 블록도이다.
- <29> 이하에서, 키 교환을 시도하려는 능동적인 클라이언트를 소스 클라이언트, 키 교환의 대상이 되는 수동적인 클라이언트를 타겟 클라이언트로 정의한다. 또한, 제1 스마트 카드는 소스 클라이언트의 스마트 카드를 의미하고, 제2 스마트 카드는 타겟 클라이언트의 스마트 카드를 의미한다.
- <30> 서버(200)는 데이터베이스(201) 및 서버 암호문 중계부(202)를 포함한다.
- <31> 데이터베이스(201)는 제1검증자 및 제2검증자를 저장한다.
- <32> 서버 암호문 중계부(202)는 타겟 클라이언트(220)에 제2난수를 포함하는 암호문을 전송한다.
- <33> 이때, 제1 스마트 카드(211)는 소스 클라이언트(210)의 아이디 및 서버(200)의 마스터키를 해쉬함수에 적용한 제1검증자를 저장하고, 제2 스마트 카드(221)는 타겟 클라이언트(220)의 아이디 및 서버(200)의 마스터키를 해쉬함수에 적용한 제2검증자를 저장할 수 있다.
- <34> 바람직하게는, 서버 암호문 중계부(202)는 데이터베이스(201)에 저장된 제1검증자를 이용하여 제2난수를 포함하는 암호문을 복호화하여 소스 클라이언트(210)의 아이디 및 타겟 클라이언트(220)의 아이디를 산출할 수 있다. 이때, 서버 암호문 중계부(202)는 제2검증자로 제2난수를 암호화한 암호문을 타겟 클라이언트(220)에 전송하여 암호문을 중계할 수 있다.
- <35> 소스 클라이언트(210)는 제1 스마트 카드(211), 스마트 카드 리더기(212) 및 소스 암호문 전송부(213)를 포함한다.
- <36> 제1 스마트 카드(211)는 서버(200)에 의해 발급되고, 인증 및 키 교환을 위해 스마트 카드 리더기(212)에 삽입된다.
- <37> 제1 스마트 카드(211)는 임의의 난수인 제1난수 및 제2난수를 선택하고, 제2난수를 포함하는 암호문 및 제1난수를 포함하는 암호문을 생성한다. 또한, 제1 스마트 카드(211)는 타겟 클라이언트(220)에서 선택된 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 제2난수 및 제4난수를 이용한 세션키를 연산하여 세션키를 공유한다.
- <38> 스마트 카드 리더기(212)는 제1 스마트카드에 저장된 정보를 독출한다.
- <39> 소스 암호문 전송부(213)는 제2난수를 포함하는 암호문을 서버(200)에 전송하고, 제1난수를 포함하는 암호문을 타겟 클라이언트(220)에 전송한다.
- <40> 타겟 클라이언트(220)는 제2 스마트 카드(221), 스마트 카드 리더기(222) 및 타겟 암호문 전송부(223)를 포함한다.
- <41> 제2 스마트 카드(221)는 서버(200)에 의해 발급되고, 인증 및 키 교환을 위해 스마트 카드 리더기(222)에 삽입된다.
- <42> 제2 스마트 카드(221)는 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출한다. 또한, 제2 스마트 카드(221)는 임의의 난수인 제3난수 및 제4난수를 선택하며, 제2난수 및 제4난수를 이용하여 세션키를 연산한다. 또한, 제2 스마트 카드(221)는 제3난수 및 제4난수를 포함하는 암호문을 생성한다.

- <43> 스마트 카드 리더기(222)는 제2 스마트카드에 저장된 정보를 독출한다.
- <44> 타겟 암호문 전송부(223)는 제3난수 및 제4난수를 포함하는 암호문을 소스 클라이언트(210)에 전송한다.
- <45> 도 3은 본 발명의 다른 실시 예에 따른 스마트 카드를 이용한 삼자간 키 교환 방법의 흐름도이다.
- <46> 먼저, 소스 클라이언트의 스마트카드에서 임의의 난수인 제1난수 및 제2난수를 선택한 후, 제2난수를 포함하는 암호문을 서버에 전송하고, 제1난수를 포함하는 암호문을 타겟 클라이언트에 전송한다(310 과정). 이때, 제1난수를 포함하는 암호문은 소스 클라이언트의 아이디를 포함하고, 제2난수를 포함하는 암호문은 소스 클라이언트의 아이디, 타겟 클라이언트의 아이디를 포함할 수 있다.
- <47> 다음, 서버에서 타겟 클라이언트에 제2난수를 포함하는 암호문을 전송한다(320 과정). 이때, 서버는 제2난수를 포함하는 암호문에 존재하는 클라이언트의 아이디 즉, 타겟 클라이언트의 아이디에 따라 암호문을 전송해줄 클라이언트를 선택한다.
- <48> 제2난수를 포함하는 암호문이 타겟 클라이언트에 전달되면, 타겟 클라이언트의 스마트 카드에서 임의의 난수인 제3난수 및 제4난수를 선택한 후, 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출하고, 제2난수 및 제4난수를 이용하여 세션키를 연산한다(330 과정).
- <49> 세션키가 연산되면, 제3난수 및 제4난수를 포함하는 암호문을 소스 클라이언트에 전송한다(340 과정).
- <50> 마지막으로, 소스 클라이언트의 스마트카드에서 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 제2난수 및 제4난수를 이용한 세션키를 연산하여 세션키를 공유한다(350 과정).
- <51> 도 4는 본 발명의 또다른 실시 예에 따른 스마트 카드를 이용한 삼자간 키 교환 방법의 흐름도이다.
- <52> 먼저, 소스 클라이언트의 스마트카드에서 임의의 난수인 제1난수 및 제2난수를 선택한 후, 제2난수를 포함하는 암호문을 서버에 전송하고, 제1난수를 포함하는 암호문을 타겟 클라이언트에 전송한다(410 과정). 이때, 제1난수를 포함하는 암호문은 소스 클라이언트의 아이디를 포함하고, 제2난수를 포함하는 암호문은 소스 클라이언트의 아이디, 타겟 클라이언트의 아이디를 포함할 수 있다.
- <53> 다음, 서버에서 타겟 클라이언트에 제2난수를 포함하는 암호문을 전송한다(420 과정). 이때, 서버는 제2난수를 포함하는 암호문에 존재하는 클라이언트의 아이디 즉, 타겟 클라이언트의 아이디에 따라 암호문을 전송해줄 클라이언트를 선택한다.
- <54> 제2난수를 포함하는 암호문이 타겟 클라이언트에 전달되면, 타겟 클라이언트의 스마트 카드에서 임의의 난수인 제3난수 및 제4난수를 선택한 후, 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출하고, 제2난수 및 제4난수를 이용하여 세션키를 연산한다(430 과정).
- <55> 세션키가 연산되면, 제3난수 및 제4난수를 포함하는 암호문을 소스 클라이언트에 전송한다(440 과정). 이때, 제3난수 및 제4난수를 포함하는 암호문은 타겟 클라이언트에서 연산된 세션키로 제1난수를 암호화한 암호문을 포함한다.
- <56> 다음, 소스 클라이언트에서 연산된 세션키로 제1난수를 암호화한 암호문을 복호화한 결과가 제1난수와 일치하지 않으면(445 과정), 타겟 클라이언트와의 프로토콜을 종료한다.
- <57> 제1난수를 암호화한 암호문을 복호화한 결과가 제1난수와 일치하면, 소스 클라이언트의 스마트카드에서 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 제2난수 및 제4난수를 이용한 세션키를 연산한다(450 과정).
- <58> 다음, 소스 클라이언트에서 제3난수 및 제4난수를 포함하는 암호문을 복호화하여 산출된 제3난수를 소스 클라이언트에서 연산된 세션키로 암호화한 암호문을 타겟 클라이언트에 전송한다(460 과정).
- <59> 마지막으로, 제3난수를 암호화한 암호문을 타겟 클라이언트에서 연산된 세션키로 복호화한 결과가 제3난수와 일치하지 않으면(465 과정), 타겟 클라이언트에서 연산된 세션키를 삭제한다(469 과정). 이때, 암호문을 타겟 클라이언트에서 연산된 세션키로 복호화한 결과가 제3난수와 일치하면, 소스 클라이언트 및 타겟 클라이언트에서 연산된 세션키가 동일한 것으로 판단하고, 소스 클라이언트 및 타겟 클라이언트가 비밀통신을 수행할 수 있다.
- <60> 도 5는 본 발명의 또다른 실시 예에 따른 스마트 카드를 이용한 삼자간 키 교환 방법의 흐름도이다.
- <61> 먼저, 소스 클라이언트 및 타겟 클라이언트가 각각의 패스워드를 서버에 등록한다.
- <62> 다음, 서버는 패스워드를 등록한 클라이언트들에게 스마트카드를 발급한다(501 과정). 이때, 소스 클라이언트는

서버로부터 소스 클라이언트의 아이디 및 서버의 마스터키를 해쉬함수에 적용한 제1검증자가 저장된 스마트 카드를 발급받고, 타겟 클라이언트는 서버로부터 타겟 클라이언트의 아이디 및 서버의 마스터키를 해쉬함수에 적용한 제2검증자가 저장된 스마트 카드를 발급받는다.

- <63> 다음, 인증을 수행하고자 하는 클라이언트 즉, 소스 클라이언트에 패스워드가 입력되면, 입력된 패스워드를 이용하여 연산된 검증자가 제1검증자와 일치하는지 판단한다(502 과정).
- <64> 이때, 입력된 패스워드를 이용하여 연산된 검증자가 제1검증자와 일치하면, 소스 클라이언트의 스마트카드에서 임의의 난수인 제1난수 및 제2난수를 선택한 후, 제2난수를 포함하는 암호문을 서버에 전송하고, 제1난수를 포함하는 암호문을 타겟 클라이언트에 전송한다(510 과정). 이때, 입력된 패스워드를 이용하여 연산된 검증자가 제1검증자와 일치하지 않으면, 모든 절차를 종료한다.
- <65> 다음, 서버에서 타겟 클라이언트에 제2난수를 포함하는 암호문을 전송한다(520 과정).
- <66> 제2난수를 포함하는 암호문이 타겟 클라이언트에 전달되면, 타겟 클라이언트의 스마트 카드에서 임의의 난수인 제3난수 및 제4난수를 선택한 후, 제2난수를 포함하는 암호문을 복호화하여 제2난수를 산출하고, 제2난수 및 제4난수를 이용하여 세션키를 연산한다(530 과정).
- <67> 세션키가 연산되면, 제3난수 및 제4난수를 포함하는 암호문을 소스 클라이언트에 전송한다(540 과정).
- <68> 마지막으로, 소스 클라이언트의 스마트카드에서 제3난수 및 제4난수를 포함하는 암호문을 복호화하고, 제2난수 및 제4난수를 이용한 세션키를 연산하여 세션키를 공유한다(550 과정).
- <69> 도 6은 도 3에서 암호문 중계 과정(320 과정)의 상세 흐름도이다.
- <70> 먼저, 서버에서 제1검증자를 이용하여 제2난수를 포함하는 암호문을 복호화하여 제2난수, 소스 클라이언트의 아이디 및 타겟 클라이언트의 아이디를 산출한다(621 과정).
- <71> 다음, 서버에서 제2검증자로 제2난수를 암호화한 암호문을 생성한다(622 과정).
- <72> 마지막으로, 제2난수를 암호화한 암호문을 타겟 클라이언트에 전송한다(623 과정). 타겟 클라이언트의 스마트카드에는 제2검증자가 저장되어 있으므로, 서버로부터 정상적으로 스마트카드를 발급받은 타겟 클라이언트는 제2검증자로 제2난수를 암호화한 암호문을 복호화할 수 있다.
- <73> 도 7은 도 4의 과정을 각 라운드별로 도시한 것이다.

<74> 이하에서, A, B는 클라이언트들의 아이디, S는 서버의 아이디를 나타낸다. PW_A 는 클라이언트 A의 패스워드이다. 또한, $SE=(K,E,D)$ 는 대칭키 암호알고리즘이고, $ASE=(PK,PE,PD)$ 는 공개키 암호알고리즘. $K(PK)$ 는 키 생성 알고리즘이고, $E(PE)$ 는 암호화 알고리즘, $D(PD)$ 는 복호화 알고리즘이다. H 는 암호학적으로 안전한 일방향 해쉬함수이다.

<75> 또한, 상술한 제1검증자 및 제2검증자는 각각 v_A, v_B 에 대응된다. 또한, 제1난수, 제2난수, 제3난수 및 제4난수는 각각 n_A, r_A, n_B, r_B 에 대응된다.

<76> 도 7에 도시된 과정을 수행하기 이전에 다음과 같은 등록 단계를 선행할 수 있다.

<77> 즉, 클라이언트 A가 서버 S로부터 스마트카드를 발급받을 때, 자신의 패스워드를 등록한다. 서버는 $PW_A = H(A \| pw_A)$, $v_A = H(A \| x_s)$ 그리고 $w_A = v_A \oplus PW_A$ 를 연산 후, 스마트카드에 (A, v_A, w_A) 키 생성에 필요한 알고리즘들 (SE, ASE, H)을 저장하여 이것을 A에게 발급한다. 여기서 x_s 는 서버의 마스터 키 값이다.

<78> 도 7에 도시된 과정을 수행하기 이전에 다음과 같은 인증 단계를 선행할 수 있다.

<79> 클라이언트 A가 클라이언트 B와 세션 키를 교환하고자 할 경우, A는 자신의 스마트카드를 카드리더기에 삽입 후, 스마트카드 발급 시에 등록했던 패스워드를 입력한다. 입력한 패스워드를 PW'_A 라 하자. 이때, 스마트카드

리더기를 스마트카드가 탑재된 모바일 기기로 생각할 수 있다.

- <80> 스마트카드는 클라이언트가 입력한 패스워드 정보가 일치하는지 확인하기 위해, $PW'_A = H(A \parallel pw'_A)$ 그리고 $v'_A = w_A \oplus PW'_A$ 를 연산한다. 그리고 $v'_A = v_A$ 인지 확인한다. 만약 두 값이 일치하지 않으면 동작을 멈춘다. 만약 이 단계를 통과하면 키 교환을 수행한다.
- <81> 라운드 1에서, 클라이언트 A의 스마트카드는 임의의 난수 $n_A, r_A \in \{0,1\}^l$ 를 선택한다. 그리고 일회용 공개키/비밀키 쌍 (y, x) 를 선택한다. A는 S에게 $A \parallel B \parallel E_{v_A}(A \parallel B \parallel r_A)$ 를 그리고 B에게 $A \parallel n_A \parallel x$ 값들을 전송한다.
- <82> 라운드 2에서, S는 $v_A = H(A \parallel x_s)$ 를 연산 후에 A에게서 받은 암호문 $E_{v_A}(A \parallel B \parallel r_A)$ 을 복호화 한다. 그 복호화 결과에 $A \parallel B$ 가 포함되어 있는지 확인한다. 그리고 $v_B = H(B \parallel x_s)$ 를 연산한 후, $A \parallel E_{v_B}(r_A)$ 를 B에게 전송한다.
- <83> 한편, B의 스마트카드는 임의의 난수 $n_B, r_B \in \{0,1\}^l$ 를 선택 후, $E_{v_B}(r_A)$ 를 복호화하여 r_A 값을 얻는다. 그리고 세션키 값 $sk = H(A \parallel B \parallel r_A \parallel r_B)$ 을 연산한 후, $n_B \parallel PE_y(r_B) \parallel E_{sk}(n_A + 1)$ 를 A에게 전송한다.
- <84> 라운드 3에서, A의 스마트카드는 $D_{sk}(E_{sk}(n_A + 1)) = n_A + 1$ 인지를 확인한다. 만약 두 값이 같지 않으면 프로토콜을 종료한다. 만약 두 값이 일치하면 A는 B와 동일한 세션 키를 공유했다는 것을 확인할 수 있다. 라운드 3에서, A의 스마트카드는 $PE_y(r_B)$ 를 복호화하여 r_B 를 얻는다. 그리고 세션 키 $sk = H(A \parallel B \parallel r_A \parallel r_B)$ 를 연산한다. A는 $E_{sk}(n_B + 1)$ 를 B에게 전송한다. B는 $D_{sk}(E_{sk}(n_B + 1)) = n_B + 1$ 가 일치하는지 확인한다. 만약 두 값이 일치하면 B는 A와 동일한 세션 키를 공유했다는 것을 확인할 수 있다. 만약 두 값이 일치하지 않으면, B의 스마트카드는 세션 키 sk를 사용하지 않고 삭제한다.
- <85> 한편, 클라이언트 A가 스마트카드에 접근하기 위해 사용하는 패스워드를 변경하고 싶을 경우, A는 스마트카드를 스마트 카드리더기에 삽입 후, 이전 패스워드 PW_A 와 새로 바꾸고자하는 패스워드 PW_A^{new} 를 입력한다. 스마트카드는 입력된 PW_A 를 이용하여 $PW'_A = H(A \parallel PW_A)$ 를 연산한 후, $v'_A = w_A \oplus PW'_A$ 를 연산한다. 그리고 $v'_A = v_A$ 인지를 확인한다. 만약 두 값이 일치하지 않으면, 패스워드 변경요청을 거절한다.
- <86> 만약 두 값이 일치하면, $PW_A^{new} = H(A \parallel PW_A^{new})$ 와 $w_A^{new} = w_A \oplus PW'_A \oplus PW_A^{new} = v_A \oplus PW_A^{new}$ 를 연산 후에 스마트카드 내에 저장된 w_A 값을 w_A^{new} 값으로 교체한다.
- <87> 본 발명에서 사용자가 스마트카드를 사용할 권한이 있는지에 대한 여부를 확인하기 위해 사용자는 패스워드 정보를 입력하게끔 되어 있다. 이 단계를 통과한 사용자들인 경우에 키 교환 단계를 수행할 수 있다.
- <88> 인증 및 키 교환 단계에서 각 클라이언트는 자신이 소유하고 있는 스마트카드를 이용해서 공통된 세션 키를 교환할 수 있다. 스마트카드 내에는 클라이언트만의 비밀 값들이 저장되어 있고, 각 클라이언트는 이 값을 이용하여 세션 키를 공유하게 된다. 이때, 두 클라이언트 간에는 공통적인 비밀 값이 없기 때문에, 각 클라이언트들의 비밀 값들을 모두 알고 있는 서버가 중간에서 키 교환을 도와주는 매개체 역할을 하게 된다.
- <89> 이에 따라, 본 발명은 클라이언트-클라이언트 간 인증 및 키 교환을 가능하게 한다.
- <90> 한편, 서버는 마스터 키 값을 알고 있는 개체이므로, 서버를 신뢰기관이라 가정한다. 비록 두 클라이언트간의 인증 및 키 교환을 위해 신뢰된 제 3기관(서버)이 중간에 매개자의 역할을 하지만, 두 클라이언트 간에 교환되는 데이터를 보고는 세션 키에 대한 정보를 알 수 없도록 한다. 이것은 서버에 대한 신뢰 의존도를 낮출 수 있

도록 한다. 본 발명에서 서버는 클라이언트 A가 선택한 임의의 난수 r_A 를 알 수는 있지만 A의 일회용 공개키 y_A 에 대응되는 비밀키 x_A 를 알 수 없기 때문에 암호문 $PEy(r_B)$ 로부터 B가 선택한 임의의 난수 r_B 를 알 수 없다.

결과적으로 세션키 $sk = H(A || B || r_A || r_B)$ 에 대한 정보를 얻을 수 없다.

<91> 이에 따라, 본 발명은 서버가 클라이언트들 간에 교환된 세션 키 정보를 알 수 없도록 한다.

<92> 또한, 본 발명은 데이터의 교환 횟수를 3번 이하로 제한할 수 있다.

<93> 표 1은 논문에 발표된 종래 기술들과 본 발명의 비교표이다.

<94> 표 1에서 본 발명은 두 클라이언트가 인증 및 세션 키를 교환하기 위해서는 3번의 데이터 교환이 필요하며, 클라이언트 A와 B는 서로가 동일한 세션 키를 연산하였는지에 대한 여부도 확인할 수 있다.

표 1

Scheme		Jaung's schemes [5]		본 발명
		Scheme1	Scheme2	SKE
Round		5	5	3
# of random number	Server	0	0	0
	User	2	2	2
Exp.	Server	0	0	0
	User	0	2	A:1 Exp(PD) B:1 Exp(PE)
Symm. Enc. Dec. fun.	Server	4	4	2
	User	4	4	2
Hash fun.	Server	1	1	2
	User	2	2	1
Size of messages	Server	2	2	
	User	A:3 B:6	A:3 B:6	A:3 + y B:2 + PE
Security		KI	KI & FS	KI & FS

<95>

<96> 종래 기술들에서 본 발명과 같은 안전성을 제공하는 기술은 Jaung의 Scheme2이지만, 이 기술은 5번의 데이터 교환 횟수가 필요하다. 본 발명과 같이 데이터 교환 횟수를 줄일 수 있다면, 더 빠른 인증 및 키 교환을 수행할 수 있다.

<97> 본 발명은 스마트카드 발급 개체인 서버를 클라이언트-클라이언트 간 인증 및 키 교환을 가능하게 도와주는 매개체로 이용하여 두 클라이언트가 간접적으로 인증 및 키 교환을 할 수 있는 기술이다.

<98> 본 발명에서는 서버의 개입이 요구되지만 서버의 신뢰 의존도를 낮추기 위해, 서버가 클라이언트 간에 교환되는 데이터를 보고는 두 클라이언트가 공유한 세션 키를 알 수 없게 한다. 그리고 인증 및 키 교환을 수행하는 과정에서 데이터의 교환 횟수를 3번으로 감소시켜 효율적으로 두 개체가 빠르게 키 교환을 수행할 수 있게 한다.

<99> 바람직하게는, 본 발명의 스마트 카드를 이용한 삼자간 키 교환 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다.

<100> 본 발명은 소프트웨어를 통해 실행될 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

<101> 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다.

<102> 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<103> 본 발명은 도면에 도시된 일 실시예를 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서

통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시예의 변형이 가능하다는 점을 이해할 것이다. 그러나, 이와 같은 변형은 본 발명의 기술적 보호범위내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

발명의 효과

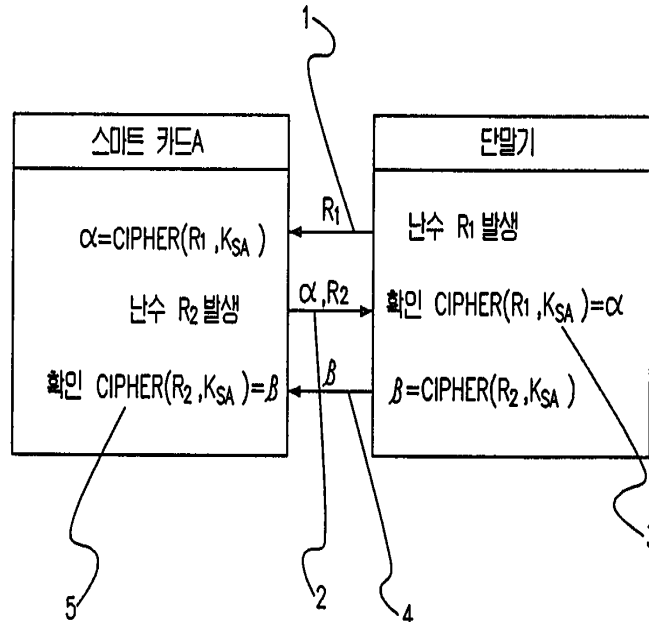
<104> 상술한 바와 같이, 본 발명에 의하면, 클라이언트-클라이언트 간 인증 및 키 교환을 가능하게 하고, 서버가 클라이언트들 간에 교환된 세션 키 정보를 알 수 없도록 하여 보안성을 향상시킬 수 있으며, 키 교환을 위한 데이터의 교환 횟수를 3번 이하로 제한할 수 있고, 스마트 카드를 이용하면서도 고속의 인증이 가능하며, 키 교환을 하는 클라이언트 간에 서로가 동일한 세션 키를 연산하였는지에 대한 여부도 확인할 수 있는 효과가 있다.

도면의 간단한 설명

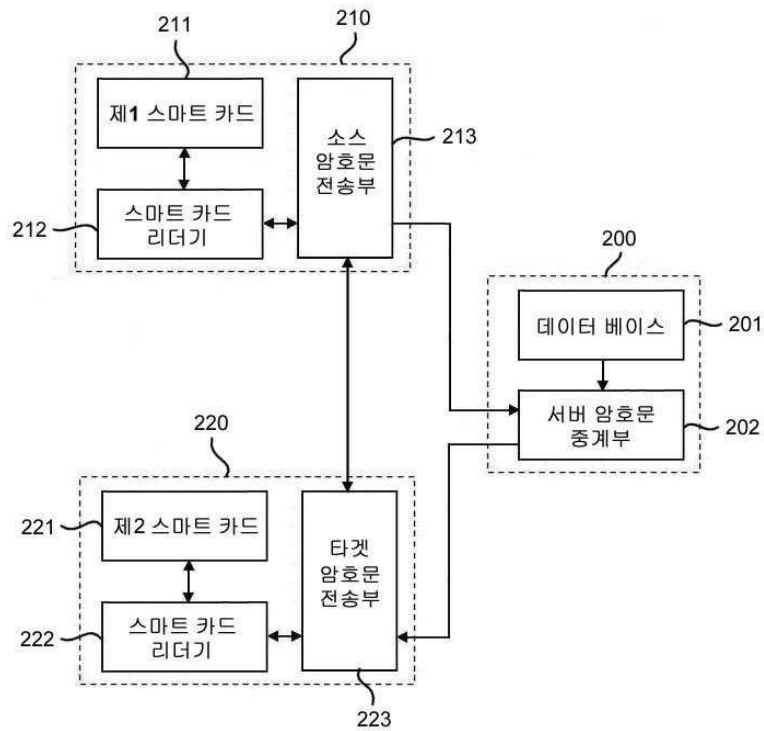
- <1> 도 1은 종래의 스마트카드/단말간의 상호 인증 방법을 도시한 것이다.
- <2> 도 2는 본 발명의 일 실시 예에 따른 스마트 카드를 이용한 삼자간 키 교환 시스템의 블록도이다.
- <3> 도 3은 본 발명의 다른 실시 예에 따른 스마트 카드를 이용한 삼자간 키 교환 방법의 흐름도이다.
- <4> 도 4는 본 발명의 또다른 실시 예에 따른 스마트 카드를 이용한 삼자간 키 교환 방법의 흐름도이다.
- <5> 도 5는 본 발명의 또다른 실시 예에 따른 스마트 카드를 이용한 삼자간 키 교환 방법의 흐름도이다.
- <6> 도 6은 도 3에서 암호문 중계 과정의 상세 흐름도이다.
- <7> 도 7은 도 4의 과정을 각 라운드별로 도시한 것이다.

도면

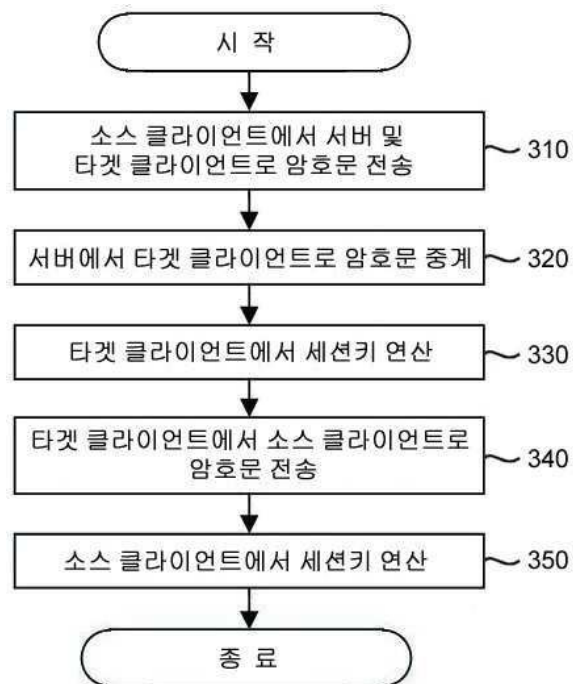
도면1



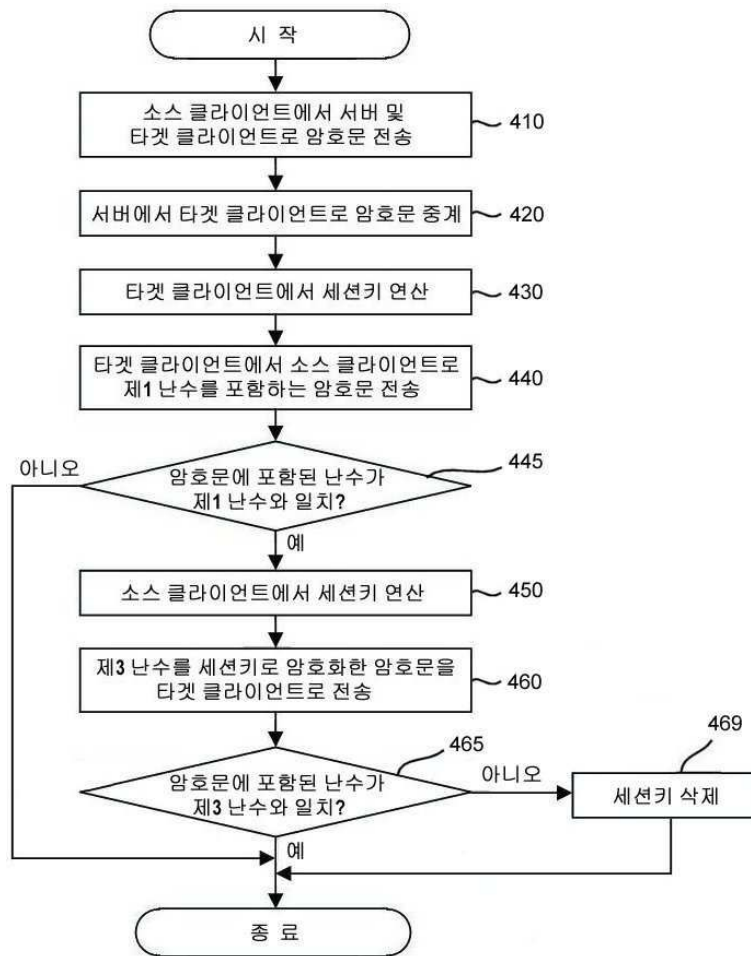
도면2



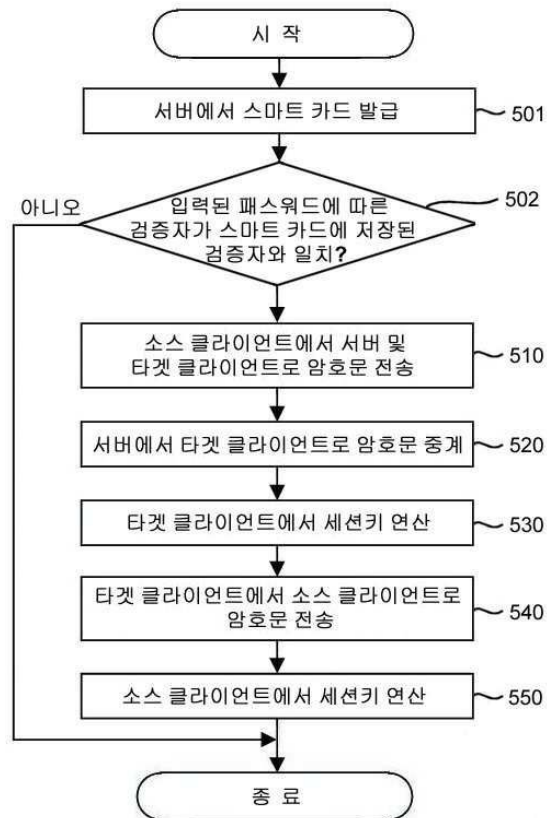
도면3



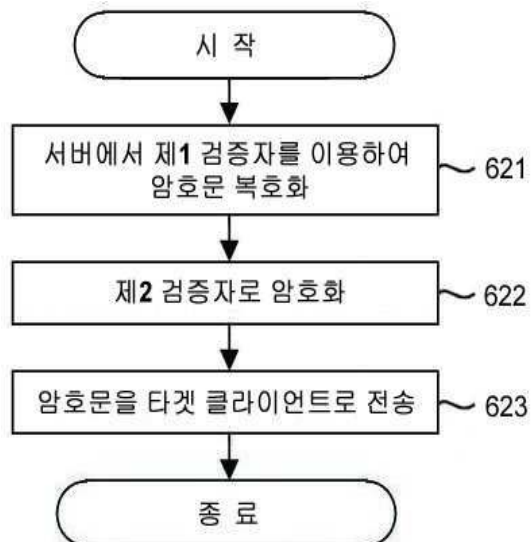
도면4



도면5



도면6



도면7

