



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0077500
(43) 공개일자 2008년08월25일

(51) Int. Cl.

H04L 9/32 (2006.01) H04L 9/30 (2006.01)

H04L 9/12 (2006.01)

(21) 출원번호 10-2007-0017124

(22) 출원일자 2007년02월20일

심사청구일자 2007년02월20일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

김범한

서울 송파구 방이1동 130-16호 201호

홍중욱

서울 동대문구 용두동 740-10 삼영오피스텔 103호

(뒷면에 계속)

(74) 대리인

현중철

전체 청구항 수 : 총 11 항

(54) 가시검증 가능한 키 교환 장치, 신뢰된 인증 기관을 이용한가시검증 가능한 키 교환 시스템, 그 방법 및 기록매체

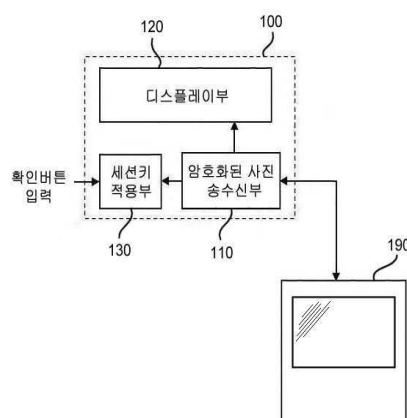
(57) 요약

가시검증 가능한 키 교환 장치, 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 시스템, 그 방법 및 기록매체가 개시된다.

본 발명은 암호화된 사용자의 사진을 다른 사용자의 단말에 전송하고, 상기 다른 사용자의 단말로부터 상기 다른 사용자의 암호화된 사진을 수신하는 암호화된 사진 송수신부; 상기 다른 사용자의 사진을 화면으로 표시하는 디스플레이부; 및 상기 사용자와 상기 다른 사용자가 상대방의 사진을 확인하여 확인 버튼을 누르면, 상기 사용자의 사진 및 상기 다른 사용자의 사진을 이용하여 생성된 세션키를 상기 사용자의 단말과 상기 다른 사용자의 단말 사이의 통신에 적용하는 세션키 적용부를 포함한다.

본 발명에 의하면, 키 교환을 수행하는 사용자의 사진을 그 사용자의 아이디로 사용함으로써, 사용자 아이디에 대한 익명성을 보장하는 것은 물론이고 키 교환을 마친 사용자는 올바른 상대방과 키 교환을 수행하였다는 것을 가시적으로 검증할 수 있으며, 사용자의 대표 사진을 등록시키고 관리하는 신뢰된 인증기관을 유지한다면 상대방에 대한 정당성도 확보할 수 있고, 특히 신뢰된 인증기관이 있는 방법은 인터넷 환경에서 제3의 신뢰된 인증기관의 운영과 각 사용자의 대표사진에 대한 등록 및 제거가 용이하여 화상이 지원되는 근거리 이동통신 및 VOIP 환경에서 유용하다.

대표도 - 도1



(72) 발명자

백정하

서울 송파구 가락동 금호아파트 105동 802호

이동훈

경기 고양시 일산동구 정발산동 밤가시마을 901동
201호

임종인

서울 종로구 내수동 95 삼성파크팰리스 101- 901

특허청구의 범위

청구항 1

암호화된 사용자의 사진을 다른 사용자의 단말에 전송하고, 상기 다른 사용자의 단말로부터 상기 다른 사용자의 암호화된 사진을 수신하는 단계; 및

상기 사용자와 상기 다른 사용자가 상대방의 사진을 확인하면, 상기 사용자의 사진 및 상기 다른 사용자의 사진을 이용하여 생성된 세션키를 상기 사용자의 단말과 상기 다른 사용자의 단말 사이의 통신에 적용하는 단계를 포함하는 가시검증 가능한 키 교환 방법.

청구항 2

제 1 항에 있어서,

상기 암호화된 사진을 수신하는 단계는

상기 사용자의 단말의 임의의 수 x 를 생성자 g 에 지수를 취한 g^x 를 상기 다른 사용자의 단말에 전송하고, 상기 다른 사용자의 단말의 임의의 수 y 를 생성자 g 에 지수를 취한 g^y 를 상기 사용자의 단말에 전송하는 단계;

상기 임의의 수 x 와 g^y 를 이용하여 생성된 암호화 인자 K 로 상기 사용자의 사진을 암호화하여 상기 다른 사용자의 단말에 전송하는 단계; 및

상기 다른 사용자의 단말에서 생성된 암호화 인자 K 로 상기 사용자의 사진을 복호화하고, 상기 다른 사용자의 사진을 상기 암호화 인자 K 로 암호화하여 상기 사용자의 단말에 전송하는 단계를 포함하는 것을 특징으로 하는 가시검증 가능한 키 교환 방법.

청구항 3

제 1 항에 있어서,

상기 통신에 적용하는 단계는

상기 사용자의 단말과 상기 다른 사용자의 단말에 상대방의 사진을 표시하는 단계; 및

상기 사용자의 단말과 상기 다른 사용자의 단말에서 확인 버튼을 누르면, 상기 사용자와 상기 다른 사용자가 상대방의 사진을 확인한 것으로 판단하는 단계를 포함하는 것을 특징으로 하는 가시검증 가능한 키 교환 방법.

청구항 4

키 생성 센터에 등록되어 있는 사용자들의 단말에 사용자들의 사진의 해쉬값을 전송하는 단계;

제2사용자의 단말로부터 수신된 상기 제2사용자의 사진의 해쉬값에 임의의 수를 곱한 값과 제1사용자의 사진의 해쉬값에 임의의 수를 곱한 값을 해쉬 함수에 대입한 암호화 인자를 생성하는 단계;

상기 암호화 인자를 이용하여 상기 제1사용자의 사진을 암호화한 제1메시지를 상기 제2사용자의 단말에 전송하는 단계;

상기 제1메시지를 이용하여 상기 암호화 인자를 생성하여 상기 제1사용자의 사진을 복호화하고, 상기 제2사용자의 사진을 상기 암호화 인자로 암호화한 제2메시지를 상기 제1사용자의 단말에 전송하는 단계; 및

상기 제1사용자와 상기 제2사용자가 상대방의 사진을 확인하면, 상기 제1사용자의 사진 및 상기 제2사용자의 사진을 이용하여 생성된 세션키를 상기 제1사용자의 단말과 상기 제2사용자의 단말 사이의 통신에 적용하는 단계를 포함하는 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법.

청구항 5

제 4 항에 있어서,

상기 사용자들의 사진의 해쉬값을 전송하는 단계는

상기 키 생성 센터에서 상기 제1사용자의 사진의 해쉬값 Q_A 와 상기 제2사용자의 사진의 해쉬값 Q_B 을 상기 제1사용자의 단말과 상기 제2사용자의 단말에 각각 전송하는 단계를 포함하고,

상기 암호화 인자를 생성하는 단계는

상기 제2사용자의 단말에서 선택된 임의의 수 r_B 를 상기 Q_B 에 곱한 $r_B Q_B$ 를 상기 제1사용자의 단말에 전송하는 단계; 및

상기 제1사용자의 단말에서 선택된 임의의 수 r_A 를 상기 Q_A 와 곱한 $r_A Q_A$ 와 상기 $r_B Q_B$ 를 해쉬 함수에 대입한 값 h 를 이용하여 암호화 인자를 생성하는 단계를 포함하는 것을 특징으로 하는 신뢰된 인증 기관을 이용한 가시 검증 가능한 키 교환 방법.

청구항 6

제 5 항에 있어서,

상기 Q_A 및 Q_B 는

타원 곡선상의 좌표인 것을 특징으로 하는 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법.

청구항 7

제 4 항에 있어서,

상기 통신에 적용하는 단계는

상기 제1사용자의 단말과 상기 제2사용자의 단말에 상대방의 사진을 표시하는 단계; 및

상기 제1사용자의 단말과 상기 제2 사용자의 단말에서 확인 버튼을 누르면, 상기 제1사용자와 상기 제2사용자가 상대방의 사진을 확인한 것으로 판단하는 단계를 포함하는 것을 특징으로 하는 신뢰된 인증 기관을 이용한 가시 검증 가능한 키 교환 방법.

청구항 8

제 5 항에 있어서,

상기 통신에 적용하는 단계는

상기 제1사용자와 상기 제2사용자가 상대방의 사진을 확인하면, 상기 암호화 인자가 K 이고, 해쉬 함수가 H_2 인 경우, 암호화 통신 및 인증을 위한 MAC 키의 마스터키로 세션키 $SK = H_2(ID_A, ID_B, r_A Q_A, r_B Q_B, K)$ 를 사용하는 단계를 포함하는 것을 특징으로 하는 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법.

청구항 9

제 1 항 내지 제 8 항 중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 10

암호화된 사용자의 사진을 다른 사용자의 단말에 전송하고, 상기 다른 사용자의 단말로부터 상기 다른 사용자의 암호화된 사진을 수신하는 암호화된 사진 송수신부;

상기 다른 사용자의 사진을 화면으로 표시하는 디스플레이부; 및

상기 사용자와 상기 다른 사용자가 상대방의 사진을 확인하여 확인 버튼을 누르면, 상기 사용자의 사진 및 상기 다른 사용자의 사진을 이용하여 생성된 세션키를 상기 사용자의 단말과 상기 다른 사용자의 단말 사이의 통신에

적용하는 세션키 적용부를 포함하는 가시검증 가능한 키 교환 장치.

청구항 11

등록되어 있는 제1사용자 및 제2사용자의 단말에 사용자들의 사진의 해쉬값을 전송하는 키 생성 센터를 포함하고,

상기 제1사용자의 단말은

상기 제2사용자의 단말로부터 수신된 상기 제2사용자의 사진의 해쉬값에 임의의 수를 곱한 값과 제1사용자의 사진의 해쉬값에 임의의 수를 곱한 값을 해쉬 함수에 대입한 암호화 인자를 생성하는 암호화 인자 생성부;

상기 암호화 인자를 이용하여 상기 제1사용자의 사진을 암호화한 제1메시지를 상기 제2사용자의 단말에 전송하는 제1메시지 전송부; 및

상기 제1사용자가 상대방의 사진을 확인하면, 상기 제1사용자의 사진 및 상기 제2사용자의 사진을 이용하여 생성된 세션키를 상기 제2사용자의 단말과의 통신에 적용하는 세션키 적용부를 포함하고,

상기 제2사용자의 단말은

상기 제1메시지를 이용하여 상기 암호화 인자를 생성하는 암호화 인자 생성부;

상기 암호화 인자를 이용하여 상기 제1사용자의 사진을 복호화하고, 상기 제2사용자의 사진을 상기 암호화 인자로 암호화한 제2메시지를 상기 제1사용자의 단말에 전송하는 제2메시지 전송부; 및

상기 제2사용자가 상대방의 사진을 확인하면, 상기 제1사용자의 사진 및 상기 제2사용자의 사진을 이용하여 생성된 세션키를 상기 제1사용자와의 통신에 적용하는 세션키 적용부를 포함하는 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 시스템.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

- <9> 본 발명은 암호 프로토콜에 관한 것으로, 특히, 가시검증 가능한 키 교환 장치, 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 시스템, 그 방법 및 기록매체에 관한 것이다.
- <10> 최근 블루투스, IEEE 802.11과 더불어 고속 근거리 무선통신 표준인 UWB(Ultra Wideband) 및 무선 USB 등의 통신 기술이 개발되고 UMPC, PDA, 휴대폰 등의 초소형 기기의 발전으로 장소의 제약 없이 기기간 멀티미디어, 비즈니스 정보 등의 교환을 위한 근거리 무선통신 환경이 각광받고 있다. 근거리 무선 네트워크란 각 노드들이 AP와 같은 중계기 혹은 중앙서버의 도움없이 기기간에 직접적으로 통신하는 네트워크를 말한다.
- <11> 이러한 무선통신 기술은 시간과 장소의 구애없이 고속으로 데이터를 주고받을 수 있는 장점을 가지고 있지만, 무선 네트워크의 특성상 도청, 중간자 공격, 가장 공격 등의 공격에 매우 취약하다. 또한, 전통적인 유선 네트워크와 달리 근거리 무선통신에서 사용자의 ID 등이 노출되면 사용자의 위치 정보가 노출되어 프라이버시를 침해하는 문제가 발생할 수 있다.
- <12> 이러한 문제를 해결하기 위해 근거리 무선 네트워크 환경에서 여러 가지 공격에 안전한 프로토콜이 제시되었다. PKI(Public Key Infrastructure)를 기반으로 하는 프로토콜은 초기에 양 사용자가 서로의 공개키가 포함된 인증서를 교환하고 서로의 공개키를 이용해서 임의의 난수를 암호화하고 이에 대한 서명을 교환하여 인증된 키교환을 수행한다. 하지만, PKI 기반 키교환 방식은 여러 가지 문제점을 가지고 있다. 첫째, 인증서의 검증을 위해서는 추가적으로 망에 접속해야 하므로 애드혹 네트워크라는 가정에 위반한다. 둘째, 인증서에 담겨있는 사용자 정보가 노출되므로 PKI 기반의 키교환은 근본적으로 익명성을 제공하지 않는다. 최근 널리 사용되고 있는 ID 기반의 키교환 방식에서는 인증서를 사용하지 않는 대신 ID를 공개키로 사용하지만, 프로토콜 세션 설립 초기에 인증 및 키교환을 위해 서로의 ID를 교환해야 하므로 이 방법 역시 익명성을 제공하지 못한다.
- <13> Pasini 등은 사람이 기억가능한 짧은 단어를 세션설립 시점에서 공유하고 이를 이용하여 인증된 키교환을 설계

하였다. 이 방법은 사전에 유한 짧은 문자와 랜덤값을 이용하여 Commit을 교환한 후 각각을 Open하여 서로 같은 문자를 공유하였는지 검증한다. Pasini 등의 방법은 짧은 문자를 사용하여도 사전공격에 안전하여 긴 패스워드 만큼의 안전성을 보장하며 중재자공격 등에 안전하다. 하지만 프로토콜 시작 시점에서 양 사용자간에 추가적으로 서로간의 비밀정보의 짧은 문자를 공유해야 하는 단점을 가지고 있다.

<14> Barreto 등은 거리기반의 인증된 키교환 방법을 제안하였다. 이 방법에서는 양 사용자간에 사전에 공유하는 비밀정보 없이 세션설립 시점에서 서로간의 거리정보를 인증요소로 하여 인증된 키교환을 수행한다. 사용자간 키정보를 1비트로 나누어 k번 전송하여 이때의 통신시간에 대한 확인을 하여 양 기기간의 통신에 다른 기기가 개입하지 않았음을 검증한다. 이 방법은 사용자간 사전에 공유하는 정보가 전혀 없는 장점이 있지만 항상 동일한 물리적 공간에서 키교환을 해야하므로 이동성을 제공해주지 못하며 제안된 방법이 통신 프로토콜에 종속적인 단점이 있다.

<15> McCune 등은 "Seeing is Believing"이라는 양자간 인증된 키교환 방법을 제안하였다. 이 방법에서는 사용자간 사전에 공유하는 정보가 필요없는 대신에 키교환 시점에서 상대방 기기에 디스플레이되는 이차원바코드를 사진으로 찍어서 인증정보로 이용한다. 이 방법에서는 사전에 공유해야 하는 비밀값이 없으며 이동성 및 익명성을 보장하지만, 해당 기기에 반드시 카메라가 있어야 하는 기기적인 제약이 있으며 사용자에게 매우 큰 불편함을 초래한다.

<16> 따라서, 종래의 인증된 키 교환 방법들은 세션 설립 이전에 비밀정보를 공유해야 하는 불편함이 있고, 근거리 이동통신 및 VOIP 환경에서 이동성, 익명성 등이 제공되지 않으며, 키 교환을 위해 기기적인 제약을 수반하는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

<17> 따라서, 본 발명이 이루고자 하는 첫번째 기술적 과제는 세션 설립 이전에 비밀정보를 공유할 필요가 없고, 근거리 이동통신 및 VOIP 환경에서 이동성, 익명성 등이 제공하며, 키 교환을 위해 기기적인 제약을 수반하지 않으면서 사람이 직접 검증할 수 있는 가시검증 가능한 키 교환 장치를 제공하는 데 있다.

<18> 본 발명이 이루고자 하는 두번째 기술적 과제는 세션 설립 이전에 비밀정보를 공유할 필요가 없고, 근거리 이동통신 및 VOIP 환경에서 이동성, 익명성 등이 제공하며, 키 교환을 위해 기기적인 제약을 수반하지 않으면서 사람이 직접 검증할 수 있는 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 시스템을 제공하는 데 있다.

<19> 본 발명이 이루고자 하는 세번째 기술적 과제는 상기의 가시검증 가능한 키 교환 장치에 적용된 가시검증 가능한 키 교환 방법을 제공하는 데 있다.

<20> 본 발명이 이루고자 하는 네번째 기술적 과제는 상기의 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 시스템에 적용된 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법을 제공하는 데 있다.

<21> 본 발명이 이루고자 하는 다섯번째 기술적 과제는 상기의 가시검증 가능한 키 교환 방법 및 상기의 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 데 있다.

발명의 구성 및 작용

<22> 상기의 첫번째 기술적 과제를 이루기 위하여, 본 발명은 암호화된 사용자의 사진을 다른 사용자의 단말에 전송하고, 상기 다른 사용자의 단말로부터 상기 다른 사용자의 암호화된 사진을 수신하는 암호화된 사진 송수신부; 상기 다른 사용자의 사진을 화면으로 표시하는 디스플레이부; 및 상기 사용자와 상기 다른 사용자가 상대방의 사진을 확인하여 확인 버튼을 누르면, 상기 사용자의 사진 및 상기 다른 사용자의 사진을 이용하여 생성된 세션 키를 상기 사용자의 단말과 상기 다른 사용자의 단말 사이의 통신에 적용하는 세션키 적용부를 포함하는 가시검증 가능한 키 교환 장치를 제공한다.

<23> 상기의 두번째 기술적 과제를 이루기 위하여, 본 발명은 등록되어 있는 제1사용자 및 제2사용자의 단말에 사용자들의 사진의 해쉬값을 전송하는 키 생성 센터를 포함하고, 상기 제1사용자의 단말은 상기 제2사용자의 단말로부터 수신된 상기 제2사용자의 사진의 해쉬값에 임의의 수를 곱한 값과 제1사용자의 사진의 해쉬값에 임의의 수를 곱한 값을 해쉬 함수에 대입한 암호화 인자를 생성하는 암호화 인자 생성부; 상기 암호화 인자를 이용하여 상기 제1사용자의 사진을 암호화한 제1메시지를 상기 제2사용자의 단말에 전송하는 제1메시지 전송부; 및 상기 제1사용자가 상대방의 사진을 확인하면, 상기 제1사용자의 사진 및 상기 제2사용자의 사진을 이용하여 생성된

세션키를 상기 제2사용자의 단말과의 통신에 적용하는 세션키 적용부를 포함하고, 상기 제2사용자의 단말은 상기 제1메시지를 이용하여 상기 암호화 인자를 생성하는 암호화 인자 생성부; 상기 암호화 인자를 이용하여 상기 제1사용자의 사진을 복호화하고, 상기 제2사용자의 사진을 상기 암호화 인자로 암호화한 제2메시지를 상기 제1사용자의 단말에 전송하는 제2메시지 전송부; 및 상기 제2사용자가 상대방의 사진을 확인하면, 상기 제1사용자의 사진 및 상기 제2사용자의 사진을 이용하여 생성된 세션키를 상기 제1사용자와의 통신에 적용하는 세션키 적용부를 포함하는 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 시스템을 제공한다.

- <24> 상기의 세번째 기술적 과제를 이루기 위하여, 본 발명은 암호화된 사용자의 사진을 다른 사용자의 단말에 전송하고, 상기 다른 사용자의 단말로부터 상기 다른 사용자의 암호화된 사진을 수신하는 단계; 및 상기 사용자와 상기 다른 사용자가 상대방의 사진을 확인하면, 상기 사용자의 사진 및 상기 다른 사용자의 사진을 이용하여 생성된 세션키를 상기 사용자의 단말과 상기 다른 사용자의 단말 사이의 통신에 적용하는 단계를 포함하는 가시검증 가능한 키 교환 방법을 제공한다.
- <25> 상기의 네번째 기술적 과제를 이루기 위하여, 본 발명은 키 생성 센터에 등록되어 있는 사용자들의 단말에 사용자들의 사진의 해쉬값을 전송하는 단계;
- <26> 제2사용자의 단말로부터 수신된 상기 제2사용자의 사진의 해쉬값에 임의의 수를 곱한 값과 제1사용자의 사진의 해쉬값에 임의의 수를 곱한 값을 해쉬 함수에 대입한 암호화 인자를 생성하는 단계; 상기 암호화 인자를 이용하여 상기 제1사용자의 사진을 암호화한 제1메시지를 상기 제2사용자의 단말에 전송하는 단계; 상기 제1메시지를 이용하여 상기 암호화 인자를 생성하여 상기 제1사용자의 사진을 복호화하고, 상기 제2사용자의 사진을 상기 암호화 인자로 암호화한 제2메시지를 상기 제1사용자의 단말에 전송하는 단계; 및 상기 제1사용자와 상기 제2사용자가 상대방의 사진을 확인하면, 상기 제1사용자의 사진 및 상기 제2사용자의 사진을 이용하여 생성된 세션키를 상기 제1사용자의 단말과 상기 제2사용자의 단말 사이의 통신에 적용하는 단계를 포함하는 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법을 제공한다.
- <27> 상기의 다섯번째 기술적 과제를 이루기 위하여, 본 발명은 상기의 가시검증 가능한 키 교환 방법 및 상기의 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.
- <28> 본 발명에서는 근거리 무선네트워크 환경 및 화상이 지원되는 VOIP에서 인증 및 암호화 통신 시 필요한 키 교환을 설계한다. 본 발명에 명시된 키 교환 방법은 사전에 비밀정보를 공유할 필요가 없으며 익명성을 제공하고, 근거리 무선네트워크 환경의 경우 이동성도 제공한다. 무엇보다도 사람이 키 교환이 올바르게 이루어졌는지에 대한 여부와 상대방에 대한 정당성의 여부를 가시적으로 검증가능 하게 지원한다.
- <29> 본 발명은 상대방의 얼굴을 키 교환을 하는 장소에서 직접 확인 가능한 정도의 근거리와 상대방의 얼굴을 화상으로 확인할 수 있는 근거리 이동통신 및 VOIP 환경에서 동일하게 적용 가능하다. 자신의 사진을 아이디로 사용하고 프로토콜이 진행되는 중간 과정에 임시로 설정된 비밀키로 사진을 주고 받아 최종적으로 사용하고자 하는 비밀키 생성에 사용하고, 사람이 가시적으로 검증 가능하게 지원한다.
- <30> 이하에서는 도면을 참조하여 본 발명의 바람직한 실시 예를 설명하기로 한다. 그러나, 다음에 예시하는 본 발명의 실시 예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시 예에 한정되는 것은 아니다.
- <31> 본 발명은 신뢰된 인증기관의 존재 여부에 따라 2가지 방법으로 나눌 수 있다.
- <32> 도 1은 신뢰된 인증기관이 없는 경우에, 가시검증 가능한 키 교환 장치(100)의 블록도이다.
- <33> 암호화된 사진 송수신부(110)는 암호화된 사용자의 사진을 다른 사용자의 단말에 전송하고, 다른 사용자의 단말(190)로부터 다른 사용자의 암호화된 사진을 수신한다.
- <34> 디스플레이부(120)는 수신된 다른 사용자의 사진을 화면으로 표시한다.
- <35> 세션키 적용부(130)는 사용자와 다른 사용자가 상대방의 사진을 확인하여 확인 버튼을 누르면, 사용자의 사진 및 다른 사용자의 사진을 이용하여 생성된 세션키를 사용자의 단말과 다른 사용자의 단말 사이의 통신에 적용한다.
- <36> 한편, 다른 사용자의 단말(190)도 암호화된 사진 송수신부(110), 디스플레이부(120), 세션키 적용부(130) 등의 구성요소를 포함한다.

- <37> 도 2는 신뢰된 인증 기관이 있는 경우에, 가시검증 가능한 키 교환 시스템의 블록도이다.
- <38> 키 생성 센터(200)는 등록되어 있는 제1사용자의 단말(210) 및 제2사용자의 단말(220)에 사용자들의 사진의 해쉬값을 전송한다.
- <39> 제1사용자의 단말(210)은 사진 해쉬값 송수신부(211), 암호화 인자 생성부(212), 제1메시지 전송부(213) 및 세션키 적용부(214)를 포함한다.
- <40> 사진 해쉬값 송수신부(211)는 키 생성 센터(200)로부터 사진의 해쉬값을 수신한다. 또한, 사진 해쉬값 송수신부(211)는 자신의 사진의 해쉬값을 상대방과 송수신한다.
- <41> 암호화 인자 생성부(212)는 제2사용자의 단말(220)로부터 수신된 제2사용자의 사진의 해쉬값에 임의의 수를 곱한 값과 제1사용자의 사진의 해쉬값에 임의의 수를 곱한 값을 해쉬 함수에 대입한 암호화 인자를 생성한다.
- <42> 제1메시지 전송부(213)는 암호화 인자를 이용하여 제1사용자의 사진을 암호화한 제1메시지를 제2사용자의 단말(220)에 전송한다.
- <43> 세션키 적용부(214)는 제1사용자가 상대방의 사진을 확인하면, 제1사용자의 사진 및 제2사용자의 사진을 이용하여 생성된 세션키를 제2사용자의 단말(220)과의 통신에 적용한다.
- <44> 제2사용자의 단말(220)은 사진 해쉬값 송수신부(221), 암호화 인자 생성부(222), 제1메시지 전송부(223) 및 세션키 적용부(224)를 포함한다.
- <45> 사진 해쉬값 송수신부(221)는 키 생성 센터(200)로부터 사진의 해쉬값을 수신한다. 또한, 사진 해쉬값 송수신부(221)는 자신의 사진의 해쉬값을 상대방과 송수신한다.
- <46> 암호화 인자 생성부(222)는 제1메시지를 이용하여 암호화 인자를 생성한다.
- <47> 제2메시지 전송부(223)는 암호화 인자를 이용하여 제1사용자의 사진을 복호화하고, 제2사용자의 사진을 암호화 인자로 암호화한 제2메시지를 제1사용자의 단말(210)에 전송한다.
- <48> 세션키 적용부(224)는 제2사용자가 상대방의 사진을 확인하면, 제1사용자의 사진 및 제2사용자의 사진을 이용하여 생성된 세션키를 제1사용자와의 통신에 적용한다.
- <49> 도 3은 본 발명에 따른 가시검증 가능한 키 교환 방법의 흐름도이다.
- <50> 먼저, 암호화된 사용자의 사진을 다른 사용자의 단말에 전송한다(310 과정).
- <51> 다음, 다른 사용자의 단말로부터 다른 사용자의 암호화된 사진을 수신한다(320 과정).
- <52> 암호화된 사진의 송수신이 완료되고 사용자와 다른 사용자가 상대방의 사진을 확인하는지 판단한다(330 과정).
- <53> 상대방의 사진을 확인하면, 사용자의 사진 및 다른 사용자의 사진을 이용하여 생성된 세션키를 사용자의 단말과 다른 사용자의 단말 사이의 통신에 적용한다(340 과정). 이때, 화면에 표시된 상대방의 사진을 보고 인증을 거부하는 등 상대방의 사진이 확인되지 않으면, 모든 과정을 종료한다. 이 과정(340 과정)은 사용자의 단말과 다른 사용자의 단말에 상대방의 사진을 표시하는 과정, 사용자의 단말과 다른 사용자의 단말에서 확인 버튼을 누르면, 사용자와 다른 사용자가 상대방의 사진을 확인한 것으로 판단하는 과정을 포함할 수 있다. 이때, 사진을 확인하였음을 알리는 수단은 확인 버튼 이외에, 음성 입력, 지문 입력, 터치 스크린에 터치 입력 등을 포함할 수 있다.
- <54> 도 4는 도 3의 과정의 일 예를 도시한 것이다.
- <55> 상대방의 실제 얼굴 IDorg, 상대방의 기기에 표시된 아이디(얼굴 이미지) IDpre, 상대방이 보낸 아이디가 IDimg 일때, HVerify 함수를 다음과 같이 정의한다.
- <56> $IDorg \neq IDpre = IDimg$ 인 경우, $HVerify(IDpre, IDimg, IDorg)$ 는 ACCEPT를 출력하며, 그렇지 않은 경우 REJECT를 출력한다.
- <57> 두 사용자가 자신의 사진만 가지고 있으면 가시적으로 검증 가능한 인증된 키 교환을 수행할 수 있다. 키 교환이 완료되면 사용자는 상대방과 상대방의 사진을 눈으로 대조하여 해당하는 상대방과 올바르게 키 교환이 수행되었다는 것을 직접 검증한다.
- <58> 키 교환 과정을 설명하면, 다음과 같다.

- <59> 먼저, 사용자 A는 임의의 수 x 를 위수가 q 인 곱셈 연산군 G 의 생성자 g 에 지수를 취한 g^x 를 키교환 상대인 사용자 B에게 전송한다.
- <60> 다음, 사용자 B도 역시 임의의 수 y 를 선택하여 g^y 를 사용자 A에게 전송한다.
- <61> 다음, 사용자 B로부터 전송 받은 g^y 에 자신이 만든 x 를 지수로 취해 암호화 인자 $K=g^{xy}$ 를 생성한다. 이 K 를 이용하여 자신의 아이디 ID_A 를 암호화하여 사용자 B에게 전송한다.
- <62> 마지막으로, 사용자 B는 전송받은 값을 이용하여 K 를 생성하고, ID_A 를 복호화하고, 자신의 아이디 ID_B 를 K 로 암호화하여 A에게 전송한다.
- <63> 이때, 검증 과정은 다음과 같다.
- <64> HVerify 함수를 이용하여 양 사용자가 동의하는 경우 양사용자는 세션키 $SK=H(ID_A, ID_B, g^x, g^y, K)$ 로 사용한다.
- <65> 도 5는 본 발명에 따른 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법의 흐름도이다.
- <66> 먼저, 키 생성 센터에 등록되어 있는 사용자들의 단말에 사용자들의 사진의 해쉬값을 전송한다(510 과정).
- <67> 다음, 제2사용자의 단말로부터 수신된 제2사용자의 사진의 해쉬값에 임의의 수를 곱한 값과 제1사용자의 사진의 해쉬값에 임의의 수를 곱한 값을 해쉬 함수에 대입한 암호화 인자를 생성한다(520 과정).
- <68> 다음, 암호화 인자를 이용하여 제1사용자의 사진을 암호화한 제1메시지를 제2사용자의 단말에 전송한다(530 과정).
- <69> 제2사용자의 단말이 제1메시지를 수신하면, 제1메시지를 이용하여 암호화 인자를 생성하여 제1사용자의 사진을 복호화하고, 제2사용자의 사진을 암호화 인자로 암호화한 제2메시지를 제1사용자의 단말에 전송한다(540 과정).
- <70> 다음, 제1사용자와 제2사용자가 상대방의 사진을 확인하는지 판단한다(550 과정).
- <71> 상대방의 사진을 확인하면, 제1사용자의 사진 및 제2사용자의 사진을 이용하여 생성된 세션키를 제1사용자의 단말과 제2사용자의 단말 사이의 통신에 적용한다. 이때, 화면에 표시된 상대방의 사진을 보고 인증을 거부하는 등 상대방의 사진이 확인되지 않으면, 모든 과정을 종료한다.
- <72> 도 6은 도 5의 과정의 일 예를 도시한 것이다.
- <73> 사용자는 자신의 대표사진을 신뢰된 인증기관에 등록하고 대표사진으로 키 교환을 수행한다. 키 교환이 완료되면 사용자는 상대방과 상대방의 사진을 눈으로 대조하여 해당하는 상대방과 올바르게 키 교환이 수행된 여부와 상대방에 대한 인증 여부를 직접 검증한다.
- <74> 이 방법은 키 생성 센터(Key Generation Center, KGC)안에 소속된 사용자간의 키교환 방법으로, 자신의 아이디로 사용될 대표 사진을 KGC에 등록을 한 사용자간의 키교환으로 자신이 만난 사용자와 올바른 키교환을 수행하였다는 것과 KGC에 등록된 올바른 사용자 ID를 사용하여 키교환을 하였다는 것을 보장해 주기 때문에, 사용자 ID 자체를 인증해 준다. 즉, KGC에 등록된 올바른 사용자라는 것을 인증한다. 사용자 ID를 인증해 주기 때문에 인증된 아이디를 다른 어플리케이션에서도 사용할 수 있다.
- <75> 키 설정 과정은 다음과 같다. KGC는 바이리니어 맵 그룹(bilinear map group) G_1, G_2 를 선택한다. 이때, 이 그룹들의 위수는 q 이다. 바이리니어 맵 $e: G_1 \times G_1 \rightarrow G_2$ 이고, G_1 의 생성자는 P 이다. KGC에 등록되어 있는 사용자들에게 사용자의 아이디 이미지의 해쉬값 $H_1(ID)=QID$ 에 KGC의 마스터 키 s 를 곱한 $sQID=dID$ 를 안전하게 전송한다.
- <76> 키 교환 과정은 다음과 같다.
- <77> 먼저, 사용자 B는 자신의 아이디의 해쉬값인 Q_B 와 임의의 수 r_B 를 곱한 $r_B Q_B$ 를 키 교환 상대인 사용자 A에게

전송한다.

<78> 다음, 사용자 A도 역시 자신의 아이디의 해쉬 값 Q_A 와 임의의 수 r_A 를 선택하여 $r_A Q_A$ 를 생성한다. 사용자 B로부터 전송 받은 $r_B Q_B$ 와 자신이 만든 $r_A Q_A$ 를 해쉬 함수 H1에 대입하여 $h=H1(r_A Q_A, r_B Q_B)$ 를 연산하고, 암호화 인자 $K=e(hd_{ID_A}, r_B Q_B)^{r_A}$ 를 생성한다. 이 K를 이용하여 자신의 아이디 ID_A 를 암호화한 $E_K(ID_A)$ 와 $r_A Q_A$ 를 사용자 B에게 전송한다.

<79> 예를 들어, Q_A 및 Q_B 는 타원 곡선상의 좌표로 정의할 수 있다.

<80> 마지막으로, 사용자 B는 전송받은 값을 이용하여 K를 연산하고, ID_A 를 복호화하고, 자신의 아이디 ID_B 를 K로 암호화하여 A에게 전송한다.

<81> 최종적인 검증 과정은 다음과 같다. 전송받은 ID, 실제 상대방의 모습 및 인증정보를 입력값으로 하여 앞서 정의한 Verify 함수를 이용하여 모든 값이 정당한지 판단한다. Verify가 성공한다면 전송받은 ID를 공개키로 갖는 상대방이 인증 값을 보냈음을 확신할 수 있다. 양 사용자가 검증을 거치게 되면 이후의 암호화 통신 및 인증을 위한 MAC키의 마스터키로 세션키 $SK=H_2(ID_A, ID_B, r_A Q_A, r_B Q_B, K)$ 를 사용한다. 이때, H2는 해쉬 함수를 나타낸다.

<82> 위장 공격의 경우, 본 발명에 따르면, 키 교환의 양 사용자에게 사전 정보가 전혀 없다. 본 발명에서는 자신의 사진을 아이디로 사용하는 경우에, 키 교환 상대방의 얼굴과 상대의 아이디 사진을 직접 눈으로 확인함으로써 올바른 사용자로 인증할 수 있게 된다.

<83> 도 7은 본 발명이 중재자 공격에 안전함을 나타낸 것이다.

<84> 중재자 공격의 경우, 본 발명에 따르면, 키 교환을 하는 양 사용자를 A, B라 하고 중재자 공격을 하는 공격자를 C라고 하면, 공격자 C는 A와 B가 통신을 하기 전에 먼저 각각 A, B와 통신을 시작하여 도 7과 같이 공격을 할 수 있다. 그러나, 검증 과정에서 이미지의 확인에 실패하므로, 중재자 공격을 막을 수 있다.

<85> 무선 환경에서의 통신은 사용기간 데이터를 쉽게 도청할 수 있으므로, 통신상에 사용자가 사용하는 아이디가 전송되면 안된다. 본 발명은 사용자의 사진 아이디를 암호화하여 전송하므로, 사용자의 익명성이 보장된다.

<86> 도 8a 내지 도 8d에서, 두 사용자는 각자의 단말기를 가지고 근거리에서 상대방과 가시검증 가능한 키교환을 시도한다.

<87> 도 8a에서, 각 사용자가 프로그램을 구동시키면, 프로그램은 필요한 라이브러리 및 변수를 초기화 한다. 어느 한쪽에서 연결을 시도하면 본 발명에 따른 키 교환 방법이 진행된다.

<88> 도 8b에서, 본 발명의 절차가 완료되면 상대방의 사진이 자신의 단말기 화면에 출력되어 상대방의 실제 얼굴과 대조가 가능하게 된다.

<89> 도 8c에서, 자신이 키교환한 상대방이 사진과 일치함을 확인하고, 연결설정을 수락하면 교환된 키를 사용하여 암호화 채팅 및 암호화된 파일 전송이 가능해진다.

<90> 도 8d는 Miracl 라이브러리의 연산 수행 속도를 포켓 피씨(PocketPC)에서 테스트한 화면이다.

<91> 바람직하게는, 본 발명의 가시검증 가능한 키 교환 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다.

<92> 바람직하게는, 본 발명의 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다.

<93> 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.

<94> 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. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<95> 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

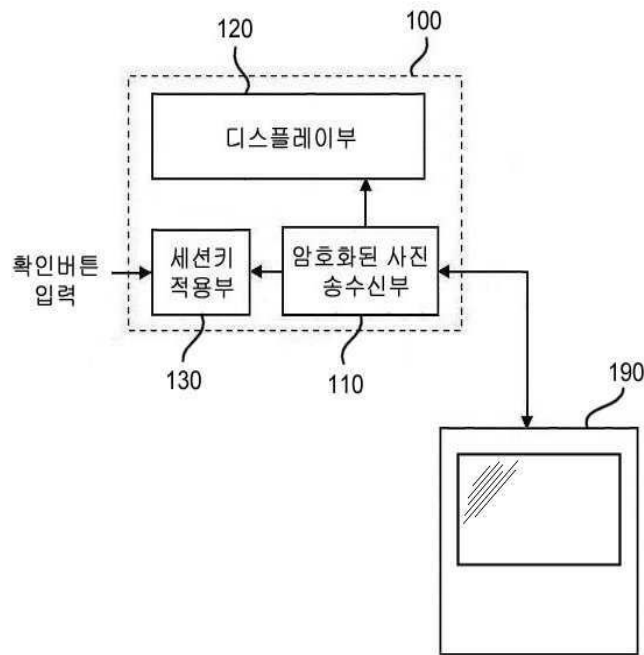
<96> 상술한 바와 같이, 본 발명에 의하면, 키 교환을 수행하는 사용자의 사진을 그 사용자의 아이디로 사용함으로써, 사용자 아이디에 대한 익명성을 보장하는 것은 물론이고 키 교환을 마친 사용자는 올바른 상대방과 키 교환을 수행하였다는 것을 가시적으로 검증할 수 있으며, 사용자의 대표 사진을 등록시키고 관리하는 신뢰된 인증기관을 유지한다면 상대방에 대한 정당성도 확보할 수 있고, 특히 신뢰된 인증기관이 있는 방법은 인터넷 환경에서 제3의 신뢰된 인증기관의 운영과 각 사용자의 대표사진에 대한 등록 및 제거가 용이하여 화상이 지원되는 근거리 이동통신 및 VOIP 환경에서 유용한 효과가 있다.

도면의 간단한 설명

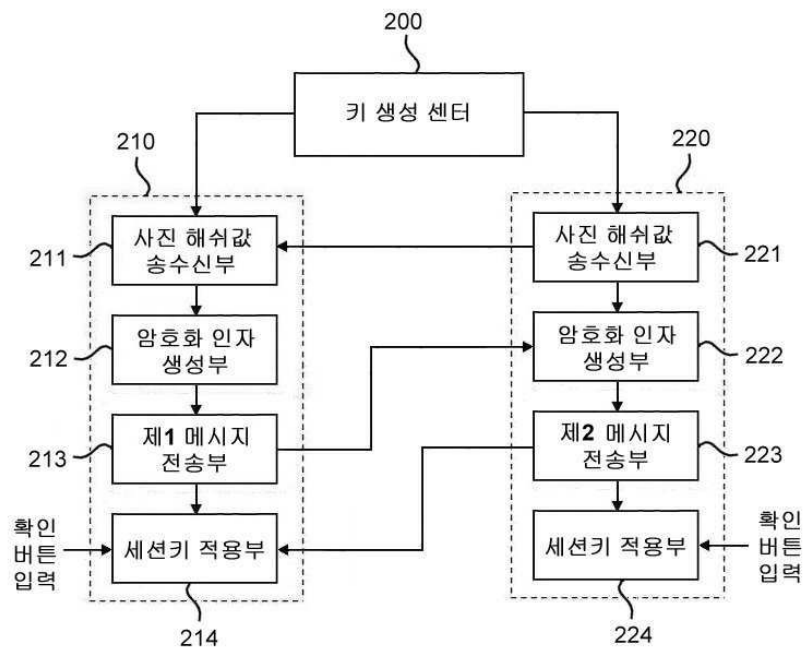
- <1> 도 1은 본 발명에 따른 가시검증 가능한 키 교환 장치의 블록도이다.
- <2> 도 2는 본 발명에 따른 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 시스템의 블록도이다.
- <3> 도 3은 본 발명에 따른 가시검증 가능한 키 교환 방법의 흐름도이다.
- <4> 도 4는 도 3의 과정의 일 예를 도시한 것이다.
- <5> 도 5는 본 발명에 따른 신뢰된 인증 기관을 이용한 가시검증 가능한 키 교환 방법의 흐름도이다.
- <6> 도 6은 도 5의 과정의 일 예를 도시한 것이다.
- <7> 도 7은 본 발명이 중재자 공격에 안전함을 나타낸 것이다.
- <8> 도 8a 내지 도 8d는 본 발명의 구현 예를 도시한 것이다.

도면

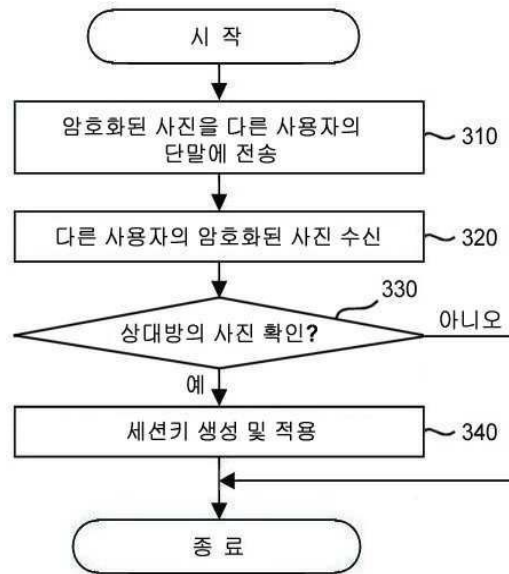
도면1



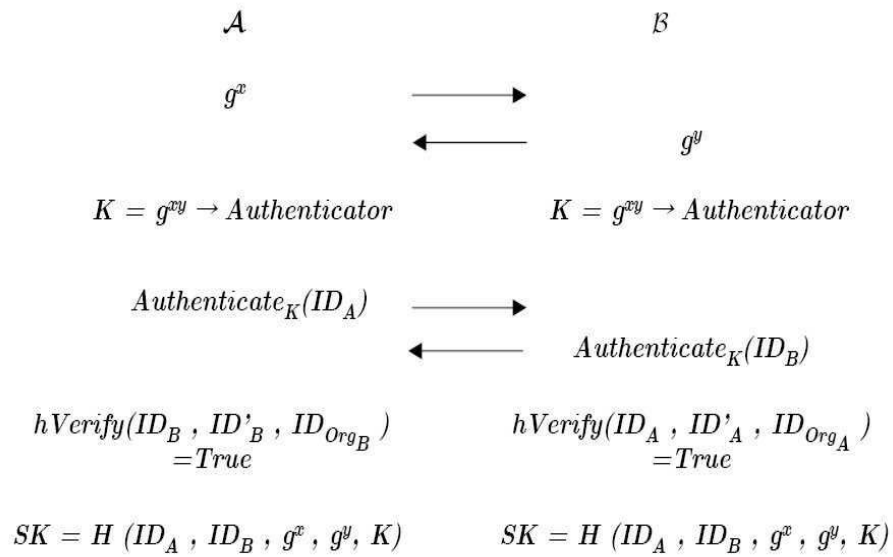
도면2



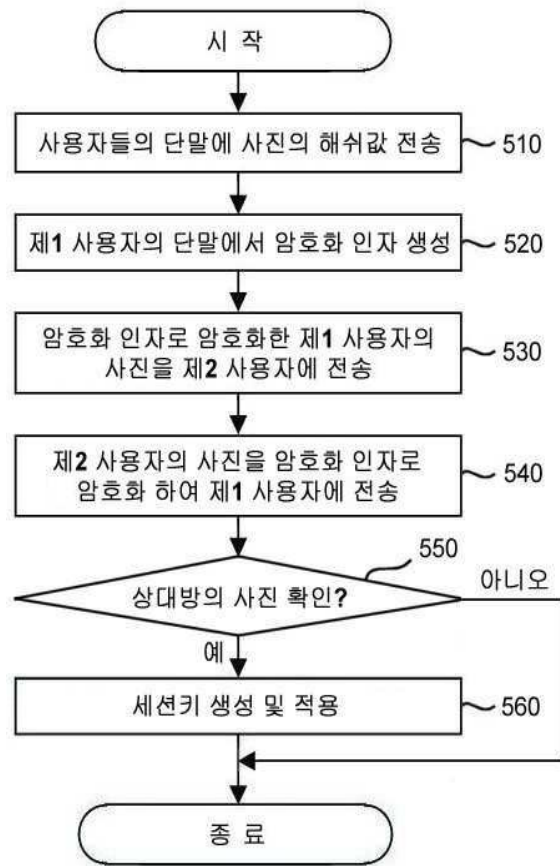
도면3



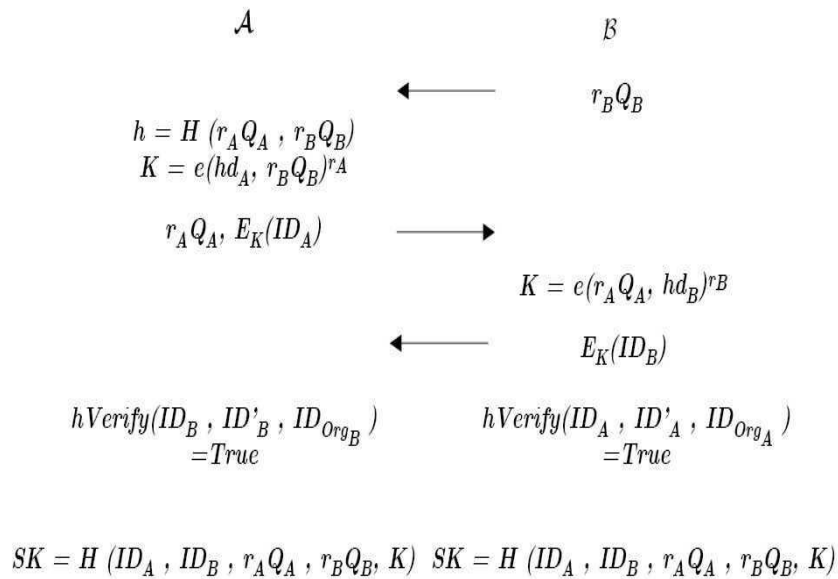
도면4



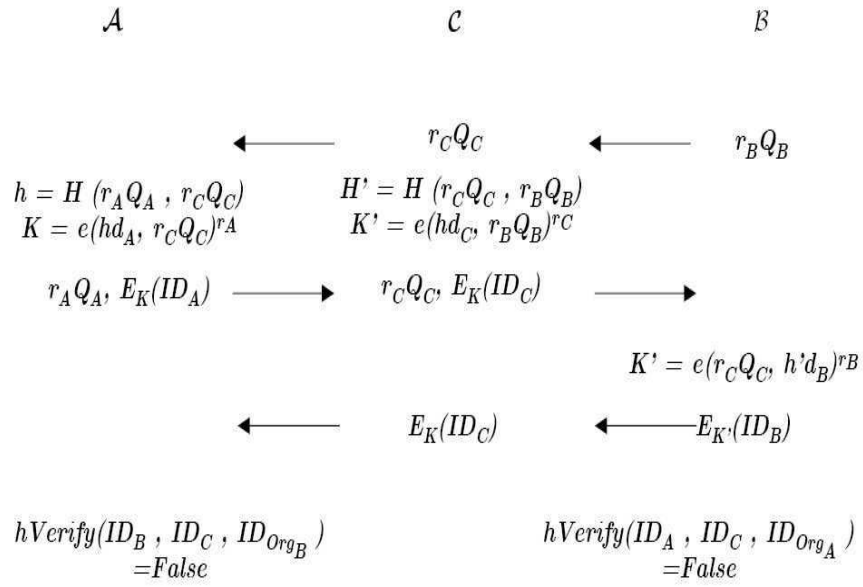
도면5



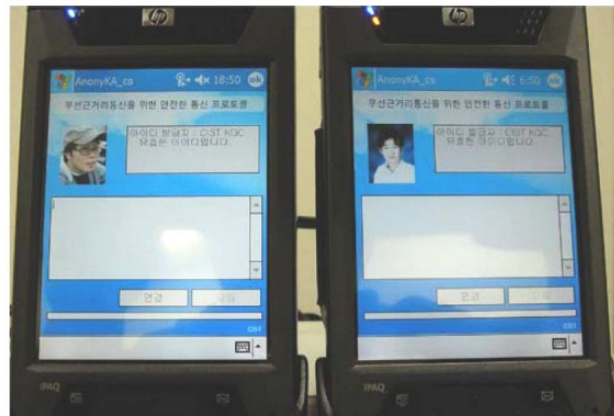
도면6



도면7



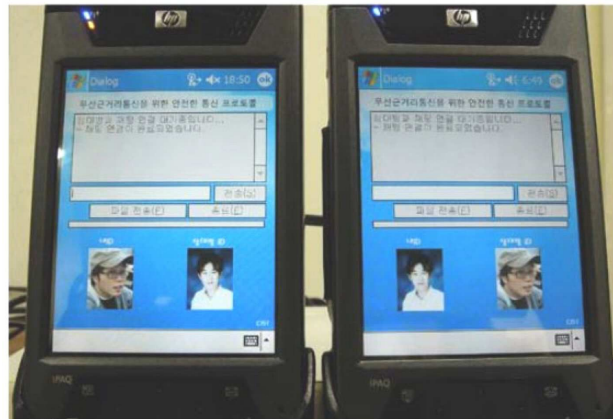
도면8a



도면8b



도면8c



도면 8d

