(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
G06F 17/60A2

(11) 공개번호 10-2004-0099943
(43) 공개일자 2004년12월02일

(21) 출원번호 10-2003-0032085
(22) 출원일자 2003년05월20일

(71) 출원인 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 최양림
경기도성남시분당구이매동124한신아파트210-1509

유용국
경기도수원시팔달구매탄동1239-9

남수현
서울특별시서초구방배2동435-26102호

장용진
경기도과천시중앙동23-6

김명선
경기도의왕시삼동우성4차아파트다동106호

(74) 대리인 김동진

심사청구 : 없음

(54) 컨텐츠 사용자 인증 시스템 및 방법

요약

본 발명은 정당한 사용자가 자신의 신분을 노출 시키지 않고 안전하게 컨텐츠를 제공받고, 불법 사용자에 의한 컨텐츠 사용을 방지하기 위한 인증 시스템 및 인증 방법에 관한 것이다.

본 발명의 일 실시예에 따른 컨텐츠 사용자 인증 방법은, 신뢰기관이 그룹 공통키를 생성하고 배포하는 제 1 단계; 사용자가 상기 그룹 공통키를 이용하여 상기 신뢰기관의 인증을 받는 제 2 단계; 상기 신뢰기관의 인증을 받은 사용자의 개인 정보 및 상기 인증된 사용자에게 발행된 임시 등록증을 상기 신뢰기관에 저장하는 제 3 단계; 상기 사용자가 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 소정의 변환 방법으로 변환하여 컨텐츠 제공자에게 제공하는 제 4 단계; 및 상기 컨텐츠 제공자가 상기 그룹 공통키를 이용하여 상기 변환된 임시 등록증을 제공한 상기 사용자에 대한 상기 신뢰기관의 인증 여부를 확인하고, 상기 확인에 따라 컨텐츠를 제공하는 제 5 단계를 포함한다.

대표도

도 7

색인어

컨텐츠, 인증, 익명화

명세서

도면의 간단한 설명

도 1은 종래에 사용자 신분 비밀 보장을 고려하지 않는 컨텐츠 제공 방식을 개념적으로 나타낸 것이다.

도 2는 종래에 익명화 장치(Anonymizer)를 이용하여 사용자 신분 보장을 고려하는 컨텐츠 제공 방식을 개념적으로 나타낸 것이다.

도 3은 본 발명에 따른 인증 시스템을 구성하는 요소를 개략적으로 나타낸 블록도이다.

도 4는 신뢰기관측의 장치의 구성요소 및 동작을 나타낸 블록도이다.

도 5는 사용자측의 장치의 구성요소 및 동작을 나타낸 블록도이다.

도 6은 컨텐츠 제공자측의 장치의 구성요소 및 동작을 나타낸 블록도이다.

도 7은 본 발명에 따른 인증 방법을 개략적으로 나타낸 흐름도이다.

도 8은 신뢰기관에 의한 키 생성과정을 나타낸 흐름도이다.

도 9는 사용자가 신뢰기관에 등록하는 과정을 나타낸 흐름도이다.

도 10은 컨텐츠 제공자가 사용자를 인증하는 과정을 나타낸 흐름도이다.

도 11은 컨텐츠 제공자가 컨텐츠를 생성하는 과정을 나타낸 흐름도이다.

도 12는 컨텐츠 제공자가 사용자의 신분을 확인하는 과정을 나타낸 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크 상의 다양한 컨텐츠를 이용하는 사용자를 인증하는 시스템 및 방법에 관한 것으로, 보다 상세하게는 정당한 사용자가 자신의 신분을 노출 시키지 않고 안전하게 컨텐츠를 제공받고, 불법 사용자에 의한 컨텐츠 사용을 방지하기 위한 인증 시스템 및 인증 방법에 관한 것이다.

인터넷을 비롯한 다양한 형태의 네트워크를 통해서 다양한 컨텐츠를 제공받는 사용자들은 통신상에 흐르는 정보의 비밀을 유지하기 위해서 다양한 암호화 기법을 사용하고 있으나 대부분의 경우 정당한 거래를 위해서는 자신의 신분에 대한 정보를 제공하여야 한다. 그러나 통신상의 데이터의 보호보다는 통신에 참여하는 개체의 신분의 기밀성 유지가 더욱 중요한 경우가 많다. 홈 네트워크의 경우에도 마찬가지로 사용자가 자신의 신분을 감추고 정당한 거래를 하고자 하는 경우를 쉽게 접할 수 있다.

종래에 컨텐츠 제공 기술은 크게 두 가지로 구분된다. 첫째는 도 1과 같이 컨텐츠 사용자의 신분의 비밀 보장을 고려하지 않는 경우이다. 이 경우에는 사용자 u_i의 홈 네트워크와 컨텐츠 제공자(CP; Content Provider)로 구성된다. 둘째는 도 2와 같이 컨텐츠 사용자의 신분을 보장하기 위해서 익명화 장치(anonymizer)를 이용한 경우이다. 이 경우는 컨텐츠 사용자 u_i의 모든 데이터로부터 사용자의 신분과 관련된 정 보의 추출을 방지하기 위한 방편의 하나로 익명화 장치(anonymizer) 서버를 컨텐츠 제공자와의 사이에 설치한다.

도 1의 경우 사용자의 신분은 암호화되지 않은 형태로 모든 트랜색션(Transaction)에서 노출된다. 그러나 컨텐츠 이용자와 사용자간의 트랜색션에 참여한 데이터는 적당한 암호학적 방법, 예컨대 관용 암호 기법이나 공개키 암호 기법 등을 사용하여 비밀이 보장되도록 할 수 있다. 도 2와 같은 시스템에서는 사용자의 모든 데이터가 익명화 장치를 경

유하여 외부와 통신 및 트랜색션이 이루어지기 때문에 익명화 장치를 통과한 데이터에 대해서는 컨텐츠 사용자의 신분의 익명성을 보장할 수 있다.

상기와 같은 종래 기술의 경우에는 사용자의 신분의 익명성을 보장하기 위한 방법이 존재하지 않거나, 존재한다 하더라도 그 방법이 암호학적으로 안전성이 보장되지 못하고 단순히 외부로 유출되는 데이터의 변경에 그치므로 한계가 있다. 익명화 장치를 이용하는 도 2의 경우에도 익명화 장치를 경유하기 이전의 데이터를 획득하는 경우라면 도 1에서와 마찬가지로 사용자의 신분을 간단하게 획득할 수 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 상기한 문제들을 해결하기 위하여 안출된 것으로서, 신뢰기관으로부터 인증된 사용자가 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 소정의 변환 방법으로 변환하여 컨텐츠 제공자에게 제공함으로써, 불필요한 개인 정보의 노출없이 컨텐츠 제공자에게 신뢰기관으로부터의 인증 여부를 확인받을 수 있는 컨텐츠 사용자 인증 시스템 및 방법을 제공하는데 있다.

발명의 구성 및 작용

상기의 목적을 달성하기 위하여, 본 발명의 일실시예에 따른 컨텐츠 사용자 인증 시스템은, 그룹 공통키를 생성하여 배포하고, 상기 그룹 공통키를 이용한 사용자를 인증하고, 상기 인증된 사용자의 개인 정보 및 상기 인증된 사용자에게 발행된 임시 등록증을 저장하는 신뢰기관; 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 소정의 변환 방법으로 변환하여 컨텐츠 제공자에게 제공하고 상기 컨텐츠 제공자가 제공하는 컨텐츠를 실행하는 사용자 장치; 및 상기 그룹 공통키를 이용하여, 상기 변환된 임시 등록증을 제공한 사용자에 대한 상기 신뢰기관의 인증 여부를 확인하고, 상기 확인에 따라 컨텐츠를 제공하는 컨텐츠 제공자를 포함한다.

또한, 상기의 목적을 달성하기 위하여, 본 발명의 일실시예에 따른 컨텐츠 사용자 인증 방법은, 신뢰기관이 그룹 공통키를 생성하고 배포하는 제 1 단계;사용자가 상기 그룹 공통키를 이용하여 상기 신뢰기관의 인증을 받는 제 2 단계; 상기 신뢰기관의 인증을 받은 사용자의 개인 정보 및 상기 인증된 사용자에게 발행된 임시 등록증을 상기 신뢰기관에 저장하는 제 3 단계; 상기 사용자가 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 소정의 변환 방법으로 변환하여 컨텐츠 제공자에게 제공하는 제 4 단계; 및 상기 컨텐츠 제공자가 상기 그룹 공통키를 이용하여 상기 변환된 임시 등록증을 제공한 상기 사용자에 대한 상기 신뢰기관의 인증 여부를 확인하고, 상기 확인에 따라 컨텐츠를 제공하는 제 5 단계를 포함한다.

도 3은 본 발명에 따른 인증 시스템을 구성하는 요소를 개략적으로 나타낸 블록도 이다. 본 도에서 보는 바와 같이 본 발명은 신뢰기관(400), 컨텐츠 사용자(500), 컨텐츠 제공자(600)의 상호작용에 의해서 이루어진다. 신뢰기관(400)은 먼저 컨텐츠 사용자(500)의 그룹에 의해서 사용될 그룹 공통키를 생성하고, 시스템에서 전역으로 사용될 시스템 파라미터들을 생성하여 공개하고 사용자 ID(개인 정보)를 데이터 베이스에 저장해 두었다가 불법 사용자 추적이나 요금 부과 등의 목적으로 사용자 정보를 파악할 필요가 있을 때 컨텐츠 제공자(600)와 합의하여 컨텐츠로부터 추출한 정보를 바탕으로 사용자 ID를 찾아낼 수 있는 기능을 갖는다. 사용자(500)는 신뢰기관(400)과 합의하에 자신의 임시 공개키와 비밀키 쌍을 생성하고 이후의 프로토콜에서 이용될 등록증을 발급받고, 그 등록증을 이용하여 컨텐츠 제공자(600)로부터 컨텐츠를 사용할 수 있도록 인증을 받고 컨텐츠를 수신 받아 사용할 수 있게 된다. 컨텐츠 제공자(600)는 사용자(500)가 자신이 해당 그룹의 정당한 사용자라는 것을 증명하면 사용자의 증명에 대하여 정당성을 검증한다. 또한 컨텐츠를 생성하고 그 컨텐츠에 암호화된 사용자 정보를 포함시킨 후 이를 해당 사용자(500)들에게 제공한다. 또한 신뢰기관(400)으로부터 암호화된 사용자 정보를 얻어 사용자를 확인할 수 있다.

도 4는 신뢰기관측 장치의 구성요소 및 동작을 나타낸 블록도이다. 신뢰기관측 장치(400)는 송수신부(450), 파라미터생성부(410), 인증부(420), 데이터 베이스(440) 및 제어부(430)로 구성될 수 있다. 상기 송수신부(450)는 사용자(500)가 전송하는 t값, 사용자 ID 및 a^{x} 값을 수신하고, 파라미터생성부(410)로부터 생성된 난수 β를 사용자(500)에게 전송하는 역할을 담당한다. 상기 파라미터생성부(410)는 모드 값 계산의 기준이 되는 n 값, 지수계산에 사용되는 지수 y, z값, 또 다른 소수 v값 및 임의의 난수 a, β 값을 생성하며, 공개되는 시스템 파라미터인 (n,v,a,Y,Z) 값을 생성하는 역할을 한다. 상기 인증부(420)는 컨텐츠 제공자(600)와의 합의하에 해당 컨텐츠 아이템에서 사용자에 대한 정보(사용자 ID)를 추출하고, 데이터 베이스에 저장된 등록자 테이블에서 R과 z값을 사용하여 사용자 ID를 얻는 역할을 한다. 상기 데이터 베이스는 상기 파라미터생성부(410)으로부터 생성된 각종 지수, 난수 및 파라미터를 저장하고, 사용자로부터 수신한 사용자 ID 및 사용자를 위한 임시 등록증에 해당하는 R 값을 등록한다. 또한 상기 제어부(430)는 상기 송수신부(450), 파라미터생성부(410), 인증부(420) 및 데이터베이스(440)의 동작을 제어하고, 각종 수학적 연산을 수행하는 기능을 담당한다.

도 5는 사용자측 장치의 구성요소 및 동작을 나타낸 블록도이다. 사용자측의 장치(500)는 송수신부(510), 컨텐츠실행부(520), 암호화부(540), 메모리(550) 및 제어부(530)로 구성될 수 있다. 상기 송수신부(510)는 난수 α로부터 계산한 t값, 사용자 ID 및 a^x 값을 신뢰기관으로 전송하고, 신뢰기관으로부터는 난수 β를 수신하며, 컨텐츠 제공자(600)에는 T_1, T_2 및 ElGamal 서명 방식에 의해 계산된 값을 전송하고, 컨텐츠 제공자로부터는 암호화된 사용자 정보가 포함된 컨텐츠 아이템을 수신하는 역할을 한다. 상기 컨텐츠실행부(520)는 상기 상기 컨텐츠 제공자(600)로부터 수신한 컨텐츠 아이템에 대하여 컨텐츠 제공자(600)로부터 사용자 인증을 거친 후에 그 컨텐츠를 실행하는 역할을 수행한다. 상기 암호화부(540)는 난수 r을 발생시키고, T_1, T_2 의 계산 및 ElGamal 서명 방식에 의한 계산을 담당한다. 상기 메모리(550)는 상기 신뢰기관(400) 및 컨텐츠 제공자(600)와 주고 받는 파라미터들을 일시 저장하는 역할을 한다. 또한, 상기 제어부(530)는 상기 송수신부(510), 컨텐츠실행부(520), 암호화부(540) 및 메모리(550)의 동작을 제어하고, 각종 수학적 연산을 수행한다.

도 6은 컨텐츠 제공자측 장치의 구성요소 및 동작을 나타낸 블록도이다. 컨텐츠 제공자측의 장치(600)는 송수신부(620), 컨텐츠생성부(650), 인증부(640), 데이터 베이스(610) 및 제어부(630)로 구성될 수 있다. 상기 송수신부(620)는 사용자(500)으로부터 T_1, T_2 및 ElGamal 서명 방식에 의해 계산된 값을 수신하고, 사용자(500)에게는 암호화된 사용자 정보가 포함된 컨텐츠 아이템을 전송하는 역할을 한다.상기 컨텐츠생성부(650)는 각종 원본 컨텐츠 아이템을 생성하고, 안전한 2자간 연산(Secure Two-party Computation)을 이용하여 상기 원본 컨텐츠로부터 새로운 암호화된 사용자 정보가 포함된 컨텐츠 아이템을 생성하는 역할을 한다. 상기 인증부(640)는 W_1 값을 이용하여 ElGamal 서명 확인 방식에 의해 계산을 하고 이를 통해 사용자가 신뢰기관에 등록된 R값을 가지는 정당한 사용자임을 확인하며, 사용자로부터 다시 접속이 있으면 다시 ElGamal 서명 확인 방식에 의해 계산을 하여 당해 사용자가 난수 r값을 알고 있는 정당한 사용자인가를 확인하는 역할을 담당한다. 상기 데이터 베이스(610)는 상기 신뢰기관(400) 및 사용자(500)와 주고 받는 파라 미터들을 저장하고, 원본 컨텐츠 아이템 및 암호화된 사용자 정보가 포함된 컨텐츠 아이템을 저장하는 역할을 담당한다. 또한 상기 제어부(630)는 상기 송수신부(620), 컨텐츠생성부(650), 인증부(640) 및 데이터 베이스(610)의 동작을 제어하고, 각종 수학적 연산을 수행하는 역할을 한다.

도 7은 본 발명에 따른 인증 방법을 개략적으로 나타낸 흐름도이다. 도 7에서 보는 바와 같이 본 발명에 따른 방법은 크게 여섯 단계로 구성되며 신뢰기관, 컨텐츠 제공자, 컨텐츠 사용자의 상호작용에 의해서 이루어진다. 첫번째는 신뢰기관이 키를 생성하는 과정이다(S710). 신뢰기관에서는 컨텐츠 사용자의 그룹에 의해서 사용될 그룹 공통키를 생성하며, 또한 시스템에서 전역으로 사용될 시스템 파라미터들을 생성하여 공개한다. 두번째는 사용자가 신뢰기관에 등록하는 과정이다(S720). 사용자는 신뢰기관과 합의하에 자신의 임시 공개키와 비밀키 쌍을 생성하고 이후의 프로토콜에서 이용될 등록증을 발급받는다. 여기서 언급된 등록증은 일종의 멤버쉽(membership)을 증명하는 카드와 같은 구실을 하는 것으로 이해될 수 있다. 세번째는 컨텐츠 제공자가 사용자를 인증하는 과정이다(S730). 사용자가 제공자에게 자신이 해당 그룹의 정당한 사용자라는 것을 증명하고 컨텐츠 제공자는 사용자의 증명에 대하여 정당성을 검증한다. 네번째는 컨텐츠 제공자가 컨텐츠를 생성하고 그 컨텐츠에 암호화된 사용자 정보를 포함시키는 과정이다(S740). 인증이 올바로 된 사용자에게 제공될 컨텐츠에 추가할 사용자 정보를 컨텐츠 제공자와 안전한 2자간 연산(Secure Two-party Computation)을 수행하여 새로 만들어진 컨텐츠를 생성한다. 다섯번째는 컨텐츠 제공자가 사용자에게 컨텐츠를 전송하고 사용자가 이러 한 컨텐츠를 수신하는 과정이다(S750). 본 과정 동안 컨텐츠 제공자는 해당 사용자들에게 지정된 컨텐츠를 제공한다. 마지막으로 컨텐츠 제공자가 신뢰기관으로부터 암호화된 사용자 정보를 얻어 사용자를 확인하는 과정이다(S760). 불법 사용자의 추적이나 요금 부과 등을 목적으로 사용자의 실제 신분을 확인하여야 하는 경우에 사용한다.

도 8은 신뢰기관에 의한 키 생성과정을 나타낸 흐름도로서 신뢰기관에서 이루어지는 과정을 나타낸 것이다. 먼저, RSA(Rivest-Shamir-Adleman) 기법과 같은 매우 큰 소수 p와 q를 선택하여, n=pq 를 얻는다(S810). 이는 매우 큰 소수의 곱으로 계산된 결과인 n값으로부터 p, q값을 찾기가 매우 어렵게 하기 위함이다. 이하에서 모든 모드(mod) 연산은 상기 n을 기준으로 한다. 다음으로 지수 계산에 사용할 지수(exponent) y, z를 선택하여 저장하고 소수 v를 선택한다(S820). 여기서 v뿐 아니라 지수 y, z도 소수로 선택하는 것이 바람직하다. 다음으로는 임의의 난수 a를 선택하여 $Y=a^{-y}$ 와 $Z=a^x$ 를 계산한다(S830). 여기서 $Y=a^{-y}$ 값은 마지막으로 상기에서 구한 파라미터 중 시스템 파라미터로 정의할 수 있는 (n,v,a,Y,Z)를 컨텐츠 제공자 및 사용자에게 공개한다(S840).

도 9는 사용자가 신뢰기관에 등록하는 과정을 나타낸 흐름도로서 사용자와 신뢰기관 간에 이루어지는 과정을 나타낸 것이다.

사용자는 난수 α를 선택하여 $t \equiv a^{\alpha}$ 를 계산한 후 이 값을 사용자 ID와 함께 신뢰기관에 전송한다(S910). 상기 $t \equiv a^{\alpha}$ 라는 표현은 a^{α} 의 모드 값을 구하여 그 값을 t로 둔다는 의미이다. 다음으로 신뢰기관은 난수 β를 선택하여 사용자에게 전송한다(S920). 사용자는 상기 전송받은 β를 이용하여 $x=\alpha \cdot \beta$를 계산한 후, a^x 를 계산하여 이를 신뢰기관에 전송한다(S930). 신뢰기관은 상기 전송받은 a^x 를 이용하여 $t^{\beta} \equiv a^x$ 를 검사한 후(S940), 즉 t^{β} 의 모드 값과 a^x 의 모드 값이 동일한지를 검사하여 두 값이 동일하면 정당한 사용자로 인정할 수 있으므로 사용자를 위한 임시 등록증, $R=a^{(x+y)v^{-1}}$ 을 계산하여 전송한다(S950). 마지막으로 신뢰기관은 자신의 데이터베이스에 상기 사용자로부터 전송 받은 사용자 ID와 상기 계산한 R값을 저장한다(S960).

도 10은 컨텐츠 제공자가 사용자를 인증하는 과정을 나타낸 흐름도로서 컨텐츠 제공자와 사용자간에 이루어지는 과정이다.

사용자가 난수 r을 선택한 후(S1010), $T_1 \equiv R \cdot a^r$ 을 계산하고 ElGamal 서명 방식을 이용하여 ElGamal('auth',a^{x+rv})을 계산한 후, 두 값을 전송한다(S1020). ElGamal 서명 방식 또는 서명 확인 방식은 이미 당업계에서는 당연히 알고 있을 정도로 인식되어 있으며 T. ElGamal의 논문 'A public key cryptosystem and a signature scheme based on discrete logarithms'(IEEE Tran. on Information Theory, pp. 469-472, 1985.)을 참조하면 보다 상세한 내용을 알 수 있을 것이다. 상기 'auth'는 인증(authentication) 내지는 서명의 의미로서 함수명과도 같이 본 발명에서 표시한 것이다.

컨텐츠 제공자는 먼저 $W_1 \equiv T_1^v \cdot Y$를 계산하여 ElGamal 서명 확인 방식을 이용하여 ElGamal('auth', W_1)를 수행한다. 이 과정을 통하여 컨텐츠 제공자는 사용자가 등록된 R 값을 가지고 있는 정당한 사용자인지 여부를 확인할 수 있다(S1030). 이 후 정당 사용자가 다시 $T_2 \equiv R^{-1} \cdot Z^r \cdot a^{-r}$ 을 계산하여 ElGamal('kwg',a^{zr})를 전송하면(S1040), 컨텐츠 제공자는 $W_2 \equiv T_1 \cdot T_2$ 를 계산하고 ElGamal('kwg',W_2,Z)로 서명을 확인한다(S1050). 이러한 과정은 T_2 를 전송한 사용자가 T_1 을 전송한 사용자와 같은가 즉 T_2 를 전송한 사용자가 난수 r 값을 알고 있는가를 확인하는 과정이다. 상기 'kwg'는 정보(knowledge)의 의미로서 이미 인증 과정을 거친 서명을 확인하는 의미를 갖는 것으로 표시한 것이다.

도 11은 컨텐츠 제공자가 컨텐츠를 생성하는 과정을 나타낸 흐름도로서 컨텐츠 제공자에서 이루어지는 과정이다.

사용자의 T_1 및 T_2 값, 컨텐츠 제공자의 임의의 j번째 트랜색션(Transaction) 값 S_j 및 컨텐츠 제공자의 공개키를 안전한 2자간 연산(Secure Two-party Computation)을 수행하는 함수에 입력한다(S1110). 여기서 트랜색션 값 S_j 는 사용자가 컨텐츠를 사용하는 것을 하나의 거래로 볼 때, 각각의 거래와 동일시 할 수 있는 거래 고유 번호 값을 의미한다. 또한 컨텐츠 제공자의 공개키는 해당 컨텐츠를 제공한 자가 누 구인지를 표시해주는 제공자 고유 번호 값을 의미한다. 상기 함수로부터 출력된 값을 원본 컨텐츠 아이템(item)에 포함시켜(S1120) 새로운 컨텐츠 아이템을 생성하여 사용자에게 전송한다(S1130, S1140).

도 12는 컨텐츠 제공자가 사용자의 신분을 확인하는 과정을 나타낸 흐름도로서 컨텐츠 제공자와 신뢰기관간에 이루어지는 과정이다.

불법 사용자 추적이나 요금 부과 등의 목적으로 컨텐츠 제공자와 신뢰기관과의 합의하에(S1210) 해당 컨텐츠 아이템에서 사용자에 대한 정보를 추출하고(S1220), 추출한 사용자에 대한 정보를 바탕으로 $T_1^{z-1} \cdot T_2^{-1} \equiv R^z$ 를 계산한다(S1230). 신뢰기관은 데이터 베이스에 저장된 등록자 테이블에서 R과 z값을 사용하여 사용자 ID를 얻는다(S1240). 사용자가 동일하다면 $T_1^{z-1} \cdot T_2^{-1}$ 의 모드 값과 R^z 의 모드 값은 같게 되므로, 신뢰기관은 이전에 사용자가 등록한 R 값과 신뢰기관 자신이 선택한 z 값을 이용하면 컨텐츠를 사용하는 자가 어떠한 사용자인지를 알 수 있다.

이상, 본 발명을 바람직한 실시예를 들어 상세하게 설명하였으나, 본 발명은 상기 실시예에 한정되지 않으며, 본 발명의 기술적 사상의 범위 내에서 당해 분야에서 통상의 지식을 가지는 자에 의하여 여러 가지 변형이 가능하다.

발명의 효과

본 발명에 의하면, 안전한 2자간 프로토콜(Secure Two-party Protocol) 및 ElGamal 암호 기법을 사용한 익명성 기법을 제공함으로써 네트워크 상에서 사용자가 본인의 사용자 정보를 누출시키지 않고 각종 컨텐츠를 안전하게 이용할 수 있다.

(57) 청구의 범위

청구항 1.

그룹 공통키를 생성하여 배포하고, 상기 그룹 공통키를 이용한 사용자를 인증하고, 상기 인증된 사용자의 개인 정보 및 상기 인증된 사용자에게 발행된 임시 등록증을 저장하는 신뢰기관;

상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 소정의 변환 방법으로 변환하여 컨텐츠 제공자에게 제공하고 상기 컨텐츠 제공자가 제공하는 컨텐츠를 실행하는 사용자 장치; 및

상기 그룹 공통키를 이용하여, 상기 변환된 임시 등록증을 제공한 사용자에 대한 상기 신뢰기관의 인증 여부를 확인하고, 상기 확인에 따라 컨텐츠를 제공하는 컨텐츠 제공자를 포함하는 컨텐츠 사용자 인증 시스템.

청구항 2.
제 1항에 있어서, 상기 신뢰기관은,

상기 그룹 공통키를 생성하는 파라미터 생성부;

상기 그룹 공통키를 이용한 사용자를 인증하는 인증부;

상기 인증된 사용자의 개인 정보 및 상기 인증된 사용자에게 발행된 임시 등록증을 저장하는 데이터베이스; 및

상기 그룹 공통키를 전송하고 상기 사용자의 인증 요청을 수신하는 송수신부를 포함하는 컨텐츠 사용자 인증 시스템.

청구항 3.
제 2항에 있어서, 상기 컨텐츠 제공자는,

상기 신뢰기관이 전송한 상기 그룹 공통키 및 상기 사용자가 제공한 상기 변환된 임시 등록증을 수신하고, 상기 확인된 사용자에게 컨텐츠를 송신하는 송수신부;

상기 그룹 공통키를 이용하여, 상기 변환된 임시 등록증을 제공한 사용자에 대한 상기 신뢰기관의 인증 여부를 확인하는 인증부; 및

상기 확인에 따라 컨텐츠를 제공하는 컨텐츠 생성부를 포함하는 컨텐츠 사용자 인증 시스템.

청구항 4.
제 3항에 있어서, 상기 사용자 장치는,

상기 신뢰기관에 대한 인증을 요청하고, 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 소정의 변환 방법으로 변환하는 암호화부;

상기 컨텐츠를 실행하는 컨텐츠 실행부; 및

상기 신뢰기관이 발행한 임시 등록증을 수신하고, 상기 변환된 임시 등록증을 상기 컨텐츠 제공자에게 송신하는 송수신부를 포함하는 컨텐츠 사용자 인증 시스템.

청구항 5.
제 4항에 있어서,

상기 사용자 장치의 암호화부는, 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 제 1 변환방법 및 제 2 변환 방법으로 각각 변환하는 컨텐츠 사용자 인증 시스템.

청구항 6.
제 5항에 있어서,

상기 컨텐츠 제공자의 인증부는, 상기 그룹 공통키를 이용하여 상기 제 1 변환된 임시 등록증을 제공한 사용자에 대한 상기 신뢰기관의 인증 여부를 확인하고,

상기 제 1 변환된 임시 등록증 및 상기 제 2 변환된 임시 등록증을 이용하여, 상기 제 1 변환된 임시 등록증을 제공한 사용자가 상기 자신의 비밀키를 알고 있는지 여부를 확인하는 컨텐츠 사용자 인증 시스템.

청구항 7.
제 6항에 있어서,

상기 컨텐츠 제공자의 컨텐츠 생성부는, 상기 제 1 변환된 임시 등록증, 상기 제 2 변환된 임시 등록증 및 컨텐츠 제공자 자신의 공개키를 이용하여 컨텐츠를 암호화하고 상기 암호화된 컨텐츠를 제공하는 컨텐츠 사용자 인증 시스템.

청구항 8.
제 7항에 있어서,

상기 컨텐츠 제공자는 상기 제 1 변환된 임시 등록증 및 제 2 변환된 임시등록증을 상기 신뢰기관에 제공하고, 상기 신뢰기관은 상기 제 1 및 제 2 변환된 임시 등록증과 상기 그룹 공통키를 이용하여 상기 신뢰기관의 데이터베이스에 등록된 상기 사용자의 개인 정보를 검색하는 컨텐츠 사용자 인증 시스템.

청구항 9.
신뢰기관이 그룹 공통키를 생성하고 배포하는 제 1 단계;

사용자가 상기 그룹 공통키를 이용하여 상기 신뢰기관의 인증을 받는 제 2 단계;

상기 신뢰기관의 인증을 받은 사용자의 개인 정보 및 상기 인증된 사용자에게 발행된 임시 등록증을 상기 신뢰기관에 저장하는 제 3 단계;

상기 사용자가 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 소정의 변환 방법으로 변환하여 컨텐츠 제공자에게 제공하는 제 4 단계; 및

상기 컨텐츠 제공자가 상기 그룹 공통키를 이용하여 상기 변환된 임시 등록증을 제공한 상기 사용자에 대한 상기 신뢰기관의 인증 여부를 확인하고, 상기 확인에 따라 컨텐츠를 제공하는 제 5 단계를 포함하는 컨텐츠 사용자 인증 방법.

청구항 10.
제 9항에 있어서, 제 4 단계는,

상기 사용자가 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 제 1 변환방법으로 변환하여 상기 컨텐츠 제공자에게 제공하는 제 4-1 단계; 및

사용자가 상기 신뢰기관이 발행한 임시 등록증을 자신의 비밀키를 이용하여 제 2 변환방법으로 변환하여 상기 컨텐츠 제공자에게 제공하는 제 4-2 단계를 포함하는 컨텐츠 사용자 인증 방법.

청구항 11.
제 10항에 있어서, 제 5단계는,

상기 컨텐츠 제공자가 상기 그룹 공통키를 이용하여, 상기 제 1 변환된 임시 등록증을 제공한 상기 사용자에 대한 상기 신뢰기관의 인증 여부를 확인하는 제 5-1단계; 및

상기 컨텐츠 제공자가 상기 제 1 변환된 임시 등록증 및 상기 제 2 변환된 임시 등 록증을 이용하여, 상기 제 1 변환된 임시 등록증을 제공한 사용자가 상기 비밀키를 알고 있는지 여부를 확인하는 제 5-2단계를 포함하는 컨텐츠 사용자 인증 방법.

청구항 12.
제 11항에 있어서,

상기 컨텐츠 제공자가 상기 제 1 변환된 임시 등록증, 상기 제 2 변환된 임시 등록증 및 컨텐츠 제공자 자신의 공개키를 이용하여 상기 컨텐츠를 암호화하여 상기 사용자에게 전송하는 제 6 단계를 더 포함하는 컨텐츠 사용자 인증 방법.

청구항 13.
제 12항에 있어서,

상기 컨텐츠 제공자가 상기 제 1 변환된 임시 등록증 및 제 2 변환된 임시등록증을 상기 신뢰기관에 제공하고, 상기 신뢰기관은 상기 제 1 및 제 2 변환된 임시 등록증과 상기 그룹 공통키를 이용하여 상기 신뢰기관에 등록된 상기 사용자의 개인 정보를 검색하는 제 7 단계를 더 포함하는 컨텐츠 사용자 인증 방법.

청구항 14.
제 13항에 있어서,

상기 그룹 공통키는, RSA 방식에 따라 선택된 소수 (1)p, (2)q, 상기 p와 q의 곱으로부터 산출된 (3)n, 소정의 난수 a에 지수 y와 z를 적용하여 계산된 (4)$Y=a^{-y}$ 와 (5)$Z=a^{x}$ 인 컨텐츠 사용자 인증 방법.

청구항 15.
제 14항에 있어서,

상기 제 2 단계는, 상기 사용자가 소정의 난수 α를 선택하여 $t\equiv a^{\alpha}$ 를 계산하고 상기 계산된 값과 상기 사용자의 개인 정보를 상기 신뢰기관에 전송하는 단계;

상기 신뢰기관이 소정의 난수 β를 선택하여 상기 사용자에게 전송하는 단계;

상기 사용자가 상기 전송받은 β를 이용하여 $x=\alpha\cdot\beta$를 계산하고, a^{x} 를 계산하여 상기 a^{x} 를 상기 신뢰기관에 전송하는 단계; 및

상기 신뢰기관이 상기 전송받은 a^{x} 를 이용하여 $t^{\beta}\equiv a^{x}$ 를 계산하고 상기 계산결과에 따라 상기 사용자를 인증하는 단계를 포함하는 컨텐츠 사용자 인증 방법.

청구항 16.
제 15항에 있어서,

상기 임시 등록증은, $R=a^{(x+y)v^{-1}}$ 인 컨텐츠 사용자 인증 방법.

청구항 17.
제 16항에 있어서,

상기 제 4-1 단계는, 상기 사용자가 자신의 비밀키 r를 선택하여, 상기 제 1 변환된 임시 등록증 $T_1\equiv R\cdot a^{r}$ 을 계산하고, ElGamal 서명 방식을 이용하여 ElGamal('auth',a^{x+rv})을 계산한 후 상기 계산값과 T_1 을 상기 컨텐츠 제공자에게 전 송하는 단계이고,

상기 제 4-2 단계는, 상기 사용자가 상기 제 1 변환된 임시 등록증 $T_2\equiv R^{-1}\cdot Z^{r}\cdot a^{-r}$ 을 계산하고, ElGamal('kwg',a^{zr})를 계산한 후 상기 계산값과 T_2 를 상기 컨텐츠 제공자에게 전송하는 단계인 컨텐츠 사용자 인증 방법.

청구항 18.
제 17항에 있어서,

상기 제 5-1 단계는,

상기 컨텐츠 제공자가 $W_1\equiv T_1^{v}\cdot Y$를 계산하고 ElGamal('auth', W_1)를 계산하여, 상기 사용자가 상기 신뢰기관에 등록된 임시 등록증 R을 가진 인증된 사용자인지 여부를 확인하는 단계이고,

상기 제 5-2 단계는,

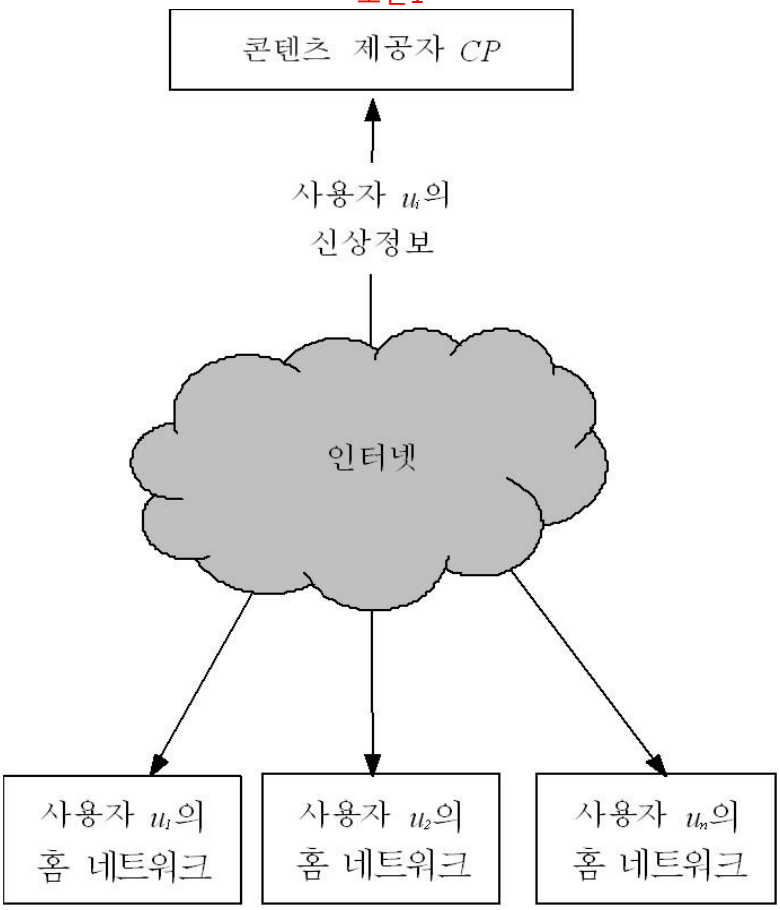
상기 컨텐츠 제공자는 $W_2\equiv T_1\cdot T_2$를 계산하고 ElGamal('kwg',W_2,Z)를 계산하여, 상기 제 2 변환된 임시 등록증 T_2 를 전송한 사용자가 상기 비밀키 r을 알고 있는지를 확인하는 단계인 컨텐츠 사용자 인증 방법.

청구항 19.
제 18항에 있어서,

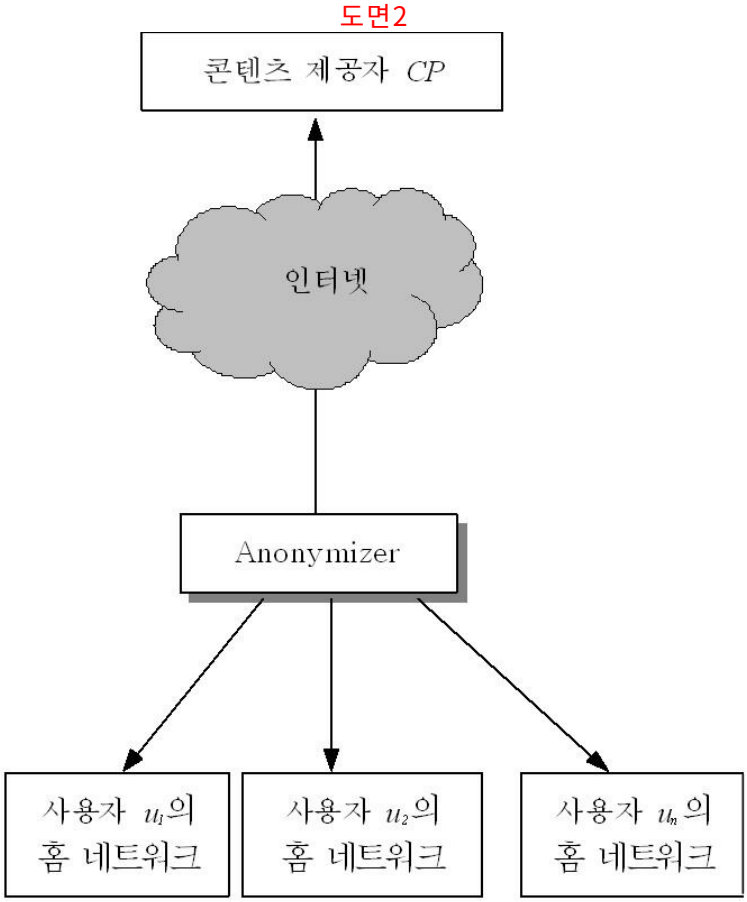
제 7 단계는 $T_1^{z-1}\cdot T_2^{-1}\equiv R^{z}$ 를 계산하여 이루어지는 컨텐츠 사용자 인증 방법.

도면

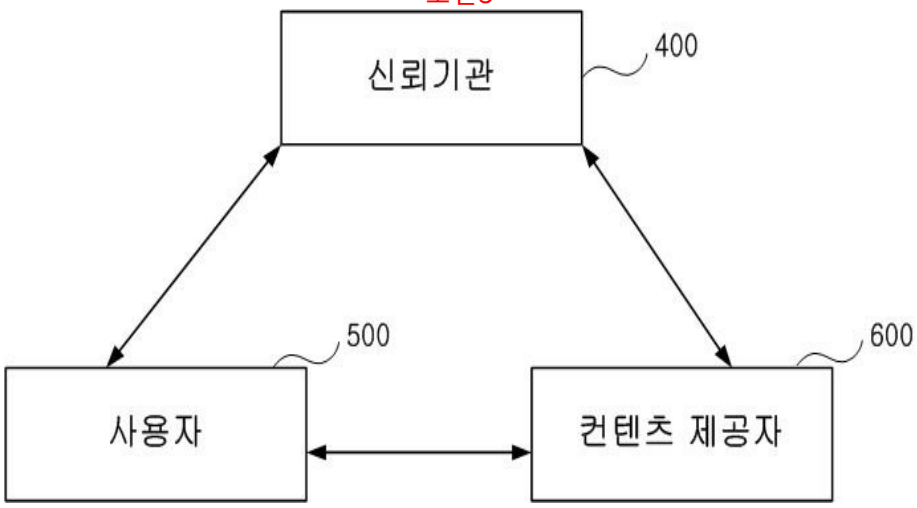
도면1


콘텐츠 제공자 CP
사용자 u_i의
신상정보
인터넷
사용자 u_1의
홈 네트워크
사용자 u_2의
홈 네트워크
사용자 u_n의
홈 네트워크

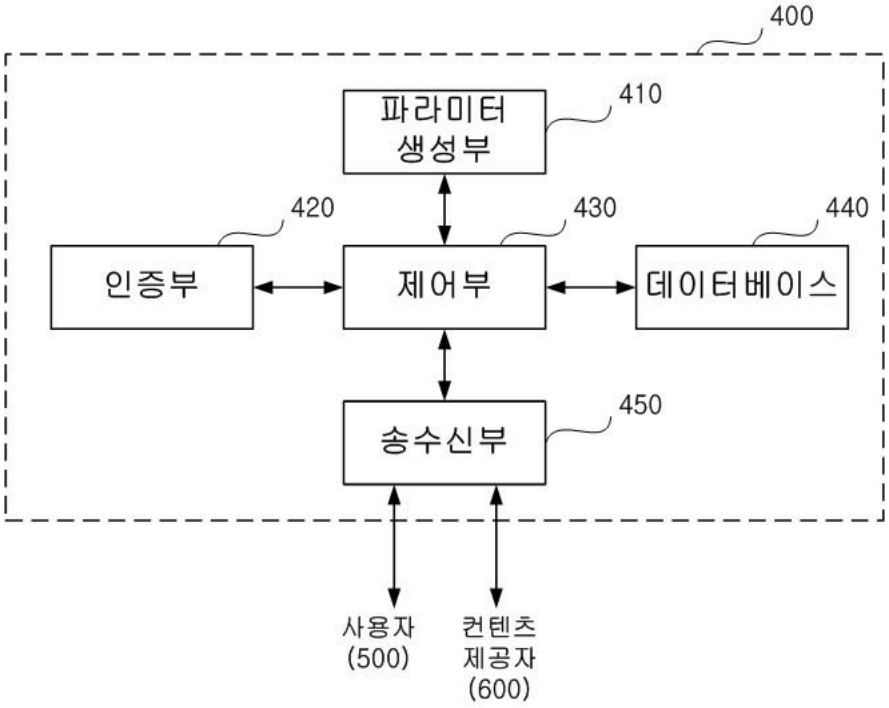
도면2


콘텐츠 제공자 CP
인터넷
Anonymizer
사용자 u_1의
홈 네트워크
사용자 u_2의
홈 네트워크
사용자 u_n의
홈 네트워크

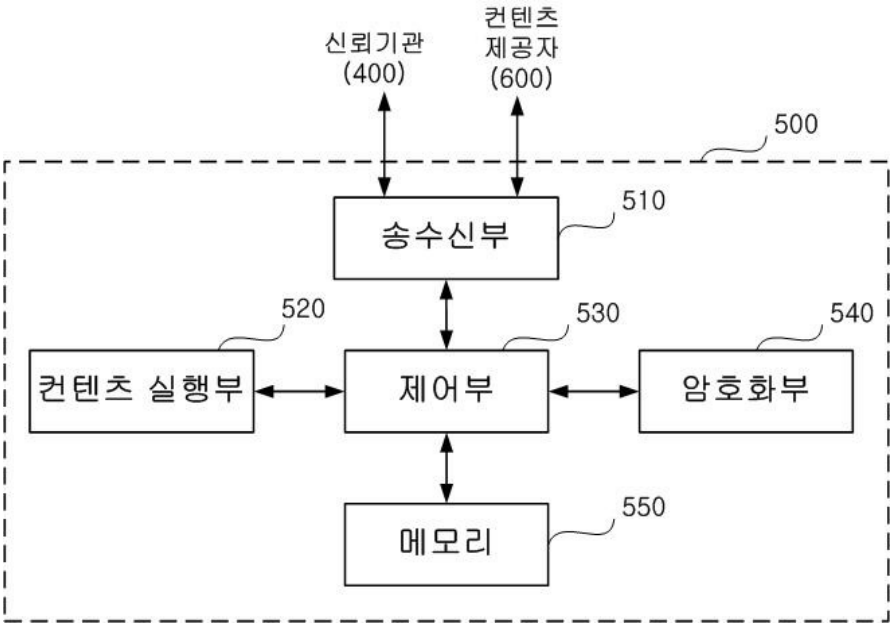
도면3


신뢰기관
400
사용자
500
컨텐츠 제공자
600

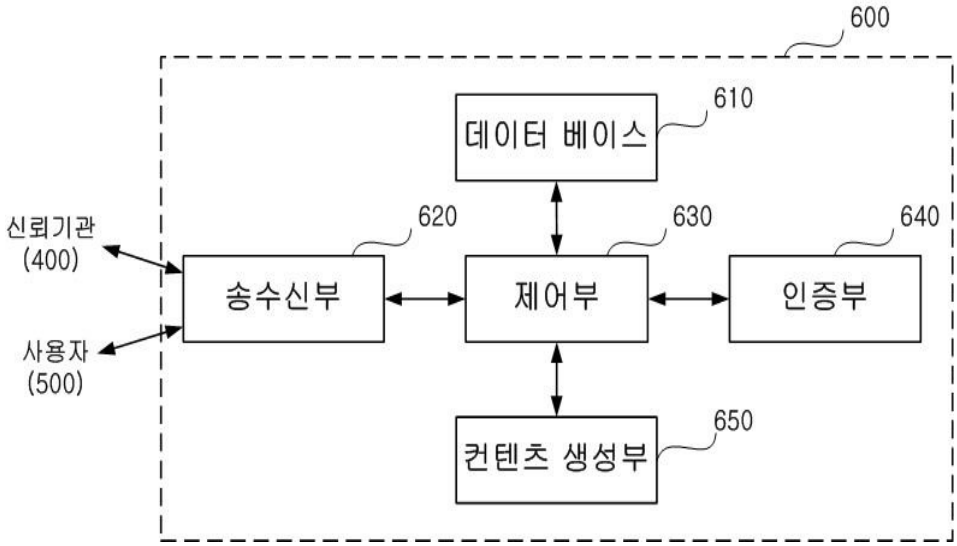
도면4


400
파라미터 생성부
410
인증부
420
제어부
430
데이터베이스
440
송수신부
450
사용자 (500)
컨텐츠 제공자 (600)

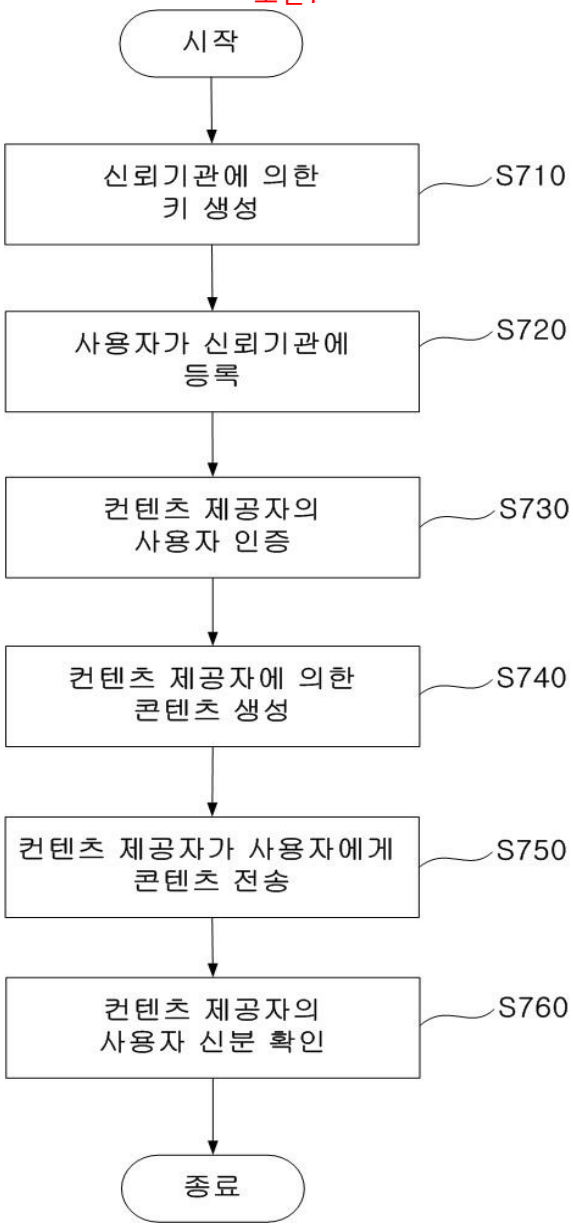
도면5


신뢰기관
(400)
컨텐츠
제공자
(600)
500
송수신부
510
520
530
540
컨텐츠 실행부
제어부
암호화부
메모리
550

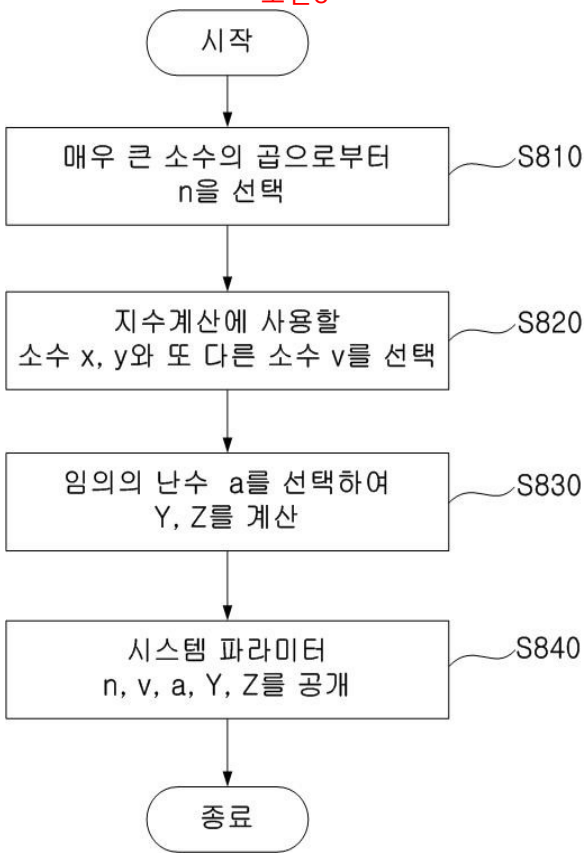
도면6


600
데이터 베이스
610
신뢰기관
(400)
620
630
640
송수신부
제어부
인증부
사용자
(500)
컨텐츠 생성부
650

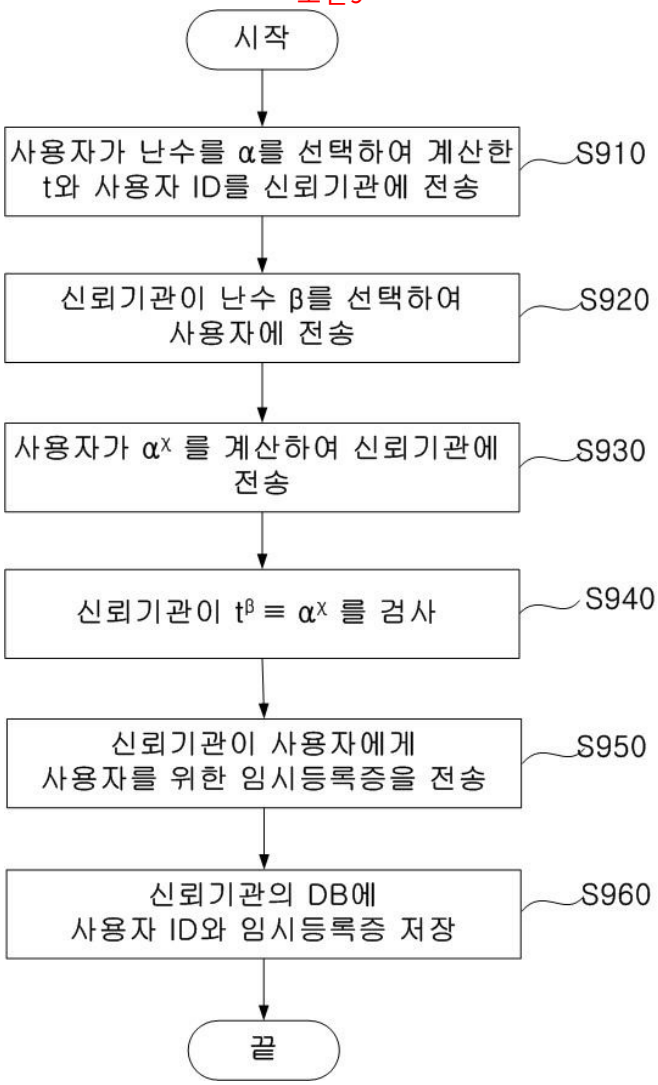
도면7


시작
신뢰기관에 의한 키 생성
S710
사용자가 신뢰기관에 등록
S720
컨텐츠 제공자의 사용자 인증
S730
컨텐츠 제공자에 의한 콘텐츠 생성
S740
컨텐츠 제공자가 사용자에게 콘텐츠 전송
S750
컨텐츠 제공자의 사용자 신분 확인
S760
종료

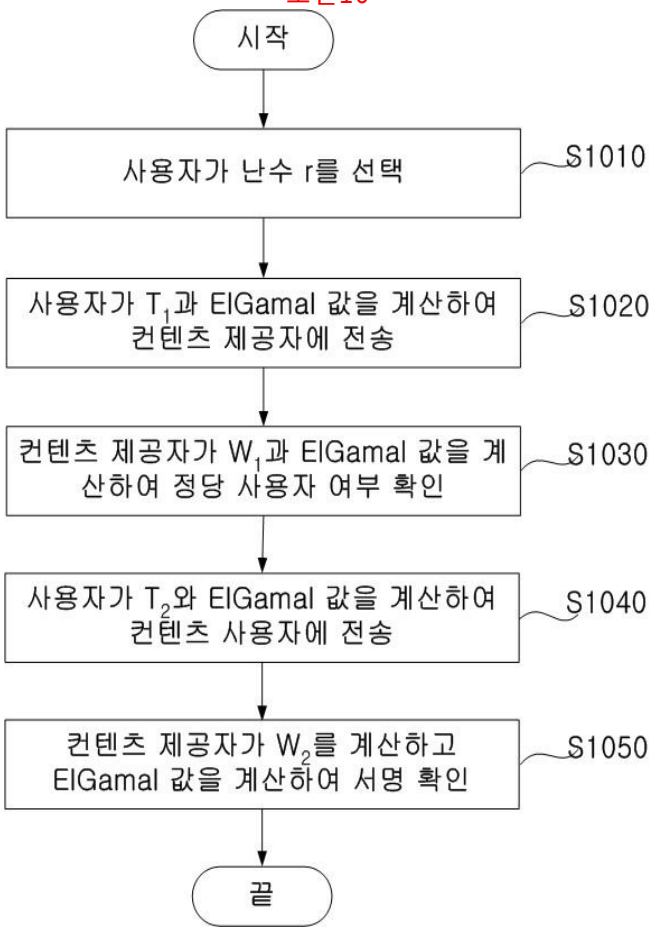
도면8


시작
매우 큰 소수의 곱으로부터 n을 선택
S810
지수계산에 사용할 소수 x, y와 또 다른 소수 v를 선택
S820
임의의 난수 a를 선택하여 Y, Z를 계산
S830
시스템 파라미터 n, v, a, Y, Z를 공개
S840
종료

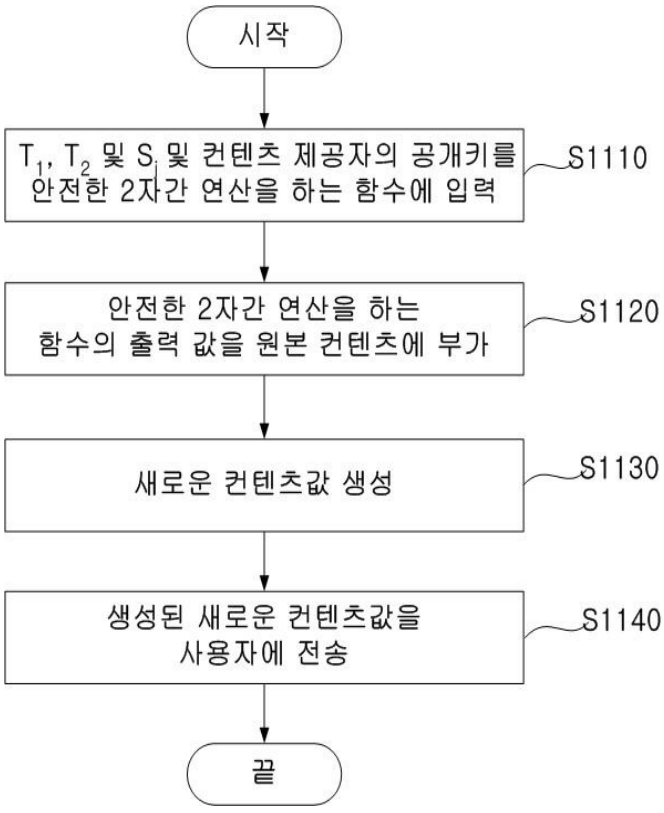
도면9


시작
사용자가 난수를 α를 선택하여 계산한 t와 사용자 ID를 신뢰기관에 전송
S910
신뢰기관이 난수 β를 선택하여 사용자에 전송
S920
사용자가 α^{x} 를 계산하여 신뢰기관에 전송
S930
신뢰기관이 $t^{\beta} \equiv \alpha^{x}$ 를 검사
S940
신뢰기관이 사용자에게 사용자를 위한 임시등록증을 전송
S950
신뢰기관의 DB에 사용자 ID와 임시등록증 저장
S960
끝

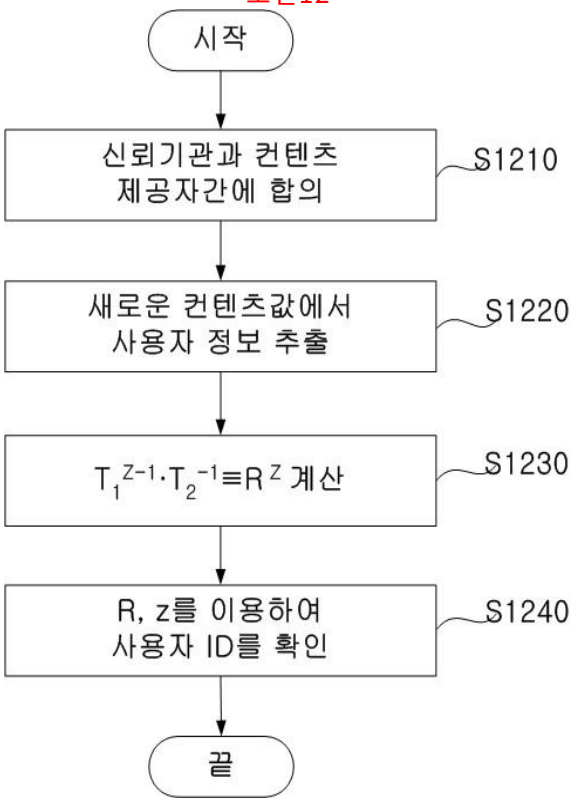
도면10


시작
사용자가 난수 r를 선택
S1010
사용자가 T_1과 ElGamal 값을 계산하여 컨텐츠 제공자에 전송
S1020
컨텐츠 제공자가 W_1과 ElGamal 값을 계산하여 정당 사용자 여부 확인
S1030
사용자가 T_2와 ElGamal 값을 계산하여 컨텐츠 사용자에 전송
S1040
컨텐츠 제공자가 W_2를 계산하고 ElGamal 값을 계산하여 서명 확인
S1050
끝

도면11


시작
T_1, T_2 및 S_1 및 컨텐츠 제공자의 공개키를 안전한 2자간 연산을 하는 함수에 입력
S1110
안전한 2자간 연산을 하는 함수의 출력 값을 원본 컨텐츠에 부가
S1120
새로운 컨텐츠값 생성
S1130
생성된 새로운 컨텐츠값을 사용자에 전송
S1140
끝

도면12


시작
신뢰기관과 컨텐츠 제공자간에 합의
S1210
새로운 컨텐츠값에서 사용자 정보 추출
S1220
$T_1^{Z-1} \cdot T_2^{-1} \equiv R^Z$ 계산
S1230
R, z를 이용하여 사용자 ID를 확인
S1240
끝