



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년05월07일
(11) 등록번호 10-1260394
(24) 등록일자 2013년04월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/20 (2006.01)
(21) 출원번호 10-2009-0032432
(22) 출원일자 2009년04월14일
심사청구일자 2009년04월14일
(65) 공개번호 10-2010-0085809
(43) 공개일자 2010년07월29일
(30) 우선권주장
1020090004691 2009년01월20일 대한민국(KR)
(56) 선행기술조사문헌
EP02012248 A2*
KR1020040099943 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
한승완
광주광역시 서구 화정로280번길 7 (농성동)
이석준
대전광역시 유성구 배울1로 119, 대덕테크노밸리
우림필유 1207-1102 (용산동)
(뒷면에 계속)
(74) 대리인
박병창

전체 청구항 수 : 총 8 항

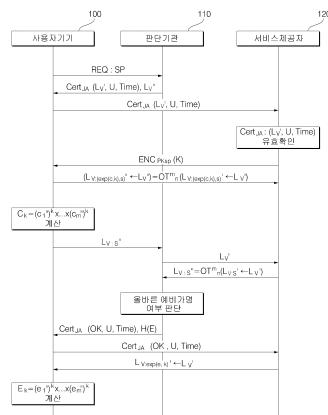
심사관 : 이강하

(54) 발명의 명칭 불확정 전송방법을 기반으로 하는 가명 인증 시스템 및 그 방법

(57) 요약

본 발명은 불확정 전송(Oblivious transfer)을 이용하여 사용자 기기가 서비스 제공자로부터 가명을 획득하고 이를 안전하게 사용하는 시스템에 관한 것이다. 서비스 제공자는 가명과 실명에 관한 연결 정보를 판단 기관과 공유함으로써 가명을 사용하는 익명 사용자에게 대한 판단 기관의 동의가 있는 경우에 한하여 실명을 추적할 수 있다. 판단 기관은 사용자 기기에게 서비스 제공자로부터 받아올 예비 가명을 지정해주고 이를 사용자 기기가 올바르게 수행했는지 확인하는 역할을 수행한다. 또한 서비스 제공자의 요청에 대하여 가명을 사용하는 사용자에게 대해서 익명성을 제한할 수 있다.

대표도 - 도2



(72) 발명자

양대현

서울특별시 서초구 서초중앙로 200, 3동 405호 (서초동, 삼풍아파트)

강전일

충청남도 공주시 무령로 300 (옥룡동)

이 발명을 지원한 국가연구개발사업

과제고유번호 2008-F-036-01

부처명 지식경제부

연구사업명 IT원천기술개발

연구과제명 익명성 기반의 u지식정보보호기술 개발

주관기관 한국전자통신연구원

연구기간 2008.03.01~2012.02.29

특허청구의 범위

청구항 1

사용자 기기, 서비스 제공자 및 판단기관이 상호 통신 가능하도록 연결되는 예비 단계;

상기 사용자 기기는 상기 판단기관으로부터 복수의 예비 가명 색인을 전송받는 단계;

상기 사용자 기기가 상기 예비 가명 색인을 이용하여 불확정 전송방법으로 상기 서비스 제공자로부터 복수의 예비 가명 및 상기 복수의 예비 가명에 대한 제1 인증키를 전송받는 단계;

상기 사용자 기기가 상기 제1 인증키를 상기 판단기관에게 전송하는 단계;

상기 사용자 기기는 상기 판단기관이 상기 제1 인증키를 확인하여 상기 예비 가명의 유효 여부를 검사하고, 유효한 경우에 발급하는 상기 예비 가명의 사용허가를 전송받는 단계; 및

상기 사용자 기기는 상기 예비 가명을 조합한 가명을 이용하여 상기 서비스 제공자에게 서비스를 요청하는 단계;를 포함하고,

상기 예비 단계는,

상기 서비스 제공자는 비밀키를 선택하고, 예비 가명 집합을 준비하는 단계; 및 상기 서비스 제공자가 상기 예비 가명에 관한 색인 집합과 부분 예비 가명 집합을 판단기관과 공유하는 단계를 포함하는 불확정 전송방법을 기반으로 하는 가명 인증 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 예비 가명은 상기 서비스 제공자가 제1 난수를 결합하여 암호화 함수 형태로 전송하는 것을 특징으로 하는 불확정 전송방법을 기반으로 하는 가명 인증 방법.

청구항 4

제3항에 있어서,

상기 사용자 기기는 상기 제1 난수를 포함하는 암호화 함수를 저장하는 것을 특징으로 하는 불확정 전송방법을 기반으로 하는 가명 인증 방법.

청구항 5

제1항에 있어서,

상기 사용자 기기는 전송받은 상기 복수의 예비 가명을 서로 곱하여 조합한 가명을 획득하는 것을 특징으로 하는 불확정 전송방법을 기반으로 하는 가명 인증 방법.

청구항 6

제1항에 있어서,

상기 서비스를 요청하는 단계는 상기 사용자 기기가 상기 예비 가명을 조합한 가명과 제2 난수와 결합하여 상기 서비스 제공자에 전송하며 상기 서비스를 요청하는 것을 특징으로 하는 불확정 전송방법을 기반으로 하는 가명 인증 방법.

청구항 7

제1항에 있어서,

상기 예비 가명의 사용허가는 상기 예비 가명의 해시 함수를 포함하고, 상기 사용자 기기는 상기 해시 함수를

상기 서비스 제공자에게 전송하는 것을 특징으로 하는 불확정 전송방법을 기반으로 하는 가명 인증 방법.

청구항 8

제1항에 있어서,

상기 예비 가명의 유효 여부는 상기 서비스 제공자가 불확정 전송방법으로 상기 판단기관으로 전송한 제2 인증키를 상기 판단기관이 상기 제1 인증키와 비교하여 판단하는 것을 특징으로 하는 불확정 전송방법을 기반으로 하는 가명 인증 방법.

청구항 9

불확정 전송방법에 의해 통신하는 사용자 기기, 서비스 제공자 및 판단기관을 포함하는 불확정 전송방법을 기반으로 하는 가명 인증 시스템에 있어서,

가명 인증에서 사용할 예비 가명 집합, 상기 예비 가명 집합의 색인 및 상기 예비 가명 집합의 인증키를 준비하고, 상기 색인은 상기 판단기관에 제공하고 상기 예비 가명 집합과 상기 인증키는 사용자 기기에게 제공하는 상기 서비스 제공자;

상기 서비스 제공자로부터 제공받은 상기 색인을 저장하고, 사용자 기기의 가명 인증 요청시 상기 색인에서 복수의 선택된 예비 가명 색인을 상기 사용자 기기에게 전송하고 상기 인증키의 유효성을 검증하는 판단기관; 및

상기 판단기관에게 상기 예비 가명 색인을 요청하고, 상기 예비 가명 색인에 해당하는 상기 예비 가명을 상기 서비스 제공자로부터 전송받아 조합하여 가명 인증에 사용하는 사용자 기기;를 포함하고,

상기 서비스 제공자는, 인증된 가명과 상기 인증된 가명의 접속 로그 기록을 저장하고, 상기 판단 기관은 상기 서비스 제공자의 가명 추적 요청시 상기 인증된 가명에 해당하는 사용자 기기의 식별자를 상기 서비스 제공자로 전송하는 것을 특징으로 하는 불확정 전송방법을 기반으로 하는 가명 인증 시스템.

청구항 10

삭제

명세서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 네트워크에서 개인의 정보를 보호하기 위한 기술에 관한 것으로 불확정 전송방법을 기반으로 하는 가명 인증방법에서 가명 생성을 예비 가명의 조합으로 사용하여 가명 부족현상을 해결하고, 제한적 실명 추적을 가능하게 하기 위한 불확정 전송방법을 기반으로 하는 가명 인증 시스템 및 그 방법에 관한 것이다.

[0002] 본 발명은 지식경제부 및 정보통신연구진흥원의 IT 성장동력기술개발 사업의 일환으로 수행한 연구로부터 도출된 것이다. [과제관리번호: 2008-F-036-01, 과제명: 익명성 기반의 u지식정보보호기술 개발]

배경 기술

[0003] 개인 정보보호를 위해 익명(Anonymity)과 가명(Pseudonym)에 관한 연구가 1980년대 후반부터 진행되고 있다. 그러나 가명 시스템은 지나치게 높은 보안 수준에 따라, 접근제어가 복잡하고, 필요에 따른 사용자 추적기능 등 실제 응용환경에서 요구하는 특징을 충족시키지 못한다. 한편, 수학적 어려움을 이용하여 설계된 가명을 이용하여 익명성을 보호하는 일반적인 가명 시스템과 달리 네트워크의 구조적인 특징을 이용하여 익명성을 확보하는 가명 시스템이 설계되고 있다.

[0004] 이중에서 불확정 전송방법을 이용한 가명 시스템을 살펴보면 다음과 같다. 가명 시스템은 판단기관과 서비스 제공자 및 사용자 기기로 구성된다. 사용자 기기는 우선 판단 기관과 서비스 제공자에게 실명으로 인증을 수행하고 보안 세션을 형성한다. 이후, 각 통신은 보안 세션을 통해 이루어진다. 실명 인증이 끝나면 판단 기관은 서비스 제공자가 가진 기명들의 색인을 다수 선택하여 사용자 기기에게 전송한다. 사용자 기기는 다수의 색인에 해당하는 가명과 가명의 인증키 쌍을 서비스 제공자에게 전송받는다.

[0005] 그 후, 사용자 기기는 판단기관에게 전송받았던 색인과 임시로 암호화된 가명의 인증키를 판단기관으로 환송한다. 판단기관은 이중 1개를 제외한 나머지 암호화 비밀키를 사용자 기기에게 요구하고 이를 이용하여 가명의 인증키들을 복호화한다. 판단기관은 이 값들을 색인과 함께 서비스 제공자에게 전송하고, 서비스 제공자는 가명의 인증키가 올바른지 확인하고 그 결과를 판단기관에게 전송한다. 만약 모두 올바른 경우, 판단기관은 사용자 기기에게 승낙의 메시지를 전송하고, 사용자 기기는 남은 하나의 가명을 사용한다.

[0006] 불확정 방법에 의한 가명 인증 시스템은 판단기관과 서비스 제공자는 각각 색인 집합과 가명 집합을 관리한다. 그러나 집합의 크기는 고정되어 있고, 사용자가 매우 많을 경우에는 집합이 고갈될 수 있다. 이를 방지하기 위해 집합이 고갈되기 전에 집합을 늘려주는 방법을 사용하나, 집합을 늘리기 전과 후의 가명이 확연히 달라져 익명성이 낮아지게 된다.

발명의 내용

해결 하고자하는 과제

[0007] 본 발명의 목적은, 예비 가명의 조합을 통한 가명 고갈 문제를 해소하고, 사용자들간 공모를 통한 가명 생산 및 위조를 방지하며, 제한적으로 실명 추적이 가능한 불확정 전송방법을 기반으로 하는 가명 인증 시스템 및 그 방법을 제공하는 것이다.

과제 해결수단

[0008] 상기 목적은, 사용자 기기, 서비스 제공자 및 판단기관이 상호 통신 가능하도록 연결되는 예비 단계; 상기 사용자 기기는 상기 판단기관으로부터 복수의 예비 가명 색인을 전송받는 단계; 상기 사용자 기기가 상기 예비 가명 색인을 이용하여 불확정 전송방법으로 상기 서비스 제공자로부터 복수의 예비 가명 및 상기 복수의 예비 가명에 대한 제1 인증키를 전송받는 단계, 상기 사용자 기기가 상기 제1 인증키를 상기 판단기관에게 전송하는 단계, 상기 사용자 기기는 상기 판단기관이 상기 제1 인증키를 확인하여 상기 예비 가명의 유효 여부를 검사하고, 유효한 경우에 발급하는 상기 예비 가명의 사용허가를 전송받는 단계, 및 상기 사용자 기기는 상기 예비 가명을 조합한 가명을 이용하여 상기 서비스 제공자에게 서비스를 요청하는 단계를 포함하는 불확정 전송방법을 기반으로 하는 가명 인증 방법에 의해 달성된다.

[0009] 또한, 불확정 전송방법에 의해 통신하는 사용자 기기, 서비스 제공자 및 판단기관에 있어서, 가명 인증에서 사용할 예비 가명 집합, 상기 예비 가명 집합의 색인 및 상기 예비 가명 집합의 인증키를 준비하고, 상기 색인은 상기 판단기관에 제공하고 상기 예비 가명 집합과 상기 인증키는 사용자 기기에게 제공하는 상기 서비스 제공자, 상기 서비스 제공자로부터 제공받은 상기 색인을 저장하고, 사용자 기기의 가명 인증 요청시 상기 색인에서 복수의 선택된 예비 가명 색인을 상기 사용자 기기에게 전송하고 상기 인증키의 유효성을 검증하는 판단기관 및 상기 판단기관에게 상기 예비 가명 색인을 요청하고, 상기 예비 가명 색인에 해당하는 상기 예비 가명을 상기 서비스 제공자로부터 전송받아 조합하여 가명 인증에 사용하는 사용자 기기를 포함하는 불확정 전송방법을 기반으로 하는 가명 인증 시스템에 의해 달성된다.

효 과

[0010] 본 발명에 따르면, 예비 가명의 조합으로 가명을 생성하므로, 가명 고갈 문제를 해결할 수 있고, 제한적으로 사용자 기기의 실명 추적이 가능하므로 응용환경에서 요구하는 불확정 전송방법을 기반으로 하는 가명 인증 방법을 제공할 수 있다.

발명의 실시를 위한 구체적인 내용

[0011] 불확정 전송방법(Oblivious Transfer : OT)은 송신자가 일정 수의 정보 중에 일부분을 수신자에게 보내주는 암호학적 프로토콜이다. OT가 다른 전송 프로토콜과 특별히 다른 점은, 송신자는 수신자가 일정수의 비밀을 가져갔다는 사실을 알 수 있지만 그것이 무엇인지 알 수 없다는 것이다.

[0012] 일반적으로, 불확정 전송방법이란, 2개의 비밀 정보를 예로써 설명하면 임의의 송신자 A가 임의의 수신자 B에게 어떤 비밀 정보를 보내고자 할 때 임의의 수신자 B가 그 비밀 정보를 1/2의 확률로 취할 수 있게 하고, 임의의 송신자 A는 임의의 수신자 B가 그 비밀 정보를 취했는지의 여부를 1/2의 확률로 추측할 수 있게 하는 프로토콜을 말한다. 물론, 임의의 수신자 B가 그 비밀 정보를 취했다면 B는 그 비밀의 내용을 알 수 있다. 이러한 경우는 하나의 비밀 정보에 대해서 불확정 전송하는 방법이다.

- [0013] 불확정 전송 방법은 몇개의 비밀 정보에 대해서 적용할 것인가에 따라 두개의 비밀 정보에 대한 2개의 정보중 하나의 정보를 불확정 전송하는 방법과, n (단, n 은 자연수임)개의 비밀 정보에 대한 임의의 정보만을 불확정 전송하는 방법 등이 있다.
- [0014] 본 발명에 따른 불확정 전송방법을 기반으로 하는 가명 인증 시스템은, 가명 인증에서 사용할 예비 가명 집합, 상기 예비 가명 집합의 색인 및 상기 예비 가명 집합의 인증키를 준비하고, 상기 색인은 상기 판단기관에 제공하고 상기 예비 가명 집합과 상기 인증키는 사용자 기기에게 제공하는 상기 서비스 제공자; 상기 서비스 제공자로부터 제공받은 상기 색인을 저장하고, 사용자 기기의 가명 인증 요청시 상기 색인에서 복수의 선택된 예비 가명 색인을 상기 사용자 기기에게 전송하고 상기 인증키의 유효성을 검증하는 판단기관; 및 상기 판단기관에게 상기 예비 가명 색인을 요청하고, 상기 예비 가명 색인에 해당하는 상기 예비 가명을 상기 서비스 제공자로부터 전송받아 조합하여 가명 인증에 사용하는 사용자 기기;를 포함한다.
- [0015] 또한, 상기 서비스 제공자는 인증된 가명과 상기 인증된 가명의 접속 로그 기록을 저장하고, 상기 판단 기관은 상기 서비스 제공자의 가명 추적 요청시 상기 인증된 가명에 해당하는 사용자 기기의 식별자를 상기 서비스 제공자로 전송할 수 있다.
- [0016] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세하게 설명한다.
- [0017] 도 1은 본 발명의 일실시예인 불확정 전송방법을 기반으로 하는 가명 인증 방법을 간략히 나타낸 도면이다.
- [0018] 사용자 기기(100)는 판단기관(110)으로부터 예비 가명 색인을 가져온다(150). 이를 이용하여 안전한 채널 통신의 불확정 전송방법(130)을 통해 서비스 제공자(120)로부터 예비 가명을 전송받는다(152). 판단기관(110)은 안전한 채널 통신의 불확정 전송방법(130)을 이용하여 사용자 기기(100)가 전송받은 예비 가명이 올바른지 서비스 제공자(120)로부터 확인한다(154, 156).
- [0019] 판단기관(110)은 서비스 제공자(120)에게 가명의 사용 허가 메시지를 전달한다(158). 이후 사용자 기기(100)는 자신의 조합된 가명을 이용하여 서비스 제공자(120)에게 서비스를 요청한다(160). 필요에 따라, 판단기관(110)과 서비스 제공자(120)은 서로 협력하여 가명의 사용자가 누구인지 추적할 수 있다. 또한 가명의 사용을 철회할 수 있다(162).
- [0020] 본 발명에 따른 불확정 전송방법을 기반으로 하는 가명 인증 방법은 사용자 기기, 서비스 제공자 및 판단기관이 상호 통신 가능하도록 연결되는 예비 단계; 상기 사용자 기기는 상기 판단기관으로부터 복수의 예비 가명 색인을 전송받는 단계; 상기 사용자 기기가 상기 예비 가명 색인을 이용하여 불확정 전송방법으로 상기 서비스 제공자로부터 복수의 예비 가명 및 상기 복수의 예비 가명에 대한 제1 인증키를 전송받는 단계; 상기 사용자 기기가 상기 제1 인증키를 상기 판단기관에게 전송하는 단계; 상기 사용자 기기는 상기 판단기관이 상기 제1 인증키를 확인하여 상기 예비 가명의 유효 여부를 검사하고, 유효한 경우에 발급하는 상기 예비 가명의 사용허가를 전송받는 단계; 및 상기 사용자 기기는 상기 예비 가명을 조합한 가명을 이용하여 상기 서비스 제공자에게 서비스를 요청하는 단계;를 포함한다.
- [0021] 여기서, 상기 예비 가명을 조합한 가명은 상기 복수의 예비 가명을 서로 곱하여 조합될 수 있다.
- [0022] 또한, 상기 예비 단계는 상기 서비스 제공자는 비밀키를 선택하고, 예비 가명 집합을 준비하는 단계; 및 상기 서비스 제공자가 상기 예비 가명에 관한 색인 집합과 부분 예비 가명 집합을 판단기관과 공유하는 단계를 포함할 수 있다.
- [0023] 또한, 상기 예비 가명은 상기 서비스 제공자가 제1 난수를 결합하여 암호화 함수 형태로 전송할 수 있으며, 상기 사용자 기기는 추후의 가명 사용시 활용하기 위하여 상기 제1 난수를 포함하는 암호화 함수를 저장할 수 있다.
- [0024] 또한, 상기 사용자 기기가 상기 예비 가명을 조합한 가명과 제2 난수와 결합하여 상기 서비스 제공자에 전송하며 상기 서비스를 요청할 수 있으며, 상기 예비 가명의 사용허가는 상기 예비 가명의 해시 함수를 포함하고, 상기 사용자 기기는 상기 해시 함수를 상기 서비스 제공자에게 전송할 수 있다.
- [0025] 또한, 상기 예비 가명의 유효 여부는 상기 서비스 제공자가 불확정 전송방법으로 상기 판단기관으로 전송한 제2 인증키를 상기 판단기관이 상기 제1 인증키와 비교하여 판단되거나, 사전에 저장된 인증키와 비교하여 검토될 수 있다.
- [0026] 하기의 설명에서 상기 과정을 상세히 검토한다.

[0027] 표 1은 본 발명의 설명을 위해 사용될 기호 및 구조체를 나타낸다.

표 1

기호		설명
함수	$(b_1, b_2, \dots, b_m) = OT_m^m(a_1, a_2, \dots, a_n)$	m -out-of- n Oblivious Transfer. $\{a_i\}$ 는 선택할 수 있는 비밀, $\{b_i\}$ 는 선택되어 전송된 값
	$H(a)$	$H: \mathbb{G} \rightarrow \mathbb{G}$ 인 일 방향 함수
	$\exp(a, k)$	a 의 k 제곱
	$n(A)$	집합 A 의 원소의 개수
	$Cert_X(a)$	a 와 참가자 X 에 의한 a 의 서명 값
	$Log(X)$	가명 X 를 사용하는 사용자의 로그
	$ENC_{PK}(a)$	공개키 PK 에 의한 a 의 암호화
	$DEC_{SK}(a)$	비밀키 SK 에 의한 a 의 복호화
레코드 구조 정의 및 선택	$\alpha_i : \beta_i$	인덱스 α_i 에 연결된 요소 β_i
	L_α	요소 α 에 대한 집합, (속성이 α 인 값들의 집합)
	$L_\alpha \Leftarrow L_\beta$	요소 β 에 해당하는 요소 α 의 집합
참여자 식별자	JA	판단 기관의 식별자
	SP	서비스 제공자의 식별자
	U	사용자의 식별자
시스템 파라미터	$\max$	최대 예비 가명 풀의 크기
	m, n	시스템 파라미터, $m \ll n \ll \max$
메시지	OK	가명 획득 절차의 확인 메시지
	REQ	가명 획득 절차의 시작 메시지
기타	$\rightarrow, \leftarrow$	메시지의 전송 방향
	$time$	현재 시간의 타임스탬프

[0028]

[0029] 암호화 함수 $ENC_{PK}()$ 는 $ENC_{PK}(a_1 \times a_2) = ENC_{PK}(a_1) \times ENC_{PK}(a_2)$ 인 특징을 만족하는 모든 암호화 함수를 사용할 수 있다. 예를 들어 RSA 및 ElGamal등이 사용 가능하다.

[0030] 도 2는 본 발명의 일실시예인 가명 획득방법에 대해 설명한 간략한 신호 흐름도이다.

[0031] 가명 획득을 위해, 필요한 위수(order)가 q 인 곱셈 순환 그룹 (Multiplicative Cyclic Group) $\mathbb{G}$ 라 하고, 그룹 $\mathbb{G}$ 의 생성자를 g 라 하면, 서비스 제공자(120)는 자신의 비밀키 $x \in_R \mathbb{Z}_q$ 와 $b \in_R \mathbb{Z}$ 를 선택하고, 예비 가명 집합 $L_{v:(c,e,s)} = \{v_1:(c_1, e_1, s_1), \dots, v_{\max}:(c_{\max}, e_{\max}, s_{\max})\}$ 을 하기의 표 2와 같이 설정한다.

표 2

v	c	e	s
1	g^{a_1}	$g^b g^{a_1 x}$	...
2	g^{a_2}	$g^b g^{a_2 x}$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$
max	$g^{a_{\max}}$	$g^b g^{a_{\max} x}$	...

[0032]

- [0033] 이때, $a_i \in_R \mathbb{Z}_q^*$ 에 대하여, $c_i = g^b g^{a_i x}$ 와 $e_i = g^{a_i}$ 를 만족하며, $s_i \in_R \mathbb{Z}_q^*$ 가 된다. v_i 는 인덱스로써, $1 \leq i \leq \max$ 에 대해서 $v_i = i$ 일 수 있으나, 이후에 집합에서 예비 가명이 제거되었을 때, 이값이 변경될 수 있다.
- [0034] 서비스 제공자(120)는 색인 집합 $L_v = \{v_1, \dots, v_{\max}\}$ 과 부분 예비 가명 집합 $L_c = \{e_1, \dots, e_{\max}\}$ 을 판단기관(110)과 공유한다. 판단기관(110)은 서비스 제공자(120)와 공유한 L_v 를 색인 직함으로 사용한다.
- [0035] 사용자 기기(100)는 서비스 제공자(120)와 판단기관(110)에 각각 실명으로 인증을 시도하고, 안전한 통신 채널을 확보한다. 또한 판단기관(110)과 서비스 제공자(120)는 자신들의 서명을 위한 비밀키를 가지고 있고, 서로의 공개키도 알고 있다. m, n 은 시스템의 보안 파라미터로 사전에 협의되어 공개되어 있다.
- [0036] 사용자 기기(100)는 판단기관(110)과 서비스 제공자(120)에 실명으로 인증을 시도하고, 안전한 통신 채널을 확보한다.
- [0037] 먼저 사용자 기기(100)는 판단기관(110)에게 가명을 얻고 싶은 서비스 제공자(120)의 식별자를 첨부하여 가명 획득 절차 시작 요청 메시지를 보낸다. ($U \rightarrow JA: REQ, SP$)
- [0038] 판단기관(110)은 L_v 로부터 무작위로 $L_v' \subset L_v$ 와 $L_v'' \subset L_v'$ 를 선택한 후 이를 사용자 기기(100)에게 전송한다. 이때, $m = n(L_v') \ll n(L_v'') \ll \max = n(l_v)$ 인 관계를 만족한다. ($JA \rightarrow U: Cert_{JA}(L_v', U, time), L_v''$)
- [0039] 사용자 기기(100)는 판단기관(110)으로부터 받은 $Cert_{JA}(L_v', U, time)$ 을 서비스 제공자(120)에게 전송한다. ($U \rightarrow SP: Cert_{JA}(L_v', U, time)$)
- [0040] 서비스 제공자(120)는 $Cert_{JA}(L_v', U, time)$ 이 유효한지 확인한다. 유효하지 않다면 절차를 중단한다. 유효한 경우, 서비스 제공자(120)는 예비 가명 집합 $L_{v:(c, e, s)}$ 로부터 L_v' 에 해당하는 $L_{v:(c, s)} = \{(v_1': (c_1', s_1')), \dots, (v_n': (c_n', s_n'))\}$ 을 선택하고, 무작위로 선택한 $k \in_R \mathbb{Z}_q$ 에 대해서 $L_{v:exp(c, k)}' = \{(v_1': (c_1')^k), \dots, (v_m': (c_n')^k)\}$ 을 생성한다. 여기서 $exp(c_i, k) = (c_i)^k = g^{bk} g^{a_i kx}$ 와 같다.
- [0041] 서비스 제공자(120)는 $ENC_{PK_{sp}}(k)$ 처럼 k 를 서명과 함께 사용자 기기(100)에게 암호화하여 전송한다. 사용자 기기(100)는 가명을 사용할 때 이용하기 위하여 $ENC_{PK_{sp}}(K)$ 를 반드시 저장해야 한다. ($SP \rightarrow U: ENC_{PK_{sp}}(k)$)
- [0042] 사용자 기기(100)와 서비스 제공자(120)는 $L_{v:(exp(c, k), s)}' = \{L_{v:exp(c, k)}', L_{v:s}'\}$ 에 대한 불확정 전송을 수행한다. ($U \leftarrow SP: (L_{v:(exp(c, k), s)}' \Leftarrow L_v'') = OT_n^m(L_{v:(exp(c, k), s)}' \Leftarrow L_v')$)
- [0043] 사용자 기기(100)는 L_v' 으로 지정된 $L_{v:(exp(c, k), s)}'$ 로부터 L_v'' 에 따라 $L_{v:(exp(c, k), s)}'' = \{L_{v:exp(c, k)}'', L_{v:s}''\}$ 을 선택하여 가져온다.
- [0044] 사용자 기기(100)는 가져온 $L_{v:(exp(c, k), s)}'' = \{L_{v:exp(c, k)}'', L_{v:s}''\}$ 의 $L_{v:exp(c, k)}''$ 로부터 $C^k = (C_1'')^k \times \dots \times (C_m'')^k$ 을 계산한다.
- [0045] 이후 사용자 기기(100)는 판단기관(110)에게 $L_{v:s}''$ 을 전송하고($U \rightarrow JA: L_{v:s}''$), 판단기관(110)은 서비스 제공자(120)에게 L_v' 을 전송한다. ($JA \rightarrow SP: L_v'$)
- [0046] 판단기관(110)은 사용자 기기(100)로부터 전송받은 $L_{v:s}''$ 에 대한 불확정 전송을 수행한다. 판단기관(110)은 $L_{v:s}'$ 중에서 L_v'' 에 따라 $L_{v:s}''$ 을 선택하여 가져온다. ($JA \leftarrow SP: L_{v:s}'' = OT_n^m(L_{v:s}' \Leftarrow L_v'')$)
- [0047] 판단기관(110)은 사용자 기기(100)로부터 전송 받은 $L_{v:s}''$ 과 서비스 제공자(120)로부터 불확정 전송을 통해 얻은 $L_{v:s}''$ 을 서로 비교하여 사용자 기기(100)가 올바른 예비 가명을 서비스 제공자(120)로부터 얻어왔는지 확인한다.
- [0048] 판단기관(110)과 서비스 제공자(120)가 미리 L_s 를 공유함으로써 예비 가명의 유효성 확인단계를 일반화할 수 있

다. 판단기관(110)은 서비스 제공자(120)로부터 L_s 의 일부를 지속적으로 추출하기 때문에 많은 시간이 흐른 후에는 모든 L_s 를 가져올 수 있다. 이에 대해 판단기관(110)은 서비스 제공자(120)로부터 L_s 전체를 처음부터 공유함으로써 본 단계 없이 사용자 기기(100)가 올바른 가명을 가져왔는지 확인할 수 있을 것이다.

[0049] 사용자 기기(100)가 올바른 예비 가명을 가져왔다면 판단기관(110)은 사용자 기기(100)에게 $E=e_1 \times \dots \times e_m$ 을 생성하고 사용자 기기(100)에게 $Cert_{JA}(OK, U, time)$ 과 $H(E)$ 를 전송한다. ($JA \rightarrow U: Cert_{JA}(OK, U, time), H(E)$) $Cert_{JA}(OK, U, time)$ 에는 시간, 사용자 기기(100)의 식별자 등의 정보 이외에 필요에 따라 다른 메시지를 담고 있을 수 있다.

[0050] 판단기관(110)은 사용자 기기(100)의 실명과 L_v 을 이용하여 구한 $E=e_1 \times \dots \times e_m$ 을 연관시켜 저장한다. 사용자 기기(100)가 올바른 예비 가명을 가져오지 못한 경우, 판단기관(110)은 서비스 제공자(120)에게 현재 프로토콜을 수행하고 있는 사용자 기기(100)의 식별자 U 를 전송함으로써, 이후 사용자 기기(100)와의 통신을 중지시키도록 요청한다. ($JA \rightarrow SP: U$)

[0051] 사용자 기기(100)는 서비스 제공자(120)에게 판단기관(110)으로 받은 $Cert_{JA}(OK, U, time)$ 를 재전송한다. ($U \rightarrow SP: Cert_{JA}(OK, U, time)$)

[0052] 서비스 제공자(120)는 사용자 기기(100)로부터 받은 $Cert_{JA}(OK, U, time)$ 가 올바른지 확인하고, 올바른 경우에만 하여 L_v' 에 의해서 지정된 $L_{v:e} = \{(v_1':e_1'), \dots, (v_n':e_n')\}$ 에 대해서 $L_{v:\exp(e,k)} = \{(v_1':(e_1')^k), \dots, (v_n':(e_n')^k)\}$ 를 계산하여 사용자 기기(100)에게 전송한다. 여기서 $\exp(e_i, k) = (e_i)^k = g^{a_i k}$ 와 같다. ($SP \rightarrow U: L_{v:\exp(e,k)}' \leftarrow L_v'$)

[0053] 서비스 제공자(120)로부터 $L_{v:\exp(e,k)}'$ 을 전송받은 사용자 기기(100)는 $(L_{v:\exp(e,k)}'' \leftarrow L_v'') \subset L_{v:\exp(e,k)}'$ 를 구하고 $E_k = (e_1'')^k \times \dots \times (e_m'')^k$ 를 계산한다.

[0054] 도 3은 본 발명의 일실시예인 가명의 사용방법에 대한 간략한 신호 흐름도이다.

[0055] 일정 시간이 흐른 후, 사용자 기기(100)는 서비스 제공자(120)에게 가명을 사용하여 서비스를 요청한다. 가명을 획득 후 바로 서비스를 요청할 경우 프로토콜 외적인 부분에서 사용자의 실명이 노출될 가능성이 매우 높다.

[0056] 사용자 기기(100)는 획득한 가명을 사용하기 위하여 $r, r' \in_R \mathbb{Z}_q$ 를 선택하고 $C' = (C^k)^r$, $E' = (E^k)^r$, $ENC_{PK_{sp}}(rk)$, $ENC_{SSK}(H(E))$ 를 계산하여 SP에게 전송한다. ($U \rightarrow SP: C' E' ENC_{PK_{sp}}(rk), ENC_{SSK}(H(E))$)

[0057] 여기서 $ENC_{PK_{sp}}(rk)$ 는 암호화 함수에 따라 $ENC_{PK_{sp}}(rk) = ENC_{PK_{sp}}(r) * ENC_{PK_{sp}}(k)$ 또는 $ENC_{PK_{sp}}(rk) = r * ENC_{PK_{sp}}(k)$ 로 나타낼 수 있으며, SSK는 익명의 사용자 기기(100)와 서비스 제공자(120)가 협의하여 만든 세션 비밀키이다.

[0058] 사용자 기기(100)가 보낸 메시지에서 $w = DEC_{SK_{sp}}(ENC_{PK_{sp}}(rk))$, $h = DEC_{SSK}(ENC_{SSK}(H(E)))$ 를 계산하고, $(g^{bw})^w = C' / (E')^x$ 인지 확인한다. 만약 그렇지 않다면 프로토콜을 중지한다.

[0059] 모두 옳다면 가명으로 $P = (E')^{1/w}$ 로 계산하고 $H(P) = h$ 인지 확인한다. 서로 값이 다르다면 역시 프로토콜을 중지한다. 가명 P에 대한 레코드에 이를 재전송 공격으로 간주할만한 기록이 있다면 이후의 통신을 차단한다. 그렇지 않다면 해당 레코드에 사용자 기기(100)가 보낸 메시지를 기록하고 이후의 접속을 허용한다. 이후의 행동은 로그로 남겨둔다.

[0060] 도 4는 본 발명의 일실시예인 사용자 실명의 조건부 추적방법에 대한 간략한 신호 흐름도이다.

[0061] 사용자의 실명을 추적하기 위해서는 판단기관(110)과 서비스 제공자(120)의 협력이 필요하다. 서비스 제공자(120)는 가명 P에 대한 접속 로그 $\text{Log}(P)$ 를 가지고 있다. 이를 근거로 판단기관(110)에게 협력을 요청하면 판단기관(110)은 이를 확인하고 서비스 제공자(120)에게 실명 정보를 제공한다. 판단기관(110)은 스스로의 $\text{Log}(P)$ 분

석 결과, 서비스 제공자(120)의 요청을 거부할 수 있다.

- [0062] 서비스 제공자(120)는 사용자 기기(100)의 가명 P와 해당 사용자 기기(100)의 $\text{Log}(P)$ 를 판단기관(110)에게 전송한다. 판단기관(110)은 $\text{Log}(P)$ 를 분석하고 P와 일치하는 E를 가진 사용자 기기(100)의 식별자 U를 서비스 제공자(120)에게 전송한다.
- [0063] 서비스 제공자(120)는 이후의 해당 사용자로부터 요청되는 가명 획득 절차 자체를 거부하거나 사용자에게 유예기한을 둘 수 있을 것이다. 한편, 서비스 제공자(120)와 판단기관(110)은 다른 형태의 협력을 통하여 완전한 실명 노출을 통하지 않고도 특정 사용자를 시스템에서 제한할 수도 있다.
- [0064] 서비스 제공자(120)는 단독으로 특정 가명의 접근을 제한할 수 있다. 그러나 서비스 제공자(120)는 사용자의 실명을 모르기 때문에 해당 사용자는 새로운 가명을 획득하여 서비스 제공자(120)에게 계속 서비스를 요청할 수도 있다. 이러한 상황을 막기 위하여 서비스 제공자(120)는 특정 가명의 접근을 제한하는 동시에 판단기관(110)에 특정 가명을 전송하여 해당 가명 사용자에게 대한 새로운 가명 획득절차를 시작하지 못하도록 요청해야 한다.
- [0065] 본 발명에 따른 프로토콜에서 사용자 기기의 가명은 판단기관에 의해서 결정된다. 가명은 판단기관이 선택한 L_v 에 의해서 선택되고 L_v , L_v' 및 L_v'' 의 관계에 의해서 서비스 제공자로부터의 사용자 익명성이 만들어지게 된다. 만약 판단기관이 선택한 L_v' 와 L_v'' 가 사용자마다 배타적으로 선택될 경우 서비스 제공자는 사용자의 실명을 추측할 수 있게 된다.
- [0066] 서비스 제공자의 입장에서 바라보았을 때, 사용자 기기가 가져가는 예비 가명 (L_c' 와 L_c'')과 판단기관이 사용자 기기의 예비 가명의 유효성을 검증하기 위하여 가져간 L_s 는 동일한 불확정 전송(OT)을 두 번 수행한 것이다. 추출을 시도하는 대상(즉, L_v')과 추출되는 대상(즉, L_v'')이 동일하다.
- [0067] 그러나 서비스 제공자는 두 번의 동일한 불확정 전송(OT)이 발생하였다 하더라도, 불확정 전송방법으로 이루어지므로 서비스 제공자는 사용자 기기가 어떠한 예비 가명을 가져갔는지 확인하기 어렵다. 따라서 서비스 제공자가 바라보았을 때 사용자 기기는 최대 n^m 개의 가명을 가질 수 있어 사용 가능한 가명집합이 증가한다.
- [0068] 외부에서 바라보았을 때, 사용자 기기의 가명을 알아내거나, 가명끼리 연결하는 것은 매우 힘들다. 가명은 매년 다른 난수로 재암호화 되어 서비스 제공자에게 전송되므로 옆에서 메시지를 엿듣는 공격자가 있다하더라도 서로 이를 연결하기 위하여서는 사용자 기기가 선택하는 난수 r을 알아내야 하지만 이는 DLP (Discrete Logarithm Problem)를 푸는 것과 같다.
- [0069] 서비스 제공자의 입장에서, 서비스 제공자는 사용자의 실명과 연결된 k를 알고 있으므로 사용자 기기의 가명이 어떠한 k에 의해서 변형되어 있는지 확인하면 서비스 제공자는 사용자의 실명을 알아낼 수 있다. 그러나 사용자 기기가 전송한 가명 정보에서 k는 언제나 사용자 기기가 선택한 r과 연결되어 있기 때문에 서비스 제공자는 이를 단독으로 확인할 수단이 없으므로 가명과 실명을 연결시킬 수 없다.
- [0070] 또한, 사용자 기기가 갖게 되는 가명과 가명의 유효성 정보는 서비스 제공자가 생성하는 난수 k에 따라 달라지므로 사용자 중에서 공모하여 가명을 생성하려는 자들은 자신이 알고 있는 예비 가명을 서로 합칠 수 없으며, 유사하게 사용자 자신이 얻은 정보를 이용하여 적법하지 않지만 유효한 가명을 만드는 것도 사용자 기기가 알지 못하는 k로 인해서 가명을 임의로 재조합할 수 없다.
- [0071] 본 발명에 따른 프로토콜에서는 사용자 기기의 익명성은 두 참여자, 즉 판단기관과 서비스 제공자가 모두 동의해야 제한적으로 실명이 추적되므로 어느 한 참여자가 실명이 가명에 대한 사용 정보를 보유하는 경우보다 더 보장된다.
- [0072] 서비스 제공자는 판단기관의 협력을 통해 어떤 익명 사용자의 실명을 알아낼 수 있다.(조건부 추적) 서비스 제공자는 이후의 해당 사용자로부터 요청되는 가명 획득 절차 자체를 거부하거나 사용자에게 유예 기한을 둘 수 있을 것이다.
- [0073] 서비스 제공자와 판단기관은 다른 형태의 협력을 통하여 완전한 실명 노출을 통하지 않고도 특정 사용자를 시스템에서 제한할 수도 있다. 서비스 제공자는 단독으로 특정 가명의 접근을 제한할 수 있다.
- [0074] 그러나 서비스 제공자는 사용자의 실명을 모르기 때문에 해당 사용자는 새로운 가명을 획득하여 서비스 제공자에게 계속 서비스를 요청할 수도 있다. 이러한 상황을 막기 위하여 서비스 제공자는 특정 가명의 접근을 제한하는 동시에 판단기관에 특정 가명을 전송하여 해당 가명 사용자에게 대한 새로운 가명 획득 절차를 시작하지 못하

도록 요청할 수 있다.

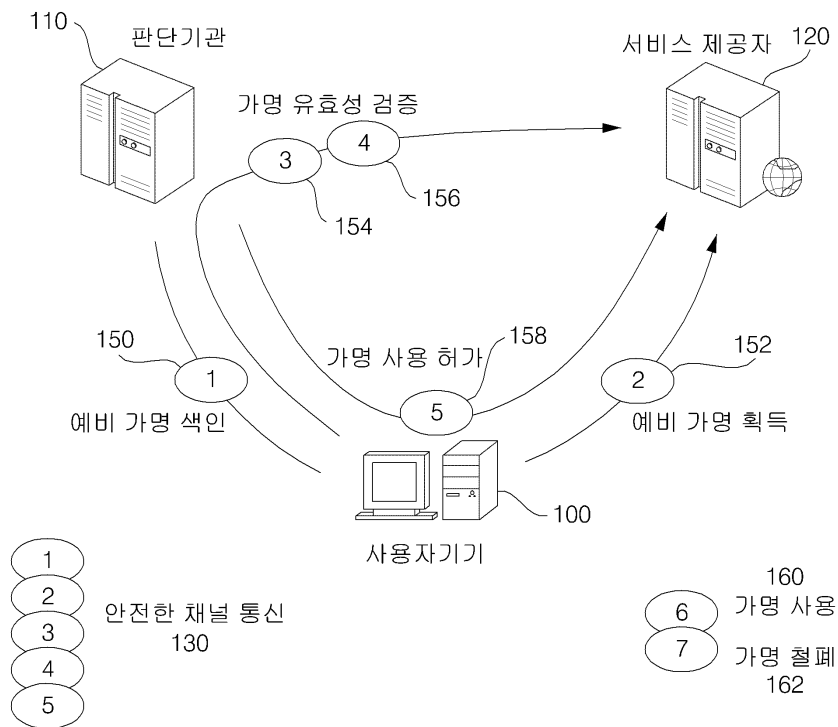
[0075] 이상 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안 될 것이다.

도면의 간단한 설명

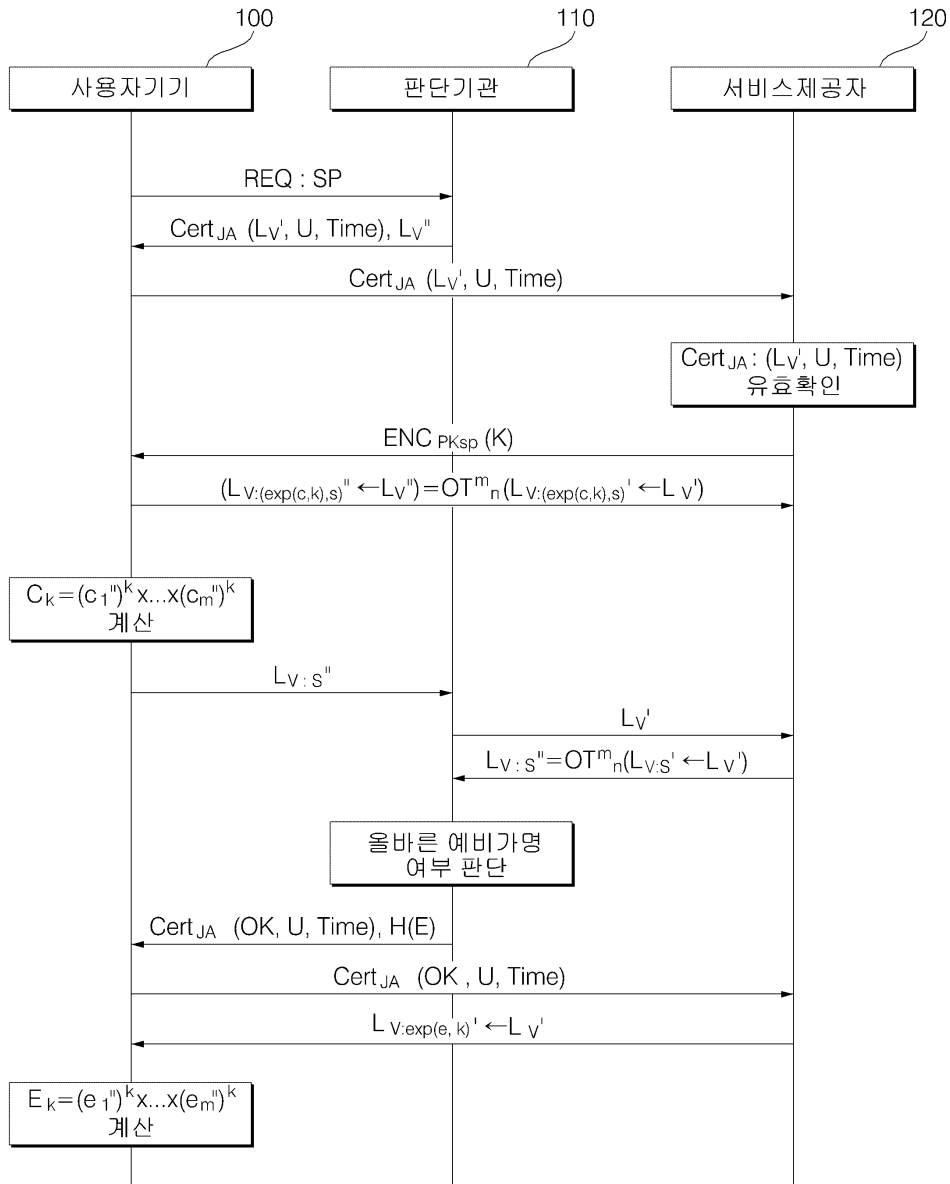
[0076] 도 1은 본 발명의 일실시예인 불확정 전송방법을 기반으로 하는 가명 인증 방법을 간략히 나타낸 도,
 [0077] 도 2는 본 발명의 일실시예인 가명 획득방법에 대해 설명한 간략한 신호 흐름도,
 [0078] 도 3은 본 발명의 일실시예인 가명의 사용방법에 대한 간략한 신호 흐름도,
 [0079] 도 4는 본 발명의 일실시예인 사용자 실명의 조건부 추적방법에 대한 간략한 신호 흐름도이다.

도면

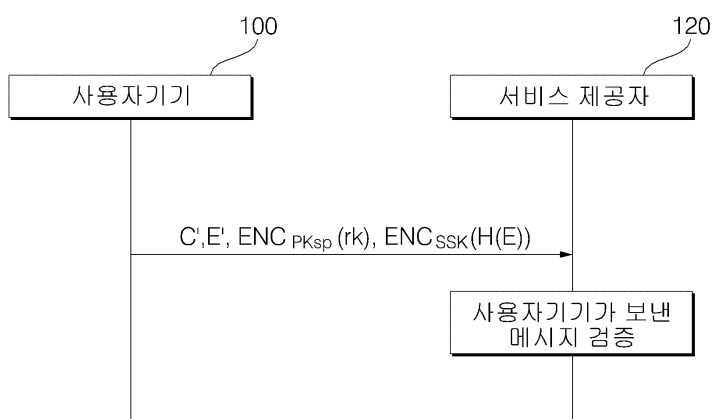
도면1



도면2



도면3



도면4

