(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0026765
(43) 공개일자 2017년03월09일

(51) 국제특허분류(Int. Cl.)
*H04L 9/32* (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
*H04L 9/3271* (2013.01)
*H04L 9/30* (2013.01)
(21) 출원번호 10-2015-0121014
(22) 출원일자 2015년08월27일
심사청구일자 2015년08월27일

(71) 출원인
**고려대학교 산학협력단**
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
**정익래**
서울특별시 광진구 아차산로 503-23, 103동 1701호 (광장동, 청구아파트)
**백목련**
경기도 안양시 동안구 동편로 4단지 405동 1702호
**김동민**
서울특별시 동대문구 약령시로 154 1동 505호 (청량리동,미주아파트)
(74) 대리인
**김등용, 김홍석**

전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **자체 인증 서명을 기반으로 하는 공공 감사 방법 및 시스템**

## (57) 요 약

본 발명은 자체 인증 서명을 기반으로 하는 공공 감사 방법 및 시스템에 관한 것으로서, 일실시예에 따른 공공 감사 방법은 인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급하는 단계, 상기 인증기관(TA, Trust Authority) 서버에서 상기 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성하여 상기 사용자 단말기를 통해 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 단계, 상기 사용자 단말기에서 상기 위트니스 전송에 상응하여 데이터에 대한 서명을 생성하고, 상기 데이터와 상기 생성된 서명을 클라우드 서버에 전송하는 단계, 및 상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고, 상기 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인하는 단계를 포함한다.

*대 표 도* - 도5

(52) CPC특허분류
*H04L 9/321* (2013.01)
*H04L 9/3247* (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 IITP-2015-H8501-15-1003
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 ITRC
연구과제명 제어시스템 보안 연구
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2015.01.01 ~ 2015.12.31

# *명 세 서*

## *청구범위*

### 청구항 1

인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급하는 단계;

상기 인증기관(TA, Trust Authority) 서버에서 상기 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성하여 상기 사용자 단말기를 통해 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 단계;

상기 사용자 단말기에서 상기 위트니스 전송에 상응하여 데이터에 대한 서명을 생성하고, 상기 데이터와 상기 생성된 서명을 클라우드 서버에 전송하는 단계; 및

상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고, 상기 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인하는 단계

를 포함하는 자체 인증 서명을 기반으로 하는 공공 감사 방법.

### 청구항 2

제1항에 있어서,

상기 데이터의 변조 여부를 확인하는 단계는,

상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 생성된 챌린지(Challenge) 메시지를 상기 클라우드 서버에 전송하는 단계; 및

상기 클라우드 서버에서 상기 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성하여 상기 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 단계; 및

상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인하는 단계

를 포함하는 자체 인증 서명을 기반으로 하는 공공 감사 방법.

### 청구항 3

제1항에 있어서,

상기 데이터의 변조 여부를 확인하는 단계는,

상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 응답(Response) 값을 미리 지정된 검증식에 대입하여 데이터의 변조 여부를 확인하는 공공 감사 방법.

### 청구항 4

제1항에 있어서,

상기 상기 인증기관(TA, Trust Authority) 서버에서 상기 위트니스를 생성하는 단계는,

사용자 단말기에서 소수를 위수로 갖는 곱셈 순환 그룹의 생성자 정보가 반영된 변수를 상기 개인키로 생성하고, 상기 생성한 개인키에 기초하여 영-지식 증명하여 상기 인증기관(TA, Trust Authority) 서버에 회신하는 단계;

상기 인증기관(TA, Trust Authority) 서버에서 검증식이 성립하는지 확인하는 단계;

상기 검증식이 성립하는 경우에 영-지식 증명을 검증하는 단계; 및

상기 인증기관(TA, Trust Authority) 서버에서 상기 영-지식 증명이 검증되면, 위트니스를 생성하여 상기 사용자 단말기로 전송하고, 데이터베이스에 저장하는 단계

를 포함하는 공공 감사 방법.

**청구항 5**

제4항에 있어서,

상기 인증기관(TA, Trust Authority) 서버에서 상기 위트니스를 생성하는 단계는,

상기 검증식이 성립하지 않는 경우, 프로토콜을 종료하는 단계

를 포함하는 공공 감사 방법.

**청구항 6**

제1항에 있어서,

상기 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성하는 단계는,

상기 챌린지(Challenge) 메시지를 구성하는 모든 원소에 대한 모드 연산을 수행하는 단계; 및

상기 수행된 모드 연산된 결과에 공개키와 해시 함수를 이용해서 증명 값을 계산하는 단계

상기 계산된 증명 값을 반영하여 상기 응답(Response) 값을 생성하는 단계

를 포함하는 공공 감사 방법.

**청구항 7**

사용자 단말기에서 소수를 위수로 갖는 곱셈 순환 그룹의 생성자 정보가 반영된 변수를 상기 개인키로 생성하는 단계;

상기 생성한 개인키에 기초하여 영-지식 증명하여 상기 인증기관(TA, Trust Authority) 서버에 회신하는 단계;

상기 인증기관(TA, Trust Authority) 서버에서 검증식이 성립하는지 확인하는 단계;

상기 검증식이 성립하는 경우에 영-지식 증명을 검증하는 단계; 및

상기 인증기관(TA, Trust Authority) 서버에서 상기 영-지식 증명이 검증되면, 위트니스를 생성하여 상기 사용자 단말기로 전송하고, 데이터베이스에 저장하는 단계

를 포함하는 공공 감사 방법.

**청구항 8**

제7항에 있어서,

상기 인증기관(TA, Trust Authority) 서버에서 상기 위트니스를 생성하는 단계는,

상기 검증식이 성립하지 않는 경우, 프로토콜을 종료하는 단계

를 포함하는 공공 감사 방법.

**청구항 9**

적어도 하나의 프로세서를 포함하는 공공 감사 시스템에 있어서, 상기 적어도 하나의 프로세서에 의해 적어도 일시적으로 구현되는:

인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급하는 개인키 발급부;

인증기관(TA, Trust Authority) 서버에서 상기 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성하는 위트니스 생성부; 및

상기 사용자 단말기를 통해 상기 생성한 위트니스를 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 전송부

를 포함하고,

상기 위트니스 전송에 상응하여 생성한 데이터에 대한 서명이 클라우드 서버에 전송되면,

상기 제3 감사자(TPA, Third Party Auditor) 서버가 상기 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고, 상기 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인하는 자체 인증 서명을 기반으로 하는 공공 감사 시스템.

**청구항 10**

제9항에 있어서,

상기 제3 감사자(TPA, Third Party Auditor) 서버는 상기 생성된 챌린지(Challenge) 메시지를 상기 클라우드 서버에 전송하고, 상기 클라우드 서버에서 상기 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성하여 상기 제3 감사자(TPA, Third Party Auditor) 서버로 전송하며, 상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인하는 자체 인증 서명을 기반으로 하는 공공 감사 시스템.

**청구항 11**

제10항에 있어서,

상기 제3 감사자(TPA, Third Party Auditor) 서버는

상기 응답(Response) 값을 미리 지정된 검증식에 대입하여 데이터의 변조 여부를 확인하는 공공 감사 시스템.

**청구항 12**

제10항에 있어서,

상기 제3 감사자(TPA, Third Party Auditor) 서버는 상기 챌린지(Challenge) 메시지를 구성하는 모든 원소에 대한 모드(mod) 연산을 수행하고, 상기 수행된 모드 연산된 결과에 공개키와 해시 함수를 이용해서 증명 값을 계산하며, 상기 계산된 증명 값을 반영하여 상기 응답(Response) 값을 생성하는 공공 감사 시스템.

**청구항 13**

기록매체에 저장되는 공공 감사 프로그램으로서, 상기 프로그램은 컴퓨팅 시스템에서 실행되는:

인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급하는 명령어 세트;

인증기관(TA, Trust Authority) 서버에서 상기 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성하여 상기 사용자 단말기를 통해 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 명령어 세트;

상기 사용자 단말기에서 상기 위트니스 전송에 상응하여 데이터에 대한 서명을 생성하고, 상기 데이터와 상기 생성된 서명을 클라우드 서버에 전송하는 명령어 세트; 및

상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고, 상기 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인하는 명령어 세트

를 포함하는 자체 인증 서명을 기반으로 하는 공공 감사 프로그램.

## 발명의 설명

### 기 술 분 야

[0001] 본 발명은 자체 인증 서명을 기반으로 하는 공공 감사 기술로서, 클라우드 서비스 사용자가 본인의 데이터를 클라우드 스토리지에 업로드한 뒤, TPA(Third Party Auditor)를 통해 클라우드 서버나 다른 공격자의 악의적인 행동으로부터 데이터의 변조 유무를 확인하는 기술적 사상에 관한 것이다.

### 배 경 기 술

[0003] 클라우드 환경에서는 무분별한 접근으로 인한 피해 사례가 빈번하다. 이를 위해, 클라우드 환경에서의 보안 관련 이슈가 부각되고 있으며, 이를 위한 다양한 기술들이 개발되고 있는 추세다.

[0004] 이 중에서, 자체 인증 서명 기법(Self-Certified Signature Scheme)은 자체 인증 공개키에 기반을 둔 방식으로, 별도의 공개키 인증서를 저장하거나 검증할 필요가 없으며 인증서 대신 공개키가 포함된 위트니스(Witness)를 생성한다. 특정 사용자의 식별자와 이에 대응되는 위트니스 쌍을 가진 사람이라면 누구나 공개키를 획득할 수 있으며, 서명을 검증할 수 있다. 자체 인증 서명 기법은 크게 셋업 과정, 키생성 과정, 위트니스 생성 과정, 증명 과정의 4 단계를 포함한다.

[0005] 먼저, 셋업 과정에서 TA(Trust Authority)는 시큐리티 파라미터를 입력 값으로 받아서 시스템 파라미터과 마스터 비밀키를 생성한다. 이후, 키생성 과정에서 사용자는 시큐리티 파라미터를 입력 값으로 받아서 공개키, 개인키 쌍을 생성한다. 위트니스 생성 과정에서, TA(Trust Authority)는 사용자의 식별자인 공개키 그리고 사용자의 개인키에 대한 영-지식 증명(Zero-Knowledge Proof)을 이용하여 위트니스를 생성한다. 또한, 증명 과정에서는 사용자가 보유한 메시지에 대한 서명을 생성하고, 메시지, 서명, 사용자 식별자 그리고 위트니스를 입력 값으로 받아 서명에 대한 정당성을 검증한다.

## 선행기술문헌

### 특허문헌

[0007] (특허문헌 0001) 대한민국 특허공보 제10-0529594호

(특허문헌 0002) 대한민국 특허공보 제10-0561847호

## 발명의 내용

### 해결하려는 과제

[0008] 실시예에 따르면, 클라우드 서비스 사용자가 본인의 데이터를 클라우드 스토리지에 업로드한 뒤, TPA(Third Party Auditor)를 통해 클라우드 서버나 다른 공격자의 악의적인 행동으로부터 데이터의 변조 유무를 확인하는 것이다.

[0009] 실시예에 따르면, 사용자의 대리인이 클라우드에 업로드된 데이터의 무결성을 감사하는 것이다.

[0010] 실시예에 따르면, 연산 복잡도를 낮추면서도 악의적인 공격에도 안전한 새로운 공공 감사 프로토콜을 제공하는 것이다.

## 과제의 해결 수단

[0012] 일실시예에 따른 공공 감사 방법은 인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급하는 단계, 상기 인증기관(TA, Trust Authority) 서버에서 상기 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성하여 상기 사용자 단말기를 통해 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 단계, 상기 사용자 단말기에서 상기 위트니스 전송에 상응하여 데이터에 대한 서명을 생성하고, 상기 데이터와 상기 생성된 서명을 클라우드 서버에 전송하는 단계, 및 상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고, 상기 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인하는 단계를 포함한다.

[0013] 일실시예에 따른 상기 데이터의 변조 여부를 확인하는 단계는, 상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 생성된 챌린지(Challenge) 메시지를 상기 클라우드 서버에 전송하는 단계, 및 상기 클라우드 서버에서 상기 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성하여 상기 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 단계, 및 상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인하는 단계를 포함한다.

[0014] 일실시예에 따른 상기 데이터의 변조 여부를 확인하는 단계는, 상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 응답(Response) 값을 미리 지정된 검증식에 대입하여 데이터의 변조 여부를 확인한다.

[0015] 일실시예에 따른 상기 인증기관(TA, Trust Authority) 서버에서 상기 위트니스를 생성하는 단계는, 상기 사용자 단말기에서 소수를 위수로 갖는 곱셈 순환 그룹의 생성자 정보가 반영된 변수를 상기 개인키로 생성하고, 상기 생성한 개인키에 기초하여 영-지식 증명하여 상기 인증기관(TA, Trust Authority) 서버에 회신하는 단계, 상기 인증기관(TA, Trust Authority) 서버에서 검증식이 성립하는지 확인하는 단계, 상기 검증식이 성립하는 경우에 영-지식 증명을 검증하는 단계, 및 상기 인증기관(TA, Trust Authority) 서버에서 상기 영-지식 증명이 검증되면, 위트니스를 생성하여 상기 사용자 단말기로 전송하고, 데이터베이스에 저장하는 단계를 포함한다.

[0016] 일실시예에 따른 상기 인증기관(TA, Trust Authority) 서버에서 상기 위트니스를 생성하는 단계는, 상기 검증식이 성립하지 않는 경우, 프로토콜을 종료하는 단계를 포함한다.

[0017] 일실시예에 따른 상기 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성하는 단계는, 상기 챌린지(Challenge) 메시지를 구성하는 모든 원소에 대한 모드 연산을 수행하는 단계, 상기 수행된 모드 연산된 결과에 공개키와 해시 함수를 이용해서 증명 값을 계산하는 단계, 및 상기 계산된 증명 값을 반영하여 상기 응답(Response) 값을 생성하는 단계를 포함한다.

[0018] 일실시예에 따른 공공 감사 방법은 사용자 단말기에서 소수를 위수로 갖는 곱셈 순환 그룹의 생성자 정보가 반영된 변수를 상기 개인키로 생성하는 단계, 상기 생성한 개인키에 기초하여 영-지식 증명하여 상기 인증기관(TA, Trust Authority) 서버에 회신하는 단계, 상기 인증기관(TA, Trust Authority) 서버에서 검증식이 성립하는지 확인하는 단계, 상기 검증식이 성립하는 경우에 영-지식 증명을 검증하는 단계, 및 상기 인증기관(TA, Trust Authority) 서버에서 상기 영-지식 증명이 검증되면, 위트니스를 생성하여 상기 사용자 단말기로 전송하고, 데이터베이스에 저장하는 단계를 포함한다.

[0019] 일실시예에 따른 상기 인증기관(TA, Trust Authority) 서버에서 상기 위트니스를 생성하는 단계는, 상기 검증식이 성립하지 않는 경우, 프로토콜을 종료하는 단계를 포함한다.

[0020] 일실시예에 따른 공공 감사 시스템은 인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급하는 개인키 발급부, 인증기관(TA, Trust Authority) 서버에서 상기 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성하는 위트니스 생성부, 및 상기 사용자 단말기를 통해 상기 생성한 위트니스를 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 전송부를 포함하고, 상기 위트니스 전송에 상응하여 생성한 데이터에 대한 서명이 클라우드 서버에 전송되면, 상기 제3 감사자(TPA, Third Party Auditor) 서버가 상기 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고, 상기 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인하는 자체 인증 서명을 기반으로 한다.

[0021] 일실시예에 따른 상기 제3 감사자(TPA, Third Party Auditor) 서버는 상기 생성된 챌린지(Challenge) 메시지를 상기 클라우드 서버에 전송하고, 상기 클라우드 서버에서 상기 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성하여 상기 제3 감사자(TPA, Third Party Auditor) 서버로 전송하며, 상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인하는 자체 인증 서명을 기반으로 한다.

[0022] 일실시예에 따른 상기 제3 감사자(TPA, Third Party Auditor) 서버는 상기 응답(Response) 값을 미리 지정된 검증식에 대입하여 데이터의 변조 여부를 확인한다.

[0023] 일실시예에 따른 상기 제3 감사자(TPA, Third Party Auditor) 서버는 상기 챌린지(Challenge) 메시지를 구성하는 모든 원소에 대한 모드(mod) 연산을 수행하고, 상기 수행된 모드 연산된 결과에 공개키와 해시 함수를 이용해서 증명 값을 계산하며, 상기 계산된 증명 값을 반영하여 상기 응답(Response) 값을 생성한다.

[0024] 일실시예에 따른 공공 감사 프로그램은 인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급하는 명령어 세트, 인증기관(TA, Trust Authority) 서버에서 상기 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성하여 상기 사용자 단말기를 통해 제3 감사자(TPA, Third Party Auditor) 서버로 전송하는 명령어 세트, 상기 사용자 단말기에서 상기 위트니스 전송에 상응하여 데이터에 대한 서명을 생성하고, 상기 데이터와 상기 생성된 서명을 클라우드 서버에 전송하는 명령어 세트, 및 상기 제3 감사자(TPA, Third Party Auditor) 서버에서 상기 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고, 상기 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인하는 명령어 세트를 포함한다.

## *발명의 효과*

[0026] 실시예들에 따르면, 클라우드 서비스 사용자가 본인의 데이터를 클라우드 스토리지에 업로드한 뒤, TPA(Third Party Auditor)를 통해 클라우드 서버나 다른 공격자의 악의적인 행동으로부터 데이터의 변조 유무를 확인할 수 있다.

[0027] 실시예에 따르면, 사용자의 대리인이 클라우드에 업로드된 데이터의 무결성을 감사할 수 있다.

[0028] 실시예에 따르면, 연산 복잡도를 낮추면서도 악의적인 공격에도 안전한 새로운 공공 감사 프로토콜을 제공할 수 있다.

## *도면의 간단한 설명*

[0030] 도 1은 일실시예에 따른 자체 인증 서명을 기반으로 하는 공공 감사 방법을 설명하는 흐름도이다.

도 2는 제3 감사자(TPA, Third Party Auditor) 서버에서 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인하는 실시예를 설명하는 흐름도이다.

도 3은 일실시예에 따른 위트니스를 생성하는 실시예를 설명하는 흐름도이다.

도 4는 응답(Response) 값을 생성하는 실시예를 설명하는 흐름도이다.

도 5는 일실시예에 따른 공공 감사 시스템을 설명하는 도면이다.

## *발명을 실시하기 위한 구체적인 내용*

[0031] 이하에서, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 이러한 실시예들에 의해 권리범위가 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0032] 아래 설명에서 사용되는 용어는, 연관되는 기술 분야에서 일반적이고 보편적인 것으로 선택되었으나, 기술의 발달 및/또는 변화, 관례, 기술자의 선호 등에 따라 다른 용어가 있을 수 있다. 따라서, 아래 설명에서 사용되는 용어는 기술적 사상을 한정하는 것으로 이해되어서는 안 되며, 실시예들을 설명하기 위한 예시적 용어로 이해되어야 한다.

[0033] 또한 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세한 그 의미를 기재할 것이다. 따라서 아래 설명에서 사용되는 용어는 단순한 용어의 명칭이 아닌 그 용어가 가지는 의미와

명세서 전반에 걸친 내용을 토대로 이해되어야 한다.

[0034] 도 1은 일실시예에 따른 자체 인증 서명을 기반으로 하는 공공 감사 방법을 설명하는 흐름도이다.

[0035] 일실시예에 따른 공공 감사 방법은 클라우드 서비스의 사용자 단말기, 인증기관(TA, Trust Authority) 서버, 제3 감사자(TPA, Third Party Auditor) 서버, 클라우드 서버 총 4개의 파티를 가정한다. 또한, 일실시예에 따른 공공 감사 방법은 이 파티들을 통해 키 생성 과정, 위트니스 생성 과정, 메시지에 대한 태그 생성 과정, 제3 감사자(TPA, Third Party Auditor) 서버의 챌린지 메시지 생성 과정, 클라우드 서버가 챌린지 메시지에 대한 응답 값 생성 과정, 최종적으로 제3 감사자(TPA, Third Party Auditor) 서버가 클라우드 서버로부터 받은 응답 값의 정당성을 확인하는 과정을 포함한다.

[0036] 구체적으로, 일실시예에 따른 공공 감사 방법은 인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급한다(101).

[0037] 클라우드의 사용자 단말기는 $x \in Z_q^*$ 와 $s \in Z_q^*$ 를 랜덤하게 선택하여 $e(g_1, g_1)^x$ 와 $e(g_1, g_1)^s$ 를 계산한다. 여기서 개인키는 $sk_v = \{sk_{v1}, sk_{v2}\} = \{x, s\}$, 공개키는 $pk_v = \{pk_{v1}, pk_{v2}\} = \{e(g_1, g_1)^x, e(g_1, g_1)^s\}$ 로 설정한다.

[0038] $G_1$과 $G_2$는 q를 위수로 가지는 곱셈 순환군이고 $q_1$은 $G_1$의 생성자이며, $e: G_1 \times G_1 \rightarrow G_t$ 는 겹선형 함수이다. 인증기관(TA, Trust Authority) 서버는 $\alpha \in Z_q^*$ 를 랜덤하게 선택하고 $g_1^\alpha$ 를 계산하여 $(MSK = \alpha, MPK = g_1^\alpha)$ 를 각각 마스터 개인키, 공개키로 설정한다. 뿐만 아니라 인증기관(TA, Trust Authority) 서버는 암호학적으로 안전한 해시(Hash) 함수 $H_1: \{0,1\}^* \rightarrow G_1$ 와 $H_2: \{0,1\}^* \rightarrow Z_q$ 를 선택한다. 최종적으로 생성된 시스템 파라미터는 $\{q, G_1, G_T, e, g_1, MPK, H_1, H_2, PK = e(g_1, g_1)\}$ 이다

[0039] 일실시예에 따른 공공 감사 방법은 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성하고(102), 사용자 단말기를 통해 제3 감사자(TPA, Third Party Auditor) 서버로 전송한다(103).

[0040] 일실시예에 따른 공공 감사 방법은 위트니스 전송에 상응하여 데이터에 대한 서명을 생성한다(104). 또한, 일실시예에 따른 공공 감사 방법은 데이터와 생성된 서명을 클라우드 서버에 전송한다(105).

[0041] 일실시예에 따른 공공 감사 방법은 제3 감사자(TPA, Third Party Auditor) 서버에서 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고(106), 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인한다(107).

[0042] 도 2는 제3 감사자(TPA, Third Party Auditor) 서버에서 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인하는 실시예를 설명하는 흐름도이다.

[0043] 데이터의 변조 여부를 확인하기 위해, 일실시예에 따른 공공 감사 방법은 제3 감사자(TPA, Third Party Auditor) 서버에서 생성된 챌린지(Challenge) 메시지를 클라우드 서버에 전송한다(201).

[0044] 다음으로, 일실시예에 따른 공공 감사 방법은 클라우드 서버에서 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성하여(202), 제3 감사자(TPA, Third Party Auditor) 서버로 전송한다(203).

[0045] 일실시예에 따른 공공 감사 방법은 제3 감사자(TPA, Third Party Auditor) 서버에서 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인한다(204).

[0046] 예를 들어, 공공 감사 방법은 데이터의 변조 여부를 확인하기 위해 제3 감사자(TPA, Third Party Auditor) 서버에서 응답(Response) 값을 미리 지정된 검증식에 대입하여 데이터의 변조 여부를 확인할 수 있다.

[0047] 클라우드에 업로드된 사용자의 데이터 파일 M의 데이터 무결성을 검증하기 위하여 제3 감사자(TPA, Third Party Auditor) 서버는 검증을 위한 챌린지 메시지를 생성한다.

[0048] 제3 감사자(TPA, Third Party Auditor) 서버는 해당 파일의 모든 블록을 검증하는 대신, $l$ 개의 샘플 블록들을 랜덤하게 선택한다. 랜덤하게 선택된 블록의 집합은 L로 표현된다. 그리고 나서 $r \in Z_q$ 를 랜덤하게 선택한다.

[0049] 제3 감사자(TPA, Third Party Auditor) 서버는 챌린지 메시지 $Chal = \{L, r\}_{1 \le L \le n}$ 를 생성하여 클라우드 서버

에게 전송한다.

[0050] 챌린지 메시지 $Chal = \{L, r\}_{1 \le L \le n}$ 를 받은 클라우드 서버는 이에 대한 정당한 증명 값을 계산하기 위해 다음의 절차를 수행한다.

[0051] 먼저 모든 $i \in L$ 에 대해 $p_i = r^i \bmod q$ 를 계산하고, $U = \prod_{i \in L} u_i^{p_i m_i H_2(m_i \| u_i \| W_{user})}$ 를 생성한다. 위에서 생성한 증명 값 $\mathrm{Proof} = (U, T)$ 를 제3 감사자(TPA, Third Party Auditor) 서버에 전송한다.

[0052] 제3 감사자(TPA, Third Party Auditor) 서버는 공개된 파라미터와 UL을 이용하여 클라우드 서버로부터 받은 $\mathrm{Proof}$ 가 검증식을 통과하는지 확인한다.

[0053] 제3 감사자(TPA, Third Party Auditor) 서버는 먼저 $P_1 = \sum_{i \in L} p_i u_i$ 와 $P_2 = \sum_{i \in L} p_i$ 를 계산한다.

[0054] 위트니스와 공개된 파라미터, 클라우드 서버로부터 받은 증명 값을 이용하여 검증식 $e(W_{user}^T, MPK) \cdot e\left(U \cdot H_1(id_{user})^{-T}, g_1\right) = e(g_1, g_1)^{P_1} \cdot \left(e(g_1, g_1)^s\right)^{P_2}$ 이 성립하는지 확인한다.

[0055] 검증식이 성립하면 사용자가 클라우드 서버에 업로드한 파일 M의 무결성을 보장받을 수 있으며, 그렇지 않을 경우에는 데이터가 변조되었음을 확인할 수 있다.

[0056] 도 3은 일실시예에 따른 위트니스를 생성하는 실시예를 설명하는 흐름도이다.

[0057] 일실시예에 따른 공공 감사 방법은 위트니스를 생성하기 위해, 곱셈 순환 그룹의 생성자 정보가 반영된 변수를 개인키로 생성한다(301).

[0058] 다음으로, 일실시예에 따른 공공 감사 방법은 생성한 개인키에 기초하여 영-지식 증명하여 인증기관(TA, Trust Authority) 서버에 회신한다(302).

[0059] 일실시예에 따른 공공 감사 방법은 인증기관(TA, Trust Authority) 서버에서 검증식이 성립하는지 확인한다(303).

[0060] 예를 들어, $id_{user}$를 사용자의 식별자라 가정하고, 위트니스를 생성하기 위해 사용자 단말기와 인증기관(TA, Trust Authority) 서버는 다음의 절차를 수행한다.

[0061] 사용자 단말기는 자신의 개인키로 V 변수, 즉 $V = g_1^{\alpha x} = MPK^x$ 를 생성하고 이에 대한 영-지식 증명 $ZPK_{user}$ 을 계산하여 인증기관(TA, Trust Authority) 서버에 $(V, pk_v, ZKP_{user})$ 를 전송한다.

[0062] 이를 받은 인증기관(TA, Trust Authority) 서버는 검증식이 성립하는지 확인하고, 영-지식 증명인 $ZPK_{user}$도 검증한다.

[0063] 일실시예에 따른 공공 감사 방법은 검증식이 성립하는 경우에 영-지식 증명을 검증한다(304).

[0064] 일실시예에 따른 공공 감사 방법은 인증기관(TA, Trust Authority) 서버에서 상기 영-지식 증명이 검증되면, 위트니스를 생성하여 사용자 단말기로 전송하고, 데이터베이스에 저장한다(305).

[0065] 검증식이 성립하면, 인증기관(TA, Trust Authority) 서버는 위트니스 $W_{user} = (V^{1/\alpha} H_1(id_{user}))^{1/\alpha}$ 를 생성하여 $(id_{user}, W_{user})$ 를 사용자 단말기에게 전송하며, 동시에 본인의 데이터베이스에 저장한다. 성립하지 않으면 위트니스를 생성하지 않으며 프로토콜을 종료한다.

[0066] 인증기관(TA, Trust Authority) 서버로부터 $(id_{user}, W_{user})$ 를 받으면 사용자 단말기는 정당한 위트니스인지 검증하기 위해 다음의 검증식 $e(W_{user}, MPK) e(H_1(id_{user})^{-1}, g_1) = pk_{v1}$ 이 성립하는지 확인한다. 검증식이 성립한다면 $(id_{user}, W_{user})$ 는 사용자 단말기의 위트니스가 되며, 추후 무결성 검증 검사를 위해 $(id_{user}, W_{user})$ 를

제3 감사자(TPA, Third Party Auditor) 서버에 전송한다.

[0067] 만약, 인증기관(TA, Trust Authority) 서버에서 상기 영-지식 증명이 검증되지 않는 다면, 즉 검증식이 성립하지 않는 경우 공공 감사 방법은 프로토콜을 종료한다.

[0068] 도 4는 응답(Response) 값을 생성하는 실시예를 설명하는 흐름도이다.

[0069] 일실시예에 따른 공공 감사 방법은 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성한다(401).

[0070] 일실시예에 따른 공공 감사 방법은 챌린지(Challenge) 메시지를 구성하는 모든 원소에 대한 모드 연산을 수행하고(402), 수행된 모드 연산된 결과에 공개키와 해시 함수를 이용해서 증명 값을 계산한다(403).

[0071] 일실시예에 따른 공공 감사 방법은 계산된 증명 값을 반영하여 응답(Response) 값을 생성한다(404).

[0072] 예를 들어, M은 클라우드에 업로드 될 데이터 파일로, n개의 블록 $M=\{m_1, m_2, ..., m_n\}$으로 구성된다. 각각의 데이터 블록 $\{m_i\}_{1\le i\le n}$에 대한 인증 태그를 생성하기 위해 사용자는 다음과 같은 절차를 수행한다.

[0073] 일실시예에 따른 공공 감사 방법은 $1 \le i \le n$ 모든 에 대하여, 랜덤 $r_i \in Z_q$을 선택한 후, $u_i = (g_1)^{r_i}$와 $t_i = \frac{s + u_i - r_i m_i H_2(m_i \| u_i \| W_{user})}{x}$ 를 계산한다. 따라서 데이터 블록 $m_i$ 에 대한 인증 태그는 $\sigma_i = (u_i, t_i)$ 이 된다.

[0074] 사용자는 본인이 클라우드에 업로드 하고자 하는 데이터 파일 M과 그에 대응되는 인증 태그 $\{\sigma_i\}_{1\le i\le n}$를 클라우드 서버에 전송한다.

[0075] 생성한 인증 값 중 메시지 블록에 대한 $u_i = (g_1)^{r_i}$ 리스트(UL)를 생성하여 제3 감사자(TPA, Third Party Auditor) 서버에게 전송한다.

[0076] 도 5는 일실시예에 따른 공공 감사 시스템(500)을 설명하는 도면이다.

[0077] 일실시예에 따른 공공 감사 시스템(500)은 동일한 연산 효율성을 보장하면서도 악의적인 공격에도 안전한 자체 인증 서명 기반 공공 감사 프로토콜을 제공한다.

[0078] 이를 위해, 일실시예에 따른 공공 감사 시스템(500)은 개인키 발급부(510), 위트니스 생성부(520), 및 전송부(530)를 포함한다.

[0079] 일실시예에 따른 개인키 발급부(510)는 인증기관(TA, Trust Authority) 서버에서 사용자 단말기로 개인키를 발급한다.

[0080] 일실시예에 따른 위트니스 생성부(520)는 인증기관(TA, Trust Authority) 서버에서 상기 발급된 개인키에 상응하는 자체 인증 공개키 기반의 위트니스를 생성한다.

[0081] 일실시예에 따른 전송부(530)는 사용자 단말기를 통해 생성한 위트니스를 제3 감사자(TPA, Third Party Auditor) 서버로 전송한다.

[0082] 이후, 위트니스 전송에 상응하여 생성한 데이터에 대한 서명이 클라우드 서버에 전송되면, 제3 감사자(TPA, Third Party Auditor) 서버는 서명의 전송에 상응하는 챌린지(Challenge) 메시지를 생성하고, 생성된 챌린지(Challenge) 메시지에 대한 응답에 기초하여 데이터의 변조 여부를 확인한다.

[0083] 이때, 제3 감사자(TPA, Third Party Auditor) 서버는 생성된 챌린지(Challenge) 메시지를 클라우드 서버에 전송하고, 클라우드 서버에서 챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성하여 제3 감사자(TPA, Third Party Auditor) 서버로 전송하며, 제3 감사자(TPA, Third Party Auditor) 서버에서 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인한다.

[0084] 제3 감사자(TPA, Third Party Auditor) 서버는 응답(Response) 값을 미리 지정된 검증식에 대입하여 데이터의 변조 여부를 확인한다. 이때, 제3 감사자(TPA, Third Party Auditor) 서버는 챌린지(Challenge) 메시지를 구성하는 모든 원소에 대한 모드(mod) 연산을 수행하고, 수행된 모드 연산된 결과에 공개키와 해시 함수를 이용해

서 증명 값을 계산하며, 계산된 증명 값을 반영하여 상기 응답(Response) 값을 생성한다.

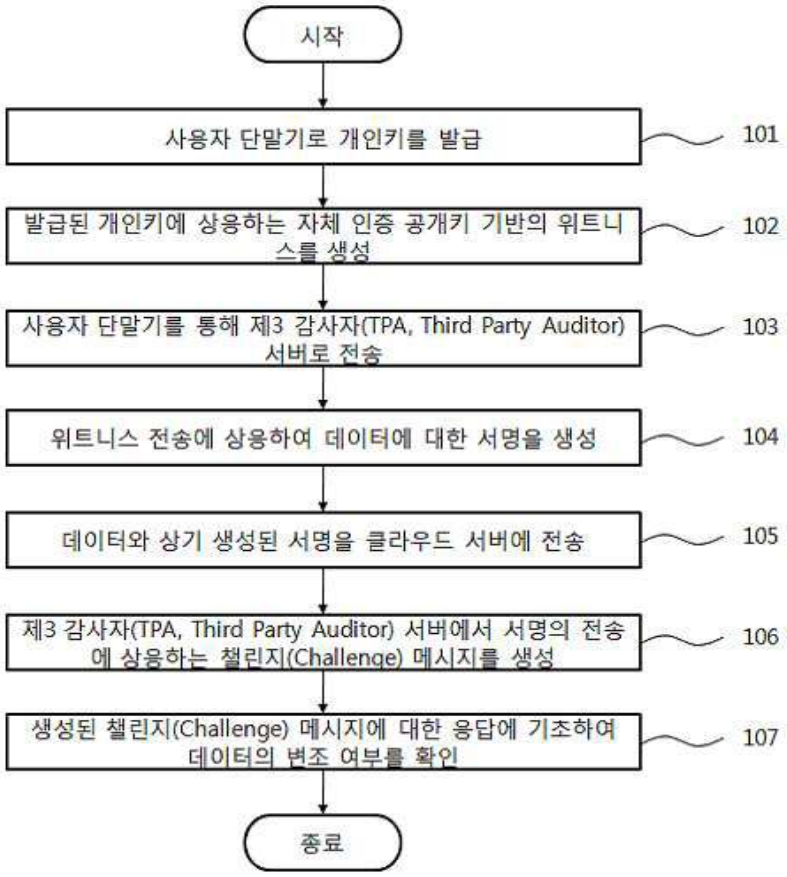
[0085] 본 발명의 일실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0086] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

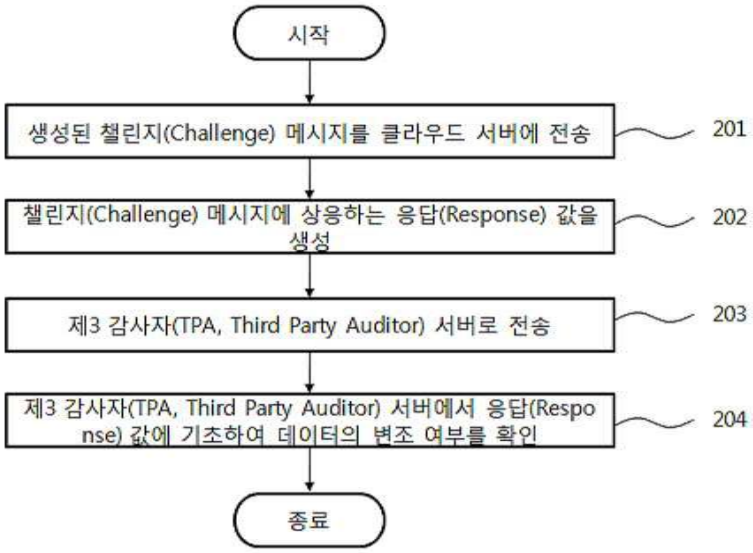
[0087] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

## 도면

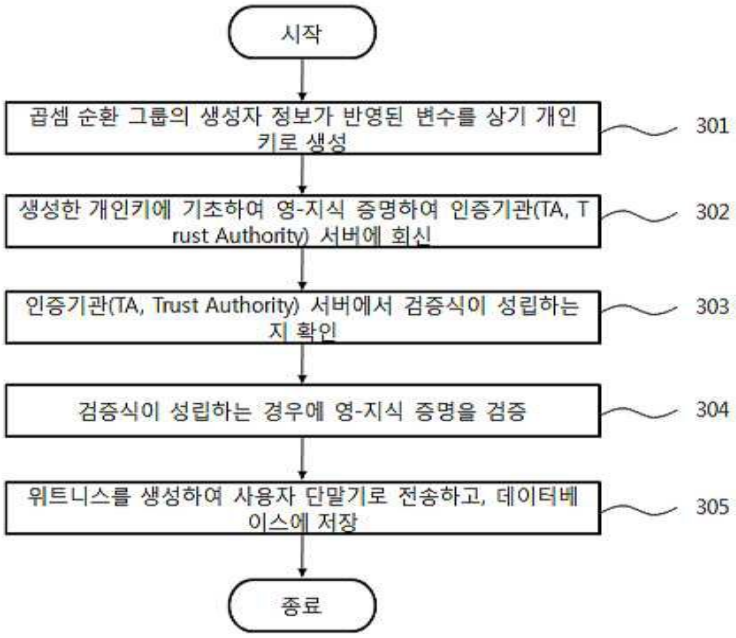
### 도면1



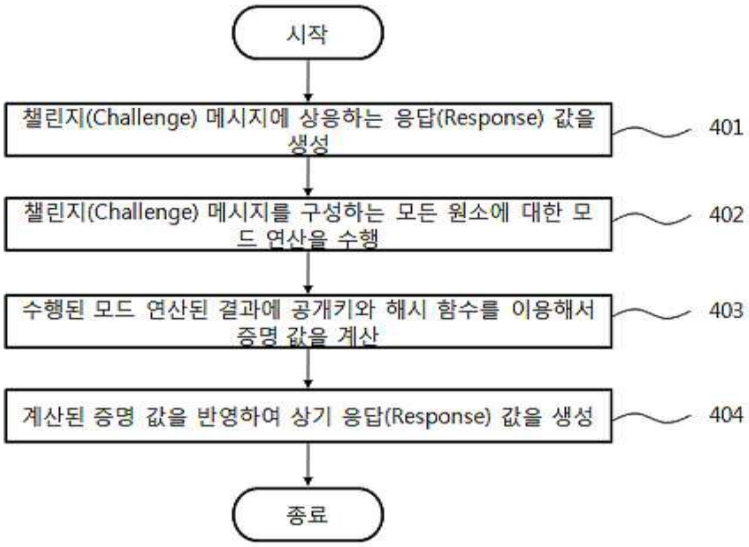
도면2


시작
생성된 챌린지(Challenge) 메시지를 클라우드 서버에 전송
201
챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성
202
제3 감사자(TPA, Third Party Auditor) 서버로 전송
203
제3 감사자(TPA, Third Party Auditor) 서버에서 응답(Response) 값에 기초하여 데이터의 변조 여부를 확인
204
종료

도면3


시작
곱셈 순환 그룹의 생성자 정보가 반영된 변수를 상기 개인키로 생성
301
생성한 개인키에 기초하여 영-지식 증명하여 인증기관(TA, Trust Authority) 서버에 회신
302
인증기관(TA, Trust Authority) 서버에서 검증식이 성립하는지 확인
303
검증식이 성립하는 경우에 영-지식 증명을 검증
304
위트니스를 생성하여 사용자 단말기로 전송하고, 데이터베이스에 저장
305
종료

도면4


시작
챌린지(Challenge) 메시지에 상응하는 응답(Response) 값을 생성
401
챌린지(Challenge) 메시지를 구성하는 모든 원소에 대한 모드 연산을 수행
402
수행된 모드 연산된 결과에 공개키와 해시 함수를 이용해서 증명 값을 계산
403
계산된 증명 값을 반영하여 상기 응답(Response) 값을 생성
404
종료

도면5


500
개인키 발급부
(510)
위트니스 생성부
(520)
전송부
(530)