(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0105371
(43) 공개일자 2024년07월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3247 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2024-7012783
(22) 출원일자(국제) 2022년10월26일
심사청구일자 없음
(85) 번역문제출일자 2024년04월17일
(86) 국제출원번호 PCT/SG2022/050769
(87) 국제공개번호 WO 2023/080842
국제공개일자 2023년05월11일
(30) 우선권주장
10202112269T 2021년11월05일 싱가포르(SG)

(71) 출원인
피큐씨이이 피티이 엘티디
싱가포르 038987 싱가포르 선택 타워 원 #12-07 테마섹 불르바드 7
(72) 발명자
탄, 테익 구안
싱가포르 038987 싱가포르 선택 타워 원 #12-07 테마섹 불르바드 7
조우, 지안잉
싱가포르 487372 싱가포르 소마파 로드 8
(74) 대리인
박영우

전체 청구항 수 : 총 24 항

(54) 발명의 명칭 **디지털 서명을 보호하기 위한 방법 및 시스템**

(57) 요 약

양자 내성 디지털 서명 방법, 개인 키 검증을 통한 데이터 출처 인증을 위한 양자 내성 디지털 서명 검증 방법 및 양자 내성 디지털 서명 시스템이 제공된다. 양자 내성 디지털 서명 시스템은 디지털 서명 시스템 및 양자 내성 보호 계층을 포함한다. 상기 디지털 서명 시스템은 공개 키 및 개인 키를 포함하며, 상기 공개 키는 상기 개인 키와 연관된다. 상기 디지털 서명 시스템은 또한 데이터 및 상기 개인 키에 응답하여 생성된 디지털 서명을 포함한다. 양자 내성 보호 계층은 디지털 서명 시스템에 적용되며, 서명-당사자-제공 개인 키의 사전 이미지에 대한 양자 보안 지식 증명을 포함한다.

대 표 도 - 도2

양자 내성 ESDSA 서명 알고리즘: Sign_q

1 **begin**
2 $G \leftarrow$ ECC base point; $P \leftarrow$ ECC order;
3 $\rho \leftarrow$ secret pre-image;
4 $M \leftarrow$ message;
5 Generate signature random r;
6 Compute r^{-1} where $r * r^{-1} \equiv 1 \ mod \ P$;
7 Compute $R = (R_x, R_y)$ where $R \equiv r \cdot G \ mod \ P$;
8 Compute hash of message $H(M)$;
9 Enumerate ZKBoo proof π = **begin**
10 Zero-knowledge computation of private key K_s where $K_s = H(\rho)$; 210
11 Zero-knowledge computation of public key K_p where $K_p \equiv K_s \cdot G \ mod \ P$;
12 Compute s where $s \equiv r^{-1} * (H(M) + R_x * K_s) \ mod \ P$; 220
13 Commit R_x, s in the proof;
14 **end**
15 destroy r, r^{-1}, K_s;
16 return $\sigma = \{R_x, s\}, \pi$;
17 **end**

200

(52) CPC특허분류
H04L 9/3218 (2013.01)

명 세 서

청구범위

청구항 1

공개 키 및 개인 키를 포함하고, 상기 공개 키는 상기 개인 키와 연관되고, 데이터 및 상기 개인 키에 응답하여 생성된 디지털 서명을 포함하는 디지털 서명 시스템; 및

상기 디지털 서명 시스템에 적용되며, 상기 개인 키의 사전 이미지에 대한 서명-당사자-제공 양자 보안 지식 증명을 포함하는 양자 내성(quantum-resistant) 보호 계층을 포함하는 양자 내성 디지털 서명 시스템.

청구항 2

제1항에 있어서,

상기 개인 키의 계산은 붕괴 해시 함수(collapsing hash function)를 포함하는 것을 특징으로 하는 양자 내성 디지털 서명 시스템.

청구항 3

제1항 및 제2항에 있어서,

미리 정해진 세기를 갖는 암호 키가 상기 공개 키 및 상기 개인 키를 생성하는 것을 특징으로 하는 양자 내성 디지털 서명 시스템.

청구항 4

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 개인 키의 상기 사전 이미지에 대한 서명-당사자-제공 양자 보안 지식 증명은 제로-지식 증명을 포함하는 것을 특징으로 하는 양자 내성 디지털 서명 시스템.

청구항 5

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 개인 키의 상기 사전 이미지에 대한 서명-당사자-제공 양자 보안 지식 증명은 부분-지식 증명을 포함하는 것을 특징으로 하는 양자 내성 디지털 서명 시스템.

청구항 6

제1항 내지 제5항 중 어느 한 항에 있어서,

상기 개인 키의 상기 사전 이미지에 대한 서명-당사자-제공 양자 보안 지식 증명은 상기 개인 키의 적어도 일부에 응답하여 생성되는 것을 특징으로 하는 양자 내성 디지털 서명 시스템.

청구항 7

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 양자 내성 보호 계층은 미리 정의된 인증서 계층을 갖는 상기 개인 키의 상기 사전 이미지에 대한 복수의 지식 증명들을 제공함으로써 둘 이상의 당사자들을 지원하는 것을 특징으로 하는 양자 내성 디지털 서명 시스템.

청구항 8

양자 내성 디지털적으로 데이터를 서명하는 방법으로서,

보안 파라미터에 응답하여 공개 키 및 사전 이미지 파라미터를 생성하는 단계;

상기 사전 이미지 파라미터에 응답하여 생성되고 상기 공개 키와 연관되는 개인 키를 생성하는 단계;

상기 데이터 및 상기 개인 키에 응답하여 서명을 생성하는 단계;

상기 사전 이미지 파라미터에 대한 지식 증명을 생성하는 단계; 및

상기 서명과 상기 사전 이미지 파라미터에 대한 지식 증명을 사용하여 상기 데이터를 디지털적으로 서명하는 단계를 포함하는 방법.

청구항 9

제8항에 있어서,

상기 데이터를 디지털적으로 서명하는 단계는 병렬 검증을 위한 상기 제로-지식 증명과 별도로 상기 서명을 저장하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 10

제8항 또는 제9항에 있어서,

상기 개인 키를 생성하는 단계는 붕괴 해시 함수(collapsing hash function)를 이용하여 상기 개인 키를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 11

제8항 내지 제10항 중 어느 한 항에 있어서,

상기 보안 파라미터는 미리 정해진 세기의 암호키를 포함하는 것을 특징으로 하는 방법.

청구항 12

제8항 내지 제11항 중 어느 한 항에 있어서,

상기 사전 이미지 파라미터에 지식 증명은 제로-지식 증명을 포함하는 것을 특징으로 하는 방법.

청구항 13

제8항 내지 제11항 중 어느 한 항에 있어서,

상기 사전 이미지 파라미터에 지식 증명은 부분-지식 증명을 포함하는 것을 특징으로 하는 방법.

청구항 14

제8항 내지 제13항 중 어느 한 항에 있어서,

상기 사전 이미지 파라미터에 대한 지식 증명은 상기 개인 키의 적어도 일부에 응답하여 생성되는 것을 특징으로 하는 방법.

청구항 15

제8항 내지 제14항 중 어느 한 항에 있어서,

상기 개인 키를 생성하는 단계는,

상기 사전 이미지 파라미터에 대한 해시 키 유도를 수행하여 상기 개인 키를 생성하는 단계;

상기 사전 이미지 파라미터에 대한 일방향 함수 키 유도를 수행하는 단계; 또는

상기 사전 이미지 파라미터에 대한 대칭 키 유도를 수행하는 단계 중 하나 이상을 포함하는 것을 특징으로 하는 방법.

청구항 16

제8항 내지 제15항 중 어느 한 항에 있어서,

상기 공개 키 및 상기 사전 이미지 파라미터를 생성하는 단계는,

상기 사전 이미지 파라미터에 대한 해시 키 유도를 수행하여 상기 공개 키를 생성하는 단계;

상기 사전 이미지 파라미터에 대한 일방향 함수 키 유도를 수행하여 상기 공개 키를 생성하는 단계; 또는

상기 사전 이미지 파라미터에 대한 대칭 키 유도를 수행하여 상기 공개 키를 생성하는 단계 중 하나 이상을 포함하는 것을 특징으로 하는 방법.

청구항 17

제8항 내지 제16항 중 어느 한 항에 있어서,

상기 데이터는 메시지를 포함하고,

상기 방법은 상기 디지털적으로 서명된 메시지를 전송하는 단계를 더 포함하고,

상기 사전 이미지 파라미터에 대한 지식 증명은 상기 메시지의 수신자에 의해 액세스가능한 것을 특징으로 하는 방법.

청구항 18

제17항에 있어서,

상기 디지털적으로 서명된 메시지를 전송하는 단계는, (i)상기 사전 이미지 파라미터의 지식 증명 또는 (ii)상기 사전 이미지 파라미터의 지식 증명이 액세스될 수 있는 디지털 저장 위치를 식별하기 위한 위치 정보 중 하나 또는 모두와 함께 상기 디지털적으로 서명된 메시지를 전송하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 19

제17항 또는 제18항에 있어서,

상기 공개 키를 전송하는 단계를 더 포함하고,

상기 공개 키를 전송하는 단계는 상기 공개 키와 함께 상기 디지털적으로 서명된 메시지를 전송하거나 상기 공개 키를 디지털 저장 위치로 전송하는 단계를 포함하고,

상기 디지털 저장 위치는 인증 기관 또는 공공 저장소를 포함하는 것을 특징으로 하는 방법.

청구항 20

개인 키를 검증하여 데이터의 출처 인증을 위한 양자 내성 디지털 서명을 검증하는 방법으로서,

상기 개인 키와 연관된 공개 키 및 상기 데이터에 상응하는 디지털 서명을 검증하기 위한 사전 이미지 파라미터의 지식 증명을 모두 사용하여 검증함으로써 데이터의 출처를 인증하는 단계를 포함하고,

상기 디지털 서명은 상기 개인 키에 응답하여 생성되는 방법.

청구항 21

제20항에 있어서,

상기 사전 이미지 파라미터에 지식 증명은 제로-지식 증명을 포함하는 것을 특징으로 하는 방법.

청구항 22

제20항 및 제21항에 있어서,

상기 인증하는 단계는 상기 공개 키를 이용한 검증과 상기 사전 이미지 파라미터의 지식 증명을 이용한 검증을 병렬 처리하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 23

제22항에 있어서,

상기 공개 키를 이용한 검증과 상기 사전 이미지 파라미터의 지식 증명을 이용한 검증을 병렬 처리하는 단계는

제1 디지털 저장 위치에서 상기 공개 키를 검색하는 단계; 및

제2 디지털 저장 위치에서 상기 사전 이미지 파라미터의 지식 증명을 검색하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 24

제20항 내지 제23항 중 어느 한 항에 있어서,

상기 데이터의 출처를 인증하는 단계는 상기 디지털 서명이 상기 개인 키에 응답하여 생성된 것으로 결정되고 상기 사전 이미지 파라미터의 지식 증명이 상기 사전 이미지 파라미터로부터 계산된 유효한 증명으로 결정되는 경우에만 상기 데이터의 검증을 수락하는 단계를 포함하는 것을 특징으로 하는 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 디지털 서명에 관한 것으로, 보다 상세하게는 양자 능력을 가진 공격자들로부터 디지털 서명들을 보호하기 위한 방법들 및 시스템들에 관한 것이다.

배 경 기 술

[0002] 비대칭 키 암호화는 디지털 영역에서 당사자 간의 신뢰를 유지하기 위해 전 세계 시스템에서 사용하는 도구이다. 디지털 서명을 사용하면 통신 당사자가 서로 인증하고, 교환된 데이터의 무결성을 확인하고, 거부 상황에서 데이터의 출처를 증명할 수 있다. 세 가지 고전적인 디지털 서명 알고리즘은 미국 국립표준기술원(National Institute of Standards and Technology, 이하 'NIST')의 디지털 서명 표준에 따라 설명되며, 이산 로그 암호화를 기반으로 하는 디지털 서명 알고리즘(Digital Signature Algorithms, 이하 'DSA'), RSA(Rivest-Shamir Adelman) 알고리즘 및 타원-곡선 암호화(Elliptic Curve Cryptography, 이하 'ECC')를 기반으로 하는 타원-곡선 디지털 서명 알고리즘(Elliptic-Curve Digital Signature Algorithm, 이하 'ESDSA')이 있다. DSA와 ECDSA의 보안은 매우 큰 수의 유한 필드에 대한 이산 로그를 푸는 것을 기반으로 하며, RSA의 보안은 매우 큰 수의 유한 필드에 대한 정수 인수분해의 어려움을 기반으로 한다.

[0003] 하지만 이러한 고전적인 디지털 서명 알고리즘을 사용하는 시스템에는 커다란 위험이 존재한다. 쇼어(Shor)의 알고리즘은 DSA와 ECDSA의 기반이 되는 이산 로그 문제와 RSA가 O(logN) 다항식-시간을 기반으로 하는 정수 인수분해 문제를 모두 해결할 수 있는 능력을 갖추고 있다. 이는 충분히 큰 양자 컴퓨터를 소유한 모든 공격자가 사용자의 공개 키를 제공하면 몇 시간 만에 사용자의 개인 서명 키를 계산할 수 있으며 이를 통해 사용자를 가장하기 위한 유효한 디지털 서명을 생성할 수 있음을 의미한다. 또한 이전에 사용자가 서명한 데이터는 더 이상 진위 여부와 신뢰성을 입증할 수 없다.

[0004] 업계는 새로운 디지털 서명 표준이 발전함에 따라 새로운 시스템 구현을 고려하도록 장려할 가능성이 높지만, 기존 또는 향후 시스템에 대한 과제는 디지털 서명과 관련된 다음과 같은 질문을 제기한다. 양자 컴퓨터 디지털 서명 무효화 기능에 직면하여 이미 디지털 서명된 문서가 어떻게 신뢰할 수 있는가? 이러한 문서에 새로운 알고리즘을 사용하여 부서(연대 서명)해야 하는가? 부서자(부서하는 사람)가 거래의 이해관계가 없는 제3자일 수 있으므로, 부서자는 검증 당사자에게 어떤 책임을 부담하는가? 마이그레이션할 수 없는 레거시(legacy) 시스템은 어떤가? 검증 당사자는 언제 새로운 알고리즘을 검증할 준비가 될 것으로 예상되는가? 기존의 양자 보안이 아닌 서명은 검증을 통과하지만 검증 당사자는 새로운 양자 보안 서명을 검증할 수 없는 경우, 검증 당사자에게 법적 의미는 무엇인가? 디지털 서명을 사용하는 시스템 운영자는 업계 표준화를 기다리는 대신 상태가 명확한 해시 기반 서명으로 암호화 마이그레이션을 시작해야 하는가?

[0005] 따라서, 현재의 디지털 서명 시스템들의 단점들을 극복하고 양자 능력을 가진 공격자들로부터 디지털 서명들을 보호하는 디지털 서명을 위한 시스템들 및 방법들이 필요하다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 특허 문헌 1: 미국 공개특허 공보 US 2021/0297255호

발명의 내용

해결하려는 과제

[0007] 본 발명의 목적은 양자 능력을 가진 공격자들로부터 디지털 서명들을 보호하는 디지털 서명을 위한 시스템들 및 방법들을 제공하는 것이다. 다른 바람직한 특성들 및 특징들은 첨부된 도면 및 본 개시의 배경과 관련된 이하의 상세한 설명 및 첨부된 청구범위로부터 명백해질 것이다.

과제의 해결 수단

[0008] 상기 목적을 달성하기 위한 본 발명의 실시예들의 적어도 일 측면에 따르면 양자 내성 디지털 서명 시스템이 제공된다. 상기 양자 내성 디지털 서명 시스템은 디지털 서명 시스템 및 양자 내성(quantum-resistant) 보호 계층을 포함한다. 상기 디지털 서명 시스템은 공개 키 및 개인 키를 포함하고, 상기 공개 키는 상기 개인 키와 연관되고, 데이터 및 상기 개인 키에 응답하여 생성된 디지털 서명을 포함한다. 상기 양자 내성 보호 계층은 상기 디지털 서명 시스템에 적용되며, 상기 개인 키의 사전 이미지에 대한 서명-당사자-제공 양자 보안 지식 증명을 포함한다.

[0009] 상기 목적을 달성하기 위한 본 발명의 실시예들의 적어도 일 측면에 따르면 양자 내성 디지털적으로 데이터를 서명하는 방법(디지털 데이터 서명 방법)이 제공된다. 상기 양자 내성 디지털적으로 데이터를 서명하는 방법에서는 보안 파라미터에 응답하여 공개 키 및 사전 이미지 파라미터를 생성하고, 상기 사전 이미지 파라미터에 응답하여 생성되고 상기 공개 키와 연관되는 개인 키를 생성하고, 상기 데이터 및 상기 개인 키에 응답하여 서명을 생성하고, 상기 사전 이미지 파라미터에 대한 지식 증명을 생성하고, 상기 서명과 상기 사전 이미지 파라미터에 대한 지식 증명을 사용하여 상기 데이터를 디지털적으로 서명한다.

[0010] 상기 목적을 달성하기 위한 본 발명의 실시예들의 적어도 일 측면에 따르면 개인 키를 검증하여 데이터의 출처 인증을 위한 양자 내성 디지털 서명을 검증하는 방법이 제공된다. 상기 개인 키를 검증하여 데이터의 출처 인증을 위한 양자 내성 디지털 서명을 검증하는 방법에서는 상기 개인 키와 연관된 공개 키 및 상기 데이터에 상응하는 디지털 서명을 검증하기 위한 사전 이미지 파라미터의 지식 증명을 모두 사용하여 검증함으로써 데이터의 출처를 인증한다. 상기 디지털 서명은 상기 개인 키에 응답하여 생성된다.

발명의 효과

[0011] 본 발명의 실시예들에 따르면 하위 호환성을 유지하면서, 양자 능력을 갖춘 공격자들로부터 디지털 서명을 안전하게 방어할 수 있다.

도면의 간단한 설명

[0012] 동일한 참조번호가 도면들 전체에 걸쳐 동일하거나 기능적으로 유사한 구성요소들을 지칭하고 하기의 상세한 설명과 함께 명세서의 일부를 형성하는 첨부된 도면들은 다양한 실시예들을 예시하고 본 발명의 실시예들에 따른 다양한 원리들 및 이점들을 설명하는 역할을 한다.

도 1은 본 발명의 실시예들에 따른 예시적인 양자 내성 ECDSA 키 생성 알고리즘($KeyGen_q$)을 나타낸다.

도 2는 본 발명의 실시예들에 따른 예시적인 양자 내성 ESDSA 서명 알고리즘($Sign_q$)을 나타낸다.

도 3은 본 발명의 실시예들에 따른 예시적인 양자 내성 ESDSA 검증 알고리즘($Verify_q$)을 나타낸다.

도 4는 테스트 중인 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식의 실생활 구현의 사용 사례를 나타내는 처리도이다.

도 5는 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식의 실생활 구현에서 미리 정의된 인증서 계층 구조를 예시한 윈도우들의 이미지들을 나타낸다.

도 6은 본 실시예들에 따른 양자 내성 디지털 서명 방식의 실생활 구현에서 타임-스탬프 클라이언트에 의한 검

증을 예시한 윈도우의 이미지를 나타낸다.

도면의 요소들이 단순함과 명확함을 위해 예시된 것이며 반드시 축척되도록 묘사된 것은 아니라는 것이 당업자들에게 자명하다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하의 상세한 설명은 본질적으로 예시적인 것일 뿐, 본 발명 또는 본 발명의 적용 및 사용을 제한하기 위한 것은 아니다. 또한, 본 명세서의 선행 배경 또는 이하의 상세한 설명에 제시된 어떠한 이론에 구속될 의도도 없다. 본 발명의 실시예들의 목적은 RSA/DSA/ECDSA 및 양자 컴퓨터를 사용하는 공격자들에 취약할 수 있는 다른 디지털 서명 알고리즘들을 사용하는 시스템들을 위한 양자 내성 보호 계층을 추가하는 새로운 수단을 제시하는 것이다. 본 발명의 실시예들에 따르면, 양자 보안 제로-지식 증명의 사용은 서명 당사자가 실제로 개인 키가 서명 당사자에 의해 생성되었고 양자 컴퓨터를 사용하여 암호화되지 않았다는 증명을 포함하도록 요구하기 위해 적용된다. 이는 서명 과정에서 서명 당사자가 검증 당사자에게 전송될 메시지를 디지털적으로 서명할 때, 개인 키로부터 생성된 디지털 서명과 함께 개인 키의 사전 이미지에 대한 양자 보안 제로-지식 증명을 포함함으로써, 본 발명의 실시예들의 따른 방법 및 시스템에 따라 달성된다. 이러한 방식으로, 본 발명의 실시예들은 RSA/DSA/ECDSA 및 다른 디지털 서명 알고리즘을 사용하는 시스템들이 디지털 서명 사용을 인정하는 기존 검증 당사자 구현 및 법 체계와의 하위 호환성을 유지하면서 양자 컴퓨터에 대한 보호를 유리하게 달성할 수 있게 한다.

[0014] 본 발명의 실시예에 따른 방법 및 시스템은 충분히 큰 양자 컴퓨터가 구축된 후에도 기존 디지털 서명이 양자 내성을 유지할 수 있다면 전환과 관련된 많은 하위 호환성 문제가 발생할 수 있다는 전제에서 형성된다. 새로운 알고리즘으로의 마이그레이션 일정은 상대방에 덜 의존하게 되며 기존 디지털 서명 문서는 포스트-양자 시대에도 신뢰성을 유지하는 이점이 있다. 본 발명의 실시예들은 (a)개인 서명 키의 사전 이미지에 대한 양자 보안 제로-지식 증명을 서명과 함께 계층화함으로써 기존 시스템이 호환성 문제에 직면하는 것을 유리하게 방지하고, (b)디지털 서명(디지털적으로 서명된 데이터)을 양자 내성으로 만들기 위해 디지털 서명에 포함되는 제로-지식 증명을 사용하여 양자 내성 디지털 서명 체계를 구현하고, (c)기존의 어도비(Adobe) PDF Acrobat Reader DC V2021.x와 호환되는 RFC3161 타임-스탬프 서버를 제공하는 Adobe®PDF 디지털 서명 솔루션을 포함한 실제 구현을 배포함으로써, X.509v3 인증서들을 가지는 양자 내성 ECDSA 타임-스탬프 디지털 서명을 기존의 어도비 PDF Acrobat Reader DC v2021.x와 호환되도록 한다.

[0015] 디지털 서명은 디지털 통신에서 무결성, 진위 여부 및 부인 방지 기능을 제공한다. 예를 들어, 앨리스(Alice)와 밥(Bob)은 통신 당사자이다 Alice는 Bob에게 보낼 메시지(M)를 갖고 있으며 Bob이 메시지를 변경되지 않은 상태로(무결성) 수신하고, 메시지가 Alice에게서 온 것임을 알 수 있도록(진정성) 확인하려고 한다. Bob은 메시지가 실제로 Alice로부터 온 것임을 제3자에게 증명할 수 있기를 원한다(부인 방지).

[0016] 디지털 서명 방식은 다항식-시간 알고리즘인 키 생성(KeyGen), 서명(Sign) 및 검증(Verification)의 3개로 정의된다. 키 생성 알고리즘(KeyGen)은 미리 결정된 강도(n)의 암호화 키 강도를 정의하는 보안 매개 변수(보안 파라미터)(1^n)를 입력으로 하고 개인 키(K_s) 및 해당 공개 키(K_p)를 출력한다. 서명 알고리즘(Sign)은 메시지(M)과 개인 키(K_s)를 입력으로 수신하고, 서명(σ)을 출력한다. 그리고 검증 알고리즘(Verify)은 메시지(M), 공개 키(K_p) 및 서명(σ)을 입력으로 하여 서명(σ)이 Sign(M, K_s)에 의해 생성된 유효한 서명인 경우에만 '수락(accept)'을 출력한다. 이러한 관계는 하기의 [수학식 1], [수학식 2] 및 [수학식 3]에 나타난다.

[0017] [수학식 1]

[0018] $KeyGen(1^n) \Rightarrow \{K_s, K_p\}$

[0019] [수학식 2]

[0020] $Sign(M, K_s) \Rightarrow \{\sigma\}$

[0021] [수학식 3]

[0022] $Verify(M, K_p, \sigma) \Rightarrow \{result\}$

[0023] Alice와 Bob의 예에서 서명 당사자인 Alice는 키 생성 알고리즘(KeyGen)을 호출하여 개인 키(K_s)와 공개 키(K_p)를 생성한다. 공개 키(K_p)는 Bob과 다른 당사자에게 공개 키(K_p)에 대한 액세스를 제공하도록 공개된다. 그러면 Alice는 자신의 개인 키(K_s)로 서명 알고리즘(Sign)을 호출하여 메시지(M)에 서명함으로써 서명(σ)을 생성한다. Alice는 Bob에게 메시지(M)와 서명(σ)을 전송한다. 검증 당사자인 Bob은 메시지(M)에 대한 서명(σ)을 검증하기 위해 Alice의 공개 키(Kp)로 검증 알고리즘(Verify)을 호출한다. 검증 알고리즘(Verify)이 '수락'을 반환하면 Bob은 변경되지 않은 메시지(M)와 서명 증명(σ)을 Alice로부터 성공적으로 수신하게 된다.

[0024] 제로-지식 증명은 명제의 정확성 외에 추가적인 지식을 전달하지 않는 증명으로 정의된다. 제로-지식 증명에 대한 구체적인 실현이 많이 있었지만, 양자 내성 비-상호작용(non-interactive) 제로-지식 증명은 ZKStark 기반 증명이거나 다자간 계산(Multi-party computation, 이하 'MPC')-in-the-head 기반 증명이다. 부분-지식 증명은 명제의 정확성 이외에도 관련된 추가 지식을 일부 전달하는 증명이다.

[0025] MPC-in-head-proof의 경우, 증명자는 n개의 분기로 이루어진 부울 계산 회로를 커밋(commitment)으로 생성해야 하며, 이 중 n-1개의 뷰는 증명자에게 지식의 증명으로 드러날 수 있다. 증명을 비-상호작용적으로 하기 위해, 증명자는 피아트-샤미르(Fiat-Shamir)의 휴리스틱을 사용하여 증명자에게 보낼 n-1개의 뷰를 결정적이지만 예측 불가능하게 결정할 수 있다. 그런 다음 검증자는 명제가 1/n의 틀릴 확률로 n-1개의 뷰를 훑어본다. 증명자가 회로를 계산하고 뷰를 제공해야 하는 (무작위 입력 매개변수(파라미터)가 다른) 라운드 수를 늘림으로써, 증명자가 거짓 주장을 할 확률이 기하급수적으로 줄어든다.

[0026] 양자 컴퓨터에 관한 쇼어의 알고리즘은 정수 인수분해 문제, 이산 로그 문제, 타원곡선 이산 로그 문제를 푸는 것이므로, 충분히 큰 양자 컴퓨터를 구축할 때 공개 키(K_p)가 주어진 모든 RSA/DSA/ECDSA 개인키(K_s)를 상대적으로 효율적으로 계산할 수 있다고 안전하게 가정할 수 있다. 그러나 대칭 키와 해시 기반의 암호학은 상대적으로 양자에 강한 상태를 유지한다. 예를 들어 양자 컴퓨터에 관한 그로버(Grover)의 알고리즘은 무차별 대입 검색을 수행할 때만 $O(\sqrt{N})$ 의 2차 속도 향상을 얻을 수 있으며, 이는 최적임이 입증되었다.

[0027] 따라서, 본 발명의 실시예에 따르면, 서명 프로세스는 서명을 보호하기 위해 개인 키의 사전 이미지에 대한 제로-지식 증명의 계층으로 확장된다. 그런 다음 확장된 검증 프로세스는 이 증거를 검증하여 서명이 양자 능력을 가진 공격자가 아닌 개인 키 소유자가 실제로 생성했는지 확인할 수 있다. 이전 버전과의 호환성을 위해 기존 검증 프로세스는 양자 내성 보증을 상실하더라도 증명 없이 디지털 서명을 검증할 수 있다.

[0028] 본 발명의 실시예들에 따른 유리한 솔루션을 구현하기 위해, 고전적인 디지털 서명 방식의 세가지 다항식-시간 알고리즘(즉, [수학식 1], [수학식 2] 및 [수학식 3])을 확장한다. 본 발명의 실시예들에 따른 확장된 양자 내성 디지털 서명 방식은 다항식-시간 알고리즘인 $KeyGen_q$, $Sign_q$ 및 $Verify_q$의 세가지로 정의된다. 키 생성 알고리즘($KeyGen_q$)은 n의 암호 키 강도를 정의하는 보안 파라미터(1^n)에 응답하여 비밀 사전 이미지 파라미터, 사전 이미지(ρ) 및 공개 키(K_p)를 출력한다. 즉, 보안 파라미터(1^n)에 응답하여, 비밀 사전 이미지 파라미터, 사전 이미지(또는 비밀 사전 이미지)(ρ) 및 공개 키(K_p)를 생성할 수 있다. 암호 키는 미리 정해진 세기를 가질 수 있다. 공개 키(K_p)는 개인 키(H(ρ))에 대한 연관된 공개 키이며, 여기서 개인 키의 계산인 H()는 붕괴 해시 함수(collapsing hash function)이다. 서명 알고리즘($Sign_q$)은 메시지(M)와 비밀 사전 이미지(ρ)에 응답하여, Sign(M, H(ρ))를 사용하여 계산된 서명(σ)과 개인 키(H(ρ))로부터 비밀 사전 이미지(ρ)를 계산하는 양자 내성 제로-지식 증명(π)을 출력하며, 개인 키(H(ρ))의 적어도 일부에 응답하여 양자 내성 제로-지식 증명(π)을 생성한다. 즉, 개인 키(H(ρ))는 사전 이미지 파라미터에 응답하여 생성되고 공개 키(K_p)와 연관될 수 있다. 개인 키(H(ρ))는 사전 이미지(ρ)에 대해 해시 키 유도를 수행하거나, 사전 이미지(ρ)에 대해 단방향 함수 키 유도를 수행하거나, 또는 사전 이미지(ρ)에 대해 대칭 키 유도를 수행하여 생성될 수 있다. 공개 키(K_p)가 개인 키(H(ρ))와 연관됨에 따라, 공개 키(K_p)는 사전 이미지(ρ)에 대해 해시 키 유도를 수행하거나, 사전 이미지(ρ)에 대해 단방향 함수 키 유도를 수행하거나, 또는 사전 이미지(ρ)에 대해 대칭 키 유도를 수행하여 생성될 수도 있다.

[0029] 검증을 위해 검증 알고리즘($Verify_q$)은 메시지(M), 공개 키(K_p) 및 서명(σ)에 응답하여 '수락(accept)'을 출력하여 Verify(M,K_p)가 '수락'을 반환하고 양자 내성 제로-지식 증명(π)이 사전 이미지(ρ)(또는 사전

이미지(ρ) 파라미터)에서 계산된 유효한 제로-지식 증명인 경우에만 메시지(M)의 출처를 인증한다. 즉, 이러한 관계는 하기의 [수학식 4], [수학식 5] 및 [수학식 6]에 나타난다.

[0030] [수학식 4]

[0031] $KeyGen_q(1^n) \Rightarrow \{\rho, K_p\}$

[0032] [수학식 5]

[0033] $Sign_q(M, \rho) \Rightarrow \{\sigma, \pi\}$

[0034] [수학식 6]

[0035] $Verify_q(M, K_p, \sigma, \pi) \Rightarrow \{result\}$

[0036] 직관적으로, 본 발명의 실시예들에 따른 디지털 서명 방식은 개인 키에 추가적인 양자 내성 계층을 갖는 고전적인 디지털 서명 방식의 고전적인 보안 속성을 계승한다. 서명 알고리즘($Sign_q$)에서 얻은 추가 정보는 비밀 사전 이미지(ρ) 또는 개인 키($K_s=H(\rho)$)를 드러내지 않는 제로-지식 증명이기 때문에 고전적인 공격자는 서명 당사자와 상호 작용할 때 검증 알고리즘($Verify_q$)의 건전성을 손상시킬 수 없다.

[0037] 따라서, 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식은 서명(σ) 및 양자 내성 제로-지식 증명(π)을 검증하는 데 검증 알고리즘($Verify_q$)을 사용하는 경우, 서명(σ) 및 양자 내성 제로-지식 증명(π)을 사용하여 생성된 디지털 서명에 대한 추가적인 양자 내성을 유리하게 제공함을 알 수 있다. 여기서 양자 내성 제로-지식 증명(π)은 개인 키의 사전 이미지(ρ)에 대한 서명-당사자-제공 양자 보안 지식의 증명이므로, 검증자가 액세스할 수 있는 양자 내성 제로-지식 증명(π)은 디지털 서명(σ)이 개인 키의 사전 이미지(ρ)로부터 계산되었음을 양자 보안으로 증명하는 데 사용된다.

[0038] 본 발명의 실시예들에 따른 디지털 서명 방식에 대한 추가적인 양자 내성은 양자 능력을 가진 공격자가 쇼어의 알고리즘을 사용하여 공개 키(K_p)로부터 개인 키($H(\rho)$)를 복구할 수 있다고 가정함으로써 나타낼 수 있다. 개인 키($H(\rho)$)를 사용하여 공격자는 검증 알고리즘(Verify)에서 수락할 서명 알고리즘(Sign)을 사용하여 유효한 서명(σ)을 임의로 생성할 수 있다. 그러나 단방향 해시 함수($H()$)가 붕괴 해시 함수(collapsing hash function)이고 양자 컴퓨터에서도 사전 이미지 공격에 내성이 있기 때문에 서명(ρ)의 값을 개인 키($H(\rho)$)의 계산에서 복구할 수 없기 때문에 공격자는 증명(π)을 생성할 수 없다. 따라서 검증 알고리즘($Verify_q$)은 양자 능력이 있는 공격자에 내성(저항성)을 가진다.

[0039] 또한, 본 발명의 실시예들에 따른 디지털 서명 방식의 키 생성 알고리즘($KeyGen_q$) 및 서명 알고리즘($Sign_q$)을 사용하는 서명 당사자는 고전적인 디지털 서명 방식의 검증 알고리즘(Verify)을 사용하여 검증 당사자와 하위 호환되는 서명(σ)을 유리하게 생성함을 알 수 있다.

[0040] 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식에 대한 하위 호환성은 서명 알고리즘($Sign_q$)에 의해 반환된 서명($H(\rho)$)이 개인 키(K_s)와 실질적으로 동일한 알고리즘(Sign)을 사용하여 생성된다는 사실에 의해 입증된다. 따라서 검증 알고리즘(Verify)을 사용하는 모든 검증 당사자는 증명(π)을 무시하고 검증 알고리즘(Verify)을 계속 호출하여 메시지(M) 및 공개 키(K_p)에 대한 서명(σ)의 유효성을 확인할 수 있다.

[0041] 따라서 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식을 구현하기 위해 디지털 서명 알고리즘, 해시 함수 및 제로-지식 증명 시스템을 포함함을 알 수 있다.

[0042] DSA 또는 ECDSA는 본 발명의 실시예들에 따른 양자 저항 디지털 서명 방식의 디지털 서명 알고리즘으로 쉽게 사용될 수 있다. DSA 및 ECDSA를 위한 개인 키 생성기는 본질적으로 유한 필드에 걸쳐 생성된 예측 불가능한 난수이며, 단방향 해시 함수($H()$)의 출력과 유리하게 잘 일치하기 때문이다. 키 생성은 해시 함수의 출력을 RSA 모듈러스를 계산하는 데 사용되는 둘 이상의 예측 불가능한 소수와 일치시키는 것을 수반하기 때문에 RSA를 서명 알고리즘으로 사용하는 것은 더 복잡하고 지루하다. 가능한 테크닉은 해시 출력을 매우 큰 소수의 순서 목록으로 매핑하거나 소수가 찾을 때까지 반복적으로 해시(또는 마이닝)하는 것을 포함한다. 더 간단한 구현을 위해, ECDSA는 가장 작은 증명 크기로 변환되는 가장 작은 키 크기를 갖기 때문에 사용되며, 선택될 수 있는 가능한

곡선은 본 실시예의 구현에 사용되는 secp256r1(또는 프라임 256v1)일 수 있다.

[0043] 본 발명의 실시예들에 따라 사용될 그리고 본 명세서의 구현 예들에 사용되는 해시 함수는 붕괴 해시 함수이고, 출력이 secp256r1 곡선과 잘 부합하기 때문에 SHA-256이다.

[0044] 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식에 사용될 제로-지식 증명 시스템은 포스트-양자 보안이 요구된다. 이러한 제로-지식 증명 시스템 중 하나는 ZKBoo이며, 이는 세 개의 가지를 가지는 MPC-in-head 구현이고 이미 준비된 SHA-256 구현이기 때문이다. 따라서, ZKBoo는 본 명세서의 구현 예들을 위한 제로-지식 증명 시스템으로 사용될 수 있다.

[0045] 도 1은 본 발명의 실시예들에 따른 예시적인 양자 저항 ECDSA 키 생성 알고리즘($KeyGen_q$)을 나타낸다.

[0046] 도 1을 참조하면, 키 생성 알고리즘($KeyGen_q$)(100)은 공개 키(K_p)를 계산하기 전에 비밀 사전 이미지(ρ)를 해시하기 위해 수행되는 추가 단계(110, 4라인)를 제외하고는 키 생성 알고리즘(KeyGen)과 매우 유사하게 기능한다.

[0047] 도 2는 본 발명의 실시예들에 따른 예시적인 양자 저항 ECDSA 서명 알고리즘($Sign_q$)을 나타낸다.

[0048] 도 2를 참조하면, 서명 알고리즘($Sign_q$)(200)은 개인키(H(ρ))를 사용하여 ECDSA 서명을 계산하는 것 외에도 개인키(H(ρ))의 사전 이미지에 대한 제로-지식 증명, 공개키(K_p)가 개인키(H(ρ))로부터 계산된다는 제로-지식 증명, H(M)가 서명되는 메시지라는 약속(commitment)을 포함하는 ZKBoo 증명(π)을 반환한다.

[0049] 단계(210, 10라인)에서 본 발명의 실시예들에 따른 구현은 지아코멜리(Giacomelli)의 SHA-256 코드를 사용한다. 증명(π)에서 계산 단계의 수가 개인 키(K_s)를 노출시킬 수 있기 때문에, 다음 단계(220, 11라인)를 코딩하기 위해 특별한 주의가 필요하다. 예를 들어, 개인 키(K_s)가 생성된 후 공개 키(K_p)를 계산할 때, 타원-곡선 암호화(ECC)에 대한 방정식은 $K_p = K_s.G \bmod P$이며, 여기서 G는 타원 곡선의 알려진 기저점이고 P는 곡선의 순서이고 mod는 모듈로 연산을 나타낸다. 정상적인 계산에서 G는 개인 키(K_s)를 곱한 내적이다. 개인 키(K_s)는 1에서 2^{256} 사이의 값이고 곱셈에 비트 시프트 방법이 사용되기 때문에, 공개 키(K_p)를 얻으려면 1에서 256 사이의 내적이 수행되어야 한다. MPC-in-the-head 제로-지식 증명에서, 공개 키(K_p)를 계산하는 데 필요한 회로의 게이트 수가 증명에 표시되며, 이는 누군가 증명 회로의 크기를 분석하면 개인 키(K_s) 값이 노출될 것임을 의미한다. 따라서, 본 발명의 실시예들에 따라, 그리고 유리하게 개인 키(K_s)의 값을 추가로 차폐/숨기기 위해, 공개 키 계산에서 회로의 수가 정적으로 유지되도록 개인 키(K_s)의 값과 관계없이 미리 정의된 내적의 수를 수행하는 회로가 생성된다. 본 실시예에서, 타원 곡선은 secp256r1 곡선이므로, 미리 정의된 계산 수는 256이다. 또한, 타원 곡선 곱셈을 수행할 때, 몽고메리(Montgomery) 사다리 이중 및 추가 항상 기법은 보안 수준을 추가하고 타이밍 및 전력 측면 채널 공격을 방지하기 위해 유리하게 구현되며, 여기서 공격자는 개인 키에서 공개 키를 계산할 때 시간 또는 전력 소비를 측정한다.

[0050] 도 3은 본 발명의 실시예들에 따른 예시적인 양자 내성 ECDSA 검증 알고리즘($Verify_q$)을 나타낸다.

[0051] 도 3을 참조하면, 양자 내성 ECDSA 검증 알고리즘($Verify_q$)(300)은 제1 파트(310)(5라인부터 12라인까지)가 검증 알고리즘(Verify)과 유사한 ECDSA 서명 검증이고, 제2 파트(320)(14라인부터 20라인까지)가 본 발명의 실시예들에 따른 양자 내성 제로-지식 증명의 추가 검증인 두 부분으로 구성됨을 알 수 있다.

[0052] 본 실시예들에 따른 양자 내성 디지털 서명 방식의 예시적인 구현은 C 언어로 구현되었으며 64비트 마이크로소프트 윈도우 10에서 Cygwin 단자를 실행하는 8개의 CPU 코어와 8GB RAM을 갖춘 Intel I5-8250U 8th Gen 머신에서 테스트되었다. 운영 체제 수준의 CPU 스케줄링이나 조정은 수행되지 않았다. ZKBoo 라운드 수를 50에서 250까지 50씩 증분으로 변경했을 때의 증명 크기뿐만 아니라 서명 알고리즘($Sign_q$)과 검증 알고리즘($Verify_q$)의 실행 시간도 측정되었다. 라운드 수를 증가시키면 증명의 비트 강도가 증가하지만 하기의 표 1과 같이 증명 크기와 실행 시간도 의도치 않게 증가한다.

표 1

[0053]

ZKBoo Rounds	50	100	150	200	250
증명 크기(Kbytes)	1,978	3,956	5,934	7,912	9,890

서명 알고리즘 수행 시간(sec)	20.9	45.9	72.9	95.1	118.2
검증 알고리즘 수행 시간(sec)	19.6	45.0	71.0	93.2	115.7

[0054] 250비트 강도 증명에 대한 측정된 오버헤드는 언뜻 보기에 약 10MB 크기의 매우 큰 증명을 보여주며 서명 알고리즘($Sign_q$) 또는 검증 알고리즘($Verify_q$) 중 하나를 수행하는 데 거의 2분이 걸린다. 그러나 이하에서 논의되는 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식의 실제 배포 구현은 증명이 비동기적으로 생성되고 인증서와 별도로 저장될 수 있기 때문에(즉, 증명이 제1 디지털 위치에 저장되고 인증서가 제2 디지털 위치에 저장되는) 사용자 경험에 대한 영향을 감소시킬 수 있다. 이는 병렬 처리 또는 비동기 검증을 유리하게 하여 사용자 경험에 대한 영향을 추가로 감소시킬 수 있다.

[0055] 하위-호환성 및 양자 내성으로의 마이그레이션(이동)과 관련된 문제를 연구하기 위해, 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식은 기존의 (변경되지 않은) Adobe Acrobat(어도비 아크로뱃) Reader DC를 사용하여 양자 내성 디지털 서명 방식의 실제 배포 구현으로 양자 내성 타임-스탬프 서명된 PDF를 요청하는 동시에 타임-스탬프 서버에 배포되었다. 배포는 클라이언트와 서버 모두에서 64비트 마이크로소프트 윈도우 10을 실행하는 8개의 CPU 코어와 8GB RAM을 갖춘 Intel I5-8250U 8세대 기계가 있는 노트북에서 수행되었다. 설정에는 타임-스탬프 클라이언트와 타임-스탬프 서버가 포함되었다. 타임-스탬프 클라이언트의 경우, 이 클라이언트가 이미 ECDSA를 지원하고 수정되지 않고 사용할 수 있도록 Adobe Acrobat Reader DC v2021.x가 사용되었다. 타임-스탬프 서버의 경우, 피에르 프랑수아 카르팡티에(Pierre-Francois Carpentier(출처 https://github.com/kakwa/uts-server)의 오픈 소스 타임-스탬프 서버가 수정되지 않은 코드와 함께 사용되었다.

[0056] 암호화 라이브러리의 경우 타임-스탬프 서버는 OpenSSL v1.1.x를 사용하여 서버 인증서의 인증 기관(Certification Authority, 이하 'CA') 발급 작업을 수행할 뿐만 아니라 RFC3161에 따른 디지털 서명을 수행한다. OpenSSL v1.1.1b 버전은 X.509 인증서 발급과 타임-스탬프 모두에 대해 확장된 디지털 서명 방식을 수행하도록 수정되었다. ZKBoo 증명을 비동기적으로 생성하면서 OpenSSL이 ECDSA 서명을 반환하도록 최적화하였다. 이를 통해 ZKBoo 증명이 완전히 생성될 때까지 기다리지 않고 ECDSA 서명된 타임-스탬프를 클라이언트에 반환할 수 있었다. 따라서 증명은 인증서와 별도로 저장되었다.

[0057] 인증서와 타임-스탬프에 대한 양자 내성 256라운드 ZKBoo 증명은 각각 10MByte이므로 클라이언트에 쉽게 전송할 수 없다. 따라서 수정된 OpenSSL 버전은 서명된 X.509 인증서 또는 호출 프로그램으로 반환된 PKCS#7 타임-스태프에 URL 링크를 포함하면서 증명을 Dropbox(드롭박스)(www.dropbox.com)에 기입하였다.

[0058] 도 4는 테스트 중인 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식의 실생활 구현의 사용 사례를 나타내는 처리 다이어그램이다.

[0059] 도 5는 본 발명의 실시예들에 따른 양자 저항 디지털 서명 방식의 실생활 구현에서 미리 정의된 인증서 계층 구조를 예시한 윈도우들의 이미지들을 나타낸다.

[0060] 도 6은 본 실시예들에 따른 양자 저항 디지털 서명 방식의 실생활 구현에서 타임-스탬프 클라이언트에 의한 검증을 예시한 윈도우의 이미지를 나타낸다.

[0061] 먼저 도 4를 참조하면, 처리 다이어그램(400)은 테스트 중인 본 실시예들에 따른 양자 저항 디지털 서명 방식의 실제 구현의 사용 사례들을 보여준다. 도 4에 도시된 바와 같이, 구현은 최종 사용자(401)가 타임-스탬프 클라이언트로서 어도비 아크로뱃(Adobe Acrobat) 리더(402)를 사용할 수 있게 하였다. 구현은 또한 인증서 발급 및 타임-스탬프를 위해 OpenSSL(406)을 사용하고, OpenSSL(406)은 증명을 드롭박스(408)에 기록하는 타임-스탬프 서버(404)를 포함한다.

[0062] 한 번만 수행되는 셋업 단계(410)에서, 최종 사용자(401)에 의하여 OpenSSL(406)은 루트 CA 인증서에 대한 키 및 인증서를 생성(412)하는 데 사용되고, 최종 사용자(401)에 의하여 타임-스탬프 서버 인증서에 대한 키 및 인증서를 생성(414)하는 데 사용된다. 본 발명의 실시예들에 따라 정의된 인증서 계층 구조가 채택되고, 여기서 루트 CA는 도 5의 이미지(500)의 윈도우들(510, 520)과 같이 중간 CA 없이 서버 인증서를 인증한다. 두 인증서는 드롭박스(408)의 양자 내성 증명을 나타내기 위해 디지털 저장 위치 정보로서 X.509 권한-정보-접근(Authority-Information-Access) 확장 하에서의 링크(416, 418)를 포함한다. 동작에서, 디지털 저장 위치는 인증 기관 또는 검증자에 의해 디지털 저장 위치를 식별하기 위한 위치 정보를 사용하여 액세스 가능한 공용 저장소일 수 있다. 루트 CA 인증서는 최종 사용자(401)에게 다운로드(420)된 다음 루트-투-트러스트(root-to-

trust)를 설정하기 위해 어도비 아크로뱃(402)으로 가져온다(422). 도 5를 참조하면, 양자 내성 보호 계층은 미리 정의된 인증서 계층을 갖는 개인 키의 사전 이미지에 대한 복수의 지식 증명들을 제공함으로써 둘 이상의 당사자들을 지원할 수 있다.

[0063] RFC3161 단계(430)에서, PDF 문서는 최종 사용자(401)가 PDF를 개봉(432)한 후에, 어도비 아크로뱃(402)으로부터 타임-스탬프 서버(404)로의 요청을 개시(434)함으로써 타임-스탬프될 수 있다. 타임-스탬프 서버(404)는 OpenSSL(406)에 ECDSA 서명 요청을 전송(436)하고, ECDSA 서명된 PKCS#7 타임-스탬프를 OpenSSL(406)로부터 수신한다(438). 타임-스탬프 서버(404)는 타임-스탬프 응답을 어도비 아크로뱃(402)에 제공한다(440). 타임-스탬프 증명(442)은 유사하게, 드롭박스(408)에, URL 링크가 타임-스탬프에 내장되어 저장된다. 이 타임-스탬프는 어도비 아크로뱃(402)에 의해 검증되고(444), 최종 사용자(401)에 의해 나중에 인증(446)을 위해 PDF에 저장될 수 있다. 검증의 예는 도 6의 이미지(600)에 나타나 있다. 수정되지 않은 어도비 아크로뱃은 ECDSA 서명된 타임-스탬프 및 인증서 체인을 검증할 뿐, ZKBoo 증명은 검증하지 않으므로, 최종 사용자가 경험하는 대기 시간에 어떠한 변화도 발생하지 않는다.

[0064] 포스트 업그레이드 단계(450)에서, 검증 알고리즘($Verify_q$)을 실행할 수 있는 모든 검증 당사자는 인증서/서명 블록에 있는 링크를 따라(452) 양자 내성 ECDSA 검증 알고리즘(300, 도 3) 방식대로 완전한 서명 검증을 위해 양자 내성 증명을 다운로드(454)할 수 있다.

[0065] 양자 내성 디지털 서명 방식으로 점진적으로 마이그레이션되는 시스템에 미치는 영향을 이해하기 위해, 상이한 마이그레이션 단계에서 서명 및 검증 당사자에 대한 상이한 결과를 표 2에 나열한다. 표 2에서 볼 수 있듯이, 본 발명의 실시예들에 따라 양자 내성을 계층화하는 적절한 마이그레이션 전략은 먼저 서명 당사자들이 양자 내성 증명을 서명에 포함하도록 업그레이드한 후, 증명을 검증할 수 있도록 검증 당사자들을 업그레이드하는 것이다. 조기 업그레이드를 선택한 검증 당사자의 경우, 아직 업그레이드되지 않았을 수도 있는 서명 당사자들과의 호환성을 유지하기 위해 위에서 논의된 고전적인 디지털 서명 방식에 따라 검증 기능을 포함하는 것이 권장된다.

표 2

[0066]

		검증 당사자	
		정의 1[1]	정의2[2]
서명 당사자	정의 1[1]	현재 시나리오. 서명된 서류는 포스트-양자 시대에 위조에 취약함	서명된 서류는 양자 내성 증명을 포함하지 않음. 검증 당사자들은 서명 당자자들에서 마이그레이션을 수행하도록 통보하면서 서류를 거부하거나 검증 알고리즘(Verify)을 사용하여 서명을 확인할 수 있음.
	정의 2[2]	마이그레이션 프로세스의 제1 단계에 해당. 서명된 서류는 양자 내성 증명을 포함함. 서명 당자사들은 검증 당사자들이 이 단계를 수행하기 전에 마이그레션하는 것을 기다릴 필요 없음. 검증 당사자들은 양자 내성 증명을 무시하는 동안 서명을 계속 검증함.	앞으로 될 상태이고, 마이그레션 프로세스의 제2 단계에 해당. 서명 당사자들이 마이그레이션하고 양자 내성 증명을 포함하는 서명된 서류를 전송하기 시작한 후에, 검증 당사자들은 시스템을 업그레이드하여 시스템이 서명과 증명을 검증하여 마이그레이션 프로세스가 완결되도록 함.

[0067] [1] 아직 마이그레이션 되지 않음. 정의 1의 키 생성 알고리즘(KeyGen), 서명 알고리즘(Sign) 및 검증 알고리즘(Verify)을 여전히 사용함.

[0068] [2] 마이그레이션 완료. 정의 2의 키 생성 알고리즘($KeyGen_q$), 서명 알고리즘($Sign_q$) 및 검증 알고리즘($Verify_q$)을 사용하도록 업그레이드됨.

[0069] 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식의 장점들은 당업자에게 쉽고 명백하며 오늘날의 기술로 도입될 수 있다. 보다 강력한 양자 컴퓨터들이 온라인에 접속됨에 따라, 포스트-양자 마감일이 다가오고 있으며, 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식의 장점들은 안전하고 인증 가능한 통신들을 위

해 필수적인 것이 될 것이다. 포스트-양자 마감일에 대한 참고로서, NIST는 2030년까지 10억 달러의 예산으로 RSA-2048을 암호화 분석할 수 있는 양자 컴퓨터가 구축될 가능성이 높다는 보고서를 제공했다. 이를 해결하기 위해, NIST는 적합한 양자-보안 디지털 서명 및 키-교환 알고리즘들을 선택하기 위한 포스트-양자 표준화 작업에 착수하고 있다. 최종 선택은 2024년까지 발표될 예정인 새로운 표준들과 함께 곧 완료될 것으로 예상된다. 이와 별도로, NIST는 조건에 따른 포스트-양자 사용을 위해 두 개의 상태형 해시 기반 서명들, 즉 레이튼-미시(Leighton-Micali) 서명들 및 eXtended-Merkle 서명 방식을 또한 추천했다.

[0070] 업계는 2024년 이후의 새로운 시스템 구현을 장려하여 새로운 디지털 서명 표준을 채택하는 것을 고려할 것으로 보이지만, 기존 또는 향후 시스템에 대한 다양한 도전이 예상된다.

[0071] 디지털 서명을 양자 보안으로 만들기 위한 본능적인 접근 방식은 대체 또는 추가적인 양자 보안 알고리즘을 사용하는 것이다. NIST의 양자 후 표준화 연습은 현재 두 개의 격자 기반 알고리즘인 Dilithium 및 Falcon과 한 개의 다변량 기반 알고리즘인 Rainbow를 최종 3개의 디지털 서명 알고리즘으로 식별했다. 다변량 기반 GeMSS, 제로-지식 기반 Picnic(또한 ZKB++를 생성하기 위한 기본 증명 시스템으로 본 실시예에서 논의된 제로-지식 증명 시스템인 ZKBoo를 사용함) 및 상태 비저장 해시 기반 SPHINCS+와 같은 세 가지 대체 알고리즘이 최종 후보에 올랐지만 2024년 마감일 이후에 추가 평가를 거칠 것이다. 이상적으로는 소프트웨어 라이브러리 또는 하드웨어 보안 모듈 형태의 "드롭-인 대체"를 사용하여 RSA/DSA/ECDSA를 표준화하는 새로운 알고리즘과 스왑 아웃 또는 증강할 것이다. 그러나 이러한 각 알고리즘은 고유한 리소스, 성능 및 플랫폼 고려 사항이 있으며 다양한 주요 세리모니(ceremony) 프로세스 및 프로토콜과 결합되어 있으므로 마이그레이션 플레이북(playbook)을 설계하고 수행해야 할 가능성이 높다.

[0072] 다른 접근법은 손상 시 정규 서명 키를 재정의할 수 있는 백업 키를 사용하는 것이다. 하나의 제안은 키 생성 과정에서 생성되고 원래 키가 손상되거나 손실될 경우 폴백(fall-back) 절차로 사용될 수 있는 양자 내성 상태 해시 기반 W-OTS+ 백업 키를 사용하는 것이다. 이러한 백업 디지털 서명 키 접근법은 인증 관련 프로토콜을 위한 계정-복구 메커니즘으로 작동할 수 있지만, 데이터의 장기 비반복 보호가 필요한 일상적인 비-상호작용 디지털 서명 사용 사례에는 적합하지 않다.

[0073] 타임-스탬핑 사용 사례와 관련하여, 해시 시퀀스를 순방향 또는 역방향으로 체인하는 것은 문서 시퀀스를 선형 해시-체인을 통해 또는 머클(Merkle) 트리를 통해 타임-스탬핑하도록 연결함으로써 디지털 타임-스탬핑을 포함할 수 있는 장기적이고 가능성이 높은 양자 보안의 타임-스탬핑을 제공하기 위한 잘 알려진 접근법이다. 오늘날 이더리움과 같은 블록체인은 이미 타임-스탬핑 스마트 계약을 지원하고 블록체인에 대한 분산형 타임-스탬프 프로토콜을 제공하여 사전/사후 데이팅을 방지할 수 있다. 이러한 기술은 일반적으로 특정 발생 시간을 결정하기 위해 공개적으로 검증 가능한 체인에 의존하기 때문에 일반적으로 디지털 서명을 보호하기 위한 양자 내성 메커니즘으로 적용할 수 없다. 공개 블록체인은 또한 수행된 트랜잭션의 수와 트랜잭션된 타이밍이 공개적으로 사용 가능하기 때문에 프라이버시 관련 우려에 직면한다.

[0074] 따라서, 본 발명의 실시예들은 안전하고 인증가능한 통신들에서 존재하는 그리고 다가오는 약점들을 유리하고 효율적으로 해결하는 현재의 해결책을 전달하는 양자 내성 디지털 서명 방식을 제공함을 알 수 있다. 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식은 포스트-양자 디지털 서명을 구현함에 있어서 다른 접근법을 취한다. 다른 양자-보안 디지털 서명 알고리즘을 대체하거나 추가하는 대신, 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식은 더 장기적인 양자 내성을 달성하면서 고전적인 RSA, DSA 또는 ECDSA 디지털 서명 알고리즘들을 계속 사용하는 것을 가능하게 한다. 이것은 디지털 서명에 더하여 개인 키의 사전 이미지의 지식의 제로-지식 증명을 계층화함으로써 달성된다. 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식으로, 양자 준비 상태에서 앞서 나가기를 원하는 디지털 서명 구현들은 기존 애플리케이션들에 대한 하위-호환성을 계속 유지한다. 이는 상이한 시스템들이 양자 준비 상태로의 마이그레이션이 발생할 때에 상이한 타임 라인들 및 스케줄들을 가질 수 있는 반면, 본 발명의 실시예들에 따른 양자 내성 디지털 서명 방식은 업그레이드된 애플리케이션들과 업그레이드되지 않은 애플리케이션들 사이의 심리스(seamless) 동작들을 보장할 수 있기 때문에 매우 유리하다.

[0075] 본 명세서에서 논의된 본 실시예들에 따른 양자 내성 디지털 서명 방식의 적용이 예시적인 PDF 문서 타임-스탬핑 방식과 관련하여 적용되는 동안, 양자 내성을 계층화하기 위해 본 발명의 실시예들에 따른 디지털 서명 방식을 이용할 수 있는 블록체인, 보안 이메일 및 전송 계층 보안과 같은 다른 응용예들이 있다.

[0076] 예시적인 실시예들이 전술한 실시예들의 상세한 설명에서 제시되었지만, 방대한 수의 변형들이 존재함을 인식해야 한다. 예시적인 실시예들은 단지 예시일 뿐이며, 어떠한 방식으로든 발명의 범위, 적용 가능성, 동작 또는

구성을 제한하기 위한 것이 아님을 추가로 인식해야 한다. 오히려, 전술한 상세한 설명은 당업자에게 본 발명의 예시적인 실시예들을 구현하기 위한 편리한 로드맵을 제공할 것이지만, 첨부된 청구항들에 기재된 바와 같이 본 발명의 범위를 벗어나지 않으면서, 예시적인 실시예들에서 설명된 단계들 및 동작 방법의 기능 및 배열에 있어서 다양한 변경이 이루어질 수 있음을 이해하여야 한다.

도면

도면1

양자 내성 ECDSA 키 생성 알고리즘: KeyGen_q

```
1 begin
2   G ← ECC base point; P ← ECC order;
3   Generate secret pre-image ρ;
4   Compute private key K_s = H(ρ);
5   Compute public key K_p = (x, y) where K_p ≡ K_s · G mod P;
6   destroy K_s;
7   return ρ, K_p;
8 end
```

110

100

도면2

양자 내성 ESDSA 서명 알고리즘: Sign_q

```
1 begin
2   G ← ECC base point; P ← ECC order;
3   ρ ← secret pre-image;
4   M ← message;
5   Generate signature random r;
6   Compute r^-1 where r * r^-1 ≡ 1 mod P;
7   Compute R = (R_x, R_y) where R ≡ r · G mod P;
8   Compute hash of message H(M);
9   Enumerate ZKBoo proof π = begin
10      Zero-knowledge computation of private key K_s where K_s = H(ρ) ;
11      Zero-knowledge computation of public key K_p where
          K_p ≡ K_s · G mod P;
12      Compute s where s ≡ r^-1 * (H(M) + R_x * K_s) mod P;
13      Commit R_x, s in the proof;
14  end
15  destroy r, r^-1, K_s;
16  return σ = {R_x, s}, π;
17 end
```

210

220

200

도면3

양자 내성 ESDSA 검증 알고리즘: Verify_q

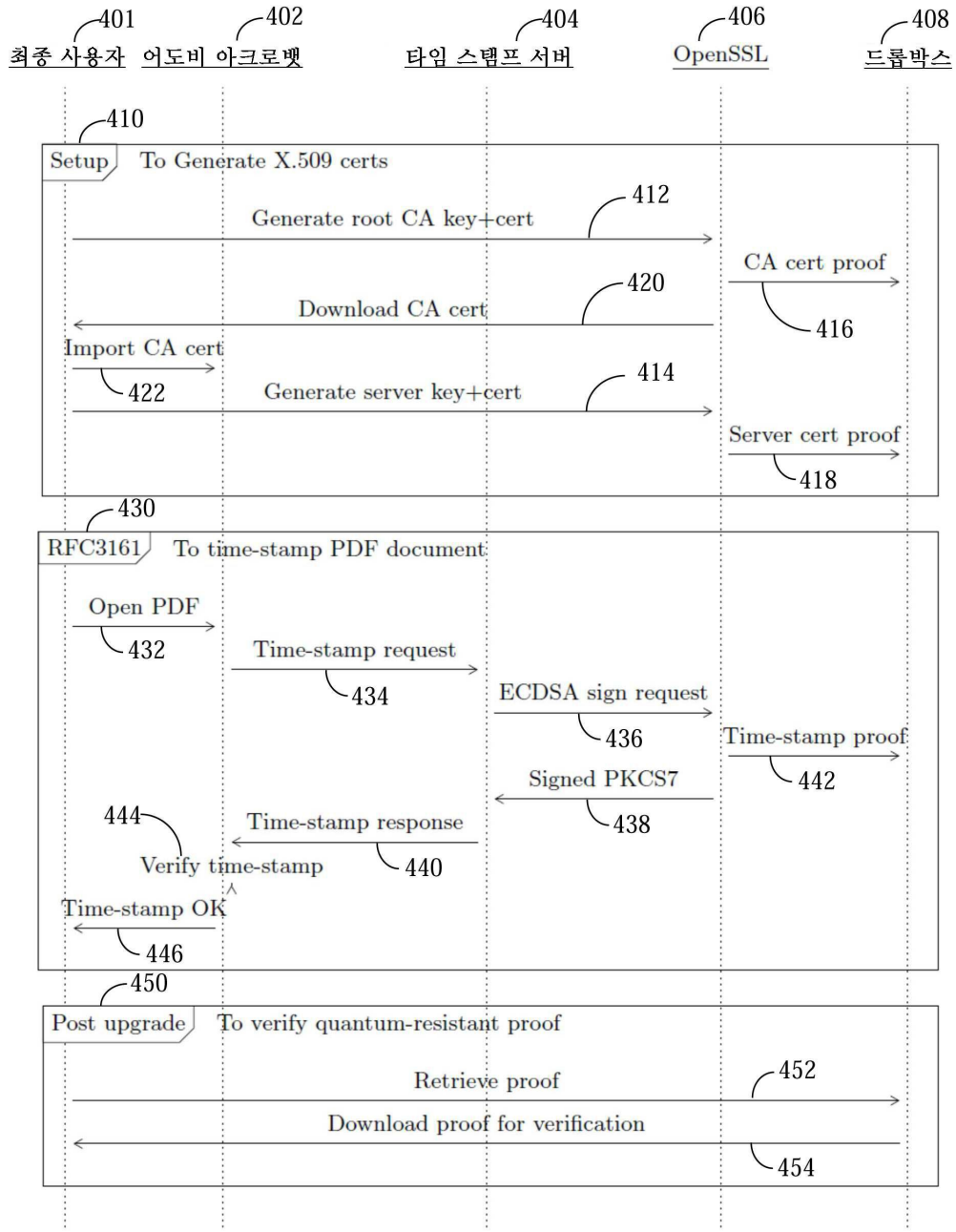
```
1  begin
2      G ← ECC base point; P ← ECC order;
3      K_p ← ECC public key;
4      R_x, s ← signature σ; π ← proof; M ← message;
5      Compute s^{-1} where s * s^{-1} ≡ 1 mod P;
6      Compute hash of message H(M);
7      Compute u_1 = s^{-1} * H(M) mod P;
8      Compute u_2 = s^{-1} * R_x mod P;
9      Compute V = (V_x, V_y) where V = u_1 · G + u_2 · K_p mod P;
10     if V_x ≠ R_x then
11         return "Failed Signature Verification"
12     end
13     else
14         Verify ZKBoo proof π = begin
15             Check that R_x, s is committed in the proof;
16             Check that zero-knowledge computation of K_p from unknown
                pre-image is correct;
17             if Check Failed then
18                 return "Failed Proof Verification"
19             end
20         end
21     end
22     return success;
23 end
```

310

320

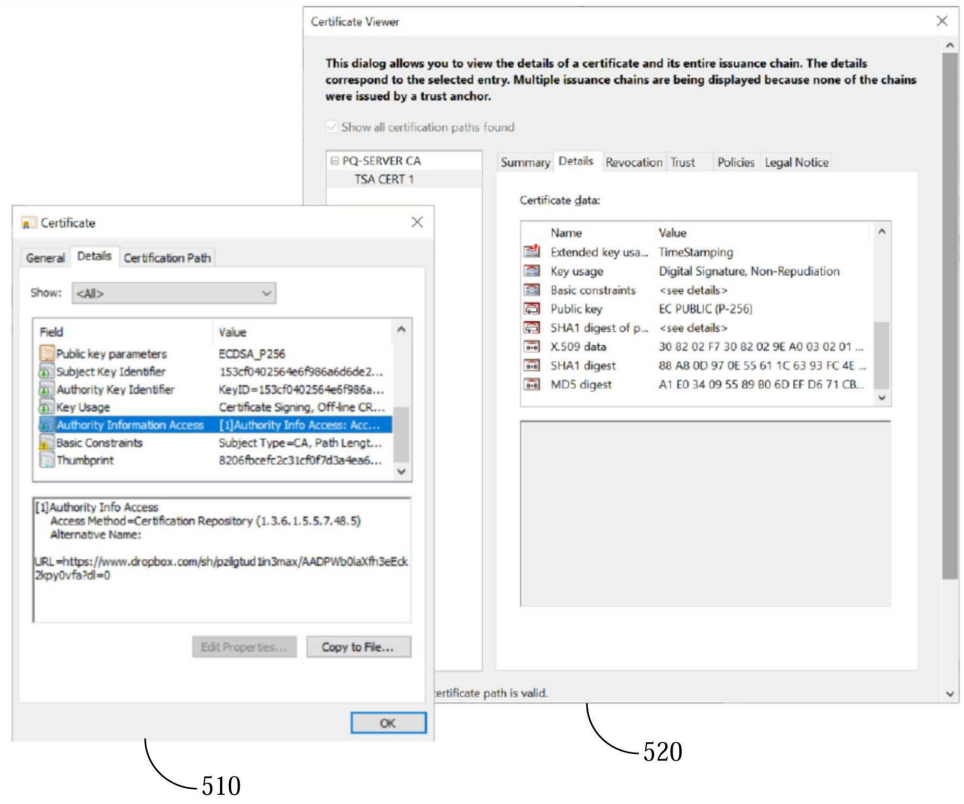
300

도면4


401
최종 사용자
402
어도비 아크로뱃
404
타임 스탬프 서버
406
OpenSSL
408
드롭박스
410
Setup
To Generate X.509 certs
412
Generate root CA key+cert
CA cert proof
420
Download CA cert
416
Import CA cert
422
Generate server key+cert
414
Server cert proof
418
430
RFC3161
To time-stamp PDF document
Open PDF
432
Time-stamp request
434
ECDSA sign request
436
Time-stamp proof
442
Signed PKCS7
438
444
Time-stamp response
440
Verify time-stamp
Time-stamp OK
446
450
Post upgrade
To verify quantum-resistant proof
Retrieve proof
452
Download proof for verification
454

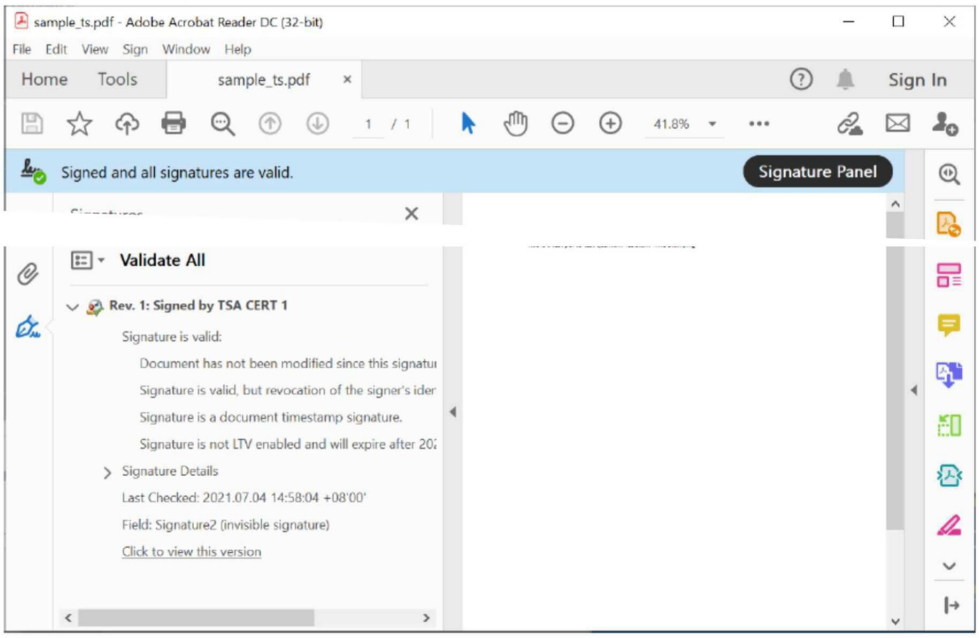
400

도면5



500

도면6



600