



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0166384
(43) 공개일자 2023년12월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
(52) CPC특허분류
H04L 9/3255 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2022-0066302
(22) 출원일자 2022년05월30일
심사청구일자 2022년05월30일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57 한빛아파트 132-801
김근영
대전광역시 유성구 장대로 87 퍼스트캐슬 202호
김준석
대전광역시 유성구 대학로 53
(74) 대리인
이은철, 김재문

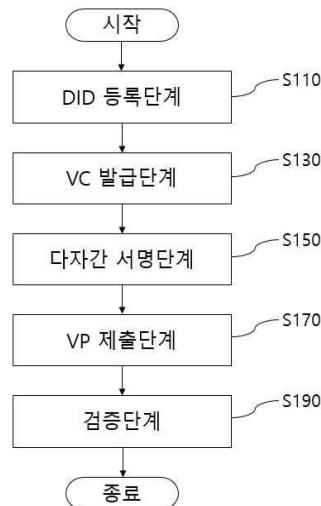
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 다자간 서명을 지원하는 DID 인증 방법 및 시스템

(57) 요약

본 발명은, 사용자의 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록단계; 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급단계; 검증자의 증명 요청을 받은 사용자와 다른 사용자가 다자간 서명을 수행하여 VC에 대한 다자간 서명값을 생성하는 다자간 서명단계; 증명 요청을 받은 사용자가 생성된 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출단계; 및 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증단계;를 포함하는 것을 일 특징으로 한다.

대표도 - 도1



(52) CPC특허분류

H04L 9/3026 (2013.01)

H04L 9/50 (2022.05)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711157470
과제번호	2020R1A2C2008864
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)
연구과제명	영지식 증명을 지원하는 스마트 컨트랙트 프레임워크 연구
기 여 율	1/1
과제수행기관명	충남대학교
연구기간	2021.03.01 ~ 2023.02.28

명세서

청구범위

청구항 1

사용자의 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록단계;

사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급단계;

검증자의 증명 요청을 받은 사용자와 다른 사용자가 다자간 서명을 수행하여 VC에 대한 다자간 서명값을 생성하는 다자간 서명단계;

증명 요청을 받은 사용자가 생성된 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출단계; 및

검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증단계;를 포함하는 DID 인증 방법.

청구항 2

제 1 항에 있어서,

상기 다자간 서명단계는,

상기 다자간 서명에 참여한 사용자들이 각각 비밀키에 대한 덧셈 공유값을 계산하고 인스턴스 키를 교환하는 단계를 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 3

제 2 항에 있어서,

상기 다자간 서명단계는,

상기 다자간 서명에 참여한 사용자 간에 곱셈 연산을 3번 반복하여 제 1 곱셈 공유값, 제 2 곱셈 공유값, 및 제 3 곱셈 공유값을 획득하고, 상기 제 2 곱셈 공유값과 제 3 곱셈 공유값을 더하여 제 4 곱셈 공유값을 계산하는 단계;를 더 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 4

제 3 항에 있어서,

상기 다자간 서명단계는,

검증자의 증명 요청을 받은 사용자가 제 1 일관성 체크값과, VC를 서명한 제 1 서명값을 포함하여 계산한 제 2 일관성 체크값을 다른 사용자에게 전달하는 단계;를 더 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 5

제 4 항에 있어서,

상기 다자간 서명단계는,

다른 사용자가 상기 제 1 일관성 체크값을 이용하여 제 2 서명값을 생성하고, 상기 제 2 일관성 체크값을 이용하여 VC에 대한 다자간 서명값을 생성하는 단계;를 더 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 6

제 5 항에 있어서,

상기 다자간 서명단계는,

다른 사용자가 생성된 VC에 대한 다자간 서명값을 검증자의 증명 요청을 받은 사용자에게 전송하는 단계;를 더 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 7

제 1 항에 있어서,

상기 DID 등록단계는,

각각의 사용자가 공개키쌍을 생성하여, 본인을 제외한 다른 사용자들에게 생성한 공개키를 전달하고, 각각의 사용자는 전달받은 공개키를 바탕으로 공동 공개키를 생성하는 단계;를 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 8

제 7 항에 있어서,

상기 DID 등록단계는,

각각의 사용자가 로컬 다항식 점($p_i(x)$)을 생성하여 다른 사용자의 인덱스에 맞는 로컬 다항식 점을 전달하고, 각각의 사용자는 전달받은 로컬 다항식 점들을 이용하여 비밀키 역할을 하는 다항식 점($p(x)$)을 구성하는 단계; 더 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 9

제 1 항에 있어서,

상기 검증단계는,

VP에 명시된 증명 요청을 받은 사용자의 DID를 통해 블록체인에서 증명 요청을 받은 사용자의 DID 문서를 조회하여 찾은 공동 공개키로 VP의 다자간 서명값을 검증하는 단계;를 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 10

제 9 항에 있어서,

상기 검증단계는,

발급자의 DID를 통해 블록체인에서 발급자의 DID 문서를 조회하여 찾은 발급자의 공개키로 VC의 다자간 서명값을 검증하는 단계;를 더 포함하는 것을 특징으로 하는 DID 인증 방법.

청구항 11

사용자의 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록부;

사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급부;

검증자의 증명 요청을 받은 사용자와 다른 사용자가 다자간 서명을 수행하여 VC에 대한 다자간 서명값을 생성하는 다자간 서명부;

증명 요청을 받은 사용자가 생성된 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출부; 및

검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증부;를 포함하는 DID 인증 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 DID 인증 방법 및 시스템에 관한 것으로서, 특히 임계 서명 기법을 이용하여 다자간 서명 기능을 제공하는 블록체인 기반 DID 인증 방법 및 시스템에 관한 것이다.

배경 기술

[0003] 분산아이디 또는 DID(Decentralized Identity)는 기존 신원확인 방식과 달리 중앙 시스템에 의해 통제되지 않으며 개개인이 자신의 정보에 완전한 통제권을 가질 수 있게 하는 기술이고, 분산신원확인 또는 탈중앙화 신원확인이라고도 한다. DID는 국제표준단체인 W3C 주도하에 표준이 제정되고 있으며 자격증, 증명서 관리 등 다양한 기능을 제공한다.

[0004] 최근에는 블록체인 기반 DID 인증 기술에 대한 연구가 활발히 진행되고 있다. 블록체인 기반 DID 인증 시스템은 사용자가 본인을 증명할 수 있는 DID document를 블록체인에 저장하고, 이를 통해 본인 인증을 수행하여 발행자로부터 VC(Verifiable Credential)를 발행받으며, 발행받은 VC를 VP(Verifiable Presentation) 형태로 만들어 검증자에게 제출하여 서비스를 요청한다.

[0005] 현행 방식은 ECDSA 암호 알고리즘을 이용한 단일 서명만 지원하므로 VC에 대해 단일 보유 주체에 대한 서명만 가능하다. 이를 해결하기 위한 방법으로 제안된 기존의 다중 서명(Multi Signature) 기법은 검증자의 검증 기능에 대한 수정이 필요하다는 문제점이 있다.

[0006] 따라서, 다자간 서명 기능을 지원하는 전자서명 알고리즘을 선정하고, 이를 위한 새로운 DID 인증 과정의 도입이 요구되고 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 기존의 알고리즘에서 검증 기능에 대한 수정 없이 다자간 서명 기능을 제공하는 블록체인 기반 DID 인증 방법 및 시스템을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0010] 상기 목적을 달성하기 위하여 본 발명은, 사용자의 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록단계; 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급단계; 검증자의 증명 요청을 받은 사용자와 다른 사용자가 다자간 서명을 수행하여 VC에 대한 다자간 서명값을 생성하는 다자간 서명단계; 증명 요청을 받은 사용자가 생성된 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출단계; 및 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증단계;를 포함하는 것을 일 특징으로 한다.

[0011] 바람직하게는, 상기 서명단계는, 상기 다자간 서명에 참여한 사용자들이 각각 비밀키에 대한 덧셈 공유값을 계산하고 인스턴스 키를 교환하는 단계를 포함할 수 있다.

[0012] 바람직하게는, 상기 서명단계는, 상기 다자간 서명에 참여한 사용자 간에 곱셈 연산을 3번 반복하여 제 1 곱셈

공유값, 제 2 곱셈 공유값, 및 제 3 곱셈 공유값을 획득하고, 상기 제 2 곱셈 공유값과 제 3 곱셈 공유값을 더하여 제 4 곱셈 공유값을 계산하는 단계;를 더 포함할 수 있다.

[0013] 바람직하게는, 상기 서명단계는, 검증자의 증명 요청을 받은 사용자가 제 1 일관성 체크값과, VC를 서명한 제 1 서명값을 포함하여 계산한 제 2 일관성 체크값을 다른 사용자에게 전달하는 단계;를 더 포함할 수 있다.

[0014] 바람직하게는, 상기 서명단계는, 다른 사용자가 상기 제 1 일관성 체크값을 이용하여 제 2 서명값을 생성하고, 상기 제 2 일관성 체크값을 이용하여 VC에 대한 다자간 서명값을 생성하는 단계;를 더 포함할 수 있다.

[0015] 바람직하게는, 상기 서명 단계는, 다른 사용자가 생성된 VC에 대한 다자간 서명값을 검증자의 증명 요청을 받은 사용자에게 전송하는 단계;를 더 포함할 수 있다.

[0016] 바람직하게는, 상기 DID 등록단계는, 각각의 사용자가 공개키쌍을 생성하여, 본인을 제외한 다른 사용자에게 생성한 공개키를 전달하고, 각각의 사용자는 전달받은 공개키를 바탕으로 공동 공개키를 생성하는 단계;를 더 포함할 수 있다.

[0017] 바람직하게는, 상기 DID 등록단계는, 각각의 사용자가 로컬 다항식 점($p_i(x)$)을 생성하여 다른 사용자의 인덱스에 맞는 로컬 다항식 점을 전달하고, 각각의 사용자는 전달받은 로컬 다항식 점들을 이용하여 비밀키 역할을 하는 다항식 점($p(x)$)을 구성하는 단계;를 더 포함할 수 있다.

[0018] 바람직하게는, 상기 검증단계는, VP에 명시된 증명 요청을 받은 사용자의 DID를 통해 블록체인에서 증명 요청을 받은 사용자의 DID 문서를 조회하여 찾은 공동 공개키로 VP의 다자간 서명값을 검증하는 단계;를 더 포함할 수 있다.

[0019] 바람직하게는, 상기 검증단계는, 발급자의 DID를 통해 블록체인에서 발급자의 DID 문서를 조회하여 찾은 발급자의 공개키로 VC의 다자간 서명값을 검증하는 단계;를 더 포함할 수 있다.

[0020] 또한 본 발명은, 사용자의 DID 문서(DID document)를 생성하여 블록체인에 등록하는 DID 등록부; 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행하는 VC 발급부; 검증자의 증명 요청을 받은 사용자와 다른 사용자가 다자간 서명을 수행하여 VC에 대한 다자간 서명값을 생성하는 다자간 서명부; 증명 요청을 받은 사용자가 생성된 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출하는 VP 제출부; 및 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증하는 검증부;를 포함하는 것을 다른 특징으로 한다.

발명의 효과

[0022] 본 발명은 검증자의 검증 기능에 대한 수정이 필요 없는 다자간 서명을 제공한다는 이점이 있다.

[0023] 또한, 본 발명은 여러 개의 VP가 아닌 단일 VP만으로 다자간 서명이 가능하다는 이점이 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 실시예에 따른 DID 인증 방법의 흐름도를 나타낸다.

도 2는 본 발명의 실시예에 따른 DID 인증 시스템의 블록도를 나타낸다.

도 3은 본 발명의 실시예에 따른 DID 등록단계의 순서도를 나타낸다.

도 4는 본 발명의 실시예에 따른 VC 발급단계의 순서도를 나타낸다.

도 5는 본 발명의 실시예에 따른 다자간 서명단계의 순서도를 나타낸다.

도 6은 본 발명의 실시예에 따른 다자간 서명단계에서 인스턴스키 교환하는 과정을 나타낸다.

도 7은 본 발명의 실시예에 따른 다자간 서명단계에서 제 1 곱셈 공유값을 획득하는 과정을 나타낸다.

도 8은 본 발명의 실시예에 따른 다자간 서명단계에서 제 2 곱셈 공유값을 획득하는 과정을 나타낸다.

도 9는 본 발명의 실시예에 따른 다자간 서명단계에서 제 3 곱셈 공유값을 획득하는 과정을 나타낸다.

도 10 내지 도 13은 본 발명의 실시예에 따른 다자간 서명단계에서 VC에 대한 다자간 서명값을 생성하는 과정을 나타낸다.

도 14는 본 발명의 실시예에 따른 검증단계의 순서도를 나타낸다.

도 15는 본 발명의 실시예에 따른 DID 인증 시스템의 구성도를 나타낸다.

발명을 실시하기 위한 구체적인 내용

- [0026] 이하, 첨부된 도면들에 기재된 내용들을 참조하여 본 발명을 상세히 설명한다. 다만, 본 발명이 예시적 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일 참조부호는 실질적으로 동일한 기능을 수행하는 부재를 나타낸다.
- [0027] 본 발명의 목적 및 효과는 하기의 설명에 의해서 자연스럽게 이해되거나 보다 분명해 질 수 있으며, 하기의 기재만으로 본 발명의 목적 및 효과가 제한되는 것은 아니다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이, 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다.
- [0028] 도 1은 본 발명의 실시예에 따른 DID 인증 방법의 흐름도를 나타낸다. 도 1을 참조하면, DID 인증 방법은 DID 등록단계(S110), VC 발급단계(S130), 다자간 서명단계(S150), VP 제출단계(S170), 및 검증단계(S190)를 포함할 수 있다.
- [0029] 도 2는 본 발명의 실시예에 따른 DID 인증 시스템의 블록도를 나타낸다. 도 2를 참조하면, DID 인증 방법은 임계 서명의 사용자인 Holder들이 공동으로 키생성 과정을 거쳐 DID 문서를 생성하고 이를 블록체인에 등록할 수 있다. DID 인증 방법은 Holder 1(사용자 1)이 Issuer(발급자)에게 자격증명을 요청하면, Issuer는 Holder의 DID를 토대로 VC(Verifiable Credential)를 발행할 수 있다. DID 인증 방법은 Holder가 Verifier(검증자)의 요청을 토대로 VP(Verifiable Presentation)를 생성 및 제출하여 Verifier가 Holder의 DID 문서를 바탕으로 VP를 검증할 수 있다.
- [0030] DID 인증 방법은 기존의 DID 인증 흐름에 임계 서명 기법(Threshold Signature Scheme)을 적용된 것일 수 있다. DID 인증 방법은 임계 서명 기법으로 Threshold ECDSA 서명을 활용하여 기존 블록체인 시스템 도입에 용이할 수 있다.
- [0031] DID 인증 방법은 본인 은행 계좌의 키를 잃어버렸을 경우 추가로 생성되어 있는 키를 사용하여 금융거래를 지속 가능하게 할 수 있다. DID 인증 방법은 의사결정과정에서 각각의 의사결정자가 하나의 키를 소유하게 되면 다수결에 의해 합의된 결정을 실행하게 할 수 있다. DID 인증 방법은 신원 확인 과정에서 혼자서 신원 확인하기 어려운 경우, 키를 갖고 있는 타인이 함께 서명을 진행하여 본인인증을 가능하게 할 수 있다. DID 인증 방법은 다중 서명(Multi Signature)을 직접적으로 지원하지 않는 이더리움에서 다자간 서명이 가능하게 할 수 있다.
- [0032] DID 인증 방법은 DID 인증 메커니즘을 바탕으로 암호 알고리즘 수정만을 통해 설계되어 다자간 서명이 가능한 방법이므로 향후 활용 가치가 높다. DID 인증 방법은 운전면허증, 백신 접종 앱 등과 연계될 수 있으며, 사용자 인증이 필요한 모든 종류의 어플리케이션에 활용될 수 있다.
- [0033] DID 인증 방법은 여러 VP가 아닌 단일 VP만으로 다자간 서명이 가능하다. DID 인증 방법은 하나의 VP에 여러 개의 서명을 추가하여 각 서명에 대해 검증자가 모두 검증하므로 여러 번의 검증이 아닌 한 번의 검증만으로 다자간 서명이 가능하다.
- [0034] 도 3은 본 발명의 실시예에 따른 DID 등록단계(S110)의 순서도를 나타낸다. 도 3을 참조하면, DID 등록단계(S110)는 사용자의 DID 문서(DID document)를 생성하여 블록체인에 등록할 수 있다. DID 등록단계(S110)는 다음과 같이 진행될 수 있다.
- [0035] DID 등록단계(S110)는 각각의 사용자가 공개키쌍을 생성하여, 본인을 제외한 다른 사용자들에게 생성한 공개키를 전달하고, 각각의 사용자는 전달받은 공개키를 바탕으로 공동 공개키를 생성할 수 있다. 즉, DID 등록단계(S110)는 사용자 Holder 1, Holder 2, ..., Holder n이 각각의 공개키쌍(sk_i, pk_i)을 생성할 수 있다. DID 등록단계(S110)는 사용자들이 본인을 제외한 사용자들에게 생성한 공개키를 전달하고, 전달받은 공개키를 바탕으로

사용자들의 공동 공개키 pk 를 생성할 수 있다.

[0036] DID 등록단계(S110)는 각각의 사용자가 로컬 다항식 점($p_i(x)$)을 생성하여 다른 사용자의 인덱스에 맞는 로컬 다항식 점을 전달하고, 각각의 사용자는 전달받은 로컬 다항식 점들을 이용하여 비밀키 역할을 하는 다항식 점($p(x)$)을 구성할 수 있다. 여기에서, $p(x)$ 는 임계 서명 기법상에서 사용자들의 비밀키 역할을 할 수 있다.

DID 등록단계(S110)는 키 생성 과정이 마무리된 후 사용자들이 pk 값을 공개키로 하는 DID Document를 생성하여 블록체인에 등록할 수 있다.

[0037] 도 4는 본 발명의 실시예에 따른 VC 발급단계(S130)의 순서도를 나타낸다. 도 4를 참조하면, VC 발급단계(S130)는 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행할 수 있다. VC 발급단계(S130)는 다음과 같은 절차로 진행될 수 있다. 아래의 설명은 참여자가 2인인 경우로 가정하였으나, 이는 실시예일뿐 참여자의 숫자는 제한되지 않는다.

[0038] VC 발급단계(S130)는 VC를 발행하고자 하는 참여자 1이 발급자에게 VC를 발행해 달라고 요청하면, 발급자는 참여자 1과 참여자 2의 DID 문서를 블록체인으로부터 얻을 수 있다. VC 발급단계(S130)는 블록체인에서 참여자 1과 참여자 2에게 DID 인증을 위한 challenge를 보내게 되면 참여자 1과 참여자 2간의 계산을 통해 response 값을 생성하여 발급자에게 전달할 수 있다. VC 발급단계(S130)는 response 값의 검증 결과가 참이면 발급자가 참여자 1에게 VC를 발행할 수 있다.

[0039] 도 5는 본 발명의 실시예에 따른 다자간 서명단계(S150)의 순서도를 나타낸다. 도 5를 참조하면, 다자간 서명단계(S150)는 검증자의 증명 요청을 받은 사용자와 다른 사용자가 다자간 서명을 수행하여 VC에 대한 다자간 서명 값을 생성할 수 있다. 다자간 서명단계(S150)는 검증자가 요구하는 정보인 proof request를 참여자 1이 받게 되면 참여자 2에게 다자간 서명 절차가 진행된다.

[0040] 다자간 서명단계(S150)는 다자간 서명에 참여한 사용자들이 각각 비밀키에 대한 덧셈 공유값(t_i^0)을 계산하고 인스턴스 키를 교환할 수 있다. 구체적으로, 다자간 서명단계(S150)는 참여자들이 비밀키 $p(x)$ 값과 랑그랑주 계수 $\lambda_{i,j}$ 를 곱하여 비밀키 덧셈 공유값 t_i^0 을 계산할 수 있다. 즉, 참여자 1의 덧셈 공유값(t_1^0)은 $\lambda_{1,1} * p(1)$ 이 되고, 참여자 2의 덧셈 공유값(t_2^0)은 $\lambda_{2,1} * p(2)$ 가 될 수 있다($i=1$ or 2 , $i+j=3$).

[0041] 도 6은 본 발명의 실시예에 따른 다자간 서명단계(S150)에서 인스턴스키를 교환하는 과정을 나타낸다. 도 6을 참조하면, 다자간 서명단계(S150)는 참여자 2가 q 를 위수로 하는 유한체 집합($\{1, 2, \dots, q-1\}$)에서 임의의 정수 값 k_2 를 고를 수 있다. 다자간 서명단계(S150)는 참여자 2가 임의의 정수 값 k_2 에 생성된 G 를 곱하여 D_2 를 구하고 참여자 1에게 전달할 수 있다. 다자간 서명단계(S150)는 참여자 1이 q 를 위수로 하는 유한체 집합에서 임의의 정수 값 k_1' 을 고를 수 있다. 다자간 서명단계(S150)는 참여자 1이 임의의 정수 값 k_1' 을 D_2 와 곱하여 R' 를 구하고 참여자 2에게 전달할 수 있다. 다자간 서명단계(S150)는 참여자 1이 [수학식 1], [수학식 2]을 통해 인스턴스 키 R 을 계산할 수 있고, 참여자 2는 [수학식 3]을 통해 인스턴스 키 R 을 계산할 수 있다. 여기에서, 참여자 1과 참여자 2가 구한 인스턴스키 R 의 값은 같다($\text{Holder1}' s R = \text{Holder2}' s R$).

[0043] [수학식 1]

$$k_1 = H(R') + k_1'$$

[0044]

[0045] [수학식 2]

$$R = k_1 * D_2$$

[0046]

[0047] [수학식 3]

$$R = H(R') * D_2 + R'$$

[0050] 다자간 서명단계(S150)는 다자간 서명에 참여한 사용자 간에 곱셈 연산을 3번 반복하여 제 1 곱셈 공유값, 제 2 곱셈 공유값, 및 제 3 곱셈 공유값을 획득하고, 제 2 곱셈 공유값과 제 3 곱셈 공유값을 더하여 제 4 곱셈 공유값을 계산할 수 있다.

[0051] 도 7은 본 발명의 실시예에 따른 다자간 서명단계(S150)에서 제 1 곱셈 공유값을 획득하는 과정을 나타낸다. 도 7을 참조하면, 다자간 서명단계(S150)는 사용자 1이 q 를 위수로 하는 유한체 집합에서 패드값 Φ 를 고를 수 있다. 다자간 서명단계(S150)는 참여자 1과 참여자 2가 Multiplication protocol(MUL)을 실행하여, 참여자 1은 $\Phi + 1/k_1$ 을, 참여자 2는 $1/k_2$ 를 입력값으로 넣을 수 있다. 다자간 서명단계(S150)는 Multiplication protocol(MUL)의 결과값으로 참여자 1은 t_1^1 을 받고, 참여자 2는 t_2^1 을 받을 수 있다.

[0052] 도 8은 본 발명의 실시예에 따른 다자간 서명단계(S150)에서 제 2 곱셈 공유값을 획득하는 과정을 나타낸다. 도 8을 참조하면, 다자간 서명단계(S150)는 참여자 1과 참여자 2가 Multiplication protocol(MUL)을 실행하여, 참여자 1은 t_1^0/k_1 을, 참여자 2는 $1/k_2$ 를 입력값으로 넣을 수 있다. 다자간 서명단계(S150)는 Multiplication protocol(MUL)의 결과값으로 참여자 1은 t_1^{2a} 을 받고, 참여자 2는 t_2^{2a} 을 받을 수 있다.

[0053] 도 9는 본 발명의 실시예에 따른 다자간 서명단계(S150)에서 제 3 곱셈 공유값을 획득하는 과정을 나타낸다. 도 9를 참조하면, 다자간 서명단계(S150)는 참여자 1과 참여자 2가 Multiplication protocol(MUL)을 실행하여, 참여자 1은 $1/k_1$ 을, 참여자 2는 t_2^0/k_2 를 입력값으로 넣을 수 있다. 다자간 서명단계(S150)는 Multiplication protocol(MUL)의 결과값으로 참여자 1은 t_1^{2b} 을 받고, 참여자 2는 t_2^{2b} 을 받을 수 있다.

[0054] 다자간 서명단계(S150)는 제 2 곱셈 공유값(t_i^{2a})과 제 3 곱셈 공유값(t_i^{2b})을 더하여 제 4 곱셈 공유값(t_i^2)을 계산할 수 있다. 즉, 다자간 서명단계(S150)는 참여자 1이 제 2 곱셈 공유값인 t_1^{2a} 와 제 3 곱셈 공유값인 t_1^{2b} 을 더하여 제 4 곱셈 공유값 t_1^2 을 얻을 수 있고, 참여자 2가 제 2 곱셈 공유값인 t_2^{2a} 와 제 3 곱셈 공유값인 t_2^{2b} 을 더하여 제 4 곱셈 공유값인 t_2^2 를 얻을 수 있다.

[0055] 도 10 내지 도 13은 본 발명의 실시예에 따른 다자간 서명단계(S150)에서 VC에 대한 다자간 서명값(sig)을 생성하는 과정을 나타낸다. 도 10 내지 도 13을 참조하면, 다자간 서명단계(S150)는 검증자의 증명 요청을 받은 사용자가 제 1 일관성 체크값(Γ^1)과, VC를 서명한 제 1 서명값(sig_1)을 포함하여 계산한 제 2 일관성 체크값(Γ^2)을 다른 사용자에게 전달할 수 있다.

[0056] 구체적으로, 다자간 서명단계(S150)는 참여자 1이 제 1 일관성 체크값(Γ^1)을 계산할 수 있다. 다자간 서명단계(S150)는 참여자 1이 제 1 일관성 체크값(Γ^1)을 패드값 Φ 과 함께 암호화 값 η^Φ 을 계산할 수 있다. 다자간 서명단계(S150)는 참여자 1이 암호화 값 η^Φ 을 참여자 2에게 전달할 수 있다.

[0057] 다자간 서명단계(S150)는 참여자 1이 서명할 메시지 m 과 제 1 곱셈 공유값(t_1^1)과 제 4 곱셈 공유값(t_1^2)을 이용하여 제 1 서명값(sig_1)을 생성할 수 있다. 다자간 서명단계(S150)는 참여자 1이 제 1 곱셈 공유값(t_1^1)과 제 4

곱셈 공유값(t_1^2)을 이용하여 제 2 일관성 체크값(I^2)을 계산할 수 있다. 다자간 서명단계(S150)는 제 2 일관성 체크값(I^2)과 제 1 서명값(sig_1)을 이용하여 암호화 값 η^{sig} 을 계산하고 참여자 2에게 전달할 수 있다.

[0058] 다자간 서명단계(S150)는 다른 사용자가 제 1 일관성 체크값(I^1)을 이용하여 제 2 서명값(sig_2)을 생성하고, 제 2 일관성 체크값(I^2)을 이용하여 VC에 대한 다자간 서명값(sig)을 생성할 수 있다.

[0059] 구체적으로, 다자간 서명단계(S150)는 참여자 2가 제 2 일관성 체크값(I^2) 생성을 위해 필요한 변수 θ 을 계산할 수 있다. 다자간 서명단계(S150)는 참여자 2가 제 4 곱셈 공유값(t_2^2)과 변수 θ 를 이용하여 제 2 일관성 체크값(I^2)을 계산할 수 있다. 다자간 서명단계(S150)는 참여자 2가 서명할 메시지 m , 변수 θ , 제 4 곱셈 공유값(t_2^2)을 이용하여 제 2 서명값(sig_2)을 생성할 수 있다. 다자간 서명단계(S150)는 참여자 2가 제 2 서명값(sig_2), 암호화 값 η^{sig} , 제 2 일관성 체크값(I^2)을 이용하여 VC에 대한 다자간 서명값(sig)을 생성할 수 있다.

[0060] 다자간 서명단계(S150)는 다른 사용자가 생성된 VC에 대한 다자간 서명값을 검증자의 증명 요청을 받은 사용자에게 전송할 수 있다. 즉, 다자간 서명단계(S150)는 참여자 2가 VC에 대한 다자간 서명값(sig)을 참여자 1에게 전달할 수 있다.

[0061] VP 제출단계(S170)는 증명 요청을 받은 사용자가 생성된 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출할 수 있다. 즉, VP 제출단계(S170)는 참여자 1이 생성된 다자간 서명값(sig)을 바탕으로 VP를 생성하여 검증자에게 제출할 수 있다.

[0062] 도 14는 본 발명의 실시예에 따른 검증단계(S190)의 순서도를 나타낸다. 도 14를 참조하면, 검증단계(S190)는 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증할 수 있다.

[0063] 검증단계(S190)는 VP에 명시된 증명 요청을 받은 사용자의 DID를 통해 블록체인에서 증명 요청을 받은 사용자의 DID 문서를 조회하여 찾은 공동 공개키로 VP의 다자간 서명값을 검증할 수 있다.

[0064] 검증단계(S190)는 발급자의 DID를 통해 블록체인에서 발급자의 DID 문서를 조회하여 찾은 발급자의 공개키로 VC의 다자간 서명값을 검증할 수 있다. 구체적으로, 검증단계(S190)는 VP 내 VC에 명시되어 있는 발급자의 DID를 바탕으로 발급자의 DID 문서를 조회하여 찾은 발급자의 공개키를 토대로 VC의 서명값이 참인지 검증할 수 있다. 검증단계(S190)는 검증자가 검증 결과를 증명 요청을 받은 사용자에게 전송할 수 있다.

[0065] 도 15는 본 발명의 실시예에 따른 DID 인증 시스템(10)의 구성도를 나타낸다. 도 15를 참조하면, 본 발명의 다른 실시예인 DID 인증 시스템(10)은 DID 등록부(100), VC 발급부(300), 다자간 서명부(500), VP 제출부(700), 및 검증부(900)를 포함할 수 있다.

[0066] DID 등록부(100)는 사용자의 DID 문서(DID document)를 생성하여 블록체인에 등록할 수 있다. DID 등록부(100)는 전술한 DID 등록단계(S110)의 동작을 수행할 수 있다.

[0067] DID 등록부(100)는 각의 사용자가 공개키쌍을 생성하여, 본인을 제외한 다른 사용자들에게 생성한 공개키를 전달하고, 각각의 사용자는 전달받은 공개키를 바탕으로 공동 공개키를 생성할 수 있다. DID 등록부(100)는 각각의 사용자가 로컬 다항식 점($p_i(x)$)을 생성하여 다른 사용자의 인덱스에 맞는 로컬 다항식 점을 전달하고, 각각의 사용자는 전달받은 로컬 다항식 점들을 이용하여 비밀키 역할을 하는 다항식 점($p(x)$)을 구성할 수 있다.

[0068] VC 발급부(300)는 사용자의 요청에 따라 발급자가 VC(Verifiable Credential)를 발행할 수 있다. VC 발급부(300)는 전술한 VC 발급단계(S130)의 동작을 수행할 수 있다.

[0069] 다자간 서명부(500)는 검증자의 증명 요청을 받은 사용자와 다른 사용자가 다자간 서명을 수행하여 VC에 대한 다자간 서명값을 생성할 수 있다. 다자간 서명부(500)는 전술한 다자간 서명단계(S150)의 동작을 수행할 수 있다.

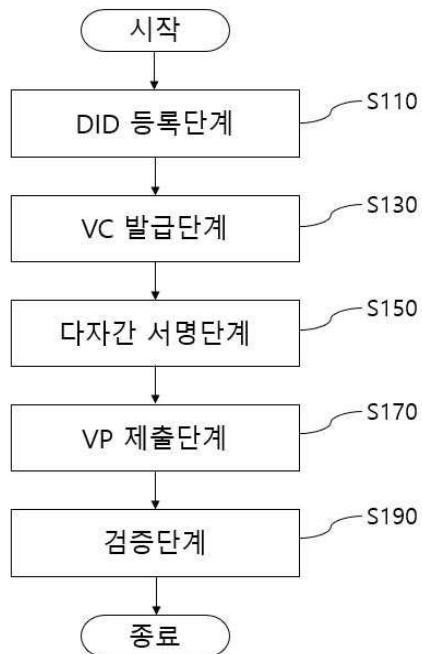
- [0070] 다자간 서명부(500)는 다자간 서명에 참여한 사용자들이 각각 비밀키에 대한 덧셈 공유값을 계산하고 인스턴스 키를 교환할 수 있다. 다자간 서명부(500)는 자간 서명에 참여한 사용자 간에 곱셈 연산을 3번 반복하여 제 1 곱셈 공유값, 제 2 곱셈 공유값, 및 제 3 곱셈 공유값을 획득하고, 상기 제 2 곱셈 공유값과 제 3 곱셈 공유값을 더하여 제 4 곱셈 공유값을 계산할 수 있다.
- [0071] 다자간 서명부(500)는 검증자의 증명 요청을 받은 사용자가 제 1 일관성 체크값과, VC를 서명한 제 1 서명값을 포함하여 계산한 제 2 일관성 체크값을 다른 사용자에게 전달할 수 있다. 다자간 서명부(500)는 다른 사용자가 상기 제 1 일관성 체크값을 이용하여 제 2 서명값을 생성하고, 상기 제 2 일관성 체크값을 이용하여 VC에 대한 다자간 서명값을 생성할 수 있다. 다자간 서명부(500)는 다른 사용자가 생성된 VC에 대한 다자간 서명값을 검증자의 증명 요청을 받은 사용자에게 전송할 수 있다.
- [0072] VP 제출부(700)는 증명 요청을 받은 사용자가 생성된 서명값을 바탕으로 VP(Verifiable Presentation)를 생성하여 검증자에게 제출할 수 있다. VP 제출부(700)는 전술한 VP 제출단계(S170)의 동작을 수행할 수 있다.
- [0073] 검증부(900)는 검증자가 증명 요청을 받은 사용자와 발급자의 서명값이 참인지 검증할 수 있다. 검증부(900)는 전술한 검증단계(S190)의 동작을 수행할 수 있다.
- [0074] 검증부(900)는 VP에 명시된 증명 요청을 받은 사용자의 DID를 통해 블록체인에서 증명 요청을 받은 사용자의 DID 문서를 조회하여 찾은 공동 공개키로 VP의 다자간 서명값을 검증할 수 있다. 검증부(900)는 발급자의 DID를 통해 블록체인에서 발급자의 DID 문서를 조회하여 찾은 발급자의 공개키로 VC의 다자간 서명값을 검증할 수 있다.
- [0075] 이상에서 대표적인 실시예를 통하여 본 발명을 상세하게 설명하였으나, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리 범위는 설명한 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 특허청구범위와 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태에 의하여 정해져야 한다.

부호의 설명

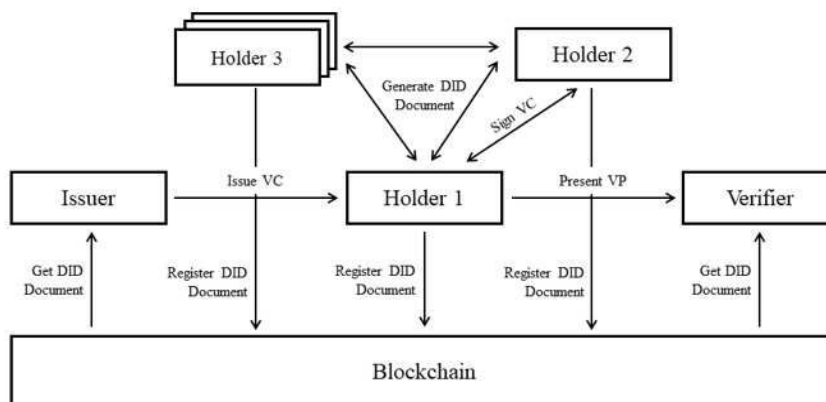
- [0077] 10 : DID 인증 시스템
- 100 : DID 등록부
- 300 : VC 발급부
- 500 : 다자간 서명부
- 700 : VP 제출부
- 900 : 검증부

도면

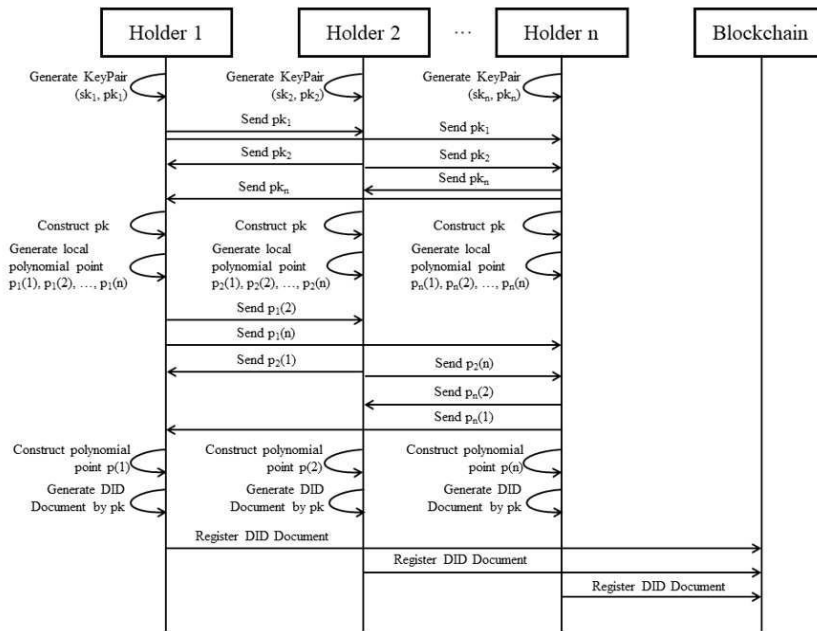
도면1



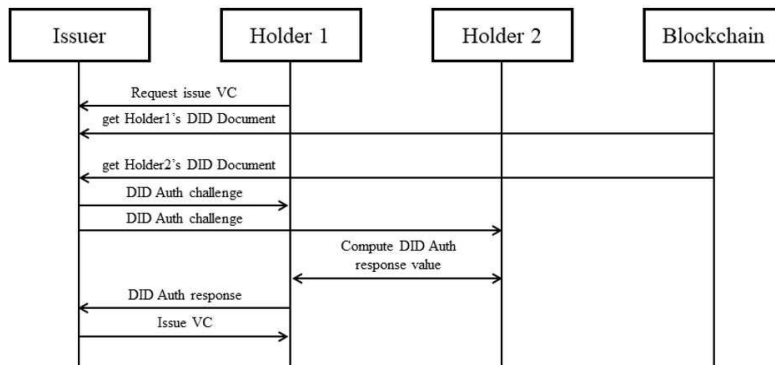
도면2



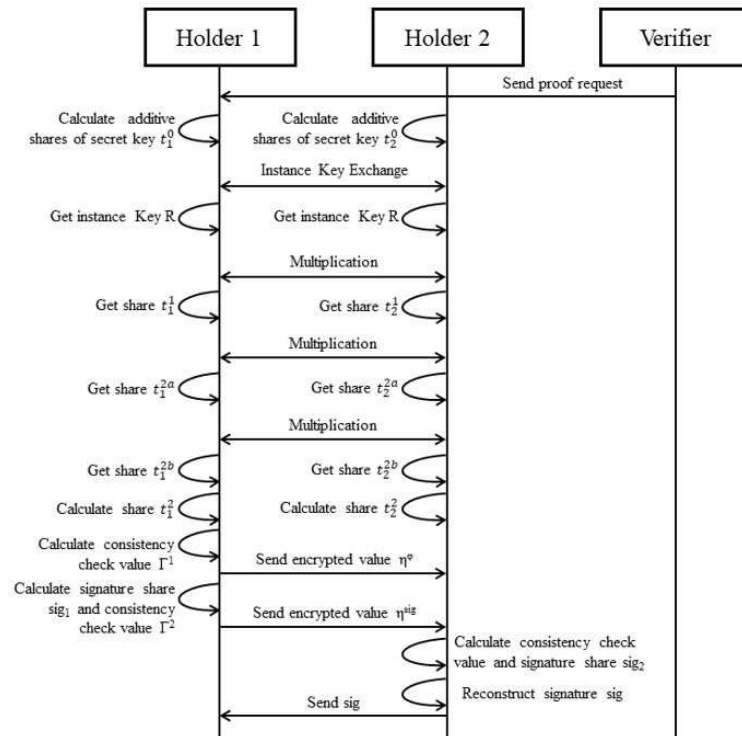
도면3



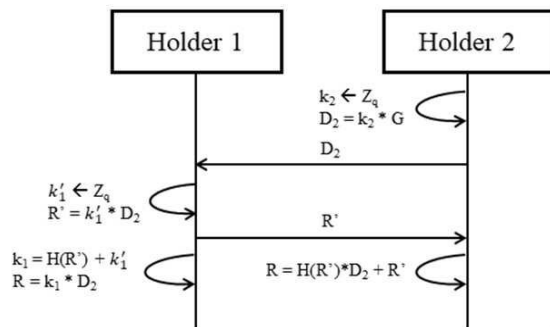
도면4



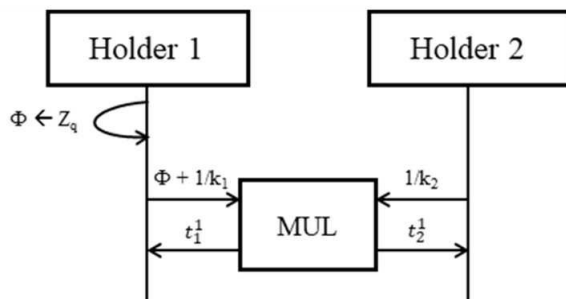
도면5



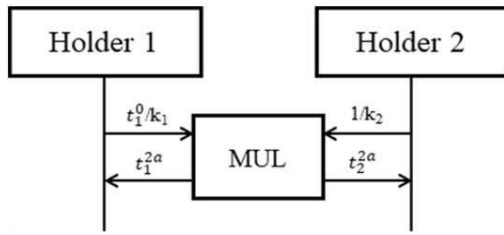
도면6



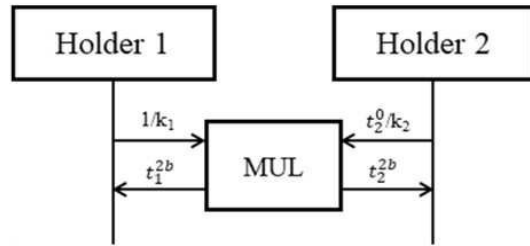
도면7



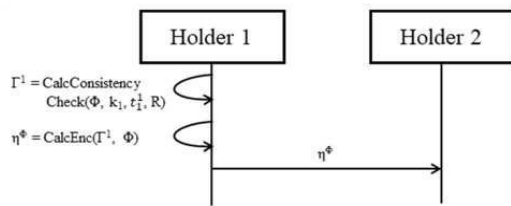
도면8



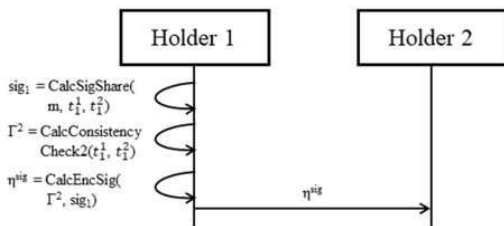
도면9



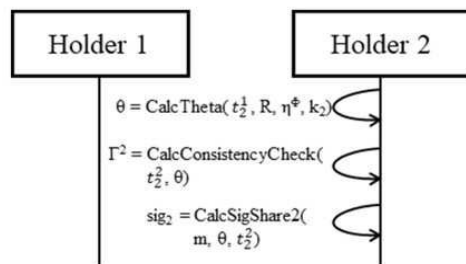
도면10



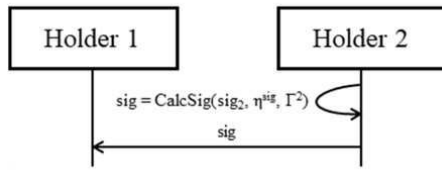
도면11



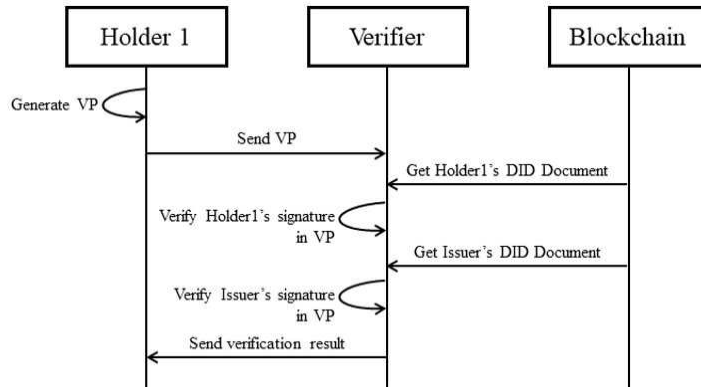
도면12



도면13



도면14



도면15

