동형암호를 이용한 익명 아이디 기반 서명 시스템 및 방법

대표발명자 : 신지선 교수

동형암호를 이용한 익명 아이디 기반 서명 시스템 및 방법

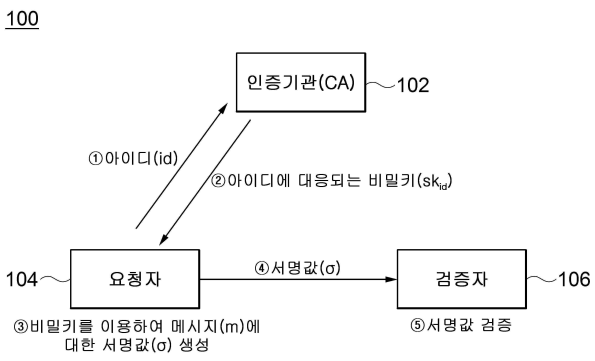
□ 기술개요

○ 본 발명은 사용자의 아이디 정보 및 비밀키 정보를 인증기관 등의 비밀키 생성자로부터 보호할 수 있는 아이디 기반 서명 관련 기술임

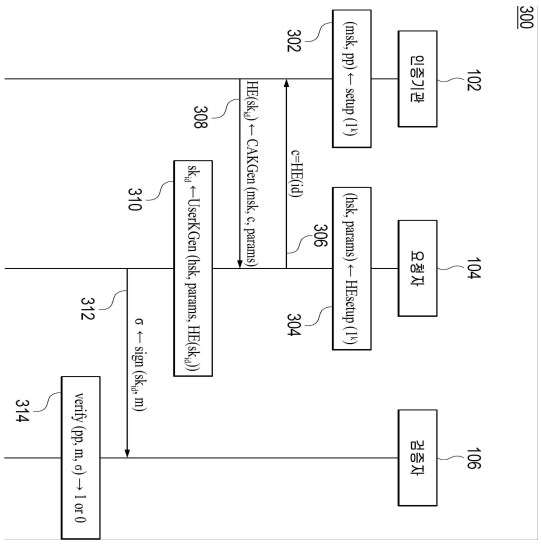
○ 인증 요청자 단말에서, 인증 요청자 단말의 대칭형 동형암호 비밀키(hsk)를 이용하여, 인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성하는 단계, 인증기관 서버에서, 인증 요청자 단말로부터 수신되는 제1 동형 암호문(c)을 이용하여, 아이디(id)에 대응되는 비밀키(sk_{id})에 대한 제2 동형 암호문($C=HE(sk_{id})$)을 생성하는 단계; 및 인증 요청자 단말에서, 제2 동형 암호문(C)을 수신하고, 수신된 제2 동형 암호문(C)으로부터 비밀키(sk_{id})를 획득하는 단계를 포함함.

○ 여기서, 제1 동형 암호문(c)을 생성하는 단계는, 비밀키 생성을 위한 랜덤값(random)을 생성하는 단계 및 대칭형 동형암호 비밀키(hsk)를 이용하여, 생성된 랜덤값(random)에 대응되는 제3 동형 암호문(HE(random))을 생성하는 단계를 포함함.

□ 대표도면



<아이디 기반 서명 시스템>



<아이디 기반 서명 방법을 설명하기 위한 흐름도 >

□ 기술의 특징 및 우수성

○ 본 기술은 인증기관 등의 키 생성자에게 아이디 및 이에 대응되는 비밀키가 노출되는 것을 방지할 수 있어 아이디 기반 서명의 보안성을 한층 높일 수 있음.

[표] 기술의 특징 및 우수성

종래기술 문제점	• 기존의 아이디 기반 서명 기법은 **인증기관에서 각 사용자의 아이디 및 비밀키 정보를 모두 알게됨**. • 그에 따라, 기존의 공개키 방식의 암호 시스템과 비교하여 **비밀 정보가 중앙에 집중되는 문제**가 있음.
해결방안	• 인증 요청자 단말에서 대칭형 동형암호 비밀키(hsk)를 이용하여, 인증 요청자 단말의 아이디(id)에 대응되는 제1 동형 암호문(c=HE(id))을 생성하여 인증기관 서버로 전송하고, 인증기관 서버에서 제1 동형 암호문(c)을 이용하여, 아이디(id)에 대응되는 비밀키(sk_{id})에 대한 제2 동형 암호문(C=HE(sk_{id}))을 생성하여 인증 요청자 단말로 전송하며, 인증 요청자 단말에서 수신된 상기 제2 동형 암호문(C)으로부터 비밀키(sk_{id})를 획득함.
기술의 특징 및 우수성	• 키 발급 과정에서 **사용자의 아이디 및 비밀키가 노출되는 것을 방지**할 수 있어 **보안성을 한층 높일 수 있음**.

□ 기술의 효과

○ 아이디 기반의 서명을 위한 키 발급 과정에서 인증기관 등과 같은 키 생성자에게 사용자의 아이디 및 비밀키가 노출되는 것을 방지하고, 비밀 정보가 중앙에 집중되는 것을 방지할 수 있음.

□ 기술의 완성도(TRL)

기초 연구 단계		실험 단계		시작품 단계		제품화 단계		사업화
기본원리 파악	기본개념 정립	기능 및 개념 검증	연구실환경 테스트	유사환경 테스트	파일럿현장 테스트	상용모델 개발	실제 환경 최종테스트	상용운영
			●					

□ 기술 키워드

한글키워드	아이디 기반, 서명, 동형 암호
영문키워드	identity-based, signature, homomorphic encryption

□ 기술의 적용분야

○ 본 기술은 사용자 인증 분야에 사용될 수 있으며, 특히 아이디 기반의 서명 기술 분야에 사용 가능함

[표] 적용분야

인증 기술	아이디 기반 서명 기술
사용자 인증	비밀키 획득

□ 기술경쟁력

○ 사용자의 아이디 및 비밀키와 같은 비밀 정보가 인증기관에게도 노출되지 않아 보안성이 우수함.

□ 기술실시에 따른 기업에서의 이점

○ 사용자 인증 및 보안 업체에서 사용자들의 비밀 정보를 노출시키지 않은 상태에서 아이디 기반 서명 인증을 수행할 수 있다는 점에서 경쟁력을 어필할 수 있음.

[표] 국내 아이디 기반 서명 기술 분야의 SWOT 분석

강점(Strength)	약점(Weakness)
• 전자상거래 활성화 등으로 인해 보안성 높은 인증 수단 요구 증가 • 인터넷 대중화로 ID 도용 등 사이버 위협 증가에 따라 비밀 정보가 노출되지 않는 인증 수단의 요구 증가	• 벤처 기업 형태의 영세성, 브랜드 인지도, 마케팅 부족으로 경제성 형성의 한계성 • 협소한 내수시장 및 업체 간 과열 경쟁
기회요인(Opportunity)	**위협요인(Threat)**
• 블록체인 기반 전자 서명 서비스의 활성화 • 모바일 전자 증명의 적용 분야가 증가하고 있는 추세	• 미국, 유럽, 일본 등 조기도입에 따른 일부 국가와 기업제품의 독점 우려

□ 특허현황

구분	발명의 명칭	출원번호 (출원일)	등록번호 (등록일)	출원 국가
1	동형암호를 이용한 익명 아이디 기반 서명 시스템 및 방법	10-2018-0138600 (2018.11.13.)	10-2005946 (2019.07.25.)	한국