[기술명] 다변수 이차식 서명 기법을 위한 생체 인식 기반 키 생성 방법

[연구자 명] 서승현 [소속] 공학대학 전자공학부

기술분류

● IT ○ BT ○ NT ○ ET ○ ST ○ CT ○ 기타

키워드

생체인식, 바이오암호 기법, 전자서명, 보안솔루션, 블록체인

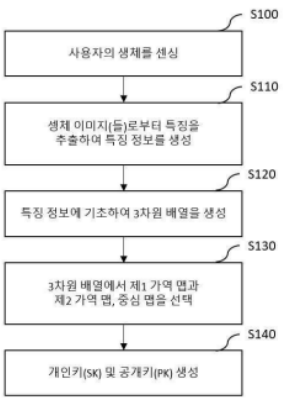
지식재산권 현황

No	발명의 명칭	특허번호	출원인	발명자
1	다변수 이차식 서명 기법을 위한 생체 인식 기반 키 생성 방법	10-2181904	한양대학교 에리카	서승현

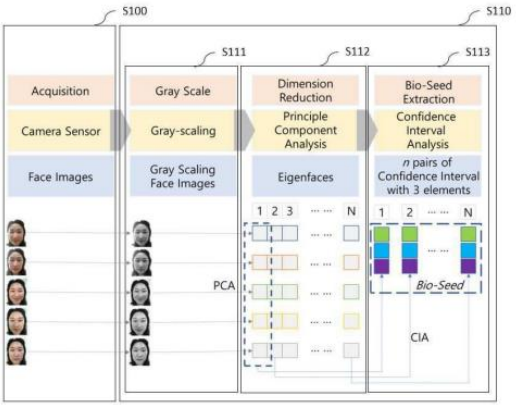
기술 개요

❖ 본 기술은 생체 인식 기반 키 생성 방법에 관한 기술로, 연산이 가볍고 빠른 양자내성 암호의 하나인 다변수 이차식 서명 기법에 관한 기술

❖ 본 기술은 생체 인식을 기반으로 하여 무단 공유 또는 무단 대리에 의한 제3자의 사용과 탈취 등에 대한 무단 사용을 차단할 수 있음



[키 생성 장치의 동작 흐름도]



[키 생성 장치의 특징 정보 생성 프로세스]

기술개발 특성

배경 기술 및 문제점

❖ 제3자의 무단 사용을 방지하기 위한 가장 좋은 대안은 생체정보와 암호 기법의 융합으로 생체 정보로부터 비밀키를 생성하거나 생체 정보와 비밀키를 결합하는 것이라 볼 수 있음

❖ 그러나 해당 방식은 높은 키 엔트로피 및 높은 키 비트열 안정성을 얻기 어려워 실현성 높거나 유의미한 대표적인 연구가 미비한 실정임

기술 내용 및 우수성

❖ 무단 공유 또는 무단 대리에 의한 제3자의 사용과 탈취 등에 의한 무단 사용을 차단할 수 있는 다변수 이차식 서명 기법을 위한 생체 인식 기반 키 생성 방법 제공이 가능함

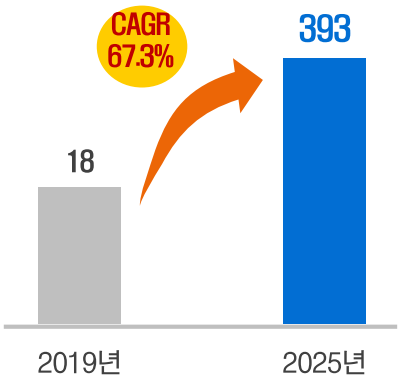
❖ 또한, 연산비용이 적어 모바일 장치 등에 적용 가능하며, 특히 IoT, IoV 등의 환경에서도 적용이 용이한 이점이 있음

시장 동향

❖ 블록체인 세계 시장은 2019년 약 18억 달러에서 2025년 약 393억 달러로 연평균 67.3%씩 성장할 전망

❖ 블록체인 기술이 재조명되고 각국의 주도권 경쟁이 치열하며 초기 시장 장악 중요성 대두, 시장 초기 과열되었던 가상자산에 대한 관심이 잦아들고, 블록체인 기술과 활용 자체의 가능성에 주목하고 있음

(단위: 억 달러)



시장 적용 분야

[블록체인 기반 분석 ID 및 인증 시스템]

기술 완성단계

TRL1 TRL2 TRL3 TRL4 TRL5 TRL6 TRL7 TRL8 TRL9

TRL 5 : 시제품제작/성능평가 단계

기술이전 방법

■ 라이센스 □ 공동연구협력 □ 기타

기술문의

한양대학교 ERICA 산학협력단 기술사업팀
김나라 매니저 031-400-4957