Blockchain Internet Economy Research Center

Blockchain 특강

Mini Theater, Central Library.1st Floor , GIST
Date: August. 27th / Time : 11:00-12:00
Language: Korean / English

Session

Title : 포스트 양자 암호 연구 동향
- NIST PQC 암호 표준화를 중심으로

수업개요 및 목표

: 본 강의는 오늘날 활발히 연구되고 있는 포스트 양자 암호(PQC, post-quantum cryptography)에 대한 최근 연구 동향을 소개한다. PQC의 개념으로부터 시작하여 현재 미국 NIST에서 추진되고 있는 PQC 표준화 과정의 개요 및 표준화 과정에서 관심을 받고 있는 주요 알고리즘들을 소개할 것이다. 또한 각각의 알고리즘에 대한 세부적인 이해를 돕기 위해 대다수의 알고리즘이 기반을 두고 있는 격자 기반 암호와 부호 기반 암호의 원리에 대해 설명할 것이다.

Speaker : 김영식 교수
(현) 조선대학교 정보통신공학부
(전) 삼성전자시스템 LSI사업부 책임연구원

블록체인경제연구센터
Blockchain Economy Research Center