

PQC MIGRATION CHALLENGE

양자내성암호 전환 기술 공모전

2025. 7. 1 TUE - 11. 14 FRI

NIA 한국지능정보사회진흥원



한국정보보호학회
Korea Institute of Information Security & Cryptology





PQC MIGRATION CHALLENGE 양자내성암호 전환 기술 공모전

개요

- 대회 개요** 양자내성암호에 대한 관심을 유도 및 미래 기술을 선도할 ICT 관련 인재 발굴
- 대회 주제**
- PQC 알고리즘 최적화 분야
 - PQC 알고리즘 응용 분야
- 진행 방식**
- 제출물 등록 (온라인 1차)
 - PT발표 (오프라인 2차)

정보

- 접수 방법** PQC 마이그레이션 플랫폼 (<https://pqcmp.kr>)을 통한 온라인 접수
- 접수 기간** 2025. 7. 1(화) ~ 10. 12(일) 1차 접수
- 참가 자격**
- 국내 ICT 관련 대학생, 대학원생
 - 개인 또는 팀(최대 5인) 구성
- 시 상**
- 대상 1팀 (500만원)
 - 최우수상 2팀 (각 300만원)
 - 우수상 2팀 (각 200만원)

※ 본 사업은 개방형 양자 테스트베드 사업의 일환으로 시행됩니다.



PQC 마이그레이션
플랫폼 바로가기



지원 분야

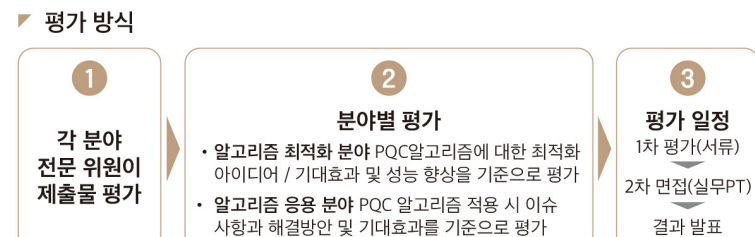
지원분야 1

- ▶ **PQC 알고리즘 최적화 분야**
PQC 알고리즘(NIST PQC, KpqC) 레퍼런스 소스코드를 활용하여 구현 최적화
※ 해당 최적화 결과물은 PQC 마이그레이션 플랫폼에서 제공하는 PQC 통합서비스의 라이브러리를 사용하고, PQC 검증서비스(S/W, 부채널) 검증을 수행하여 안전성 검증을 받아야함.
- ▶ **제출물 포함 내용**
- ① 제출물의 보고서(구현 최적화 방안, 성능 비교 결과, PQC MP 안전성 검증 결과, 등)
 - ② 알고리즘 소스코드

지원분야 2

- ▶ **PQC알고리즘 응용 분야**
PQC알고리즘(NIST PQC, KpqC)을 적용한 응용 S/W 개발
※ PQC 마이그레이션 플랫폼에서 제공하는 라이브러리를 활용하여 응용(암호모듈, 인증서, 프로토콜, 서비스, 등)S/W를 개발해야 함.
- ▶ **제출물 포함 내용**
- ① 제출물의 보고서(PQC 응용 S/W 소개, 응용 S/W에 적용 시 이슈사항 및 해결 방안, PQC MP 라이브러리 사용 여부, 등)
 - ② PQC응용 S/W 소스코드

제출물 평가



※ PQC 공모전을 통한 결과물의 지식재산권 또는 소유권은 참가자와 PQC 마이그레이션 플랫폼이 공동 소유함.
※ 참가자는 해당 결과물을 추후 국내외 학회, 저널, 논문, 프로젝트 등에서 자유롭게 활용 가능함.

문의사항

- ▶ PQC 마이그레이션 플랫폼 질의응답 게시판 또는 이메일(pqc_office@naver.com)으로 문의 부탁드립니다.

