**양자내성암호 전환 기술 공모전 제출 가이드라인**

**1. 공모전 개요**

공모전 명 : PQC Migration Challenge : 양자내성암호 전환 기술 공모전

주최 : NIA 한국지능정보사회진흥원

주관 : LG 유플러스, 크립토랩, 한국정보보호학회

목적 : 양자내성암호에 대한 관심을 유도 및 현대암호로부터 양자내성암호로의 전환에 대한 관심을 촉진시키고 미래 기술을 선도할 ICT 관련 인재 발굴

참가 대상 및 구성 : 국내 ICT 관련 대학생, 대학원생으로 이루어진 개인 또는 팀(최대 5인) 구성

**2. 제공 서비스 및 자료**

PQC 마이그레이션 플랫폼 ( 링크 : [www.pqcmp.kr](http://www.pqcmp.kr) )

PQC 마이그레이션 통합서비스 :

* NIST PQC 및 KpqC 알고리즘이 담긴 통합 API 라이브러리, 경량 라이브러리(임베디드 환경) 제공
* PQC 보안 프로토콜 라이브러리 IPSec/TLS 제공

PQC 마이그레이션 검증서비스 :

* 사용자 라이브러리 S/W 구현 검증 (확장된 Known Answer Test 방식)
* 부채널 취약점 검증 (Constant-time) 및 취약점 리포트, 가이드라인 제공
* 사용자 프로토콜(TLS 라이브러리) 취약점 검증 및 리포트 제공

**3. 공모전 주제 및 제출 방식**

주제 유형 ( 택 1 )

1. 알고리즘 최적화 분야

PQC 알고리즘(NIST PQC, KpqC) 레퍼런스 소스코드(통합서비스 라이브러리)를 활용하여 구현 최적화  
※ 해당 최적화 결과물은 PQC 마이그레이션 플랫폼 PQC 검증서비스(S/W, 부채널) 검증을 수행하여 안전성을 검증 받아야함

예시 :

* FPGA/ASIC 등의 H/W에서 PQC 알고리즘 동작 시의 최적화 방안 도출  
  (속도, 메모리 사용량, 저지연용 등)
* PQC 임베디드 시스템, IoT 디바이스 등의 부채널 공격 관련 분석 및 취약점 분야
* 다중 알고리즘 지원 방법(하이브리드 암호화, PQC + 현대암호) 및 최적화 방안 도출 및 분석
* 인증서 발급 및 키생성 저장,관리 등에서의 H/W, S/W 호환성 고려 사항 및 적용 기법
* 수학적 기법을 활용한 알고리즘 최적화(연산 부하 감소, 등)

제출물 구성 :

* 제출물의 보고서(구현 최적화 방안, 성능 비교 결과, PQC MP 안전성 검증 결과, 등)
* 알고리즘 소스코드

2. 응용 소프트웨어 분야

PQC 알고리즘(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

예시 :

* TLS, IPSec, OpenSSH, WireGuared, 등 통신 기반의 프로토콜 및 블록체인, AI 등의 소프트웨어의 PQC 적용 기법
* 웹(아파치, 등), 클라우드 등의 데이터 암호화시 PQC 적용  
  (하이브리드 암호화 기법 적용 및 호환 여부)
* 기존 통신 프로토콜에 PQC 적용 후 업데이트 등의 사후 개발 사항 최적화 기법  
  (업데이트 유지 보수 용이성)
* 각 물리적 환경에 따른 프로토콜 응용 기법 제안(항공, 우주, 기계, 등)

제출물 구성 :

* 제출물의 보고서 ( PQC 응용 S/W 소개, 응용 S/W에 적용 시 이슈사항 및 해결 방안,   
  PQC MP 라이브러리 사용 여부 등)
* PQC 응용 S/W 소스코드

※ 제출물 가이드라인 (공통 구성)

최적화 성능 테스트는 오픈소스(Valgrind, perf, 등)/측정도구를 이용한 분석 결과물을 첨부한다.

주요한 알고리즘 소스코드에는 주석을 달아 채점 시의 가독성을 높인다.

제출물의 전체 또는 일부에 해당하는 주요 알고리즘(PQC 기능이 포함된 부분)은 PQC 마이그레이션 플랫폼 검증서비스를 이용하여 결과물을 첨부한다(항목 2 참고).

대회 방식

참가 등록 (온라인)

* PQC 마이그레이션 홈페이지 – PQC Migration 공모전 란 - 참가 접수 신청에서 첨부 양식(참가 신청서, 개인 정보 및 저작권 동의서, 서약서, 기타 증빙서류)을 작성하여 등록

제출물 등록 (온라인, 1차 심사 제출물)

* 제출물 등록은 PQC 마이그레이션 홈페이지 – PQC Migration 공모전 란 - 참가 접수/제출물 등록에 제출

PT 발표 진행 (오프라인, 2차 심사 제출물)

* 1차 결과 발표에 따른 2차 제출물(PPT)를 작성하여 PQC 마이그레이션 홈페이지 – PQC Migration 공모전 란 - 참가 접수/제출물의 2차 제출란에 첨부파일로 제출
* 2차 PT 발표 진행

**4. 평가기준**

각 분야 전문 위원이 제출물을 평가하며, PQC 알고리즘에 대한 최적화 아이디어/기대효과 성능 향상[알고리즘 최적화분야] 또는 PQC 알고리즘 적용 시 이슈사항과 해결방안 및 기대효과를 기준으로 평가

점수 배분

* 기술 설명 (10점) : 기존 프로토콜 또는 알고리즘 대비 제출물의 필요성 및 차별성, 기술적 타당성
* 설계 및 적용 방안 (40점) : 알고리즘 설계 과정의 명확성, 상용화 및 실용 가능성
* 실험 및 검증 결과 (40점) : 테스트 데이터 및 실험 환경, 보안성 검증
* 문서 완성도 및 가독성 (10점) : 논리적 구성도, 참고문헌, 그래프 등의 풀이

**5. 일정안내**

참가 접수기간 : 2025년 7월 1일 ~ 25년 9월 12일

결과물 제출 마감 : 25년 9월 12일

1차 제출물 심사 기간 : 25년 9월 15일 ~ 25년 10월 1일

2차 PT발표자료 제출 : 25년 10월 2일 ~ 25년 10월 20일

2차 PT 발표 기간 : 25년 10월 24일

최종 심사 기간 : 25년 10월 27일 ~ 25년 11월 11일

결과 발표 및 시상 : 25년 11월 14일

(※ 일정은 주최측의 일정에 따라 변동될 수 있음.)

**6. 시상 및 상금**

우수한 성적을 얻은 팀에게 상장 및 상금을 수여함.

* 대상 : 1팀, NIA 한국지능정보사회진흥원장 상 – 500 만원
* 최우수상 : 2팀, 한국정보보호학회장 상 – 300 만원
* 우수상 : 2팀, LG유플러스 상 – 200 만원

(※ 상장 수여기관은 주최측의 협의로 변동될 수 있음.)

**7. 유의사항**

제출된 모든 결과물은 반환되지 않으며, 공모전을 통한 결과물의 지적재산권/지식재산권/소유권은 PQC 마이그레이션 플랫폼에 있음.

타인의 저작물을 무단 도용한 경우 수상에서 제외되며, 민형사상의 책임은 참가자에게 있음.

공모전 일정은 주최 측의 사정에 따라 일부 변동될 수 있음.

**8. 문의처**

PQC 마이그레이션 홈페이지 게시판 – 질문 게시판 이용

이메일 : pqc\_office@naver.com