양자내성암호 국가공모전[KpqC 공모전]
제안 요청서(Request For Proposal)

□ KpqC 공모전 개요

양자내성암호연구단(KpqC 연구단, www.kpqc.or.kr)은 교육, 세미나, 연구결과 공유, 연구개발 지원 등을 통하여 국내 양자내성암호 분야의 경쟁력 제고 및 기술 저변 확대를 목표로 활동 중인 산·학·연·관 관련 전문가로 구성된 연구단입니다.

본 연구단에서는 양자컴퓨터에 의한 보안 위협에 선제적으로 대비하기 위하여 '양자내성암호 국가공모전'(이하 'KpqC 공모전')을 통해 양자내성암호 알고리즘을 선정하고자 합니다. 공모전을 통해 선정된 암호알고리즘은 향후 국내 암호모듈 검증제도(KCMVP)의 검증대상 암호알고리즘으로 제안될 예정입니다.

KpqC 공모전에 관심 있는 분들의 많은 참여 부탁드립니다.

[KpqC 공모전 주요 일정(안)]

시기	내용	비고
'22. 2. 18.	'개발 계획서' 접수 마감	
'22. 3. 18.	'개발 계획서' 평가 완료	결과는 개별 통보 예정
'22. 7.	2022 KpqC 1차 워크숍	알고리즘 설계 현황 발표
'22. 10.	'1라운드 제안서' 접수 마감	
- KpqC 공모전 1라운드 -		
'22. 11.	2022 KpqC 2차 워크숍	1라운드 제안 알고리즘 발표
'23. 7./11.	2023 KpqC 1/2차 워크숍	알고리즘 분석/개선 결과 공유
'23. 12.	공모전 1라운드 결과 발표	2라운드 후보 목록 공개
'24. 2.	'2라운드 제안서' 접수 마감	
- KpqC 공모전 2라운드 -		
'24. 3.	2024 KpqC 1차 워크숍	2라운드 제안 알고리즘 발표
'24. 9.	2024 KpqC 2차 워크숍	알고리즘 분석/개선 결과 공유
	KpqC 공모전 최종 결과 발표	알고리즘 ○종 선정 예정

※공모전 제안 알고리즘 대상 구현 경진대회 검토 중

□ KpqC 공모전 참여 방법

KpqC 공모전 참여를 위한 'KpqC 공모전 알고리즘 개발 계획서'(이하 '개발 계획서')를 다음과 같이 접수합니다.

- 제출 기한: 2022년 2월 18일(금) 24시
- 제출 방법: 이메일(kpqcrypto@gmail.com)로 제출
- 제출 요건
  · 개발 책임자 및 공동 개발자 전원 실명으로 참여
  · 개발 책임자는 반드시 대한민국 국적 소지자
  · 개발자의 국내외 저널/학회에 기존 게재/발표된 연구 결과도 제출 가능
  · 복수의 개발 계획서 제출 가능
- 제출물 목록: (붙임) 'KpqC 공모전 알고리즘 개발 계획서' 1부
- 문의: 이메일 kpqcrypto@gmail.com

□ '개발 계획서' 평가 항목

제출된 '개발 계획서'는 다음과 같은 항목을 기준으로 평가됩니다.

- 암호알고리즘의 우수성, 독창성
- 암호알고리즘 기반 문제를 통한 안전성 근거의 타당성
- 개발 목표의 구체성, 실현 가능성 및 개발 계획의 적절성

□ '개발 계획서' 평가 이후의 절차

평가를 통하여 선정된 '개발 계획서'의 개발자는 다음 사항에 참여할 수 있습니다.

- 'KpqC 공모전 1라운드 제안서' 제출
  ※ 제출 기한 내 개발 계획서 미제출 시 KpqC 공모전에 알고리즘 제안 불가
- KpqC 연구단 추진 사업 및 개최 행사