다시 도약하는 대한민국
함께 잘사는 국민의 나라

2025년 양자내성암호 시범전환 지원사업 설명회

2025. 1. 16.

한국인터넷진흥원
차세대암호기술팀

과학기술정보통신부

KISA 한국인터넷진흥원

Contents

Ⅰ 양자내성암호 시범 전환 지원 사업 배경 및 목적

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

1 사업 개요

2 주요 추진 일정

3 지원대상, 참여방법, 지원조건

4 참여기관 수행내용

5 지원 분야 및 지원 내용

Ⅲ 신청 유의 사항 및 주요 질의

Ⅰ. 양자내성암호 시범 전환 지원 사업 배경 및 목적

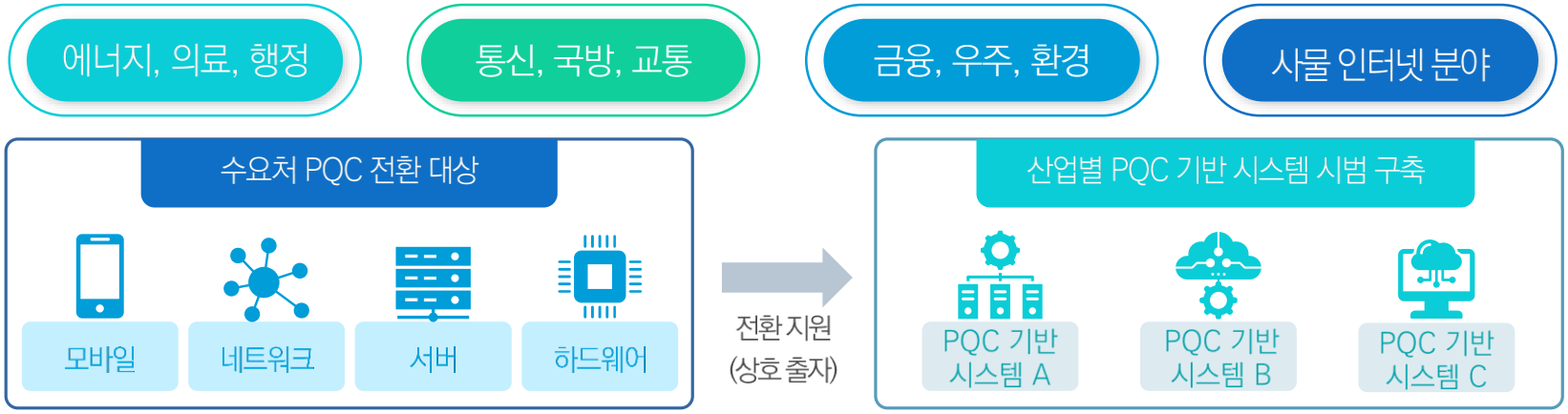
추진 배경

- 양자컴퓨터 출현으로 인한 기존 암호체계의 무력화 우려로 각 산업 분야에서 사용 중인 암호체계를 양자내성암호로 전환 필요

사업 목적

- 암호 체계 시범 전환 사업을 통해 산업 분야별 적용 사례를 확보하고, 전환 경험을 축적한 기업·기관을 중심으로 주변 산업까지 양자내성암호 확산 유도
- 양자내성암호 실환경 적용 후 기술 검증*, 양자내성암호 전환 관련 이슈 파악, 방법론 마련

  * 양자내성암호 알고리즘 성능 비교, 호환성 등



Ⅱ 양자내성암호 시범 전환 지원 사업 내용

01 사업 개요

주요 내용

- 산업 분야별 정보시스템의 양자내성암호 전환을 위해 암호 모듈 기술 및 응용 기술 개발·적용 지원

- 사 업 명 : 2025년 양자내성암호 시범 전환 지원
- 사업 규모 : 1개 과제당 정부지원금 최대 9억원 이내, 최종 3개 과제 선정
- 사업 기간 : 2025년 4월 ~ 2025년 11월
  ※ 상기 일정은 추진 일정에 따라 변동 될 수 있음
- 지원 내용 : 산업 분야*별 정보시스템의 양자내성암호 체계 전환 및 시범 비용 지원
  *** 에너지, 의료, 행정**

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

02 주요 추진 일정

공고 및 접수 (1월 말 ~ 2월 중)	평가 (2월)	사업자 선정 (3월)	사업 추진 (4월 ~ 11월)	사업 완료 (11~12월)
· 사업 공고 · 신청서 접수	· 1차 평가(서류) · 2차 평가(발표)	· 지원금 원가조사 · 협약체결	· 시범 전환 지원	· 사업 결과 평가 · 회계 정산

기업 선정 프로세스

- 1차 평가(서류) : 사업 계획의 타당성, 신청 자격 및 조건 충족 여부 등을 평가하여 **분야별 3배수 이내 과제 선정**
- 2차 평가(발표) : 사업 수행 계획 적정성 등을 평가하여 총 3개 과제 선정**(분야별 1개)**

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

03 지원 대상, 참여 방법, 지원 조건

지원 대상

- 에너지, 의료, 행정 분야 정보시스템의 암호 체계를 양자내성암호체계로 전환하고자 하는 기업·기관 (대기업 참여 제한 없음)

  - 해당 산업 분야의 정보시스템을 보유하지 않은 기업・기관도 사업 참여 가능
    단, 수요기관(사업 대상 시스템 보유)과 협의하여 공동으로 사업 참여 필요

  - 정부 지원금 : 총 27억원

구 분	에너지	의 료	행 정	합 계
정부 지원금 규모	9억원 이내	9억원 이내	9억원 이내	27억원 이내
선정 과제 수	1개	1개	1개	3개
정보시스템 예시	· 스마트 그리드 · 에너지 관리	· 디지털헬스케어 · 의료 행정 · 진료 지원	· G2C · G2B · G2G	-

※ 사업 참여 시 정부지원금 9억원 이상 집행 계획 수립 필수

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

03 지원 대상, 참여 방법, 지원 조건

참여 방법

주관기관은 컨소시엄을 필수 구성하여 참여

구 분	역 할
주관 기관 (필수)	· 전체 사업 관리 · 양자내성암호체계 전환을 위한 개발, 기능· 성능 시험 등 수행
참여 기관	· 주관기관의 업무를 협력 및 수행
수요 기관	· 암호 체계 시범 전환 대상 시스템 소유 및 운영, 전환 시스템 제공

※ 비영리기관(대학, 공공기관, 정부/지자체, 협회 등)도 참여 가능하나, 주관기관으로 참여 불가

※ 수요기관이 주관/참여기관에 포함될 경우, 별도 수요기관은 불필요

컨소시엄에 수요기관이 포함되지 않은 경우?

- 컨소시엄에 수요기관이 포함되지 않는 경우, 주관기관은 반드시 수요처와 별도 협약 체결 후 확약서 제출

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

03 지원 대상, 참여 방법, 지원 조건

지원 조건

- 상호출자방식(매칭펀드)으로 지원하며 과제당 최대 9억 원 이내 정부 지원

[기업 규모 별 예산 지원 사항]

〈대기업〉
정부지원 50%
기업부담 50%

〈중견기업〉
정부지원 70%
기업부담 30%

〈중소기업〉
정부지원 75%
기업부담 25%

- 각 기업 규모별 민간 부담금의 현금 부담 비율은 기업 규모에 따라 부담

[기업 규모 별 민간 부담금의 현금 부담 비율]

〈대기업〉
현금부담비율
15%이상

〈중견기업〉
현금부담비율
13%이상

〈중소기업〉
현금부담비율
10%이상

- 선정된 기관의 제안 금액 대상, 원가산정 등을 통해 적정 규모를 평가 후 최종 지원금 확정
- 사업비는 사업 착수 시 70%를 지급하고, 중간평가 후 30% 지급

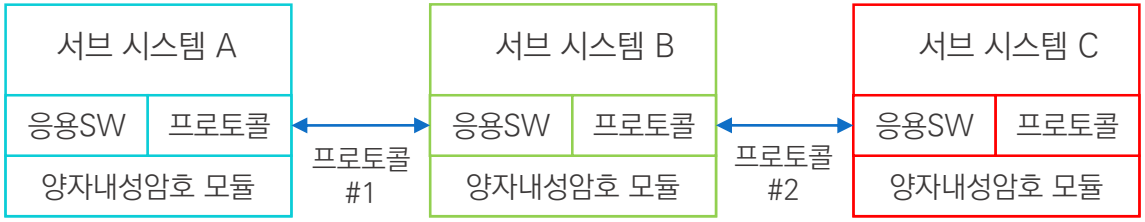
Ⅱ 양자내성암호 시범 전환 지원 사업 내용

04 참여기관 수행 내용

개발 목표 및 사업 대상

- 양자내성암호 모듈, 응용 SW, 프로토콜 라이브러리 등 개발 및 사업 대상 시스템의 암호체계 시범 전환
- 산업 특화 응용 서비스/시스템에 양자내성암호 적용 기술 실증, 전환 방법론(Know-How) 확보

〈 양자내성암호 전환 시스템 목표 예시 〉



사업 대상 정보시스템 기준

- 단순 독립형(Standalone) 시스템이 아닌, 서비스를 구성하는 연계 시스템
- 기존 운영 중인 정보시스템
- 산업 특화 응용 서비스/기능을 포함하는 정보시스템
- 키교환, 전자서명 등 기능을 포함하여 공개키 암호를 사용하는 정보시스템

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

04 참여기관 수행 내용

계획 수립

- 암호체계 전환 계획 수립

대상 시스템의 공개키 사용 현황

- 시범 사업 대상 시스템에서 사용 중인 공개키 암호 종류(RSA 등), 적용 위치 등 분석
  ※ 대상 시스템을 구성하는 서비스 시스템별 사용 중인 공개키 암호 및 프로토콜 분석하여 결과 제시

전환·시험 계획

- 양자내성암호체계로 전환 목표, 범위, 전환 방법 등 계획 제시
  ※ OS, 미들웨어 등에 포함된 암호 체계를 실제 서비스 구동 시 미사용하는 경우 전환 범위에서 제외 가능
- 해당 공개키 암호를 양자내성암호로 전환 시 필요한 데이터 처리 절차 변경, 프로토콜 변경, 장비 변경 등 범위 분석 결과(기본 계획) 제시
- 전환 사업 성공 여부를 결정할 수 있는 기능 검증 기준, 성능 기준 제시

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

04 참여기관 수행 내용

개발사항

- 전환 대상 시스템의 **암호 체계 전환을 위해 필요한** 요소 기술 개발

양자내성암호 모듈

- 대상 시스템의 암호 전환을 위해 필요한 암호 모듈 개발
  ※ 예시 : 양자내성암호 기반 통합인증(SSO), DB암호화, 문서암호화(DRM 등), 가상사설망(VPN), 보안USB 등
- KpqC, NIST PQC 양자내성암호 알고리즘 지원 필요
  ※ 국내 최종 선정 양자내성암호(KpqC), 미국 표준화 양자내성암호(NIST PQC) 필수 지원
- 하이브리드 기능*을 갖추도록 암호 모듈 개발
  * 기존 공개키 및 양자내성암호 설정에 따라 선택할 수 있는 기능 지원

응용 SW·프로토콜 라이브러리 등 필요 기술 개발

- 양자내성암호를 지원하는 보안용 통신 프로토콜* 및 전자서명 필요 기술 개발 및 적용
  * 예시 : IPsec/VPN, SSL/TLS, DTLS, Kerberos, SNMP, HTTPS 등
- 양자내성암호를 지원하도록 기존 응용 SW 수정 및 신규 개발(예 : 설비 원격제어 SW, 헬스케어 SW 등)

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

04 참여기관 수행 내용

시범 전환 및 사업 결과물

- 운영환경 또는 동일 시험 환경을 이중 구성하여 개발 기술의 기능, 호환성, 상호 운용성 검증

시범 전환 및 시험

- 기존 시스템과 호환성 및 상호운용성 확보 전략 수립
- 개발된 시스템에 대한 기능·성능 시험 검증 방안 도출 및 공인시험기관 시험성적서 제출
- 양자내성암호 알고리즘별 성능 비교 분석 결과 제출

- 전환 이슈·방법, 홍보 계획, 활용 계획 등 제출

사업 결과물

- 해당 산업 분야에서 벤치마킹 가능하도록 대상 시스템의 암호 체계 전환 과정에서 발생한 이슈, 방법론을 정리한 결과 제시
- 사업 결과물에 대한 홍보 및 향후 활용 계획 제출

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

05 지원 분야 및 지원 내용

지원 분야

- ① 에너지, ② 의료, ③ 행정 분야 정보 시스템

양자내성암호체계 시범전환 대상 시스템 예시

분 야	정보 시스템 예시	설 명
에너지	스마트 그리드 시스템	전력 에너지 인프라에 대한 모니터링, 원격제어, 데이터 수집 등 관리 시스템
	에너지 관리 시스템	전력 이외(가스, 석유, 신재생 에너지 등) 인프라에 대한 모니터링, 원격제어 등 관리 시스템
의 료	디지털 헬스케어 시스템	원격의료, 모바일 헬스, 보건의료분석, 디지털보건의료 등 IT 기반 건강 관리 시스템
	의료 행정 시스템	환자 관리, 의료 기록 관리, 의료 자원 관리 등 시스템
	진료 지원 시스템	처방 전달, 전자 처방, 의료영상 저장· 통신 등 환자 진료(검사, 수술, 재활 등) 지원 시스템
행 정	G2C 시스템	국민 대상 제공 디지털 행정 시스템(예 : 정부24, 국민신문고, 홈텍스, 건강보험서비스 등)
	G2B 시스템	기업과 정부 간 계약 등 이행을 위한 디지털 시스템(예: 나라장터, 규제정보포털, 수출입통관서비스 등)
	G2G 시스템	정부 기관 간 효율 데이터 공유 및 업무 지원을 위한 디지털 시스템(예: 공공기관 간 DB 연계 서비스 등)

- 지원 분야별 1개 과제(총 3개 과제) 최종 선정 예정(평가결과 70점 이상)

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

05 지원 분야 및 지원 내용

세부 지원 내용

- (예산 지원) 산업 분야 정보시스템의 양자내성암호체계 전환 및 시험 비용 지원

전환 계획 수립	❖ 정보시스템 현황 분석 및 전환 계획 수립 비용(인건비 등)
암호 모듈 개발	❖ 양자내성암호(국내 KpqC, 미국 NIST PQC) 모듈 개발 비용 (인건비, 클라우드 기반 개발 환경 이용료, 장비비 등)
응용 SW 등 개발	❖ 양자내성암호 기반 응용 SW 및 통신 프로토콜 라이브러리 개발 비용 (인건비, 클라우드 기반 개발 환경 이용료, 장비비 등)
시범 전환	❖ 전환 대상 시스템에 암호 모듈, 응용 SW 등 적용 비용(수정· 개발) (인건비, 클라우드 기반 개발 환경 이용료, 장비비 등)
환경 구축· 시험	❖ 양자내성암호 기반 시스템의 시험을 위한 환경 구축 비용 ❖ 공인시험인증기관 시험 평가 비용
보고서 작성 · 회계 감사	❖ 암호체계 전환 이슈· 방법론 등 안내서 제작 비용(인건비 등) ❖ 예산 집행 관련 회계 감사 비용

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

06 사업 신청 안내

신청서 접수 및 문의처

- 모집 공고 : 한국인터넷진흥원 홈페이지 (https://www.kisa.or.kr) 을 입찰공고 게시판에 게시
  - 공고문, 공모 안내서, 신청서 양식 등 확인 가능
- 접수 기간 : 2025년 1월 4주차 ~ 2025년 2월 4주차 16:00 까지
  - 제출 기한 마감일 16:00 이후 접수 절대 불가
  - 마감 시간에 임박하여 접수를 시도할 경우 시스템 사용 미숙에 따른 오류, 등록 집중으로 인한 시스템 장애 등이 발생할 수 있으니 가급적 1~2일 전부터 여유를 갖고 접수 요망
- 제출 방법 : KISA 전자 계약 시스템을 통한 온라인 접수(https://cont.kisa.or.kr)
  - 접수는 온라인으로만 제출 및 접수 가능
  - 주관기관, 참여기관 각각 별도로 회원가입 후 관련 서류 제출
- 지원사업 관련 문의처 : 이메일 접수 (blcok_128@kisa.or.kr)

Ⅱ 양자내성암호 시범 전환 지원 사업 내용

시제품 개발 및 사업화 지원사업 추진 일정

2025년 사업 전체 일정

추진내용	2025년											
	1	2	3	4	5	6	7	8	9	10	11	12
지원사업 공고·접수 및 평가	■	■										
원가산정 및 협약체결		■	■									
사업 지원			■	■	■	■	■	■	■	■	■	
착수 보고				■								
현장실사							■					
중간 평가									■			
최종 평가											■	
사업 정산												■

※ 상기 일정은 추진상황에 따라 변동 가능

신청 유의사항
&
주요 질의

01 신청 시 유의 사항

01 신청시유의사항

공동 수급(컨소시엄) 구성 시 각 사업자별 회원가입 및 접수(필수)

※ 참여기관 제출 자료는 주관 기업 취합없이 전자계약시스템에 직접 제출

※ 주관기관은 전자계약시스템에서 참여 기관을 호출하여 컨소시엄으로 구성

※ 다만 부득이한 경우, 주관기관이 참여 기관의 자료를 취합하여 신청할 수 있으나,
그 경우, 불가피한 사유 등을 포함한 **사유서**를 마감 일시 이전에 이메일(block_128@kisa.or.kr)로 접수

01 신청 시 유의 사항

02 지원 관련 유의사항

- 사업자가 출연한 **자기부담금을 우선 집행** 될 수 있도록 사업계획서에 반영
- 집행계획서 상에 **정부지원금 상한액**(9억원) 을 **모두 계상** (권고)
- 지원 대상 사업자(주관기관)은 회계 감사 비용으로 연구활동비 책정 필요(금액 명시 예정)
- 참여 인력 한 명에 대한 인건비는 정부출연금/자기 부담금 혼합 구성을 자제 해 주시기 바랍니다.
- **민간부담금 현물 미 집행분**에 관하여는 **현금으로 반납** 하셔야 하오니 유의하여 주시기 바랍니다.

지원사업 비용 불인정 사례 예시

연구장비 재료비

- 범용성 장비비
  - 협약 시 명시하지 않은 **범용성 장비**(PC, 프린터, 복사기 등 사무용 기기) 구매비용

연구 활동비

- 범용성 비품 구입비
  - 협약 시 명시하지 않은 **연구와 무관한** USB, 멀티탭 등 **범용성 비품 구입**에 대한 사용액 불인정
- 중복 집행된 식대
  - 컨퍼런스, 교육 참가 시 참가비에 **식대가 포함**되어 있으나, **별도로 식대비를 추가 집행한 경우** 해당 금액 불인정

02 주요 질의 안내

01 주요 질의

Q. 에너지, 의료, 행정 이외 타 산업 분야에 대한 지원 사업 계획은?

- 금년은 상기 3개 분야에 대해 지원사업을 추진하며, 차년도 타 산업에 대해서 추진 계획 중

Q. PQC 알고리즘은 업체 선택인가요?

- PQC 알고리즘은 국내 최종 선정 KpqC (발표 예정) 전부, 미국 NIST PQC 표준 전부(3종)를 개발

Q. 하이브리드 방식은?

- 설정에 따라 기존 공개키(RSA 등) 암호 및 양자내성암호를 전환하여 사용 가능하도록 하는 기능

Q. 전환 대상 범위? 예를 들어 키 교환만 적용인지, 아니면 디지털 서명까지 적용인지?

- 본 사업의 목적은 양자취약암호에 대한 시범 전환으로 RSA 등 기존 알고리즘이 적용된 영역(키교환, 전자서명)이라면 모두 전환 대상 가능

Q. 기술적 지원 방안은?

- 본 사업에서는 예산만 지원하며, 별도 기술 지원은 없음(예산 활용하여 자문 등 시행)

다시 도약하는 대한민국
함께 잘사는 국민의 나라

Q&A

지원사업 관련 문의처 : 이메일 접수(block_128@kisa.or.kr)

과학기술정보통신부

KISA 한국인터넷진흥원

다시 도약하는 대한민국
함께 잘사는 국민의 나라

감사합니다.

과학기술정보통신부

KISA 한국인터넷진흥원