

## 2025년도 암호연구회 위탁 연구과제 공모

한국정보보호학회 산하 암호연구회에서는 암호 이론 및 분석 기술의 관심 제고 및 인력 양성을 위하여 2025년도 위탁 연구과제를 공개 모집하오니 전문가 여러분의 많은 참여를 바랍니다.

### 1. 공모분야: 1년 단기 자유주제 및 지정주제 (5,500만원 내외)

#### ○ 자유주제

암호 이론·분석과 관련된 주제를 자유롭게 정하여 공모에 참여할 수 있습니다.

#### ○ 지정주제 1

주 제	산 출 물
원격 장비관리 통신 프로토콜(TR-069) 분석 ○ 광통신장비·홈게이트웨이등을 관리하기 위해 사용되는 원격 장비관리 통신 프로토콜 (TR-069)의 보안 취약성	○ 분석 보고서(필수) ○ 분석결과 검증용 S/W(필요시)
IoT 장비 안전성 분석 연구 ○ 국내 시장 점유율이 높은 로봇청소기(2종)에 탑재된 펌웨어 및 통신 프로토콜의 보안 취약성을 분석	○ 분석 보고서(필수) ○ 분석결과 검증용 S/W(필요시)
랜섬웨어분석 및 대응기술 연구 II ○ 서비스형 랜섬웨어(RaaS)·AI 결합 랜섬웨어 등 고도화된 랜섬웨어방지 및 사고처리 대응을 위해, 랜섬웨어3종의 동작 프로세스 등 암호체계 분석	○ 분석 보고서(필수) ○ 분석결과 검증용 S/W(필요시)

※ 과제 선정 후, 연구범위 및 산출물은 일부 조정될 수 있음

#### ○ 지정주제 2

구분	주 제	산 출 물
암호분석	CPU/GPU 고속연산에 대한 내성암호 관련 연구	○ 분석 보고서(필수) ○ 분석결과 검증용 S/W(필요시)
	HBOM - MCU/PCB 수준의 위협 분석 등 H/W기반 암호분석 * HBOM: Hardware Bill of Materials	
	공공·민간 PQC 등 암호 관련 Open API 안전성 분석	
블록체인	CBDC 관련 안전성 등 연구 * CBDC: Central Bank Digital Currency	○ 분석 보고서(필수) ○ 분석결과 검증용 S/W(필요시)
	(Block Chain기반/None) 공공·민간 전	

	자지감에 대한 안전성 연구	
AI 융합	AI 활용 패스워드/생체인식특징 추정	o 분석 보고서(필수)
	AI 활용 암호 안전코드 생성, 역난독화 분석, 자동화 등 연구	o 분석결과 검증용 S/W(필요시)

※ 과제 선정 후, 연구범위 및 산출물은 일부 조정될 수 있음

## 2. 신청 자격

- 1인 1과제만 응모 가능
- 해당 분야에 전문 연구개발능력을 보유한 자
- 국내외 연구과제 수행과 관련하여 제재 조치를 받지 않은 자
- 선정된 과제의 책임자와 참여 연구원은 암호 연구회에 가입하여야 함

## 3. 위탁연구기간 및 추정예산

- 위탁연구기간 : 2025년 2월 ~ 2025년 11월 (9개월)
- 예산 : 과제당 55,000,000원 내외(과제 선정 후 예산 재편성)
  - ※ 상기 일정은 암호연구회의 사정에 의하여 변경될 수 있음. 총 9개 내외의 위탁연구과제 선정 예정

## 4. 제안서 접수

- 제출서류(한국정보보호학회(www.kiisc.or.kr) 공지사항 참조)
  - 위탁연구개발제안서 2부(제본 금지, 25페이지 내외) 및 제안서 파일 원본 메일로 제출
  - ※ cryptoresearch.s@gmail.com
  - ※ 제출서류는 일체 반환하지 않음
- 제출방법: 우편제출(우편제출은 마감일 도착분에 한함)
- 제출기한: 2024. 12. 27(금요일) 18:00 까지
- 접수처: 우) 30019 세종특별자치시 세종로 2511 고려대학교세종캠퍼스 과학기술2관 205호 인공지능사이버보안학과 행정실 암호연구회 간사 앞  
(등기우편으로 발송요함)

## 5. 선정방법 및 결과통보

- 암호연구회 운영위원회의 및 발주기관의 심의에 의하며, 기준점수를 통과한 적격자 중 최고점수를 획득한 응모기관(위탁연구책임자) 선정
- 선정평가 시 고려사항

- 연구주제의 적절성 (연구목표, 일정계획, 연구내용, 연구범위 등)
  - 연구수행능력 (연구책임자, 참여연구원, 연구시설 및 장비 등)
  - 연구목표의 달성 가능성 및 연구 방법의 창의성
  - 연구추진전략의 적정성
  - 예상 연구결과의 질적 수준
  - 연구비 편성의 적정성
  - 기타 : 분야 별 별도 선정 기준
- 평가결과 통보 : 선정된 응모기관에 한하여 개별 통보

## 6. 기타사항

- 재위탁은 허용하지 않음
- 연구책임자는 해당과제에 실질적으로 참여하여 수행 및 관리하는 자이어야 함

2024. 11. 22.

한국정보보호학회 암호연구회 위원장 최두호