2024년도 암호연구회 위탁 연구과제 공모

한국정보보호학회 산하 암호연구회에서는 암호 이론 및 분석 기술의 관심 제고 및 인력 양성을 위하여 2024년도 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

과 제 명	산 출 물
국내 상용 인터넷 환경 'RSA-CRT 오류분석 공격' 안전성 분석 연구 o 국내 인터넷 환경에 'RSA-CRT 오류 분석공격'을 적용, 보안취약성 검증 연구 * USENIX '22에서 발표된 [On the passive compromise of TLS keys via transient errors]에 대한 국내 인터넷 환경 안전성 검증 o 同 분석기법을 활용, 인증서 서명키 복원 위험성 및 대응 방안 도출	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)
非표준 VPN 프로토콜 안전성 분석 o 非표준 VPN 프로토콜 3種 (Wireguard, Nordlynx, LightwayProtocol)에 대한 통신체계 · 안전성 분석 o VPN 프로토콜別 주요 특징 도출 및 설계 · 운영상의취약요소 등 안전성평가	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)
랜섬웨어분석 및 대응기술 연구 o 랜섬웨어동작 프로세스 · 파일암호화 방식 등 암호체계 분석 o 랜섬웨어암호체계 분석 공개자료를 조사하고, 암호체계 상세 분석 및 암호 해독을 위한 취약점 분석	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)
국산 AI 반도체를 활용한 암호논리 연산성능 비교 분석 o 국산 AI 반도체 4종(사피온, 리벨리온, 퓨리오사, ETRI)대상으로 제품별 특징과 연산 성능을 비교 분석 * 오픈소스 암호논리를 활용, 제품別 성능을 면밀 분석(전력 효율, 연산시간 등), 장단점 도출	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)
블록체인 보안 취약점 탐지 연구 o 블록체인上 '스마트 컨트렉트'를 악용한 가상자산 탈취 사례를 분석, 취약점 및 해킹 메커니즘 · 대응전략 연구 o '스마트 컨트렉트'의 설계상 오류 · 취약점을도출하고, 同 기술로 인한 화폐 생태계 해킹 위험성 등을 분석	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)

※ 과제 선정 후, 연구범위 및 산출물은 일부 조정될 수 있음

○ **지정주제 2**

과 제 명	산 출 물
악성행위탐지, 공급망 보안, 화이트박스 시험,평가 등 H/W 기반의 암호분석 기술	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)
다자간 연산(MPC), 경량 대칭키암호등 암호 이론 분야	o 분석 보고서(필수) 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

○ 공모분야 Ⅰ: 위탁연구기간 : 2024년 2월 ~ 2024년 11월 (9개월)

○ 예산 : 과제당 55,000,000원 내외(과제 선정 후 예산 재편성)

○ 공모분야 Ⅱ: 위탁연구기간 : 2024년 2월 ~ 2025년 11월 (18개월)

- 1차년도 : 2024년 2월 ~ 2024년 11월 (9개월)
- 2차년도 : 2025년 2월 ~ 2025년 11월 (9개월)

○ 예산 : 과제당 연 55,000,000원 내외(과제 선정 후 예산 재편성)

※ 상기 일정은 암호연구회의 사정에 의하여 변경될 수 있음

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: 2023. 12. 22(금요일) 18:00 까지

○ 접 수 처: 우) 30019 세종특별자치시 세종로 2511 고려대학교세종캠퍼스 과학기술2관 205호 인공지능사이버보안학과 행정실 암호연구회 간사 앞
(**등기우편**으로 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

2023. 11. 16.

한국정보보호학회 산하 암호연구회 회장 최두호