2022년도 암호연구회 위탁 연구과제 공모

한국정보보호학회 산하 암호연구회에서는 암호 이론 및 분석 기술의 관심 제고 및 인력 양성을 위하여 2022년도 위탁 연구과제를 공개 모집하오니 전문가 여러분의 많은 참여를 바랍니다.

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

○ **자유주제**

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

○ **지정주제**

과 제 명	산 출 물
애플 iWork 문서보안 안전성 분석	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)
컴퓨터 비젼을 활용한 문자 입력패턴 시각화/분석기술 연구	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)
웹애플리케이션 보안위협 및 대응기술 연구	o 분석 보고서(필수) o 분석결과 검증용 S/W(필요시)

※ 과제 선정 후, 연구범위 및 산출물은 일부 조정될 수 있음

2. 공모분야 Ⅱ: 2년 장기 지정주제 (연 5,500만원 내외)

○ 지정주제 1

연구주제	가상화 난독화 적용 실행파일 분석연구
내용	• 가상화 난독화가 적용된 실행파일에 대한 분석기법 연구 - 상용 난독화 S/W 대한 가상화 난독화 구조를 분석 후 원본 파일 복원 방안 연구
필요성	• 최근 악성코드는 분석가의 역분석을 방지하기 위한 안티디버깅, 난독화 등 분석 방지기법에 코드 가상화까지 적용되어 악성코드 분석에 장시간 소요 • 특히, 일부 악성코드는 상용 S/W가 아닌 자체 난독화 기법을 적용하여 더욱 분석이 난해함
연구개발 방안	• (1차년도) 상용 가상화 난독화 기술(1種)에 대한 동작구조 분석 및 최신 가상화 역난독화 관련 기술조사 • (2차년도) 가상화 난독화가 적용된 실행파일에 대한 복원도구를 개발하고 다양한 수준(기초수준 예제 → 악성코드)의 시험 예제에 적용하여 도구 평가

※ 과제 선정 후, 연구범위 및 산출물은 일부 조정될 수 있음

○ 지정주제 2

연구주제	화상회의 솔루션 안전성 분석연구
내용	• 상용 화상회의 솔루션의 보안체계 및 취약점 분석 * 화상회의 솔루션: 원격에 위치한 두 개 이상의 시스템에서 동시에 양방향 비디오·오디오를 주고받는 플랫폼
필요성	• 비대면 시대에 온라인 화상회의 솔루션 사용이 급증·지속되면서 보안 문제도 함께 야기 * 줌(화상회의 앱 1위)은 클라이언트-서버 암호화 구조 中 소재 서버 사용으로 보안 이슈가 발생('20) • 다자간 영상 보안 전송에 대한 적합한 암호기술이 필요하나, 현재 체계화된 연구가 없음 * 텍스트 기반의 다자간 그룹 채팅은 IETE의 MLS(Messaging Layer Security) 워킹 그룹에서 표준화 진행중
연구개발 방안	• (1차년도) 상용 화상회의 3種을 분석하여 인증 절차, 암호키 분배/관리, 영상 암호화 등 사용 암호체계 규명 • (2차년도) 안전성 분석을 바탕으로 취약점 발굴 및 화상회의에 적합한 암호체계/프로토콜 제안

3. 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

4. 위탁연구기간 및 추정예산

○ 공모분야 Ⅰ: 위탁연구기간 : 2022년 2월 ~ 2022년 11월 (9개월)

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

○ 공모분야 Ⅱ: 위탁연구기간 : 2022년 2월 ~ 2023년 11월 (22개월)

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

※ 상기 일정은 암호연구회의 사정에 의하여 변경될 수 있음

5. 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: ~~2021. 12. 24(금요일) 18:00 까지~~ 2022. 01. 05(수요일) 18:00까지

○ 접 수 처: 우) 02707 서울특별시 성북구 정릉로 77 국민대학교 과학관 309호
암호연구회 간사 앞 (**등기우편**으로 발송요함)

6. 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

7. 기타사항

○ 재위탁은 허용하지 않음

○ 연구책임자는 해당과제에 실질적으로 참여하여 수행 및 관리하는 자이어야 함

2021. 12. 27.

한국정보보호학회 산하 암호연구회 회장 한동국