

22-6 유럽연 정책동향 보고: Saarland IT 분야 ERC 펀딩

(2022 년 2 월 25 일, 변재선 책임연구원)

I. ERC 펀드: Saarland 캠퍼스 교수 3 인 / 450 만 유로 확보

<https://idw-online.de/de/news786412>

1. 헬름홀츠 사이버보안연구소(CISPA) 양자정보보안 연구

□ ERC 과제: 차세대 라코닉 암호 프로젝트

- Next Generation Laconic Cryptography/LACONIC (PI, 2022-2026)
- 대용량 데이터 교환시 보안을 보장하는 새로운 효율적 암호화 기술 개발 목표
- 의료 데이터 분야 등에서 머신러닝 도입시 안전성을 확보하는 암호 기술로 활용 기대
- 연구비: 150 만 유로/5 년 ERC 펀드

○ 책임자: 니코 되틀링(NICO DÖTTLING) 박사



- KIT 박사, 덴마크 Aarhus/미국 버클리 대학 포닥(DAAD Fellow)
- 에어랑엔-뉘른베르그 대학 주니어 교수
- 2018 년이후 CISPA 테뉴어트릭 교수/
Modern Cryptograph 연구 그룹장
- 양자컴퓨터 위협에 대응, 최소 비용으로 가능한 차세대 양자 보안에 관심
- doettling@cispa.de
- +49 681 302 70783 (CISPA 커뮤니케이션 대표전화)
- <https://sites.google.com/site/nicodoettling/>

○ 연구그룹: Modern Cryptograph

- SIHANG PU 등 연구원 총 4 인 규모 신진연구 그룹
- 상트 잉베르트 캠퍼스: Kaiserstraße 170-174, 66386 St. Ingbert (Germany)

○ 수행 과제:

- German Cybersecurity Agency Project Encrypted Computing Compass (PI, 2022)
- Helmholtz Pilot Project Trusted Federated Data Analytics (Co-PI, 2020-2023)

□ 시사점

- * 현재 CISPA 내 중점 분야는 아니지만 기관 확장기에 양자정보 보안분야가 확대 가능
- * 되틀링 박사의 지도교수 KIT 의 죄른 뮐러 크바되(Jörn Müller-Quade)교수 2018 년 8 월 국보연 관계자와 방문시 한국과 협력 가능성에 긍정적(협력 분야 후보 제안 별첨 1)
- * 현재 진행중인 KAIST 협력 분야를 확대 의료분야 정보보안을 위한 인공지능(기계학습), 차세대 양자암호 등으로 다양한 국내 파트너와 협력 가능성 검토 필요