부대 행사 (11. 14(목) 서울 엘타워)

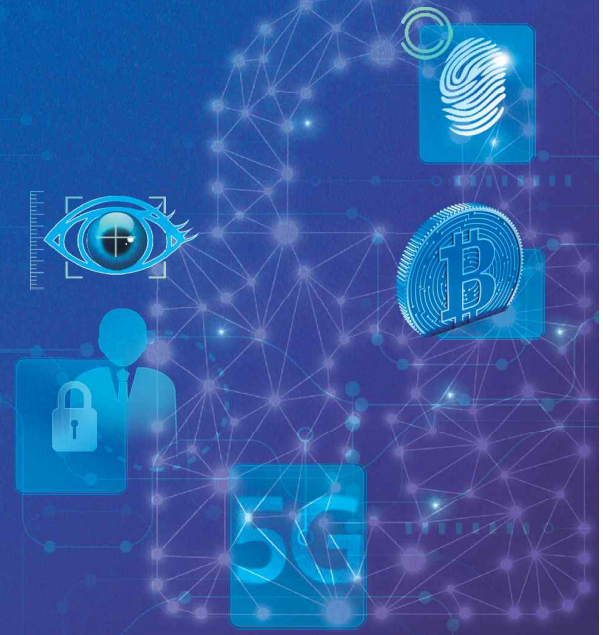
시간	프로그램	비고
10:30~12:00	한국암호포럼 시상식 - 2019 국가암호공모전 시상식 - 대학 암호동아리 시상식 - 국가 암호기술 전문인력 양성과정 시상식	7F 그랜드홀
18:00~20:00	2019 한국암호포럼 정기총회	4F 디오디아

참가 방법

- **등록비** : 무료
- **등록 방법** : **11월 8일(금)**까지 한국암호포럼 홈페이지에서 온라인 등록 바랍니다.
  * 한국암호포럼 홈페이지 : http ://www.kcryptoforum.or.kr
  * 등록 링크 : https ://forms.gle/3ppmiJiCiMiemqj2A
- Tutorial은 **100명** 이내로 신청자 접수를 받습니다.
- **등록 시 초청 연사**에게 질문을 남겨 주시면 선별하여 공개 강연 후에 **경품**을 드립니다.

Future
Crypto
Workshop
2019

한국암호포럼
미래암호워크숍
Future Crypto Workshop 2019



일시 2019년 11월 14일(목)~15일(금)

장소 서울 엘타워(7F 그랜드홀),
서울대학교 상산수리과학관(1F 강당)

주최 한국암호포럼, 한국정보보호학회

후원 국가정보원

프로그램

	시간	프로그램	비고
11.14 (목) 서울 엘타워		워크숍 부대행사	
	10:30~12:00	**한국암호포럼 시상식** - 2019 국가암호공모전 시상식 - 대학 암호동아리 시상식 - 국가 암호기술 전문인력 양성과정 시상식	7F 그랜드홀
		해외석학 초청 강연(동시 통역 지원)	
	13:30~14:00	등록	
	14:00~15:30	**Invited Talk 1:** Why has computer security failed to scale, and what we can do about it? **Paul Kocher**(Cryptographic Research, Inc.)	7F 그랜드홀
	15:30~16:00	휴식(break)	
	16:00~17:30	**Invited Talk 2:** From error-correction coding to cryptography for resisting quantum computer **Marco Baldi**(Marche Polytechnic Univ.)	7F 그랜드홀
		워크숍 부대행사	
	18:00~20:00	2019 한국암호포럼 정기총회	4F 디오디아
11.15 (금) 서울대학교		해외석학 초청 Tutorial	
	08:30~09:00	등록	
	09:00~10:30	**Tutorial 1:** Side channel and other gaps between theory and practice **Paul Kocher**(Cryptographic Research, Inc.)	상산수리 과학관 1F 강당
	10:30~11:00	휴식(break)	
	11:00~12:30	**Tutorial 2:** The challenge of using sparse and structured codes in code-based cryptography **Marco Baldi**(Marche Polytechnic Univ.)	
		암호기술 워크숍	
	14:00~14:50	PQC 기술 동향 및 적용 고려사항 **한대완 실장**(국가보안기술연구소)	상산수리 과학관 1F 강당
	14:50~15:40	신경망 기반 암호기술 **조남수 박사**(한국전자통신연구원)	
	15:40~16:00	휴식(break)	
	16:00~16:50	블록체인과 영지식 증명 **김명선 교수**(수원대)	
	16:50~17:40	5G 시대, 프라이버시 보호와 암호기술 **조지훈 상무**(삼성 SDS)	

석학 강연 1

11. 14(목) 14:00 ~ 15:30, 서울 엘타워 7F 그랜드홀

Why has computer security failed to scale, and what we can do about it?

Paul Kocher

- Cryptography Research, Inc. President, Chief-Scientist
- Cryptographic Protocol, 부채널 분석(Side-Channel Cryptanalysis) 전문가
- IACR(International Association Cryptographic Research) Fellow

석학 강연 2

11. 14(목) 16:00 ~ 17:30, 서울 엘타워 7F 그랜드홀

From error-correction coding to cryptography for resisting quantum computer

Marco Baldi

- Professor, Dept. of Information Engineering, Marche Polytechnic University, Italy
- Code-based Cryptography 전문가
- LEDAcrypt(NIST PQC competition Round 2 candidate) 개발자

Tutorial 1 (11. 15(금) 09:00 ~ 10:30, 서울대학교 상산수리과학관 1층 강당)

- **Speaker** : Dr. Paul Kocher
- **Title** : Side channel and other gaps between theory and practice

Tutorial 2 (11. 15(금) 11:00 ~ 12:30, 서울대학교 상산수리과학관 1층 강당)

- **Speaker** : Prof. Marco Baldi
- **Title** : The challenge of using sparse and structured codes in code-based cryptography