■ (2025년도 상반기) 정보보호 전문가를 위한 암호교육

▷ 기간: 7월 7일(월) ~ 7월 11일(금)
▷ 장소: 온라인 교육
▷ 주최: 한국암호포럼, 한국정보보호학회
▷ 주관: 한국암호포럼

<table>
<tr><td>프로그램 위원장</td><td>서화정 교수 (한성대학교)</td></tr>
<tr><td>프로그램 위원</td><td>최형민 박사 (㈜크립토랩), 박종환 교수 (상명대학교),
김성광 박사 (삼성SDS), 서화정 교수 (한성대학교)</td></tr>
<tr><td>등록 안내</td><td>
○ 교육비
<table>
<tr><th>구 분</th><th>교 육 비</th></tr>
<tr><td>학 생</td><td>30 만원</td></tr>
<tr><td>일 반</td><td>50 만원</td></tr>
</table>
○ 온라인 등록
<table>
<tr><th>구 분</th><th>상 세</th></tr>
<tr><td>사전 등록</td><td>2025년 7월 4일 (금)까지</td></tr>
<tr><td>기타 사항</td><td>1) 교육 증명서 발급
2) 온라인 접속 링크 등록자 개별 공지</td></tr>
<tr><td>등록 방법</td><td>학회홈페이지(https://www.kiisc.or.kr)
→ 학회행사 → 사전등록바로가기</td></tr>
<tr><td>결제 방법</td><td>등록정보 작성 후 결제방법 선택 및 결제</td></tr>
</table>
○ 사전 등록 송금처
<table>
<tr><th>구 분</th><th>상 세</th></tr>
<tr><td>예금주</td><td>한국정보보호학회</td></tr>
<tr><td>계좌번호</td><td>국민은행 754201-04-135596
(예금주: 한국정보보호학회)</td></tr>
<tr><td>안내사항</td><td>1) 사전등록시 등록비는 위의 구좌로
송금하시고, 입금자가 대리일 경우 연락바람
2) 신용카드 결제시 세금계산서 발급 불가
(부가가치세법 시행령 제 57조)</td></tr>
<tr><td>문의처</td><td>한국정보보호학회
- 전화 : 02-564-9333~4 (내선번호 0)
- 전자우편 : kiisc@kiisc.or.kr</td></tr>
</table>
</td></tr>
</table>

■ 교육 일정

날 짜	주제	강 의 제 목	강 사
7월 7일 (월) ~ 7월 11일 (금)	HAETAE & SMAUG-T	1.1 공개키 암호 기초	최형민 박사 (㈜크립토랩)
		1.2 격자 이론과 격자기반 암호	
		1.3 HAETAE: 격자기반 전자서명	
		1.4 SMAUG-T: 격자기반 KEM	
	NTRU+	2.1 NTRU 개요	박종환 교수 (상명대학교)
		2.2 NTRU+ 설계의 문제점	
		2.3 NTRU+ 기법 (1)	
		2.4 NTRU+ 기법 (2)	
	AIMer	3.1 MPC 개요	김성광 박사 (삼성SDS)
		3.2 MPC-in-the-Head 개요	
		3.3 AIMer 개요	
		3.4 Vector semi-commitment (VSC)를 이용한 최적화 개요 (심화)	
	공개키 암호 (RSA, ECC, PQC) 핵심연산 최적화 구현 알고리즘	4.1 암호구현 개요 및 핵심연산	서화정 교수 (한성대학교)
		4.2 현대 공개키 암호 핵심 연산	
		4.3 양자내성암호 핵심 연산	

■ 교육 개요

▷ HAETAE & SMAUG-T

강 사	최형민 박사 (㈜크립토랩)	
약 력	2019년 ~ 2025년	서울대학교 수리과학부 이학박사 (암호학)
	2025년 ~ 현재	㈜크립토랩 박사후연구원 (Cryptography Engineer)
E-mail	hyeongmin.choe@cryptolab.co.kr	

주 제	내 용
1.1 공개키암호 기초	- 공개 키 암호화 방식 (PKE), 전자서명, 키 캡슐화 메커니즘 (KEM) - 공개키암호 안전성 정의 - 기존의 현대암호 및 양자내성암호 소개
1.2 격자 이론과 격자기반 암호	- 격자의 정의와 성질 및 격자기반 난제 - NIST PQC & KpqC Competition - 격자기반 양자내성암호 설계
1.3. HAETAE: 격자 기반 전자서명	- NIST 선정 CRYSTALS-Dilithium, KpqC 선정 HAETAE 알고리즘 소개 - Fiat-Shamir with Aborts 격자기반 전자서명 패러다임 - 공개키 설계 및 랜덤니스 샘플링 방법
1.4. SMAUG-T: 격자기반 KEM	- NIST 선정 CRYSTALS-Kyber, KpqC 선정 SMAUG-T 알고리즘 소개 - MLWE/MLWR 기반의 공개키 암호화 방식 (PKE) - FO 변환과 키 캡슐화 메커니즘 (KEM)

▷ NTRU+

강 사	박종환 교수 (상명대학교)	
약 력	2013년 ~ 2019년	상명대학교 컴퓨터과학과 조교수
	2019년 ~ 2024년	상명대학교 컴퓨터과학과 부교수
	2024년 ~ 현재	상명대학교 컴퓨터과학과 정교수
E-mail	jhpark@smu.ac.kr	

주 제	내 용
2.1 NTRU 개요	- 수학적 Ring에서의 NTRU 문제 - Cyclotomic 삼항식을 이용한 수학적 Ring 설계
2.2 NTRU+ 설계의 문제점	- Correctness error를 처리하는 문제 - SOTP 메시지 인코딩 방법
2.3 NTRU+ 기법 (1)	- $ACWC_2$ 변환방법 - FO 변환에서 재암호화를 제거하는 방법
2.4 NTRU+ 기법 (2)	- 기존 기법과의 성능비교 - Cyclotomic 삼항식에서의 NTT 연산 특징

▷ AIMer

강 사	김성광 박사 (삼성SDS)	
약 력	2022년	한국과학기술원 정보보호대학원 공학박사
	2022년~현재	삼성SDS 연구원
E-mail	sk39.kim@samsung.com	

주 제	내 용
3.1 MPC 개요	- MPC 정의와 모델 - MPC 프로토콜의 종류 - Additive secret sharing의 이해
3.2 MPC-in-the-Head 개요	- MPC-in-the-Head 소개 및 toy example - MPC-in-the-Head 최적화 기법
3.3 AIMer 개요	- AIM2 단방향 함수 소개 - AIMer 전자서명의 장단점 및 안전성, 성능 - AIMer 버전 역사 소개
3.4 Vector semi-commitment (VSC)를 이용한 최적화 개요 (심화)	- Vector (semi-)commitment 소개 - VSC를 MPC-in-the-Head에 적용하는 법 소개 - VSC로 인한 증명 변화 소개

▷ 공개키 암호 (RSA, ECC, PQC) 핵심연산 최적화 구현 알고리즘

강 사	서화정 교수 (한성대학교)	
약 력	2015년 ~ 2015년	싱가포르 난양공대 인턴
	2016년	부산대학교 컴퓨터공학과 공학박사
	2016년 ~ 2017년	싱가포르 과학기술청 연구원
	2017년 ~ 2023년	한성대학교 IT융합공학부 조교수
	2023년 ~ 현재	한성대학교 융합보안학과 부교수
E-mail	hwajeong84@gmail.com	

주 제	내 용
4.1 암호구현 개요 및 핵심 연산	- 암호구현 개요 - 암호구현 고려 사항 - 암호구현 핵심 연산
4.2 현대 공개키 암호 핵심 연산	- 곱셈 연산 최적화 기술 (Karatsuba) - 모듈러 연산 최적화 기술 (Montgomery, Barrett) - CRT 알고리즘
4.3 양자내성암호 핵심 연산	- 격자기반 암호의 핵심 연산 - NTT 알고리즘