류지은 (Jieun Ryu)

J.ryu.jieun@gmail.com Seoul, South Korea

Education

Depart. of Financial Information Security, Kookmin University, Cryptography — Seoul, South Korea
- Cryptography — Feb 2024 – present
- Advisor: Prof. Yongjin Yeom

Depart. of Financial Information Security, Kookmin University, Cryptography — Seoul, South Korea
- A Study of Public-Key Cryptographic Primitive based on Combinatorics — Mar 2022 – Feb 2024

Depart. of Information Security, Cryptography and Mathematics, Kookmin University, Cryptography — Seoul, South Korea, Mar 2018 – Feb 2022

Interests

Post-Quantum Cryptography (PQC)

White-Box Cryptography (WBC)

Random Number Generator (RNG)

Quantum

Publications

[Conference] 외부 가속기를 이용한 Kyber 역캡슐화에 관한 연구
류지은 (First Author), 강주성, 염용진

[Conference] Cascade 프로토콜의 오류정정 확률 분석
원희정, 류지은 (Co-Author), 안진우, 강주성, 염용진

[Conference] 저사양 스마트카드의 PQC 인증 방안에 관한 연구
류지은 (First Author), 김덕상, 강주성, 염용진

[Conference] An Experimental Analysis of Several Variants of CASCADE Protocol for QKD
Heejeung Won, Jieun Ryu (Co-Author), Ju-Sung Kang, Yongjin Yeom

[Conference] 블록암호 LEA의 음함수 기반 화이트박스 구현 기법에 관한 연구
류지은 (First Author), 강주성, 염용진

[Paper] Entropy Harvest and Key Derivation from the Image Sensors in IP Camera
Jieun Ryu (First Author), Gwangjae Kim, Jeongbeen Ko, Dongkeun Kang, Ju-Sung Kang, Yongjin Yeom
doi.org/10.1109/ACCESS.2024.3349704

[Paper] IPCC7: Post-Quantum Encryption Scheme Based on a Perfect Dominating Set in 3-Regular Graph
Jieun Ryu (First Author), Yongbhin Kim, Seungtai Yoon, Ju-Sung Kang, Yongjin Yeom
doi.org/10.1109/ACCESS.2024.3349704

[Conference] 1xN 암호통신프로그램 키 설정 과정의 Kyber 적용 가능성에 관한 연구
원희정, 최찬, 류지은 (Co-Author), 강주성, 염용진

[Paper] End-to-End Post-Quantum Cryptography Encryption Protocol for Video Conferencing System Based on Government Public Key Infrastructure
Yeongjae Park, Hyeondo Yoo, Jieun Ryu (Co-Author), Young-Rak Choi, Ju-Sung Kang, Yongjin Yeom
doi.org/10.3390/asi6040066

[Paper] NTRU를 결합한 하이브리드 세션 보호 프로토콜을 이용한 금융 오픈 API 환경의 거래 세션 안전성 강화
권수진, 김덕상, 박영재, 류지은 (Co-Author), 강주성, 염용진
doi.org/10.13089/JKIISC.2023.33.1.75

[Conference] End-to-End PQC Encryption Protocol for GPKI-Based Video Conferencing Systems
Yeongjae Park, Hyeondo Yoo, Jieun Ryu (Co-Author), Young-Rak Choi, Ju-Sung Kang, Yongjin Yeom

[Conference] 양자내성암호가 적용된 MODBUS 환경 구축에 관한 연구
류지은 (First Author), 김용빈, 강주성, 염용진

[Conference] 병렬 잡음원 기반 난수발생기에 적합한 엔트로피 건전성 시험
류지은 (First Author), 유현도, 강주성, 염용진

[Conference] 복수 그래프의 조합을 통한 그래프 기반 PDF 암호시스템 개선 방법 제안
류지은 (First Author), 강주성, 염용진

[Conference] 그래프 기반 PDF 암호시스템 개선 방법에 관한 연구
류지은 (First Author), 강주성, 염용진

[Patent] 양자 난수 기반 단일 채널 암호화를 이용한 스트리밍 데이터 보호 장치 및 방법
고정빈, 류지은, 염용진, 강주성, 원희정, 강동근, 이성환

[Patent] 양자 난수 기반 이중 채널 암호화를 이용한 스트리밍 데이터 보호 장치 및 방법
고정빈, 류지은, 염용진, 강주성, 강동근, 이성환

[Patent] 10-2025-0013714: 음함수를 이용한 화이트박스 블록암호 장치 및 방법
류지은, 고정빈, 염용진, 김동찬, 강주성

[Patent] 10-2759297: 이미지 센서 기반 난수발생기 헬스 테스트 장치 및 방법
유현도, 류지은, 강주성, 염용진

[Patent] 10-2023-0191332: 모바일 환경에 적합한 EC-KCDSA 전자서명의 화이트박스 암호 구현 장치 및 방법
박영재, 류지은, 김광제, 강주성, 염용진

[Patent] 10-2023-0022413: 모드버스 오류 처리 장치 및 방법
류지은, 박영재, 김용빈, 강주성, 염용진

[Patent] 10-2022-0009241: 일방향 함수를 이용한 암호 운영모드 기반의 화이트박스 암호화 방법 및 장치
류지은, 유현도, 강주성, 염용진

Projects

양자내성암호Kyber를 이용한 스마트카드 인증 기술개발 (25-26) Sept 2025 – Aug 2026
저사양 단말 환경에 PQC 인증 기술을 적용 위한 외부가속기 활용 모델 개발 및 구현
- PQC

암호기술 가이드라인 개발 체계 구성 및 방안 연구 (25)] Apr 2025 – Oct 2025

```
    #summary[암호 기술에 관한 가이드라인 개발 동향 조사 및 국내 현황을 반영한 절차, 방법론,
체계 구성 방안 연구]

    - Policy

    - Guideline

  ],
  [
    May 2025 – Nov 2025

  ],
)

#regular-entry(
  [
    #strong[글로벌 보안시스템 관련 국제 표준 및 주요국 제도 연구 (25)]
```

주요국의 보안시스템 수출입 정책 및 국제 표준 동향 조사 및 국내 현황 분석

- Policy
- Cryptographic module; HW, SW, etc.

일대다(1:N) 구조의 양자암호통신 시스템 구축 (24-25) Sept 2024 – Aug 2025

QKD 기반의 일대다(1:N) 구조의 양자암호통신 시스템 구축을 위한 후처리 기술 개발

- QKD post-processing

양자내성암호 구현 기술 개발 (24)] Apr 2024 – Oct 2024

```
    #summary[PQC 이론 분석 자료화 및 표준 알고리즘 3종 구현물의 기존 암호 모듈 통합 (기업
과제)]

    - PQC

    - Cryptographic module

  ],
  [
    Apr 2024 – Dec 2024

  ],
)

#regular-entry(
  [
    #strong[양자내성암호 전환 및 확산방안 연구 (24)]
```

미국 NCCoE의 PQC 전환 프로젝트 현황 분석을 기반으로 국내 양자내성암호의 전환을 위한 절차 및 방법 연구

- PQC
- Policy

화이트박스 암호 설계/구현 기술 공동연구 (24)] May 2023 – Nov 2023

```
    #summary[음함수 기반 화이트박스 전자서명 구현 기술 개발 (기업 과제)]

    - WBC

  ],
  [
    Mar 2024 – Dec 2024

  ],
)

#regular-entry(
  [
    #strong[KpqC 알고리즘 적용 및 확산 방안 연구 (23)
```

NIST 및 주요국의 PQC 표준화와 전환 정책 시행 현황 분석에 기반한 국내 KpqC 알고리즘의 저변 확대 기반 조성 연구

- PQC
- Policy

화이트박스 암호 설계/분석 기술 공동연구 (23-24) Mar 2023 – Feb 2024

음함수 기반 화이트박스 블록암호 구현 기술 분석 및 개발 (기업 과제)

- WBC

양자기술 기반 보안문제 차단 IP카메라 개발 (22-26) July 2022 – Jan 2026

IP카메라 내 은닉채널 존재 가능성을 원천 차단한 이미지센서 기반 QRNG 활용 암호 체계 구축

- RNG

양자내성암호 활용을 위한 전환 정책 및 절차에 관한 연구 (22)] Mar 2022 – present
4 years

```
    #summary[암호전환정책 분석 및 하이브리드 방식 적용 방안 분석을 통한 신규 암호 알고리즘
산업계 지원 방향 연구]

    - PQC

    - Policy

  ],
  [
    Apr 2022 – Oct 2022

  ],
)

#regular-entry(
  [
    #strong[국가·공공 정보시스템 안전성 및 활용성 제고를 위한 차세대 암호체계 개발 (22-24)]

    #summary[국가·공공 정보시스템 고도화를 위한 암호 알고리즘, 암호모듈 개발 및 차세대 암
호 인증 기술 개발 연구]

    - QKD

    - WBC

  ],
  [
    Mar 2022 – Dec 2024

  ],
)

#regular-entry(
  [
    #strong[양자컴퓨팅 환경에 대비한 분산자원 플랫폼 관리용 암호 기술 연구 (21-24)]

    #summary[BEMS 등의 분산자원 플랫폼 관리를 위한 QKD-PQC 기반 보안 인프라 개발 연구]

    - PQC

    - QKD

    - Modbus protocol

  ],
  [
    Sept 2021 – Feb 2024

  ],
)

== Experience

#regular-entry(
  [
    #strong[\[Certification Test\] 양자기술 기반 보안문제 차단 IP 카메라 V1.0]

  ],
  [
    Nov 2025

  ],
)
```

[Club] 학술 동아리 RB
대표(21.06-22.02)

Jan 2021 – Feb 2022
1 year 2 months

[Club] 연합 동아리 CCC
교내 회계(19.06-20.06), 교내 대표(20.07-21.06)

Mar 2018 – Feb 2022
4 years