류지은 (Jieun Ryu)

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

Education

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

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

[Paper] Entropy Harvest and Key Derivation from the Image Sensors in IP Camera

With the widespread use of connected surveillance systems using IP cameras, the security of video data has become a critical issue. In response to the potential compromise of sensitive information via covert channels, the United States and the United Kingdom warned against the use of suspicious cameras in critical infrastructure. To mitigate the security concerns, it is indispensable to investigate every component inside IP cameras using evaluation and validation programs such as Common Criteria and Cryptographic Module Validation Program. However, such compliance tests on implementation under test cannot suffice to prevent the products from malicious attacks using a Trojan-horse in a black-box component, particularly inserted in the image-sensing module or the random number generator (RNG).In this paper, we categorize potential vulnerabilities and argue that IP cameras should disclose the components of the modules to mitigate the threats of backdoor. Based on this, we provide a way to construct backdoor-free RNG. To remove the possibility of the backdoor inside the RNG, we extract randomness from optical black pixels of the image sensor and apply two entropy accumulation methods to guarantee the min-entropy of accumulated data under weak assumptions, which means the IP camera already has a hardware entropy source in itself without additional suspicious entropy source. In the experiment using an IP camera with a Cortex-A53 processor, we can harvest entropy at the rate of 7.3kbps. The operating speed of the RNG is sufficient to provide random bits without delay when a symmetric key is updated every minute.

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

Post-quantum cryptography (PQC) has been actively explored to meet the requirements arising with the rapid development of quantum computers. The National Institute of Standards and Technology (NIST) conducted a competition to establish the next-generation cryptographic standards. While previous competitions selected a single cryptographic standard, this competition aimed to standardize several algorithms based on various mathematical problems since the security of PQC has not been studied as extensively as that of legacy cryptosystems. The recent exclusion of the isogeny-based key-establishment algorithm, SIKE, from the competition emphasizes the necessity of exploring cryptographic algorithms based on various fundamental problems. In this study, we propose the Improved Perfect Code Cryptosystem 7 (IPCC7), a new post-quantum encryption scheme, as an improved version of the perfect code cryptosystem (PCC) based on combinatorics conceptualized by Koblitz. The security of our cryptosystem relies on the intractability of finding the perfect dominating set in a given graph. A PCC proposed previously by Koblitz did not receive much attention because of its low efficiency for handling higher-order polynomials. To overcome these drawbacks, we used the product of low-degree polynomials and demonstrated the feasibility of a graph-based encryption scheme. IPCC7 has some limitations for use as a general-purpose PQC. However, considering its relatively small key size (768 bytes public-key and 64 bytes secret key), fast decryption speed (2.0 Gbps), and usable encryption speed (8.6Mbps), IPCC7 is particularly suitable for environments with low-memory constraints, such as white-box encryptions.

Jieun Ryu (First Author), Yongbhin Kim, Seungtai Yoon, Ju-Sung Kang, Yongjin Yeom

doi.org/10.1109/ACCESS.2024.3349704

[Paper] End-to-End Post-Quantum Cryptography Encryption Protocol for Video Conferencing System Based on Government Public Key Infrastructure

Owing to the expansion of non-face-to-face activities, security issues in video conferencing systems are becoming more critical. In this paper, we focus on the end-to-end encryption (E2EE) function among the security services of video conferencing systems. First, the E2EE-related protocols of Zoom and Secure Frame (SFrame), which are representative video conferencing systems, are thoroughly investigated, and the two systems are compared and analyzed from the overall viewpoint. Next, the E2EE protocol in a Government Public Key Infrastructure (GPKI)-based video conferencing system, in which the user authentication mechanism is fundamentally different from those used in commercial sector systems such as Zoom and SFrame, is considered. In particular, among E2EE-related protocols, we propose a detailed mechanism in which the post-quantum cryptography (PQC) key encapsulation mechanism (KEM) is applied to the user key exchange process. Since the session key is not disclosed to the central server, even in futuristic quantum computers, the proposed mechanism, which includes the PQC KEM, still satisfies the E2EE security requirements in the quantum environment. Moreover, our GPKI-based mechanism induces the effect of enhancing the security level of the next-generation video conferencing systems up to a quantum-safe level.

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
현재 금융거래 서비스에서 보편적으로 사용하는 RSA와 ECC 같은 공개키 암호 알고리즘은 양자 컴퓨터가 실현되면 더 이상 안전성을 보장할 수 없으므로 기존 레거시 알고리즘을 양자내성암호로 전환해야 한다. 하지만 다양한 서비스에 사용 중인 알고리즘을 교체하는 데에는 상당한 시간이 소요될 것으로 예상된다. 다가올 전환기를 대비하기 위하여 두 알고리즘을 결합하는 하이브리드 방식에 관한 연구가 필요하다. 본 논문에서는 레거시 알고리즘인 ECDH 알고리즘과 양자내성암호 알고리즘인 NTRU 알고리즘을 결합하여 세션키를 생성하는 하이브리드 세션키교환 프로토콜을 제안한다. TLS 1.3 기반 하이브리드 키 교환을 위해 IETF에서 제안한 방식들을 적용해본 결과 기존 금융거래 세션 보호 솔루션에 우리가 제안한 프로토콜을 사용하면 안전성을 강화할 수 있을 것으로 기대된다.
권수진, 김덕상, 박영재, 류지은 (Co-Author), 강주성, 염용진
doi.org/10.13089/JKIISC.2023.33.1.75

[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

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

[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
본 발명은 양자 난수 기반 단일 채널 암호화를 이용한 스트리밍 데이터 보호 장치에 관한 것으로, 상기 장치는 양자 난수 기반의 세션 키를 생성하는 세션 키 생성부; 상기 세션 키를 기초로 프레임의 식별코드가 부여된 스트리밍 데이터를 암호화하여 암호문을 생성하는 스트리밍 데이터 암호화부; 상기 프레임의 식별코드와 사전에 상호 공유된 공유 키를 기초로 상기 세션 키를 암호화하는 세션 키 암호화부; 및 상기 암호화된 세션 키와 상기 암호문을 기초로 상기 프레임을 생성하고 상기 프레임을 단일 채널을 통해 전송하는 스트리밍 데이터 전송부를 포함한다.
고정빈, 류지은, 염용진, 강주성, 원희정, 강동근, 이성환

[Patent] 양자 난수 기반 이중 채널 암호화를 이용한 스트리밍 데이터 보호 장치 및 방법
본 발명은 양자 난수 기반 이중 채널 암호화를 이용한 스트리밍 데이터 보호 장치에 관한 것으로, 상기 장치는 양자 난수 기반의 세션 키를 생성하는 세션 키 생성부; 상기 세션 키를 사전에 상호 공유된 마스터 키로 암호화하는 세션 키 암호화부; 상기 암호화된 세션 키를 제1 채널을 통해 전송하는 세션 키 전송부; 상기 세션 키를 입력받아 스트리밍 데이터를 암호화하는 스트리밍 데이터 암호화부; 및 상기 암호화된 스트리밍 데이터를 제2 채널을 통해 전송하는 스트리밍 데이터 전송부를 포함한다.
고정빈, 류지은, 염용진, 강주성, 강동근, 이성환

[Patent] 10-2025-0013714: 음함수를 이용한 화이트박스 블록암호 장치 및 방법
본 발명은 음함수를 이용한 화이트박스 블록암호 장치에 관한 것으로, 상기 장치는 평문을 입력받는 평문 입력부; 상기 암호문을 출력하는 암호문 출력부; 및 상기 평문을 최초의 입력 데이터로 입력하고 상기 암호문을 최종의 출력 데이터로 생성하는 음함수 기반의 라운드 구조를 포함하고, 상기 라운드 구조는 직렬로 연결된 복수의 라운드 함수들로 구성되며 각각은 암호키를 통한 화이트박스를 생성하고 상기 화이트박스를 통한 암호화를 진행함으로써 상기 최초의 입력 데이터를 상기 최종의 출력 데이터로 변환하는 화이트박스 암호화부를 포함한다.
류지은, 고정빈, 염용진, 김동찬, 강주성

[Patent] 10-2023-0191332: 모바일 환경에 적합한 EC-KCDSA 전자서명의 화이트박스 암호 구현 장치 및 방법
본 발명은 모바일 환경에 적합한 EC-KCDSA 전자서명의 화이트박스 암호 구현 장치 및 방법에 관한 것으로, 상기 장치는 반복되는 라운드 동안 인코딩된 입력을 수신하여 사전 저장된 음함수(Implicit) 방정식을 기초로 인코딩된 출력을 생성하는 제1 라운드 연산부; 상기 반복되는 라운드의 마지막 라운드에서 적어도 하나의 중간값을 마스킹하여 상기 인코딩된 출력을 생성하는 제2 라운드 연산부; 및 상기 인코딩된 출력의 인코딩을 해제한 결과로서 획득된 마스킹된 중간값을 이용하여 서명을 생성하는 서명 생성부;를 포함한다.
박영재, 류지은, 김광제, 강주성, 염용진

[Patent] 10-2023-0022413: 모드버스 오류 처리 장치 및 방법
본 발명은 모드버스 오류 처리 장치 및 방법에 관한 것으로, 상기 장치는 모드버스 통신 환경의 서버와 클라이트 사이에 TLS(Transport Layer Security) 통신 환경을 추가하여 모드버스 패킷에 대한 암호화 통신을 수행하는 TLS 통신 제공부; 상기 TLS 통신 과정에서 사전 지정된 오류 목록을 기초로 상기 모드버스 패킷에 대해 오류를 감지하는 오류 감지부; 및 상기 오류의 감지 횟수가 설정된 임계값을 초과하면 제어 서버에 오류 메시지를 송신하고 상기 제어 서버로부터 제어 메시지를 수신하여 수신한 제어 메시지에 따라 해당 오류의 조치를 수행하는 오류 조치부를 포함한다.
류지은, 박영재, 김용빈, 강주성, 염용진

[Patent] 10-2022-0009241: 일방향 함수를 이용한 암호 운영모드 기반의 화이트박스 암호화 방법 및 장치
본 발명은 암호키를 보호하고 필요한 기능만을 제공하여 안전성을 강화하기 위해 화이트박스 암호화 기술에 확률론적 일방향성을 갖는 출력 인코딩을 추가한 블록암호 운영모드에 관한 것으로, 블록 암호의 출력을 인코딩 과정에 공개키만을 사용하기 때문에 대응되는 비밀키 없이는 복호화 기능을 수행할 수 없도록 할 수 있다. 이를 통해, 호환성을 고려하여 취약한 표준 암호화이트박스 기술로 불가피하게 암호화하는 경우에도 일방향성(즉, 암호화만 가능하고 복호화는 할 수 없음)을 유지할 수 있다.
류지은, 유현도, 강주성, 염용진

[Patent] 10-2759297: 이미지 센서 기반 난수발생기 헬스 테스트 장치 및 방법
본 발명은 이미지 센서 기반 난수발생기 헬스 테스트 장치 및 방법에 관한 것으로, 상기 장치는 이미지 센서로부터 수집된 픽셀별 데이터를 디지털화(digitization) 하여 난수 생성을 위한 픽셀 단위의 잡음원을 생성하는 잡음원 수집부; 상기 잡음원에 대한 헬스 테스트를 수행하여 난수 생성 과정에서의 사용 가능성을 결정하는 헬스 테스트부; 및 상기 헬스 테스트를 통과한 잡음원만을 이용한 난수 생성 과정을 통해 난수를 반복적으로 생성하는 난수 생성부;를 포함한다. 따라서, 본 발명은 이미지 센서를 잡음원으로 사용하는 난수발생기의 엔트로피 소스를 검정하여 난수발생기가 정상적으로 동작하고 있는지 확인하는 기능을 제공할 수 있다.
유현도, 류지은, 강주성, 염용진

Projects

양자내성암호Kyber를 이용한 스마트카드 인증 기술개발 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 Mar 2023 – Dec 2024
암호 기술에 관한 가이드라인 개발 동향 조사 및 국내 현황을 반영한 절차, 방법론, 체계 구성 방안 연구
- Policy
- Guideline

글로벌 보안시스템 관련 국제 표준 및 주요국 제도 연구 Mar 2023 – Dec 2024
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 Sept 2024 – Aug 2025
QKD 기반의 일대다(1:N) 구조의 양자암호통신 시스템 구축을 위한 후처리 기술 개발
- QKD post-processing

양자내성암호 구현 기술 개발 (기업 과제) Apr 2024 – Dec 2024
PQC 이론 분석 자료화 및 표준 알고리즘 3종 구현물의 기존 암호 모듈 통합
- PQC
- Cryptographic module

양자내성암호 전환 및 확산방안 연구 Apr 2024 – Oct 2024
미국 NCCoE의 PQC 전환 프로젝트 현황 분석을 기반으로 국내 양자내성암호의 전환을 위한 절차 및 방법 연구
- PQC
- Policy

화이트박스 암호 설계/구현 기술 공동연구 (기업 과제) Mar 2024 – Dec 2024
음함수 기반 화이트박스 전자서명 구현 기술 개발
- WBC

KpqC 알고리즘 적용 및 확산 방안 연구 May 2023 – Nov 2023
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 (기업 과제) Mar 2023 – Feb 2024
음함수 기반 화이트박스 블록암호 구현 기술 분석 및 개발
- WBC

양자기술 기반 보안문제 차단 IP카메라 개발 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 Apr 2022 – Oct 2022
암호전환정책 분석 및 하이브리드 방식 적용 방안 분석을 통한 신규 암호 알고리즘 산업계 지원 방향 연구
- PQC
- Policy

국가·공공 정보시스템 안전성 및 활용성 제고를 위한 차세대 암호체계 개발 Mar 2022 – Dec 2024
국가 · 공공 정보시스템 고도화를 위한 암호 알고리즘, 암호모듈 개발 및 차세대 암호 인증 기술 개발 연구
- QKD
- WBC

양자컴퓨팅 환경에 대비한 분산자원 플랫폼 관리용 암호 기술 연구 Sept 2021 – Feb 2024
BEMS 등의 분산자원 플랫폼 관리를 위한 QKD-PQC 기반 보안 인프라 개발 연구
- PQC
- QKD
- Modbus protocol

Work Experience

[Certification Test] 양자기술 기반 보안문제 차단 IP 카메라 V1.0 Nov 2025

[Certification Test] 이미지 센서 기반 난수발생기 건전성 평가 함수 Nov 2023

[Certification Test] KMU-CHAM-DRBG 난수발생기 Nov 2021

[Class] 2024년 국가 암호기술 전문인력 양성과정 (10기) May 2024 – Sept 2024

[Class] MS-20483: .NET Framework Programming with Visual C# .NET Oct 2023 – Oct 2023

[SW Registration] C-2023-058431: 카이버(KYBER)가 적용된 모드버스(Modbus) 패킷 중계용 티엘에스(TLS) Dec 2023

[SW Registration] C-2023-058432: 의사난수발생기(DRBG)에 경량 블록 암호 참(CHAM)을 사용하는 카이버(KYBER) Dec 2023

[SW Registration] C-2022-053510: NTRU가 적용된 Modbus-TLS 통신 Dec 2022

[Conference] MILCOM 2025 Oct 2025 – Oct 2025

[Conference] ICMC 2025 Apr 2025 – Apr 2025

[Conference] Crypto 2024 Aug 2024 – Aug 2024

[Conference] IEEE INFOCOM 2023 May 2023 – May 2023

Other Experience

[Rab] 난수성분석및안전성평가연구실

[Club] 학술 동아리 RB

[Club] 연합 동아리 CCC