정 보 보 호 학 회 지
제 33 권 제2호, 2023. 4

양자암호통신과 양자난수발생기 최신 동향

권 혁 동*, 심 민 주*, 송 경 주*, 이 민 우**, 서 화 정***

요 약

양자는 물리학에서 더 이상 나눌 수 없는 물리량의 최소 단위이다. 양자에는 일반적인 물리법칙이 적용되지 않는 대신, 양자역학이라는 법칙이 적용된다. 이를 활용한 알고리즘으로 양자암호통신과 양자난수발생기가 존재한다. 양자암호통신은 기존 암호통신과는 다른 차원의 보안성을 제공하는 통신기술이다. 이는 양자를 관측하면 양자상태가 붕괴된다는 특징을 활용하여 도청자를 손쉽게 발견할 수 있게 한다. 양자난수발생기는 의사난수를 대체할 수 있는 알고리즘으로, 가장 완벽한 난수 장치로 여겨진다. 의사난수는 결정론적 알고리즘이기 때문에 값을 예측할 수 있는 반면, 양자난수는 자연 현상에서 뽑아내는 난수이기 때문에 예측할 수 없다. 다만 수학적 연산을 통해 계산하는 의사난수와는 다르게 양자난수는 난수를 추출할 장치가 필요하다. 본 고에서는 양자암호통신과 양자난수발생기의 최신 동향에 대해 확인해 보도록 한다.

Ⅰ. 서 론

양자컴퓨터를 필두로하여 양자역학을 컴퓨터 공학에 적용하고자 하는 사례가 늘어나고 있다. 양자는 일반적인 물리법칙이 아닌 양자역학이라는 법칙이 적용된다. 이를 활용한 기술로는 양자암호통신과 양자난수발생기가 있다. 양자암호통신은 기존 암호통신과는 다른 차원의 보안성을 제공하고자 제안된 차세대 보안 통신 기법이다. 양자암호통신을 통해 양자키를 분배하며 이는 현존하는 통신시스템과 접목되어 안전성을 보장하게 된다. 양자난수발생기는 결정론적 알고리즘인 의사난수의 한계를 넘어 완전한 난수를 발생시키는 기법이다.

본 기고에서는 양자암호통신과 양자난수발생기의 동향에 대해서 확인하도록 한다. 본 기고의 구성은 다음과 같다. 2장에서 양자암호통신에 대한 개요와 최신 연구 동향에 대해서 알아본다. 3장에서는 양자난수발생기의 기본적인 개념과 개발 근황에 대해서 확인한다. 4장에서 본 기고의 결론을 맺는다.

Ⅱ. 양자암호통신

양자암호통신은 양자역학의 원리에 기초하여 통신 시 절대적인 안전성이 보장되는 기술이다[1]. 양자통신 시 양자상태에 담겨있는 정보는 0 혹은 1의 이진 정보이며, 중첩되어있을 수도 있고, 그렇지 않을 수도 있다. 이때 전송되는 이진 정보를 누군가가 도청하게 되면, 양자 상태가 소멸되어 수신자가 즉각 도청자의 존재를 인식할 수 있다. 양자암호는 이러한 특성을 암호키 전송에 응용한 것이다.

일반적인 양자 암호 통신의 구조는 양자키 분배 장비(QKD, Quantum Key Distribution), 키 관리 시스템(KMS, Key Management System), 암호화 장비로 구성된다. QKD는 송신자 및 수신자로 구분되며, 공개 채널과 양자 채널로 연결되어있다. 키 분배 프로토콜로는 양자암호통신의 대표적인 프로토콜인 BB84를 사용한다.

BB84는 비밀키를 나누기 위한 매개체로 단일 광자를 사용하는 프로토콜이다. 양자상태는 복제될 수 없기 때문에 공격자가 정보를 성공적으로 도청하기 위해선 단일광자를 측정하고 수신자에게 다시 측정한 정보

본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 50%) 그리고 본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천기술 연구, 50%).

* 한성대학교 정보컴퓨터공학과 (대학원생, korlethean@gmail.com, minjoos9797@gmail.com, thdrudwn98@gmail.com)
** 한성대학교 IT융합공학부 (대학원생, minunejip@gmail.com)
*** 한성대학교 융합보안학과 (부교수, hwajeong84@gmail.com)

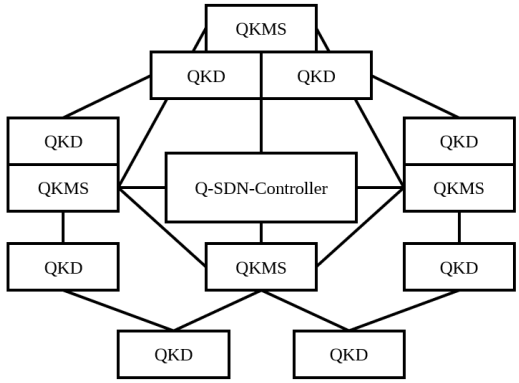
를 보내야한다. 하지만 공격자가 단일광자를 완벽하게 같은 상태로 만들어서 보낼 수는 없기 때문에 송신자와 수신자는 후처리 과정에서 공격여부를 감지할 수 있다. BB84는 공개채널과 양자채널의 두 가지 채널을 사용한다. 양자채널은 비밀키가 될 수 있는 키 정보를 전송하는 채널이고, 공개채널은 양자채널을 이용하여 나눈 정보를 비밀키가 될 수 있도록 조정하는 채널이다[2].

QKD의 키 생성 절차는 raw키 생성, 걸러진 키 생성, 그리고 비밀키 생성 단계로 나눌 수 있다. KMS는 QKD 장비와 암호화 장비를 중개해주는 역할을 하며, QKD로부터 전송받은 키 스트림을 재가공 후 암호화 장비에게 전달하는 역할을 한다. 암호화 장비는 하드웨어 또는 소프트웨어가 될 수 있으며, KMS로부터 키를 수신한 뒤에 암호화를 수행하는 장비를 의미한다. 암호화 장비와 KMS 간 인터페이스에 대한 표준으로는 ETSI GS QKD 014가 있다[3].

2.1. Quantum Software Defined Network Controller(Q-SDN-Controller)

2023년 한국 과학 기술 정보 연구원(Korea Institute of Science and Technology Information, KISTI)은 국가 과학기술연구망(Korea Research Environment Open Network, KREONET) 양자암호통신 구축을 위한 양자키관리 시스템 및 Q-SDN-Controller 기능을 제안했다[4]. KREONET은 연구데이터를 전송하기 위한 연구망으로, 전국적으로 17개의 지역망을 중심으로 한 네트워크에 연결되어있다. 해당 프로젝트에서는 국가 과학기술연구망에 양자암호통신을 적용하기 위해 Q-SDN-Controller와 양자 키 관리 시스템(Quantum Key Management System, QKMS)을 구축하여 연동하고, 양자암호 통신망 관리를 위한 Q-SDN-Controller의 GUI 프로그램을 제안하였다.

SDN(Software Defined Network)은 하드웨어와 소프트웨어의 기능을 분리한 기술로 API와 애플리케이션을 이용해 네트워크를 프로그래밍 할 수 있는 기술이다. 네트워크 장비는 데이터가 흐르는 경로를 설정하고 관리하는 제어 평면과 데이터의 전달을 담당하는 데이터 평면으로 구성된다. 장비의 설정을 변경하거나 경로를 유지 관리할 때 각 장비의 제어평면을 개별적으로 관리해야하기에 작업 절차의 복잡성이 높고, 중앙 관리와 운영의 자동화가 어렵다. SDN은 이런 어려움의 해결을 위해 개별 장비로부터 제어평면을 분리해 소프트웨어로 중앙 집중화하고, 네트워크의 동작을 프로그램을 통해 효율적으로 제어와 관리를 할 수 있다.



〔그림 1〕 양자암호통신망 구성

해당 프로젝트에서 제안한 양자암호 통신망 시스템은 [그림 1]과 같은 구조를 지니며, Q-SDN-controller를 중심으로 한 중앙집중형 양자암호통신망이다. QKMS는 노드 당 한 대로 구성되며, 해당 노드를 구성하는 QKD 및 링크 상태를 수신받을 수 있고 양자키 전달 경로 등을 설정 및 관리한다. 해당 정보를 양자 키관리 시스템에서 Q-SDN-Controller로 전송하여 양자암호통신망 관리를 가능하게 한다. 그리고 이를 GUI 시스템을 통해 구현하여 Q-SDN-Controller의 정보들을 관리자가 쉽게 조회 및 제어하며 네트워크 토폴로지를 쉽게 관리할 수 있음을 보였다.

2.2. Quantum Key pooling in multi-domain QKD optical networks (QKD-ON)

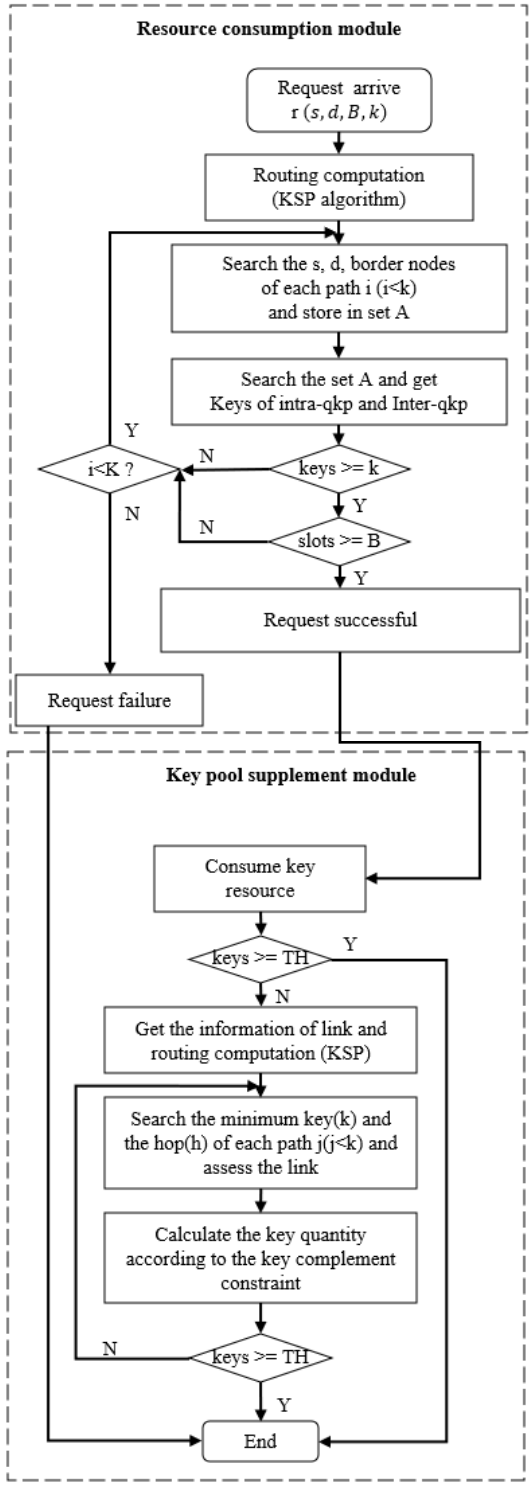
2021년 Wang은 multi-domain QKD Optical Networks(QKD-ON)에서의 양자키 구축 및 분배 방식을 제안했다[5]. 해당 논문에서는 Multi-domain QKD-ON에서 키 자원과 라우팅 홉의 균형을 기반으로 multi-domain QKP 방식을 구현하였으며 주요 작업인 QKP의 키 자원과 라우팅 홉의 균형을 기반으로 한 CASS(Capacity Adaptive Supplement Scheme)은 서비스 차단 확률을 줄인 결과를 보였다. 제안하는 키 자원과 라우팅 홉의 균형 기반의 CASS는 [그림 2]와 같다.

다중 도메인 QKD 네트워크에서 서비스 요청이 지

속적으로 발생 시 주요 리소스가 빠르게 소모되며 생성된 키 자원이 연결된 링크 사이의 키 풀을 제공하므로 도메인간의 키 풀 구성은 매우 중요하다. 즉, 생성된 자원을 합리적으로 사용하는 방식이 서비스에 큰 영향을 미친다. 제안 방식으로 실험한 결과, CASS 알고리즘의 요소가 적절히 설정되면 네트워크 자원 할당이 최적화 된다는 것을 시험으로 확인하였으며 적절한 후보 경로 및 주요 경로가 QKD 광 네트워크의 차단 확률을 줄인 결과를 보였다.

2.3. $2\times N$ PnP(plug-and-play) TF-QKD

2022년 한국 과학 기술 연구원 (Korea Institute of Science and Technology, KIST)은 양자암호 상용화 핵심 기술인 $2\times N$ PnP TF-QKD(Plug-and-Play Twin-Field Quantum Key Distribution)을 제안했다 [6]. 2018년 제안된 기존 TF-QKD는 시스템 통신 거리를 늘릴 수 있어 장거리 통신에 적합하지만 개발이 어려워 상용화 및 연구가 더뎠다. 이에 대해 TF-QKD를 변형하여 PnP 구조, NPP(No Phase Post-selection)- TF-QKD 및 SNS(Sending or Not-Sending) -TF-QKD 들이 연구되었으며 이러한 방식의 TF-QKD 들은 428~511km 통신이 가능하여 장거리 QKD에 대한 해결책으로 기대되고 있다. 이에 대해 KIST에서 제안한 Sagnac-based PnP 구조의 $2\times N$ PnP TF-QKD는 자동 mode-matching 기능을 통해 효율적으로 일관성을 유지하는 네트워크 방식이며 자세한 구조는 [6]의 <Fig. 1>에서 확인할 수 있다. $2\times N$ 네트워크 구현을 위해 세 가지 다중화 방식인 PDM-WDM-TDM(Polarization, Wavelength, and Time Division Multiplexing)을 사용하여 $2\times N$ 네트워크를 구성하며, PDM의 사용은 WDM 만을 사용할 때보다 서버 및 클라이언트 채널 용량을 두 배로 늘렸다. 제안한 PnP QKD 구조는 양자 신호에서 광원 하나로 송/수신을 동작하며, 이러한 방식은 동일 양자 신호가 통신 채널을 오가기 때문에 편광으로 인한 노이즈를 방지할 수 있다. 해당 방식은 단방향 TF-QKD 네트워크 방식과 비교할 때, 적은 수의 active controller로 구성되며 50km 광섬유에 대한 실험을 성공하여 평균 비밀 키 속도를 펄스 당 1.31×10^{-4}bit (초당 1.52bit)을 달성했다.



〔그림 2〕 Multi-domain QKD-ON에서의 리소스 소비 및 키 보완 흐름도[5]

Ⅲ. 양자 난수 생성기

현대 암호와 보안 분야에서는 난수가 차지하는 비중은 매우 높다. 특히 난수는 암호 분야에서 중요하게 여겨지는데, 이는 대부분의 암호 알고리즘이 내부에 난수 발생기를 활용하여 킷값을 생성하고 있기 때문이다. 즉 난수가 불안정할 경우, 암호 알고리즘에 치명적인 보안 취약점으로 발생할 수 있다[7]. 하지만 일반적으로 활용되고 있는 결정론적 난수발생기에는 다음과 같은 문제가 존재한다. 첫 번째는 완전한 난수를 수학적 계산으로 생성하는 것은 불가능하다는 점이다. 현재 사용 중인 결정론적 난수발생기는 난수를 흉내 낸 의사난수라는 점이다. 즉 난수 값이 입력 값에 의존하게 된다 [8].

의사난수는 난수를 모방한 개념이기 때문에, 진짜 난수 값을 생성하고자 하는 노력은 계속되어 왔다. 의사난수가 아닌 진짜 난수는 주로 자연계에서 발생하는 엔트로피를 추출하여 사용함으로써 예측이 불가능하다. 그 중에서 양자난수는 의사난수를 탈피하고자 연구되고 있는 분야로써 양자역학의 원리에 내포된 불확실성을 가져오는 역할을 한다. 양자난수는 여러 동작 원리가 있으며 대표적으로 광자를 사용한 방법이 있다 [9]. 이는 빛이 입자와 파동의 성질을 동시에 가지는 것을 활용한 것으로, 광자의 검출 확률과 도착 시간을 기반으로 난수를 생성한다.

3.1. QRANGE 프로젝트

여러 국외 기업 Quside, ID Quantique 등이 참여하는 QRANGE(Quantum Random Number Generators) 프로젝트는 Quantum Flagship 프로그램의 일환으로, 2018년 European Commission이 수여한 310만 유로 규모의 프로젝트이다. 기존 상업적으로 사용되고 있는 QRNG보다 빠르고 저렴하며 안전한 QRNG를 개발하는 것을 목표로 한다[10]. 표준 CMOS (Complementary metal oxide semiconductor) 기술을 기반으로 제작되는 IoT를 위한 QRNG의 가격은 1유로로 매우 저렴하다. QRANGE의 QRNG는 최대 10Gb/s의 bit rates를 특징으로 하는 임의의 random phase relationship을 갖는 레이저 펄스의 간섭을 기반으로 하는 고속 위상 확산 방식을 사용한다.

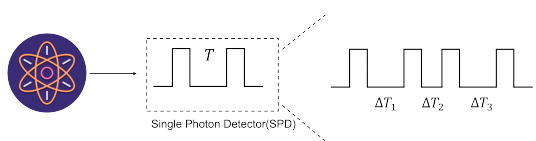
스위스 기업인 ID Quantique는 2020년 초소형 QRNG 칩 IDQ250C2를 발표하였다[11]. IDQ250C2는 모바일 헤드셋, 엣지 장치, IoT를 위해 설계되고 체조된 최초의 양자 난수 생성기로, ID Quantique의 독자적인 양자 기술인 CMOS 이미지센서로 캡쳐한 광원의 shot noise에서 첫 번째 비트부터 높은 엔트로피로 편향되지 않고 예측이 불가한 난수를 생성한다.

스페인 기업인 Quside는 2020년 상용화 가능한 첫 번째 양자 무작위성 모듈 Quside™ FMC 400을 발표하였다. Quside™ FMC 400은 고성능 FPGA 기반 시스템용으로 설계되었으며, Quside의 독자적인 기술인 위상 확산 양자 생성 기술을 기반으로 개발되었다. 그리고 최첨단 최소 엔트로피 경계(90% 초과)를 갖는 400Mb/s의 raw random number를 제공한다. 2021년 Galician Supercomputing Center(CESGA)는 Galician Quantum Technologies Pole과 관련된 인프라의 일부에 Quside의 양자난수 생성기를 사용하였다. 결과적으로, 몬테카를로 시뮬레이션 등 random workload는 최대 10배의 성능 향상을 달성하였으며, 더 정확한 결과를 얻을 수 있다. 2022년 Barcelona Supercomputing Center (BSC)도 Quside의 QRNG를 배치하여 무작위 알고리즘과 몬테카를로 알고리즘에 새로운 자원의 사용을 시범적으로 시행되었으며, 10배 이상의 성능 향상을 달성하였다 [12].

3.2. 광자 도착 시간 기반 양자난수생성기

2022년 [13]은 광자 도착 시간 기반 양자난수열을 생성하는 시스템을 구현하였다. 광자 도착 시간 기반 QRNG는 단일 광자의 생성 확률과 소실 확률 그리고 검출기의 데드 타임과 검출 확률에 의해 난수열이 생성되는 방식이다[14]. [그림 3]은 광자 도착 시간을 기반으로 하는 QRNG를 표현한 것으로, 2개의 detection events 사이의 시간 간격인 $\triangle T$를 측정하여 임의의 비트를 생성할 수 있다.

광자 도착 시간 기반의 양자난수생성은 검출기 시간 간격과 동작 설정 방식에 따라 설계 방식이 다르다. 따라서 설계된 광자 도착 시간 기반의 QRNG는 free-running mode로 동작되는 검출기를 사용하여 레



〔그림 3〕 광자 시간 도착 기반 양자 난수생성기

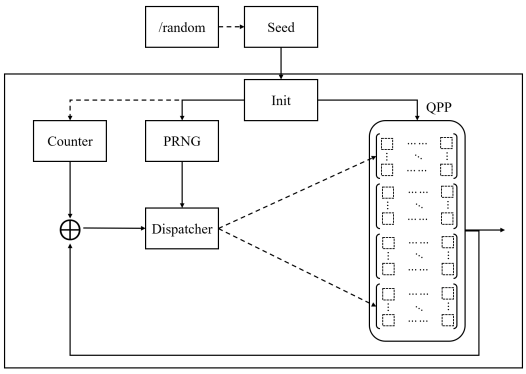
이저는 100MHz로 펄스를 생성하였고, 검출기의 데드타임보다 큰 펄스 검출 시간 간격인 δ 를 갖도록 설계되었다. 난수 생성은 δ 시간을 δ_1, δ_2, δ_3, δ_4 로 나누어 펄스가 δ_1, δ_2, δ_3, δ_4에 측정될 경우, 각각 00, 01, 10, 11bit가 생성되도록 설계되었다. 생성된 난수열의 난수생성속도는 레이저의 100MHz 펄스 생성 속도에서 1834.19bps로 측정되었다. 생성된 난수열은 NIST의 SP800-90B에서 제시한 난수성 검증방식으로 계산되었다. 결과적으로 총 10회 난수열 생성의 평균값으로 계산된 엔트로피는 1bit 기준으로 0.871bit 계산되었다.

3.3. Pseudo QRNG with Quantum Permutation Pad(QPP)

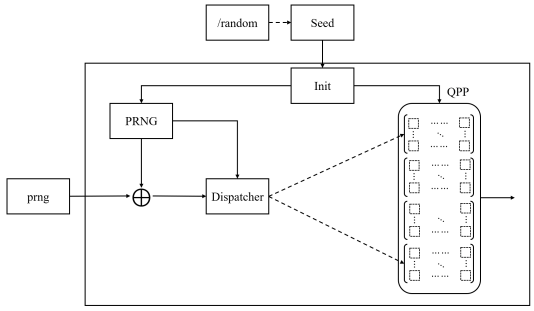
2021년 [15]는 quantum permutation의 높은 엔트로피를 bijective 변환을 활용하여 Quantum Permutation Pad(QPP)라고 불리는 양자 알고리즘을 사용하는 pQRNG(Pseudo Quantum Random Number Generator)를 제안하였다. [그림 4]는 제안하는 deterministic pQRNG를 나타낸 것이다.

PRNG는 입력 seed와 함께 deterministic 의사 난수를 생성하여 Dispatcher가 QPP에서 특정 permutation 행렬을 선택하도록 제어 가능하다. 이때, seed의 길이는 16KB이다. Counter도 제공된 seed에 의해 초기화되며, 출력 피드백은 XOR된 후, 변환을 위해 특정 permutation 행렬로 무작위로 발송된다. 결과적으로, QPP의 출력은 의사 난수 혹은 pQRN으로 간주된다.

[그림 5]는 양자 엔트로피 부스터 또는 qeBooster를 표현한 것으로, [그림 4]의 변형된 구조를 갖고 있다.



〔그림 4〕 Deterministic pQRNG의 구조도



〔그림 5〕 qeBooster의 구조도

qeBooster는 낮은 엔트로피 pesudo 난수 생성기의 엔트로피 부스터 역할을 하여 prng의 무작위성을 향상시키는 특징을 갖는다.

결과적으로 pQRNG는 우수한 무작위성을 보여주었으며, 엔트로피 부스터로서 모든 입력 데이터의 무작위성을 개선을 하였다. 2.5KB 작은 공간을 차지하기 때문에 시스템 내장이 가능하여 시스템의 의사 난수 생성을 향상 시킬 수 있는 특징을 갖는다.

Ⅳ. 결 론

본 기고에서는 양자암호통신과 양자난수발생기에 대해서 확인하였다. 양자역학의 발전에 따라 컴퓨터 공학에 많은 영향을 주고 있으며, 현재 양자컴퓨터와 함께 많은 연구가 진행 중이다. 두 기술은 암호 분야에 있어서 획기적인 기술이다. 양자암호통신은 기존 암호통신과는 다른 차원의 보안성을 제공하며, 양자난수발생기는 의사난수의 한계를 벗어난 난수를 양자의 특성을 통해 생성하고 이러한 난수가 많은 수의 암호 알고리즘에서 사용할 수 있다. 따라서 해당 분야에 대한 지속적인 연구와 개발을 통해 안전한 보안통신이 가능한 환경을 구축해 나갈 수 있도록 노력해야 할 것이다.

참 고 문 헌

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” *Reviews of Modern physics*, 74(1)), pp. 145, 2002.

[2] J. Y. Park, B. I. Kim, and J. Heo, “양자암호통신 프로토콜의 발전,” *Journal of the IEIE*, 48(5), pp. 26-33, 2021.

[3] H. I. Kim, G. W. Park, Y. S. Lee, and Y. D. Kim,

"A Study on Testing Metricusing Quantum Communication Testbed," *Proceedings of the Korean Institute of Communication Sciences Conference*, pp. 872-873, 2021.

[4] K. S. Shim, Y. H. Kim, C. K. Lee, and W. H. Lee, "The Implementation of Quantum Key Management System and Q-SDN-Controller Functions for KREONET Quantum Cryptography Network," *Proceedings of the Korean Institute of Communication Sciences Conference*, 80(1), 2023, Feb.

[5] Q. Wang, X. Yu, Q. Zhu, Y. Zhao, and J. Zhang, "Quantum key pool construction and key distribution scheme in multi-domain QKD optical networks (QKD-ON)," *4th Optics Young Scientist Summit (OYSS 2020)*, 11781, pp. 509-512, 2021, Feb.

[6] C. H. Park, M. K. Woo, B. K. Park, Y. S. Kim, H. J. Baek, S. W. Lee, H. T. Lim, S. W. Jeon, H. J. Jung, S. G. Kim, and S. W. Han, "2×N twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing," N*pj Quantum Information*, 8(1), pp. 48, 2022.

[7] P. Ayubi, S. Setayeshi, A. M. Rahmani, "Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application," *Journal of Information Security and Applications*, 52, 2020.

[8] E. B. Barker, and J. M. Kelsey, "Recommendation for random number generation using deterministic random bit generators (revised)," *Washington, DC, USA: US Department of Commerce, Technology Administration, National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory*, 2007.

[9] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *Journal of Modern Optics*, 47(4), pp. 595-598. 2000.

[10] QRANGE-Quantum Random Number Generators: Cheaper, Faster, More Secrue, Online: https://qrange.eu/.

[11] ID Quantique, Online: https://www.idquantique.com.

[12] Quside, Online: https://quside.com.

[13] Y. J. Seo, and H. Jun, "Quantum random number generation and analysis based on photon arrival time," *Proceedings of the Korean Institute of Communication Sciences Conference*, pp. 1241-1242, 2021, June.

[14] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number gerneration," *Npj Quantum Information*, 2(1), pp1-9, 2016.

[15] R. Kuang, D. Lou, A. He, C. McKenzie, and M. Redding, "Quantum Random Number Generator with Quantum Permutation Pad," *2021 IEEE international conference on quantum computing and engineering, IEEE*, pp 359-364, 2021.

〈저자소개〉

권혁동 (Hyeok-Dong Kwon)
학생회원
2018년 2월 : 한성대학교 IT융합공학부 졸업
2020년 2월 : 한성대학교 IT융합공학부 석사
2020년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정
<관심분야> 정보보안, 암호구현

심민주 (Min-Joo Sim)
학생회원
2021년 2월 : 한성대학교 IT융합공학부 졸업
2023년 2월 : 한성대학교 IT융합공학부 석사
2023년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정
<관심분야> 정보보안, 암호구현

송 경 주 (Gyeong-Ju Song)

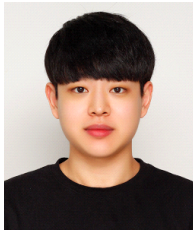
학생회원

2021년 2월 : 한성대학교 IT융합공학부 졸업

2023년 2월 : 한성대학교 IT융합공학부 석사

2023년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정

<관심분야> 양자컴퓨팅, 암호구현, 정보보안



이 민 우 (Min-Woo Lee)

학생회원

2023년 2월 : 한성대학교 IT융합공학부 졸업

2023년 3월~현재 : 한성대학교 IT융합공학부 석사과정

<관심분야> 정보보안, 암호구현

서 화 정 (Hwa-Jeong Seo)

종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 졸업

2012년 2월 : 부산대학교 컴퓨터공학과 석사

2016년 2월 : 부산대학교 컴퓨터공학과 박사

2017년 4월~2023년 2월 : 한성대학교 IT융합공학부 조교수

2023년 3월~현재 : 한성대학교 융합보안학과 부교수

<관심분야> 정보보안, 암호구현