양자 키 분배 간 양자내성암호 접목 사례 동향

차정현[1], 서승현[2]
[1]한양대학교 전자공학과 석박사통합과정
[2]한양대학교 ERICA캠퍼스 전자공학부 교수
jhcha0822@hanyang.ac.kr, seosh77@hanyang.ac.kr

Recent Studies on Quantum Key Distribution with Post Quantum Cryptography

Jeong-Hyun Cha[1], Seung-Hyun Seo[2]
[1]Dept. of Electrical Engineering, Hanyang University
[2]School of Electrical Engineering, Hanyang University ERICA

요 약

양자 키 분배는 물리적 안전성에 기반을 두어 지속가능한 보안성을 제공한다. 양자내성암호는 양자 컴퓨터로 풀이가 어려운 문제에 기반을 둔 공개키 암호이다. 양자 키 분배 네트워크를 구성하여 안전한 통신을 구현하기 위해서는 키 조합 혹은 인증 단에서 양자내성암호의 적용이 필요하다. 본 논문에서는 양자 키 분배 네트워크의 해결 과제를 살펴보고, 이를 극복하기 위한 연구와 표준화 동향에 대해 살펴본다.

1. 서론

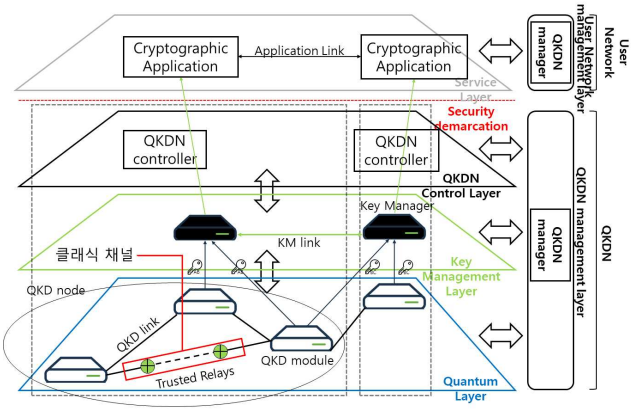
Peter Shor가 1994년 제안한 쇼어(Shor) 알고리즘과 1996년 Lov Grover가 제안한 그로버(Grover) 알고리즘으로 인해 RSA 및 타원곡선 암호(ECC: Elliptic Curve Cryptography)와 같은 현대 공개키 암호화 방식이 더는 안전하지 않은 것으로 알려져 있다[1].

이에 양자컴퓨터 시대에서도 안전한 통신을 위해 두 방식이 고려된다. 수학적 계산 복잡성이 아닌 물리적 안전성에 기반을 둔 양자 키 분배(QKD: Quantum Key Distribution)와, 양자 컴퓨터로 풀기 어려운 문제에 기반하는 공개키 암호 시스템인 양자내성암호(PQC: Post Quantum Cryptography)이다. 양자 키 분배는 1984년 Charles Bennett과 Gilles Brassard에 의해 처음 제안[2]되어 현재까지 활발히 연구되어 오고 있으나, 실제 관측 장비의 한계 및 비용적 문제, 현대암호 인프라에 적용하기 어렵다는 문제와 더불어 인증이 불가하고 점대점(point to point) 통신만을 제공한다[3]. 이는 QKD에 PQC를 적용하여 상호보완적으로 해결할 수 있다.

본고에서는 양자 키 분배 네트워크(QKD Network)에서의 QKD-PQC 접목 사례를 알아보고, 적용 범위를 분류하여 이후 안전한 양자통신의 요구사항을 분석하고자 한다.

2. 양자 키 분배 네트워크

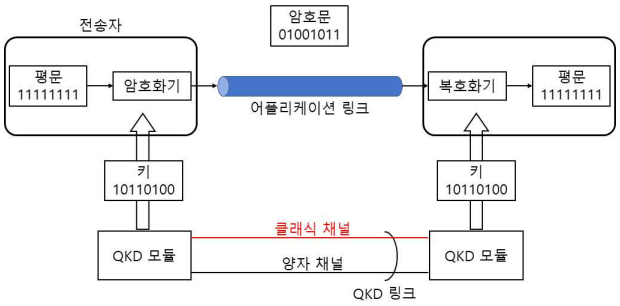
양자 키 분배는 빛의 양자적 성질을 이용하여 대칭키를 공유하는 기술이다. QKD 기술 자체는 점대점 통신만 가능하며 양자의 비복제성 원리와 전송거리의 한계를 보유하고 있기에 QKDN의 구성이 필요하다. 이에 유럽전기통신표준협회(ETSI), 국제전기통신연합-전기통신표준화부문(ITU-T), 한국정보통신기술협회(TTA) 등에서는 양자암호 통신망 표준화 작업을 진행 중이다.



[그림 1] ITU-T QKDN 권고사항[4]

ITU-T QKDN 권고 사항[4]에서 생성된 키들은 Key Management 계층의 Key Manager 사이의 키 릴레이를 통해 서로 공유된다. 이때 안전한 릴레이를 구성하기 위해 이웃 QKD 링크의 키를 사용하거나 이전에 릴레이되었던 키를 이용하여 OTP를 하

는 것이 가장 이상적이겠지만, 이를 만족할 만한 양의 키가 존재하지 않기에 다른 암호화 기법을 이용할 것을 권고한다.



[그림 2] 점대점 암호화 통신 QKD 예시

실제 QKD가 이루어지는 Quantum Layer는 큐비트(qubit)를 전달하는 양자통신 채널과 비트 기반 통신이 이루어지는 클래식 채널(classic channel)로 구성된다. 양자통신은 양자의 물리적인 성질인 비복제성과 불확정성으로 인하여 안전하게 보호되지만 이를 이용하여 키를 결정하기 위한 정보가 전달되는 채널인 클래식 채널은 암호화가 필수적이다.

3. QKD-PQC 접목 사례

ITU-T의 기술 보고서[5]에 따르면 QKDN에 PQC를 접목한 기법은 크게 두 가지로 분류할 수 있다. 1. QKD를 하나의 키 교환 방식으로 생각하여 다른 키 교환과 결합하는 기법과 2. QKD 계층 내에서 PQC를 이용하는 기법이다.

3.1. QKD 키와 PQC의 결합

2020년 Dowling 등은 PQC와 QKD를 결합해 이용하는 인증된 키 교환 기법을 제시했다[6]. 당해 Xu 등도 두 키 교환을 결합한 robust combiner에서 하나를 QKD로 대체하는 시도를 했다[7].

ETSI TS 103 744는 양자 내성 키 교환 기법에 대한 표준이다[8]. 두 키 교환의 사전 공유 키는 Diffie-Hellman과 양자내성 키 캡슐화 기법(KEM) 대신 QKD를 이용하여 설정 가능하다고 명시한다.

NIST 또한 SP 800-133 Rev.2[9]에서 적어도 하나의 NIST 표준으로 인정된 KEM을 결합한다면 QKD를 이용할 수 있다고 허용한다.

IETF RFC 8784[10]는 IKEv2에서 사전 공유 키를 생성하는 과정으로, QKD의 사용을 허가한다. 이 경우 양자내성 사전 공유 키 및 키 식별자를 생성하는 하나의 방식으로 이용된다.

저자/기관	구분	내용	인용
Dowling 등	Muckle	QKD와 PQC KEM 결합	6
Xu 등	robust combiner	KEM 대신 QKD로 대체	7
ETSI	TS 103 744	사전 공유키 QKD 대체	8
NIST	SP 800-133 R.2	NIST PQC-QKD 가능	9
IETF	RFC 8784	IKEv2 사전 공유 키로 QKD 허용	10

[표 1] 키 결합 방식 요약

3.2 QKD 프로토콜 내 PQC 적용

ETSI의 Quantum Safe White Paper[11]에 따르면, 사전 공유키가 존재하지 않을 때 초기 QKD 세션의 인증 시 공개키 서명을 이용해야 한다. 이 공개키 서명이 QKD 세션 내에 해독되지 않는다면 생성된 키가 이론적으로 안전하며, 차후에 공개키가 깨져도 이전 QKD 세션의 QKD 키의 일부를 사용하여 인증이 가능하기에, 공개키 서명의 단기적인 보안만 요구된다. 이때 양자컴퓨터로 단시간 내 해독이 불가하다고 여겨지는 PQC를 이용한다면 정보 이론적 안전(information theoretically secure)성이 보장된다.

2021년 Wang 등은 PQC와 PKI(Public Key Infrastructure)를 이용하여 각 사용자들이 인증 기관으로부터 받은 하나의 전자 인증서만 보유한다면 클래식 채널의 인증이 가능해 효율적이고 안전한 QKD가 가능하다고 제안하였다[12]. PQC를 에러 정정 혹은 최종 키 확인 과정 등에 이용할 경우, 생성된 부분은 키 정보를 포함하고 있기에 일반적인 QKD는 사전 공유 키를 기반으로 하여 인증을 진행한다. 이들은 2022년에 PQC에 기반한 프로토콜 두 가지로 QKD 데이터의 후처리를 위한 완전한 인증을 구현하였다[13].

2022년 Hassane 등[14]은 클래식 채널에서 전송되는 정보의 암호화를 위해 NIST의 PQC 3라운드 후보였던 NTRU를 이용하였다. NTRUrobust-PKE와 KEM을 이용하여 전송자의 편광과 측정 정보를 암호화해 세션 간 양자 공유 키를 생성한다. Parksan 등[15] 또한 클래식 채널에서의 세션 인증과 교환 정보 암호화를 위하여 NTRU를 이용하였다. 이들은 추가로 서명을 전송하고, 에러 정정 과정에서 기저를 전송할 때, 마지막으로 키 재조정(reconciliation) 과정에서 PKI를 이용하여 정보를 보호한다.

한국의 국가과학기술연구망인 KREONET의 양자암호 통신망 구성 시, 망이 관리하지 않는 사용자 종단까지 QKD를 배치하면 소요가 크기에 효율적인 망 구현을 위해 해당 네트워크 액세스 구간의 데이터 채널 암복호화와 인증에 PQC를 이용하였다[16].

ITU-T는 X.sec_QKDN_AA[17] 권고를 작성 중이다. QKDN에 인증 및 권한 부여를 위하여 PQC를 적용할 때의 고려사항을 위한 표준으로, 2023년 9월 작성 완료될 예정이다.

저자/기관	구분	내용	인용
Wang 등	PQC Authentication	클래식 채널, 후처리 과정의 인증	12 13
Hassane 등	PQC Encryption	클래식 채널 정보 암호화	14
Paraksan 등	PQC Authentication, Encryption	클래식 채널 인증, 암호화	15
KISTI	PQC Authentication	QKDN망 종단 데이터 채널 암복호화, 인증	16

[표 2] 클래식 채널 인증 & 암호화 방식 요약

4. 결론

본고에서는 ITU-T의 기술보고서에 근거해 QKDN에 PQC를 접목한 사례를 알아보고, 분류하였다. QKD 기술은 이제 막 실용화 단계에 올라가고 있으나, 관련 표준은 최근 제시되었고 일부는 아직 작성 중인 상태이다. QKDN의 구현을 할 때 선행 연구들의 사례를 적절히 조합한다면 안전한 양자통신이 가능할 것으로 예상한다.

Acknowledgement

본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2021R1A2C1095591)

참고문헌

[1] Mosca, Michele. "Cybersecurity in an era with quantum computers: will we be ready?." IEEE Security & Privacy 16.5, 2018, pp.38-41.

[2] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proceedings of the IEEE Int. Conf. Comput. Syst. Signal Process., Bangalore, India, 1984, pp.175 - 179.

[3] Sasaki, Masahide. "Quantum key distribution and its applications." IEEE Security & Privacy 16.5, 2018, pp.42-48.

[4] ITU-T SG 13, “Overview on networks supporting quantum key distribution”, Standard ITU-T Y.3800 Corrigendum 1, International Telecommunication Union, 2020b.

[5] ITU-T SG 17, “Security considerations for quantum key distribution networks”, Publication XSTR-SEC-QKD, Corrigendum 1. International Telecommunication Union, 2020.

[6] B. Dowling, Torben B. Hansen, and Kenneth G. Paterson. "Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange." Post-Quantum Cryptography: 11th International Conference, PQCrypto Paris, France, 2020, pp.483-502

[7] Xu, Jia, Yiwen Gao, and H. Lim. "Practical quantum-safe stateful hybrid key exchange protocol." Cryptology ePrint Archive, 2020.

[8] ETSI TS 103 558 V1.3.1, Methods for objective assessment of listening effort, 2021.

[9] Barker, Elaine, et al. "Recommendation for cryptographic key generation.", 2012

[10] Fluhrer, S., et al. "RFC 8784 Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security.", 2020.

[11] ETSI White Paper No. 8, “Quantum Safe Cryptography and Security. An introduction, benefits, enablers and challenges”, 2015, ISBN No. 979-10-92620-03-0.

[12] Wang, Liu-Jun, et al. "Experimental authentication of quantum key distribution with post-quantum cryptography." npj quantum information 7.1, 2021, pp.67.

[13] Wang, Liu-Jun, et al. "Authentication of quantum key distribution with post-quantum cryptography and replay attacks." arXiv preprint arXiv:2206.01164, 2022.

[14] A. Azizi. "A Combination of BB84 Quantum Key Distribution and An Improved Scheme of NTRU Post-Quantum Cryptosystem." Journal of Cyber Security and Mobility, 2022, pp.673-694.

[15] Prakasan, Avani, Kurunandan Jain, and Prabhakar Krishnan. "Authenticated-Encryption in the Quantum Key Distribution Classical Channel Using Post-Quantum Cryptography." 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2022.

[16] 김용환, and 이원혁. "포스트 퀀텀 시대의 안전한 통신-Quantum KREONET.", 2022.

[17] ITU-T SG 17, “Authentication and authorization in QKDN using quantum safe cryptography”, Drafting ITU-T X.sec_QKDN_AA, International Telecommunication Union, 2022.