포스트 퀀텀 암호 및 양자 키 분배 기술 연구 동향

조병현*, 박종혁*
*서울과학기술대학교 컴퓨터공학과
{jbh1020, jhpark1}@seoultech.ac.kr

The Post Quantum Cryptography and Quantum Key Distribution Technology Research Trends Analysis and Reflections

Jo Byung Hyun*, Jong Hyuk Park*
*Dept. of Computer Science, Seoul National University of Science and Technology

요 약

ICT 기술과 IoT 기술의 급속한 발전으로 인해 인간은 네트워크와 밀접한 관계를 형성하며 이를 통해 다양한 서비스를 경험하고 있다. 그러나 ICT 기술의 발전과 함께 사이버 공격의 급증으로 인해 네트워크 보안에 대한 필요성이 대두되고 있다. 또한 양자 컴퓨팅을 활용한 다양한 공격은 기존 암호화 체계를 무너뜨려 빠른 대응 및 솔루션이 필요하다. 양자 기반 공격으로부터 안전한 네트워크 환경을 구축하기 위해 양자 키 분배 시스템 및 양자 내성 암호가 활발히 연구되고 있으며 NIST 에서 발표한 양자 내성 암호화 기법의 성능, 취약점, 실제 네트워크 상의 구현 가능성, 향후 발전 방향 등 다각적 관점에서 연구 및 분석이 진행되고 있다. 본 논문에서는 양자 기반 공격에 대해 설명하고 양자 내성 암호화 기법의 연구 동향에 대해 분석한다. 또한, 양자 중첩, 양자 불확실성 등 양자의 물리적 성질을 활용함으로써 양자 공격으로 부터 안정성을 제공할 수 있는 양자 키 분배 기법에 대해 설명한다.

1. 서론

최근 ICT 기술의 발전과 함께 사이버 공격이 급증하고 있으며 이로 인한 피해를 정확하게 추정하기 어려워 교통, 에너지, 금융 등 다양한 산업 분야에서 유무선 통신 네트워크 보안 및 디바이스 보안에 대한 안전성이 중요한 이슈로 대두되고 있다.

현재 서비스 중인 대부분의 유무선 통신망의 보안은 RSA 암호와 타원곡선암호(ECC)를 기반으로 하고 있으나 Shor 알고리즘 및 Grover 알고리즘을 활용한 양자 컴퓨팅 기술의 최신 암호화 체계에 대한 단시간 해독 가능성이 제기되면서 기존 유무선 통신망의 암호화 체계로는 통신 안전을 보장하기 어려워 심각한 사이버 보안 문제를 야기할 수 있다. 이에 양자 컴퓨팅 기반 사이버 공격으로부터 유무선 통신 네트워크 환경을 보호하기 위해 전 세계적으로 포스트 양자 암호(PQC: Post Quantum Cryptography) 기술에 대한 연구가 진행되고 있으며, 2016 년 12 월 미국 국립표준기술연구소(NIST)는 포스트 양자 컴퓨팅 표준화 과정을 공개 요청[1]하고 세 차례의 평가와 분석을 통해 1 차 알고리즘을 선정했다[2].

현재 양자 내성 네트워크 구축을 위하여 양자 내성 암호와 더불어 양자 키 분배(QKD:Quantum Key Distribution)시스템이 활발하게 진행되고 있다. 양자 키 분배 시스템은 수학적 복잡성에 기반한 현대 암호화 방식과 달리 양자의 불확실성, 중첩, 양자 채널 등 양자의 물리적 성질 및 양자 전용 채널을 통해 제 3 자의 도청을 방지하고 안전하게 키를 공유할 수 있어 PQC 와 함께 양자 공격으로부터 안전한 네트워크 환경을 구축할 수 있는 방법으로 여겨지고 있다.

본 논문에서 양자 기반 공격으로부터 안전한 네트워크 통신 환경을 구축하기 위하여 양자 컴퓨팅을 활용하여 실행 가능한 공격들에 대해 설명한다. 3 장에서 양자 공격으로부터 안전성을 제공할 수 있는 PQC 연구 동향에 대해 설명하고, 4 장에서 QKD 시스템의

연구 동향에 대해 설명한다.

2. 양자 기반 공격

양자의 특성을 활용한 양자 컴퓨팅은 기존의 컴퓨터와 비교하여 빠른 계산 및 처리 속도를 향상시켜 최적화, 시뮬레이션, 의료 및 인공지능 등 다양한 분야와 결합하여 큰 발전을 이루어 낼 수 있으나 양자의 병렬성, Shor 알고리즘, Grover 알고리즘 등을 활용한 양자 기반 공격들은 현재 강력한 보안 체계로 여겨지는 대부분의 암호화 알고리즘을 무너뜨릴 수 있다.

- Shor 알고리즘: Shor 알고리즘은 양자 컴퓨팅을 활용하여 큰 수를 효율적으로 소인수 분해하는 알고리즘이다. Shor 알고리즘을 활용할 경우 다항시간 내에 큰 수의 인수를 찾는 것이 가능하며 이는 큰 수의 소인수분해가 난해하다는 수학적 복잡성에 기반하는 현대 암호 시스템의 큰 위협이 된다 [3].
- Grover 알고리즘: 양자 컴퓨팅을 활용한 Grover 알고리즘은 짧은 시간안에 정렬되지 않은 데이터베이스에서 특정 항목을 찾을 수 있게 한다. N 개의 항목이 정렬되지 않은 데이터 베이스에서 특정 항목을 $\sqrt{n}$ 번의 탐색으로 찾을 수 있으며 [4], Bone 과 Castro [5]는 56 비트의 키를 가지는 DES 의 경우 단 185 번의 탐색만으로 비밀 키를 찾을 수 있음을 확인하였다.
- 양자 머신러닝 기반 공격: Hyun-Ji Kim [6]등은 양자 컴퓨터의 머신러닝 알고리즘 중 하나인 양자 지원 벡터 머신(QSVM: Quantum Support Vector Machine)을 활용하여 평문과 암호문 쌍을 입력하여 키 값을 찾아내는 공격을 수행하였으며 이는 2 비트 데이터셋에 대해 0.93 의 정확도를 달성하였다.
- 해시 함수 충돌쌍 공격: 해시 함수 충돌쌍 공격은 2020 년 Hosoyamada 와 Sasaki [7]이 제안한 공격 기법으로서 양자 컴퓨터를 보유한 공격자가 기존 성능을 가진 컴퓨터를 이용하는 공격자와 비교하여 해시함수의 더 많은 라운드에 대한 공격 횟수가 더 많음을 입증하였으며 이를 통해 많은 보안 기법에 사용되는 해시함수가 양자 컴퓨팅 공격으로부터 안전성이 위협받을 수 있음을 보여준다. 현재 양자 컴퓨팅 환경 내 해시 함수 충돌쌍 공격부터 블록암호 기반 해시함수, 전용 해시함수의 안전성에 대한 연구가 진행되고 있다 [8].

3. 양자 내성 암호 연구 동향

양자 내성 암호는 양자 기반 공격으로부터 보안을 유지하기 위해 개발 및 연구되고 있는 암호화 기법으로서 양자 컴퓨팅과 더불어 기존의 암호화 체계를 발전시킴으로써 미래의 안전한 네트워크 환경을 구축할 수 있다.

JA Septien-Hernandez 등 [9] 등은 IoT 디바이스에 적합한 양자 내성 암호 시스템을 연구하여 기존의 통신 및 암호화 기법과 함께 사용될 수 있도록 LightSaber, Kyber512, NTRUhps2048509, NTRULPr653, FrodoKEM-640 의 격자 기반 양자 내성 암호의 RAM, CPU 등의 성능 측정을 수행하였다. 연구 결과, Lightsaber 와 Kyber512 가 가장 높은 성능을 보였으며, 이외에도 상당수가 현재 IoT 디바이스 환경에서 효율적으로 실행될 수 있으며 양자 기반 공격으로부터 안전성을 제공할 수 있음을 입증하였다.

Aleksei Vambol [10]등은 양자 기반 공격으로부터 안전한 네트워크 환경을 구축하기 위해 McEliece, Niederreiter 암호시스템에 대해 암호화 강도, 성능, 공개 키 크기, 암호문 등의 특성 및 기타 비대칭성을 분석하였다. 이진 Goppa 코드를 기반으로 하는 McEliece, Niederreiter 암호시스템은 모두 양자 내성 기능을 제공하며 RSA 기법과 비교하여 암호화, 복호화, 키 생성가 빠르다는 장점이 존재하나 키 크기가 매우 크다는 단점이 존재한다.

Mohammed Gharib [11]등은 Zero Trust(ZT) 환경에서 5G 네트워크 상의 안전한 비상 중요 통신 보안(SGG5G:Secure Critical-mission Communication) 아키텍처를 제안하였다. SGG5G 아키텍처는 ZT 환경에서 5G 네트워크를 비상 통신으로 활용하여 데이터 통신을 종단간으로 암호화하고 종단 사용자를 상호 인증하여 양자 내성 암호화를 지원함으로써 5G 네트워크 환경에서 양자 내성을 제공하고 이에 따른 실현 가능성 및 신뢰성을 검증하였다.

4. 양자 키 분배 시스템 연구 동향

양자 키 분배 시스템은 양자 중첩, 양자의 불확실성, 양자의 복제 불가능성 등 양자의 물리적 성질을 활용하여 키를 교환하는 기법으로 양자 채널을 통해 정보를 포함한 양자를 통신 및 측정함으로써 제 3 자의 도청이 불가능하여 양자 기반 공격으로 안전하게 키를 공유할 수 있다.

Rongyu Wei [12]등은 양자 통신 네트워크의 보안성 향상 및 중간자 기반 공격의 안전성 향상을 위해 공격 기반 검출 전략(WN19)를 제안하였다. WN19 기법은 공격 기반 검출 결과에 따라 송신자의 양자 상태의 초기 상태를 조정함으로써 양자비트 오류율

(QBER: Quantum Bit Error Rat)를 0.1367 로 감소시키고 도청자가 정보를 획득할 확률을 줄일 수 있다.

Muskan 등[13]은 위성 기반 상향 및 하향 링크에 대하여. BB84, B92, E91, BBM92 등 양자 키 분배 프로토콜에 대한 성능 분석을 진행하였다. 연구 결과, 특정 거리에 대해 BB84 프로토콜의 키 분배 속도가 가장 뛰어난 것으로 확인되었으며 BBM92 과 E91 을 비교하였을 때 BBM92 이 더 높은 키 속도를 보장함을 입증하였다.

5. 결론

최근 정보통신기술(ICT) 기술의 빠른 발전으로 사용자와 수많은 디바이스가 연결되어 네트워크를 형성하고 있으며 이는 네트워크 및 어플리케이션 사용자에게 다양한 편의성을 제공하나, 네트워크 및 디바이스 보안 취약점을 겨냥한 사이버 공격 또한 증가하고 있는 추세이다. 사이버 공격으로 네트워크 보안의 중요성이 대두되고 있으며 유무선 통신 네트워크의 보안이 중요한 이슈로 떠오르고 있다.

기존의 주요 통신시스템으로 비대칭 키, 대칭 키 암호화 방식이 널리 사용되고 있으며 매우 큰 수에 대한 소인수 분해의 복잡성에 기반하여 안전성을 제공한다. 그러나 양자 컴퓨팅의 등장과 Shor 알고리즘, Grover 알고리즘을 활용한 양자 기반 공격은 단시간에 기존의 암호화 기술을 복호화 할 수 있어 기존 암호 체계를 무너뜨릴 수 있다.

본 논문에서 양자 기반 실행 가능한 공격에 대해 설명하고 양자 공격의 내성을 갖는 PQC 의 연구 동향에 대해 분석하였다. Shor 알고리즘은 매우 큰 수의 소인수 분해를 가능하게 하며 Grover 알고리즘은 N 개의 항목이 정렬되지 않은 데이터 베이스에서 특정 항목을 $\sqrt{n}$ 번의 탐색으로 찾을 수 있어 현대 암호 방식을 단시간에 복호화 할 수 있다. 머신러닝 기반 공격 및 해시 함수 충돌쌍 공격은 높은 정확도로 비밀키와 해시함수 값을 찾아낼 수 있다.

이에 안전한 네트워크 환경을 구축하기 위해 양자 키 분배 및 양자 내성 암호 방식이 연구되고 있으며 미국 국립 표준 기술 연구소에서 공개한 양자 내성 암호의 성능, 구현 가능성, 취약점 분석 등 다양한 분석 및 연구가 진행되고 있다.

양자 키 분배 시스템은 양자의 물리적 성질을 기반으로 무조건부의 안전성을 제공하는 키 교환 기법으로서 기존의 하드웨어 한계점으로 인한 키 생성률, 양자 오류율, 통신 거리 등을 개선하기 위한 연구가 지속적으로 진행되고 있다.

Acknowledgement

This research was supported by Strategic Networking & Development Program funded by the Ministry of Science and ICT through the National Research Foundation of Korea (RS-2023-00267476)

참고문헌

[1] Kimball, K. "Announcing request for nominations for public-key post-quantum cryptographic algorithms." Federal. Regi. 81.244 (2016): 92787-92788.

[2] Alagic, Gorjan, et al. "Status report on the third round of the NIST post-quantum cryptography standardization process." US Department of Commerce, NIST (2022).

[3] Bhatia, Vaishali, and K. R. Ramkumar. "An efficient quantum computing technique for cracking RSA using Shor's algorithm." 2020 IEEE 5th international conference on computing communication and automation (ICCCA). IEEE, 2020.

[4] Mavroeidis, Vasileios, et al. "The impact of quantum computing on present cryptography." arXiv preprint arXiv:1804.00200 (2018).

[5] Hidary, Jack D., and Jack D. Hidary. "A brief history of quantum computing." Quantum Computing: An Applied Approach (2021): 15-21.

[6] Kim, Hyun-Ji, et al. "Cryptanalysis of caesar using quantum support vector machine." 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). IEEE, 2021.

[7] Hosoyamada, Akinori, and Yu Sasaki. "Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound." Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30. Springer International Publishing, 2020.

[8] 백승준, 조세희, and 김종성. "양자 컴퓨팅 환경에서의 해시함수 충돌쌍 공격 동향." 정보보호학회지 32.1 (2022): 57-63.

[9] Septien-Hernandez, Jose-Antonio, et al. "A Comparative study of post-quantum cryptosystems for Internet-of-Things applications." Sensors 22.2 (2022): 489.

[10] Vambol, Aleksei, et al. "McEliece and Niederreiter Cryptosystems Analysis in the Context of Post-Quantum Network Security." 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI).

[11] Gharib, Mohammed, and Fatemeh Afghah. "SCC5G: A PQC-based Architecture for Highly Secure Critical Communication over Cellular Network in Zero-Trust Environment." arXiv preprint arXiv:2308.10696 (2023).

[12] Wei, Rongyu, Min Nie, and Guang Yang. "The Strategy of Beating the Intermediate Basis Attack in Quantum Communication Networks." 2020 International Conference on Computer Engineering and Application (ICCEA). IEEE, 2020.

[13] Yuan, Bo, Faguo Wu, and Zhiming Zheng. "Post quantum blockchain architecture for internet of things over NTRU lattice." Plos one 18.2 (2023): e0279429.