Quantum neural network를 활용한 암호 연구 동향

송경주*, 장경배*, 엄시우*, 심민주*, 서화정**
*한성대학교 IT융합공학부
**한성대학교 IT융합공학부
thdrudwn98@gmail.com, starj1023@gmail.com, shuraatum@gmail.com,
minjoos9797@gmail.com, hwajeong84@gmail.com

Cryptographic Research Trend Using Quantum Neural Network

Gyeong-Ju Song*, Kyung-bae Jang*, Si-Woo Eum*, Min-Joo Sim*,
Hwa-Jeong Seo**
*Dept. of IT Convergence Engineering, Hansung University
**Dept. of IT Convergence Engineering, Hansung University

요 약

고전적인 인공 신경망을 암호 분야에 사용하기 위한 연구들이 이뤄지고 있으며 다양한 암호 관련 분야에서의 사용이 제안되었다. 더 나아가 최근에는 양자 컴퓨터의 연산속도 이점을 활용해서 고전적인 인공 신경망을 학습하기 위한 연구들이 진행되고 있다. 양자컴퓨터의 양자 알고리즘은 기존 컴퓨터에서 보여주지 못한 연산속도를 보여주었으며 앞으로의 잠재력이 기대되고 있다. 본 논문에서는 Quantum Neural Network (QNN)를 활용한 암호 연구 동향에 대해 살펴본다.

I. 서론

고전적인 인공 신경망을 암호 분야에 사용하기 위한 연구들이 이뤄지고 있으며 키 분배 시스템, 암호화, 암호분석(cryptanalysis) 등의 암호관련 분야에서의 사용이 제안되었다[1][2]. 더 나아가 최근에는 양자컴퓨터의 연산속도에 대한 잠재력이 주목받으면서 방대한 양의 빅데이터를 고전적인 신경망에 학습시키기 위해 양자컴퓨터를 사용하는 Quantum Neural Network (QNN) 연구들이 진행되고 있다. 양자컴퓨터의 양자 알고리즘은 0과 1의 상태를 동시에 갖는 큐비트의 성질을 이용하여 고전적인 컴퓨터에서 보여주지 못했던 속도의 연산을 보여주었고 인공 신경망에 적용한 결과 연산 속도 향상을 보였다[5]. 이러한 긍정적인 결과를 바탕으로 더 많은 인공지능 암호 분야에 적용할 수 있을 것이라는 잠재력이 기대되고 있다.

본 논문에서는 Quantum neural network를 활용한 암호 연구 동향에 대해 살펴본다.

II. 관련연구

2.1 Quantum computing

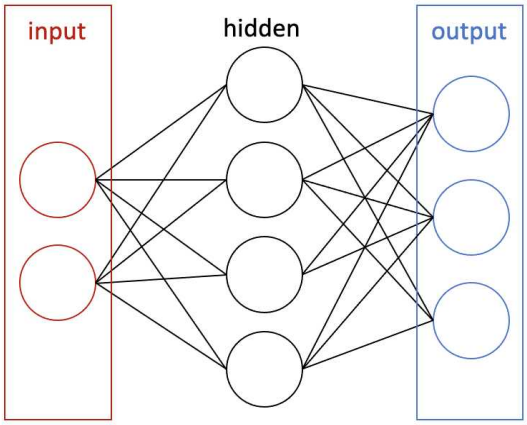
Quantum computing은 기존의 비트와 다르게 0과 1의 상태를 동시에 갖는 큐비트의 특징을 이용하여 계산효율을 증가시키는 특정 알고리즘을 통해 기존 컴퓨터 보다 월등한 속도향상을 보여주었다. 대표적인 양자 알고리즘은 인수분해를 위한 Shor와 데이터 검색을 위한 Grover 알고리즘이 있다. 큐비트는 얽힘과 중첩 상태를 가지므로 다루기 매우 까다롭다. 큐비트를 다루기 위해서는 Quantum-gate를 사용하여 상태의 변화를 주어야 한다. (1) 은 다양한 양자 게이트 중 단일 큐비트에 대한 rotation-gate를 보여준다. rotation-gate R_x, R_y, R_z 는 큐비트를 각 x, y, z 축을 기준으로 회전시킨다.

$$R_x(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix} \quad (1)$$

$$R_y(\theta)=\begin{pmatrix}\cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{pmatrix},\ R_z(\theta)=\begin{pmatrix}e^{-i\frac{\theta}{2}} & 0\\ 0 & e^{i\frac{\theta}{2}}\end{pmatrix}$$

2.2 인공신경망

인공 신경망은 인간의 뇌 구조를 인공적으로 구축한 신경망이다. 신경망은 여러 layer을 쌓아 만들어지며 layer은 뉴런들로 이루어져 있다. 뉴런은 입력을 통해 만든 출력을 다음 뉴런으로 전달한다. 그림 1은 3개의 layer로 구성된 인공신경망의 구조이다. 신경망은 크게 입력층(input layer), 은닉층(hidden layer), 출력층(output layer) 으로 나뉘는데 입력층은 처음 입력 값이 들어오는 layer이며 출력층은 모든 layer을 거친 후 학습 결과의 데이터를 가지는 layer이다. 은닉층은 입력층과 출력층을 제외한 데이터가 드러나지 않는 모든 layer 이다. 뉴런들은 모두 각자의 가중치(weight)와 바이어스(bias)를 가지며 전파 및 역전파를 통해 값을 갱신한다.



(그림 1) 인공신경망 구조.

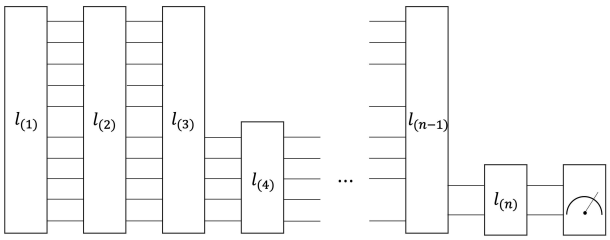
2.3 양자신경망

양자신경망(QNN)은 양자 이론의 특성과 신경망을 결합한 시스템이다. 기존 신경망에 양자 이론을 적용을 통해 중첩 상태를 이용하는 양자 컴퓨팅과 병렬처리의 신경망 컴퓨팅의 장점을 동시에 활용하여 강력한 잠재력이 있다고 주목받고 있다. 또한 양자 머신러닝 알고리즘은 빅데이터를 처리하기 위한 중요한 역할로서 주목받고 있다[3].

III. 연구동향

3.1 Continuous-variable quantum neural network[4][5]

양자모델은 이산변수 양자모델과 연속변수 양자모델 두 가지 범주로 나눌 수 있다. 이산변수 양자모델은 Pauil 행렬과 같은 단일 연산을 수행하는 반면에 연속변수 양자모델은 대부분 Gaussian과 non-Gaussian 연산을 사용하여 양자 상태를 변환한다. 그림 2 은 일반적인 연속변수 quantum neural network 이다. $l_N(N=0,\cdots,n)$은 양자 신경망의 각 layer를 나타내며 마지막 layer에서 측정을 통해 정보를 얻는다. 각 layer $l_N(N=0,\cdots,n)$의 뉴런들은 단일 Gaussian 게이트 $R(\varnothing), S(r), D(\alpha)$, $(\varnothing\in[0,2\pi], \alpha\in C\cong R^2, r\geq 0)$ 을 사용하여 $l_{newron}:=\varphi\circ D\circ R_2\circ S\circ R_1$ 연산을 수행한다.

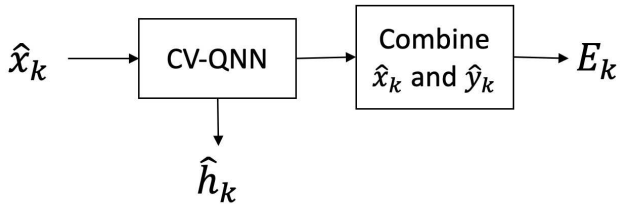


(그림 2) 연속변수 양자신경망.

$R_{1,2}$은 rotation gate, S는 Squeezing gate, D는 displacement gate, φ은 비선형 함수를 나타낸다. 신경망 모델을 암호화 및 복호화에 사용하기 위해서는 훈련을 통해 정확도를 높여야 한다. QNN의 훈련방법은 두 가지로 나뉘는데 첫 번째 방법은 기존 양자 알고리즘을 사용하여 신경망의 매개변수를 최적화하는 방법이다. 예를 들어 네트워크에 대해 최적의 가중치를 찾을 때 양자 검색 알고리즘을 활용한다. 두 번째 방법은 target function 의 최적의 값을 찾기 위해 기존 학습 알고리즘과 동일한 양자 학습 알고리즘을 생성한다. 경사하강법에 양자 계산을 이용하는 것은 두 번째 방법에 속하는데 많은 프로그래밍 플랫폼은 이미 보편적으로 최적의 경사를 계산할 수 있다. 그 중 [5]에서는 양자 신경망에 확률적 경사 하강 알고리즘인 Adam 알고리즘을 사용하였다. Adam알고리즘은 비결정적이지만 최적화된 출력을 제공하기 때문에 양자 신경 암호 시스템을 최적화하

기에 적합하다.

그림 3은 Continuous-variable quantum neural network (CV-QNN)를 이용한 암호화 과정을 대략적으로 보여준다. 암호화를 진행하기 위해서 평문 메시지 M을 위상을 가진 양자 상태 $\hat{x_k}$로 만든다. CV-QNN이 hidden layer 일 경우 출력 값은 $\hat{h_k}$ 으로 나타내며 CV-QNN이 output layer 일 경우 출력 값은 $\hat{y_k}$ 로 나타낸다. hidden layer의 출력인 $\hat{h_k}$ 은 데이터의 무결성을 확인하는데 사용 가능하며 output layer의 출력인 $\hat{y_k}$의 예상 값은 $\hat{x_k}$과 결합하여 오류 함수를 형성하고 블록암호를 구성한다.



(그림 3) CV-QNN 의 암호화 과정.

결과적으로 CV-QNN을 암호화에 이용한 결과 고전적인 신경망 보다 높은 보안성과 암호화 프로세스 속도 향상을 실험으로 보였다[5].

IV. 결론

본 논문에서는 기존 인공신경망에 양자회로를 적용한 Quantum Neural Network (QNN)을 암호 분야에 적용한 연구들을 살펴보았다. 고전적인 인공 신경망에 양자회로를 적용하기 위한 방법을 이해하고 양자회로를 적용한 결과 보안성 및 암호화 프로세스의 속도를 모두 높일 수 있음을 결과를 통해 확인하였다. 이를 통해 QNN의 잠재력을 확인하고 앞으로 더 다양한 인공지능 보안 분야에 양자회로를 적용할 가능성을 볼 수 있었다.

V. Acknowledgment

이 논문은 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%) 그리고 부분적으로 2021년도 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%).

[참고문헌]

[1] Jaewoo So, "Deep Learning-Based Cryptanalysis of Lightweight Block Ciphers", Security and Communication Networks, vol. 2020, Article ID 3701067, 11 pages, 2020. https://doi.org/10.1155/2020/3701067

[2] Gohr Aron, “Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning.” Annual International Cryptology Conference. Springer, Cham, 2019

[3] Schuld, Maria, Ilya Sinayskiy, and Francesco Petruccione. "The quest for a quantum neural network." Quantum Information Processing 13.11 (2014): 2567-2586.

[4] Killoran, N., Bromley, T. R., Arrazola, J. M., Schuld, M., Quesada, N., & Lloyd, S. (2019). Continuous-variable quantum neural networks. Physical Review Research, 1(3), 033063.

[5] Shi, J., Chen, S., Lu, Y. et al. An Approach to Cryptography Based on Continuous-Variable Quantum Neural Network. Sci Rep 10, 2107 (2020). https://doi.org/10.1038/s41598-020-58928-1