정 보 보 호 학 회 지
제 31 권 제5호, 2021. 12

양자컴퓨터를 이용한 암호분석 최신동향

장 경 배*, 김 현 지*, 송 경 주*, 서 화 정**

요 약

본 고에서는 최근 급격히 발전하고 있는 양자컴퓨터와 이를 이용한 암호분석의 최신 동향에 대해 확인해 보도록 한다. 특히 양자컴퓨터를 이용한 블록암호에 대한 대표적인 공격 기법인 Grover 알고리즘과 최근에 연구가 진행되고 있는 양자 인공지능을 활용한 암호 공격에 확인해 보도록 한다.

Ⅰ. 서 론

2019년도 10월 구글에서는 오류율을 대폭 낮춘 54 큐빗 양자 프로세서 시커모어를 개발함과 동시에 해당 양자 프로세서 상에서 양자 우월성 달성이 가능함을 연구 논문을 통해 발표하였다. 이로써 양자컴퓨터가 현존하는 슈퍼컴퓨터의 최고 성능을 능가할 수 있음을 세계 최초로 객관화하였다[1]. 해당 연구 결과는 지금까지 실현 가능성이 낮을 것으로 간주되었던 양자컴퓨터의 실용적 특성을 전세계 연구자들에게 제시함으로써 앞으로 다가올 양자컴퓨터시대에 보다 집중할 수 있는 연구 분위기를 조성하였다고 볼 수 있다.

양자컴퓨터에 대한 개발은 전통적인 IT 기업인 구글, IBM, 아마존, 그리고 마이크로소프트를 중심으로 활발히 진행 중에 있다. 특히 구글과 IBM에서 양자컴퓨터를 실제로 만들뿐 아니라 이를 프로그래밍할 수 있는 양자컴퓨터 플랫폼까지 연계하는 작업을 선도적으로 수행하고 있다. 구글의 경우 일반연구자의 양자컴퓨터 그 자체에 대한 접근보다는 양자컴퓨터를 활용한 양자 알고리즘 기반 서비스에 집중하고 있다. 그 예시로는 2020년도에 제안된 TensorFlow Quantum이 있다[2]. TensorFlow Quantum을 활용하기 위해서는 구글에서 제공하는 Cirq라는 양자 프로그래밍 프레임워크를 사용한다. Cirq는 양자 컴퓨터 또는 시뮬레이션된 양자 컴퓨터에서 양자 회로를 생성, 수정 및 호출하기 위해 큐비트, 게이트, 회로 및 측정과 같은 연산을 제공한다. IBM의 경우 Qiskit 양자 프로그래밍 프레임워크를 제공하며 내부 양자 알고리즘 라이브러리를 통해 일반연구자들의 접근이 용이하도록 하고 있다. 2021년도 11월 IBM에서 세계최초로 100-큐빗의 한계를 뛰어넘는 127-큐빗 양자 프로세서 Eagle을 발표하였다. 양자컴퓨터의 성능을 나타내는 척도 중 하나인 큐빗의 개수는 양자큐빗의 품질도 중요하지만 기본적으로 큐빗이 높을수록 좋은 양자컴퓨터임을 나타낸다. 즉 IBM에서 양자컴퓨터의 큐빗 개수 관점에서는 현재 가장 기술이 진일보해 있다고 볼 수 있다[3]. IBM은 2023년도에는 1,121-큐빗의 양자 프로세서 Condor를 출시할 예정이며 이는 [표 1]과 같이 IBM의 양자프로세서 개발 로드맵에 잘 나타나 있다[4].

전세계 IT 기업들이 막대한 연구 비용을 양자컴퓨터에 투자하고 있는 이유는 추후 실용성을 가진 양자컴퓨터를 활용할 경우 인공지능, 시뮬레이션, 그리고 빅데이터 처리와 같은 최첨단 분야에서 지금까지 높은 연산 부하로 인해 불가능하였던 난제들을 해결하는 것이 가능할 것으로 예상하기 때문이다. 하지만 이러한 난제들에는 암호학이 기반을 두고 있는 인수분해와 같

〔표 1〕 IBM 양자컴퓨터 개발 로드맵

년도	19	20	21	22	23	30
Qubits	27	65	127	433	1,121	100 만 이상
Processor	Falcon	Hummingbird	Eagle	Osprey	Condor	-

본 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478).
* 한성대학교 IT융합공학부 (대학원생, starj1023@gmail.com, khj1594012@gmail.com ,thdrudwn98@gmail.com)
** 한성대학교 IT융합공학부 (조교수, hwajeong84@gmail.com)

은 문제들까지 포함하고 있어 양자컴퓨터의 개발은 암호분야에 있어 큰 위협으로 다가오고 있다.

1996년 Lov Grover는 n개의 분류되지 않은 데이터 상에서 특정 데이터를 찾아내는 양자 알고리즘을 개발하였다. Grover 알고리즘은 고전 컴퓨터에서 무차별 대입 시 최대 $O(2^n)$의 검색 횟수가 필요한 경우 Grover 알고리즘을 활용할 경우 최대 $O(2^{n/2})$만의 검색으로 결과를 찾을 수 있도록 하였다. 해당 알고리즘은 대칭키와 해시함수에 대한 가장 효과적인 공격으로 알려져 있으며 이를 이용한 활발한 암호 분석 연구가 진행 중에 있다[5].

최근들어 급격한 발달을 하고 있는 인공지능 기술을 활용한 암호분석 연구도 활발히 진행 중에 있다. 인공지능을 이용한 암호분석은 암호 알고리즘이 가진 무작위성 속에 내재되어 있는 규칙성을 대량의 데이터로부터 찾아내는 휴리스틱한 기법을 취하고 있다. 다만 무수히 많은 경우의 수를 가지는 암호 해석에 있어서 딥러닝과 같은 접근 방법은 높은 연산 부하와 메모리 사용량이라는 한계에 직면할 수 밖에 없는 문제를 가지고 있다. 이에 대한 해결책으로써 최근에는 양자컴퓨터 상에서의 인공지능이 활발히 연구되고 있다. 양자인공지능은 양자컴퓨터와 머신러닝 알고리즘을 결합한 기술로써 일반적으로 머신러닝 연산 시 필요한 데이터에 대한 분석을 양자컴퓨터 상에서 수행하는 것을 의미한다. 특히 양자컴퓨터의 특징을 이용하면 연산 속도와 데이터 저장공간을 향상시키는 것이 가능하다. Quantum Neural Networks (QNN)의 경우 양자 정보와 양자 연산을 기존 신경망 연산에 적용하는 것을 의미한다[6]. 연구 결과에 따르면 QNN의 경우 전통적인 컴퓨터에서 불가능했던 연산이 가능해 짐과 동시에 기존 신경망과 비교 시 연산 횟수, 큐빗, 그리고 연산 시간을 향상시킬 수 있을 것이다[7]. 현재 양자인공지능을 활용한 암호 분석을 연구 초창기 단계로써 많은 연구가 진행되지는 않았지만 이에 대한 관심과 기대는 점차 높아질 것으로 사료된다.

본 고에서는 양자컴퓨터를 이용한 전통적인 공격기법인 Grover 알고리즘에 대한 최신 연구 결과에 대해 확인해 봄과 동시에 양자컴퓨터 개발과 함께 본격화될 것으로 사료되는 양자인공지능을 통한 암호 분석 최신 동향에 대해 확인해 보도록 한다.

본 고의 구성은 다음과 같다. 2장에서는 Grover 알고리즘을 통한 암호 분석 최신 동향에 대해 확인해 보도록 한다. 3장에서는 인공지능을 통한 암호분석에 대해 확인해 보도록 한다. 4장에서는 본 고의 결론을 내리도록 한다.

Ⅱ. 그루버 알고리즘을 통한 암호분석

Grover 알고리즘은 양자 컴퓨터의 큐비트가 표현 가능한 범위의 모든 데이터를 가지고 있다는 양자 중첩 성질을 활용한다. Grover 알고리즘은 탐색 대상이 되는 데이터 집합에 Hadamard 게이트를 적용하여 양자 중첩 상태로 만든다. 양자 중첩으로 인해 n개의 데이터가 동시에 확률로서 존재하게 되고 Grover 알고리즘의 주요 모듈인 Oracle과 Diffusion operator를 사용하여 확인하고 싶은 데이터의 확률에 영향을 미침으로써 결과를 찾아낼 수 있다. 특정 데이터를 빠르게 찾아내는 Grover 알고리즘은 대칭키 암호에 대한 전수 조사 가속화에 활용될 수 있다. n-bit 키를 사용하는 대칭키 암호의 경우, 고전 컴퓨터는 키를 복구하기 위해 $O(2^n)$번의 탐색이 필요하지만 Grover 알고리즘을 활용하는 양자 컴퓨터는 약 $\sqrt{2^n} \cdot 2^{\frac{n}{2}}$번 만에 높은 확률로 키를 복구할 수 있다. 즉 n-bit 보안 강도를 제공하는 대칭키 암호의 보안 강도가 절반 ($\frac{n}{2}$)으로 감소하게 된다.

Grover 알고리즘을 양자컴퓨터 상에서 동작시키기 위해서는 목표로하는 암호화 알고리즘을 양자회로로 구현하는 것이 중요하다. 구현된 양자회로는 Oracle 모듈에 대입되어 Grover iteration을 수행하게 된다. 즉 양자컴퓨터 상에서 블록암호의 보안 강도를 나타내는 척도는 해당 블록암호가 양자회로로 쉽게 표현이 가능한지 아닌지로 재정의할 수 있다. 지금까지 많은 블록암호가 제시되며 전통적인 보안강도와 함께 고려되었던 부분이 소프트웨어 혹은 하드웨어 상에서 효율적인 구현 가능성이었다. 하지만 양자컴퓨터는 하드웨어 구현이 효율적으로 수행되는 블록암호의 경우 양자회로로의 구성이 용이하다는 특징으로 인해 양자컴퓨터 상에서는 보다 취약한 특징을 보이게 된다.

블록암호의 구조는 크게 Substitution-Permutation-Network (SPN)와 Addition-Rotation-XOR (ARX)로 나누어 볼 수 있다. SPN 구조는 S-layer를 통해 값을 변환하고 이를 P-layer를 통해 전체 메시지 블록에 확산시키는 특징을

〔표 2〕 SPN 구조와 ARX 구조 경량 암호의 양자 회로 구현 비용

알고리즘	Qubits	Toffoli gates	CNOT gates	X gates	Depth
PRESENT-64/128[9]	192	2,232	4,838	1,164	311
GIFT-64/128[9]	192	1,792	1,792	3,261	308
PIPO-64/128[10]	192	1,248	2,248	1,477	248
SIMON-64/128	192	1,408	7,396	1,216	2,643
SPECK-64/128	194	3,223	10,669	3,131	1,863
CHAM-64/128[8]	204	2,320	13,200	2,320	2,615
HIGHT-64/128[8]	228	5,824	22,614	4,496	2,479
LEA-128/128[8]	388	10,248	32,616	11,152	6,505

가지고 있으며 ARX의 경우 Addition을 통해 메시지에 대한 비선형성을 증가시키고 이를 Rotation을 통해 확산시키는 형식으로 수행하게 된다.

따라서 두 블록암호 구조에 대한 효율적인 양자회로 구현은 해당 구조 내에서 가장 복잡한 연산에 큰 영향을 받게 된다. SPN의 경우 S-layer 그리고 ARX의 경우 Addition 연산을 최적화 구현하는 것으로 귀결된다. 최근 SPN 구조 기반의 블록암호의 경우 S-layer를 하드웨어 상에서 경량으로 구현할 수 있는 4-비트 S-BOX 혹은 비트슬라이싱이 용이한 구조를 채택하고 있다. 하지만 이러한 구조는 양자회로로의 구현 또한 용이하기 때문에 적은 양자 자원을 통해서도 양자 회로 구현이 가능하다. Addition의 경우 다중의 큐빗에 대한 연산이 필요한데 여기서 각 큐빗간에 발생하는 올림값을 처리해 주기 위해 많은 양자 자원이 소모되게 된다. 최근에는 사물인터넷 장비에 적합한 경량성을 지님과 동시에 부채널 방어에 용이한 SPN에 대한 연구가 활발히 진행되고 있다. 하지만 이를 양자 컴퓨터 상에서의 공격에 대입할 경우 ARX 암호에 비해서 적은 자원으로 양자회로 설계가 가능한 SPN 암호가 보안 취약성을 가짐을 확인할 수 있다. 이에대한 구체적인 양자자원의 비교는 [표 2]에 나타나 있다. 따라서 추후 개발될 블록암호의 경우 양자컴퓨터 상에서의 Grover 알고리즘에 강인한 특성을 가지도록 설계되어야 할 것이다.

Ⅲ. 인공지능을 통한 암호분석

인공신경망은 컴퓨터를 학습시키기 위해 인간 뉴런의 동작 원리에 기초하여 컴퓨터 상에 이를 인공적으로 구축한 신경망이다. 인공신경망은 입력데이터의 특징을 추출하고 학습하여 분류 및 예측과 같은 작업을 수행할 수 있다. 신경망은 입력층, 출력층, 그리고 하나 이상의 은닉층으로 구성되며, 각 층은 여러 개의 노드로 이루어져 있다. 각 층의 각 노드들은 연결되어 있으며, 가중치를 가진다. 학습 시 입력 데이터가 신경망에 입력되고 연산은 입력층에서 출력층 방향으로 진행된다. 각 노드에서는 입력 값에 대해 비선형 함수인 활성화 함수를 적용한다. 해당 값이 임계값 이상인 경우 활성화되며 다음 층으로 전달한다. 신경망을 통과한 후 손실을 계산하고, 해당 값을 최소화하기 위해 역전파 과정을 거쳐 가중치를 갱신하며 입력 데이터에 대한 특징을 적절히 추출할 수 있도록 학습된다.

2018년도에 발표된 연구에서는 안전한 난수생성기를 제작하기 위한 용도로 인공신경망을 사용하였다[11]. 난수생성기에 대한 대표적인 공격으로는 생성될 난수의 값을 사전에 예측하는 것이다. 이는 난수생성기에 활용되는 source의 결정론적인 특징에 기인하게 된다. 이러한 결정론적인 특징을 인공신경망을 통해 확인하고 이에 대한 필터링을 통해 안전성을 확보한 Quantum Random Number Generators (QRNGs) 제작이 가능함을 보였다.

2020년도에 발표된 연구에서는 Simplified-DES, SIMON 32/64, 그리고 SPECK 32/64에 대해 평문과 암호문 쌍을 학습하여 사용된 키를 유추하는 known-plaintext 공격을 인공신경망을 통해 수행하였다[12]. 공격을 위해 무작위 키로 평문을 암호화하여 암호문을 생성하고 해당 평문과 암호문 쌍을 입력데이터로 하여 사용된 키 비트를 예측하도록 신경망 네트워크를 구성하여 학습하였다. 여기서 키 공간은 64개의 ASCII 문자로 제한하였고, S-DES (8-비트 평문과 10-비트 키), SIMON32/64, 그리고 SPECK32/64의 전체 라운드에 대한 암호 분석에 성공하였다. S-DES의 경우, $2^{8.08}$개의 알려진 평문 존재 시 90% 확률로 키를 예측하였으며, SPECK32/64는 $2^{12.34}$개의 알려진 평문 존재 시 99%의 확률로 56비트 키를 찾아낼 수 있었다.

〔표 3〕 고전 신경망과 양자 신경망 비교

특징	전통적인 신경망	양자 신경망
프레임 워크	Tensorflow, Pytorc	Qiskit, Tensorflow, cirq
주 연산	행렬 곱	행렬 곱 (양자 게이트)
매개변수	가중치, 바이어스	θ (큐비트 회전각)
활성화 함수	Relu, Swish 등의 비선형 함수	비선형 연산 사용 (양자 게이트)
최적화 함수	Adam, RMSProp	전통적인 신경망의 최적화 함수, SPSA, COBYLA, SLSQP

마지막으로 SIMON32/64에 대해서는 $2^{12.33}$개의 알려진 평문 존재 시 99% 확률로 56비트 키 예측에 성공하였다. 그러나 전통적인 신경망을 통한 알려진 평문 공격을 위해서는 많은 평문과 암호문 쌍 그리고 메모리가 필요하다는 한계점이 존재한다. 따라서 많은 데이터와 연산을 수행할 경우 높은 정확도를 확보할 수 있는 인공지능 기술에 있어 현재 컴퓨터 상에서는 분명한 한계점이 있음을 확인할 수 있다. 이러한 한계점을 돌파할 수 있을 것으로 사료되는 기술이 바로 양자컴퓨터 상에서의 양자인공지능이다.

양자신경망은 양자컴퓨터가 가지는 양자역학 현상(얽힘과 중첩)을 활용하여 인공지능 기술을 실현한 기술이다. 양자신경망은 양자 컴퓨터의 큐비트와 양자 게이트를 통해 구성되고 연산된다. 즉 해당 기술은 고전 컴퓨터의 신경망 대신 양자 회로를 사용함으로써 양자컴퓨터 상에서의 신경망 연산이 가능하도록 하는 기술이다. 고전 컴퓨터상의 데이터를 양자컴퓨터 상에서 연산하기 위해서는 해당 데이터를 큐비트를 이용하여 양자 상태로 인코딩한 후 양자회로를 통해 목적으로 하는 연산을 수행하는 형식을 취한다. 큐비트는 해당 양자회로를 거치며 상태가 변하며 최종적으로 동작이 완료되면 양자회로 상의 결과 값을 측정하고 손실을 계산하도록 한다. 여기서 파라미터화된 양자회로는 파라미터에 따라 큐비트 회전과 같은 연산이 수행되며 이는 매개변수에 따라 그 값이 변하기 때문에 갱신 및 학습이 이루어지게 된다. 기존 신경망에서 가중치 값을 갱신하는 역전파 과정처럼 양자 회로의 파라미터를 갱신하여 적절한 결과를 낼 수 있도록 수정한다. 고전 신경망과 양자신경망에 대한 비교는 [표 3]과 같다.

현재까지 양자인공지능을 통해 암호분석을 수행한 연구 결과는 많지 않은 상황이다. 최초로 Quantum Support Vector Machine (QSVM) 기반 암호 분석한 연구에서는 평문과 암호문 쌍을 입력하여 고전 암호의 키 값을 찾아내는 알려진 평문 공격을 양자 컴퓨터 상에서 수행하였다[13]. 데이터는 평문과 암호문 쌍으로 구성되었으며, 해당 데이터들을 암호화할 때 사용된 키 값을 Label로 지정 후 QSVM 기반 지도학습을 수행하여 키 값을 찾아내었다. 양자인공지능 적용을 위해 비트로 표현되는 초기 데이터를 양자 데이터 형식으로 변환해 주었다. 이를 저장하기 위해 각 평문과 암호문에 해당하는 각 비트들을 큐비트에 할당해 주고 중첩 상태를 만들기 위해 Hadamard 게이트와 회전 연산을 적용하여 양자 데이터로 인코딩을 수행하였다. 결과적으로 QSVM을 통해 설정한 Label로 분류되도록 지도학습을 수행됨을 결과적으로 확인할 수 있다.

실험 결과는 [표 4] 그리고 [표 5]와 같다. [표 4]에서는 양자 컴퓨터 시뮬레이터를 통해 수행한 결과이며 학습이 진행될수록 높은 정확도로 귀결됨을 확인할 수 있다. 다만 현재 가용가능한 양자컴퓨터 시뮬레이터의 큐빗의 한계로 인해 현대 암호에 대한 양자인공지능 분석은 용이하지 않은 시점이다. [표 5]에서는 실제 양자컴퓨터를 통한 연구 결과가 제시되어 있다. 주목할 점은 실제 양자컴퓨터를 활용할 경우 정확도가 감소한다는 점이다. 이는 현재 개발 중인 양자컴퓨터가 높은

〔표 4〕 시뮬레이터에서 키 예측 정확도

Shots	2-비트 데이터셋	3-비트 데이터셋
1	0.66	0.6
5	1.0	0.7
100	-	0.81
150	-	0.84

〔표 5〕 실제 양자 하드웨어 상에서의 키 예측 정확도 (2-비트 평문 및 암호문)

실행시간 (초)	정확도 (%)
780	93

안전성을 아직 확보하지 못함으로 인해 발생하는 오류로 볼 수 있다. 양자컴퓨터를 활용한 응용은 아직까지 안정화되지 않은 양자컴퓨터의 특징으로 인해 양자컴퓨터에 대한 연구 개발이 보다 활발히 진행되어야 할 것으로 사료된다.

Ⅳ. 결 론

본 고에서는 최근에 활발한 연구 및 개발되고 있는 양자컴퓨터로 인해 영향을 받고 있는 암호 분석 분야의 최신 동향에 대해 확인해 보았다. 양자컴퓨터는 기존 슈퍼컴퓨터와 전혀 다른 구조를 가지고 접근하기 때문에 새로운 양자기반 공격을 통해 기존에 안전성을 확보한 암호에 대해서도 신규 취약성을 찾아낼 수 있다. IBM 로드맵에 따라 양자컴퓨터 위협이 현실화 될 것으로 예상되는 근 10년 안에 양자컴퓨터와 암호에 대한 연구를 보다 활발히 수행하여 양자컴퓨터로부터 안전한 암호화 시스템 구축에 집중해야 할 것으로 사료된다.

참 고 문 헌

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, ..., J. M. Martinis, “Quantum supremacy using a programmable superconducting processor,” *Nature,* 574(7779), pp. 505-510, 2019.

[2] H. Alan, M. Masoud, "Announcing TensorFlow Quantum: An Open Source Library for Quantum Machine Learning," *Google Research,* available in https://ai.googleblog.com/2020/03/announcing-tensorflow-quantum-open.html, 2020.

[3] J. Chow, O. Dial, J. Gambetta, “IBM Quantum breaks the 100-qubit processor barrier,” *IBM Research Blog,* available in https://research.ibm.com/blog/127-qubit-quantum-processor-eagle, 2021.

[4] J, Gambetta, “IBM’s Roadmap For Scaling Quantum Technology,” *IBM Research Blog*, available in https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap, 2020.

[5] L. K. Grover, “A fast quantum mechanical algorithm for database search,” *In Proceedings of the twenty- eighth annual ACM symposium on Theory of computing,* pp. 212-219, 1996.

[6] A. A. Ezhov, D. Ventura, “Quantum neural networks,” *In Future directions for intelligent systems and information sciences*, pp. 213-235, 2000.

[7] S. Gupta, R. K. P. Zia, “Quantum neural networks,” *Journal of Computer and System Sciences*, 63(3), pp. 355-383, 2001.

[8] K. Jang, G. Song, H. Kim, H. Kwon, H. Kim, H. Seo, “Parallel Quantum Addition for Korean Block Cipher,” *Cryptology ePrint Archive*, 2021.

[9] K. Jang, G. Song, H. Kim, H. Kwon, H. Kim, H. Seo, “Efficient Implementation of PRESENT and GIFT on Quantum Computers,” *Applied Sciences*, 11(11), pp. 4776, 2021.

[10] K. Jang, G. Song, H. Kwon, S. Uhm, H. Kim, W. K. Lee, H. Seo, “Grover on PIPO,” *Electronics*, 10(10), 1194, 2021.

[11] N. D. Truong, J. Y. Haw, S. M. Assad, P. K. Lam, O. Kavehei, “Machine learning cryptanalysis of a quantum random number generator,” *IEEE Transactions on Information Forensics and Security*, 14(2), pp. 403-414, 2018.

[12] J. So, “Deep learning-based cryptanalysis of lightweight block ciphers,” *Security and Communication Networks*, 2020.

[13] H. Kim, G. Song, K. Jang, H. Seo, “Cryptanalysis of Caesar using Quantum Support Vector Machine,” *Cryptology ePrint Archive*, 2021.

〈저 자 소 개〉

장 경 배 (Kyungbae Jang)

학생회원

2019년 2월 : 한성대학교 IT응용시스템공학과 학사

2021년 2월 : 한성대학교 IT융합공학과 석사과정

2021년 3월~현재 : 한성대학교 IT융합공학과 박사과정

<관심분야> 양자 컴퓨터, 정보보안

김 현 지 (Hyunji Kim)

학생회원

2020년 2월 : 한성대학교 IT응용시스템공학과 학사

2020년 3월~현재 : 한성대학교 IT융합공학과 석사과정

<관심분야> 정보보안, 인공지능

송 경 주 (Gyeongju Song)

학생회원

2021년 2월 : 한성대학교 IT응용시스템공학과 학사

2021년 3월~현재 : 한성대학교 IT융합공학과 석사과정

<관심분야> 양자 컴퓨터, 정보보안

서 화 정 (Hwajeong Seo)

종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 학사

2012년 2월 : 부산대학교 컴퓨터공학과 석사

2016년 1월 : 부산대학교 컴퓨터공학과 박사

2016년 1월~2017년 3월 : 싱가포르 과학기술청

2017년 4월~현재 : 한성대학교 IT 융합공학부 조교수

<관심분야> 암호구현