정 보 보 호 학 회 지
제 33 권 제1호, 2023. 2

〈Q|Crypton〉: 암호 양자안전성 검증 기술

최 두 호*, 강 유 성**, 이 석 준***

요 약

현존 암호인프라에 대한 양자컴퓨터 위협이 가시화됨에 따라, 다각도의 양자리스크 대응 연구가 이루어지고 있다. 그 중에서 양자컴퓨터 상에서 주어진 암호를 해독하기 위해서 소요되는 양자자원량(큐비트수, 양자게이트수, 수행시간 등)을 계산하여 양자보안강도를 추정하는 양자안전성 검증 기술은 대규모의 큐비트를 컨트롤할 수 있는 범용 양자컴퓨터가 아직 없는 상태에서는 쉽지 않은 기술이라 할 수 있다. 이에, 본 고에서는 암호 양자안전성 검증을 위한 현실적이고 유일한 접근이라 할 수 있는 <Q|Crypton> 기술 개념을 설명하고, 이러한 개념을 바탕으로 개발되고 있는 <Q|Crypton> 플랫폼의 전반적인 설명을 제공하고자 한다. 이러한 <Q|Crypton> 기술은 향후, 효율적이면서 높은 양자 저항성을 가지는 암호를 선별하는 데 있어서 실제적인 기여를 할 것으로 예상되고 있다.

Ⅰ. 서 론

2022년 노벨물리학상은 양자컴퓨팅 및 양자키분배 분야에서 가장 중요한 개념인 양자얽힘에 대해 실험적으로 입증한 연구자 세명 – 알란 에스페, 존 클라우저, 안톤 차이링거 –에게 주어졌다. 이는, 최근 양자컴퓨팅 기술의 발전과 맞물리어 그 시사점이 크다고 할 수 있다. 또한, IBM에서는 433큐비트 양자칩 개발을 발표('22.11)[1]하는 등 현존하는 암호인프라의 붕괴시기가 점점 가까이 다가오고 있다는 점에서 이러한 양자컴퓨터에 의한 암호붕괴 위기는 피할 수 없는 양자리스크라 할 수 있다. 이러한 양자리스크에 대한 대비를 위해, 미국 NIST를 중심으로 2016년 양자내성암호(PQC, Post-Quantum Cryptography) 공모를 시작한 이래, '22년 4종의 표준문서 대상 PQC를 선정하고, 현재 표준문서 작업과 추가적인 4라운드 후보 선정 작업을 진행 중이다[2].

이제, 암호에 대해 기존의 비트기반 컴퓨터상에서 얼마나 안전한지를 검증하는 연구뿐만 아니라, 동시에 양자컴퓨터에서도 주어진 암호가 얼마나 안전한지 분석하고 검증하는 것 또한 중요한 연구 주제가 되고 있다고 볼 수 있다. 그러나, 양자 보안강도 검증은 기존의 컴퓨터상의 보안강도 검증과는 다르게 다음과 같은 어려움이 있다.

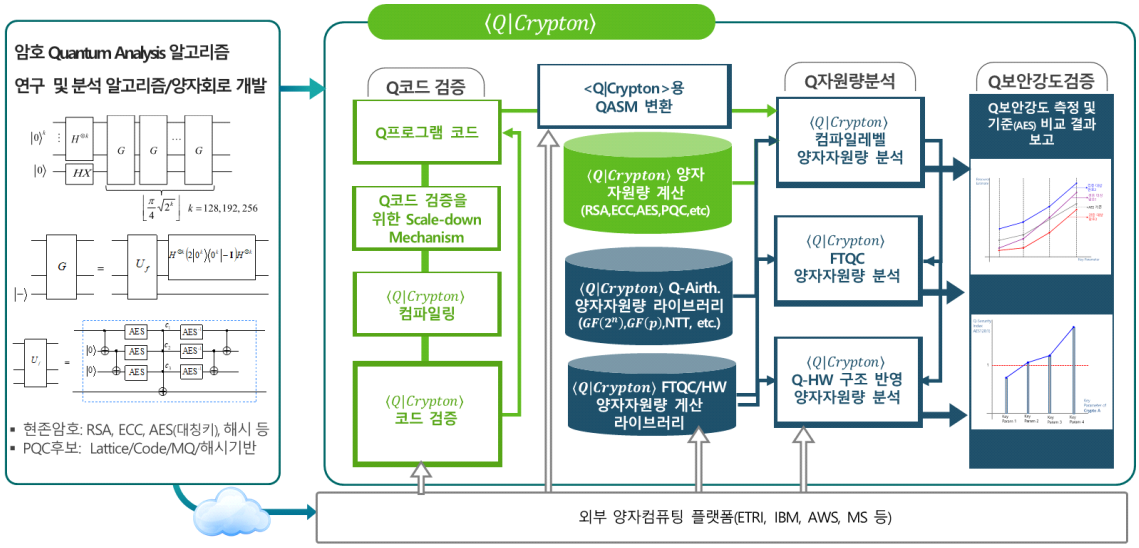
- 양자 보안강도 개념에 대한 공통적인 정의 부재: 양자컴퓨터 환경에서 보안강도를 어떻게 정의하고 비교할지에 대한 공통적인 기준이 없다.
- 대규모 범용 양자컴퓨터의 부재: 현재까지는 암호에 대한 양자 계산복잡도를 측정하고 추정할 정도의 수천~수백만 큐비트 규모의 양자컴퓨터가 아직 없다는 점이 양자 보안분석을 더욱 어렵게 한다.

이에, 본 고에서는 이러한 어려움들을 극복하고 현실적으로 양자보안성을 분석하고 검증할 수 있는 개념인 <Q|Crypton> 기술을 소개하고자 한다.

Ⅱ. 암호 양자 안전성 검증을 위한 <Q|Crypton> 기술

본 장에서는 우선, 암호 양자안전성 검증 플랫폼인 <Q|Crypton>의 개념에 대해 설명하고자 한다[그림 1]. <Q|Crypton>은 다음과 같은 프로세스 내지는 기술이 결합되어 암호 양자보안성을 검증하는 개념을 담고 있다고 할 수 있다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성 지원사업(IITP-2023-RS-2022-00164800), 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발(2019-0-00033)의 연구결과로 수행되었음.
* 고려대학교 세종캠퍼스 인공지능사이버보안학과 (교수, doohochoi@korea.ac.kr)
** 한국전자통신연구원 미래암호공학연구실 (실장, youskang@etri.re.kr)
*** 가천대학교 IT융합대학 컴퓨터공학부 스마트보안전공 (교수, junny@gachon.ac.kr)



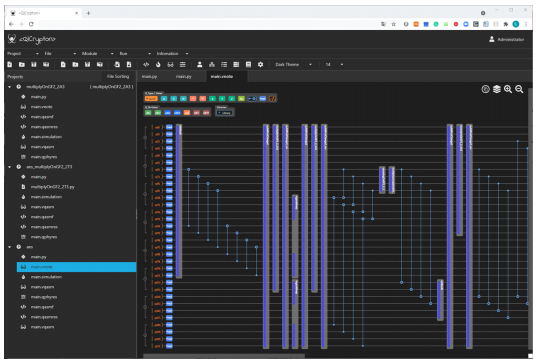
〔그림 1〕〈Q|Crypton〉 암호 양자안전성 검증 플랫폼 개념도

- PQC암호를 포함한 다양한 암호에 대한 최신 양자분석 알고리즘: 가장 최신의 개별 암호의 양자분석 알고리즘을 적용하여야 최적의 양자보안성을 검증할 수 있다.
- 암호 양자분석 알고리즘에 대한 양자회로 설계 및 구현: 다양한 외부 양자컴퓨팅 플랫폼 자원-예를 들어, ETRI 양자플랫폼, IBM 양자플랫폼 등-을 활용하여 주어진 암호 양자분석 알고리즘에 대한 양자프로그램 코드를 작성한다.
- Q코드 검증: 프로그램한 암호 양자분석 알고리즘 양자코드가 실제 제대로 프로그램된 양자코드인지를 검증을 수행해야 한다. 그러나, 현재까지 대용량 큐비트의 양자프로세서가 없기 때문에, 소규모 큐비트의 양자플랫폼(수십~수백 큐비트 양자칩 기반 또는 수십 큐비트 양자시뮬레이터 기반)을 활용하여 대규모 큐비트 Q코드를 검증하기 위해서는 다음과 같은 두가지 접근 방법이 있다. 첫 번째, QFT(Quantum Frourier Transform)과 같이 소규모 큐비트 버전으로 축소하여 검증하여 Q코드 검증을 할 수 있다. 두 번째는 소규모 큐비트 버전으로 축소가 불가능한 경우(대부분의 암호 양자분석 알고리즘은 이 경우에 해당함)에는 전체 Q코드를 구성하고 있는 소규모 양자회로별로 Q코드 무결성을 검증하여 전체 Q코드의 무결성을 검증하는 간접적인 방안이 있을 수 있다. 이렇게 두가지 방법을 동원하여 소규모 큐비트 양자플랫폼을 최대한 이용하여 Q코드 검증을 수행하게 된다.
- <Q|Crypton>용 QASM(Quantum Assembly Language) 변환: 양자프로그램을 수행한 양자플랫폼별로 다양한 양자어셈블리 코드를 획득할 수 있는데, <Q|Crypton>을 통해 양자자원량을 측정 및 추정하기 위해 <Q|Crypton>용 양자어셈블리 코드를 변환을 하게 된다. 이렇게 하면, 모두 공통의 Q-Arithmetic 라이브러리를 사용하게 되어, 양자자원량에 대한 상호 비교가 가능하게 된다.
- 양자자원량 분석: 이렇게 공통의 Q-라이브러리를 사용하여 양자자원량 상호 비교가 가능한 형태의 QASM로부터, 양자컴파일링 레벨, 결함허용 양자컴퓨팅(FTQC, Fault-Tolerant Quantum Computing) 레벨 및 양자칩의 구조를 반영한 Q-HW 레벨의 양자자원량을 계산하고 추정하여 주어진 암호 양자분석알고리즘에 대한 다양한 레벨의 양자자원량을 추정해주는 과정을 통해, 보다 구체적인 양자보안성 검증 기준을 수립할 수 있을 것이다.
- Q보안강도 검증: 상기 절차들을 통해 산출된 양자자원량 추정치를 기준으로, 첫째, 다양한 암호들 간의 양자보안성을 상호 비교할 수 있을 것이며, 둘째, 주어진 암호의 키파라미터별 양자자원량 추정치를 통해, 어떠한 키파라미터가 적절한 양자보안성을 담보하는지를 분석할 수 있을 것이다.

Ⅲ. <Q|Crypton> 플랫폼 소개

본 장에서는 II장에서 살펴본 암호 양자안전성 검증에 관한 개념을 구체화한 플랫폼인, <Q|Crypton> 플랫폼의 구성에 대해 살펴보고자 한다.<Q|Crypton> 플랫폼은 정확하고 정밀하게 양자안전성을 평가하기 위해, 암호 알고리즘을 공격하기 위해 필요한 양자 리소스를 분석해 준다.

<Q|Crypton> 플랫폼은 웹 기반 인터페이스를 통해 접속할 수 있도록 되어 있으며, [그림 2]는 <Q|Crypton> 플랫폼의 웹 화면을 보여주고 있다. <Q|Crypton>은 웹환경에서 운영되며, 중심적인 기능들의 대부분은 서버에서 수행되는 구조로 되어 있기 때문에 사용자측에서는 웹접속외에 추가 프로그램은 요구받지 않는다. <Q|Crypton>은 필요한 양자회로를 시각적으로 설계하는 것도 가능하면, 파이선 기반의 프로그래밍을 통해 설계하는 것도 가능한 환경을 제공하고 있다. 설계가 완료된 양자회로를 라이브러리로 등록하여 추후에 등록한 양자회로 라이브러리를 재사용할 수 있는 환경도 제공되고 있다.

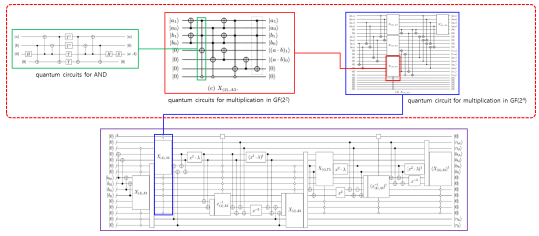


〔그림 2〕〈Q|Crypton〉 플랫폼 사용자 화면

3.1. <Q|Crypton>을 통한 암호 양자자원량 분석 방법

주어진 암호에 양자분석 알고리즘이 있을 때, <Q|Crypton> 플랫폼을 이용하여 다음과 같은 절차를 통해 암호 양자분석에서 소요되는 양자자원량을 추정하게 된다.

(1) 먼저 주어진 암호에 대한 양자분석 알고리즘이나 핵심이 되는 양자회로를 준비한다(그림 3 참고).



〔그림 3〕 AES S-box inversion 양자회로[3]

(2) 주어진 양자회로를 <Q|Crypton>의 시각화 프로그래밍 도구(Q-VisNOTE)나 파이선 코딩 환경을 이용하여 양자 프로그램밍을 한다(그림 4 참고).

이때, 양자알고리즘에서 필요한 Q-Arithmetic은 <Q|Crypton> 라이브러리에서 불러내어 사용할 수 있다(그림 5 참고).

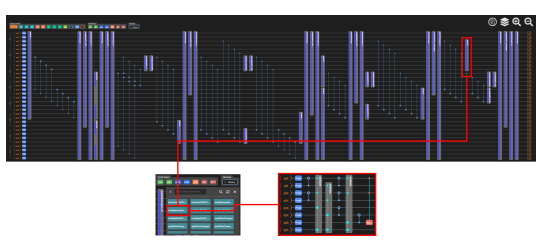
(3) 이렇게 프로그래밍한 양자회로 코드를 양자컴파일하여 <Q|Crypton>용 QASM 코드로 변환한다(그림 6 참고).

(4) 이제 QASM 코드를 <Q|Crypton> 양자시뮬레이터(Q-VM)를 통해 실행하여 제대로 프로그램된 양자코드인지를 검증한다(그림 7 참고).

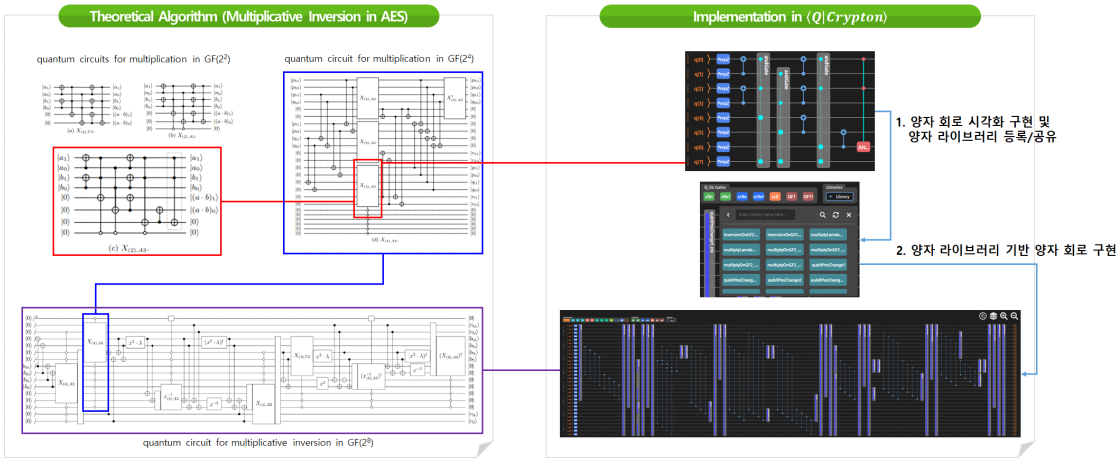
이때, 프로그래밍한 양자코드에서 사용되는 큐비트가 약 30여 큐비트 이상되는 경우에는 Q-VM을 통한 코드 검증이 불가능하기 때문에, 주어진 양자회로의 부분 회로들을 실행하여 코드 검증을 수행할 수 있다.

(5) 이렇게, 프로그램한 양자코드가 제대로 된 코드임을 확인한 후, 양자자원량 분석을 수행할 수 있다. 양자자원량 분석을 위해, <Q|Crypton> 플랫폼에서는 다음과 같은 선택사항들을 제공하고 있다.

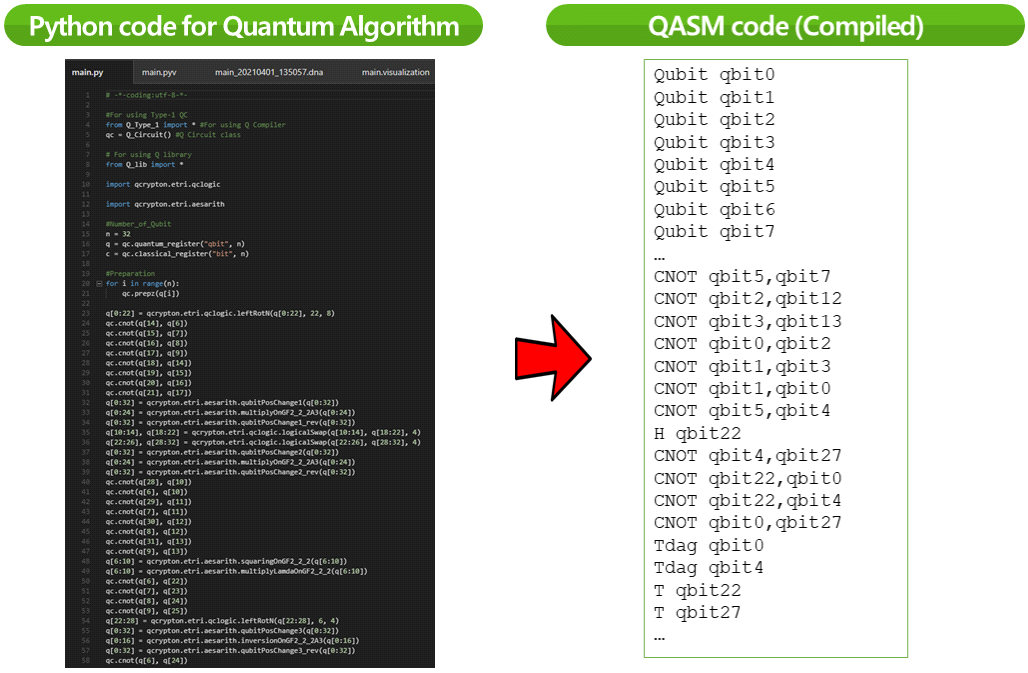
- 양자에러정정코드 선택: QEC(Quantum Error Correction)를 사용하지 않는 옵션과 함께, Steane코드 및 Surface코드를 선택할 수 있는 옵션을 제공하



〔그림 4〕 Q-VisNOTE를 통한 양자프로그래밍



〔그림 5〕 주어진 양자회로에 대한 Q-Arithmetic 라이브러리 적용 화면



〔그림 6〕 양자프로그램 코드를 양자컴파일하여 변환된 〈Q|Crypton〉 QASM 코드 예

고 있다.

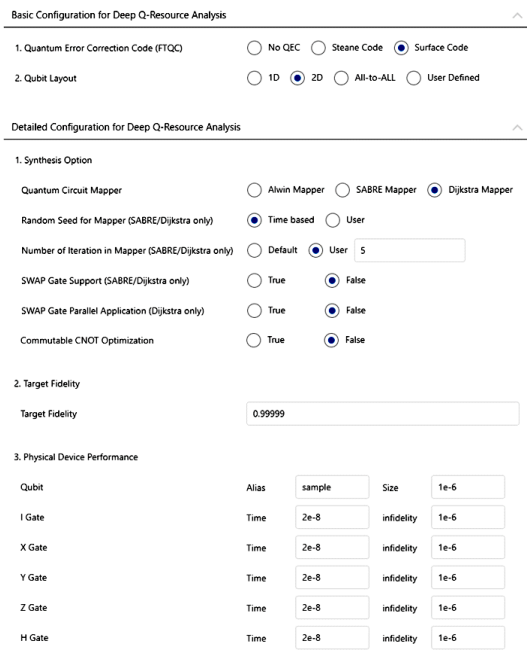
- 큐비트 레이아웃 선택: 1-차원, 2-차원, 그리고 모든 큐비트들이 서로 상호작용할 수 있는 모델(All-to-All)를 제공하고 있으며, 추가적으로 개별 양자프로세서에 맞게 사용자가 큐비트 레이아웃을 설정할 수 있을 옵션도 제공하고 있다.
- 그 외, 합성 옵션 및 물리적 디바이스의 성능 관련 옵션도 제공하고 있다(그림 8 참고).

(6) 이제, 옵션 선택 후, 양자자원량 분석을 수행하게 되면, [그림 9]와 같은 상세한 양자자원량 분석 결과를 얻을 수 있다. 이때, 기본적인 논리큐비트 및 논리게이트 수준의 양자자원량뿐 아니라, 선택한 옵션을 기반으로 한, 물리큐비트 및 물리게이트 사용량에 대한 추정 결과까지 얻을 수 있는 것이 본 <Q|Crypton> 플랫폼의 타 플랫폼과 차별되는 양자자원량 분석결과라고 할 수 있다.

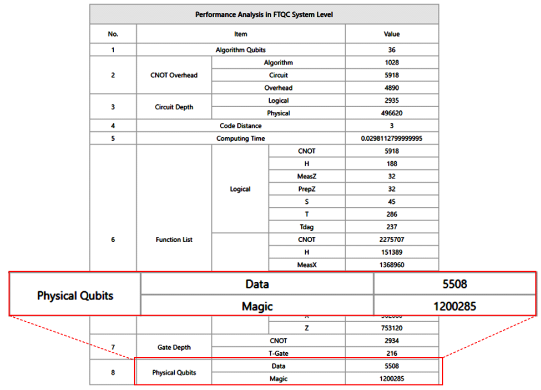
Execution in Q-VM

```
PrepZ qbit0
+(1.0+0.0i)|0000000000000000000>
...
X qbit2
+(1.0+0.0i)|0010000000000000000>
...
X qbit4
+(1.0+0.0i)|0010100000000000000>
...
X qbit5
+(1.0+0.0i)|0010110000000000000>
...
Tdag qbit1
+(1.0+0.0i)|0010110000000000000>
...
H qbit2
+(0.707107-0.707107i)|
0010110000000000000 >
+(0.707107+0.707107i)|
0000110000000000000 >
...
CNOT qbit5,qbit7
+(0.707107-0.707107i)|
0010110100000000000 >
+(0.707107+0.707107i)|
0000110100000000000 >
```

〔그림 7〕 Q-VM을 통한 양자회로 실행 결과 화면



〔그림 8〕 양자자원량 분석을 위한 선택 항목 화면



〔그림 9〕 〈Q|Crypton〉을 통한 양자자원량 분석결과

3.2. <Q|Crypton> 플랫폼 특징

3.1 절에서 설명한 <Q|Crypton> 플랫폼을 통한 양자자원량 분석 절차를 바탕으로 <Q|Crypton> 플랫폼을 특징을 요약하면 다음과 같다.

- 주어진 양자알고리즘 및 양자회로에 대한 시각화 양자프로그램 환경을 제공한다.
- 암호 양자분석에 필요한 Q-Arithmetic들에 대한 공통 라이브러리 사용환경을 제공한다. 이를 통해, <Q|Crypton>내에서 공통의 Q-Arithmetic 라이브러리를 사용하여 양자자원량을 분석할 수 있기 때문에, 표준적인 양자보안강도 비교가 가능할 것으로 예상된다.
- 논리큐비트 및 논리게이트 수준에서의 양자자원량 측정뿐 아니라, 양자에러정정 및 양자프로세서의 구성에 맞는 물리큐비트 및 물리게이트 수 등에 대한 자원량 추정 결과를 제공함으로써, 기존의 이론적인 복잡도보다 엄밀한 계산복잡도를 분석하고 비교할 수 있다.

Ⅳ. 향후 연구 계획

암호 양자안전성 검증을 위해서는 궁극적으로는 다음 두가지에 대한 엄밀한 추정이 가능하여야 한다고 볼 수 있다. 첫째, 기준이 되는 AES나 SHA의 양자자원량 추정치와 분석 대상이 되는 암호의 양자자원량 추정치를 비교 가능하여야 한다. 이를 통해, 주어진 암호가 어느정도의 양자보안성을 가지는 추정할 수 있게 된다. 둘째는 주어진 암호의 키 파라미터별로 양자분석 양자자원량이 어떻게 변화하는지를 추정할 수 있어

야 한다. 이를 통해, 주어진 암호에 대한 안전한 양자보안성을 주기 위해 어떤 키 파라미터를 사용해야 하는지에 대한 정보를 제공할 수 있다.

따라서, 향후에는 <Q|Crypton> 플랫폼의 엄밀한 양자자원량 분석 결과들을 추이와 엄밀한 예측을 통해 상기 두가지를 제공하여 양자보안성을 엄밀하게 검증할 수 있는 기술이 될 수 있도록 해야 할 것이다.

Ⅴ. 결 론

본 고에서는 암호 양자안전성 검증을 위한 현실적이고 유일한 접근이라 할 수 있는 <Q|Crypton> 기술 개념을 설명하고, 이러한 개념을 바탕으로 개발되고 있는 <Q|Crypton> 플랫폼에 대한 소개 및 <Q|Crypton> 플랫폼을 이용하여 암호 양자자원량 분석을 하는 절차를 설명하였다. 또한, <Q|Crypton>은 논리큐비트 및 논리게이트 수준의 양자자원량뿐만 아니라, 양자에러정정을 포함하는 물리큐비트 및 물리게이트 소요량에 대한 분석 결과도 제공하고 있기 때문에, 보다 엄밀한 암호 양자보안성을 검증할 수 있는 검증 도구로 활용될 수 있을 것으로 생각되며, 향후, 효율적이면서 높은 양자저항성을 가지는 암호를 선별하는 데 있어서 실제적인 기여를 할 것으로 예상되고 있다.

참 고 문 헌

[1] IBM, “IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two”, https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

[2] NIST, “PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates”, https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

[3] D. Chung, S. Lee, D. Choi, and J. Lee, “Alternative Tower Field Construction for Quantum Implementation of the AES S-box”, IEEE Transactions on Computers, vo. 71, no. 10, pp 2553-2564, 2021

〈저자소개〉

최 두 호 (Dooho Choi)

종신회원

1994년 2월 : 성균관대학교 수학과 졸업
1996년 2월 : KAIST 수학과 석사
2002년 2월 : KAIST 수학과 박사
2002년 1월~2021년 2월 : 한국전자통신연구원 정보보호연구본부 실장
2021년 3월~현재 : 고려대학교 세종 인공지능사이버보안학과 교수

<관심분야> 암호 양자분석, 부채널분석, IoT보안, 암호엔지니어링

강 유 성 (Yousung Kang)

종신회원

1997년 2월 : 전남대학교 전자공학과 졸업
1999년 8월 : 전남대학교 전자공학과 석사
2015년 8월 : KAIST 전기및전자공학부 박사
1999년 11월~현재 : 한국전자통신연구원 정보보호연구본부 실장/책임연구원
2011년 1월~2012년 4월 : 영국 북아일랜드 퀸즈대학교 방문연구원

<관심분야> 암호 양자분석, 부채널 분석, IoT/드론 보안, 암호엔지니어링

이 석 준 (Sokjoon Lee)

종신회원

1998년 2월 : 서울대학교 컴퓨터공학과 졸업
2000년 2월 : 서울대학교 컴퓨터공학과 석사
2019년 8월 : KAIST 전산학과 박사
2000년 2월~2022년 2월 : 한국전자통신연구원 정보보호연구본부 책임연구원/PL
2022년 3월~현재 : 가천대학교 IT융합대학 컴퓨터공학부 스마트보안전공 교수

<관심분야> 암호 양자분석, 암호엔지니어링, 제로트러스트, 위험관리