정 보 보 호 학 회 지
제 33 권 제2호, 2023. 4

양자컴퓨터를 통한 대칭키 및 공개키 해킹 동향

오 유 진*, 양 유 진*, 장 경 배*, 서 화 정**

요 약

양자 알고리즘이 구동 가능한 양자 컴퓨터는 현대 암호들이 기반하고 있는 수학적 난제들을 빠르게 해결할 수 있다, 대칭키 암호의 경우, Grover 알고리즘을 사용한 전수조사 가속화가 가능하며, 공개키 암호의 경우, Shor 알고리즘을 사용하여 RSA와 ECC가 기반하고 있는 난제들을 다항시간 내에 해결할 수 있다. 이에 다양한 대칭키 암호, 그리고 RSA와 ECC의 양자 해킹 방법론에 대한 연구들이 수행되고 있다. 물론 양자컴퓨터의 제한적인 성능으로 인해 실제 해킹이 가능한 수준은 아니지만, 양자 공격 회로를 제시하고 그에 필요한 양자 자원들을 분석하는 방식으로 실제 해킹 가능성에 대해 추정해 보는 연구 결과들이 발표되고 있다. 이에 본 기고에서는 양자 컴퓨터를 통한 대칭키 및 공개키 암호 해킹 동향에 대해 살펴보고자 한다.

Ⅰ. 서 론

국가 및 국제 대기업이 양자 컴퓨터의 개발에 앞장섬에 따른 그 성능 발전이 빠르게 이루어지고 있다. 양자 컴퓨터는 인공지능, 시뮬레이션, 화학에서의 특정 컴퓨팅 분야의 난제들에 대해 다른 차원의 해결 능력을 보여줄 것으로 기대되고 있다. 이는 양자 컴퓨터에서 사용하는 양자 비트인 큐비트의 양자 역학 성질 때문이다. 대표적으로 큐비트의 양자 중첩과 양자 얽힘이 그러하다. 양자 중첩이란 0과 1을 블로흐 구면에서 표현함으로써 고전 컴퓨터에서는 비트가 0 또는 1로 확정되는 반면, 큐비트는 0과 1이 확률로서 존재하는 성질이다. 이를 통해 n개의 큐비트는 2^n개의 경우의 수를 확률로써 표현할 수 있다. 양자 얽힘이란 과거에 상호작용 했던 큐비트라면, 어느 한 큐비트의 상태 변화가 얽혀 있는 다른 큐비트의 상태 변화에 영향을 미치는 성질이다. 이러한 양자 역학적 성질을 사용하는 양자 컴퓨터는 다른 측면으로는 암호 학계의 보안성을 위협하고 있다.

양자 알고리즘인 Grover 알고리즘 [1]과 Shor 알고리즘 [2]을 동작시킬 수 있는 고성능의 양자 컴퓨터가 개발되는 시점에서 대칭키 암호의 경우, 고전 컴퓨터상에서 보장되던 보안 강도가 제곱근만큼 감소하게 되고, 공개키 암호의 경우, 널리 사용되고 있는 RSA와 ECC (Elliptic Curve Cryptography)의 수학적 난제가 해결될 수 있다.

다시 설명하자면 대칭키 암호의 경우, Grover 알고리즘을 사용하여 전수 조사를 수행하면, 보안 강도가 제곱근만큼 감소하게 된다. 다행히 키의 길이를 2배 증가시킴으로써 기존의 보안강도를 유지할 수 있다. 반면, 공개키 암호의 경우 기반 수학적 난제가 해결되기 때문에 완전한 교체 이외에는 해결책이 존재하지 않는다. 양자 알고리즘인 Shor 알고리즘은 고전 컴퓨터상에서의 난제인 소인수 분해 문제와 이산대수 문제를 다항 시간 내에 해결할 수 있다. 따라서 파라미터의 증가와 관계없이 해당 난제들에 기반하고 있는 RSA와 ECC의 보안성이 완전히 무너지게 된다. 이러한 암호 시스템의 붕괴 위협에 대비하여 NIST (National Institute of Standards and Technology)에서는 양자내성암호를 표준화하기 위한 공모전을 주최하였다. 현재 공개키/KEM (Key Encapsulation Mechanism)의 경우 격자기반암호인 CRYSTAL-Kyber가 표준화 되었으며,

본 연구는 2023년도 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%) 그리고 본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%).

* 한성대학교 IT융합공학과 (대학원생, oyj0922@gmail.com, yujin.yang34@gmail.com, starj1023@gmail.com)
** 한성대학교 융합보안학과 (부교수, hwajeong84@gmail.com)

전자 서명에는 격자기반의 CRYSTAL- Dilithium, FALCON 그리고 해시기반의 SPHINCS+가 표준화된 상태이다. NIST는 공개키/KEM 분야에 격자기반문제가 아닌 다른 수학적 문제에 기반 한 암호 알고리즘을 표준화하기 위해 추가적으로 Round 4를 진행 중이다.

기술 개발의 한계로 인해, 아직 양자 컴퓨터를 사용하여 현대 암호들을 해킹할 순 없지만 잠재적인 양자 공격에 대해 연구하는 것은 안전한 양자내성암호 체계 구축을 위해 반드시 필요하다. 이에 다양한 양자 암호 분석 연구들이 발표되고 있다. 양자 암호 분석 연구의 경우, 대상 암호 알고리즘에 대한 양자 공격 회로를 제시하고, 구현에 필요한 양자 자원들을 추정하는 방식으로 수행된다. 이에 본 기고에서는 양자 컴퓨터를 사용한 대칭키, 공개키 암호에 대한 해킹 관련 동향을 살펴보고자 한다.

Ⅱ. 관련 연구

2.1. Grover 알고리즘

양자 알고리즘인 Grover 알고리즘은 N개의 데이터 집합에서 특정 데이터를 $\sqrt{N}$번 만에 높은 확률로 찾아낼 수 있다. 고전 컴퓨터에서는 $O(N)$의 복잡도인 것과 비교하면 제곱근만큼 줄어드는 것이다. 이에 n-bit 키를 사용하는 암호에 대한 고전 컴퓨터를 사용한 전수 조사는 $O(2^n)$의 복잡도를 가지지만, Grover 알고리즘을 사용하는 양자 컴퓨터의 경우 $2^{n/2}$번 만에 높은 확률로 키를 복구할 수 있다. 즉, 보안 강도가 제곱근만큼 감소하게 되지만, 다행히 키의 길이를 두 배로 늘리면, 고전 컴퓨터상에서 주장하던 보안 강도를 양자 컴퓨터상에서도 주장할 수 있다.

2.2. Shor 알고리즘

1994년 Peter Shor에 의해 제안된 Shor 알고리즘은 지수 시간이 소요되는 소인수 분해 문제와 이산대수 문제를 다항 시간에 풀 수 있게 돕는다. 이러한 Shor 알고리즘의 핵심은 인수분해 문제를 주기 찾기 문제로 바꾸게 된다.

$$f(x) = a^r \bmod N \ (0 \le r < N) \quad (1)$$

$$a^r \equiv 1 (\bmod N) \quad (2)$$

수식 (1)은 두 소인수의 곱인 큰 정수 N의 주기 r을 찾기 위한 주기 함수이다. 주기를 찾기 위해선 수식 (2)를 만족하는 r을 찾아야 한다. 여기서 a는 N과 서로소 관계인 임의의 정수로 r이 짝수가 아닌 경우 다시 선택된다. r이 짝수이면 공식에 따라 $a^r - 1 = (a^{r/2}-1)(a^{r/2}+1)$로 인수분해가 가능하기에 이 공식을 이용하여 N의 소인수 분해를 보다 쉽게 할 수 있다. 그런데 조건을 만족하는 가장 작은 자연수 주기 r을 찾는 일은 고전 컴퓨팅 환경에서 지수 시간이 소요된다. 해당 문제는 양자 컴퓨터와 양자 푸리에 변환 적용을 통해 해결할 수 있다.

양자 푸리에 변환은 시간 영역의 함수를 주파수 영역의 함수로 변환해 주는 수학적 연산인 푸리에 변환을 양자 상태에 작용한 것이다. 이 단계에서는 $f(x)$의 위상을 추정하고 역 양자 푸리에 변환을 통해 측정할 수 있는 계산 기반으로 변환 후 측정을 수행하여 고윳값 $e^{2\pi i\phi}$에 포함된 주기를 얻는다. Shor 알고리즘 과정 중 주기 r을 찾는데 소요되는 시간은 양자 컴퓨터의 개발과 양자 푸리에 변환의 적용을 통해 다항 시간으로 줄일 수 있다.

2.3. NIST 양자 후 보안 강도 평가 [3]

NIST는 AES와 SHA-2/3에 대한 양자 공격에 필요한 비용을 기준으로, 암호의 양자 후 보안강도를 추정하고 있다. 특정 암호를 양자 해킹하는데 필요한 비용이 AES와 SHA-2/3를 양자 해킹하기 위한 비용과 비교함으로써 양자 후 보안 강도를 평가할 수 있으며 구체적으로는 [표 1]과 같다. 양자 공격에 필요한 복잡도는 양자 회로의 크기로 측정되며, 양자 회로의 크기는 총 양자 게이트 수와 회로 depth를 곱하여 산정된다. Level 1, 3, 5에 해당하는 AES에 대한 양자 공격 복잡도의 경우, 2016년도의 Grassl et al.의 AES 양자 공격 비용 추정 연구 [4]를 인용하고 있다. 따라서, AES-128 (Level 1)에 대한 공격 비용은 Grover 알고리즘을 사용하는 키 복구 회로의 총 게이트 수 × depth인 2^{170}이며 AES-192는 2^{233}, AES-256은 2^{298}으로 측정된다.

〔표 1〕 NIST 양자 후 보안 강도 평가

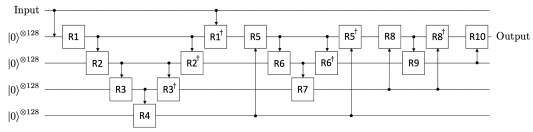
Security	Requirements
Level 1	Attack complexity requirements for quantum hacking of AES-128 or higher
Level 2	Attack complexity requirements for quantum hacking of SHA256/SHA3-256 or higher
Level 3	Attack complexity requirements for quantum hacking of AES-192 or higher
Level 4	Attack complexity requirements for quantum hacking of SHA384/SHA3-384 or higher
Level 5	Attack complexity requirements for quantum hacking of AES-256 or higher

Ⅲ. 양자 컴퓨터를 통한 대칭키 해킹 동향

Grover 해킹 비용은 오라클 내부의 암호화 양자 회로가 얼마나 효율적으로 구현되었느냐에 따라 결정된다. 이에 다양한 대칭키 암호들을 양자 회로 상에서 효율적으로 구현하기 위한 연구들이 수행되고 있다. 본 장에서는 AES를 중심으로, Grover 해킹을 위해 제시된 다양한 양자 회로 구현들에 대해 살펴본다.

3.1. Grassl et al.의 AES 양자 회로 구현

2016년, Grassl et al.은 최초로 AES 양자 회로 구현을 제시함으로써 Grover 해킹에 필요한 양자 비용을 추정하였다. AES에서 가장 많은 양자 비용이 요구되는 연산은 S-box 연산이다. Grassl et al.은 S-box 양자 회로 구현을 위해 유한체 $\mathbb{F}_{2^8}(x)/(x^8+x^4+x^3+x+1)$ 상에서의 역치연산을 양자 회로로서 구현하였다. 곱셈과 제곱의 조합으로 지수 승을 계산하는 Itoh-Tsujii 기반의 역연산이 구현되었다. 양자 컴퓨터상에서 곱셈 연산이 높은 비용을 차지하기 때문에 구현된 AES 양자 회로에서 대부분의 양자 자원들이 S-box 구현에 사용되었다. MixColumn의 경우, 선형 연산으로 분류되기 때문에 (32 × 32)의 선형 행렬에 대한 PLU 분해를 통해, MixColumn의 입력 값인 32-qubit이 그대로 출력 값으로 변경되는 in-place 구현이 제시되었다. AES 양자 회로를 설계하는데 있어 큐비트 수를 감소시키기 위한 [그림 1]의 Zig-zag 아키텍처가 제시되었



〔그림 1〕 Zig-zag 아키텍처

는데, 해당 아키텍처는 현재까지의 연구들에서도 자주 채택되며 개선되고 있다. 아키텍처가 중요한 이유는 8-qubit 입력의 S-box의 output을 새로운 8-qubit에 저장해야 되기 때문이다. 즉, 라운드마다 128-qubit 중간 값에 대한 S-box들의 output을 저장하기 위한 128-qubit이 새롭게 할당되어야 하는 것이다. Zig-zag 아키텍처는 전 라운드에서 새롭게 할당한 128-qubit을 재사용하는 방식이다. 이를 위해 이전 라운드들을 거꾸로 (Reverse) 수행하여 할당한 128-qubit을 0 값으로 초기화시켜 다음 라운드에서 재사용한다.

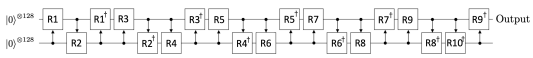
Grassl et al.은 제일 먼저 구현된 만큼, 최근 구현들과 비교하였을 때, 성능이 매우 낮다. 가장 큰 이유는 S-box를 구현하는데 있어 내부 연산인 유한체의 역치연산을 그대로 양자 회로로서 구현하였기 때문이다. 최근 구현들은 S-box 구현을 최적화 하는 방식으로 그 비용을 크게 줄이고 있다.

3.2. Langenberg et al.의 AES 양자 회로 구현 [5]

Langenberg et al.은 AES 양자 회로의 S-box를 구현 비용을 크게 감소시켰다. S-box의 유한체 지수 승 연산을 구현하는 것이 아닌, Boyer-Peralta의 AES S-box 하드웨어 최적화 구현을 선택하였다. 때문에 높은 비용의 양자 곱셈을 구현하는 것이 아닌, 32개의 AND 게이트와 83개의 XOR/XNOR 게이트를 양자 회로상에서 구현하였다. 이를 통해 회로 depth와 게이트 수를 크게 감소시킴으로써 Grover 공격 비용 또한 크게 감소시켰다.

3.3. Zou et al.의 AES 양자 회로 구현 [6]

Zou et al.은 AES 양자 회로에 대한 개선된 Zig-zag 아키텍처를 제시함으로써 큐비트 수를 크게 감소시켰으며 해당 연구 결과는 Asiacrypt'20에서 발표되었다. [그림 1]의 Zig-zag 아키텍처의 경우 Input을 제외하고 4개의 128-qubit 라인들이 사용되지만, 해당 구현에서는 [그림 2]와 같이 1개의 128-qubit



〔그림 2〕 개선된 Zig-zag 아키텍처

layer만이 사용되는, 개선된 Zig-zag 아키텍처를 제시하였다. Zou et al.은 Boyer-Peralta의 S-box 구현을 수정함으로써 필요 큐비트 수를 일차적으로 감소시켰으며 S-box^{-1} 양자 회로를 추가적으로 사용함에 따라 Input과 128-qubit 1개의 라인만을 교대로 S-box 출력 값을 초기화 시키고 다음 라운드를 수행하는 방식을 가능케 하였다. 하지만 [그림 2]에서 볼 수 있듯이, 개선된 Zig-zag 아키텍처는 필요 큐비트 수를 감소시킬 순 있지만, Input, 128-qubit 이 두 라인만을 사용함에 따라 회로 depth가 기존 Zig-zag 아키텍처보다 크게 증가한다는 단점이 있다.

3.4. Jaques et al.의 AES 양자 회로 구현 [7]

기존 연구들이 모두 큐비트 수를 줄이는데 초점을 맞추었다면, Jaques et al.은 양자 회로의 depth를 줄이는 데 초점을 맞추었다. 가장 큰 특징은 Grassl et al.의 양자 회로부터 사용된 Zig-zag 아키텍처에서 벗어났다는 것이다. 오히려 일반적인 Pipeline 아키텍처를 선택함으로써, 매 라운드마다 새로운 128-qubit을 매번 할당하지만 reverse 연산이 불필요해짐으로써 회로 depth를 크게 줄일 수 있었다. 최종적으로 해당 논문에서는 적절한 큐비트 수를 유지하면서 낮은 공격 비용이 제시되었지만, 이후 사용된 Microsoft Q#의 자원 추정기의 오류로 인해 추정된 자원이 불일치하는 것으로 보고되었다.

3.5. Huang et al.의 AES 양자 회로 구현 [8]

Huang et al.은 Boyer-Peralta의 S-box 구현을 수정함으로써 낮은 Toffoli depth를 가지는 AES S-box를 제시하였다. 기존 Boyer-Peralta의 구현을 그대로 양자 회로 상에서 구현하면 Toffoli depth가 6이지만, 해당 구현에서는 Toffoli 게이트들을 동시적으로 실행 시키도록 기존 연산들을 수정함으로써 AND 연산의 동기화를 수행하였다. 이를 통해 Toffoli depth가 3, 4인 두 가지 새로운 S-box 구현을 제시하였다. 회로 전체 아키텍처는 Zou et al.의 개선된 Zig-zag 아키텍처를 선택하였다.

3.6. Jang et al.의 AES 양자 회로 구현 [9]

Jang et al.은 Jaques et al.의 AES 양자 회로 구현 오류를 분석하고 수정하여 올바른 자원을 추정하였다. Jaques et al.의 논문에 보고된 큐비트-depth의 비일관성을 수정하기 위해, 큐비트 수가 유지되었을 때 실제로 어느 만큼의 depth를 가지는지 보고하였다. 또한 낮은 Toffoli depth와 full depth를 가지는 AES 양자 회로 구현을 제시하였다. Huang et al.의 Toffoli depth 3, 4 S-box를 선택함과 동시에, 개선된 Pipeline 아키텍처를 제시하여 S-box와 S-box에 대한 reverse 연산을 동시에 수행함으로써 최소 Toffoi depth, full depth를 달성하였다.

3.7. Lin et al.의 AES 양자 회로 구현 [10]

Lin et al.은 Zou et al.의 큐비트 수를 적게 사용하는 S-box 구현 방식에서 Toffoli depth를 더욱 감소시켰다. 또한 개선된 Zig-zag 아키텍처에서 초기 키 값을 XOR 하는 키 화이트닝 부분을 최적화함으로써 128-qubit을 절약하였다. 이를 통해 매우 낮은 qubit 수를 유지함과 동시에 상대적으로 낮은 Toffoli depth를 가지는 AES 양자 회로 구현을 제시하였다. 그 결과, 현재 모든 AES 양자 회로 중 Toffoli depth × 큐비트 수의 지표에서 가장 높은 성능을 제공하고 있다.

Ⅳ. 양자 컴퓨터를 통한 공개키 해킹 동향

Shor 알고리즘은 대칭키의 보안 레벨을 감소시키는 Grover 알고리즘과 달리 소인수 분해, 이산대수 문제에 기반한 공개키 암호의 안전성을 완전히 붕괴시킨다. Shor 알고리즘은 RSA와 ECC의 핵심 연산을 양자 회로 상에서 얼마나 효율적으로 구현하는지에 따라 필요 양자 자원이 결정된다. 본 장에서는 Shor 알고리즘을 사용한 RSA, ECC 해킹에 대해서 살펴보고자 한다.

4.1. RSA 양자 해킹

양자 컴퓨팅 환경에서 RSA 암호는 소인수 분해 문제에 기반하고 있기 때문에 Shor 알고리즘을 통해 공격받을 수 있다. 이러한 이유에서 많은 논문이 Shor 알고리즘을 적용하여 RSA 암호의 수학적 기반인 소

인수분해 문제를 해결하는 방향으로 진행되고 있다.

Bhatia과 Ramkumar는 논문 [11]에서 Shor 알고리즘을 통해 RSA 암호 체계를 크래킹 할 수 있는 방법을 제안하였다. 논문에서는 해당 방법을 IBM에서 제공하는 양자 컴퓨팅 툴인 Qiskit을 통해 구현하였고 실행 시간에 대한 비트 수를 나타내는 그래프를 통해 다양한 양자 모델이 존재함을 보였다.

Thombre et al. [12]과 Albuainain et al. [13] 또한 Shor 알고리즘을 통해 소인수 분해하고 RSA를 공격하는 방법에 대해 논의하였다. 두 논문 모두 IBM에서 제공하는 시뮬레이터를 통해 짧은 길이의 정수 인수분해를 성공하며 Shor 알고리즘을 통한 RSA 암호시스템 크래킹 공격을 개념적으로 증명하였다.

일반적으로 Shor 알고리즘 과정 중에 주기 r이 홀수인 경우, 다시 첫 번째 단계로 넘어간다. 그러나 Dong et al.은 r이 홀수인 경우에도 인수분해를 가능하게 하는 최적화 알고리즘을 제안하였다[14]. [14]는 r이 3의 배수이거나 a가 완전제곱수 경우에도 인수분해가 가능함을 보였고 제안하는 최적화 알고리즘을 사용할 경우 RSA 크래킹의 성공률이 향상됨을 증명하였다.

[15]에서는 Qiskit에서 동작하는 RSA 암호 알고리즘 크래킹 프로그램을 제안하였다. 논문에서 제안한 프로그램은 평문과 공개키, 암호문을 입력으로 넣으면 Shor 알고리즘과 양자 회로 프로그램을 거쳐 인수분해 결과를 획득하고, 이 결과를 기반으로 개인키를 얻어 평문을 획득하는 프로세스로 구성되어 있다. Shor 알고리즘을 통한 소인수 분해 구현에 집중한 논문들과 달리 [15]는 직접 암호를 복호화하는 과정까지 구현하였다는 점에서 의미를 갖는다.

대규모 양자 컴퓨팅 환경을 가정하고 RSA-2048에서 사용되는 2048-bit 정수의 인수분해에 필요로 하는 큐비트 수를 추정하는 연구도 있다. Gidney et al.의 논문[16]은 정수 분해와 유한 필드 상에서의 이산 대수 계산을 효율적으로 할 수 있도록 기존에 제안된 여러 기술들을 결합하고 대규모 초전도 큐비트 플랫폼을 물리적으로 가정하여 큐비트 수를 대략적으로 추정한 연구이다. 물리적 큐비트로 10억 개를 추정한 [17]의 연구를 포함하여 이전 연구들의 큐비트 추정치는 억 단위였다. 그러나 [16]에서는 오류수정, 라우팅, distillation에서 발생하는 오버헤드를 무시하는 회로 모델을 구성하여 2천만 개의 큐비트를 통해 2048-bit 정수를 약 8시간 만에 분해할 수 있다고 결론지었다.

이와 비슷하게 Mosca는 논문 [18]에서 2시간의 저장시간을 가진 다중 모드 메모리와 13,436개의 물리적 큐비트를 포함하는 프로세서를 사용하면 177일 동안 2048-bit 정수를 분해할 수 있다고 하였다.

[19]는 RSA 공격을 위해 Shor 알고리즘 대신 양자 근사 최적화 알고리즘 (QAOA)과 고전적인 격자 감소를 결합한 양자 알고리즘을 제안하였다. [19]에 따르면 10-큐비트의 초전도 양자 컴퓨터 기반 하이브리드 시스템에서 48-bit 정수의 분해를 성공하였고, 이를 기반으로 RSA에 필요로 하는 양자 자원을 파라미터별로 추정하였다. 자원 추정치에서 depth의 경우 시스템 토폴로지별로 다른 값이 나온다. 시스템 토폴로지는 All Connected System (Kn), 2D-lattice system (2DSL), 1D-Chain System (LNN)이 있다. RSA-2048의 경우 372개의 물리적인 큐비트를 필요로 하고 depth는 토폴로지 별로 1118, 1139, 1490가 나왔다. 그 외의 파라미터 추정치는 [표 2]에서 확인할 수 있다.

〔표 2〕 RSA 파라미터별 양자 자원 추정 〔19〕

RSA	qubits	depth		
		Kn	2DSL	LNN
128	37	113	121	150
256	64	194	204	258
512	114	344	357	458
1024	205	617	633	822
2048	372	1,118	1,139	1,490

4.2 ECC 양자 해킹

현재 타원곡선 상에서의 이산 대수 문제도 Shor의 알고리즘을 사용하는 양자 공격으로 깨질 수 있다.

[20]에서는 prime field 상에서의 타원 곡선 이산로그를 계산하기 위한 Shor 알고리즘의 양자 자원을 추정하였다. 해당 논문에서는 double-and-add와 몽고메리 곱셈 두 가지를 제시하였고, 그 결과 몽고메리 곱셈에서 더 좋은 성능을 도출했다. 이에, Greatest Common Divisor (GCD)를 통해 Kaliski 알고리즘에 기반한 몽고메리 역 연산을 구현하였고, 큐비트 수와 Toffoli 게이트 수 최적화를 목적으로 양자 회로를 구현하였다.

[21]에서는 [20]의 회로를 개선할 뿐만 아니라 큐비트 및 다른 trade-off 메트릭을 탐색하기 위해 depth, T-gate, T-depth 등의 자원을 추정하였다. 회로를 개선하고자 GCD를 재구성하여 모듈러 역 연산을 구현하였고, 제곱기 구현 시에 multiply-then-add 연산을 사용하여 게이트 수와 제곱 depth를 절반으로 줄이고, 보조 큐비트 수를 줄였다. [표 3]에서는 큐비트 수의 감소와 새로운 메트릭의 depth 추정 결과를 볼 수 있다.

Prime field 상에서의 타원곡선을 선택한 이전 논문들과는 달리, [22]에서는 Binary field 상에서의 타원곡선을 선택하여 양자 공격 자원을 추정하였다. double-and-add 방식으로 스칼라 곱셈을 구현하고 곱셈 연산으로 카라추바 곱셈 [23]을 사용하여 Toffoli 게이트 수를 줄였다. 이 논문에서는 [24]에 의한 GCD와 Fermat's little theorem(FLT) 역 연산을 비교하였다. GCD는 큐비트 수에서 더 나은 성능을 보이고 FLT는 Toffoli 게이트 수와 depth에서 더 나은 성능을 보인다. 전반적으로 FLT가 GCD보다 Toffoli 게이트의 1/5를 사용하는 반면 큐비트는 2배 더 사용한다. 해당 논문은 큐비트 수의 최적화를 위해 FLT 대신 GCD를 선택하였다. 또한, 제곱 연산에서는 PLU 분해를 사용하여 CNOT 게이트와 Swap 연산으로 제곱기를 구현하여 최적화하였다.

이전 연구인 [22]을 개선한 [25]는 큐비트 수보다 depth 최적화에 초점을 두었다. depth 최적화를 위해 카라추바 곱셈과 FLT 기반 역 연산 회로를 개선하였는데, 카라추바 곱셈을 개선하여 depth는 줄이고 Toffoli 게이트와 큐비트 수는 비슷하게 유지하면서 더 적은 CNOT 게이트를 사용하였다. 추가로 Shor 알고리즘뿐 아니라 이진 점 덧셈에 대한 양자 분석을 수행하여 depth 최적화와 별개로 이전 연구 [22]에 비해 점 덧셈에서의 단일 단계 계산에서 Toffoli 게이트를 최대 90%까지 줄였다. [표 4]를 보면 전체적으로 [25]가 [22]보다 큐비트를 더 많이 사용하는 대신 depth 부분에서 최적화가 이루어진 것을 볼 수 있다.

〔표 3〕 Prime Field 상에서의 Shor 알고리즘 양자 자원 추정

	〔20〕		〔21〕	
	qubits	depth	qubits	depth
P256	2,338	-	2,124	$1.38 \cdot 2^{32}$
P384	3,492	-	3,151	$1.77 \cdot 2^{34}$
P521	4,727	-	4,258	$1.09 \cdot 2^{36}$

〔표 4〕 Binary Field 상에서의 Shor 알고리즘 자원

	〔22〕		〔25〕	
	qubits	depth	qubits	depth
B233	1,647	$1.14 \cdot 2^{21}$	4,228	$1.42 \cdot 2^{15}$
B283	1,998	$1.67 \cdot 2^{21}$	5,694	$1.06 \cdot 2^{15}$
B571	4,015	$1.57 \cdot 2^{23}$	13,167	$1.42 \cdot 2^{16}$

V. 결 론

암호 시스템에 대한 잠재적인 양자 컴퓨터의 공격을 분석하고 연구하는 것은 안전한 양자 후 암호 시스템을 구축하는 기반이 된다. 이에 본 기고에서는 Grover 알고리즘과 Shor 알고리즘을 사용한 대칭키, 공개키 암호양자 공격 연구들을 살펴보았다. 본 동향 분석 결과를 바탕으로 다가올 양자컴퓨터의 위협으로부터 안전한 암호시스템을 구축하는 노력이 필요한 시점이다.

참 고 문 헌

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

[2] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review* 41.2, pp. 303-332, 1999.

[3] NIST, "Submission requirements and evaluation criteria for the post-quantum cryptography standar dization process," [internet], https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[4] M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt, "Applying Grover's algorithm to AES: quantum resource estimates," *Post-Quantum Cryptography, PQCrypto'16,* LNCS, 9606, pp. 29–43, 2016.

[5] B. Langenberg, H. Pham, R. Steinwandt, “Reducing the cost of implementing AES as a quantum circuit.”, *Cryptology ePrint Archive*, 2019.

[6] J. Zou, Z. Wei, S. Sun, X. Liu, W. Wu, “Quantum circuit implementations of AES with fewer qubits,” *International Conference on the Theory and Application of Cryptology and Information Security*, *Springer,* pp. 697-726, 2020.

[7] S. Jaques, M. Naehrig, M. Roetteler, F. Virdia, “Implementing Grover oracles for quantum key search on AES and LowMC,” *Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer,* pp. 280–310, 2020.

[8] J. Huang, S. Sun, “Synthesizing Quantum Circuits of AES with Lower T -depth and Less Qubits”, *28th International Conference on the Theory and Application of Cryptology and Information Security*, *ASIACRYPT22,* pp. 614-644, 2023.

[9] K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, A. Chattopadhyay, “Quantum analysis of aes,”. *Cryptology ePrint Archive*. 2022.

[10] D. Lin, Z. Xiang, R, Xu, S. Zhang, X. Zeng, “Optimized Quantum Implementation of AES,”, *Cryptology ePrint Archive*, 2023.

[11] Bhatia, Vaishali, 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*. *IEEE,* 2020.

[12] Thombre, Ritu, Babita Jajodia. “Experimental Analysis of Attacks on RSA & Rabin Cryptosystems using Quantum Shor’s Algorithm,” *Proceedings of International Conference on Women Researchers in Electronics and Computing*, 2021.

[13] Albuainain, Aminah, et al. “Experimental Implementation of Shor's Quantum Algorithm to Break RSA,” 2022 *14th International Conference on Computational Intelligence and Communication Networks (CICN). IEEE,* 2022.

[14] Y. Dong, H. Liu, X. Che, C. Liu, L. Sun, and G. Wen, “Improving the Success Rate of Quantum Algorithm Attacking RSA Encryption System”, *Research Square,* 2022.

[15] Ogi, Dion, Fitra Hutomo, Rini Wisnu Wardhani. “Implementasi Algoritme Shor pada Sirkuit Kuantum untuk Cracking Algoritme RSA,” *Info Kripto* 16.3, pp.111-118, 2022.

[16] Gidney, Craig, Martin Ekerå. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” *Quantum* 5, 433, 2021.

[17] Mosca, Michele. “Cybersecurity in an era with quantum computers: will we be ready?,” *IEEE Security & Privacy* 16.5 (2018): 38-41.

[18] Gouzien, Élie, Nicolas Sangouard. “Factoring 2048-bit rsa integers in 177 days with 13 436 qubits and a multimode memory,” *Physical review letters* 127(14), 140503, 2021.

[19] Yan, Bao, et al. “Factoring integers with sublinear resources on a superconducting quantum processor,” *arXiv preprint* arXiv:2212.12372, 2022.

[20] Roetteler, Martin, et al. “Quantum resource estimates for computing elliptic curve discrete logarithms,” *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security,* Hong Kong, China, December 3-7, 2017, *Proceedings, Part II 23. Springer International Publishing,* 2017.

[21] Häner, Thomas, et al. “Improved quantum circuits for elliptic curve discrete logarithms,” *PQCrypto 2020,* Paris, France, April 15–17, 2020, *Proceedings 11. Springer International Publishing,* 2020.

[22] Banegas, Gustavo, et al. “Concrete quantum cryptanalysis of binary elliptic curves,” *Cryptology ePrint Archive*, 2020.

[23] I. Van Hoof, “Space-efficient quantum multiplication of polynomials for binary finite fields with sub-quadratic Toffoli gate count,” *arXiv preprint* arXiv:1910.02849, 2019.

[24] Bernstein, Daniel J. Bo-Yin Yang. “Fast con-

stant-time gcd computation and modular inversion," *IACR Transactions on Cryptographic Hardware and Embedded Systems,* pp.340-398, 2019.

[25] Putranto, Dedy Septono Catur, et al. "Another concrete quantum cryptanalysis of binary elliptic curves," *Cryptology ePrint Archive*, 2022.

〈저 자 소 개〉

오 유 진 (Yujin Oh)

학생회원

2023년 2월 : 한성대학교 IT융합공학부 졸업

2023년 3월~현재 : 한성대학교 융합보안학과 석사과정

<관심분야> 양자 컴퓨터, 암호구현

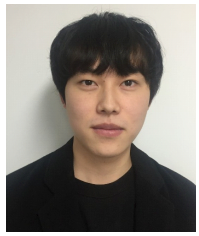
양 유 진 (Yujin Yang)

학생회원

2022년 2월 : 한성대학교 IT융합공학부 졸업

2022년 3월~현재 : 한성대학교 IT융합공학과 석사과정

<관심분야> 양자 컴퓨터, 정보보안



장 경 배 (Kyungbae Jang)

학생회원

2019년 2월 : 한성대학교 IT응용시스템공학과 공학 학사

2021년 2월 : 한성대학교 IT융합공학과 석사과정

2021년 3월~현재 : 한성대학교 IT융합공학과 박사과정

<관심분야> 양자 컴퓨터, 정보보안

서 화 정 (Hwa-jeong Seo)

종신회원

2010년 2월 : 부산대학교 컴퓨터공학과 졸업

2012년 2월 : 부산대학교 컴퓨터공학과 석사

2016년 1월 : 부산대학교 컴퓨터공학과 박사

2016년 1월~2017년 3월 : 싱가포르 과학기술청

2017년 4월~2023년 2월 : 한성대학교 IT융합공학부 조교수

2023년 2월~현재 : 한성대학교 융합보안학과 부교수

<관심분야> 정보보안, 암호구현