정 보 보 호 학 회 지
제 32 권 제1호, 2022. 2

# 양자 컴퓨팅 환경에서의 해시함수 충돌쌍 공격 동향

백 승 준*, 조 세 희*, 김 종 성**

요 약

공개키 암호에 치명적인 위협이 될 것으로 예상하는 양자 컴퓨터가 빠르게 발전하면서, 암호학계에서는 공개키 암호를 대체하기 위한 양자 내성 암호 개발이 주요 화두로 떠올랐다. 이와 더불어 양자 컴퓨팅 환경에서의 대칭키 암호 및 구조의 안전성에 관해서도 많은 연구가 제안됐다. 하지만, 해시함수에 대한 분석은 2020년 Hosoyamada와 Sasaki가 양자 컴퓨팅 환경에서 해시함수의 충돌쌍 공격을 제안하면서 비로소 연구자들의 관심을 받기 시작했다. 그들의 연구는 양자 컴퓨터를 이용할 수 있는 공격자가 고전 컴퓨터만을 이용할 수 있는 공격자보다 해시함수의 더 많은 라운드를 공격할 수 있음을 보여준다. 또한, 양자 컴퓨팅 환경에서 해시함수의 충돌쌍을 찾는 문제는 해시함수 자체의 안전성에도 영향이 있지만, 양자 내성 암호의 안전성에도 영향을 준다는 점에서 매우 중요하다. 본 논문에서는 해시함수 충돌쌍 공격이 수행되는 양자 환경과 기 제안된 양자 충돌쌍 공격을 제시한다.

## Ⅰ. 서 론

양자 컴퓨터는 양자중첩과 얽힘 현상을 이용하여 계산을 수행하는 계산 장치이며, 기존의 고전 컴퓨터와 달리 정보를 0과 1의 상태를 동시에 갖는 큐비트 단위로 처리한다. 양자 컴퓨터는 고전 컴퓨터보다 월등히 뛰어난 연산 속도를 제공할 수 있으며, 암호해독, 인공지능, 빅데이터 처리, 항공우주, 화학, 물류 등 여러 분야에 활용될 수 있다. 이러한 특징 때문에 주요 선진국 및 세계적 기업들은 양자 컴퓨터 분야에 많은 투자를 하고 있다. 2011년 캐나다의 D-wave 사가 128-큐비트의 양자 어닐링(quantum annealing) 컴퓨터를 개발한 것을 시작으로 미국 구글사에서는 2019년에 53-큐비트 양자 컴퓨터 시커모어를 제안했다. 미국 IBM사도 양자 컴퓨터 개발에 많은 투자를 하고 있는데, 2020년 제안된 65-큐비트 양자 컴퓨터 허밍버드, 2021년 제안된 127-큐비트 양자 컴퓨터 이글 등이 대표적이다[1].

현재 공개키 암호로 널리 사용되는 RSA는 소인수 분해의 어려움을 기반으로 설계되었다. 하지만 이미 1994년 미국 벨 연구소의 쇼어가 양자 푸리에 변환을 기반으로 하며 다항 시간에 소인수 분해를 할 수 있는 쇼어 알고리즘을 제안한 바 있다[2]. 여기에 양자 컴퓨터의 빠른 발전까지 더해져 암호학계에서는 양자 내성 암호(post-quantum cryptography)의 개발이 주요 화두로 떠오르게 된다. 미국 NIST가 양자 내성 암호의 개발을 선도하고 있으며[3], 이러한 양자 내성 암호의 목표는 양자 컴퓨터와 기존 컴퓨터 모두에 대해 안전하고 기존 통신 프로토콜 및 네트워크와 상호 운용할 수 있는 암호화 시스템을 개발하는 것이다[4].

양자 컴퓨터는 대칭키 암호 및 구조의 안전성에도 심각한 영향을 초래할 수 있다. 이미 사이먼 알고리즘과 쇼어 알고리즘을 사용한 분석들이 다수 제안된 바 있으며[5,6,7,8], 고전 컴퓨터만 이용할 수 있는 고전 환경보다 더 많은 라운드를 공격 혹은 구별할 수 있음이 알려져 있다. 하지만, 양자 컴퓨팅 환경에서의 해시함수 충돌쌍 공격은 2020년 Hosoyamada와 Sasaki의 AES-MMO, AES-MP와 Whirlpool 해시함수에 대한 공격을 통해 본격적인 관심을 받을 수 있었다[9]. 그들은 기존 고전 환경의 충돌쌍 공격을 양자 컴퓨팅 환경에서 몇 라운드 더 확장할 수 있음을 밝혔다. 이 제안논문 이후 양자 컴퓨팅 환경에서 다양한 블록암호 기반 해시함수, 전용 해시함수들이 분석되고 있다. 본 논문에서는 양자 컴퓨팅 환경에서 해시함수 충돌쌍을 찾는 공격을 양자 충돌쌍 공격이라 지칭한다.

본 연구는 고려대 암호기술 특화연구센터(UD210027XD)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.
* 국민대학교 금융정보보안학과 (대학원생, hellosj3@kookmin.ac.kr, ghfaos7708@kookmin.ac.kr)
** 국민대학교 금융정보보안학과/정보보안암호수학과 (교수, jskim@kookmin.ac.kr)

양자 충돌쌍 공격이 수행되는 양자 환경으로는 현재 3가지가 주로 고려되고 있으며, 양자중첩을 이용해 효율적인 연산을 할 수 있도록 하는 qRAM의 사용 가능 여부가 환경 요소에 중요하게 작용한다. 구체적으로는 큰 규모의 양자 메모리 qRAM (quantum Random Access Memory)을 이용할 수 있는 환경, qRAM과 고전 메모리(cRAM)를 함께 이용할 수 있는 환경, 공격의 효율성이 시간($T$)과 공간($S$)의 트레이드오프로 결정되는 환경이 주로 고려되고 있다. 현재 암호학자들은 상기 환경에서 기존 해시함수 충돌쌍 공격을 어느 수준까지 확장할 수 있는지에 대해 많은 연구를 수행하고 있다.

해시함수는 데이터베이스, 영지식 증명, 무결성 검증 등의 영역에서 사용되며 최근에는 블록체인과 비트코인 분야에서도 다수 활용되고 있다. 이러한 해시함수의 안전성 자체만 고려하더라도 해시함수의 양자 충돌쌍 공격을 분석하는 것은 중요하다. 하지만 해시함수의 양자 충돌쌍 공격 분석은 양자 내성 암호에까지 영향을 미칠 수 있다. 양자 내성 암호 설계 시, 일반적으로 양자 랜덤 오라클 모델에서의 양자 안전성 증명을 수행한다. 그런데 해시함수가 양자 랜덤 오라클을 인스턴스화 하는데 사용된다면, 각 양자 환경의 일반적 공격보다 효과적인 충돌쌍 공격이 존재해서는 안 된다. 만약 그러한 공격이 존재한다면 양자 내성 암호의 안전성에까지 영향을 줄 수 있기 때문이다[9]. 따라서 양자 환경에서 해시함수의 충돌쌍 공격 분석은 매우 중요하다.

본 논문에서는 해시함수의 양자 충돌쌍 공격이 수행되는 양자 환경들과 기 제안된 양자 충돌쌍 공격을 제시한다. 2장에서는 암호학적 해시함수의 안전성을 논한다. 3장에서는 현재 고려되고 있는 양자 충돌쌍 공격의 환경들과 각각의 특징을 설명한다. 4장에서는 현재까지 제안된 양자 충돌쌍 공격을 설명한다. 마지막으로, 5장에서는 향후 전망을 제시하며 본 논문의 결론을 맺는다.

## Ⅱ. 암호학적 해시함수의 안전성

해시함수는 임의 길이의 메시지를 입력으로 받아 고정된 길이의 출력값을 생성한다. 해시함수 중 암호학적 해시함수는 다음 성질들을 만족해야 한다.

- 역상 저항성 : 주어진 출력에 대해 입력값을 구하는 것이 계산적으로 불가능. 즉, $y=h(x)$가 주어졌을 때, $x$를 구하는 것은 계산적으로 불가능.
- 제2 역상 저항성 : 주어진 입력에 대한 출력값과 같은 출력값을 갖는 서로 다른 입력을 구하는 것이 계산적으로 불가능. 즉, $x$가 주어졌을 때, $h(x)=h(x^*)$를 만족하는 $x^*(\neq x)$를 구하는 것은 계산적으로 불가능.
- 충돌 회피성 : 같은 출력값을 갖는 서로 다른 입력값을 찾는 것이 계산적으로 불가능. 즉, $h(x)=h(x^*)$를 만족하는 $x$, $x^*(\neq x)$을 찾는 것은 계산적으로 불가능. 여기서 $x$와 $x^*$를 충돌쌍이라 지칭.

$n$-비트 해시함수를 고려할 때, 역상 저항성과 제2 역상 저항성은 $O(2^n)$개의 메시지를 통해 무력화할 수 있다. 하지만 충돌 회피성은 $O(2^{n/2})$개의 메시지로도 무력화할 수 있으므로, 일반적으로 해시값의 길이가 $n$-비트인 해시함수의 안전성을 $O(2^{n/2})$로 설정한다.

## Ⅲ. 양자 충돌쌍 공격이 수행되는 3가지 양자 컴퓨팅 환경

고전 환경에서 $n$-비트 해시함수의 충돌쌍을 찾는 일반적인 공격 복잡도는 생일 역설에 의해 $O(2^{n/2})$이다. 따라서 공격자가 $O(2^{n/2})$보다 낮은 복잡도로 충돌쌍을 찾을 수 있는 공격을 구성한다면 그 공격은 의미 있는 것으로 여겨진다. 그러나, 양자 환경에서 충돌쌍을 찾는 일반적인 공격 복잡도는 공격자가 이용할 수 있는 자원에 따라 다르다. 따라서 전용 양자 충돌쌍 공격을 수행할 때에는 각 환경에서 수행되는 최상의 알고리즘에 필요한 복잡도와 비교되어야 한다.

고려되는 양자 환경 1은 작은 규모(polynomial size)의 양자 컴퓨터와 큰 규모(exponential size)의 qRAM을 이용할 수 있는 환경이며, 이 환경에서 작동하는 최상의 알고리즘은 BHT 알고리즘[10]이다. 양자 환경 2는 작은 규모의 양자 컴퓨터와 큰 규모의 cRAM을 이용할 수 있는 환경으로, 이 환경에서는 CNS 알고리즘[11]이 최상의 알고리즘이다. 마지막 양자 환경 3은 공격의 효율성이 공격 알고리즘의 시간 복잡도와 공간 복잡도의 트레이드오프로 결정되는 환경이며, 이 환경에서는 Parallel Rho 알고리즘[12]의 복잡도를 일반 공격 복잡도로 설정한다.

일반적으로 차분 분석을 기반으로 하여 해시함수의 충돌쌍 공격을 수행하며, 공격에 적용할 수 있는 차분

〔표 1〕 가용 자원별 이용 가능한 차분 경로 확률 비교

| 환경 | | 가용 자원 | 공격 알고리즘 | 일반적 공격 복잡도 | 이용 가능한 차분 경로 확률($p$) |
|---|---|---|---|---|---|
| 고전 | | 고전 컴퓨터 | 생일 공격 | $2^{n/2}$ | $p > 2^{-n/2}$ |
| 양자 | 환경 1 | 작은 규모의 양자 컴퓨터 + 큰 규모의 qRAM | BHT〔10〕 | $2^{n/3}$ | $p > 2^{-2n/3}$ |
| | 환경 2 | 작은 규모의 양자 컴퓨터 + 큰 규모의 cRAM | CNS〔11〕 | $2^{2n/5}$ | $p > 2^{-4n/5}$ |
| | 환경 3 | 시간($T$)-공간($S$) 트레이드오프 | Parallel Rho〔12〕 | $T \cdot S = 2^{n/2}$ | $p > S^2 \cdot 2^{-n}$ |

경로의 확률 범위는 각 환경에 따라 달라진다. [표 1]은 가용 자원별 이용 가능한 차분 경로의 확률을 비교한 것이다.

### 3.1. 양자 환경 1 – BHT 알고리즘

양자 환경 1은 큰 규모의 qRAM을 이용할 수 있는 환경이라는 특징이 있다. 이 환경에서는 Brassard, Høyer와 Tapp가 개발한 BHT 알고리즘이 최상의 공격 알고리즘으로 알려져 있다. BHT는 $O(2^{n/3})$의 qRAM이 이용 가능할 때 $O(2^{n/3})$의 시간으로 해시함수의 충돌쌍을 찾는 양자 알고리즘이다. 여기서 $O(2^{n/3})$ 양자 질의가 필요하지만, 온라인 중첩 질의가 필요하지는 않다. 아래는 BHT 알고리즘을 사용하여 $n$-비트 해시함수의 충돌쌍을 찾는 과정이다.

(1) 함수 $f:\{0,1\}^n \rightarrow \{0,1\}^n$을 랜덤 함수라고 하자. $|X| = 2^{n/3}$ 크기의 부분 집합 $X \subset \{0,1\}^n$을 선택하고, 모든 $x \in X$에 대하여 $f(x)$를 계산한다.

(2) 양자중첩 상태로 접근할 수 있도록 $2^{n/3}$쌍의 $\{(x, f(x))\}_{x \in X}$를 qRAM에 저장한다.

(3) $f(x) = f(x^*)$를 만족하는 $x^* \in \{0,1\}^n \backslash X$를 찾기 위해 그로버 알고리즘을 수행한다.

과정 (3)이 $O(\sqrt{2^n/L}) = O(2^{n/3})$ 시간에 수행되므로, 충돌쌍을 찾기 위해 BHT 알고리즘은 $O(2^{n/3})$의 질의 복잡도와 $O(2^{n/3})$의 qRAM이 필요하다. 시간 복잡도 $T$와 공간 복잡도 $S$(필요한 qRAM의 양)의 트레이드오프는 $T \cdot S = O(2^{2n/3})$을 만족한다.

하지만, 이 환경에서 각 큐비트가 프로세서 혹은 메모리로 작동할 수 있다고 가정하면 $2^{n/3}$개의 프로세서를 병렬 처리하여 $O(2^{n/6})$의 시간 복잡도로 충돌쌍을 찾을 수 있으며, 이는 고전 컴퓨터로도 가능한 수치이다 [13]. 따라서 작은 규모의 양자 컴퓨터 조건이 반드시 고려되어야 BHT 알고리즘이 이 환경에서 최상의 알고리즘이 될 수 있다.

양자 환경 1의 약점은 BHT 알고리즘의 핵심 요소인 큰 규모의 qRAM이 실현될 수 있을지에 대한 의구심이 남아있다는 점이다.

### 3.2. 양자 환경 2 – CNS 알고리즘

양자 환경 2는 큰 규모의 cRAM을 이용할 수 있는 환경이라는 특징이 있다. 이 환경에서는 Chailloux, Naya-Plasencia와 Schrottenloher가 개발한 CNS 알고리즘이 최상의 공격 알고리즘으로 알려져 있다. CNS는 $O(n)$ 규모의 양자 컴퓨터와 $O(2^{n/5})$의 cRAM을 이용할 수 있을 때 $O(2^{2n/5})$의 시간으로 해시함수의 충돌쌍을 찾는 양자 알고리즘이다. 아래는 CNS 알고리즘을 사용하여 $n$-비트 해시함수의 충돌쌍을 찾는 과정이다.

(1) 함수 $f:\{0,1\}^n \rightarrow \{0,1\}^n$을 랜덤 함수라고 하자. 그로버 알고리즘을 적용하여 집합 $S_L^f$의 원소로 이루어진 $|L| = 2^{t-r}$ 크기의 부분 집합 $L$을 구성한다. 구성한 부분 집합 $L$은 cRAM에 저장한다.

$(S_r^f := \{(x,f(x)) : \exists z \in \{0,1\}^{n-r}, f(x) = 0...0 \| z\},$
$|S_r^f| = 2^{n-r})$

(2) 양자중첩 상태로 그로버 알고리즘을 적용하여 전체 집합에서 $S_r^f$에 포함되는 원소 $x \in \{0,1\}^n$을 조사한다. 구해진 $x$에 대해 $f(x)$을 계산하여 순서쌍 $(x,f(x))$를 구성한다.

(3) 순차적으로 부분 집합 $L$의 원소들과 과정 (2)에서 구성된 순서쌍 $(x,f(x))$와 비교하여 $f(x) = f(x^*)$ $((x^*,f(x^*)) \in L)$이 존재하는지 확인한다.

(4) (2), (3) 과정을 $2^{\frac{n-t-1}{2}}$번 반복한다.

위 CNS 알고리즘 실행 과정에서 발생하는 시간 복잡도는 $2^{\frac{n-t-1}{2}}(2^{r/2}+2^{t-r})+2^{t-r/2}$이며 $t = \frac{3n}{5}$, $r = \frac{2t}{3} = \frac{2n}{5}$로 설정했을 때 가장 낮은 복잡도인 $O(2^{2n/5})$이 필요하다. 공간 복잡도는 과정 (1)에서 $O(2^{n/5})$의 cRAM, 그리고 양자중첩 상태를 이용하기 위한 $O(n)$ 규모의 양자 컴퓨터가 필요하다. 본 알고리즘은 그로버 알고리즘의 일반화된 버전인 amplitude amplification 기술[14]을 사용하여 수행되며, 이와 관련된 사실은 CNS 알고리즘의 제안논문 [11]을 참고하라.

CNS 알고리즘은 BHT 알고리즘과 달리 큰 규모의 qRAM이 필요하지 않으며, 상대적으로 현실적인 큰 규모의 cRAM이 필요하다. 따라서, 양자 환경 2는 양자 환경 1에 비해 더 현실적인 양자 환경이라고 할 수 있다.

### 3.3. 양자 환경 3 – Parallel Rho 알고리즘

양자 환경 3은 공격 알고리즘에 필요한 시간 복잡도와 공간 복잡도를 모두 고려하여 공격의 효율성이 평가됨과 동시에 큰 규모의 qRAM을 사용할 수 없는 환경이라는 특징이 있다. 이 환경에서는 Oorschot와 Wiener가 제안한 고전 환경의 Parallel Rho 알고리즘의 시간-공간 트레이드오프를 일반적 공격 복잡도로 설정한다. Parallel Rho 알고리즘은 $S$ 규모의 고전 컴퓨터를 이용할 수 있을 때, $T = O(2^{n/2}/S)$의 시간으로 충돌쌍을 찾을 수 있다. 이는 본래 고전 컴퓨터에 대해 제안된 알고리즘이지만 양자 컴퓨터에 적용하더라도 논리적 하자가 없다. 또한, 이 고전적인 알고리즘보다 더 나은 트레이드오프를 제공하는 양자 공격은 존재하지 않는다[15]. 이러한 맥락에서, Parallel Rho 알고리즘의 시간-공간 트레이드오프인 $T \cdot S = 2^{n/2}$를 양자 충돌쌍 공격의 일반적 공격 복잡도로 설정하는 것은 합리적이다. 이 복잡도에 의하면 공격자가 $T \cdot S < 2^{n/2}$를 만족하는 양자 공격을 구성했을 때, 의미 있는 공격이 구성됐다고 여겨진다. 한편, Jaques와 Schanck의 연구는 양자 메모리가 능동적으로 수정되는 경우 양자 오류 정정 관점에서 양자 환경 3이 합리적이라는 사실을 보여준다[16].

## Ⅳ. 기 제안된 양자 충돌쌍 공격

Hosoyamada와 Sasaki의 AES 해시모드와 Whirlpool에 대한 양자 충돌쌍 공격[9]이 제안된 후, 해시함수의 양자 안전성 분석 분야가 암호학자들의 많은 관심을 받기 시작했다. AES 해시모드에 대한 향상된 양자 충돌쌍 공격, Hirose, Gimli, SHA-256/512, Simpira v2 등 많은 대상 해시함수에 대해 분석이 진행됐다[17,18,19,15,20]. 이 분석들은 양자 컴퓨터를 이용할 수 있는 공격자가 고전 컴퓨터만을 이용할 수 있는 공격자보다 해시함수의 더 많은 라운드를 공격할 수 있음을 보여준다. 본 장의 내용은 각 공격 제안논문들의 공격을 요약한 것이며, [표 6]에 요약 정리되어 있다.

### 4.1. AES 해시모드 및 Whirlpool

Eurocrypt 2020에서 Hosoyamada와 Sasaki가 발표한 AES 해시모드 AES-MMO, AES-MP와 해시함수 Whirlpool에 대한 양자 충돌쌍 공격은 고전 환경에서 이용할 수 없는 확률의 차분 경로를 양자 환경에서는 이용할 수 있음을 입증했다[9]. 그들은 AES-MMO와 AES-MP에 대해 6라운드까지 가능했던 고전 환경의 충돌쌍 공격을 7라운드로 확장했고, Whirlpool에 대해서는 고전 환경의 5라운드 공격을 6라운드까지 확장했다. 이 공격들은 Mendel 등이 제안한 리바운드 공격[21] 기반 충돌쌍 공격이다. 또한, super-sbox 분석 기술을 사용하여 입력 차분과 출력 차분에 맞는 시작 점들을 찾을 때 그로버 알고리즘을 적절히 사용하고 outbound phase

〔표 2〕 기 제안된 양자 충돌쌍 공격

| 대상 해시함수 | 공격 라운드 | 공격 종류 | 양자 환경 | 참조 |
|---|---|---|---|---|
| AES-MMO/MP | 7/10 | 충돌쌍 공격 | 1,3 | 〔9,17〕 |
| Whirlpool | 6/10 | 충돌쌍 공격 | 3 | 〔9〕 |
| AES-256-Hirose | 10/14 | free-start 충돌쌍 공격 | 1,2,3 | 〔18〕 |
| Gimli | 14/24<br>20/24 | 충돌쌍 공격<br>semi free-start 충돌쌍 공격 | 1 | 〔19〕 |
| SHA-256<br>SHA-512 | 38/64<br>39/80 | 충돌쌍 공격 | 3 | 〔15〕 |
| Simpira v2($b=2$)<br>Simpira v2($b=4$) | 9/15<br>11/15 | 충돌쌍 공격 | 2 | 〔20〕 |

의 차분 경로를 수정하는 방식으로 공격이 수행된다.

뒤이은 Asiacrypt 2020에서 Dong 등은 non-full-active super S-box 기술을 사용하여 [9]의 AES-MMO와 AES-MP 해시모드 공격에 필요한 qRAM의 규모를 상당히 줄일 수 있음을 밝혔다[17]. 이를 통해 아직 실현될지 알 수 없는 qRAM 의존도를 크게 낮추었다.

### 4.2. AES-256-Hirose

ToSC 2021 Issue 1에서 Chauhan 등은 AES-256으로 인스턴스화 된 Hirose 이중 블록 길이 압축함수에 대한 양자 free-start 충돌쌍 공격을 제안했다[18]. 고전 환경에서는 9라운드까지 free-start 충돌쌍을 생일 공격보다 빠르게 찾을 수 있음이 밝혀져 있었으나, 그들은 이를 양자 환경에서 10라운드로 확장했다. 이 공격은 리바운드 공격을 기반으로 하며, 2개의 inbound phase를 설정하고 이를 연결하는 phase를 구성하여 기존보다 inbound phase를 확장한다. 2개의 inbound phase를 연결하는 논리에는 AES-256을 해시함수의 내부 프리미티브로 사용 시 키를 선택할 수 있다는 점이 중요하게 작용한다.

### 4.3. Gimli

Gimli[22]는 2015년부터 진행되고 있는 NIST 경량 암호 공모사업의 2라운드 후보였으며, 3라운드 후보로는 선정되지 못한 알고리즘이다. Asiacrypt 2020에서 Gutiérrez 등은 Gimli 퍼뮤테이션을 기반으로 하는 Gimli-Hash에 대한 양자 충돌쌍 공격 및 free-start 충돌쌍 공격을 수행했다[19]. 그들은 먼저 Gimli 퍼뮤테이션의 느린 확산 성질과 내부 대칭성을 지적하며, Gimli-Hash에 대한 고전 환경에서의 충돌쌍 및 semi free-start 충돌쌍 공격을 제안한다. 여기에 amplitude amplification 기술을 적용하여 고전 환경보다 각각 두 라운드 더 확장된 14라운드 양자 충돌쌍 공격, 20라운드 양자 semi free-start 충돌쌍 공격을 제안하기에 이른다.

### 4.4. SHA-256/512

Crypto 2021에서 Hosoyamada와 Sasaki는 SHA-256/512에 대한 양자 충돌쌍 공격을 제안했다[15]. 이는 전용 해시함수에 대해서 최초로 수행된 양자 충돌쌍 공격으로, 현재 가장 중요하게 취급되는 SHA-2 family에 대한 공격이라는 데 의미가 있다. 그들의 연구는 SHA-256과 SHA-512에 대해 제안된 고전 환경의 각 38, 39라운드 semi free-start 충돌쌍 공격을 양자 환경에서는 실제 충돌쌍을 찾는 공격으로 변환할 수 있음을 보여준다. 공격의 핵심은 2-블록 충돌쌍을 찾는 것이며, 여기서 블록 간 실제값의 연결에서 양자 연산을 적용하는 것이다. 그들의 semi free-start 충돌쌍 공격을 실제 충돌쌍 공격으로 변환하는 아이디어는 간단하지만, 양자 환경에서만 적용할 수 있다는 점에서 해시함수의 양자 안전성 연구에 한 방향을 제시했다고 할 수 있다.

### 4.5. Simpira v2

ToSC 2021 Issue 2에서 Ni 등은 AES 기반 퍼뮤테이션 Simpira v2을 내부 함수로 하는 Davies-Meyer 해시모드 대한 양자 충돌쌍 공격을 제안한다[20]. 그들은

먼저 Simpira v2의 활성 S-box 패턴을 차분 경로의 확률 관점에서 최적화할 수 있는 MILP(Mixed Integer Linear Programming) 모델을 제안한다. 제안된 모델을 통해 양자 환경에 적합한 차분 경로를 찾고, 이를 리바운드 공격을 기반으로 한 양자 충돌쌍 공격에 적용한다. Ni 등은 Simpira v2에 대한 고전 환경과 양자 환경에서의 충돌쌍 공격을 동시에 제안하며, 구조의 브랜치 수에 따라 최대 11라운드까지 공격할 수 있다. 연구에는 알고리즘의 충돌이 발생하는 브랜치의 위치에 따라 복잡도가 달라질 수 있다는 점까지 상세하게 서술되어 있으며, Simpira v2가 최근 제안된 양자 내성 암호 SPHINCS-Simpira[23]의 내부 프리미티브로 사용된다는 점에서 의미 있는 분석이라 할 수 있다.

## Ⅴ. 결 론

본 논문에서는 최근 들어 많은 관심을 받는 양자 컴퓨팅 환경에서의 해시함수 충돌쌍 공격 동향을 살펴봤다. 이와 더불어 해시함수의 충돌쌍 공격이 수행될 것으로 고려되는 3가지 양자 환경과 그것들의 각 특징을 분석했다. 서두에도 언급했듯이 해시함수에 대한 전용 양자 공격을 제안하는 것은 해시함수 자체의 안전성뿐만 아니라 양자 내성 암호의 안전성까지 영향을 미친다는 점에서 매우 중요하다. 하지만 해시함수에 대한 전용 양자 공격 연구는 아직 초기 단계이므로, 향후 국내 표준 해시함수 및 세계적으로 사용되는 해시함수들이 양자 컴퓨터를 사용할 수 있는 공격자로부터 얼마나 안전한지 연구할 필요가 있다.

## 참 고 문 헌


[1] https://research.ibm.com/blog/ibm-quantum-road-map, Visited on January 20, 2022.

[2] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, *FOCS‘94*, pp.124-134, 1994.

[3] Lightweight Cryptography, *NIST*, https://csrc.nist.gov/Projects/lightweight-cryptography, Visited on January 20, 2022.

[4] Post-Quantum Cryptography, *NIST*, https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization

[5] X. Bonnetain, M. Naya-Plasencia and A. Schrottenloher, “Quantum Security Analysis of AES”, *IACR Trans. Symmetric Cryptol.*, pp.55-93, 2019.

[6] X. Dong, Z. Li and X. Wang, “Quantum cryptanalysis on some generalized Feistel schemes”, *Sci. China Inf. Sci.*, 2019.

[7] A. Hosoyamada and K. Aoki, “On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers”, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, pp.27-34, 2019.

[8] M. Kaplan, G. Leurent, A. Leverrier and M. Naya-Plasencia, “Quantum Differential and Linear Cryptanalysis”, *IACR Trans. Symmetric Cryptol.*, pp.71-94, 2016.

[9] A. Hosoyamada and Y. Sasaki, “Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound”, *EUROCRYPT’20*, LNCS 12106, pp.249-279, 2020.

[10] G. Brassard, P. Høyer and A. Tapp, “Quantum Cryptanalysis of Hash and Claw-Free Functions”, *LATIN‘98*, LNCS 1380, pp.163-169, 1998.

[11] A. Chailloux, M. Naya-Plasencia and A. Schrottenloher, “An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography”, *ASIACRYPT’17*, LNCS 10625, pp.211-240, 2017.

[12] P. C. van Oorschot and M. J. Wiener, “Parallel Collision Search with Application to Hash Functions and Discrete Logarithms”, *CCS‘94*, pp.210-218, 1994.

[13] D. J. Bernstein, “Cost Analysis of Hash Collisions: Will Quantum Computers Make SHARCS Obsolete?”, *SHARCS*, 2009.

[14] G. Brassard, P. Høyer, M. Mosca and A. Tapp, “Quantum Amplitude Amplification and Estimation”, *Contemporary Mathematics*, pp.53-74, 2002.

[15] A. Hosoyamada and Y. Sasaki, “Quantum Collision Attacks on Reduced SHA-256 and SHA-512”, *CRYPTO’21*, pp.616-646, 2021.

[16] S. Jaques and J. M. Schanck, “Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE”, *CRYPTO‘19*, LNCS 11692, pp.32-61, 2019.

[17] X. Dong, S. Sun, D. Shi, F. Gao, X. Wang and L. Hu, “Quantum Collision Attacks on AES-like Hashing with Low Quantum Random Access Memories”, *ASIACRYPT’20*, pp.727-757, 2020.

[18] A. Kumar Chauhan, A. Kumar and S. Kumar Sanadhya, “Quantum Free-Start Collision Attacks on Double Block Length Hashing with Round-Reduced AES-256”, *IACR Trans. Symmetric Cryptol.*, pp.316-336, 2021.

[19] A. Flórez-Gutiérrez, G. Leurent, M. Naya-Plasencia, L. Perrin, A. Schrottenloher and F. Sibleyras, “New Results on Gimli: Full-Permutation Distinguishers and Improved Collisions”, *ASIACRYPT‘20*, pp.33-63, 2020.

[20] B. Ni, X. Dong, K. Jia and Q. You, “(Quantum) Collision Attacks on Reduced Simpira v2”, *IACR Trans. Symmetric Cryptol.*, pp.222-248, 2021.

[21] F. Mendel, C. Rechberger, M. Schläffer and S. S. Thomsen, “The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl”, *FSE’09*, pp.260-276, 2009.

[22] D. J. Bernstein, S. Kölbl, S. Lucks, P. Maat Costa Massolino, F. Mendel, K. Nawaz, T. Schneider, P. Schwabe, F.-X. Standaert, Y. Todo and B. Viguie, “Gimli Submission to the NIST Lightweight Cryptography project”, Available online: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/gimli-spec.pdf

[23] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe and Z. Wilcox-O’Hearn, “SPHINCS: Practical Stateless Hash-Based Signatures.”, *EUROCRYPT‘15*, LNCS 9056, pp.368-397, 2015.

## 〈저자소개〉

**백 승 준 (Seungjun Baek)**

학생회원

2019년 2월 : 국민대학교 수학과 졸업
2020년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 정보보호, 암호 알고리즘

**조 세 희 (Sehee Cho)**

학생회원

2021년 2월 : 국민대학교 정보보안암호수학과 졸업
2021년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
<관심분야> 정보보호, 암호 알고리즘

**김 종 성 (Jongsung Kim)**

종신회원

2000년 8월/2002년 8월 : 고려대학교 수학 전공 학사/이학석사
2006년 11월 : K.U.Leuven. ESAT/SCD-COSIC 정보보호 전공 공학박사
2007년 2월 : 고려대학교 정보보호대학원 공학박사
2007년 3월~2009년 8월 : 고려대학교 정보보호기술연구센터 연구교수
2009년 9월~2013년 2월 : 경남대학교 e-비즈니스학과 조교수
2013년 3월~2017년 2월 : 국민대학교 수학과 부교수
2014년 3월~2020년 8월 : 국민대학교 일반대학원 금융정보보안학과 부교수
2017년 3월~2020년 8월 : 국민대학교 정보보안암호수학과 부교수
2020년 9월~현재 : 국민대학교 정보보안암호수학과/일반대학원 금융정보보안학과 교수
<관심분야> 정보보호, 암호 알고리즘, 디지털 포렌식