Grover's Collision Search

https://youtu.be/dJ72fdFtBrs

장경배

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Grover's Algorithm

- **Search space N에 대한 검색 복잡도를 O($\sqrt{N}$)으로 감소 시킬 수 있는 양자 알고리즘**
  - **Input Setting**

$$H^{\otimes n}|0\rangle^{\otimes n} = |\psi\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle$$

  - **Oracle**

$$f(x) = \begin{cases} 1 \text{ if } \mathrm{Hash}(x) = \text{target output} \\ 0 \text{ if } \mathrm{Hash}(x) \neq \text{target output} \end{cases}$$

$$U_f(|\psi\rangle|-\rangle) = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle|-\rangle$$

Grover on Hash Functions

- **Pre-image attack**
  - **주어진 (known) 해시 값을 생성하는 input 값 (unknown)을 찾아내는 것**
    - Hash(x) = Known-output
    - **n-bit이 known-output이 주어졌을 때, n-bit input을 대상으로 search**
      → 블록암호에 대한 key search와 유사

- **Collision search**
  - **다른 input 값이지만, 동일한 해시 값을 생성하는 쌍을 찾아내는 것**
    - Hash (x_1) = Hash (x_2)
  - Pre-image attack과는 달리, 다양한 접근이 가능
    - **Second pre-image attack**
    - **BHT algorithm**

Grover on Hash Functions

- **Second pre-image attack** (Quantum)
  - Input에 대한 output 해시가 주어졌을 때, **output을 생성하는 또 다른 input을 찾는 것**
    - Hash(Known-input (n-bit)) = Known-output (n-bit)
    - Hash($x \neq$ Known-input) = Known-output

      → Quantum complexity: $\boldsymbol{O(2^{n/2})}$

- 기본적인 방법이며, **복잡도는 Pre-image attack과 동일**함
- 간단하며, **Quantum ram이 필요 없다는 것이 장점**

Grover on Hash Functions

- NIST의 post-quantum security level을 고려했을 때, **Second pre-image attack (Quantum, $\boldsymbol{O(n^{1/2})}$) 은 적절하지 않음**

Search Complexity	Category	Cipher	Quantum gate count
2^{64} (key search)	Level 1	AES-128	2^{157}/MAXDEPTH
$\boldsymbol{2^{128}}$ (second pre-image)	**Level 2**	**SHA-2-256/SHA-3-256**	**Unspecified**
2^{96} (key search)	Level 3	AES-192	2^{221}/MAXDEPTH
$\boldsymbol{2^{192}}$ (second pre-image)	**Level 4**	**SHA-2-384/SHA-3-384**	**Unspecified**
2^{128} (key search)	Level 5	AES-256	2^{285}/MAXDEPTH
$\boldsymbol{2^{256}}$ (second pre-image)	**Level 6**	**SHA-2-512/SHA-3-512**	**Unspecified**

[1] Note that, barring some truly surprising technological development during the standardization process, NIST will assume that the five security strengths are correctly ordered in terms of practical security. (E.g., NIST will assume that a brute-force collision attack on SHA-256 will be technologically feasible before a brute-force key search attack on AES-192.)

Grover on Hash Functions

- **BHT algorithm**
  - Birthday paradox와 Grover's search를 결합한 알고리즘
    → Birthday paradox: 지정한 생일에 대한 확률은 낮지만, 같은 생일을 찾을 확률은 높음

    1. **$2^{n/3}$의 무작위 input**으로 구성되는 **Subset L**을 구성
    2. Subset L에서 collision이 발생하는지 확인 (Classical) → $O(2^{n/3})$
       → Hash($x_0 \in K$) = Hash($x_1 \in L$), Go to step 5.
    3. **Subset L을 제외한 input $2^{2n/3}$**으로 구성되는 **Subset K**를 구성
    4. Grover's search는 Subset K ($2^{2n/3}$)에서 다음 솔루션을 찾음 → $O(2^{n/3})$
       → Hash($x_0 \in K$) = Hash($x_1 \in L$)
    5. return (x_0, x_1)

- **Quantum ram이 필요하다는 고려 사항이 있음 + 논쟁?의 여지가 있음**

Grover on Hash Functions

Algorithm 3: BHT algorithm for collision search.

Input: Input set N
Output: *Collision*

Select a subset K (size of $N^{1/3}$) $\in N$ at random and query the hash function
if there is a *Collision* in K **then**
    return the *Collision*
else
    Construct a subset L (size of $N^{2/3}$) $\in N$ that does not include K
end if
Grover's algorithm finds $x_1 \in L$ that collides with $x_0 \in K$
return (x_0, x_1)

Grover on Hash Functions

- NIST의 post-quantum security level을 고려했을 때, **BHT 알고리즘은 적절할 수 있음**

Search Complexity	Category	Cipher	Quantum gate count
2^{64} (key search)	Level 1	AES-128	2^{157}/MAXDEPTH
$2^{85\sim}$ (BHT)	**Level 2**	**SHA-2-256/SHA-3-256**	**Unspecified**
2^{96} (key search)	Level 3	AES-192	2^{221}/MAXDEPTH
2^{128} (BHT)	**Level 4**	**SHA-2-384/SHA-3-384**	**Unspecified**
2^{128} (key search)	Level 5	AES-256	2^{285}/MAXDEPTH
$2^{170\sim}$ (BHT)	**Level 6**	**SHA-2-512/SHA-3-512**	**Unspecified**

[1] Note that, barring some truly surprising technological development during the standardization process, NIST will assume that the five security strengths are correctly ordered in terms of practical security. (E.g., NIST will assume that a brute-force collision attack on SHA-256 will be technologically feasible before a brute-force key search attack on AES-192.)

Grover on Hash Functions

- **Levels 4, 5에 대한 Complexity (iteration)는 동일**
  → SHA2/3-384, AES 256에 대한 **양자 회로 비용에 따라 결정**됨

Search Complexity	Category	Cipher	Quantum gate count
2^{64} (key search)	Level 1	AES-128	2^{157}/MAXDEPTH
$2^{85\sim}$ (BHT)	**Level 2**	**SHA-2-256/SHA-3-256**	**Unspecified**
2^{96} (key search)	Level 3	AES-192	2^{221}/MAXDEPTH
2^{128} (BHT)	**Level 4**	**SHA-2-384/SHA-3-384**	**Unspecified**
2^{128} (key search)	Level 5	AES-256	2^{285}/MAXDEPTH
$2^{170\sim}$ (BHT)	**Level 6**	**SHA-2-512/SHA-3-512**	**Unspecified**

Grover on Hash Functions

- Level 4 (SHA2/3-384) 2^{292} / 2^{285}
- Level 5 (AES-256) 2^{285}

Category	Cipher	Quantum gate count
Level 1	AES-128	2^{157}/MAXDEPTH
Level 2	**SHA-2-256/SHA-3-256**	**Unspecified**
Level 3	AES-192	2^{221}/MAXDEPTH
Level 4	**SHA-2-384/SHA-3-384**	**Unspecified**
Level 5	AES-256	2^{285}/MAXDEPTH
Level 6	**SHA-2-512/SHA-3-512**	**Unspecified**

Table 2: Security levels defined in this work.

Strength	Category	Hash function	Quantum gate count
Level 2	A	SHA-2-256	2^{205}/MAXDEPTH
	B	SHA-3-256	2^{200}/MAXDEPTH
	C	ASCON-Hash-256	2^{201}/MAXDEPTH
Level 4	A	SHA-2-384	2^{292}/MAXDEPTH
	B	SHA-3-384	2^{285}/MAXDEPTH
	C	ASCON-Hash-384	2^{287}/MAXDEPTH
Level 6	A	SHA-2-512	2^{377}/MAXDEPTH
	B	SHA-3-512	2^{370}/MAXDEPTH
	C	ASCON-Hash-512	2^{374}/MAXDEPTH

Grover on Hash Functions

- Level 4 (SHA2/3-384) 2^{292} / 2^{285}
- Level 5 (AES-256) 2^{285}

Combine

Level 5

Category	Cipher	Quantum gate count
Level 1	AES-128	2^{157}/MAXDEPTH
Level 2	**SHA-2-256/SHA-3-256**	**Unspecified**
Level 3	AES-192	2^{221}/MAXDEPTH
Level 4	**SHA-2-384/SHA-3-384**	**Unspecified**
Level 5	AES-256	2^{285}/MAXDEPTH
Level 6	**SHA-2-512/SHA-3-512**	**Unspecified**

Table 2: Security levels defined in this work.

Strength	Category	Hash function	Quantum gate count
Level 2	A	SHA-2-256	2^{205}/MAXDEPTH
	B	SHA-3-256	2^{200}/MAXDEPTH
	C	ASCON-Hash-256	2^{201}/MAXDEPTH
Level 4	A	SHA-2-384	2^{292}/MAXDEPTH
	B	SHA-3-384	2^{285}/MAXDEPTH
	C	ASCON-Hash-384	2^{287}/MAXDEPTH
Level 6	A	SHA-2-512	2^{377}/MAXDEPTH
	B	SHA-3-512	2^{370}/MAXDEPTH
	C	ASCON-Hash-512	2^{374}/MAXDEPTH

Grover on Hash Functions

Birthday attack

19 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

A **birthday attack** is a bruteforce collision attack that exploits the mathematics behind the birthday problen
abuse communication between two or more parties. The attack depends on the higher likelihood of collisior
degree of permutations (pigeonholes). With a birthday attack, it is possible to find a collision of a hash funct
being the classical preimage resistance security with the same probability. There is a general (though disputed[1]) result that quantum computers can perform birthday attacks, thus breaking collision resistance, in $\sqrt[3]{2^n} = 2^{n/3}$.[2]

Daniel J. Bernstein. "Cost analysis of hash collisions : Will quantum computers make SHARCS obsolete?" (PDF). *Cr.yp.to*. Retrieved 29 October 2017.

Grover on Hash Functions

Consideration

- BHT algorithm의 $O(2^{n/3})$ 는 이상적인 복잡도

There is a popular myth that the Brassard–Høyer–Tapp algorithm reduces the cost of b-bit hash collisions from $2^{b/2}$ to $2^{b/3}$; this myth rests on a nonsensical notion of cost and is debunked in this paper.

- Classical algorithm이 더 효율적임
  - Van Oorschot-Wiener algorithm → $O\left(2^{\frac{n}{4}}\right)$
  - 이건 크게 상관 없을 듯함

Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?

Daniel J. Bernstein *

Department of Computer Science (MC 152)
The University of Illinois at Chicago
Chicago, IL 60607–7053
djb@cr.yp.to

Abstract. Current proposals for special-purpose factorization hardware will become obsolete if large quantum computers are built: the number-field sieve scales much more poorly than Shor's quantum algorithm for factorization. Will *all* special-purpose cryptanalytic hardware become obsolete in a post-quantum world?

A quantum algorithm by Brassard, Høyer, and Tapp has frequently been claimed to reduce the cost of b-bit hash collisions from $2^{b/2}$ to $2^{b/3}$. This paper analyzes the Brassard–Høyer–Tapp algorithm and shows that it has fundamentally worse price-performance ratio than the classical van Oorschot–Wiener hash-collision circuits, even under optimistic assumptions regarding the speed of quantum computers.

Grover on Hash Functions

- **Consideration**

Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?

Daniel J. Bernstein *

Department of Computer Science (MC 152)
The University of Illinois at Chicago
Chicago, IL 60607–7053
djb@cr.yp.to

Abstract. Current proposals for special-purpose factorization hardware will become obsolete if large quantum computers are built: the number-field sieve scales much more poorly than Shor's quantum algorithm for factorization. Will *all* special-purpose cryptanalytic hardware become obsolete in a post-quantum world?

A quantum algorithm by Brassard, Høyer, and Tapp has frequently been claimed to reduce the cost of b-bit hash collisions from $2^{b/2}$ to $2^{b/3}$. This paper analyzes the Brassard–Høyer–Tapp algorithm and shows that it has fundamentally worse price-performance ratio than the classical van Oorschot–Wiener hash-collision circuits, even under optimistic assumptions regarding the speed of quantum computers.

Grover on Hash Functions

Consideration # 1

- **BHT algorithm의 $O(2^{n/3})$ 는 이상적인 복잡도** (두 가지 이유)

> There is a popular myth that the Brassard–Høyer–Tapp algorithm reduces the cost of b-bit hash collisions from $2^{b/2}$ to $2^{b/3}$; this myth rests on a nonsensical notion of cost and is debunked in this paper.

- **1.** Quantum ram access 및 size 비용
- 2. Search수는 Grover에 의해 줄어들지만, 내부의 해시 값 비교 step은 줄어들지 않음

> - Realistic two-dimensional models of quantum computation, just like realistic models of non-quantum computation, need time $M^{1/2}$ for random access to a table of size M. This $M^{1/2}$ loss is as large as the $M^{1/2}$ speedup claimed by Brassard, Høyer, and Tapp.
> - A straight-line circuit to compare $H(y)$ to $H(x_1), H(x_2), \ldots, H(x_M)$ uses $\Theta(Mb)$ bit operations, so a quantum circuit has to use $\Theta(Mb)$ qubit operations. Sorting the table $H(x_1), H(x_2), \ldots, H(x_M)$ does not reduce the size of a *straight-line* comparison circuit, so it does not reduce the number of quantum operations. The underlying problem

Grover on Hash Functions

- **Consideration # 2**
  - Classical algorithm이 더 효율적임
    - Van Oorschot-Wiener algorithm → $O(2^{n/4})$

Many authors have claimed that quantum computers will have an impact on the complexity of hash collisions, reducing time $2^{b/2}$ to time $2^{b/3}$. In fact, time $2^{b/3}$ had already been achieved by non-quantum machines of size just $2^{b/6}$, and smaller time $2^{b/4}$ had already been achieved by non-quantum machines of size $2^{b/4}$. Anyone afraid of quantum hash-collision algorithms already has much more to fear from non-quantum hash-collision algorithms.

Grover on Hash Functions

- Van Oorschot-Wiener algorithm → $O(2^{n/4})$
  - Quantum 구현? → 비효율적이며 굳이

Search Complexity

2^{64} (key search)	AES-128	2^{157}/MAXDEPTH quantum gates or 2^{143} classical gates
2^{64} (VW)	SHA3-256	2^{146} classical gates
2^{96} (key search)	AES-192	2^{221}/MAXDEPTH quantum gates or 2^{207} classical gates
2^{96} (VW)	SHA3-384	2^{210} classical gates
2^{128} (key search)	AES-256	2^{285}/MAXDEPTH quantum gates or 2^{272} classical gates
2^{128} (VW)	SHA3-512	2^{274} classical gates

- SHA-3 비용이 AES보다 낮음 (SHA-2는 AES 보다 더 높음)

- **Quantum security level의 구분이 모호해짐**

Grover on Hash Functions

- 우선 BHT algorithm로 채택 → $O(2^{n/3})$

Category	Cipher	Quantum gate count
Level 1	AES-128	2^{157}/MAXDEPTH
Level 2	**SHA-2-256/SHA-3-256**	**Unspecified**
Level 3	AES-192	2^{221}/MAXDEPTH
Level 4	**SHA-2-384/SHA-3-384**	**Unspecified**
Level 5	AES-256	2^{285}/MAXDEPTH
Level 6	**SHA-2-512/SHA-3-512**	**Unspecified**

Combine

Level 5

Table 2: Security levels defined in this work.

Strength	Category	Hash function	Quantum gate count
Level 2	A	SHA-2-256	2^{205}/MAXDEPTH
	B	SHA-3-256	2^{200}/MAXDEPTH
	C	ASCON-Hash-256	2^{201}/MAXDEPTH
Level 4	A	SHA-2-384	2^{292}/MAXDEPTH
	B	SHA-3-384	2^{285}/MAXDEPTH
	C	ASCON-Hash-384	2^{287}/MAXDEPTH
Level 6	A	SHA-2-512	2^{377}/MAXDEPTH
	B	SHA-3-512	2^{370}/MAXDEPTH
	C	ASCON-Hash-512	2^{374}/MAXDEPTH

In Bernstein's analysis [Ber09], the author assessed the impact of quantum collision search on classical search and the impact of quantum attacks. This paper focuses on presenting regularized quantum complexities for levels 2, 4, and 6 that have yet to be defined, rather than developing stronger quantum attacks than non-quantum attacks.

Thank you!