Quantum Collision Attacks on Reduced SHA-256 and SHA-512

Basic operators used in Quantum computing (1/2)

n - bit strings : x,y

Eg. - x = $\underbrace{1000010101\ldots11.1010,}_{\text{n-bits}}$ y = $\underbrace{10011010101\ldots11.1010}_{\text{n-bits}}$

Bitwise AND: x Λ y

Bitwise OR: x V y

Bitwise XOR: x ⊕ y

Negation x : ¬ x

Basic operators used in Quantum computing (2/2)

n - bit strings : x

$m \in Z^+$ (set of positive integers)

$m \leq n$

m - bit right shift operator on x : $x \gg m$

m - bit circular right shift operator on x : $x \ggg m$

Modular addition : $\boxplus$, +

Set of n- bit strings : $\{0,1\}^n$

Explanation of some Keywords

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Function
- SHA- 256 and SHA- 512
- Collision Attack
- Quantum Attack
- Merkle Damgard Construction
- Davies - Meyer Construction
- 2-Block Collision attack

Symmetric Key Cryptography

Also known as Symmetric Encryption

Symmetric means a single secret key is used for both encryption and decryption.

Data is changed to a format that can't be read or inspected by anyone who doesn't have the secret key used to encrypt it throughout symmetric encryption process.

There is one secret key (ciphertext) which is used to encrypt the message from Bob and decrypt the message to Alice.

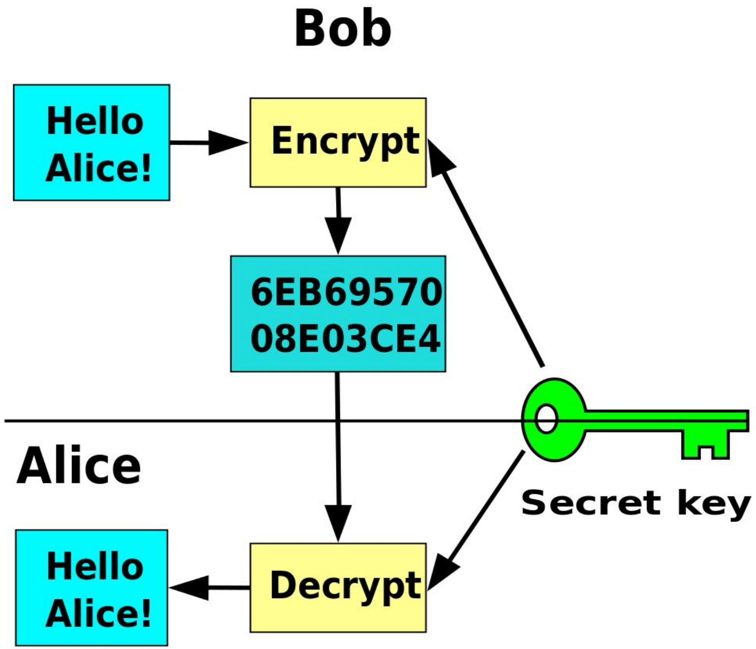


Fig: Symmetric key encryption

Asymmetric Key Cryptography

Also known as Public Key Cryptography

It protects sensitive and classified information going into wrong hands.

To encrypt and decode a message and safeguard it from unauthorised access or use, we'll need pair of keys : one public key and one private key for both sender and receiver.

The corresponding private key is used for decryption if the public key is used for encryption and vice-versa.

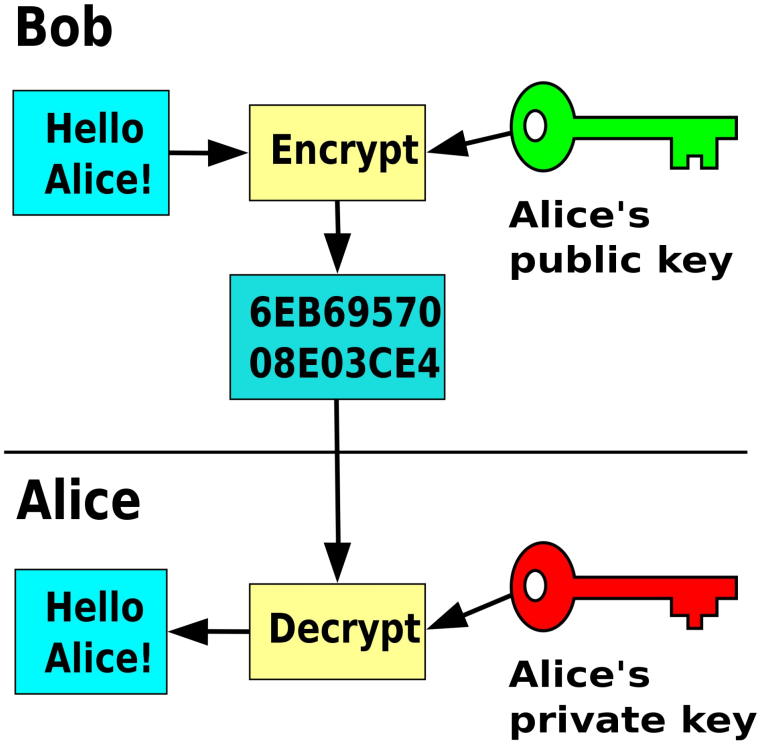


Fig: Asymmetric key encryption

Hash function

A hash function turns a numerical input value into another compressed numerical value. The hash function accepts any length input, but the output is always of the same length.

Hash functions converts arbitrary length data to fixed length data. Output is very much smaller than the data we take as input.Output is also called digest (smaller length).

Computing h(x) for any hash function h with input x is a quick procedure and hash functions are much faster than symmetric cryptography.

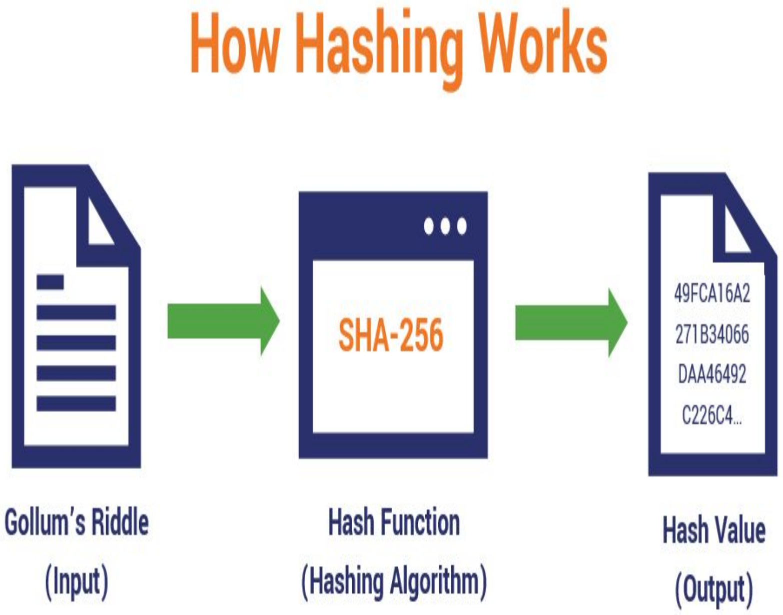


Fig: Hashing using SHA-256 Algorithm

SHA-256 and SHA-512

Consists in SHA-2 family (Davies-Meyer + Merkle-Damgard) and for a text, SHA-256 provides a nearly-unique 256-bit (32-byte) signature.

SHA-256 is one of the most powerful hash functions known, and it is one of the successor hash functions to SHA-1 (together referred to as SHA-2). SHA-256 isn't substantially more difficult to code than SHA-1, and it hasn't been hacked yet.

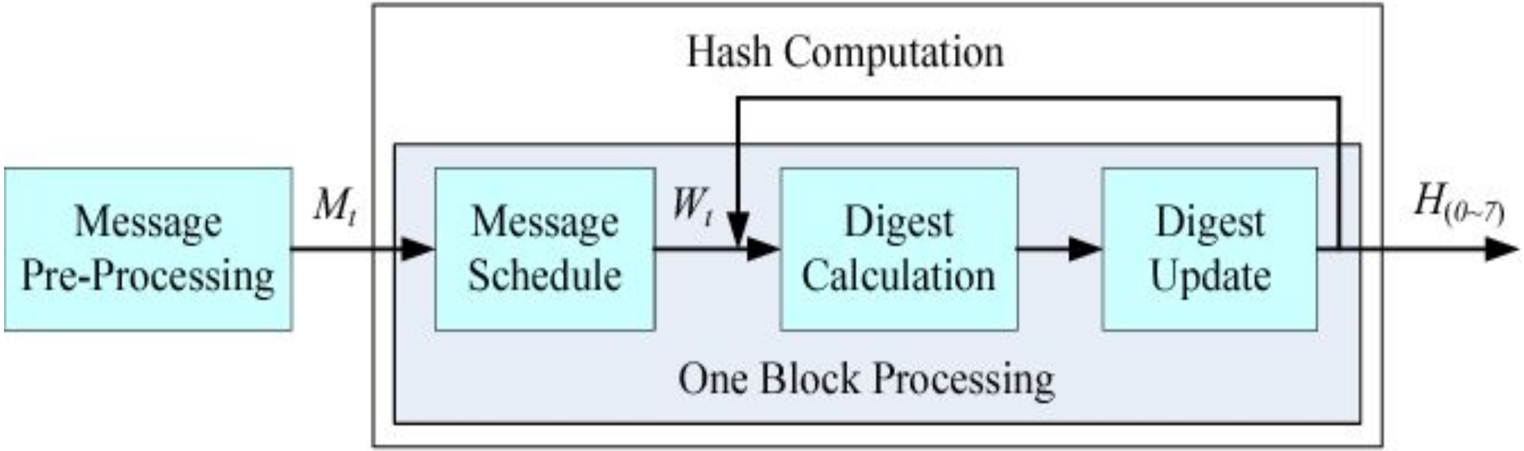
SHA-512 provides a nearly-unique 64-byte signature.

SHA-512 is faster than SHA-256 because of its blocks size (operation rounds are more).

SHA-512 has 4 stages: Input formatting, Hash buffer initialization, Message processing, Output.

SHA-256 algorithm flow diagram

II. SHA-256 HASH FUNCTION



Collision Attack

Collision Attack means if two inputs giving the same output (A Hash Collision Attack aims to locate two hash function input strings that generate the same hash result).

There will be possibility of collision attack because of infinite input length but finite output length

For example:

$$\left.\begin{array}{l}\text{hash(cat)=2345643} \\ \text{hash(34546542) = 2345643}\end{array}\right\}$$

Different input, but have same output

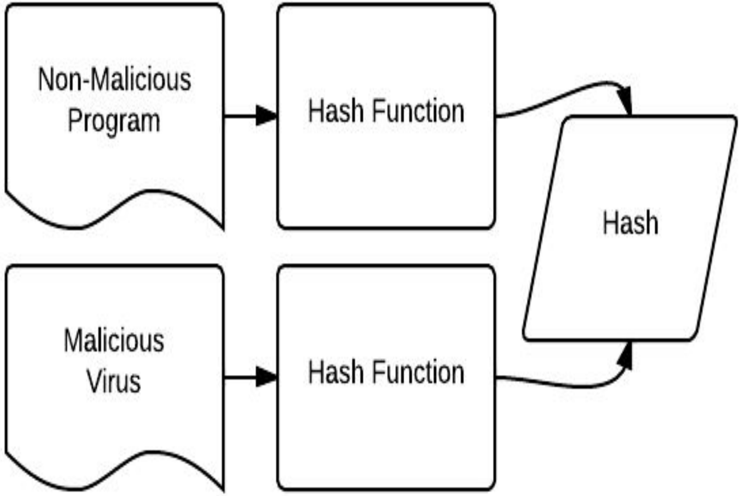


Fig: Hash collision Attack

Quantum attack

Also known as post-quantum cryptography (also known as quantum-proof, quantum-safe, or quantum-resistant).

Cryptographic methods (typically public-key algorithms) that are expected to be secure against a cryptanalytic attack by a quantum computer.

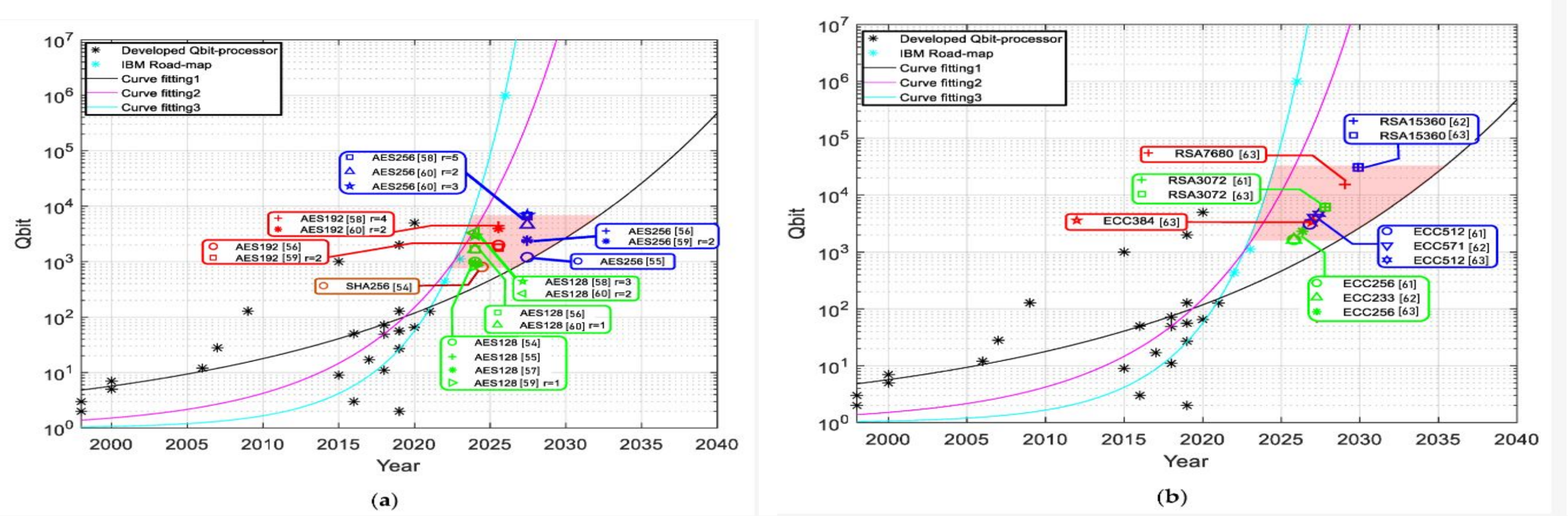


Fig.: Quantum road map and expected quantum attack timing: (**a**) symmetric-k algorithm (AEAD) (**b**) key exchange and signature and certification.

Specification of SHA-256

1) Construction adopt : Merkle-Damgård
2) Compression functions adopt : Davies -Meyer
3) Word size : w
   a) |w| = 32
4) Message block : M
   a) |M| = 16|w| bits = 16 * 32 bits = 512 bits
5) Chaining values : H
   a) |H| = 8|w| bits = 8 * 32 bits = 256 bits
6) Final output
   a) |Final output| = 8|w| bits = 8 * 32 bits = 256 bits
7) Number of steps : r
   a) r = 64

Specification of SHA-512

1) Construction adopt : Merkle-Damgård
2) Compression functions adopt : Davies -Meyer
3) Word size : w
   a) |w| = 64
4) Message block : M
   a) |M| = 16|w| bits = 16 * 64 bits = 1024 bits
5) Chaining values : H
   a) |H| = 8|w| bits = 8 * 64 bits = 512 bits
6) Final output
   a) |Final output| = 8|w| bits = 8 * 64 bits = 512 bits
7) Number of steps : r
   a) r = 80

Merkle-Damgård Construction (1/n) …continue

Let $h : \{0,1\}^{n+t} \rightarrow \{0,1\}^n$ be a compression function. Then the Merkle-Damgård transformation of h is $MD_h : \{0,1\}^* \rightarrow \{0,1\}^n$, where:

```
$\mathbf{MDPAD_t(x)}$
$\ell := |x|$, as length-t binary number
While $|x|$ not a multiple of $t$:
    $x := x||0$
return $x||\ell$
```

Merkle-Damgård Construction (2/n) …continue

```
**$MD_h(x)$**
$x_1||...||x_{k+1}$ := $MDPAD_t(x)$
// each $x_i$ is t bits
$y := 0^n$
For i=1 to k+1:
        $y := h(y_{i-1}||x_i)$
Output $y_{k+1}$
```

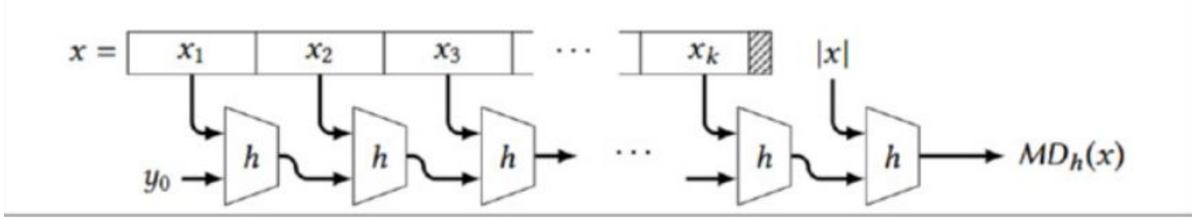


Fig: Merkle-Damgård Construction

Davies - Meyer Construction

Davies-Meyer is a compression function that can be used to create cryptographic hash functions.

The simple idea of the Davies-Meyer construction is that you compress a block of text into "n" bits with the use of an encryption algorithm putting an "n" bit random initial value as message and using your block of text as the key. Thus the result after encryption is an n-bit block.

It is very important to XOR the results of the encryption with the initial value, otherwise, it will be very difficult to prevent a collision which will result in bad cryptographic hash function.

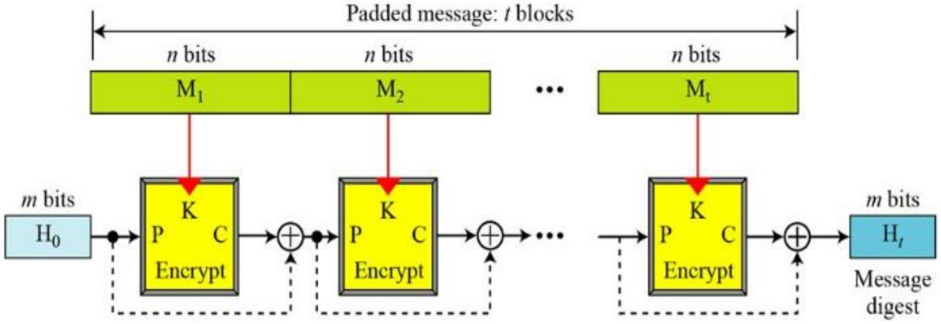


Fig. Davies - Meyer construction

Chaining values or Initial values IV

Length of Chaining values : H

$|H| = 8|w|$ bits = 8 * 32 bits = 256 bits

(For SHA-256)

$H = (H_0,H_1,H_2.....,H_7) \in (\{0,1\}^w)^8$

Message block M

For SHA-256, $M = (M_0,M_1,M_2.....,M_{15}) \in (\{0,1\}^w)^{16}$

Output value of compression function : f(H,M)

Message expansion 1/3

For SHA-256, r = 64

For SHA-512, r = 80

Compute, all W_i (i = 0,1,2,3,.........,r-1)

$$W_i = \begin{cases} M_i & , i = 0,1,2,3,.........,15 \\ \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15})+W_{i-16} & , i = 16,17,18.....,(r-1) \end{cases}$$

$\sigma_0, \sigma_1 : \{0,1\}^w \rightarrow \{0,1\}^w$

Iterative states update (1/n)

Initially set,

$$st_{0-1} := H = (H_0,H_1,H_2.....,H_7) \in (\{0,1\}^w)^8$$

We have to update the state for i=0,1,2,3, ….., (r-1)

$$st_{i-1} = (A_{i-1} ,A_{i-2} ,A_{i-3} ,A_{i-4} ,E_{i-1} ,E_{i-2} ,E_{i-3} ,E_{i-4})$$

$$\downarrow$$

$$st_{i} = (A_{i} ,A_{i-1} ,A_{i-2} ,A_{i-3} ,E_{i} ,E_{i-1} ,E_{i-2} ,E_{i-3})$$

Iterative states update (2/n) ….Continue

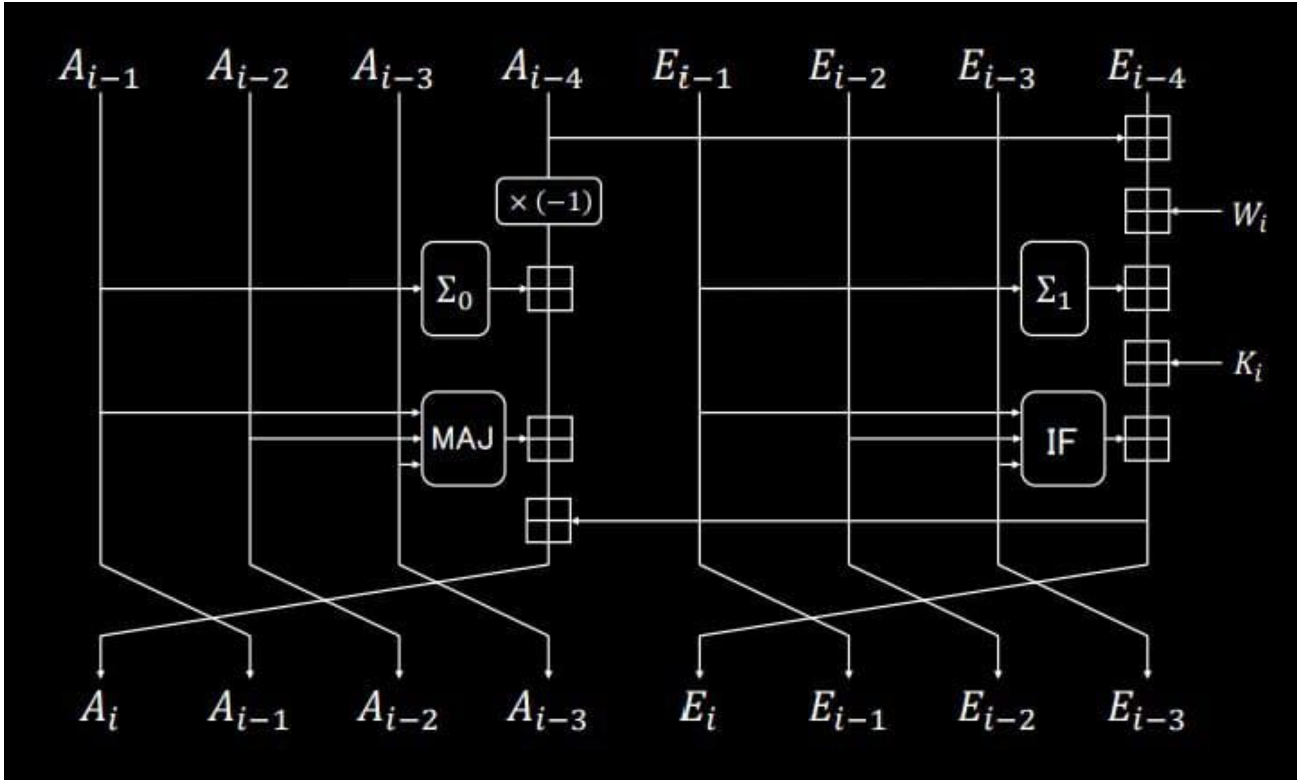


Fig. State update function

Iterative states update (3/n) ….Continue

$E_i := E_{i-4} + A_{i-4} + \Sigma_1(E_{i-1}) + \mathrm{IF}(E_{i-1}, E_{i-2}, E_{i-3}) + K_i + W_i$

$A_i := \Sigma_0(A_{i-1}) + \mathrm{MAJ}(A_{i-1}, A_{i-2}, A_{i-3}) + E_i - A_{i-4}$

IF, MAJ : $(\{0,1\}^w)^3 \rightarrow \{0,1\}^w$

K_i : step-dependent constant

We can remove K_i (as it doesn’t affect our attacks)

Computing next chaining value f(H,M) (1/n)

Next chaining value, $f(H,M) := st_{r-1} + H$

(Here + is word-wise modular addition)

IF, MAJ : $(\{0,1\}^w)^3 \rightarrow \{0,1\}^w$

For both SHA-256 and SHA-512,

IF $(x,y,z) = (x \wedge y) \oplus ((\neg\ x) \wedge\ y)$

MAJ$(x,y,z) = (x \wedge y) \oplus (y \wedge z) \oplus (z \wedge x)$

Computing next chaining value f(H,M) (2/n) ….Continue

For SHA-256,

$\Sigma_0(x) = (x \ggg 2) \oplus (x \ggg 13) \oplus (x \ggg 22)$

$\sigma_0(x) = (x \ggg 7) \oplus (x \ggg 18) \oplus (x \ggg 3)$

$\Sigma_1(x) = (x \ggg 6) \oplus (x \ggg 11) \oplus (x \ggg 25)$

$\sigma_1(x) = (x \ggg 17) \oplus (x \ggg 19) \oplus (x \ggg 10)$

Computing next chaining value f(H,M) (3/n) ….Continue

For SHA-512,

$\Sigma_0(x) = (x \ggg 28) \oplus (x \ggg 34) \oplus (x \ggg 39)$

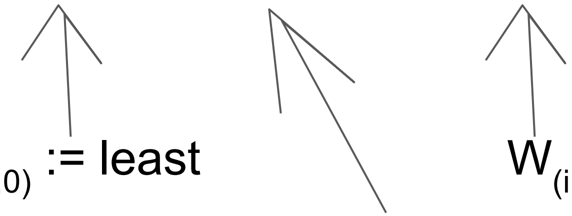
$\sigma_0(x) = (x \ggg 1) \oplus (x \ggg 8) \oplus (x \ggg 7)$

$\Sigma_1(x) = (x \ggg 14) \oplus (x \ggg 18) \oplus (x \ggg 41)$

$\sigma_1(x) = (x \ggg 19) \oplus (x \ggg 61) \oplus (x \ggg 6)$

Message Expansion bit notation : $W_{i,j}$

$W_i = \underline{0}10101\ldots\underline{1}\ldots..101\ldots\underline{0}$



$W_{(i,0)}$:= least significant bit

$W_{(i,w-1)}$:= most significant bit

$W_{(i,j)}$:= j^{th} bit in $W_i = W_{(i,j)} = 1$

Quantum Computation

H := Hadamard Operator

$H\,|b\rangle = \sum_{c\in\{0,1\}} (-1)^{b\cdot c}\,|c\rangle$, for $b \in \{0, 1\}$

$f:\ \{0, 1\}^m \longrightarrow \{0, 1\}^n$

Quantum Oracle

$f:\ \{0, 1\}^m \longrightarrow \{0, 1\}^n$

Quantum oracle of f , O_f (unitary operator)

$:= O_f\,|x\rangle|\,y\rangle = |\,x\rangle\,|\,y \oplus f(x)\,\rangle$, for $x \in \{0, 1\}^m$ and for $y \in \{0, 1\}^n$

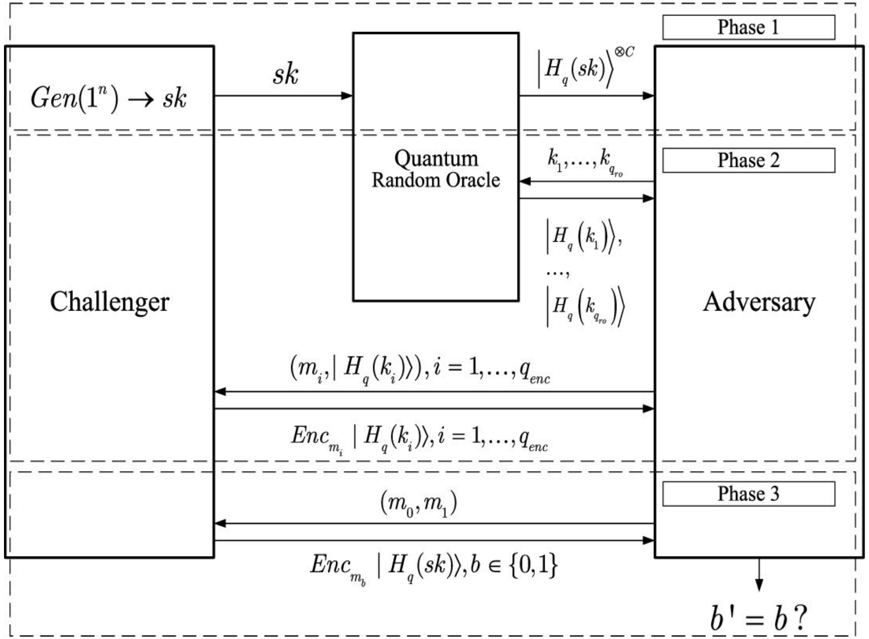

Phase 1
$Gen(1^n) \to sk$
sk
Quantum Random Oracle
$|H_q(sk)\rangle^{\otimes C}$
Phase 2
$k_1,\ldots,k_{q_{ro}}$
Challenger
$|H_q(k_1)\rangle,$
$\ldots,$
$|H_q(k_{q_{ro}})\rangle$
Adversary
$(m_i, |H_q(k_i)\rangle), i = 1,\ldots,q_{enc}$
$Enc_{m_i}|H_q(k_i)\rangle, i = 1,\ldots,q_{enc}$
Phase 3
(m_0, m_1)
$Enc_{m_b}|H_q(sk)\rangle, b \in \{0,1\}$
$b' = b?$

Fig: Quantum random Oracle Model

Grover’s Algorithm (1/n)

It is quantum algorithm to solve database search problem.

Let $F : \{0, 1\}^{n} \rightarrow \{0, 1\} : | F^{-1}(1)| > 0$

To find $x : F(x) = 1 \Leftrightarrow$ data has x points to search

And we have also considered that there is only one point assume which satisfies this condition.

Suppose we have $t := |F^{-1}(1)|$ for which $t/2^n << 1$

Grover’s Algorithm (2/n) …. Continue

To solve the problem,

Queries are required for classical algorithms = $O(2^n/t)$

Queries are required for classical algorithms = $O((2^n/t)^{1/2})$

Suppose ∃ Q (Quantum circuit that computes F) ,

Time taken = T_F (depth of circuit)

Qubits used = S_F (width of circuit)

Grover's Algorithm (3/n) ....Continue

Then Grover's algo finds a solution in time :

T_F . (π/4). $(2^n/t)^{1/2}$ (using S_F+1 qubits)

Quantum algo on F := Grov(F,i)

i $\in Z^+$ (set of positive integers)

Step - 1: Prepare initial state ,$|\Psi_{init}\rangle := H^{\otimes(n+1)} |0^n\rangle| 1\rangle$

Step - 2 : Processing/Iterative steps (1/m)

Let θ be the value satisfies $\sin^2 \theta = t/2^n$, $0 \leq \theta \leq \pi/2$

Grover’s Algorithm (4/n) ….Continue

Step - 2 : Processing/Iterative steps (2/m)

Apply the unitary operator $Q_F := -(H^{\otimes n} \otimes I)(O_0 \otimes I)(H^{\otimes n} \otimes I)O_F$

iterativeIy i times on $|\Psi_{init}\rangle$.

Here, quantum oracle of F := O_F

& O_0 is the operator such that

$O_0 |x\rangle = (-1)^{\delta(x,0^\wedge n)} |x\rangle$

$\delta_{(x,y)}$:= Kronecker’s delta such that $\delta_{x,y} = 1$ if $x = y$ and $\delta_{x,y} = 0$ if $x \neq y$

Grover's Algorithm (5/n) ….Continue

Step - 3 : Measure the resulting state $Q_F^{\,i}\ |\psi_{init}\rangle$

Output will be most significant n bits

i : = number of iterations

When we set i = $\lfloor\pi/4\theta\rfloor$, then algorithm Grov(F, $\lfloor\pi/4\theta\rfloor$) outputs x :F(x) = 1 with a probability at least $(1 - t/N)$

Since $\pi/4\ \theta \le \pi/(4 \sin\theta) = (\pi/4)(2^n/t)^{½}$ holds (as $\sin^2\theta = t/2^n$, $0 \le \theta \le \pi/2$)

The running time of Grov(F, $\lfloor\pi/4\theta\rfloor$) is at most $T_F \cdot (\pi/4)(2^n/t)^{½}$

Grover’s Algorithm (6/n) ….Continue

Parallelization :

Let’s denote quantum computers by P.

When P ≥ 2, by running P copies of Grov(F, Lπ/4θ⌋√ P) in parallel,

We can find a solution in time

$= T_F \cdot (\pi/4)(2^n/t.P)^{½}$ with probability at least 1-1/e

(we always consider the case that $(t \cdot P)/2^{n} << 1$)

Cost Evaluation

The running time of a quantum circuit is proportional to the depth of the circuit

The costs of quantum error corrections are not considered

We assume that there exists an implementation of the attack target primitive (i.e., SHA-256 or SHA-512) on a quantum circuit C

We regard that the unit of depth and width of quantum circuits is the depth width of C respectively.

Communication costs will not be significant in our attacks because we use quantum circuits just for running the Grover search

2-Block Collision Attack (classical and quantum) (1/n)

We can locate a 2-block collision in time 2^{n-x} if we can make many semi-free-start collisions for 2^{x} choices of IVs.

We can locate a 2-block collision in time 2^{n-x} if we can make many semi-free-start collisions for 2^{x} IV alternatives (Grover).

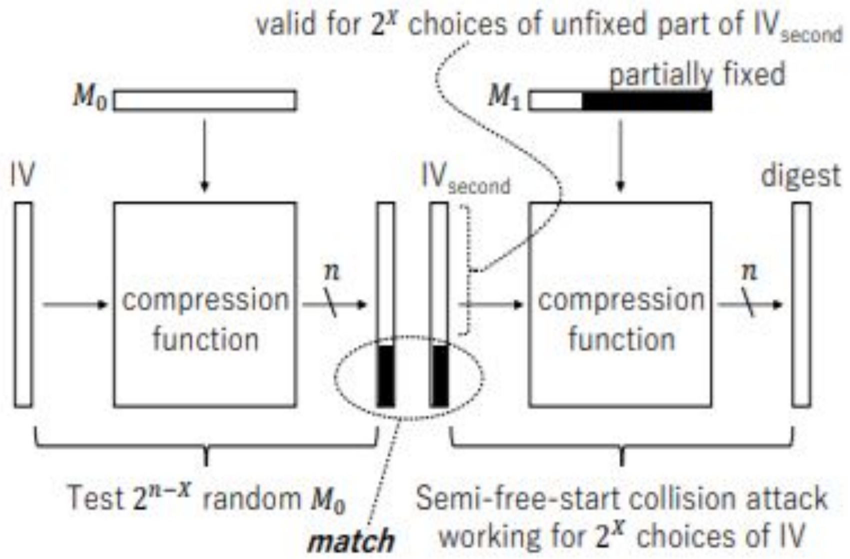

valid for 2^x choices of unfixed part of IV_{second}
M_0
M_1
partially fixed
IV
IV_{second}
digest
compression function
compression function
n
n
Test 2^{n-x} random M_0
match
Semi-free-start collision attack working for 2^x choices of IV

Fig. Converting semi free collision into 2-block collisions

2-Block Collision Attack (classical and quantum) (2/n)

The attack can be parallelized if S-qubits are available: T=√ 2 $^{n-x}$ /S. Here, generic attack = √ 2 ^{n} /S

The generic is valid if √ 2 $^{n-x}$ /S < √ 2 ^{n} /S if X>0 and S < 2 ^{x} (X condition is stronger).

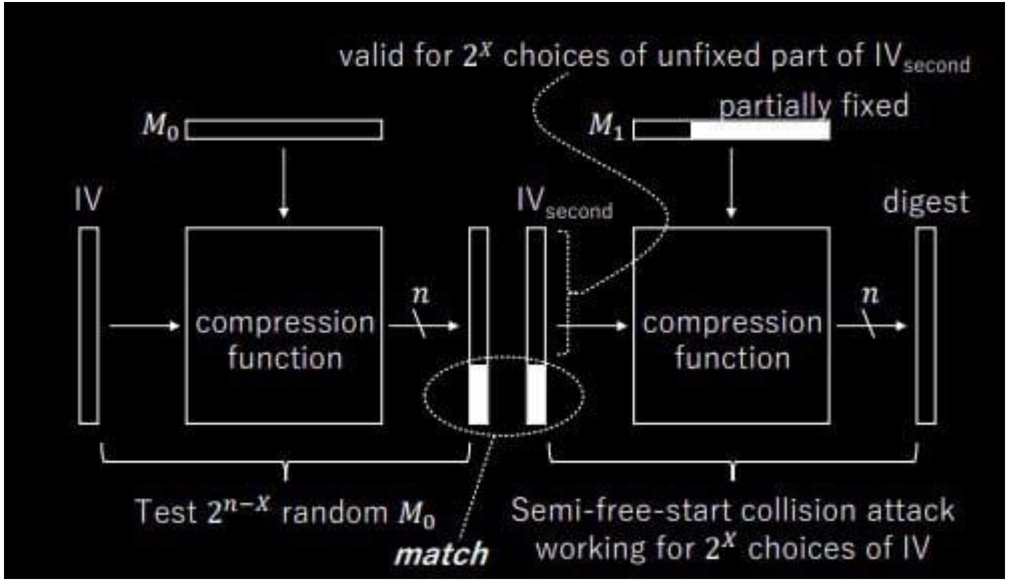

valid for 2^X choices of unfixed part of IV_{second}
M_0
M_1
partially fixed
IV
IV_{second}
digest
compression function
n
compression function
n
Test 2^{n-X} random M_0
match
Semi-free-start collision attack working for 2^X choices of IV

Fig. Converting semi free collision into 2-block collisions

Collision Attack on 31-Step SHA-256 (1/n)

It is a 2-block collision with time complexity $2^{65.5}$.

2-block collision := $(M^{\sim} || M, M^{\sim} || M')$

(here, $M, M', M^{\sim}$ are in $\{0, 1\}^{512}$, $M \neq M'$)

Construction of 2-block collision:

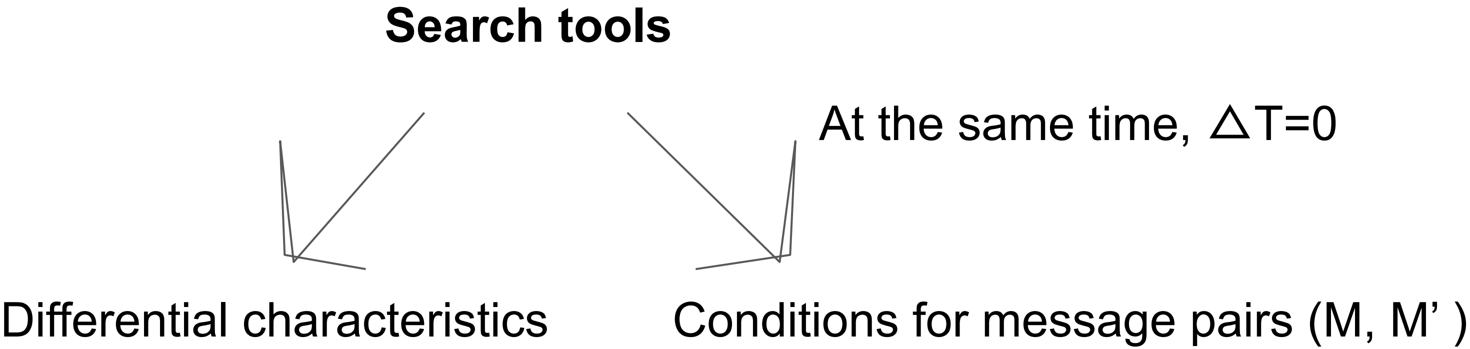
It is constructed by searching for a random message $M^{\sim}$ for the first block and a semi-free-start collision (M, M') for the second block

Such that the output of the first block is the IV of the second block.

Collision Attack on 31-Step SHA-256 (2/n) ….Continue

Semi-free-start collisions in the second block are constructed

Semi-free-start collisions is based on a local collision that starts at step 5 and ends at step 18, which is found by using heuristic automated search tools.



Search tools

At the same time, $\triangle T=0$

Differential characteristics

Conditions for message pairs (M, M’)

Collision Attack on 31-Step SHA-256 (3/n) ….Continue

Notations for differential characteristic and conditions for (M, M’)

1. “-” indicates that the bit associated with M at the position must be equal to the corresponding bit associated with M’ .

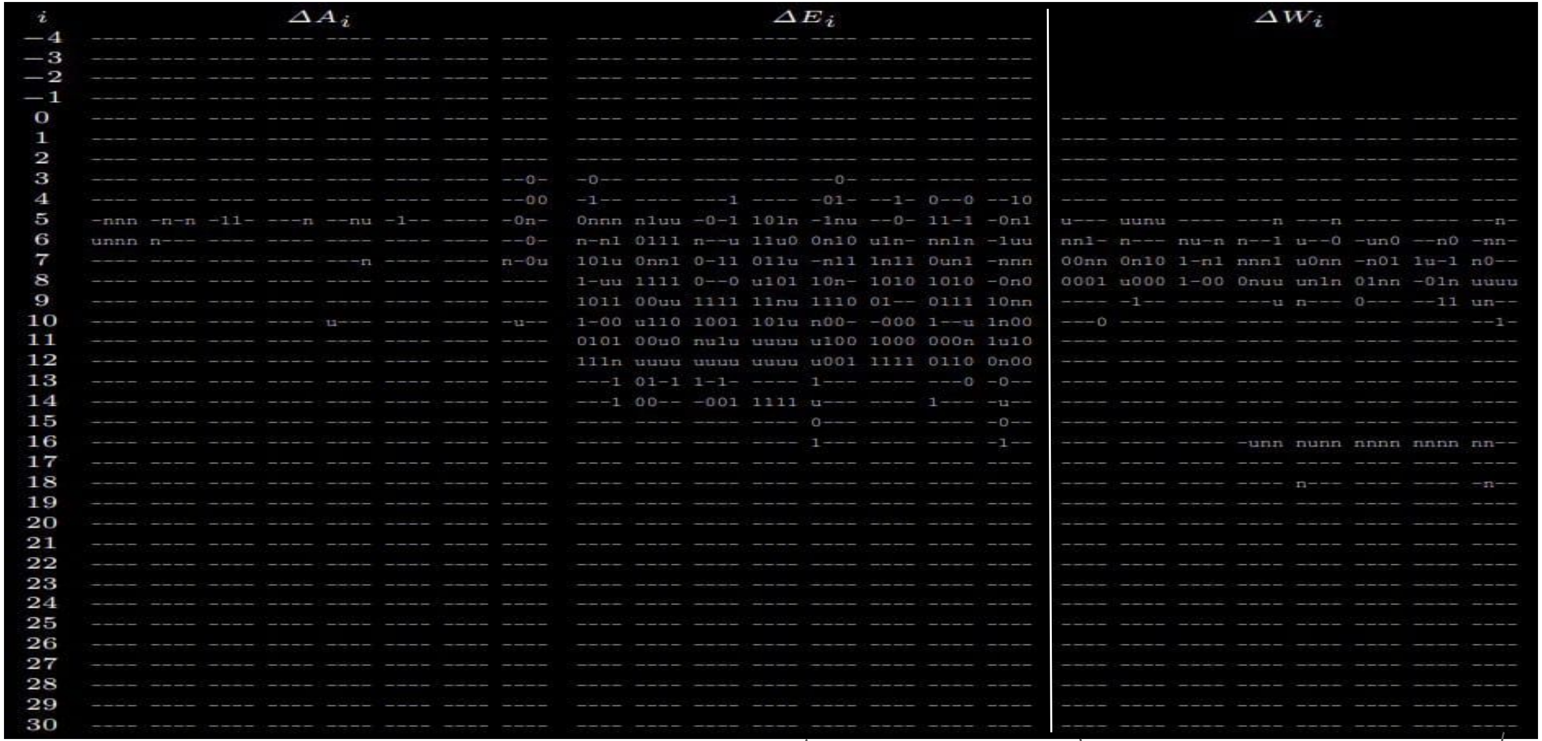
2. “0” indicates that the bit at the position must be 0 for both of M and M’ .

3. “1” indicates that the bit at the position must be 1 for both of M and M’ .

4. “u” indicates that the bit at the position must be 1 for M and 0 for M’ .

5. “n” indicates that the bit at the position must be 0 for M and 1 for M’ .

31-step differential characteristic for SHA-256



i	ΔA_i	ΔE_i	ΔW_i
−4	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
−3	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
−2	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
−1	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
0	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
1	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
2	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
3	---- ---- ---- ---- ---- ---- ---- --0-	-0-- ---- ---- ---- --0- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
4	---- ---- ---- ---- ---- ---- ---- --00	-1-- ---- ---1 ---- -01- --1- 0--0 --10	---- ---- ---- ---- ---- ---- ---- ----
5	-nnn -n-n -11- ---n --nu -1-- ---- -0n-	0nnn n1uu -0-1 101n -1nu --0- 11-1 -0n1	u--- uunu ---- ---n ---n ---- ---- --n-
6	unnn n--- ---- ---- ---- ---- ---- --0-	n-n1 0111 n--u 11u0 0n10 u1n- nn1n -1uu	nn1- n--- nu-n n--1 u--0 -un0 --n0 -nn-
7	---- ---- ---- ---- ---n ---- ---- n-0u	101u 0nn1 0-11 011u -n11 1n11 0un1 -nnn	00nn 0n10 1-n1 nnn1 u0nn -n01 1u-1 n0--
8	---- ---- ---- ---- ---- ---- ---- ----	1-uu 1111 0--0 u101 10n- 1010 1010 -0n0	0001 u000 1-00 0nuu un1n 01nn -01n uuuu
9	---- ---- ---- ---- ---- ---- ---- ----	1011 00uu 1111 11nu 1110 01-- 0111 10nn	---- -1-- ---- ---u n--- 0--- --11 un--
10	---- ---- ---- ---- u--- ---- ---- -u--	1-00 u110 1001 101u n00- -000 1--u 1n00	---0 ---- ---- ---- ---- ---- ---- --1-
11	---- ---- ---- ---- ---- ---- ---- ----	0101 00u0 nu1u uuuu u100 1000 000n 1u10	---- ---- ---- ---- ---- ---- ---- ----
12	---- ---- ---- ---- ---- ---- ---- ----	111n uuuu uuuu uuuu u001 1111 0110 0n00	---- ---- ---- ---- ---- ---- ---- ----
13	---- ---- ---- ---- ---- ---- ---- ----	---1 01-1 1-1- ---- 1--- ---- ---0 -0--	---- ---- ---- ---- ---- ---- ---- ----
14	---- ---- ---- ---- ---- ---- ---- ----	---1 00-- -001 1111 u--- ---- 1--- -u--	---- ---- ---- ---- ---- ---- ---- ----
15	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- 0--- ---- ---- -0--	---- ---- ---- ---- ---- ---- ---- ----
16	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- 1--- ---- ---- -1--	---- ---- ---- -unn nunn nnnn nnnn nn--
17	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
18	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- n--- ---- ---- -n--
19	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
20	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
21	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
22	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
23	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
24	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
25	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
26	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
27	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
28	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
29	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
30	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----

Internal Stage Conditions

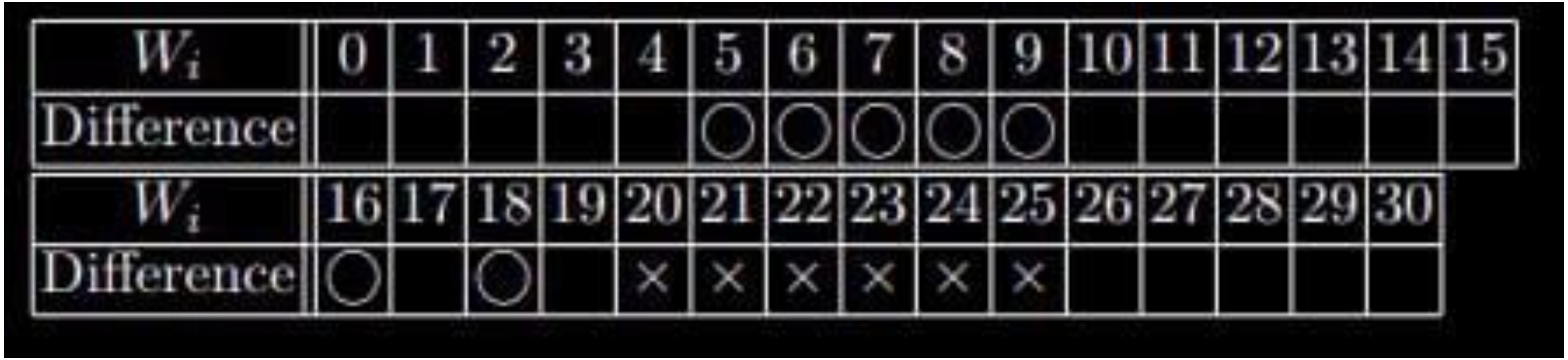
Message words Conditions

Collision Attack on 31-Step SHA-256 (4/n) ….Continue

For each i, by A_i , E_i , W_i we denote the words of internal states and expanded messages.

Attack procedure :

1) The position of the message words W_i where non-zero differences appear.



W_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Difference						○	○	○	○	○						

W_i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Difference	○		○		×	×	×	×	×	×					

Fig. position of the message words where non-zero differences appear

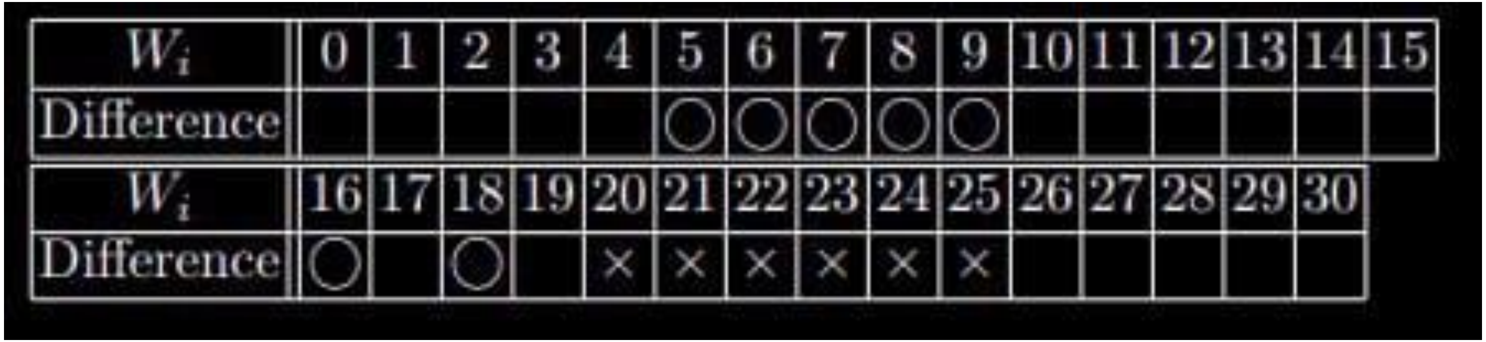
Collision Attack on 31-Step SHA-256 (5/n) ….Continue

Notation : "○" indicates that the word has non-zero difference.

"×" indicates that the word is computed from previous words

(but with non-zero differences but the difference is canceled out)

The position of the message words W $_i$ are computed from W_{i-2}, W_{i-7}, W_{i-15}, and W_{i-16} for i ≥ 16.



W_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Difference						○	○	○	○	○						

W_i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Difference	○		○		×	×	×	×	×	×					

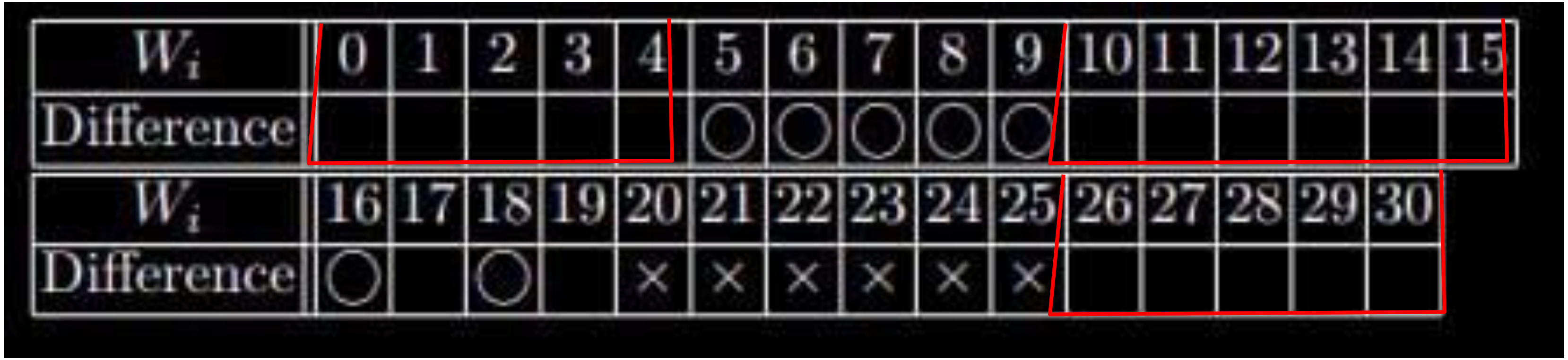
Collision Attack on 31-Step SHA-256 (6/n) ….Continue

Since W_0, . . . , W_4, W_{10}, . . . , W_{15} do not have differences,

W_{17}, W_{19}, W_{26}, . . . , W_{30} do not have differences, either.

Only seven message words (W_5, . . . , W_9, W_{16}, W_{18}) have differences.

The differences at W_{20}, . . . , W_{25} need to be canceled out



W_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Difference						○	○	○	○	○						

W_i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Difference	○		○		×	×	×	×	×	×					

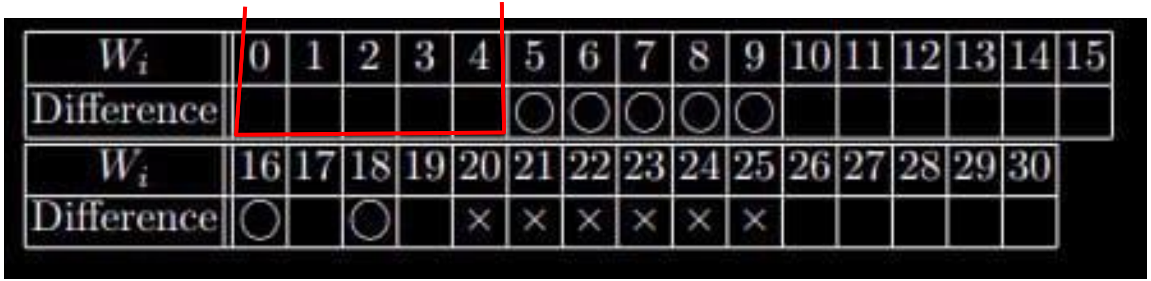
Collision Attack on 31-Step SHA-256 (7/n) ….Continue

Attack procedure :

2) W_0, . . . , W_4 can be chosen freely as no condition is imposed on these messages.

By 1) & 2) attack complexity will be $2^{99.5}$

Hence, the first attack with complexity $2^{99.5}$ and we will be reducing complexity to $2^{65.5}$ later.



W_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Difference						○	○	○	○	○						

W_i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Difference	○		○		×	×	×	×	×	×					

Collision Attack on 31-Step SHA-256 (8/n) ….Continue

A. The first attack with complexity 2 $^{99.5}$

f := the (31-step) compression function.

Procedure of collision attack with complexity $2^{99.5}$

Step-1: Determining the message words $W_5, \ldots, W_{12}$

Computing the internal states from the beginning of step 5 to the end of step 12 (in the second block).

The values of the variables $E_1, \ldots, E_4$ and $A_{-3}, \ldots, A_4$ are completely determined by the internal state at the beginning of step 5

Collision Attack on 31-Step SHA-256 (9/n) ….Continue

$A_{-1}||A_{-2}||A_{-3}$ correspond to the 96 most significant bits of the initial value of the second block.

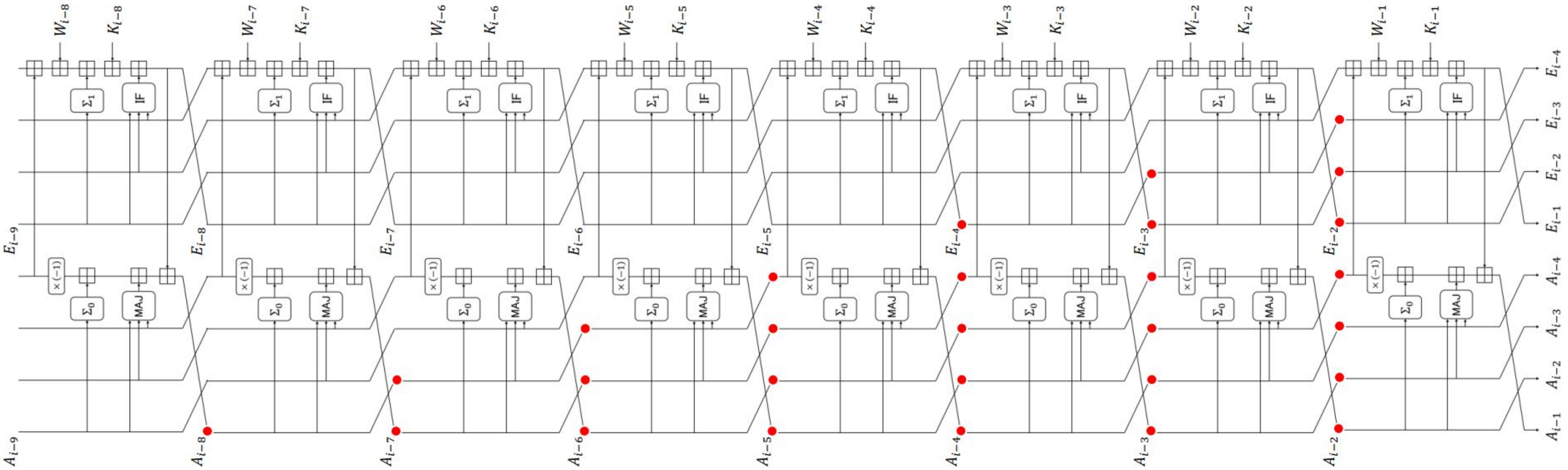
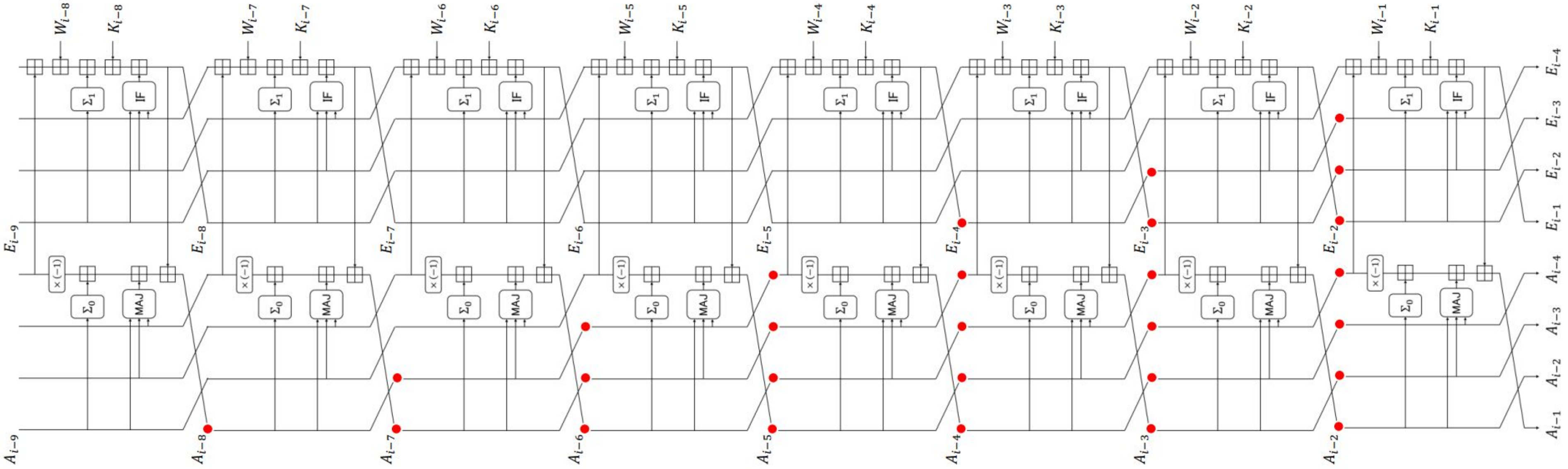


Fig. Internal state variables (pointed with red dots)

Collision Attack on 31-Step SHA-256 (10/n) ….Continue

The internal state variables (pointed with red dots) that are determined by computing step functions backwards from the internal state A_{i-1}|| · · · ||A_{i-4}||E_{i-1}|| . . . ||E_{i-4} at the beginning of step i.



Collision Attack on 31-Step SHA-256 (11/n) ….Continue

The attack in **Step-1** takes only seconds.

Step-2: To make 96 most significant bits of f(IV, $\tilde{M}$) is equal to $A_{-1}||A_{-2}||A_{-3}$,

We have to find a message $\tilde{M}$ for the first block

Compute the (uniquely determined) values $W_0, \ldots, W_4$ that is

compatible with chaining value f(IV, $\tilde{M}$) and the state at the beginning of step 5.

This step of the attack takes 2^{96} time.

Collision Attack on 31-Step SHA-256 (12/n) ….Continue

Step-3: Select W_0, . . . , W_{12} this time.

To fulfill the conditions on E_{13}, E_{14}, E_{15}, W_{16}, and W_{18} , use degrees of freedom in W_{13}, W_{14}, W_{15}

(in addition to the cancellation of differences at W20, . . . , W25).

Go back to **Step-2** if we fail to do it.

Due to the lack of degrees of freedom in W_{13}, W_{14}, W_{15} , this step of the attack

succeeds with 1/12 probability.

The total time complexity is estimated = $12 \cdot 2^{96} \approx 2^{99.5}$.

Collision Attack on 31-Step SHA-256 (13/n) ….Continue

B. The second attack with complexity $2^{65.5}$

Suppose that ℓ solutions can be found for Step-1 (of first attack with complexity $2^{99.5}$) Then, the complexity of Step-2 can be reduced from 2^{96} to $2^{96}/\ell$.

If a single solution in Step-1 can be found in time T_l ,

then the overall complexity = $T_l \cdot \ell + 12 \cdot 2^{96}/\ell$.

By experiment, $T_l \approx 2^{25.5}$, and they can expect $\ell \approx 2^{34}$

they deduced that a collision can be found with complexity

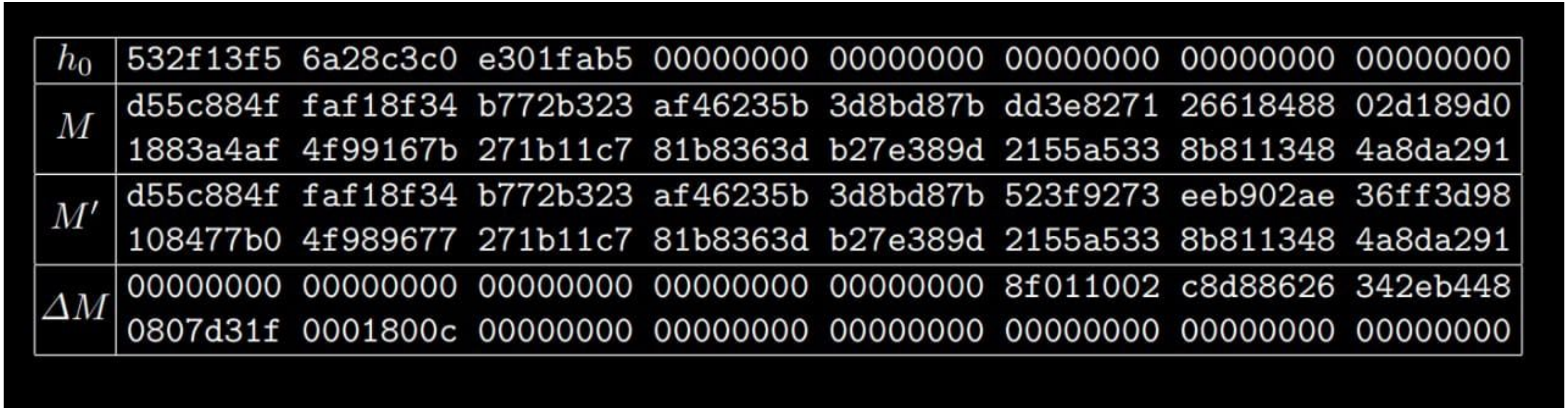
= $2^{25.5} \cdot 2^{34} + 12 \cdot 2^{96}/2^{34} \approx 2^{65.5}$.

Semi-free-start collision of 31-step SHA-256

$\Delta M := M \oplus M'$

h_0 := initial value of the compression function

First 5 message words can be chosen freely as $h_0 = 0$



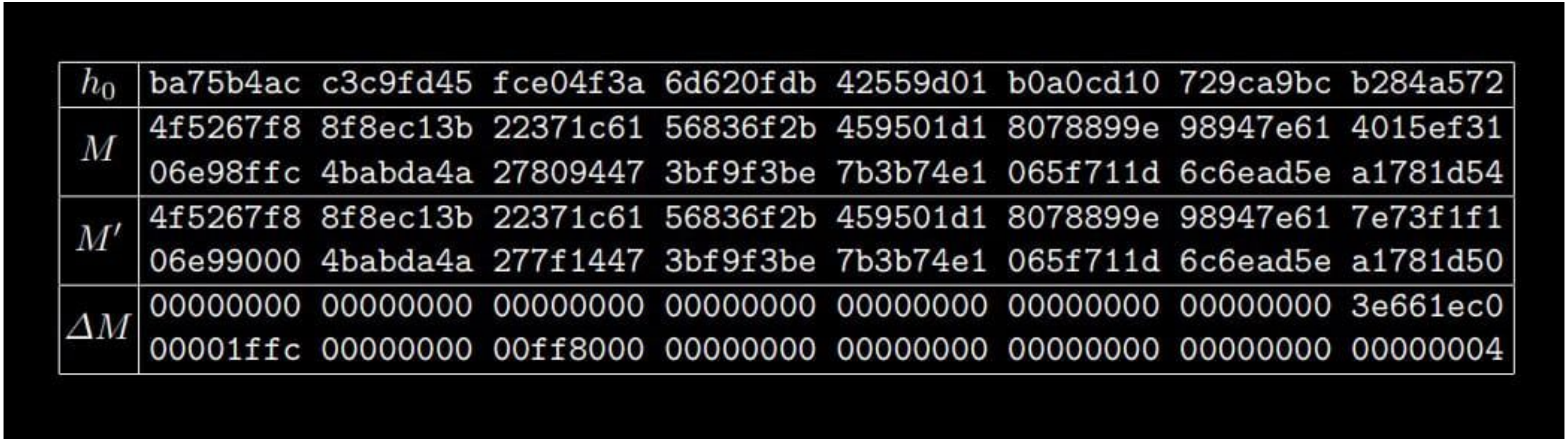
h_0	532f13f5	6a28c3c0	e301fab5	00000000	00000000	00000000	00000000	00000000
M	d55c884f	faf18f34	b772b323	af46235b	3d8bd87b	dd3e8271	26618488	02d189d0
	1883a4af	4f99167b	271b11c7	81b8363d	b27e389d	2155a533	8b811348	4a8da291
M'	d55c884f	faf18f34	b772b323	af46235b	3d8bd87b	523f9273	eeb902ae	36ff3d98
	108477b0	4f989677	271b11c7	81b8363d	b27e389d	2155a533	8b811348	4a8da291
ΔM	00000000	00000000	00000000	00000000	00000000	8f011002	c8d88626	342eb448
	0807d31f	0001800c	00000000	00000000	00000000	00000000	00000000	00000000

Fig. The semi-free-start collision of 31-step SHA-256

Semi-Free-Start Collision Attack on 38-Step SHA-256

$\Delta M := M \oplus M'$

h_0 := initial value of the compression function



h_0	ba75b4ac	c3c9fd45	fce04f3a	6d620fdb	42559d01	b0a0cd10	729ca9bc	b284a572
M	4f5267f8	8f8ec13b	22371c61	56836f2b	459501d1	8078899e	98947e61	4015ef31
	06e98ffc	4babda4a	27809447	3bf9f3be	7b3b74e1	065f711d	6c6ead5e	a1781d54
M'	4f5267f8	8f8ec13b	22371c61	56836f2b	459501d1	8078899e	98947e61	7e73f1f1
	06e99000	4babda4a	277f1447	3bf9f3be	7b3b74e1	065f711d	6c6ead5e	a1781d50
ΔM	00000000	00000000	00000000	00000000	00000000	00000000	00000000	3e661ec0
	00001ffc	00000000	00ff8000	00000000	00000000	00000000	00000000	00000004

Fig. The semi-free-start collision of 38-step SHA-256

Observations and Ideas for Quantum Collision Attacks

The 38-step semi-free-start collision is not converted into a collision for SHA-256.

For SHA-256, the 31-step semi-free-start collision is converted.

For SHA-512, the 39-step semi-free-start collision is not converted.

For a particular classical setting, the semi-free-start collisions of 38-step SHA-256 and 39-step SHA-512 are not converted into collisions.

Obstacles for Conversions in the Classical Setting

A Brief about 31-Step SHA-256

The initial value IV was produced from first block and semi-free-start collisions in the second block.

We get 31-step collision by matching **the initial value IV.**

チ:= the degree of freedom

We have some message words W_0, W_1,.....,W_4 and チin W_0, W_1,.....,W_4 are used to generate result of the 1st block and the local collision in the 2nd block compatible in **step-2 of the attack.**

Obstacles for Conversions in the Classical Setting…(2/n)

A Brief about 31-Step SHA-256

α := number of free bits in the message words (compatible)

α can be used to compatible the values

We have some message words W_0, W_1,.....,W_4 , they can be chosen freely here ñ = 5 (number of message words).

So, α will be equal to n.|w|, i.e. α = ñ .|w| = 5*32 = 160 holds

If we choose M˜ randomly and a single solution in Step-1 , the compatible probability will be $2^{\alpha}/2^{n}$.

Obstacles for Conversions in the Classical Setting…(3/n)

A Brief about 31-Step SHA-256

α := number of free bits in the message words (compatible)

p := a process succeeds with a probability p

Suppose that ℓ solutions can be found for Step-1 and prob(Step-3) = p

Then If we choose M˜ randomly. It leads to a collision with probability $\ell\cdot(2^\alpha/2^n)\cdot p$.

Hence the time complexity T by ignoring the complexity of Step-1 will be ,

$T = [\ell\cdot(2^\alpha/2^n)\cdot p]^{-1} = 2^n/ [\ell\cdot(2^\alpha)\cdot p]$

Obstacles for Conversions in the Classical Setting…(4/n)

A Brief about 31-Step SHA-256

By experiment, and we can expect $\ell \approx 2^{34}$ and $p \approx 1/12 = 2^{-3.5}$

The time complexity T by ignoring the complexity of Step-1 will be ,

$T = [\ell\cdot(2^{\alpha}/2^{n})\cdot p]^{-1} = 2^{n}/ [\ell\cdot(2^{\alpha})\cdot p]$ (n=256)

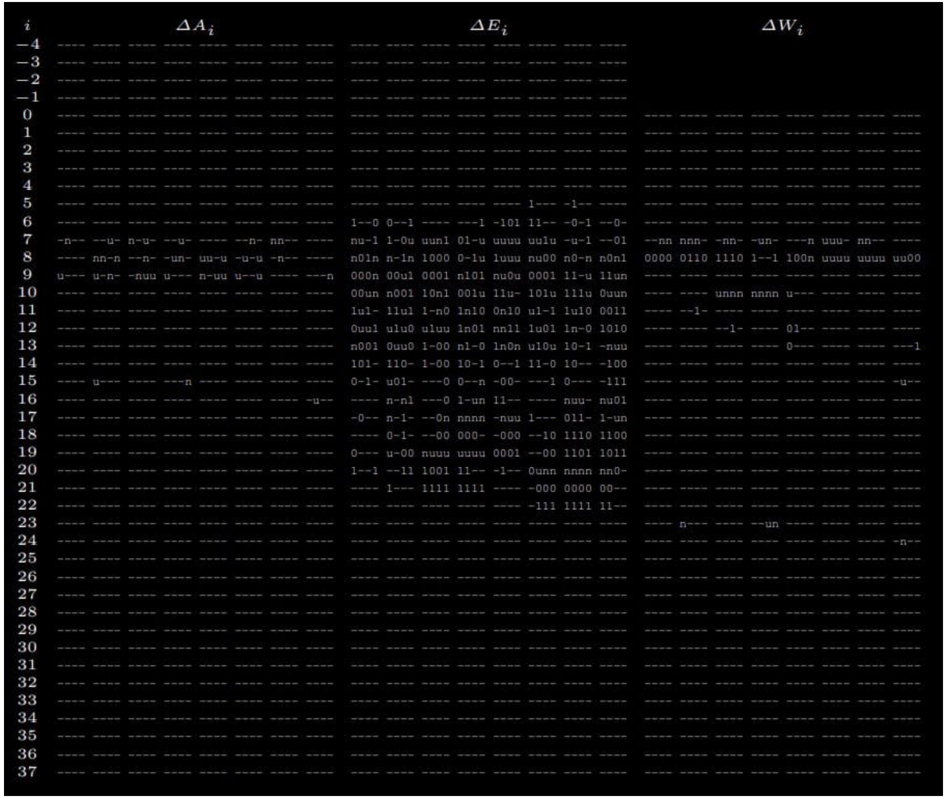
$= 2^{256}/ [2^{34}\cdot(2^{160})\cdot 2^{-3.5}]$ ($\alpha = \tilde{n}\ .|w| = 5*32 = 160$)

$= 2^{256} / 2^{190.5}$

$= 2^{65.5}$

Obstacles for Conversions in the Classical Setting…(5/n)

Lack of Degrees of Freedom in 38-Step SHA-256



i	ΔA_i	ΔE_i	ΔW_i
-4	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
-3	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
-2	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
-1	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	
0	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
1	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
2	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
3	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
4	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
5	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- 1--- -1-- ----	---- ---- ---- ---- ---- ---- ---- ----
6	---- ---- ---- ---- ---- ---- ---- ----	1--0 0--1 ---- ---1 -101 11-- -0-1 --0-	---- ---- ---- ---- ---- ---- ---- ----
7	-n-- --u- n-u- --u- ---- --n- nn-- ----	nu-1 1-0u uun1 01-u uuuu uulu -u-1 --01	--nn nnn- -nn- -un- ---n uuu- nn-- ----
8	---- nn-n --n- -un- uu-u -u-u -n-- ----	n01n n-1n 1000 0-1u 1uuu nu00 n0-n n0n1	0000 0110 1110 1--1 100n uuuu uuuu uu00
9	u--- u-n- -nuu u--- n-uu u--u ---- ---n	000n 00u1 0001 n101 nu0u 0001 11-u 11un	---- ---- ---- ---- ---- ---- ---- ----
10	---- ---- ---- ---- ---- ---- ---- ----	00un n001 10n1 001u 11u- 101u 111u 0uun	---- ---- unnn nnnn u--- ---- ---- ----
11	---- ---- ---- ---- ---- ---- ---- ----	1u1- 11u1 1-n0 1n10 0n10 u1-1 1u10 0011	---- --1- ---- ---- ---- ---- ---- ----
12	---- ---- ---- ---- ---- ---- ---- ----	0uu1 u1u0 u1uu 1n01 nn11 1u01 1n-0 1010	---- ---- --1- ---- 01-- ---- ---- ----
13	---- ---- ---- ---- ---- ---- ---- ----	n001 0uu0 1-00 n1-0 1n0n u10u 10-1 -nuu	---- ---- ---- ---- 0--- ---- ---- ---1
14	---- ---- ---- ---- ---- ---- ---- ----	101- 110- 1-00 10-1 0--1 11-0 10-- -100	---- ---- ---- ---- ---- ---- ---- ----
15	---- u--- ---- ---n ---- ---- ---- ----	0-1- u01- ---0 0--n -00- ---1 0--- -111	---- ---- ---- ---- ---- ---- ---- -u--
16	---- ---- ---- ---- ---- ---- ---- -u--	---- n-n1 ---0 1-un 11-- ---- nuu- nu01	---- ---- ---- ---- ---- ---- ---- ----
17	---- ---- ---- ---- ---- ---- ---- ----	-0-- n-1- --0n nnnn -nuu 1--- 011- 1-un	---- ---- ---- ---- ---- ---- ---- ----
18	---- ---- ---- ---- ---- ---- ---- ----	---- 0-1- --00 000- -000 --10 1110 1100	---- ---- ---- ---- ---- ---- ---- ----
19	---- ---- ---- ---- ---- ---- ---- ----	0--- u-00 nuuu uuuu 0001 --00 1101 1011	---- ---- ---- ---- ---- ---- ---- ----
20	---- ---- ---- ---- ---- ---- ---- ----	1--1 --11 1001 11-- -1-- 0unn nnnn nn0-	---- ---- ---- ---- ---- ---- ---- ----
21	---- ---- ---- ---- ---- ---- ---- ----	---- 1--- 1111 1111 ---- -000 0000 00--	---- ---- ---- ---- ---- ---- ---- ----
22	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- -111 1111 11--	---- ---- ---- ---- ---- ---- ---- ----
23	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- n--- ---- --un ---- ---- ---- ----
24	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- -n--
25	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
26	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
27	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
28	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
29	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
30	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
31	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
32	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
33	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
34	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
35	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
36	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----
37	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ----

Fig. The 38-step differential characteristic for SHA-256

Obstacles for Conversions in the Classical Setting…(6/n)

Lack of Degrees of Freedom in 38-Step SHA-256

E_i := the state variable for i, i $\in Z^+$

For the 38-step semi-free-start collision of SHA-256, Almost all the bits of E_i

(i=7,8,9,....20)

Implying $\triangle W_i$ and W_i are fixed, where i $\in$ 7,8,9,....20.

Due to massage expansion, 16 message words that are W_7, W_8, W_9….W_{20} fixed

and 16 successive words are fixed.

Obstacles for Conversions in the Classical Setting…(7/n)

Lack of Degrees of Freedom in 38-Step SHA-256

We can use W_0, W_1, W_2….W_7 message words

to make the first block and

local collision in the second block compatible.

W_5 and W_6 will have degrees of freedom, so ñ = 2 and |w| = 32

Then number of free bits α will be ñ*|w|, (where ñ = 2 and |w|=32)

α = ñ*|w| = 2*32 = 64 (in total)

Obstacles for Conversions in the Classical Setting…(8/n)

Lack of Degrees of Freedom in 38-Step SHA-256

If we have ℓ solutions that are available.

The time complexity T will be ,

$T = [\ell \cdot (2^{\alpha}/2^{n}) \cdot p]^{-1} = 2^{n} / [\ell \cdot (2^{\alpha}) \cdot p]$ $(n' = n - \alpha = 256-64 = 192)$

$= 2^{256} / [\ell \cdot (2^{64}) \cdot p]$ $(\alpha = \tilde{n} \,.|w| = 2*32 = 64)$

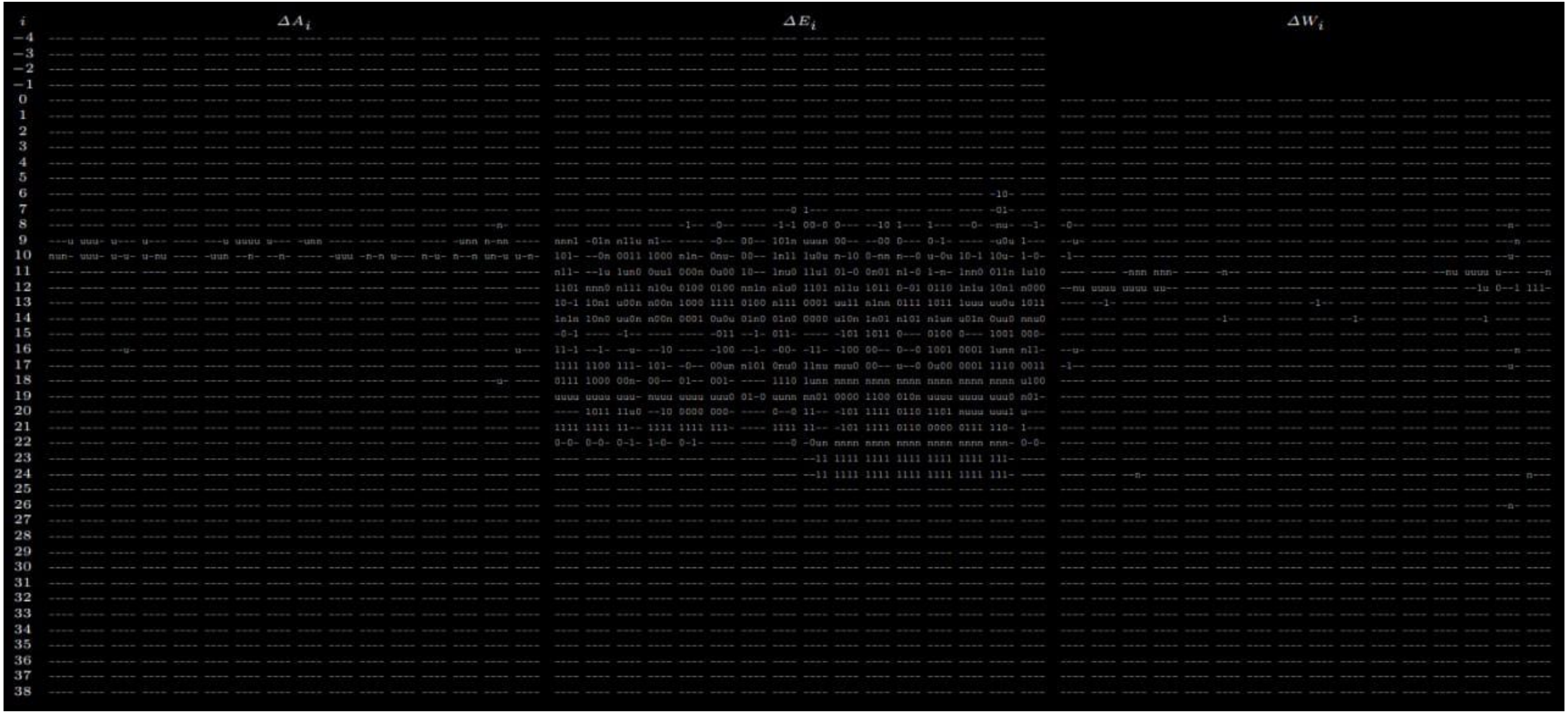
$= 2^{192} / [\ell \cdot p]$ ($\ell \approx 2^{34}$ for 31-step collisions)

The 38-step semi-free-start collision cannot be converted into a collision as

X<128.

Obstacles for Conversions in the Classical Setting…(9/n)

Lack of Degrees of Freedom in 39-Step SHA-512



i	ΔA_i	ΔE_i	ΔW_i
−4	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	
−3	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	
−2	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	
−1	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	
0	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
1	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
2	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
3	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
4	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
5	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
6	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- -10- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
7	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---0 1--- ---- ---- ---- ---- ---- -01- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
8	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- --n- ----	---- ---- ---- ---- -1-- -0-- ---- -1-1 00-0 0--- --10 1--- 1--- --0- -nu- --1-	-0-- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- --n- ----
9	---u uuu- u--- u--- ---- ---u uuuu u--- -unn ---- ---- ---- ---- -unn n-nn ----	nnn1 -01n n11u n1-- ---- -0-- 00-- 101n uuun 00-- --00 0--- 0-1- ---- -u0u 1---	--u- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---n ----
10	nun- uuu- u-u- u-nu ---- -uun --n- --n- ---- -uuu -n-n u--- n-u- n--n un-u u-n-	101- --0n 0011 1000 n1n- 0nu- 00-- 1n11 1u0u n-10 0-nn n--0 u-0u 10-1 10u- 1-0-	-1-- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- --u- ----
11	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	n11- --1u 1un0 0uu1 000n 0u00 10-- 1nu0 11u1 01-0 0n01 n1-0 1-n- 1nn0 011n 1u10	---- ---- -nnn nnn- ---- -n-- ---- ---- ---- ---- ---- ---- --nu uuuu u--- ---n
12	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	1101 nnn0 n111 n10u 0100 0100 nn1n n1u0 1101 n11u 1011 0-01 0110 1n1u 10n1 n000	--nu uuuu uuuu uu-- ---- ---- ---- ---- ---- ---- ---- ---- ---- --1u 0--1 111-
13	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	10-1 10n1 u00n n00n 1000 1111 0100 n111 0001 uu11 n1nn 0111 1011 1uuu uu0u 1011	---- --1- ---- ---- ---- ---- ---- ---- -1-- ---- ---- ---- ---- ---- ---- ----
14	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	1n1n 10n0 uu0n n00n 0001 0u0u 01n0 01n0 0000 u10n 1n01 n101 n1un u01n 0uu0 nnu0	---- ---- ---- ---- ---- -1-- ---- ---- ---- --1- ---- ---- ---- ---1 ---- ----
15	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	-0-1 ---- -1-- ---- ---- -011 --1- 011- ---- -101 1011 0--- 0100 0--- 1001 000-	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
16	---- ---- --u- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- u---	11-1 --1- --u- --10 ---- -100 --1- -00- -11- -100 00-- 0--0 1001 0001 1unn n11-	--u- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---n ----
17	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	1111 1100 111- 101- -0-- 00un n101 0nu0 11nu nuu0 00-- u--0 0u00 0001 1110 0011	-1-- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- --u- ----
18	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- --u- ----	0111 1000 00n- 00-- 01-- 001- ---- 1110 1unn nnnn nnnn nnnn nnnn nnnn nnnn u100	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
19	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	uuuu uuuu uuu- nuuu uuuu uuu0 01-0 uunn nn01 0000 1100 010n uuuu uuuu uuu0 n01-	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
20	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- 1011 11u0 --10 0000 000- ---- 0--0 11-- -101 1111 0110 1101 nuuu uuu1 u---	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
21	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	1111 1111 11-- 1111 1111 111- ---- 1111 11-- -101 1111 0110 0000 0111 110- 1---	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
22	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	0-0- 0-0- 0-1- 1-0- 0-1- ---- ---- ---0 -0un nnnn nnnn nnnn nnnn nnnn nnn- 0-0-	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
23	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- --11 1111 1111 1111 1111 1111 111- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
24	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- --11 1111 1111 1111 1111 1111 111- ----	---- ---- --n- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- n---
25	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
26	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- --n- ----
27	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
28	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
29	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
30	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
31	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
32	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
33	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
34	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
35	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
36	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
37	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
38	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----	---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----

Fig. The 39-step differential characteristic for SHA-512

Obstacles for Conversions in the Classical Setting…(10/n)

Lack of Degrees of Freedom in 39-Step SHA-512

E_i := the state variable for i, i $\in Z^+$

For the 39-step semi-free-start collision of SHA-512, Almost all the bits of E_i

(i=8,9,....22)

Implying E_i and W_i are fixed, where i $\in$ 8,9,....22.

W_7 will have degrees of freedom, so ñ = 1 and |w| = 64 (for SHA-512)

Then number of free bits α will be ñ*|w|, (where ñ = 1 and |w|=64)

α = ñ*|w| = 1*64 = 64 (in total)

Obstacles for Conversions in the Classical Setting…(11/n)

Lack of Degrees of Freedom in 39-Step SHA-512

We can use first 8 message words

to make the first block and

local collision in the second block compatible. ($\alpha = 64$)

Differential characteristic has dense conditions for i, (where $i = 8, \ldots, 22$)

The time complexity T will be ,

$T = [\ell \cdot (2^{\alpha}/2^{n}) \cdot p]^{-1} = 2^{n} / [\ell \cdot (2^{\alpha}) \cdot p] > 2^{256}$

Observations and Ideas on Conversion in the Quantum Setting

Observations

t := number of IVs of the 2nd block that will be compatible with the local collisions in

the 2nd block

Suppose $t = 2^X$.

Then, the time complexity to find the first message block will be

$T = 2^n/2^X = 2^{(n-X)}$

Validity of the attack will be as long as $X > n/2 = 256/2 = 128$.

Hence, for a valid attack, $X > n/2$ must be satisfied.

Observations on Conversion in the Quantum Setting…(2/n)

Observations

For $X<n/2$, we can mount valid 2-block collision attacks in quantum setting of time-space tradeoff.

Grover search requires negligible memory.

By applying the Grover search, we can minimize time complexity of 2-block collision attacks from $2^n/2^X$ to $\sqrt{(2^n/2^X)}$

we can mount valid 2-block collision attacks in quantum setting of time-space tradeoff, if $\sqrt{(2^n/2^X)} < 2^{n/2}$, $X>0$

Observations on Conversion in the Quantum Setting…(3/n)

Observations

By converting the semi-free-start collisions into 2-block collisions ,

we can mount quantum collision attacks on 38-step SHA-256 and 39-step

SHA-512 (with the Grover search)

Goal : Using Grover search, Mounting quantum collision attacks on 38-step

SHA-256 and 39-step SHA-512

We have to consider two points to achieve our goal.

Observations on Conversion in the Quantum Setting…(4/n)

Observations

We have to consider two points to achieve our goal.

For classical attack on 31-step SHA-256,

A1) If we have ℓ solutions that are available. complexity of **Step-2** is degrade by factor of ℓ, if we stored ℓ solutions.

Memory is relatively cheap in classical setting.

Memory-less algorithms are favorable.

Observations on Conversion in the Quantum Setting…(5/n)

Observations

For classical attack on 31-step SHA-256,

A2) The values of $W_0, . . . , W_4$ do not alters the steps with dense conditions in the differential characteristic. So, we can choose $W_0, . . . , W_4$ freely.

For classical attack on 38-step SHA-256,

A3) Through the message expansion, We have to select the message words $W_0, . . . , W_6$ as they alters on some of

the message words in the steps with dense conditions $W_7, . . . , W_{20}$.

Observations on Conversion in the Quantum Setting…(6/n)

Observations

For classical attack on 39-step SHA-512,

A4) Through the message expansion, We have to select the message words

W_0, . . . , W_7 as they alters on some of

the message words in the steps with dense conditions W_8, . . . , W_{22} .

ℓ := number of solutions that are available.

To minimize the required memory size, we set ℓ=1

Observations on Conversion in the Quantum Setting…(7/n)

Observations

For classical attack on 38-step SHA-256,

Choice of message words : $W_0, \ldots, W_6$

Modification :

We will modify W_j to $W_j\hat{}$ for $\forall$ j $\in$ {0,1,...,4,5}

(Without changing $W_7, \ldots, W_{21}$)

$W_j\hat{} := W_j - (\sigma_0(W_{j+1}\hat{}) - \sigma_0(W_{j+1})$, $\forall$ j $\in$ {0,1,..,5}

Observations on Conversion in the Quantum Setting…(8/n)

Observations

But W_6 is changed to another value $W_6\hat{}$

then W_{21} and W_{22} will be changed

As $W_i = \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15})+W_{i-16}$, i = 16,17,18…..,(r-1)

If we modifying W_5 to $W_5\hat{}$using $W_j\hat{} := W_j - (\sigma_0(W_{j+1}\hat{}) - \sigma_0(W_{j+1})$

, $\forall\ j \in \{0,1,..,5\}$

$W_5\hat{} := W_5 - (\sigma_0(W_6\hat{}) - \sigma_0(W_6)$,

Then change of the value of W_{21} can be canceled out.

Observations on Conversion in the Quantum Setting…(9/n)

Observations

We can also keep W_{20}, . . . , W_{16} unchanged.

For j=0,1,..,4,

When we modifying

W_j to $W_j\hat{}$ using $W_j\hat{} := W_j - (\sigma_0(W_{j+1}\hat{}) - \sigma_0(W_{j+1})$, $\forall\ j \in \{0,1,..,5\}$

W_7, . . . , W_{15} are not also kept changed because When we modify

W_0, . . . , W_6 then W_7, . . . , W_{15} , are not altered or changed.

Observations on Conversion in the Quantum Setting…(10/n)

Observations

For 39-step SHA-512

Choice of message words : $W_0, \dots, W_7$

Modification :

We will modify W_j to W_j^for $\forall$ j $\in$ {0,1,...,5,6}

(Without changing $W_8, \dots, W_{22}$)

W_j^ := $W_j - (\sigma_0(W_{j+1}\hat{}) - \sigma_0(W_{j+1})$, $\forall$ j $\in$ {0,1,..,6}

Ideas on Conversion in the Quantum Setting

Attack Idea

i := number of the step

where the local collision starts

in the differential Characteristic.

For 38-step SHA-256, i=7

For 39-step SHA-512, i=8

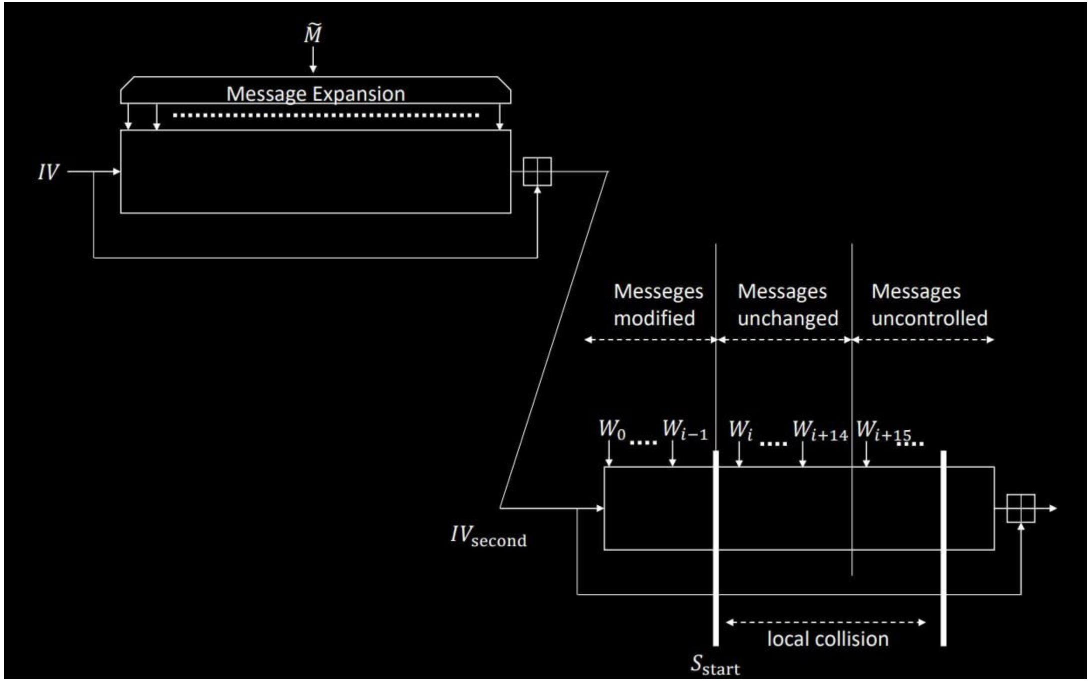


Fig. The idea of our quantum attack

Ideas on Conversion in the Quantum Setting…(2/n)

Attack procedure

Step-1) Search Initial value for the 2nd block that yield a semi-free-start collision.

We have to find a pair of messages (M, M’)

S_{start} := Internal state at the beginning of step i

W_j := message word j expanded from M

$W_j’$:= message word j expanded from M’

Also $W_0 = W_0’ , . . . , W_{i−1} = W’_{i−1}$ hold.

Ideas on Conversion in the Quantum Setting…(3/n)

Attack procedure

Step-2) $M^{\sim}$:= message $M^{\sim}$ (for the first block) that fulfill **2A) and 2B)**

2A) IV_B := input chaining value for block B

From $M^{\sim}$, we derived S_{start} and IV_{second} which are compatible

by applying some modification operator on W_0, . . . , W_{i-1}, W_0' , . . . , W'_{i-1}

While keeping W_i, . . . , W_{i+14}, W_i' , . . . , W'_{i+14} unchanged.

Ideas on Conversion in the Quantum Setting…(4/n)

Attack procedure

2A) Mˆ := message 1 for the 2nd block after the modification

M’ˆ := message 2 for the 2nd block after the modification

$Mˆ := Wˆ_0|| \cdot \cdot \cdot ||Wˆ_{i-1}||W_i || \cdot \cdot \cdot ||W_{15}$

$M’ ˆ := Wˆ_0|| \cdot \cdot \cdot ||Wˆ_{i-1}||W’_i || \cdot \cdot \cdot ||W’_{15}$

(Mˆ ,Mˆ’) : = modified message pair

2B) (Mˆ ,Mˆ’) and S_{start} yield a collision at the end of the 2nd block.

Ideas on Conversion in the Quantum Setting…(5/n)

Attack procedure

Step-3) To obtain (Mˆ ,Mˆ’) again, do computations in steps 2A) and 2B) using M˜ found in Step-2 that causing collision at the end of 2nd block.

We follow different steps from **Step-2)** so that we can apply grover search on M˜ in Step-2

Output : (M˜ ||Mˆ, M˜ ||Mˆ’).

Ideas on Conversion in the Quantum Setting…(6/n)

Attack Idea

Step-1) of classical collision attack corresponds to Step-1) of the attack procedure of our quantum attacks that are common between 38-step SHA-256 and 39-step SHA-512.

The attack will be memory-less as we stored only a single solution in Step-1) of our attack. Only single solution is required in this step.

Step-2) of classical collision attack corresponds to Step-2A) of the attack procedure of our quantum attack on 31-step SHA-256.

Attack Complexity and Validity

For grover’s algorithm, F is boolean function,

We applied boolean function F in **step-2** of the attack.

In **step-2** , we set $\theta = \sin^{-1}(\sqrt{p})$ and run **Grover**(F, $\lfloor \pi/4\theta \rfloor$)

F ($\tilde{M}$) := 1 ⇔ M satisfies **2A** and **2B** (the above conditions)

p := probability that F ($\tilde{M}$) = 1 where M is uniform random message for first block.

Let F be implementation of quantum circuit in which width (S_F) and depth(T_F).

Time Complexity from both Step 1 and Step 3 is negligible as compared to step 2 of grover’s function F i,e. T_F . $\pi/4 \sqrt{1/p}$.

Attack Complexity and Validity …continue(1/n)

If size $S(> S_F)$, for quantum computer means Grover’s function

be parallelized and the factor of $\sqrt{S/S_F}$, and attack complexity will be :

$(T_F \cdot (\pi/4).\sqrt{(1/p)}) / \sqrt{(S/S_F)} = T_F \cdot (\pi/4) \cdot \sqrt{(S_F /pS)}$

Suppose n be size of hash function.

When we have availability of quantum computer of size S the time

complexity of generic attack is $2^{n/2}/S$.

Then, attack is valid if $T_F \cdot (\pi/4) \cdot \sqrt{(S_F /pS)} < 2^{n/2} /S$ this condition holds ------(2)

Attack Complexity and Validity …continue(2/n)

When we run our setup in classical setting. Usual exhaustive search works instead of Grover search.

If we don't consider parallelization, then Attack time complexity will be $(T_F \cdot S_F)/p$ the time complexity of generic attack is $2^{n/2}$.

Then, attack is valid if $(T_F \cdot S_F)/p < 2^{n/2}$ this condition holds.

Rearranging above inequality, $p > (T_F \cdot S_F)/2^{n/2}$

If $p < 1/2^{n/2}$, classical attack is invalid. Equation (2) : $T_F \cdot (\pi/4) \cdot \sqrt{}(S_F /pS) < 2^{n/2} /S$

If we set S=1, (2) becomes $p > S_F \cdot (\pi^2/16) \cdot T^2{}_F /2^n$, Even attack may be valid if $p < 1/2^{n/2}$

Collision Attack on 38-Step SHA-256

(M, M’) := semi-free-start collision

h_0 := initial value in previous collision

W_j and W'_j := message word j associated with M and M’

S_{start} := the state at the beginning which is computed from (M, M’) and h_0.

S := size of the quantum computer

Step-2 Observation

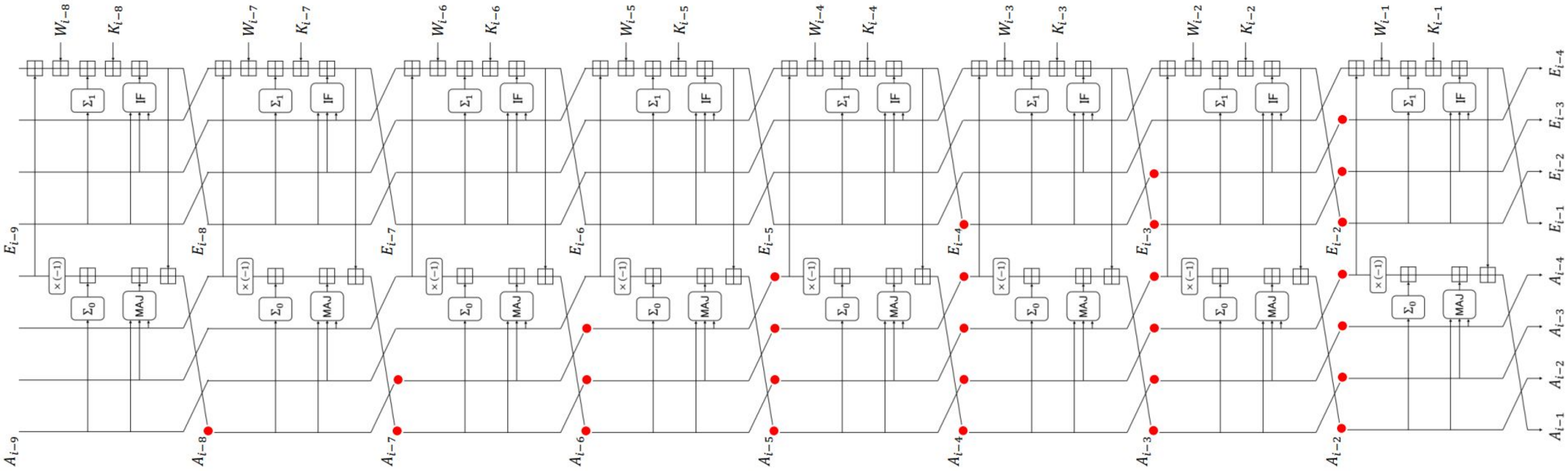
I) Internal state variables : $A_{-1}, A_0, A_1, A_2, \ldots, A_6, E_3, E_4, E_5, E_6$

$S_{start} = A_6 || \cdots || A_3 || E_6 || \cdots || E_3$

Internal state variables are derived from S_{start}

Collision Attack on 38-Step SHA-256 ….Continue(1/n)

The internal state variables (pointed with red dots) that are determined by computing step functions backwards from the internal state A_{i-1}|| · · · ||A_{i-4}||E_{i-1}|| . . . ||E_{i-4} at the beginning of step i.



Collision Attack on 38-Step SHA-256 ….Continue(2/n)

Step-2 Observation

I) ∃ a tuple $(\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, \ldots, \hat{W}_6)$ that's compatible with IV_{second} and S_{start}

⇔ A_{-1} matches the highest significant of IV_{second} (32 bits)

By equation $IV_{second} = A_{-1} \| \cdots \| A_{-4} \| E_{-1} \| \cdots \| E_{-4}$, we can determine A_{-2}, A_{-3}, A_{-4}, $E_{-1}, \ldots, E_{-4}$, only if A_{-1} matches with the values A_{-2}, A_{-3}, A_{-4}, $E_{-1}, \ldots, E_{-4}$

$\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, \ldots, \hat{W}_6$:= message words in the first observation

$\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, \ldots, \hat{W}_6$ can be determined from the values $A_6, \ldots, A_{-2}$, A_{-3}, A_{-4}, $E_6, \ldots, E_3$, $E_{-1}, \ldots, E_{-4}$ uniquely.

Collision Attack on 38-Step SHA-256 ….Continue(3/n)

Step-2 Observation

II) For $\hat{W}_6 \in \{0, 1\}^{32}$, we checking all possible values, we see ∃ 1179647 tuples

$(\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, \ldots, \hat{W}_6)$ that fulfill the following conditions :

(For all 2^{32} choices of W_6 , we count the number of semi-free-start collisions,

and modified the values W_5 ,W_4 ,W_3 ,W_2 ,W_1 ,W_0)

- $\hat{W}_j = W_j - (\sigma_0(\hat{W}_{j+1}) - \sigma_0(W_{j+1}))$, for j = 0,1,2,3,4,5
- The messages ($\hat{M}$, $\hat{M}'$) and S_{start} and for the 2nd block gives a collision at the end of the 2nd block.

We can generate semi-free-start collisions for at least 2^{20} initial values.

Collision Attack on 38-Step SHA-256 ….Continue(4/n)

Analysis and Implementation of F

T_F := represents the running time of the circuit or depth of the circuit

S_F := represents the width of the quantum circuit of F

We will have to show $T_F \leq 6.8$ and $S_F \leq 3.9$. So, we are going to discuss about the analytical view and implementation of F.

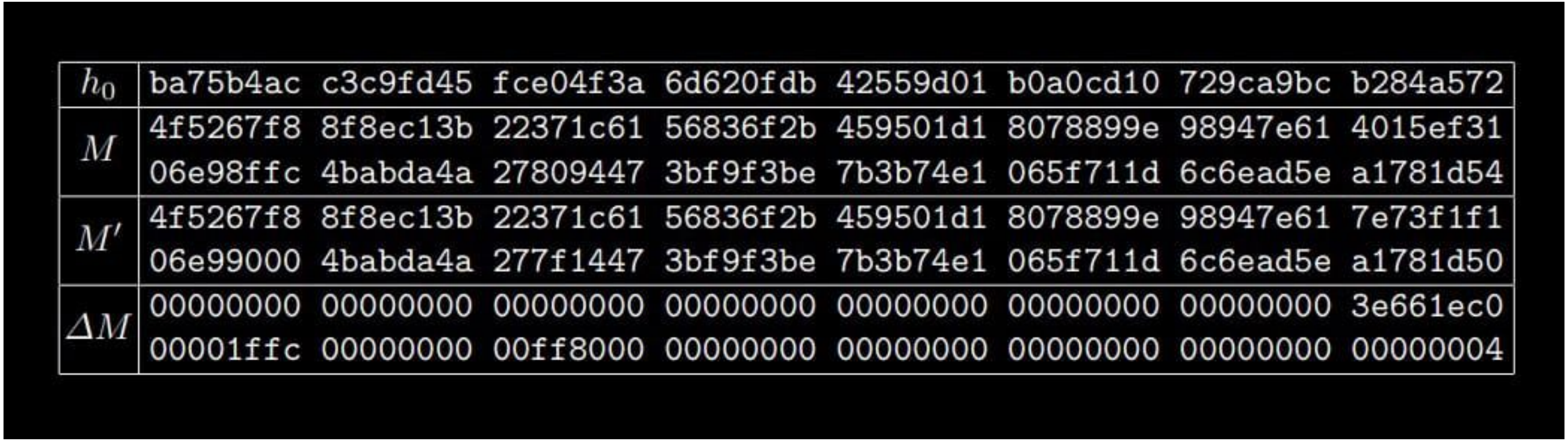
Implementation of F ~ Basic Idea

We compute internal state variable A_{-1}, internal state S_{start} , message words W_j and W'_j values and store those values into memory.

Collision Attack on 38-Step SHA-256 ….Continue(5/n)

h_0 := initial value of the compression function and $\Delta M := M \oplus M'$

We compute A_{-1}, S_{start} ,W_j and W'_j values from the below table and store those values into memory.



h_0	ba75b4ac	c3c9fd45	fce04f3a	6d620fdb	42559d01	b0a0cd10	729ca9bc	b284a572
M	4f5267f8	8f8ec13b	22371c61	56836f2b	459501d1	8078899e	98947e61	4015ef31
	06e98ffc	4babda4a	27809447	3bf9f3be	7b3b74e1	065f711d	6c6ead5e	a1781d54
M'	4f5267f8	8f8ec13b	22371c61	56836f2b	459501d1	8078899e	98947e61	7e73f1f1
	06e99000	4babda4a	277f1447	3bf9f3be	7b3b74e1	065f711d	6c6ead5e	a1781d50
ΔM	00000000	00000000	00000000	00000000	00000000	00000000	00000000	3e661ec0
	00001ffc	00000000	00ff8000	00000000	00000000	00000000	00000000	00000004

Fig. The semi-free-start collision of 38-step SHA-256

Collision Attack on 38-Step SHA-256 ….Continue(6/n)

Implementation of F ~ Basic Idea

The values A_{-1}, internal state S_{start} , message words W_j and W'_j values are computed and stored before the start of the attack and kept unaltered throughout the whole attack procedure.

$M^{\tilde{}}$:= input value

Computation of output value F($M^{\tilde{}}$)

1) Determine the result of first block from $M^{\tilde{}}$ and suppose IV_{second} represents the output.

Collision Attack on 38-Step SHA-256 ….Continue(7/n)

Computation of output value F(M˜)

2) Check if A_{-1} == the highest significant of IV_{second} (32 bits)

If it is not satisfied then output 0 and abort.

If it is satisfied then proceed to the further steps.

3) Compute ($Wˆ_0$,$Wˆ_1$,$Wˆ_2$,$Wˆ_3$, . . . , $Wˆ_6$) that's compatible with IV_{second} and S_{start}. And ($Wˆ_0$,$Wˆ_1$,$Wˆ_2$,$Wˆ_3$, . . . , $Wˆ_6$) should be unique.

4) Check if the below conditions are fulfilled or not :

- $Wˆ_j = W_j − (\sigma_0(Wˆ_{j+1}) − \sigma_0(W_{j+1}))$, for j = 0,1,2,3,4,5
- The messages (M ˆ, Mˆ ') and S_{start} and for the 2nd block gives a collision at the end of the 2nd block.

Collision Attack on 38-Step SHA-256 ….Continue(8/n)

Computation of output value F(M˜)

5) If the below conditions are fulfilled :

- $Wˆ_j = W_j − (σ_0(Wˆ_{j+1}) − σ_0(W_{j+1}))$, for j = 0,1,2,3,4,5
- The messages (M ˆ, Mˆ ‘) and S_{start} and for the 2nd block gives a collision at the end of the 2nd block.

Then output 1. Otherwise output 0.

Each computational processes should have to be reversible.

Whatever the inputs we passed, it doesn’t affect the running time of quantum circuit while implementing a quantum circuit.

Collision Attack on 38-Step SHA-256 ….Continue(9/n)

Implementation of F ~ Formal Description

f := 38-step compression function

L : = A list to store internal state variable A_{-1}, internal state S_{start} , message words W_j and W'_j values.

M˜ := input value

Computation of output value F(M˜)

Computation Step-0)

|y〉:= the single qubit register where machine output F(M˜) will be added

Quantum state is |M˜ 〉|L〉 |y〉. (In initial state)

Collision Attack on 38-Step SHA-256 ….Continue(10/n)

Computation of output value F(M˜)

Computation Step-1)

Determination of output from 1st block from M˜. and

suppose IV_{second} represents

the output. Check if A_{-1} == the highest significant of IV_{second} (32 bits)

If it is not satisfied then set b := 0

If it is satisfied then set b := 1.

Quantum state is $|M^{\sim}\rangle|L\rangle\ |y\rangle \otimes |\ IV_{second}\rangle|b\rangle$ (In present state ~ step 1)

Collision Attack on 38-Step SHA-256 ….Continue(11/n)

Computation of output value $F(M^{\sim})$

Computation Step-2)

IV'_{second} := the concatenation of A_{-1} and the less significant 224 bits of IV_{second}

If IV'_{second} = IV_{second} then b = 1

Compute ($\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, \ldots, \hat{W}_6$) that's compatible with initial chaining value IV'_{second} and S_{start}. And ($\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, \ldots, \hat{W}_6$) should be unique.

Quantum state is $|M^{\sim}\rangle|L\rangle\,|y\rangle \otimes |\,IV_{second}\rangle|b\rangle\,|\hat{W}_0, \ldots, \hat{W}_6\rangle$(In present state ~ step 2)

Collision Attack on 38-Step SHA-256 ….Continue(12/n)

Computation of output value $F(\tilde{M})$

Computation Step-3)

$\hat{M} := \hat{W}_0 || \cdot \cdot \cdot || \hat{W}_6 || W_7 || \cdot \cdot \cdot || W_{15}$

$\hat{M}' := \hat{W}_0 || \cdot \cdot \cdot || \hat{W}_6 || W'_7 || \cdot \cdot \cdot || W'_{15}$

Determination of the values $f(IV'_{second}, \hat{M}), f(IV'_{second}, \hat{M}')$

Quantum state is

$|\tilde{M}\rangle |L\rangle |y\rangle \otimes | IV_{second}\rangle |b\rangle |\hat{W}_0, . . . , \hat{W}_6\rangle | f(IV'_{second}, \hat{M})\rangle$

$| f(IV'_{second}, \hat{M}')\rangle$ (In present state ~ step 3)

Collision Attack on 38-Step SHA-256 ….Continue(13/n)

Computation of output value $F(\tilde{M})$

Computation Step-4)

We know that $F(\tilde{M}) = 1 \Leftrightarrow b = 1$ and the below condition holds :

1) $\hat{W}_j = W_j - (\sigma_0(\hat{W}_{j+1}) - \sigma_0(W_{j+1}))$, for $j = 0,1,2,3,4,5$
2) $f(IV'_{second}, \hat{M}) = f(IV'_{second}, \hat{M}')$

Determine output value $F(\tilde{M})$ by proceeding if $b=1$ and above two conditions

And addition of output value $F(\tilde{M})$ to $|y\rangle$register

Quantum state is

$|\tilde{M}\rangle|L\rangle\,|y\rangle \otimes F(\tilde{M})\,\rangle|\,IV_{second}\rangle|b\rangle\,|\hat{W}_0, \ldots, \hat{W}_6\rangle\,|\,f(IV'_{second}, \hat{M})$

$\rangle|\,f(IV'_{second}, \hat{M}')\,)\rangle$ (In present state ~ step 4)

Collision Attack on 38-Step SHA-256 ….Continue(14/n)

Computation of output value F(M˜)

Computation Step-5)

Uncompute 1 to 3 steps to get $|\tilde{M}\rangle|L\rangle\ |y\rangle \otimes F(\tilde{M})\,\rangle$

Analysis

The unit of width (S_F) and depth (T_F) of quantum circuits is the width (S_F) and depth (T_F) required to produce 38-step SHA-256. And it takes only 1-block inputs.

For single step, depth (T_F) of quantum circuit required to compute SHA-512 is equal to 0.02631578947 = 1/38

Collision Attack on 38-Step SHA-256 ….Continue(15/n)

Analysis

512 bits = input length of 1-block SHA256

256 bits = output length of 1-block SHA256

Hence, amount of qubits are required to generate the function on

a quantum circuit Q will be at least = 512 qubits + 256 qubits = 768 qubits

Width (S_F)

$|M^{\sim}|$ = 16 words

Word data in L = 8+(7+15+15)+1 = 46 words

Qubits used in step 0 = (16 + 46) × 32 + 1 = 62 × 32 + 1 = 1985 qubits

Collision Attack on 38-Step SHA-256 ….Continue(16/n)

Width (S_F)

Qubits used in step 1 to store b and IV_{second} = 1 + 8×32 qubits = 257 qubits

Qubits used in step 2 to store $(\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, \ldots, \hat{W}_6)$ = 7*32 qubits =

224 qubits

Qubits used in step 3 to store $f(IV'_{second}, \hat{M}), f(IV'_{second}, \hat{M}')$ = (8 + 8) × 32 =

16 × 32 = 512 qubits

Total Qubits used = (62 + 8 + 7 + 16) × 32 + 2 = 2978 qubits

Therefore, $S_F \leq 2978/768 \leq 3.9$

Collision Attack on 38-Step SHA-256 ….Continue(17/n)

Depth (T_F)

Depth required in step 1 to compute compression function = 1

Depth required in step 2 for message words ($Wˆ_0$,$Wˆ_1$,$Wˆ_2$,$Wˆ_3$, . . . , $Wˆ_6$) = 7/38

Depth required in step 3 to compute compression function twice = 2

Depth required in step 4 = 6/38 (at most 6 steps of SHA-256)

Total Depth required for 1-4 steps = 1 + 7/38 + 2 + 6/38 = 3.34210526316 ≤ 3.4

Total Depth required, T_F, (uncomputations) = 3.34210526316*2 ≤ 3.4 × 2 = 6.8

Collision Attack on 38-Step SHA-256 ….Continue(18/n)

Total Complexity

p := probability that $F(\tilde{M}) = 1$ where M is uniform random chosen message

$F(\tilde{M}) := 1 \Leftrightarrow$ M satisfies **2nd** and **4th** steps in computational implementation of F

$\tilde{M}$ satisfies condition in the **2nd** step with probability 2^{-32}

- $\hat{W}_j = W_j - (\sigma_0(\hat{W}_{j+1}) - \sigma_0(W_{j+1}))$, for j = 0,1,2,3,4,5
- The messages $(\hat{M}, \hat{M}')$ and S_{start} and for the 2nd block gives a collision at the end of the 2nd block.

Above steps are satisfied with probability $1179647/(2^{32})^7 > 2^{20}/2^{224}$.

Collision Attack on 38-Step SHA-256 ….Continue(19/n)

Total Complexity

Hence, $p = 2^{-32} .(1179647/(2^{32})^{7} > 2^{-32} . (2^{20}/2^{224}) = 1/2^{236}$, $p = 2^{-236}$ holds

We can use $(T_F \cdot (\pi/4).\sqrt{(1/p)}) / \sqrt{(S/S_F)} = T_F \cdot (\pi/4) \cdot \sqrt{(S_F /pS)}$ for computation of attack time complexity. We proved $T_F \leq 6.8$ and $S_F \leq 3.9$

When we have availability of quantum computer of size S, the time complexity to find collision for our attack will be

$6.8 \cdot (\pi/4).\sqrt{(3.4 / \sqrt{(2^{-236} \cdot S)})} = 6.8 \cdot (\pi/4) \cdot \sqrt{(3.9 /2^{-236}S)} \leq 2^{122}/ \sqrt{S}$

attack time complex $2^{122}/ \sqrt{S}$ < generic complexity $2^{128}/S$

Hence, the attack is valid as long as S satisfies $3.9 \leq S < 2^{12}$

Collision Attack on 39-Step SHA-512

(M, M’) := semi-free-start collision

h_0 := initial value in previous collision

W_j and W'_j := message word j associated with M and M’

Differences between Attack on 39-Step SHA-512 and Attack on 38-Step

SHA-256 :

1) probability p (= $|F^{-1}(1)|/2^{512}$) satisfies $p > 2^{-498.4}$
2) production of F satisfies $T_F \leq 6.8$ and $S_F \leq 4.1$
3) Collision starts from step-8 but not from step-7 locally.

Collision Attack on 39-Step SHA-512 ….Continue(1/n)

Step-2 ~ Observation

I) IV_{second} := chaining initial input value

∃ unique tuple ($\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, . . . , \hat{W}_6$) that's compatible with IV_{second} and S_{start}

Because for 39-step SHA-512, in the differential characteristic, the local collision starts at step-8.

II) Experimentally, ∃ 13184 (> $2^{13.6}$) tuples ($\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, . . . , \hat{W}_7$) that fulfill the below conditions :

Collision Attack on 39-Step SHA-512 ….Continue(2/n)

Step-2 ~ Observation

II) Experimentally, ∃ 13184 (> $2^{13.6}$) tuples ($Wˆ_0$,$Wˆ_1$,$Wˆ_2$,$Wˆ_3$, . . . , $Wˆ_7$) that fulfill the below conditions :

- $Wˆ_j = W_j - (\sigma_0(Wˆ_{j+1}) - \sigma_0(W_{j+1}))$, for j = 0,1,2,3,4,5,6
- The messages (M ˆ, Mˆ ‘) and S_{start} and for the 2nd block gives a collision at the end of the 2nd block, where Mˆ := $Wˆ_0|| \cdot\cdot\cdot ||Wˆ_7||W_8|| \cdot\cdot\cdot ||W_{15}$

  Mˆ ‘ := $Wˆ_0|| \cdot\cdot\cdot ||Wˆ_7||W'_8|| \cdot\cdot\cdot ||W'_{15}$
- For j = 5,6,7,8,...,29, $Wˆ_{(23,j)} = W_{(23,j)}$, where $Wˆ_{(23,j)}$ and $W_{(23,j)}$ are bit j of message word 23 derived from Mˆ and M.
- The above condition to reduce the search space for $Wˆ_7$

Collision Attack on 39-Step SHA-512 ....Continue(3/n)

Analysis and Implementation of F

T_F := represents the running time of the circuit or depth of the circuit

S_F := represents the width of the quantum circuit of F

We will have to show $T_F \leq 6.8$ and $S_F \leq 4.1$. So, we are going to discuss about the analytical view and implementation of F.

Implementation of F ~ Basic Idea

∃ unique tuple $(\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, . . . , \hat{W}_6)$ that's compatible with IV_{second} and S_{start}, $(\hat{W}_0, \hat{W}_1, \hat{W}_2, \hat{W}_3, . . . , \hat{W}_6)$ should be unique, for arbitrary IV_{second} due to the first observation

Collision Attack on 39-Step SHA-512 ….Continue(4/n)

Implementation of F

Basic Idea:

For first block, we consider message m and from M, we calculate the IV_{second} (initial vector of second block).

Definition:

F(M˜) := 1 ⇔ conditions i, ii and iii (above observation of **step 2**) are true for the unique tuple i.e, (Wˆ 0, . . . , Wˆ 7) which needs to be compatible with the S_{start} and IV_{second} .

Collision Attack on 39-Step SHA-512 ….Continue(5/n)

Implementation of F

Formal Implementation :

Firstly, we compute internal state S_{start} and message words like

$W_0 = W_0'$, $W_1 = W_1'$,........, $W_7 = W_7'$,W_8 ,W_9 ,W_{10} ,.....W_{22} ,$W\,'_8$,$W'\,_9$,W'_{10} ,......$W'_{22'}$ W_{23} .

F($M^{\tilde{}}$) computation :

The given input message is $M^{\tilde{}}$.

Now, we will evaluate the value of F($M^{\tilde{}}$) .

Collision Attack on 39-Step SHA-512 ….Continue(6/n)

Steps to compute $F(\tilde{M})$:

Step-1 : Initially, the quantum state is $|\tilde{M}\rangle\,|L\rangle\,|y\rangle$.

Here, $|y\rangle :=$ single qubit register

Step-2 : Compute first block output. Suppose the generated output will be IV_{second}. Then, $|\tilde{M}\rangle\,|L\rangle\,|y\rangle \otimes |IV_{second}\rangle$ is the current quantum state.

Step-3 : Compute the unique $(\hat{W}_0, \ldots, \hat{W}_7)$ that is compatible with IV_{second} and S_{start}. The current quantum state is $|\tilde{M}\rangle\,|L\rangle\,|y\rangle \otimes |IV_{second}\rangle|\hat{W}_0, \ldots, \hat{W}_7\rangle$

Collision Attack on 39-Step SHA-512 ….Continue(7/n)

Steps to compute $F(\tilde{M})$:

Step-4 : Let $\hat{M}$ denote $\hat{W}_0|| \cdot \cdot \cdot ||\hat{W}_7||W_8|| \cdot \cdot \cdot ||W_{15}$

and Mˆ ‘ denote Wˆ 0|| · · · ||Wˆ 7||W’ 8 || · · · ||W’ 15.

Compute $f(IV_{second}, \hat{M})$, $f(IV_{second}, \hat{M}')$, and $\hat{W}_{23}$,

where $\hat{W}_{23}$ is word 23 derived from $\hat{M}$.

The current quantum state is $|\tilde{M}\rangle\ |L\rangle\ |y\rangle$

$\otimes\ |IV_{second}\rangle|\hat{W}_0, \ldots , \hat{W}_7\rangle|f(IV_{second}, \hat{M})\rangle$

$|f(IV_{second}, \hat{M}')\rangle|\hat{W}_{23}\rangle$.

Collision Attack on 39-Step SHA-512 ....Continue(8/n)

Steps to compute F(M˜) :

Step-5 : We know that F(M˜) := 1

⇔ the following three statements hold :

S1 : $f(IV_{second}, \hat{M}) = f(IV_{second}, \hat{M}')$

S2 : $\hat{W}_j = W_j - (\sigma_0(\hat{W}_{j+1}) - \sigma_0(W_{j+1}))$ holds for j = 0, ... , 7-1.

S3 : $\hat{W}_{23,j} = W_{23,j}$ holds for j = 5, ... , 30-1

Now, by checking S1, S2 and S3, compute F(M˜)

Add the value F(M˜) value to register |y⟩

Collision Attack on 39-Step SHA-512 ….Continue(9/n)

Steps to compute $F(\tilde{M})$:

Step-5 : Add the value $F(\tilde{M})$ value to register $|y\rangle$

Now, the current quantum state is $|\tilde{M}\rangle\ |L\rangle\ |y \otimes |\ F(\tilde{M})\ \rangle \otimes |IV_{second}\rangle|\hat{W}_{0}, \ldots, \hat{W}_{7}\rangle|f(IV_{second}, \hat{M})\rangle$
$|f(IV_{second}, \hat{M}'))\rangle|\hat{W}_{23}\rangle$.

Step-6 :

Uncompute steps 2,3 and 4 to find

$|\tilde{M}\rangle\ |L\rangle\ |y \otimes |\ F(\tilde{M})\ \rangle$

Analysis

For SHA-512,

The depth required to implement 39-step SHA-512 that

takes 1-block inputs is the unit of depth of quantum circuits.

The depth required to compute a single step of SHA-512 is equal to 1/39.

Since, the input length of 1-block SHA-512 is 1024 bits.

And the output length is 512 bits.

To implement the function on a quantum circuit,

At least 1024 + 512 = 1536 qubits are required .

Total Complexity

p := When $\tilde{M}$ is randomly chosen then probability that $F(\tilde{M}) = 1$ holds.

And $F(\tilde{M}) := 1$

⇔ the following three statements hold :

S1 : $f(IV_{second}, \hat{M}) = f(IV_{second}, \hat{M}')$

S2 : $\hat{W}_j = W_j - (\sigma_0(\hat{W}_{j+1}) - \sigma_0(W_{j+1}))$ holds for $j = 0, \ldots, 7-1$.

S3 : $\hat{W}_{23,j} = W_{23,j}$ holds for $j = 5, \ldots, 30-1$

From the following observations :

- $\hat{W}_j = W_j - (\sigma_0(\hat{W}_{j+1}) - \sigma_0(W_{j+1}))$, for $j = 0,1,2,3,4,5,6$

Total Complexity

From the following observations :

- $Wˆ_j = W_j − (σ_0(Wˆ_{j+1}) − σ_0(W_{j+1}))$, for j = 0,1,2,3,4,5,6
- The messages (M ˆ, Mˆ ‘) and S_{start} and for the 2^{nd} block gives a collision at the end of the 2^{nd} block, where $Mˆ := Wˆ_0 || \cdot\cdot\cdot ||Wˆ_7||W_8|| \cdot\cdot\cdot ||W_{15}$

  $Mˆ ‘ := Wˆ_0 || \cdot\cdot\cdot ||Wˆ_7||W’_8|| \cdot\cdot\cdot ||W’_{15}$
- For j = 5,6,7,8,...,29, $Wˆ_{(23,j)} = W_{(23,j)}$, where $Wˆ_{(23,j)}$ and $W_{(23,j)}$ are bit j of message word 23 derived from Mˆ and M.

These are satisfied by with probability at least $2^{13.6}/(2^{64})^{8}$.

Total Complexity

The observations are satisfied by with

probability at least $2^{13.6}/(2^{64})^{8}$

So, $p > 2^{13.6}/(2^{64})^{8} = 2^{-498.4}$ holds.

We already computed attack time complexity as in this equation

$(T_F \cdot (\pi/4).\sqrt{(1/p)}) / \sqrt{(S/S_F)} = T_F \cdot (\pi/4) \cdot \sqrt{(S_F /pS)}$

We showed $T_F \leq 6.8$ and $S_F \leq 4.1$

Total Complexity

Therefore, when a quantum computer of size S is available,

our attack finds a collision in time

$6.8\cdot(\pi/4)\sqrt{(4.1/(2^{-498.4}\cdot S))} = 6.8\pi/4\sqrt{(4.1)}\cdot 2^{249.2}/\sqrt{S} \le 2^{252.7}/\sqrt{S}$

when $S < 2^{6.6}$, the attack time complexity $2^{252.7}/\sqrt{S}$ is lower than the generic complexity $2^{256}/S$

Therefore our attack is valid as long as $4.1 \le S < 2^{6.6}$.

Conclusion

When the attacker can access to quantum machines under the time-space tradeoff metric, we showed collision attacks on 38 and 39 steps of SHA-256 and SHA-512, respectively.

The complexity is $2^{122}/\sqrt{S}$ and $2^{252.7}/\sqrt{S}$ where $S < 2^{12}$ and $S < 2^{6.6}$ for SHA-256 and SHA-512, respectively.

We observed that even a small X may lead to an attack faster than the generic one.

Contribution

Kashish - Paper reading, Literature review, understanding of keywords

Gmail - 1111kashish1111@gmail.com

Mohammad Talib - Paper reading, Literature review, understanding of keywords

Gmail - www.talibbinjawed@gmail.com

References

Content:

https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

https://medium.com/@zaid960928/cryptography-explaining-sha-512-ad896365a0c1

https://en.wikipedia.org/wiki/SHA-2

https://privacycanada.net/hash-functions/hash-collision-attack/

Images : From Google

THANK YOU!