Collisions for Step-Reduced SHA-256

Ivica Nikolić and Alex Biryukov

University of Luxembourg

FSE, 2008

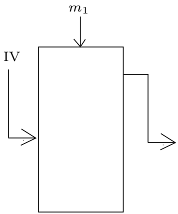
Outline

SHA-256 is based on Merkle-Damgard construction

- Divide the message in 512-bits message blocks

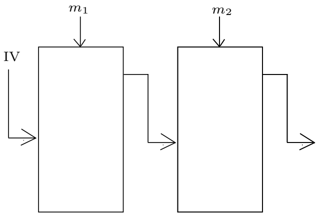
SHA-256 is based on Merkle-Damgard construction

- Divide the message in 512-bits message blocks
- One message block per compression function



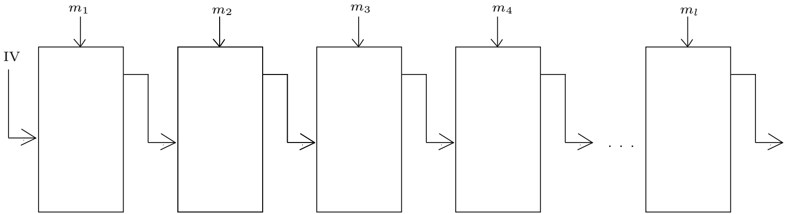
SHA-256 is based on Merkle-Damgard construction

- Divide the message in 512-bits message blocks
- One message block per compression function



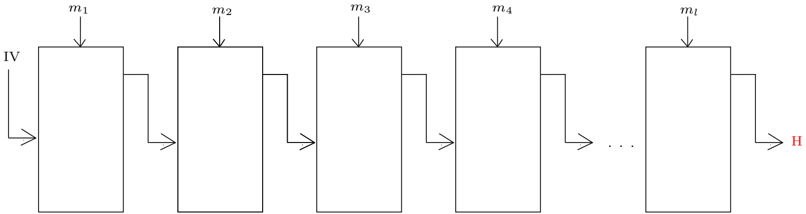
SHA-256 is based on Merkle-Damgard construction

- Divide the message in 512-bits message blocks
- One message block per compression function



SHA-256 is based on Merkle-Damgard construction

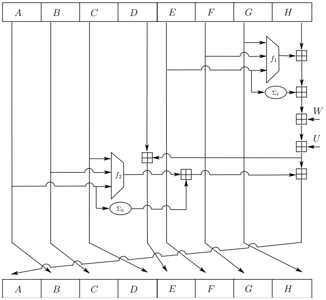
- Divide the message in 512-bits message blocks
- One message block per compression function



- Last output H is the hash of the message

Compression function for SHA-256

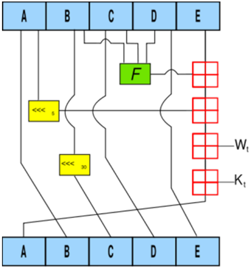
- Input: 512-bits message block + 256-bits chaining value
- 64 steps
- State update function



$$f_1(X,Y,Z) = Maj(X,Y,Z)$$
$$f_2(X,Y,Z) = Ch(X,Y,Z)$$
$$\Sigma_0(X) = ROTR^2(X) \oplus ROTR^{13}(X) \oplus ROTR^{22}(X)$$
$$\Sigma_1(X) = ROTR^6(X) \oplus ROTR^{11}(X) \oplus ROTR^{25}(X)$$

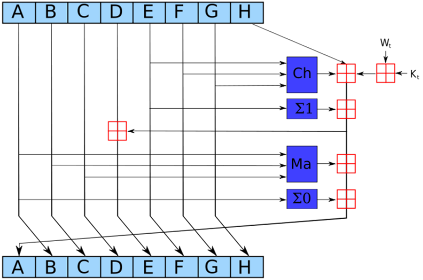
- Feed forward
- Output: 256-bits value

SHA-1



$$W_i = (W_{i-3} \oplus W_{i-8} \oplus W_{i-14} \oplus W_{i-16}) << 1$$

SHA-2



$$W_i = \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15}) + W_{i-16}$$

Differences

- Number of internal variables
- Additional functions Σ_0, Σ_1
- Message expansion

Difference between SHA-1 and SHA-2

Limit the influence of the new innovations !!!

Difference between SHA-1 and SHA-2

Limit the influence of the new innovations !!!

Additional functions (Σ_0, Σ_1)

Difference between SHA-1 and SHA-2

Limit the influence of the new innovations !!!

Additional functions (Σ_0, Σ_1)

Find fixed points,i.e. $\Sigma(x) = x$
If x, y are fixed points then $\Sigma(x) - \Sigma(y) = x - y$, i.e. Σ preserves difference

Difference between SHA-1 and SHA-2

Limit the influence of the new innovations !!!

Additional functions (Σ_0, Σ_1)

Find fixed points,i.e. $\Sigma(x) = x$
If x, y are fixed points then $\Sigma(x) - \Sigma(y) = x - y$, i.e. Σ preserves difference

Message expansion

Difference between SHA-1 and SHA-2

Limit the influence of the new innovations !!!

Additional functions (Σ_0, Σ_1)

Find fixed points,i.e. $\Sigma(x) = x$
If x, y are fixed points then $\Sigma(x) - \Sigma(y) = x - y$, i.e. Σ preserves difference

Message expansion

Expanded words don't use words with differences.

Technique for finding collisions for SHA-256

General technique

Technique for finding collisions for SHA-256

General technique

- Introduce perturbation

Technique for finding collisions for SHA-256

General technique

- Introduce perturbation
- Use as less differences as possible to correct the perturbation in the following 8 steps

Technique for finding collisions for SHA-256

General technique

- Introduce perturbation
- Use as less differences as possible to correct the perturbation in the following 8 steps
- After the perturbation is gone don't allow any other new perturbations

Technique for finding collisions for SHA-256

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i	0	0	0	0	0	0	0	0	1
i+1	1	0	0	0	1	0	0	0	δ_1
i+2	0	1	0	0	-1	1	0	0	δ_2
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0
i+5	0	0	0	0	1	0	0	-1	0
i+6	0	0	0	0	0	1	0	0	0
i+7	0	0	0	0	0	0	1	0	0
i+8	0	0	0	0	0	0	0	1	δ_4
i+9	0	0	0	0	0	0	0	0	0

Technique for finding collisions for SHA-256

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i	0	0	0	0	0	0	0	0	1
i+1	1	0	0	0	1	0	0	0	δ_1
i+2	0	1	0	0	-1	1	0	0	δ_2
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0
i+5	0	0	0	0	1	0	0	-1	0
i+6	0	0	0	0	0	1	0	0	0
i+7	0	0	0	0	0	0	1	0	0
i+8	0	0	0	0	0	0	0	1	δ_4
i+9	0	0	0	0	0	0	0	0	0

- Perturbation in step i

Technique for finding collisions for SHA-256

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i	0	0	0	0	0	0	0	0	1
i+1	1	0	0	0	1	0	0	0	δ_1
i+2	0	1	0	0	-1	1	0	0	δ_2
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0
i+5	0	0	0	0	1	0	0	-1	0
i+6	0	0	0	0	0	1	0	0	0
i+7	0	0	0	0	0	0	1	0	0
i+8	0	0	0	0	0	0	0	1	δ_4
i+9	0	0	0	0	0	0	0	0	0

- Perturbation in step i
- Correct in the following 8 steps

Technique for finding collisions for SHA-256

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i	0	0	0	0	0	0	0	0	1
i+1	1	0	0	0	1	0	0	0	δ_1
i+2	0	1	0	0	-1	1	0	0	δ_2
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0
i+5	0	0	0	0	1	0	0	-1	0
i+6	0	0	0	0	0	1	0	0	0
i+7	0	0	0	0	0	0	1	0	0
i+8	0	0	0	0	0	0	0	1	δ_4
i+9	0	0	0	0	0	0	0	0	0

- Perturbation in step i
- Correct in the following 8 steps
- Require the differences for A and E as shown in the table

Technique for finding collisions for SHA-256

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i	0	0	0	0	0	0	0	0	1
i+1	1	0	0	0	1	0	0	0	δ_1
i+2	0	1	0	0	-1	1	0	0	δ_2
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0
i+5	0	0	0	0	1	0	0	-1	0
i+6	0	0	0	0	0	1	0	0	0
i+7	0	0	0	0	0	0	1	0	0
i+8	0	0	0	0	0	0	0	1	δ_4
i+9	0	0	0	0	0	0	0	0	0

- Perturbation in step i
- Correct in the following 8 steps
- Require the differences for A and E as shown in the table
- Get system of equations with the respect to δ_i and A_i or E_i

Technique for finding collisions for SHA-256

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i	0	0	0	0	0	0	0	0	1
i+1	1	0	0	0	1	0	0	0	δ_1
i+2	0	1	0	0	-1	1	0	0	δ_2
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0
i+5	0	0	0	0	1	0	0	-1	0
i+6	0	0	0	0	0	1	0	0	0
i+7	0	0	0	0	0	0	1	0	0
i+8	0	0	0	0	0	0	0	1	δ_4
i+9	0	0	0	0	0	0	0	0	0

- Perturbation in step i
- Correct in the following 8 steps
- Require the differences for A and E as shown in the table
- Get system of equations with the respect to δ_i and A_i or E_i
- Solve the system

Technique for finding collisions for SHA-256

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i	0	0	0	0	0	0	0	0	1
i+1	1	0	0	0	1	0	0	0	δ_1
i+2	0	1	0	0	-1	1	0	0	δ_2
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0
i+5	0	0	0	0	1	0	0	-1	0
i+6	0	0	0	0	0	1	0	0	0
i+7	0	0	0	0	0	0	1	0	0
i+8	0	0	0	0	0	0	0	1	δ_4
i+9	0	0	0	0	0	0	0	0	0

- Perturbation in step i
- Correct in the following 8 steps
- Require the differences for A and E as shown in the table
- Get system of equations with the respect to δ_i and A_i or E_i
- Solve the system

Technique for finding collisions for SHA-256

Example - step $i + 4$

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0

Technique for finding collisions for SHA-256

Example - step $i+4$

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0

- From the definition of SHA-256, we have:
  $\Delta A_{i+4} - \Delta E_{i+4} = \Delta\Sigma_0(A_{i+3}) + \Delta Maj_{i+3}(\Delta A_{i+3}, \Delta B_{i+3}, \Delta C_{i+3}) - \Delta D_{i+3}$
  $\Delta E_{i+4} = \Delta\Sigma_1(E_{i+3}) + \Delta Ch_{i+3}(\Delta E_{i+3}, \Delta F_{i+3}, \Delta G_{i+3}) + \Delta H_{i+3} + \Delta D_{i+3} + \Delta W_{i+3}$

Technique for finding collisions for SHA-256

Example - step $i+4$

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0

- From the definition of SHA-256, we have:
  $\Delta A_{i+4} - \Delta E_{i+4} = \Delta\Sigma_0(A_{i+3}) + \Delta Maj_{i+3}(\Delta A_{i+3}, \Delta B_{i+3}, \Delta C_{i+3}) - \Delta D_{i+3}$
  $\Delta E_{i+4} = \Delta\Sigma_1(E_{i+3}) + \Delta Ch_{i+3}(\Delta E_{i+3}, \Delta F_{i+3}, \Delta G_{i+3}) + \Delta H_{i+3} + \Delta D_{i+3} + \Delta W_{i+3}$

- From the condition for step $i+3$, we have
  $\Delta D_{i+3} = 0, \Delta H_{i+3} = 0, \Delta\Sigma_0(A_{i+3}) = 0, \Delta\Sigma_1(E_{i+3}) = 0.$

Technique for finding collisions for SHA-256

Example - step $i+4$

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0

- From the definition of SHA-256, we have:
  $\Delta A_{i+4} - \Delta E_{i+4} = \Delta\Sigma_0(A_{i+3}) + \Delta Maj_{i+3}(\Delta A_{i+3}, \Delta B_{i+3}, \Delta C_{i+3}) - \Delta D_{i+3}$
  $\Delta E_{i+4} = \Delta\Sigma_1(E_{i+3}) + \Delta Ch_{i+3}(\Delta E_{i+3}, \Delta F_{i+3}, \Delta G_{i+3}) + \Delta H_{i+3} + \Delta D_{i+3} + \Delta W_{i+3}$
- From the condition for step $i+3$, we have
  $\Delta D_{i+3} = 0, \Delta H_{i+3} = 0, \Delta\Sigma_0(A_{i+3}) = 0, \Delta\Sigma_1(E_{i+3}) = 0.$
- We require $\Delta A_{i+4} = 0, \Delta E_{i+4} = 0.$

Technique for finding collisions for SHA-256

Example - step $i+4$

step	ΔA	ΔB	ΔC	ΔD	ΔE	ΔF	ΔG	ΔH	ΔW
i+3	0	0	1	0	0	-1	1	0	δ_3
i+4	0	0	0	1	0	0	-1	1	0

- From the definition of SHA-256, we have:
  $\Delta A_{i+4} - \Delta E_{i+4} = \Delta\Sigma_0(A_{i+3}) + \Delta Maj_{i+3}(\Delta A_{i+3}, \Delta B_{i+3}, \Delta C_{i+3}) - \Delta D_{i+3}$
  $\Delta E_{i+4} = \Delta\Sigma_1(E_{i+3}) + \Delta Ch_{i+3}(\Delta E_{i+3}, \Delta F_{i+3}, \Delta G_{i+3}) + \Delta H_{i+3} + \Delta D_{i+3} + \Delta W_{i+3}$
- From the condition for step $i+3$, we have
  $\Delta D_{i+3} = 0, \Delta H_{i+3} = 0, \Delta\Sigma_0(A_{i+3}) = 0, \Delta\Sigma_1(E_{i+3}) = 0.$
- We require $\Delta A_{i+4} = 0, \Delta E_{i+4} = 0.$
- So we deduce:
  $\Delta Maj_{i+3}(0,0,1) = 0$
  $W_{i+3} = -\Delta Ch_{i+3}(0,-1,1)$

  Solution:
  $A_{i+3} = A_{i+2}$
  $\delta_3 = -\Delta Ch_{i+3}(0,-1,1)$

Technique for finding collisions for SHA-256

Solution of the system of equations

$$A_{i-1} = A_{i+1} = A_{i+2} = A_{i+3}$$
$$A_{i+1} = -1$$
$$E_{i+3} = E_{i+4}$$
$$E_{i+6} = 0$$
$$E_{i+7} = -1$$

$$\delta_1 = -1 - \Delta Ch_{i+1}(1,0,0) - \Delta\Sigma_1(E_{i+1})$$
$$\delta_2 = \Delta\Sigma_1(E_{i+2}) - \Delta Ch_{i+2}(-1,1,0)$$
$$\delta_3 = -\Delta Ch_{i+3}(0,-1,1)$$
$$\delta_4 = -1$$

Unsolved equation (no degrees of freedom left)
$\Delta Ch_{i+3}(0,0,-1) = -1$
It holds with probability $\frac{1}{3} \approx 2^{-1.5}$

20-step reduced SHA-256

W	5	6	7	8	13
0					
1					
2					
3					
4					
5	X				
6		X			
7			X		
8				X	
9					
10					
11					
12					
13					X
14					
15					
16					
17					
18					
19					

Collision

- Perturbation in W_5
- Corrections in W_6, W_7, W_8, W_{13}
- Message expansion after the step 13 doesn't use any of these words
- Complexity $= \frac{1}{3}$

21-step reduced SHA-256

W	6	7	8	9	14
0					
1					
2					
3					
4					
5					
6	X				
7		X			
8			X		
9				X	
10					
11					
12					
13					
14					X
15					
16				X	X
17					
18				X	X
19					
20				X	X

Collision

- Perturbation in W_6
- Corrections in W_7, W_8, W_9, W_{14}
- Message expansion uses W_9, W_{14}
- Additional equation is introduced: $\Delta\sigma_1(W_{14}) + \Delta W_9 = 0$, where $\Delta W_{14} = -1$
- Total complexity is 2^{19}

23-step reduced SHA-256

W	9	10	11	12
0				
1				
2				
3				
4				
5				
6				
7				
8				
9	X			
10		X		
11			X	
12				X
13				
14				
15				
16	X			
17		X		
18	X		X	
19		X		X
20	X		X	
21		X		X
22	X		X	

Semi-free start collision

- Perturbation in W_9
- Corrections in W_{10}, W_{11}, W_{12}. W_{17} is extended word, so it is not possible to control it directly
- Message expansion uses $W_9, W_{10}, W_{11}, W_{12}$
- In the original differential path there is no difference in W_{16}
  We have to slightly change our differential path
  New system of equations is introduced and solved
- Semi-free start in order to control W_{16}, W_{17}
- Additional equations are introduced in order to keep the differences zero after the last step of the path
- Total complexity is 2^{21}

25-step reduced SHA-256

W	9	10	11	12
0				
1				
2				
3				
4				
5				
6				
7				
8				
9	X			
10		X		
11			X	
12				X
13				
14				
15				
16	X			
17		X		
18	X		X	
19		X		X
20	X		X	
21		X		X
22	X		X	

Semi-free start near collision with Hamming distance of 17 bits

- Extend semi-free start collision for 23-step reduced SHA-256
- Minimize the Hamming distance of the introduced differences for A and E registers
- Total complexity is 2^{34}

Conclusions

- Low complexities allow to find real collisions
- Technique applicable to SHA-224, SHA-384, and SHA-512
- No real treat for the security of SHA-2