Some applications of the Biham-Chen attack

Conference Hash Functions

Conference Center of the Jagiellonian University
Przegorzały (Kraków)
Jun. 24th, 2005

Hirotaka Yoshida
Systems Development Laboratory, Hitachi, Ltd., Japan
Alex Biryukov, Bart Preneel
Katholieke Universiteit Leuven, Belgium

Overview of the talk

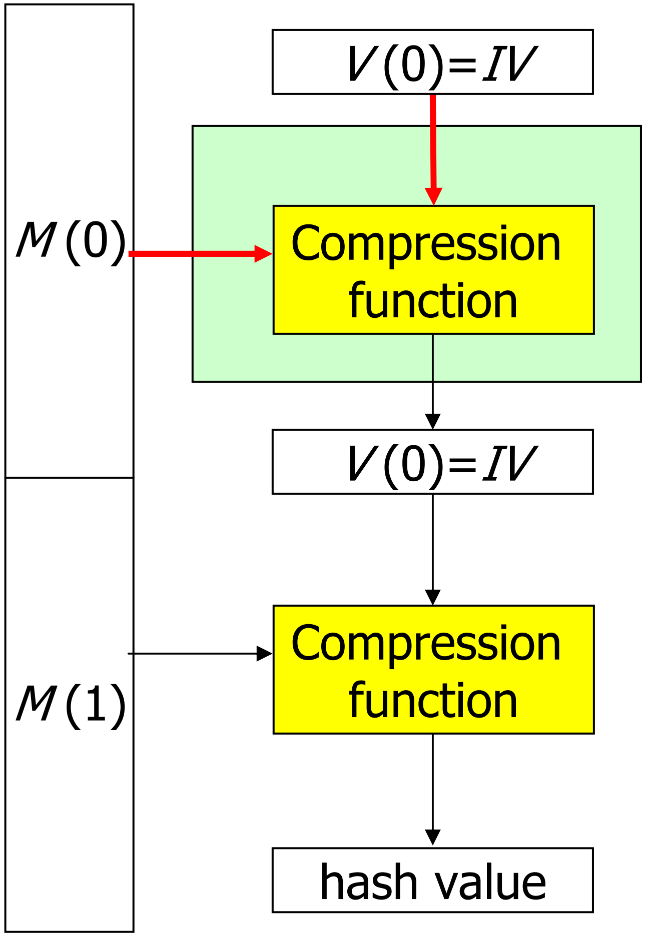
- Introduction to some resistances of hash functions
- Cryptanalysis of hash functions in encryption mode.
- Description of the Biham-Chen attack
- Applications to MD5 and a SHA-256 variant
- Conclusions

Some resistances of hash functions

- Near-collision resistance
  - Resistance against attacks finding a pair of hash values which differ in only small number of bit positions.
- Pseudo-collision resistance
  - Resistance against collision attacks where different initial vectors can be chosen.
- Randomness
  - Resistance against attacks distinguishing it from a random function.

Pseudo-collision resistance

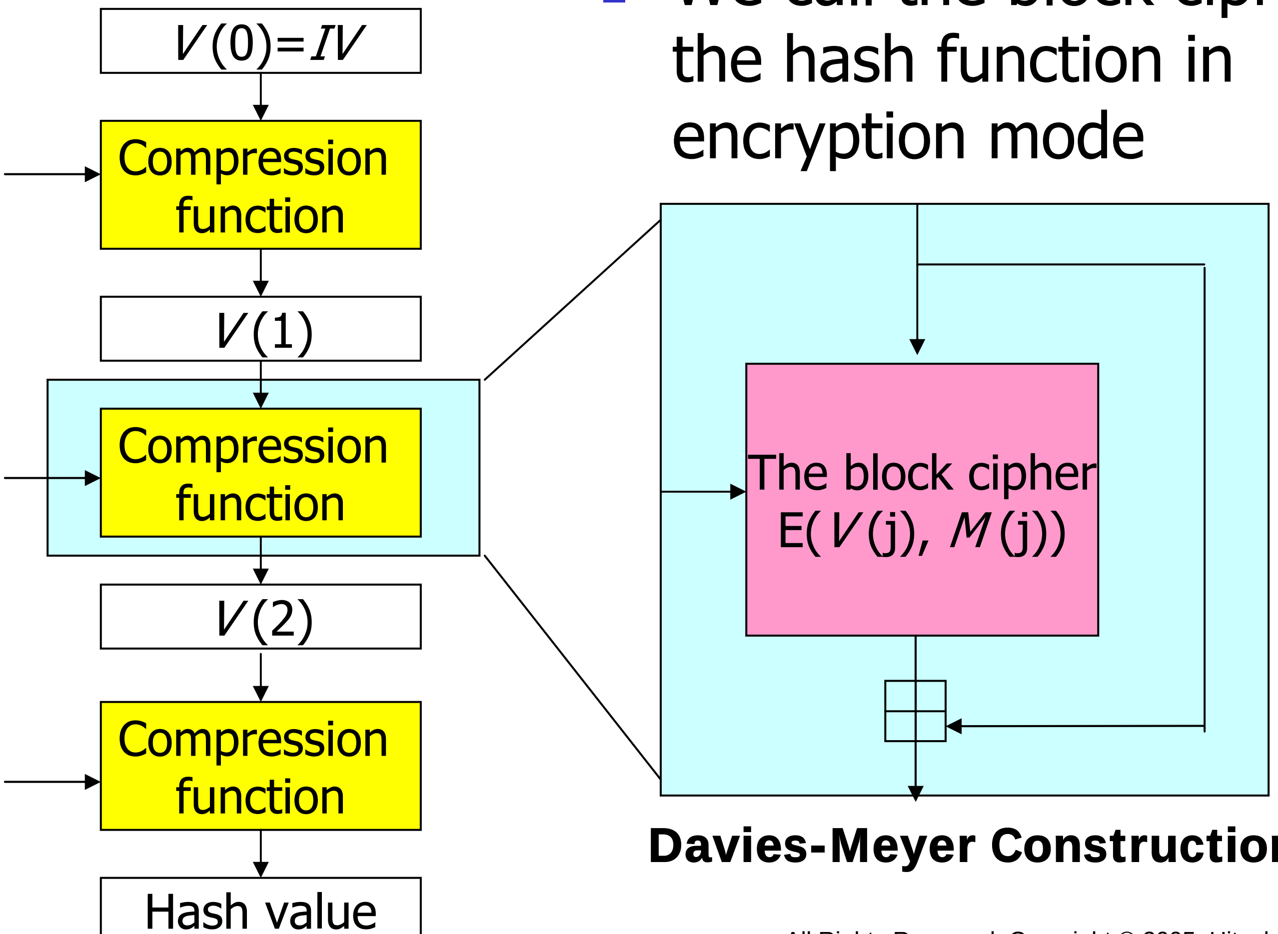
The MD-construction



- Resistance when 2 inputs controlled.
- Important in the theory of the MD-construction
- There could be some application which requires the underlying hash function to have this resistance
  - Knudsen *et al*, Preimage and pseudo-collision attack on MD2, FSE2005

Hash Function in encryption mode

- We call the block cipher *E* the hash function in encryption mode



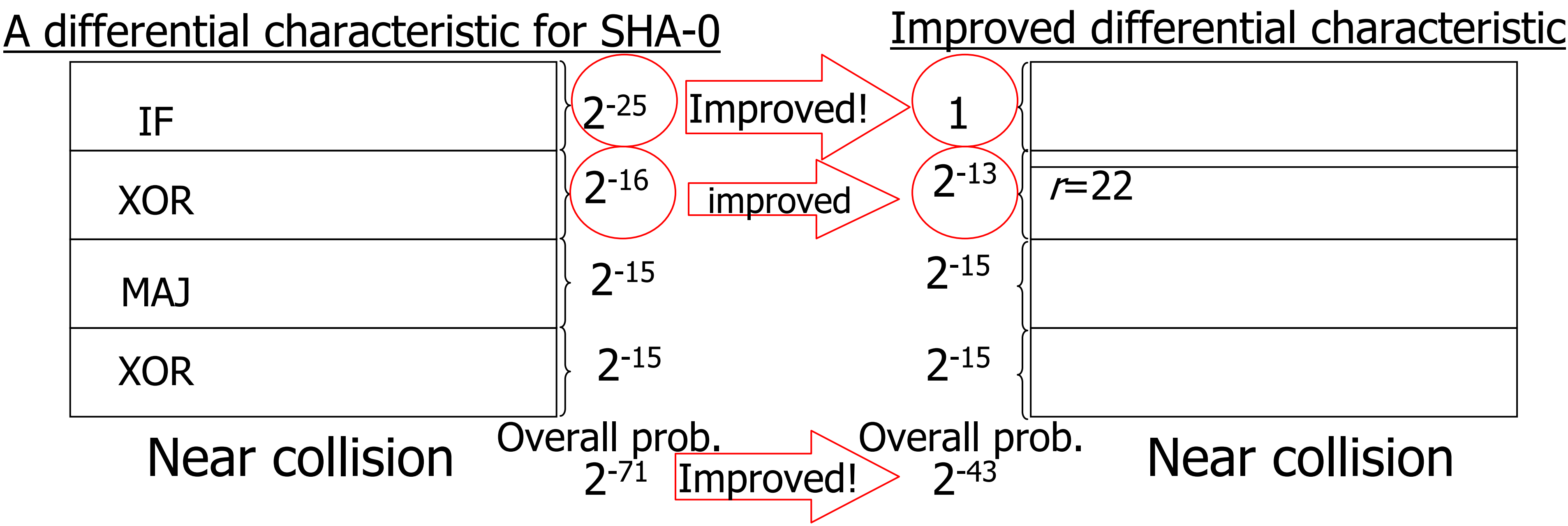
Davies-Meyer Construction

Cryptanalysis of Hash functions in Encryption Mode

- Differential cryptanalysis of SHA-1
  - Handschuh *et al.*, SHACAL, Submission to the NESSIE project, 2000.
- Slide attack on SHA-1
  - Saarinen, Cryptanalysis of Block Ciphers Based on SHA-1 and MD5, FSE2003.
- Attack on MD5 which finds one high-probability differential characteristic.
  - Saarinen, Cryptanalysis of Block Ciphers Based on SHA-1 and MD5, FSE2003.
- Attack which distinguishes HAVAL from a random function.
  - Yoshida *et al.*, Non-randomness of the Full 4 and 5-pass HAVAL, SCN2004.

Description of Biham and Chen attack

- Near-collision attack on SHA-0
  - Biham and Chen, near-collision of SHA-0, CRYPTO 2004



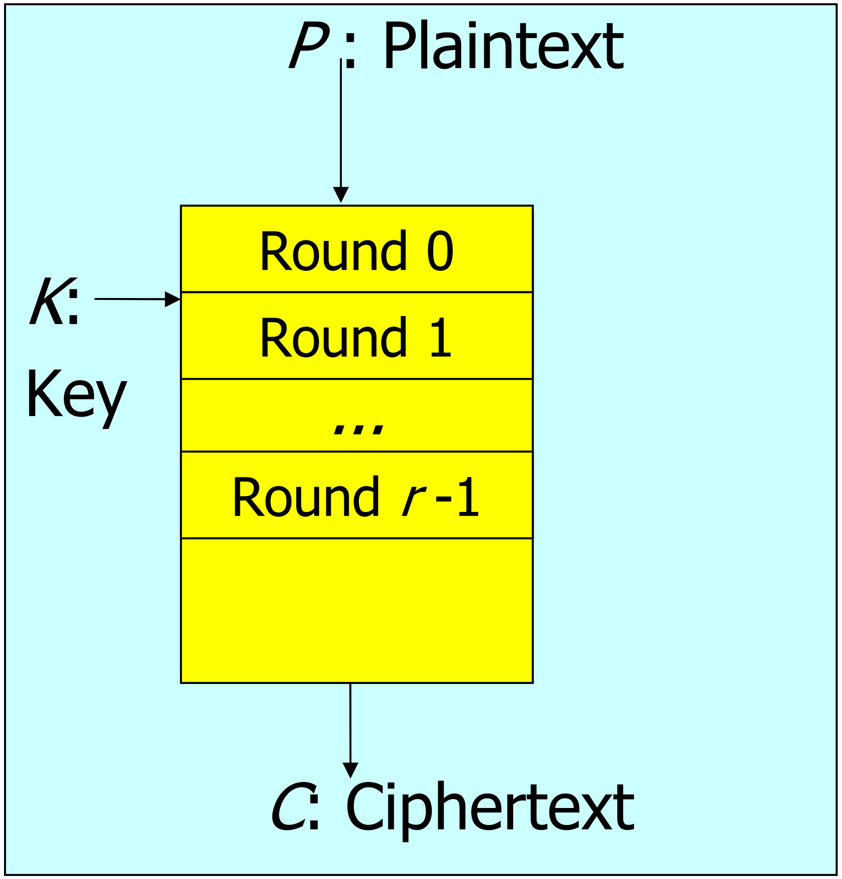
- Start the collision search from some intermediate round *r*.
- Use messages generated from *neutral bits*

Concept of neutral bits

- *Neutral bits* do not affect the difference for r rounds.
- Obtaining $k(r)$ neutral bits allows to generate a set of $2^{k(r)}$ messages.
- Using this set gives us a better probability for r rounds than the probability when using a set of randomly chosen messages.

Differential Cryptanalysis of a Hash Function in Encryption Mode

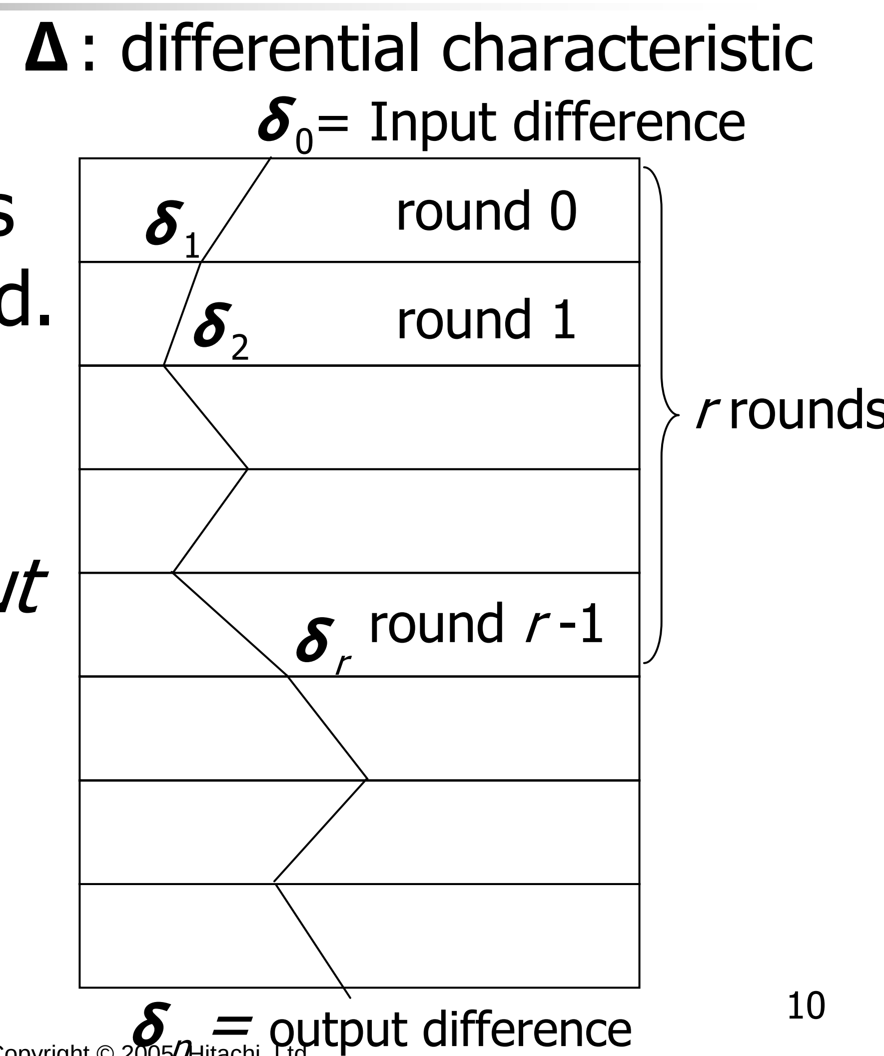
- We assume:
  - A differential characteristic, Δ has already been found
  - the key value K is fixed to one value $K=K_0$



$E(K, P)$

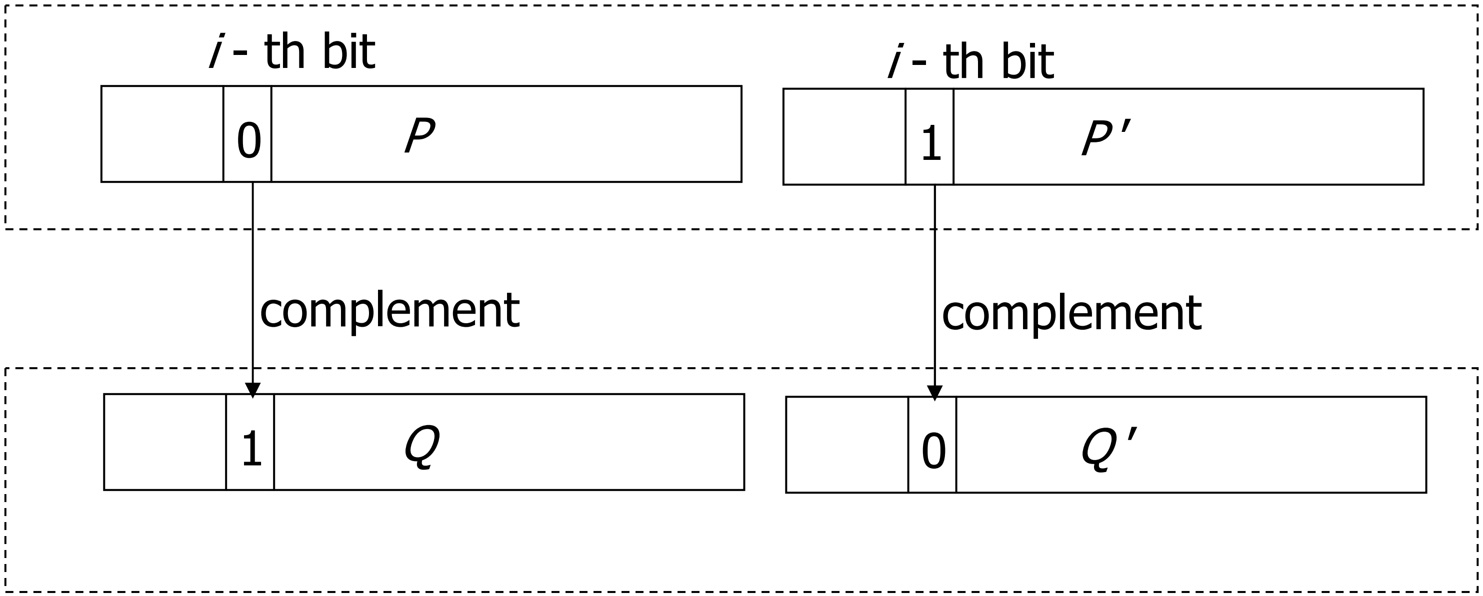
Differential Cryptanalysis of a Hash Function in Encryption Mode

- *Δ* defines the expected differences δ_r of the values of all registers in each round.
- Definition.
  (P, P') conforms to Δ_r if the differences at the output of the first r rounds are as expected.



Differential Cryptanalysis of a Hash Function in Encryption Mode

Assume that (P, P') conforms to Δ_r

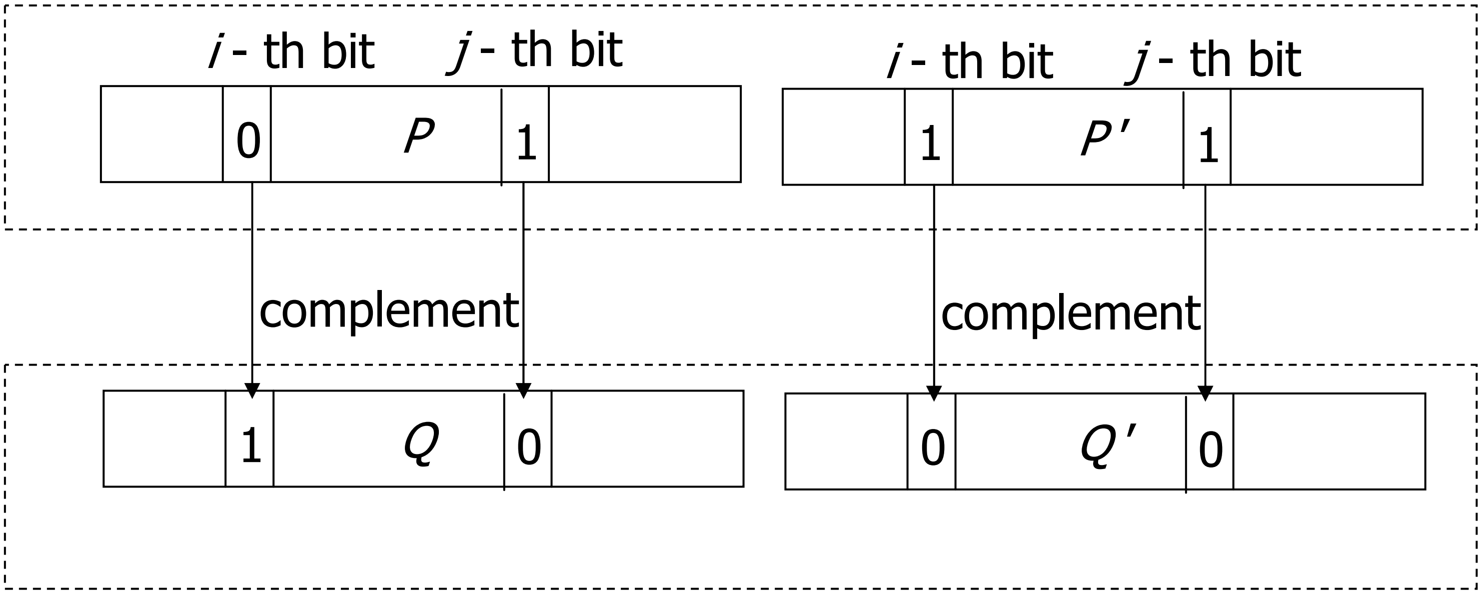


If (Q, Q') conforms to Δ_r, the *i* -th bit is called neutral bit.

Differential Cryptanalysis of a Hash Function in Encryption Mode

Assume that *(P, P′)* conforms to Δ_r

Let *i* -th bit and *j* -th bit be neutral bits.



If *(Q, Q')* conforms to Δ_r , there is an edge between *i* -th bit and *j* -th bit.

An algorithm for finding a 2-neutral set

Step1: Find a pair of plaintexts that conforms to Δ_r for some r

Step2: Find the set S of singles of neutral bits

Step3: Find neutral pairs in S

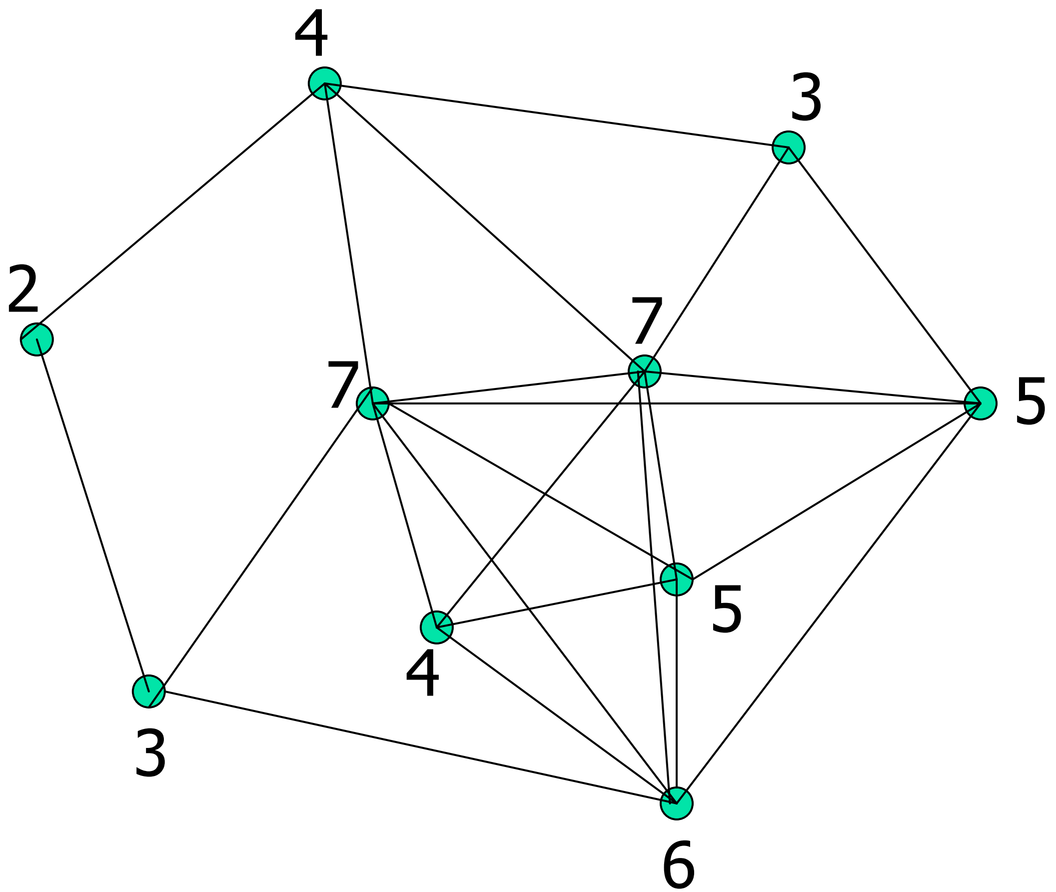
Step4: Count the number of edges for each element of S

Step5: If the resulting set is a neutral set, break

Otherwise remove from S one of the elements which has the least number of edges.

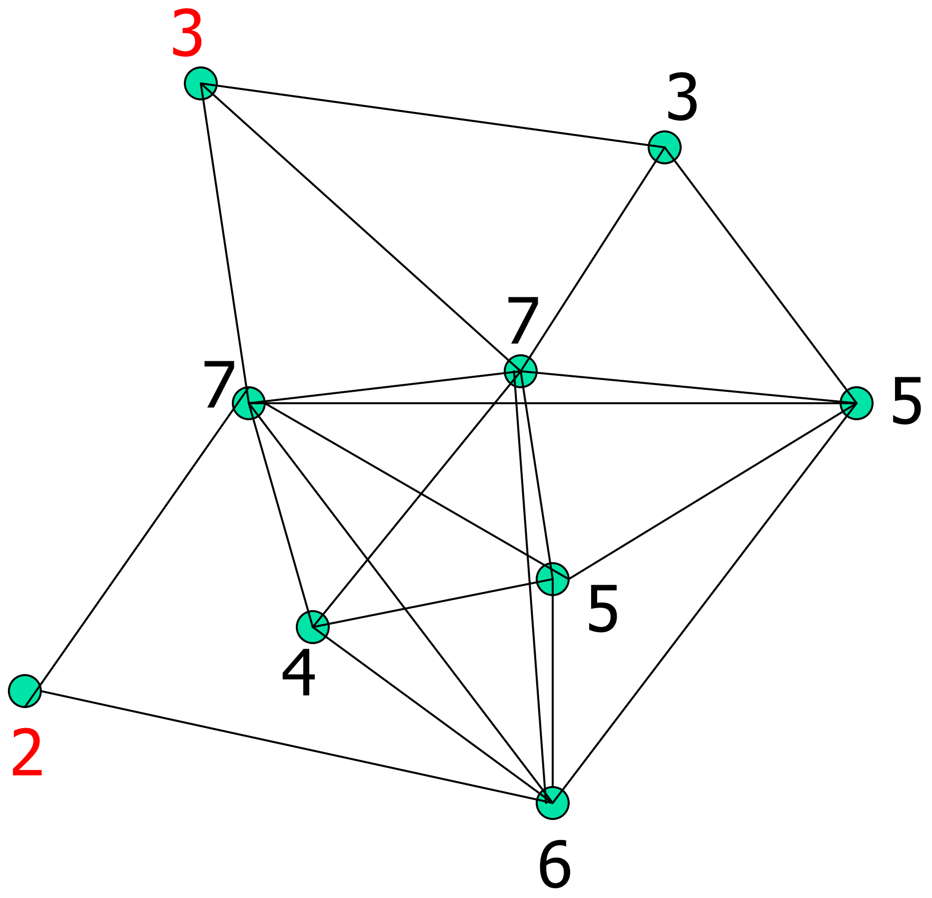
Let the resulting set be S go to step 3

How to construct 2-neutral sets

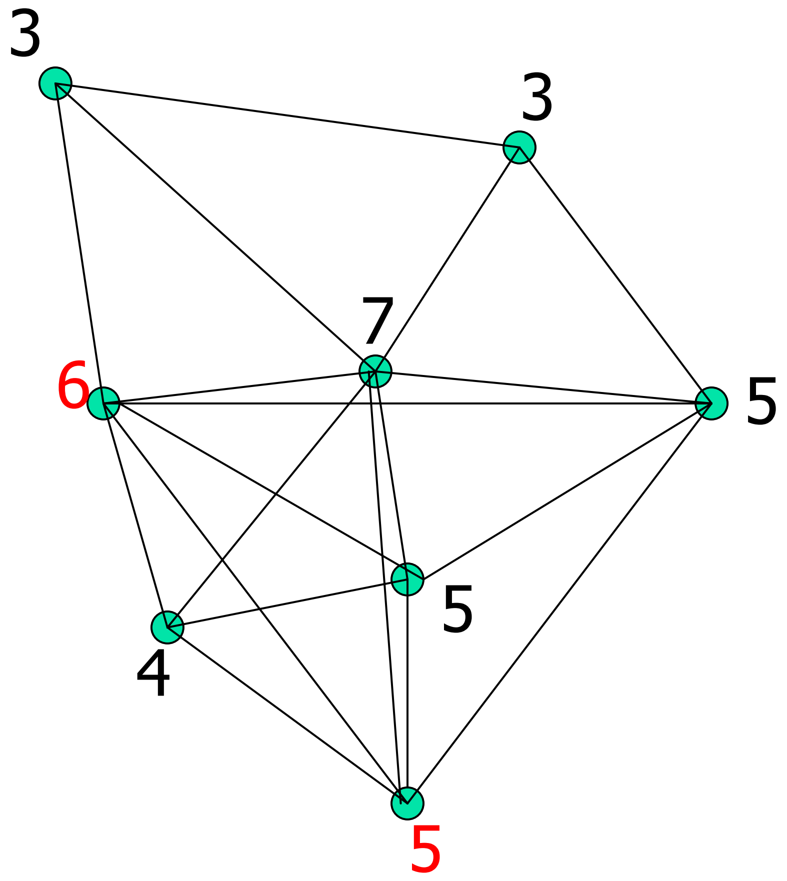


- *neutral bits* do not affect the difference for *r* rounds.

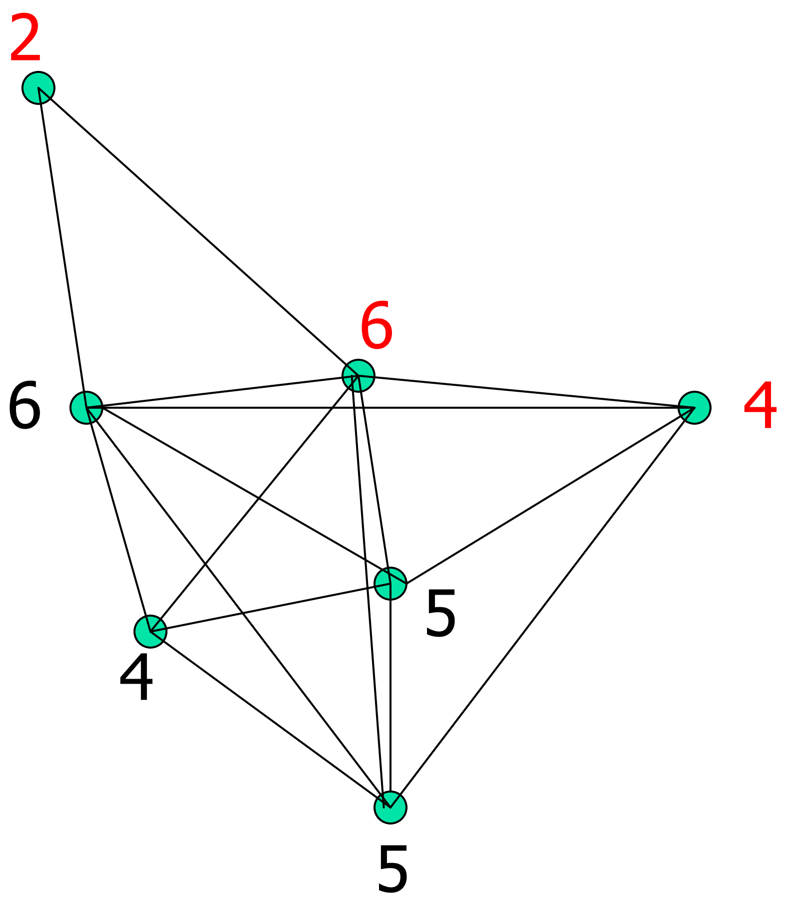
How to construct 2-neutral sets



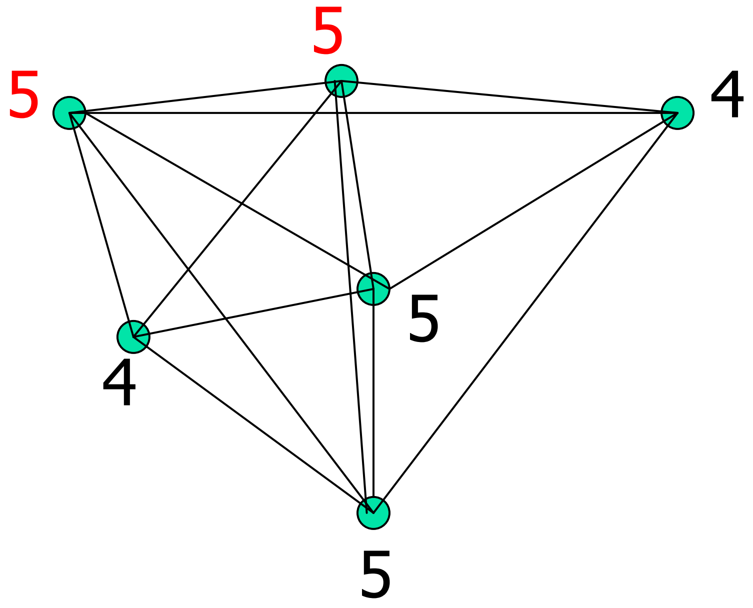
How to construct 2-neutral sets



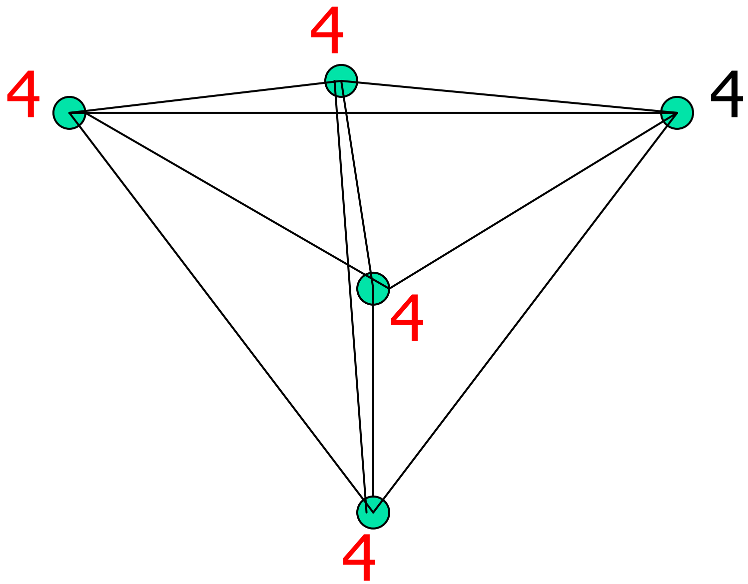
How to construct 2-neutral sets



How to construct 2-neutral sets

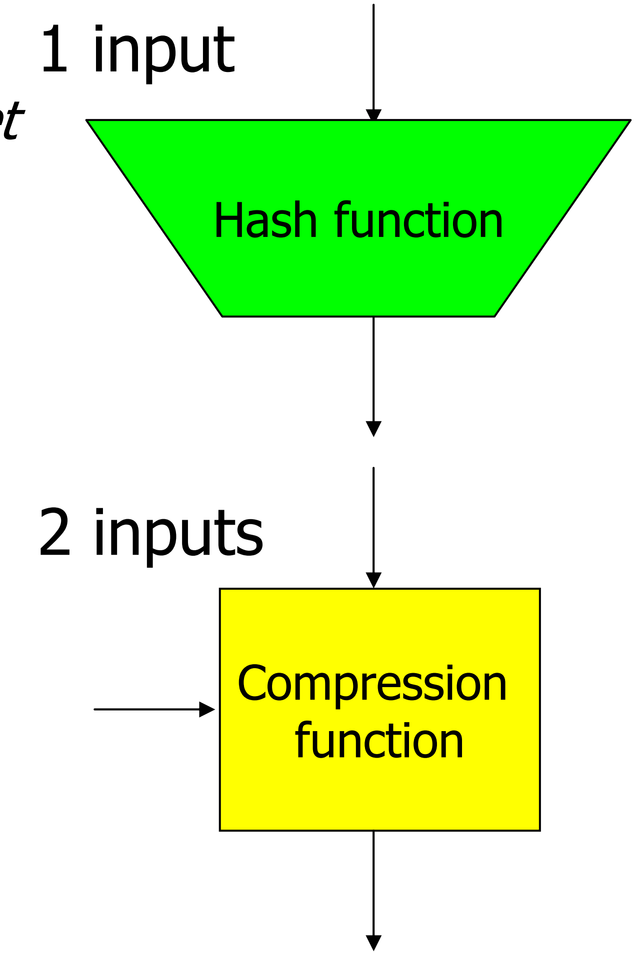


How to construct 2-neutral sets

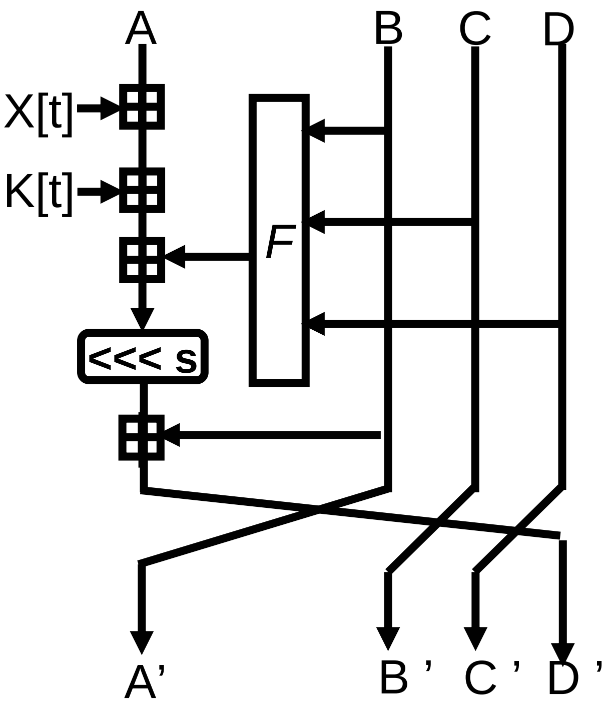


Application to MD5 hash function

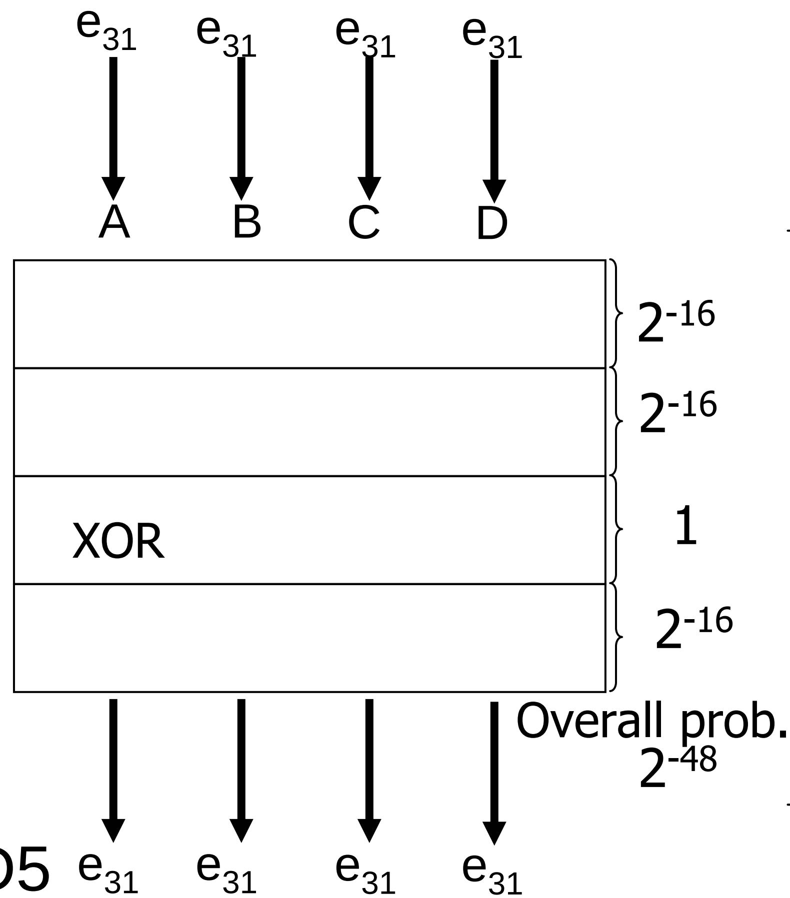
- Attacks on MD5
  - Attacks for finding collisions (Wang *et al.*, Eurocrypt 2005).
- Attacks on the compression function of MD5
  - Attacks for finding pseudo-collisions (Dobbertin. Cryptanalysis of MD5 Compress., at Eurocrypt '96 rump session)
  - Attacks for finding pseudo-collisions (Saarinen, FSE 2003)

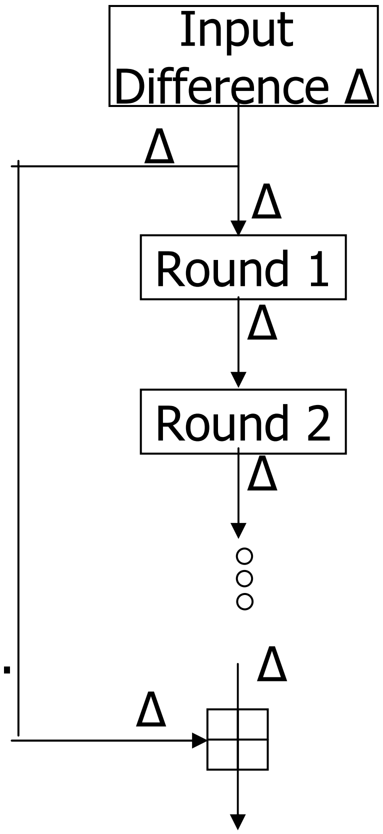


Saarinen’s iterative characteristic



The step function of MD5





Pseudo-collision

Experimental results

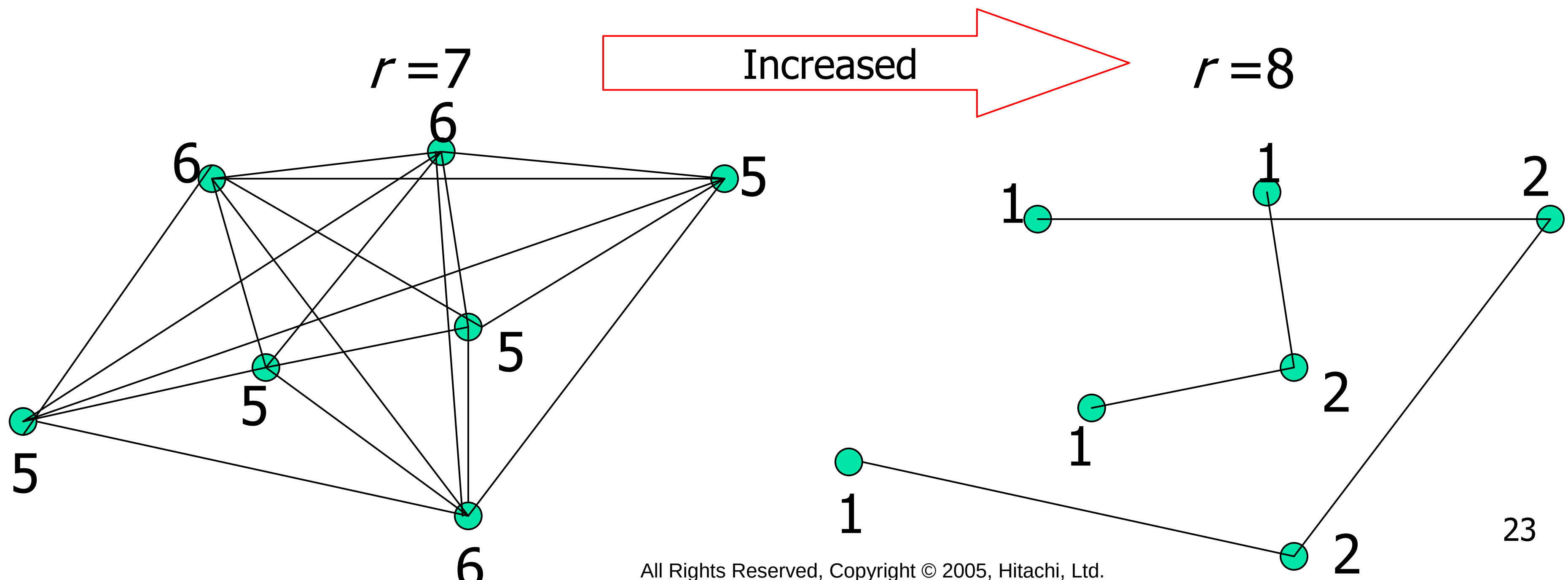
- 4 different non-linear functions are used.
- It is interesting to see the improvements for each of the 16 rounds.

Probability comparison

Rounds	Previous probability	Improved probability
0-15	2^{-16}	$2^{-6.46}$
16-31	2^{-16}	$2^{-9.33}$
32-47	1	1
48-63	2^{-16}	$2^{-7.22}$

Observations

- The obtained sets could be too small to attack many rounds.
- When *r* is increased, the number of edges for each element is rapidly decreased.



Experimental results

A set of neutral bits of size 34 for $r = 7$, which is almost 2-neutral
(The bits are numbered in the range 0, ..., 127)

P = 0x938858dc 0xf310b6b4 0xa9f02359 0x1207a9e3
P'= 0x138858dc 0x7310b6b4 0x29f02359 0x9207a9e3
S = {3,4,6,8,9,13,20,21,22,30,33,34,40,41,43,47,57,58,59, 62,65,66,74,88,96,104,105,106,107,108,113,123,125,126}

Experimental results

- Probability of the 49-round characteristic obtained from *S* is about 2^{-27}, which is 2^{6} higher than the original probability.
- In practice, we found 132 pseudo collisions for 49 rounds of MD5 with complexity 2^{34}

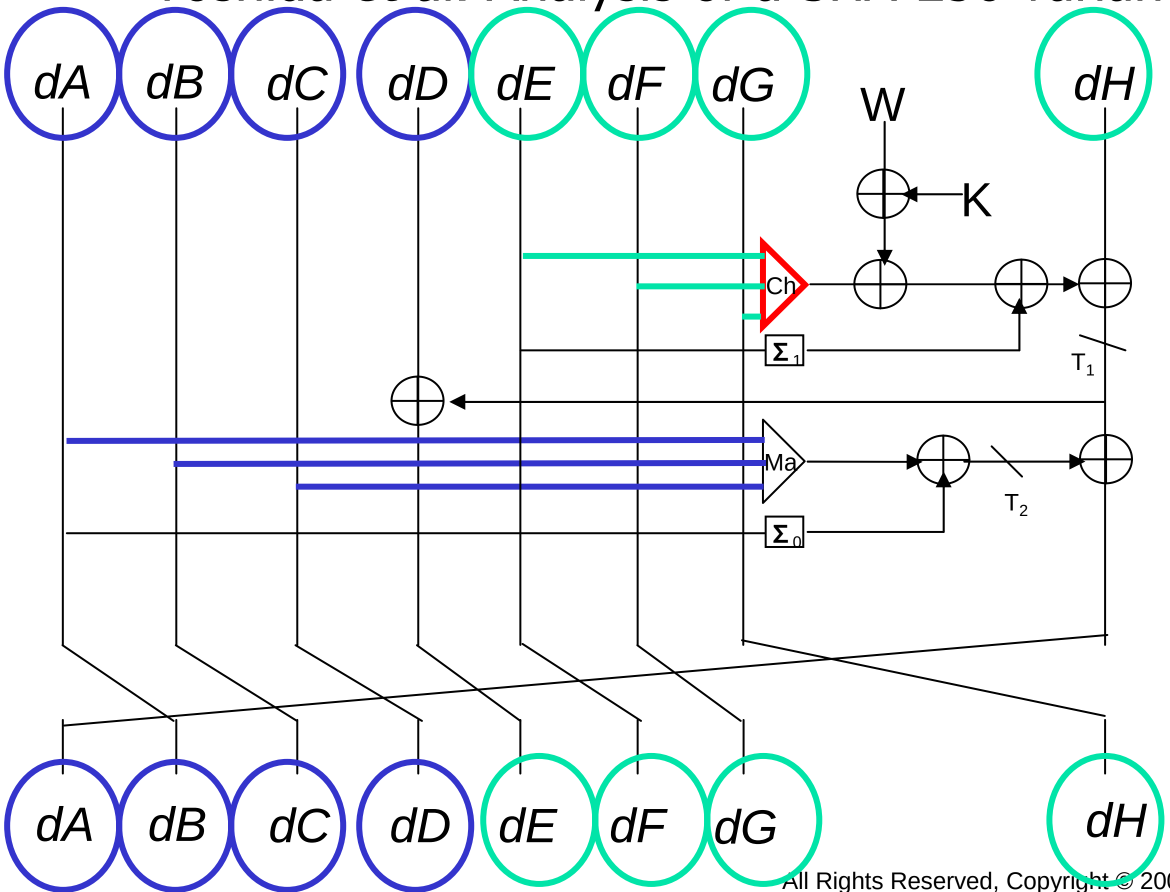
Plaintext pair which produces a pseudo collision for 49 rounds:

Q = 0xd3b8788c 0xf910b4b6 0xa9f02359 0x1a05b4e3
Q'= 0x53b8788c 0x7910b4b6 0x29f02359 0x9a05b4e3

Application to a SHA-256 variant

One-round iterative for a SHA-256 variant (SHA-2-XOR) presented

- Yoshida *et al*. Analysis of a SHA-256 variant., at FSE 2005 rump session



- Best probability 2^{-8}
- Pseudo-collision for 4-round SHA-2-XOR with complexity 2^{32}

Apply our technique here

- Pseudo-collision for 8-round with same complexity

Conlusions

- We discussed some resistances and tried to apply the Biham-Chen attack to study hash functions regarding these resistances.
- Some improved results on MD5 and a SHA-256 variant were presented.
- The generic approach here may find interesting results on hash functions regarding these two resistances for which differential characteristics have been already found.