Generalized condition propagation, and Meet-in-the-middle attacks

Christian Rechberger

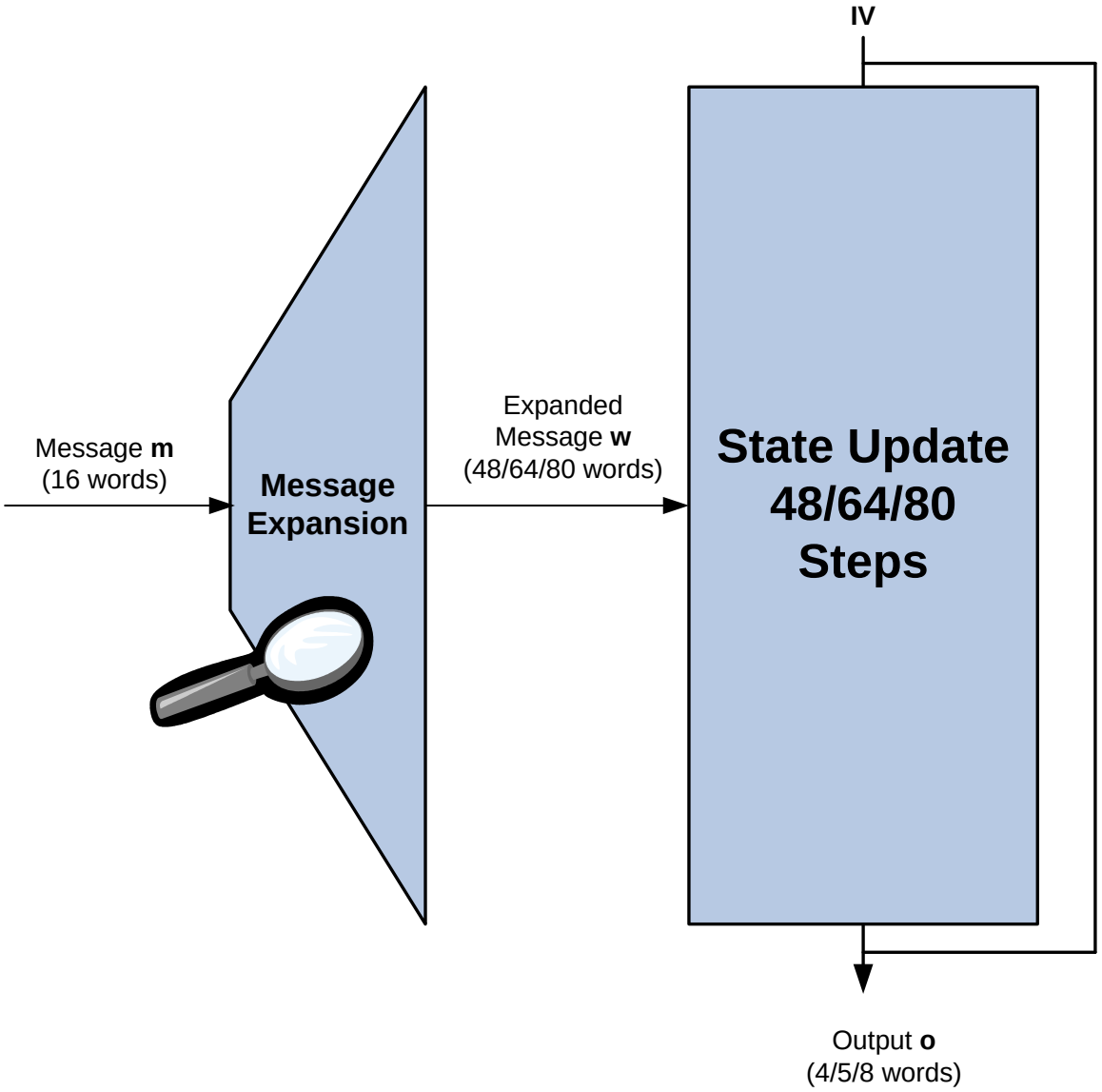
Šibenik, 2014

Overview

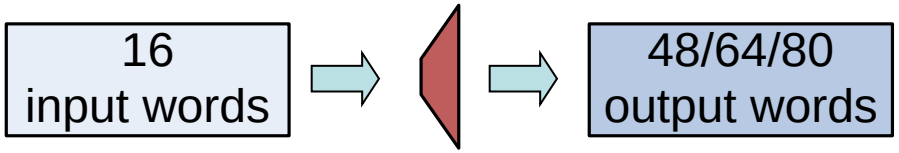
- Two methods, both applicable for hash and cipher cryptanalysis
  - Generalized condition propagation
    - Use case SHA-0/1/2
  - Meet-in-the-middle:
    - Use case: Bicliques and AES

Generalized condition propagation

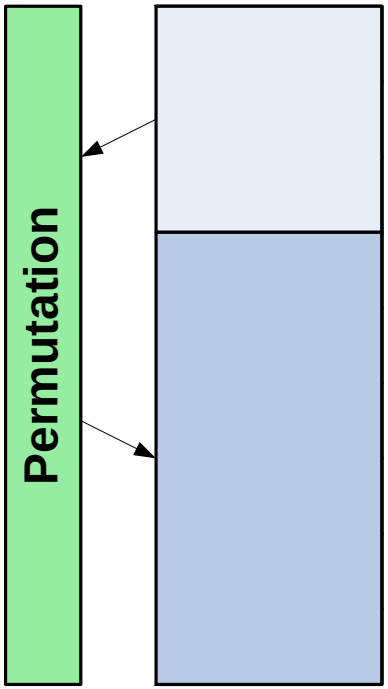
Outline of MD4-style Hash Functions



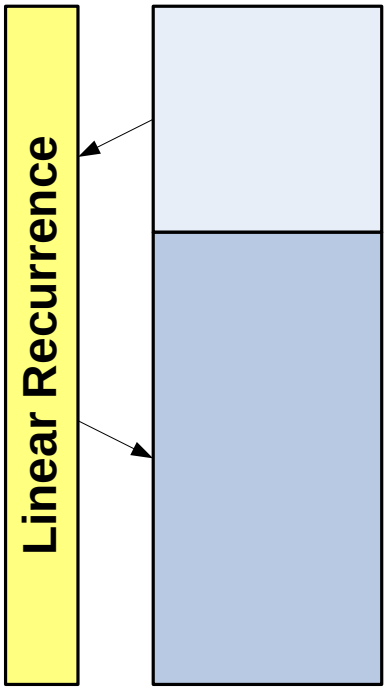
Message Expansions in the MD4 family



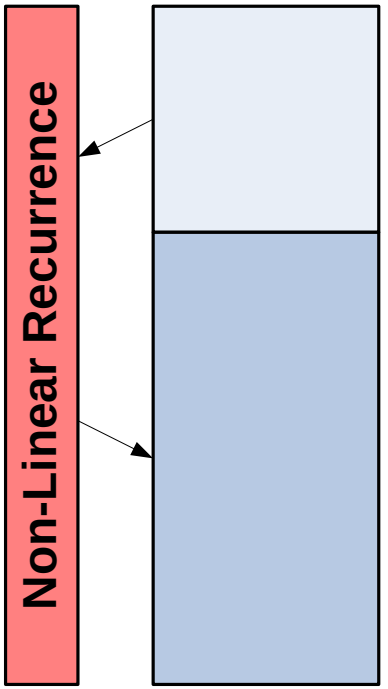
MD4/5, RIPEMD



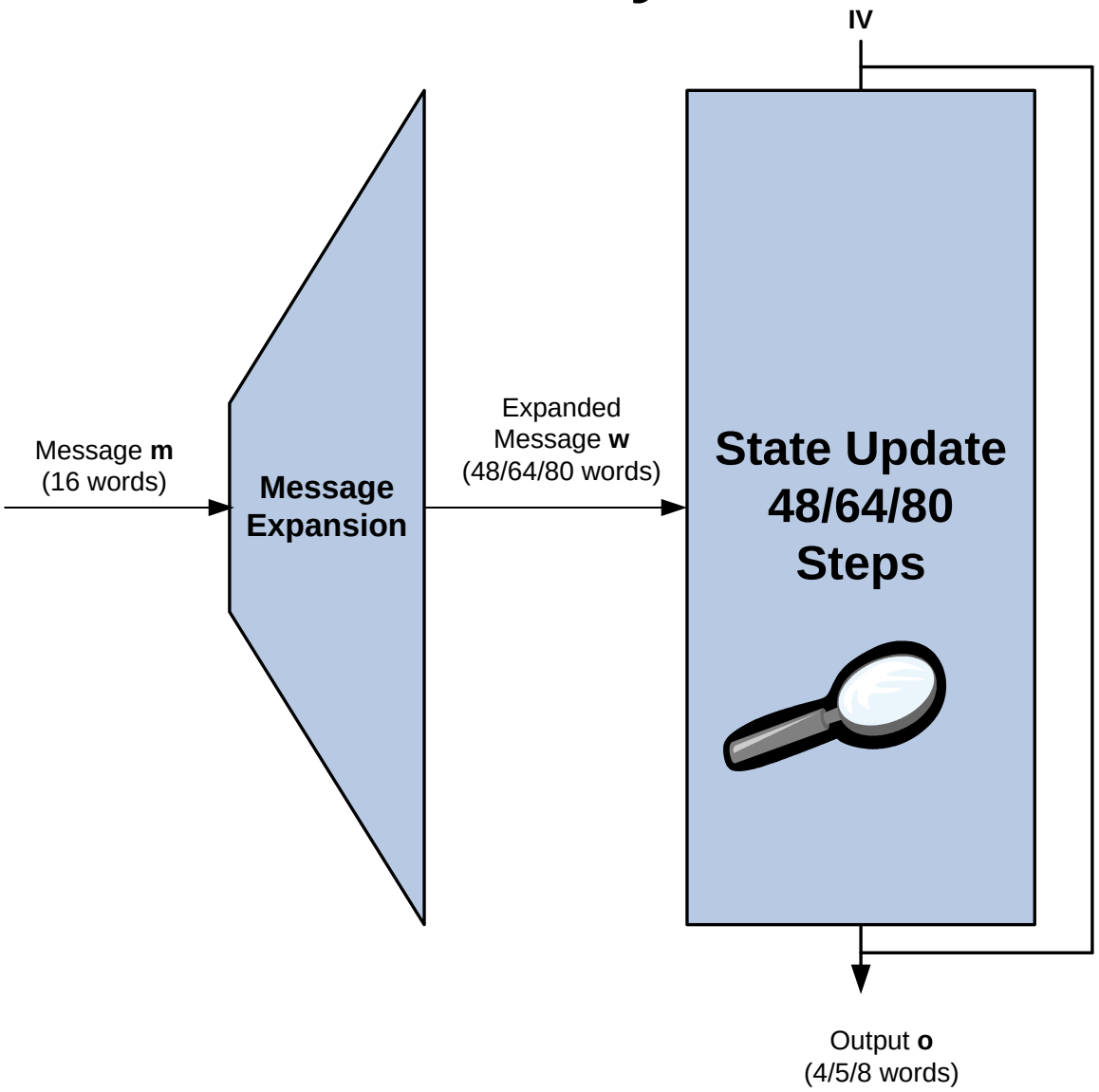
SHA / SHA-1



SHA-2 members

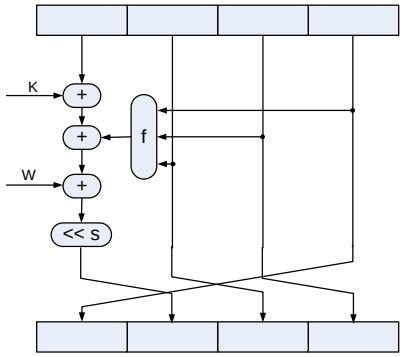


Outline of MD4-style Hash Functions

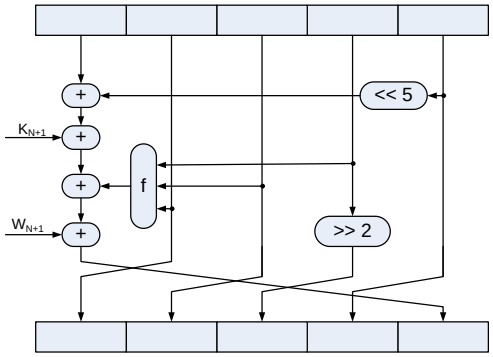


Evolution of the State Updates in the MD4 Family

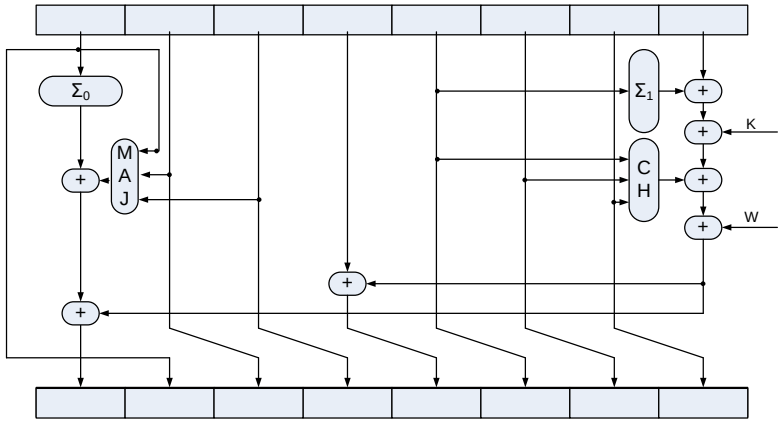
MD4



SHA/SHA-1

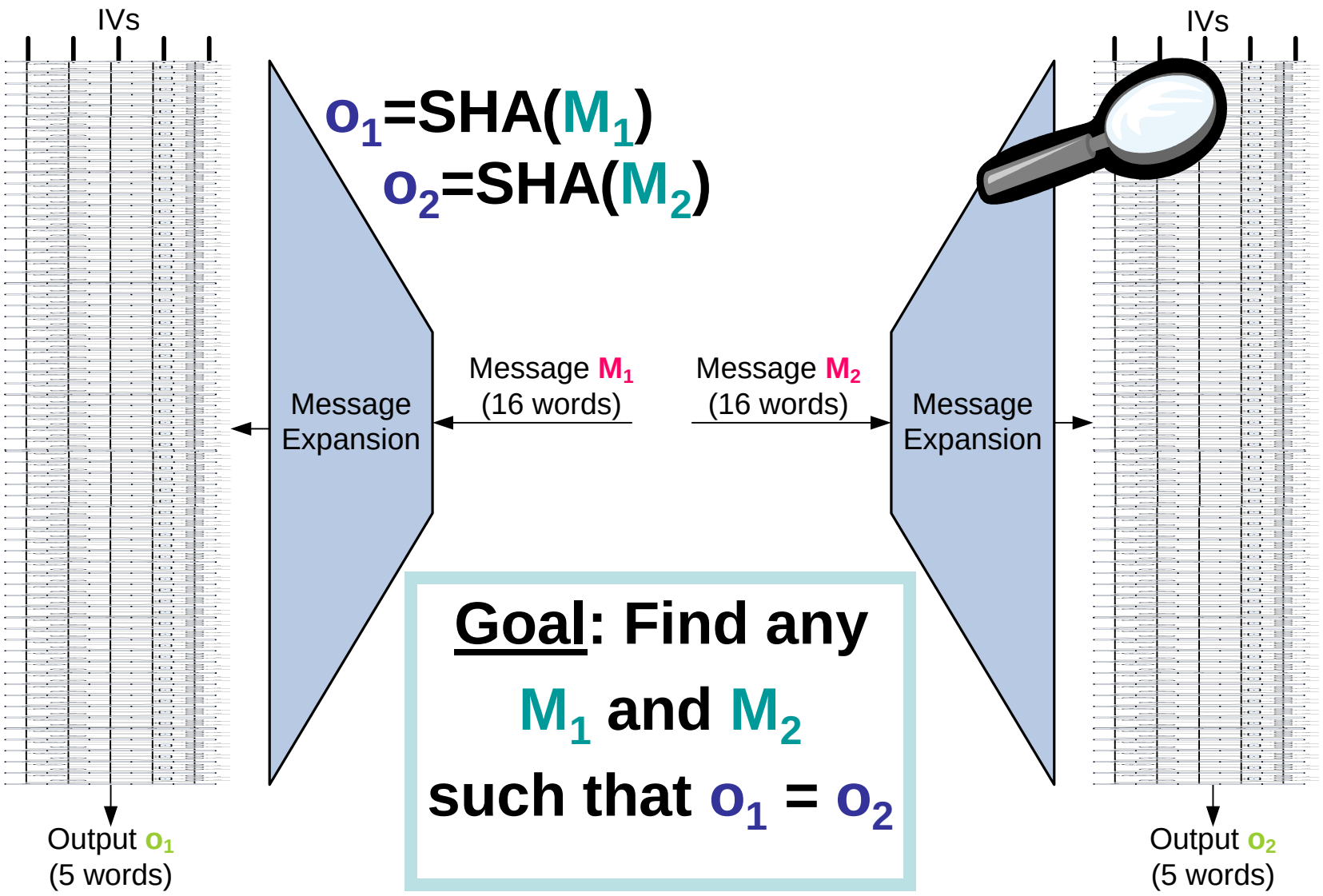


SHA-2 members



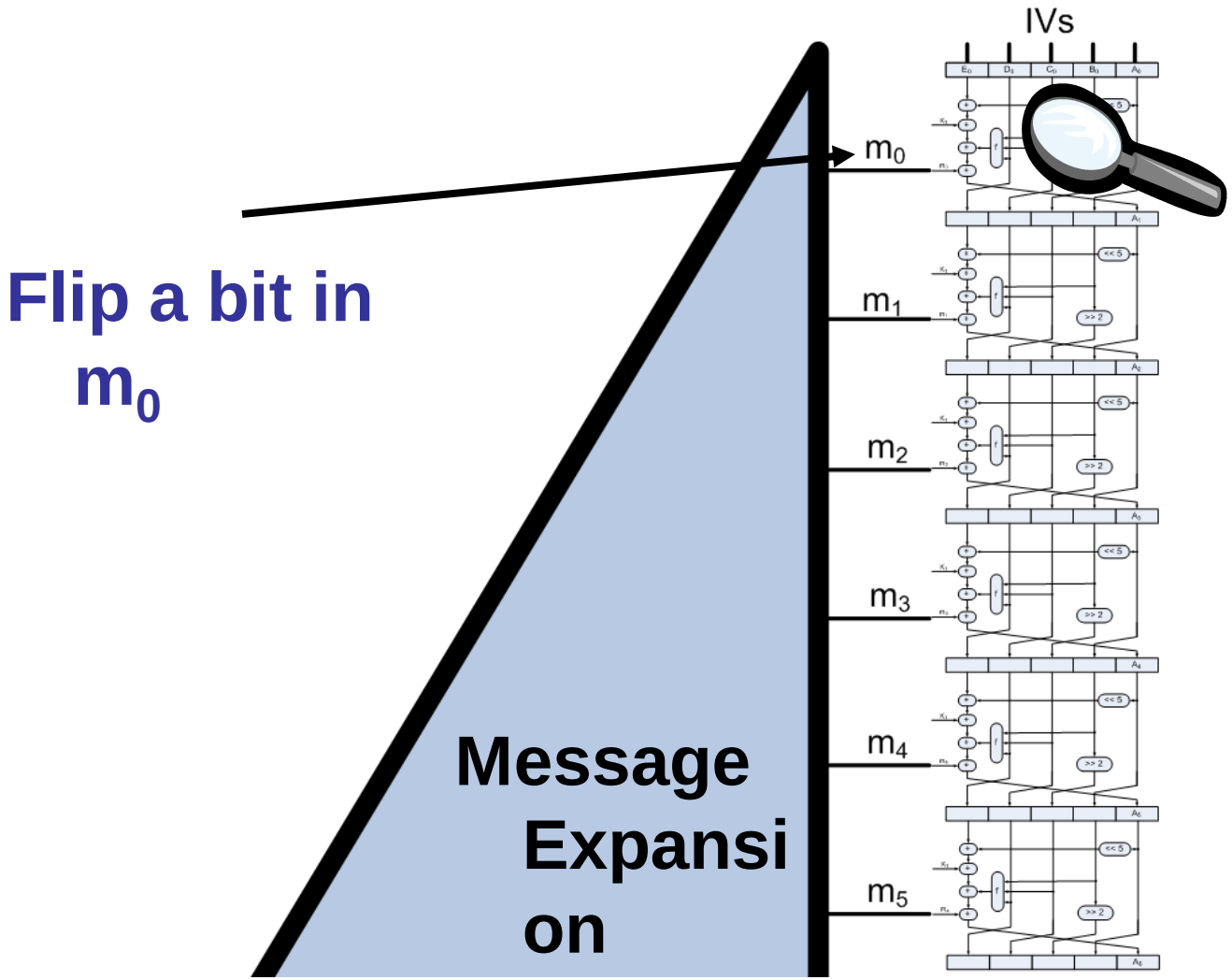
Design Complexity

How to produce a collision?

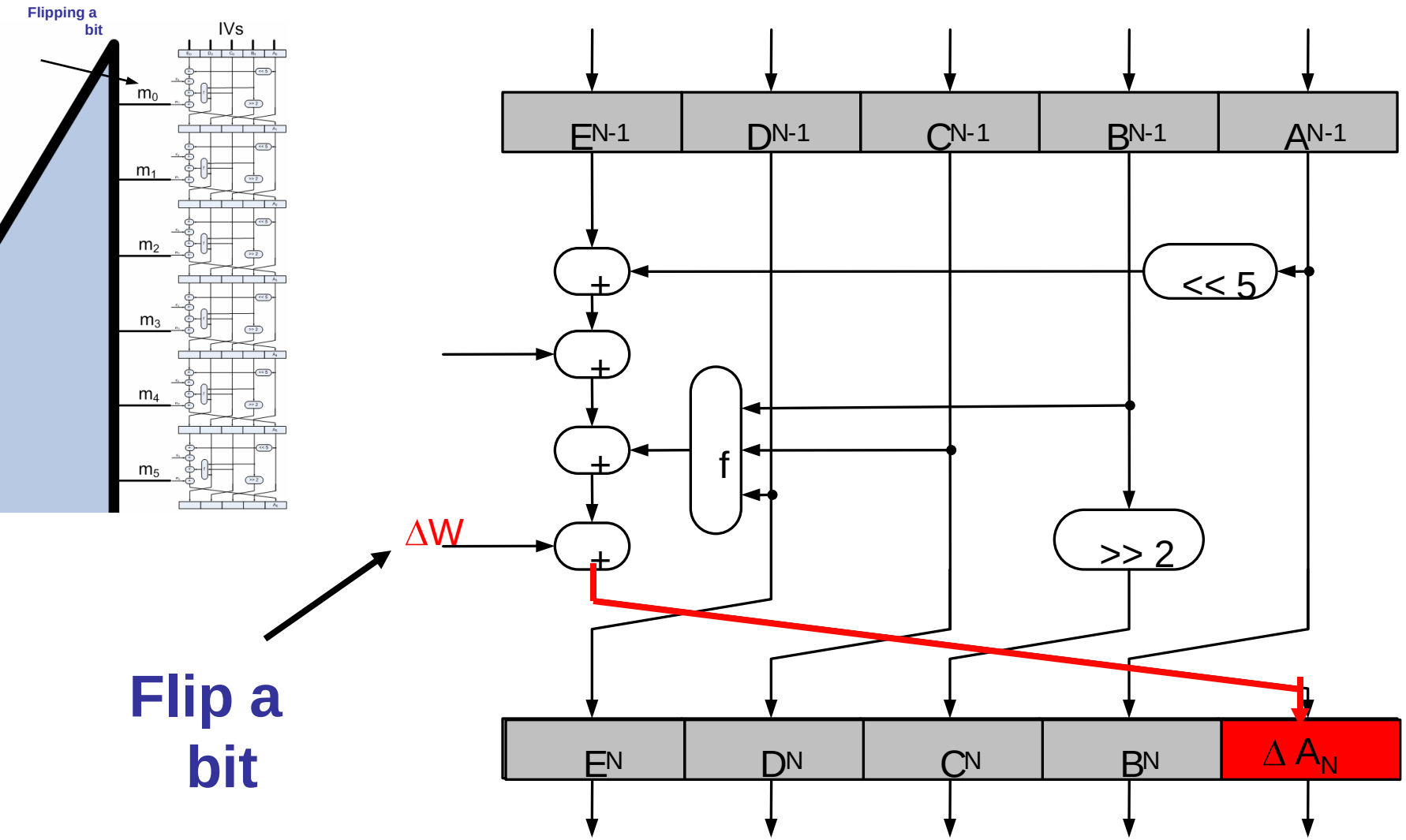


Goal: Find any M_1 and M_2 such that $o_1 = o_2$

Propagation of a small difference

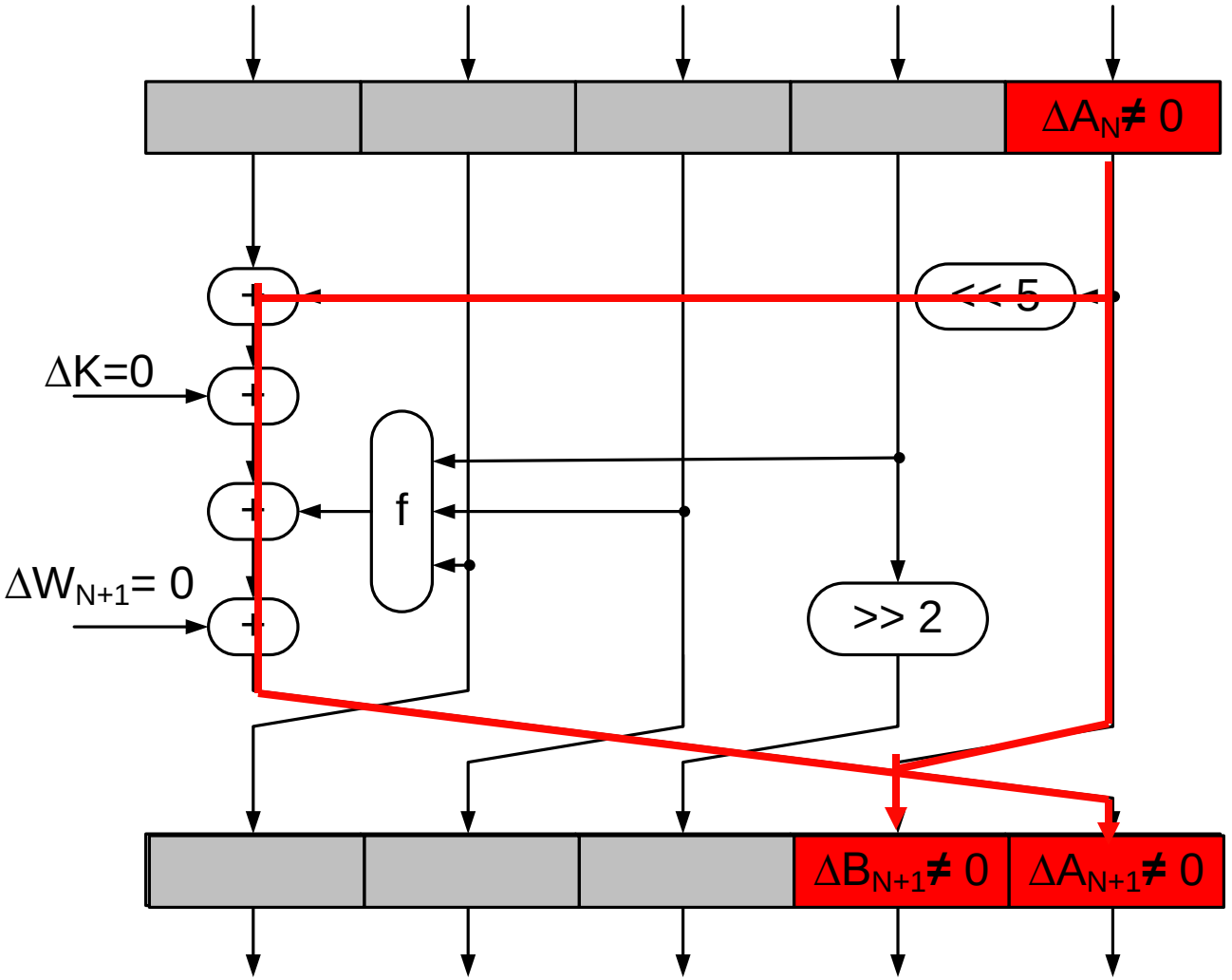


Propagation of a small difference



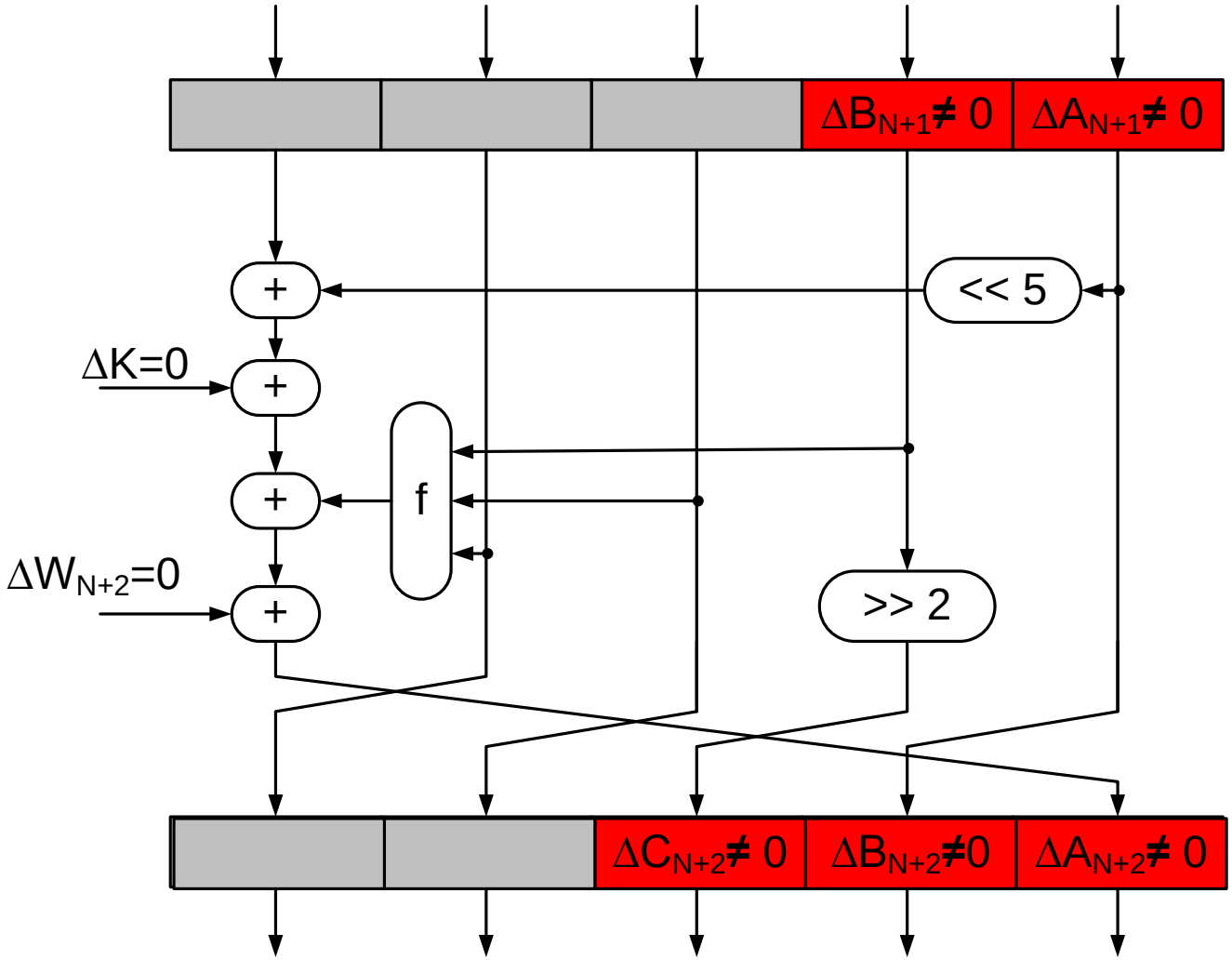
Propagation of a small difference

Step N+1

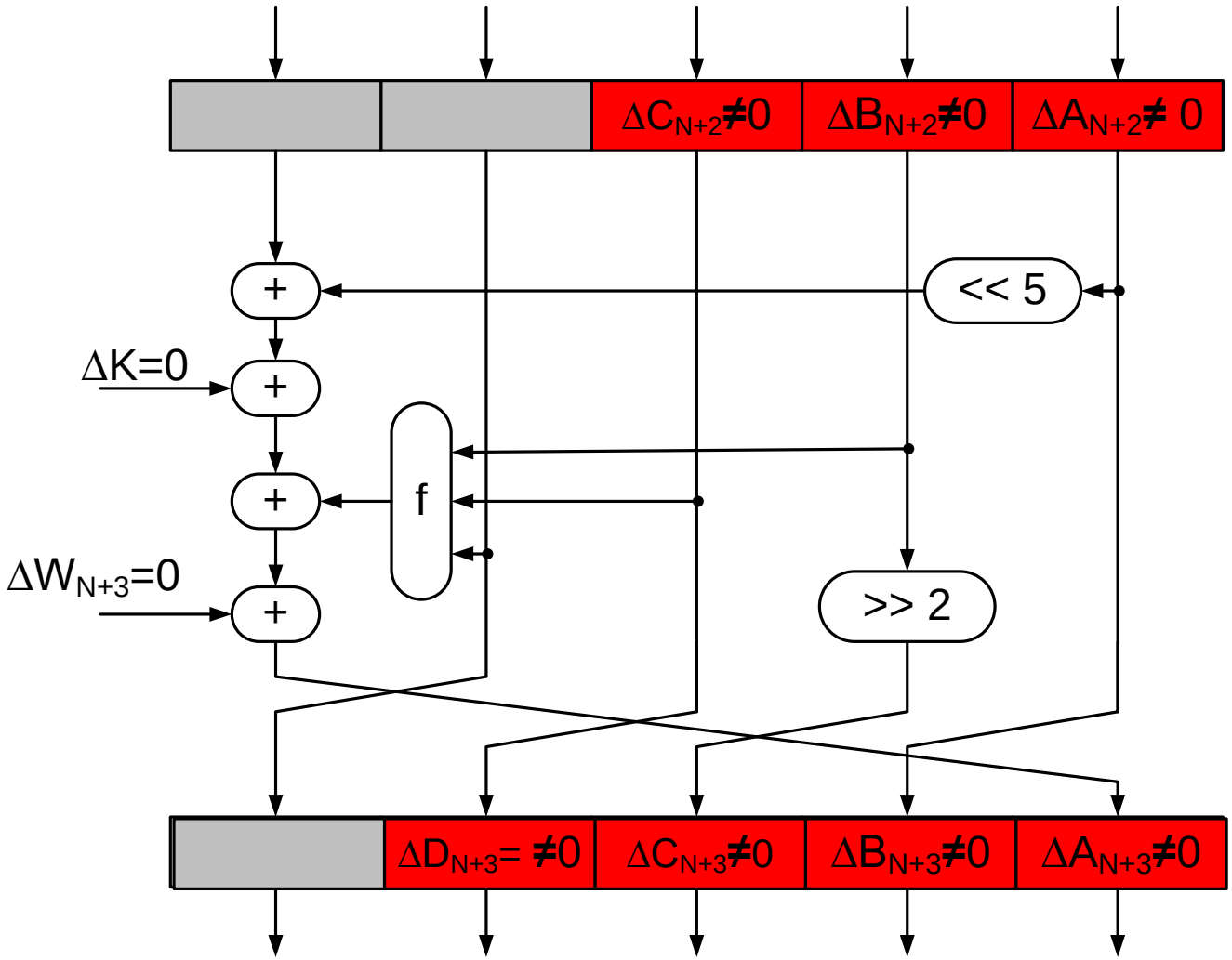


Propagation of a small difference

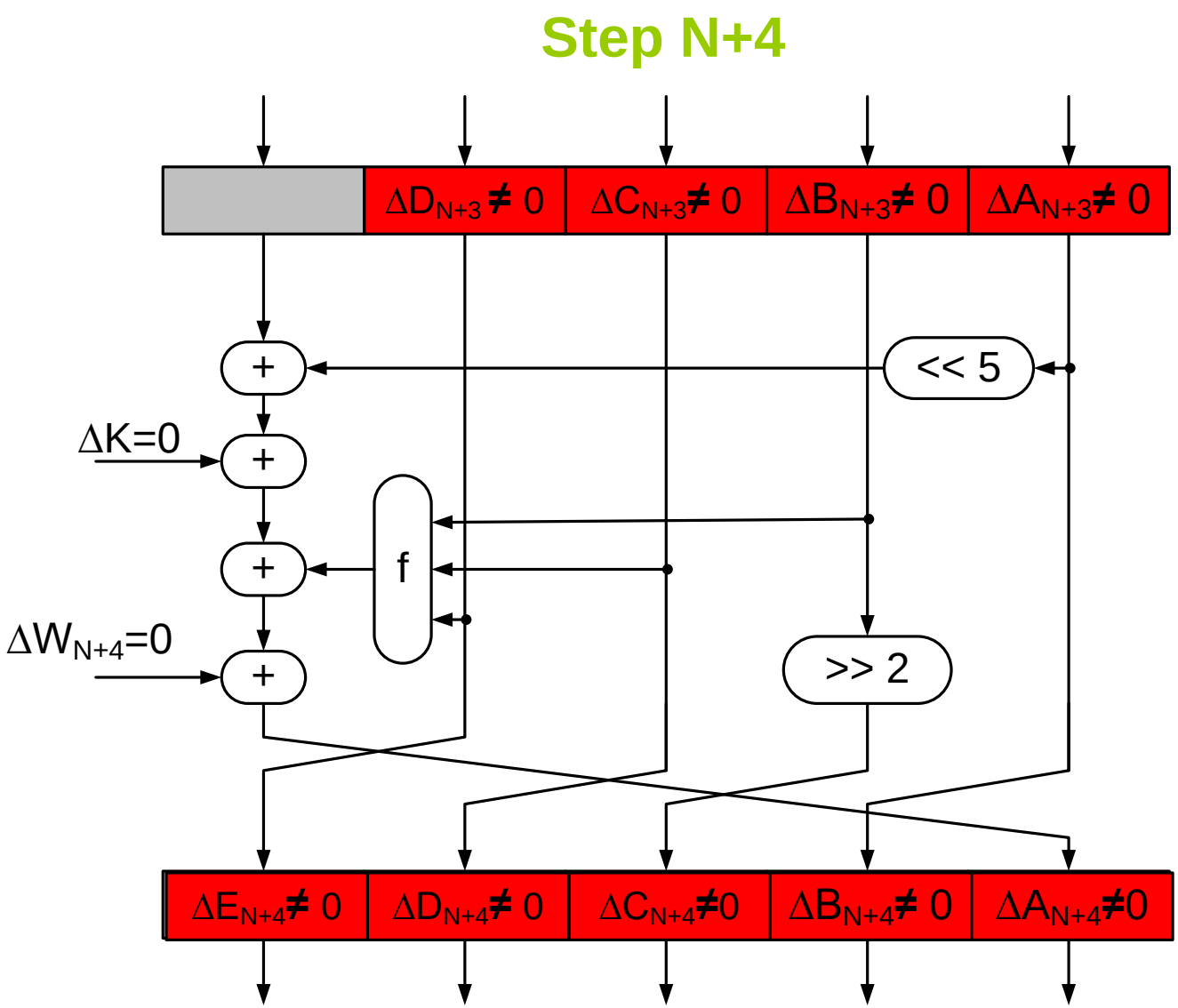
Step N+2



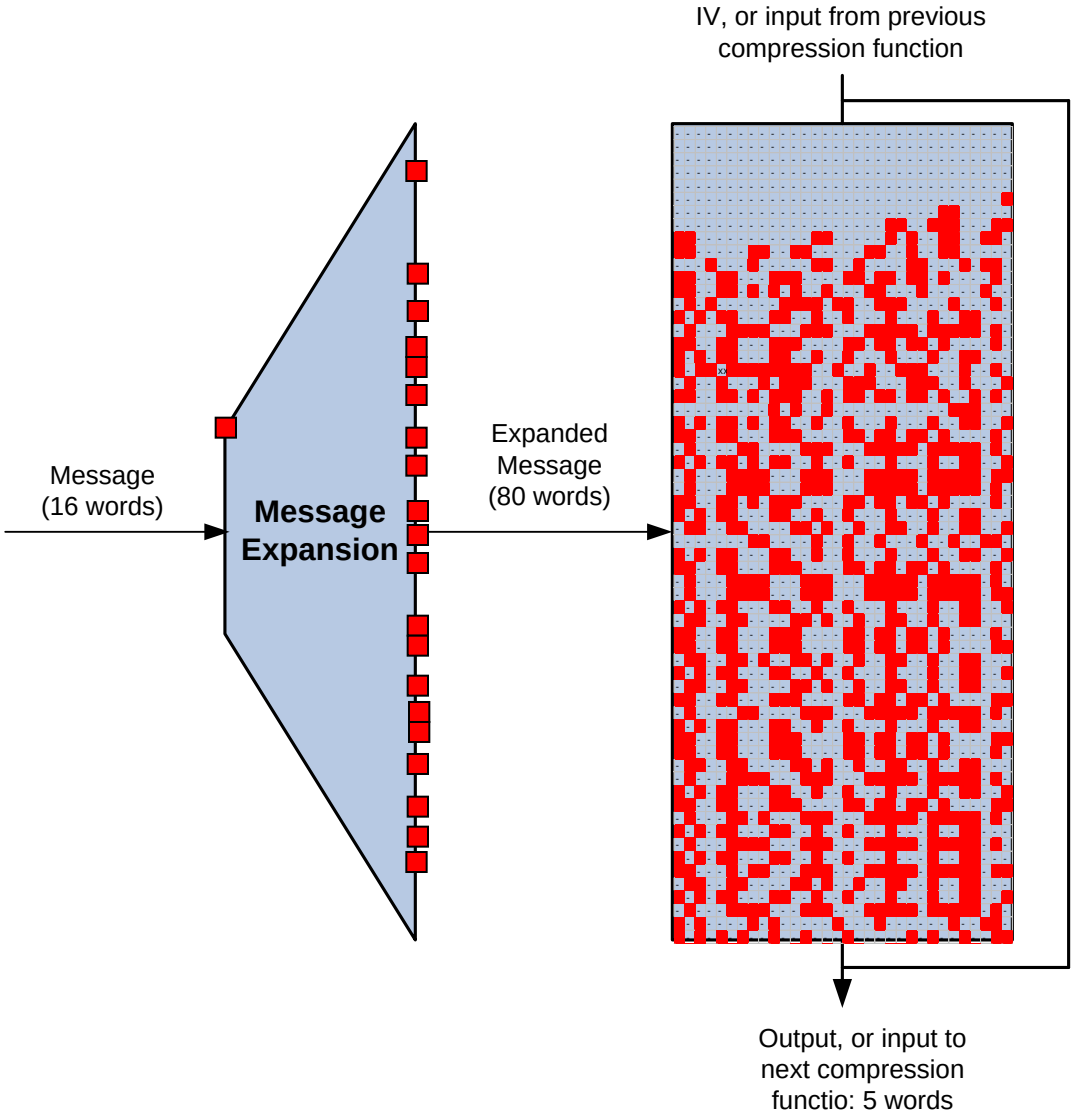
Propagation of a small difference



Propagation of a small difference



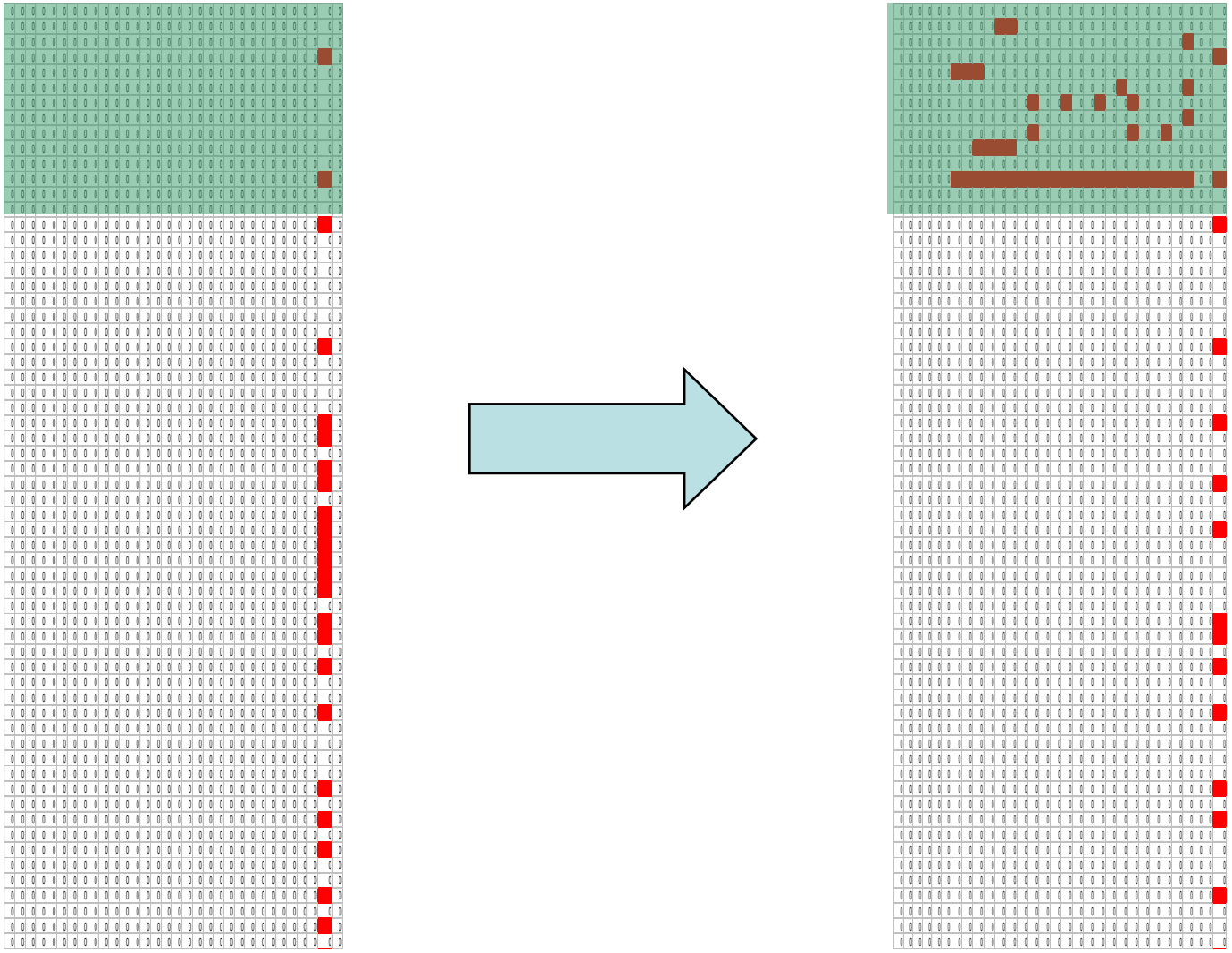
Effect of a single bit flip



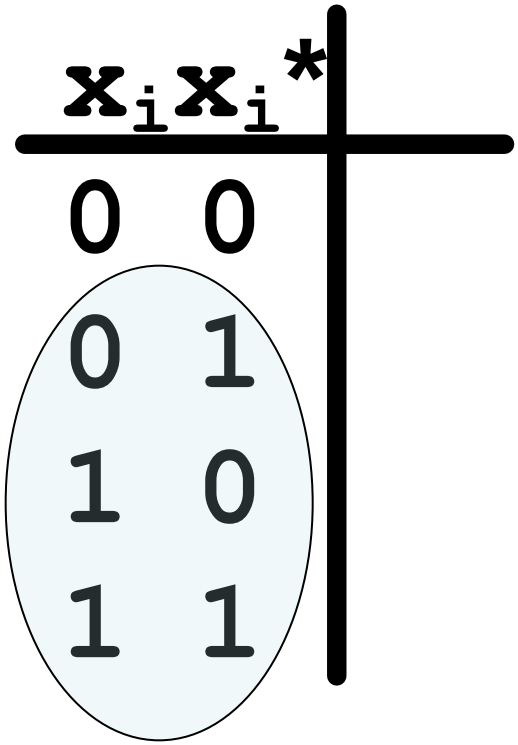
Differential attacks: ciphers vs. hash functions

- Good characteristics for block ciphers:
  - –Optimise probability
  - –Minimise number of chosen plaintexts
- Good characteristics for hash functions:
  - –Optimise probability
  - –Minimise effort to solve equations
  - –Equations in “first” steps are always easy
    - Only a small part of the message involved
    - Inputs are known
    - Late start / Early stop

Good characteristics



Generalized conditions



Type	Possibilities
XOR	2
Signed-bit	4-6

Generalized Conditions - Notation

(x_i, x_i^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
?	✓	✓	✓	✓
-	✓	-	-	✓
x	-	✓	✓	-
0	✓	-	-	-
u	-	✓	-	-
n	-	-	✓	-
1	-	-	-	✓
#	-	-	-	-

Generalized condition propagation

- First proposed in [DR06] for SHA-1 attacks
- SAT-solver-like Guess&Determine of generalized conditions to construct complex differential characteristics

Example

Real collisions for (reduced) SHA-1

40 rounds: Biham, Chen, 2005

58 rounds: Wang, Yu, Yin, 2005

64 rounds: De Cannière, R., 2006

70 rounds: De Cannière, Mendel, R., 2007

…

Full 80 rounds?

"recommend until 2010"

Real collisions for (reduced) SHA-1

40 rounds: Biham, Chen, 2005

58 rounds: Wang, Yu, Yin, 2005

64 rounds: De Cannière, R., 2006

70 rounds: De Cannière, Mendel, R., 2007

72 rounds: Cilardo et al., 2010

73-75 rounds: Grechnicov, 2010-2011

Full 80 rounds? No collision before 2011, NSA won

Ongoing work

- It took a while, but now people pick it up! E.g.
  - Best SHA-2 collision by Mendel/Nad/Schlaeffer (AC11, EC13)
  - Best Skein results: Leurent (AC12, Crypto13)
  - First RIPEMD-128 results by Landelle/Peyrin (EC13)

- How about non-ARX?
  - Look at Boura/Cannteaut from FSE13 for good starting point to express generalized conditions
  - Also, best/new results on Keccak (Eichlseder-Koelbl-Mendel-Schlaeffer)

Meet-in-the-middle / Biclique Attacks

Cryptanalysis 101

- Differential attacks
- Linear attacks

Cryptanalysis 101

- Differential attacks
- Linear attacks

- Why? Powerful, versatile, found many applications since early 90s
- Many variants
- Impact on cipher design: proofs against classes of those attacks are state-of-the-art

The simple setting

- Given: a block cipher
- Goal: find the single unknown key
- Cryptanalyst is allowed to choose plaintexts and ask for their ciphertexts (CPA) or vice versa

Brute-force:

guess all 2^k keys for success probability 1

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

MITM on 2-key 2-DES

Merkle-Hellman 81

MITM on 2-key 3-DES

Chaum-Evertse 85

6-7 rounds of DES

Hash functions

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Hash functions

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Hash functions

Lai-Massey 92

2nd-preimage on iterated constructions

Aoki-Sasaki et al. 08-10

Preimage for MD5, ...

Guo-R. et al. 10

Preimages for Tiger, ...

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

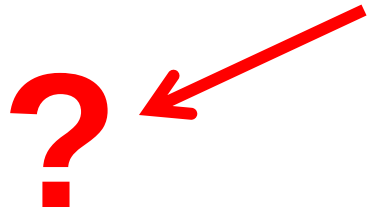
Chaum-Evertse 85

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10



MITM attacks on Symmetric Primitives

Block ciphers	**Hash functions**
Diffie-Hellman 77	
Merkle-Hellman 81	
Chaum-Evertse 85	
	Lai-Massey 92
Bogdanov-R. 10	Aoki-Sasaki et al. 08-10
KTANTAN Key-recovery	Guo-R. et al. 10
Wei-R. et al. 11	
Improved KTANTAN Key-recovery	

MITM attacks on Symmetric Primitives

Block ciphers	**Hash functions**
Diffie-Hellman 77	
Merkle-Hellman 81	
Chaum-Evertse 85	
	Lai-Massey 92
Bogdanov-R. 10	Aoki-Sasaki et al. 08-10
Wei-R. et al. 11	Guo-R. et al. 10

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

Improvements with „Biclique“ view: SHA-2,

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Hash functions

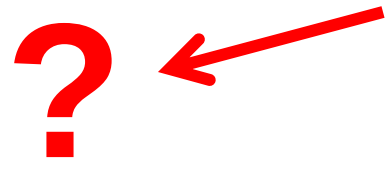
Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

Improvements with „Biclique“ view: SHA-2,



MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Bogdanov-Khovratovich-R.

New AES Results

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

Improvements with „Biclique“ view: SHA-2,

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Bogdanov-Khovratovich-R.

Khovratovich-Leurent-R.

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

Improvements with „Biclique“ view: SHA-2,

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Bogdanov-Khovratovich-R.

Khovratovich-Leurent-R.

Hash functions

Lai-Massey 92

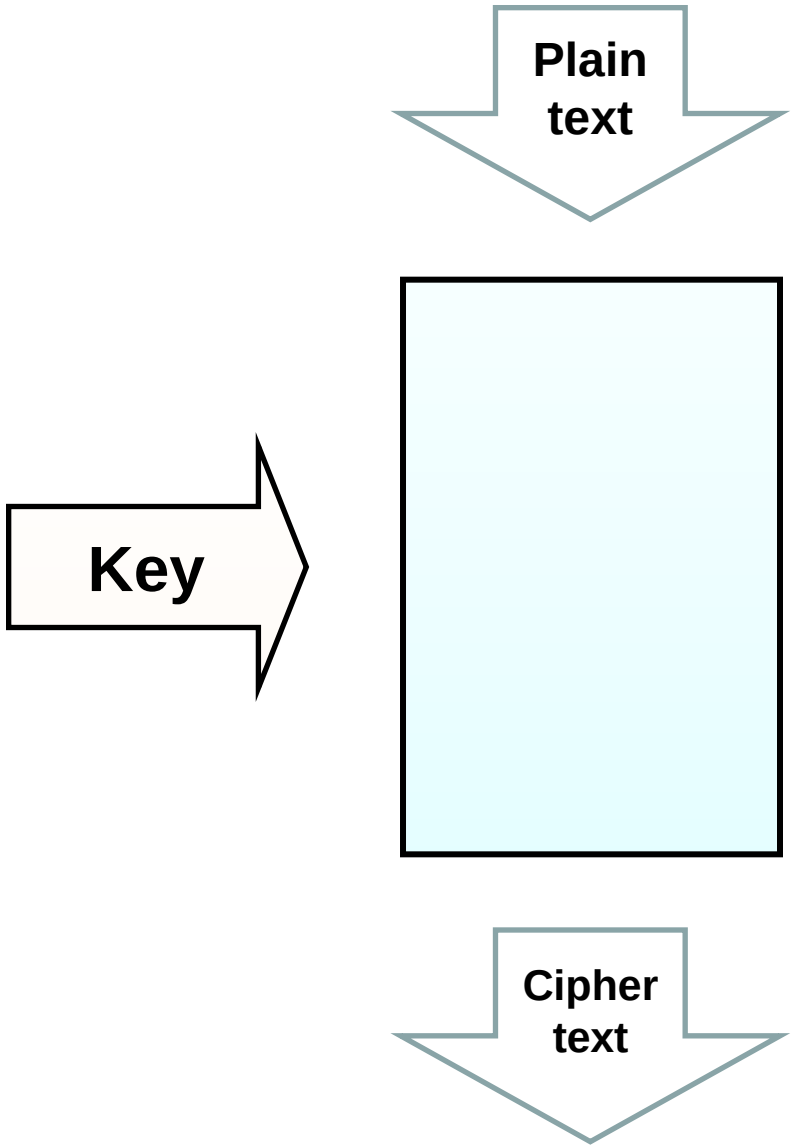
Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

Improvements with „Biclique“ view: SHA-2,

What is a secure block cipher?



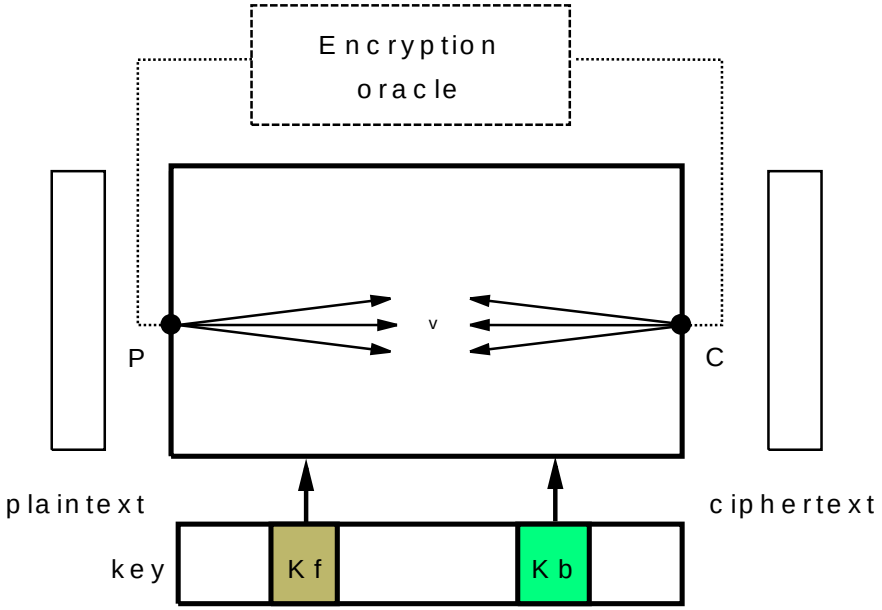
"**Secure**" if

1) Knowledge of a set of plaintext/ciphertext pairs does not allow to deduce new plaintext/ciphertext pairs

2) Finding a key requires testing all keys

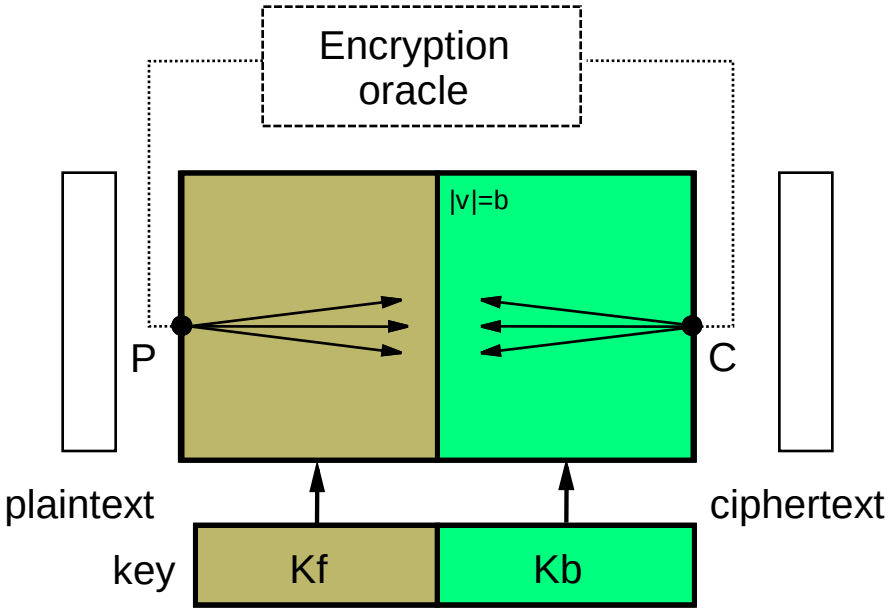
MITM

- Overshadowed by differential and linear attacks in recent 20+ years



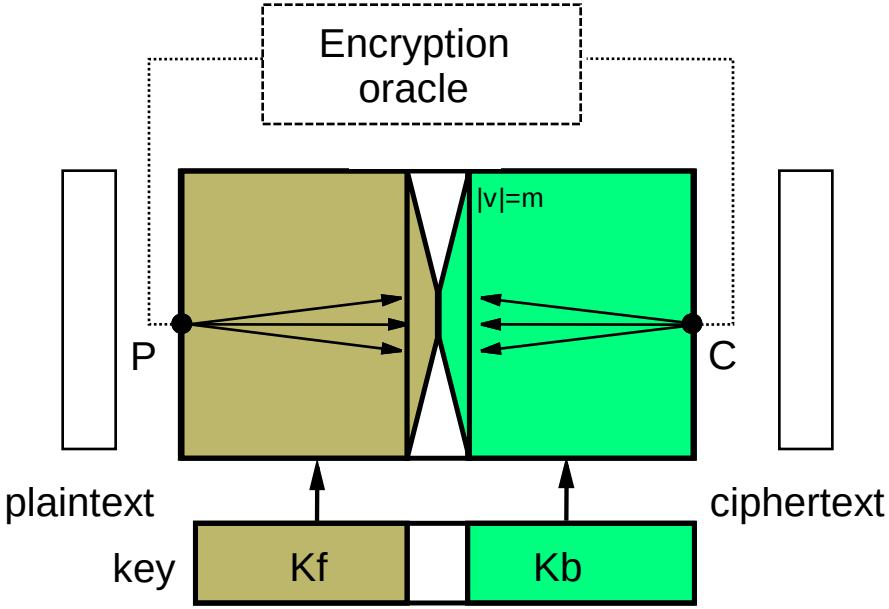
- Changing since attack on lightweight cipher KTANTAN (2010 and later), after progress in hash cryptanalysis

Basic MITM



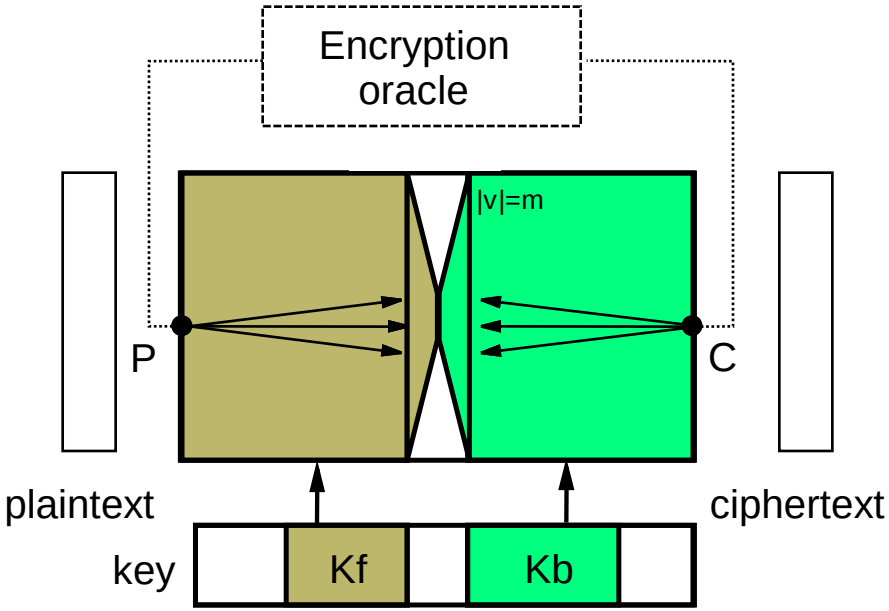
- Guess K_f and K_b independently
- Compute forwards from x
- Compute backwards from y
- Matching at full state b
- Complexity: $2^{|Kf|}+2^{|Kb|}+2^{|K-b|}$ computations

Partial Matching MITM



- Guess K_f and K_b independently
- Compute forwards from x
- Compute backwards from y
- Matching at part of state m
- Complexity: $2^{|Kf|}+2^{|Kb|}+2^{|K-m|}$ computations

Intersecting key-space case



- 3 keyspaces:
  - A_1(K_f only), A_2 (K_b only)
  - A_0 (both in K_f and K_b)
- Guess A_0, then A_1 and A_2 independently
- Complexity: $2^{|A0|}*(2^{|A1|}+2^{|A2|})+2^{|K-m|}$

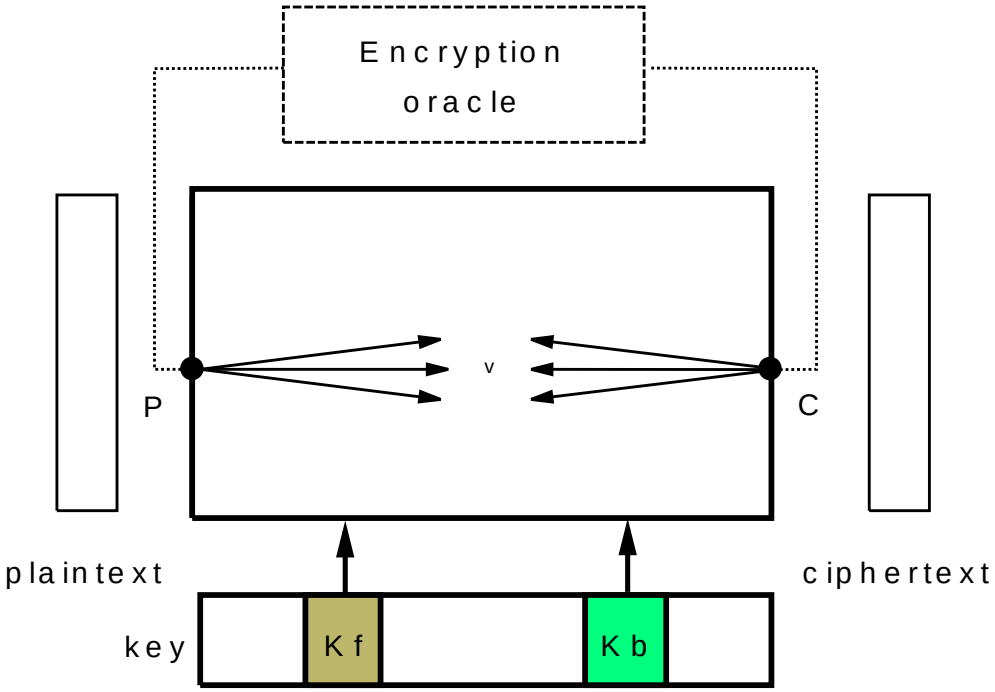
Examples in earlier literature

- $A_0=\{\}$, $|A_1|=|A_2|$
  - Diffie-Hellman 77 (2-key DES)
  - Merkle-Hellman 81 (3-key DES) (+splice&cut)
- $|A_0|$= large, $A_1=A_2$
  - Chaum-Evertse 85: 6-7 rounds DES
  - Mouha et al., 2011, 3x rounds XTEA
  - Gautham et al., 2011, 2x rounds GOST
- Distinct A_0, A_1, A_2
  - Bogdanov-R., 2010, full KTANTAN
  - Wei-R.et al., full KTANTAN (+splice&cut)
  - Isobe, 2011, full GOST (+fixed points)
- Some other MITM approaches that do not fit in this framework
  - Dunkelman-Sakar-Preneel, 7-round DES, 2007
  - Demirci-Selcuc et al, reduced AES and IDEA, 2003-2009
  - Bouillaguet-Derbez-Foque-Jean, reduced-round AES, 2011-2013

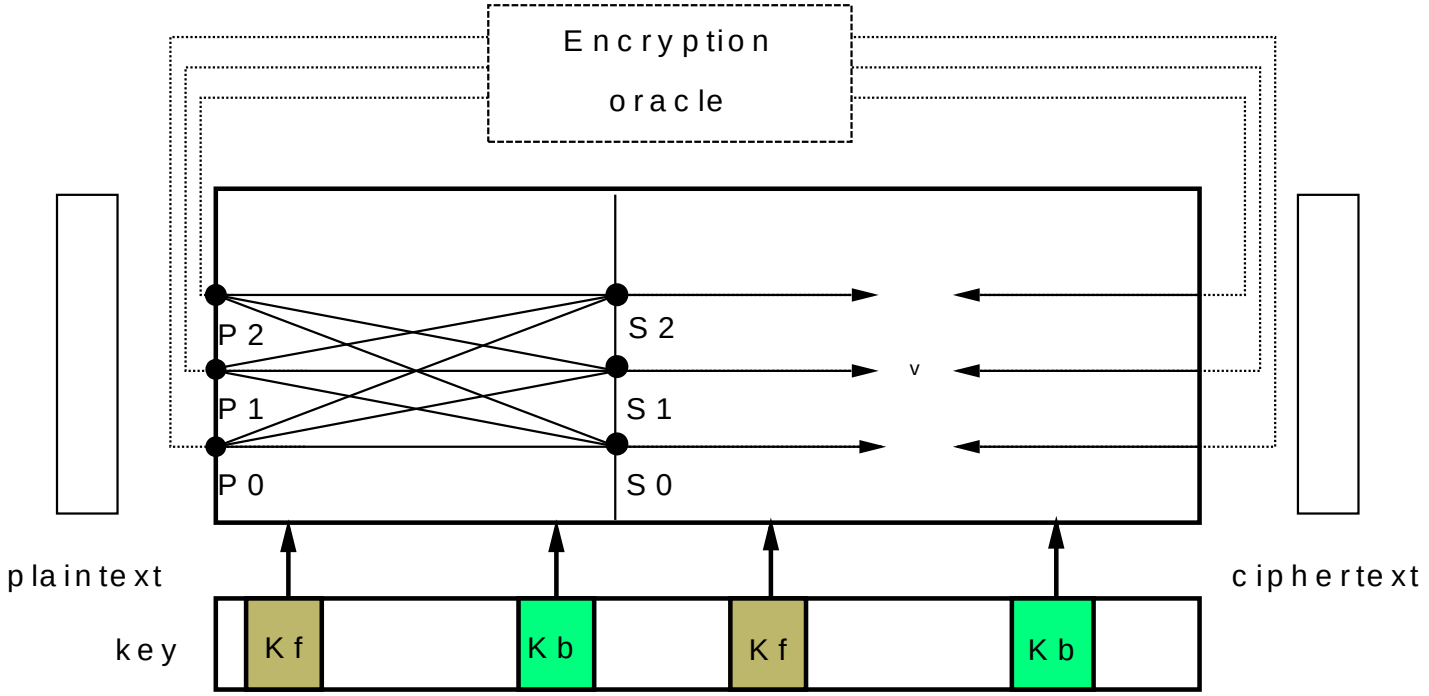
The Biclique approach

- Formalization of „Initial structure“ concept due to Aoki-Sasaki 09
- Mapping to differential framework possible and intuitive
  - Differential characteristics/trails
  - Neutral bits
  - Rebound techniques
- Results
  - on more rounds possible
  - better time/memory complexities possible

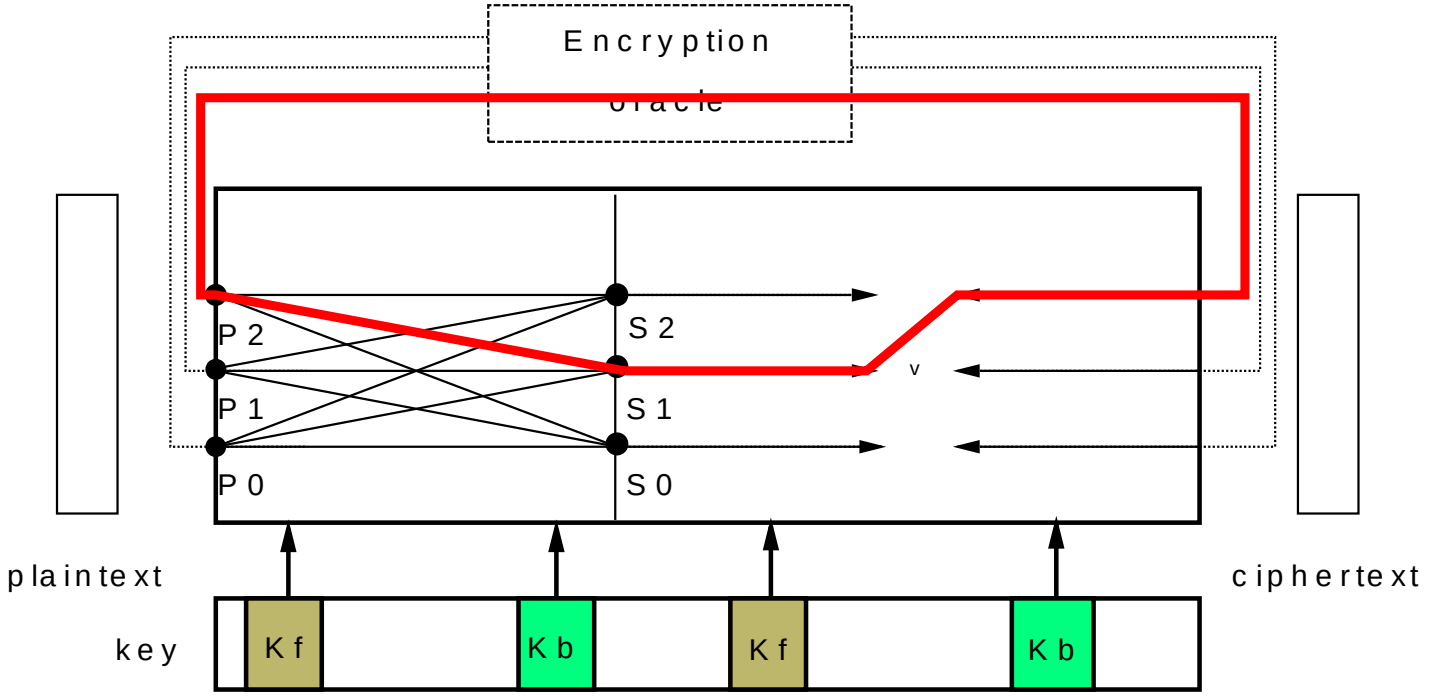
Biclique approach to MITM



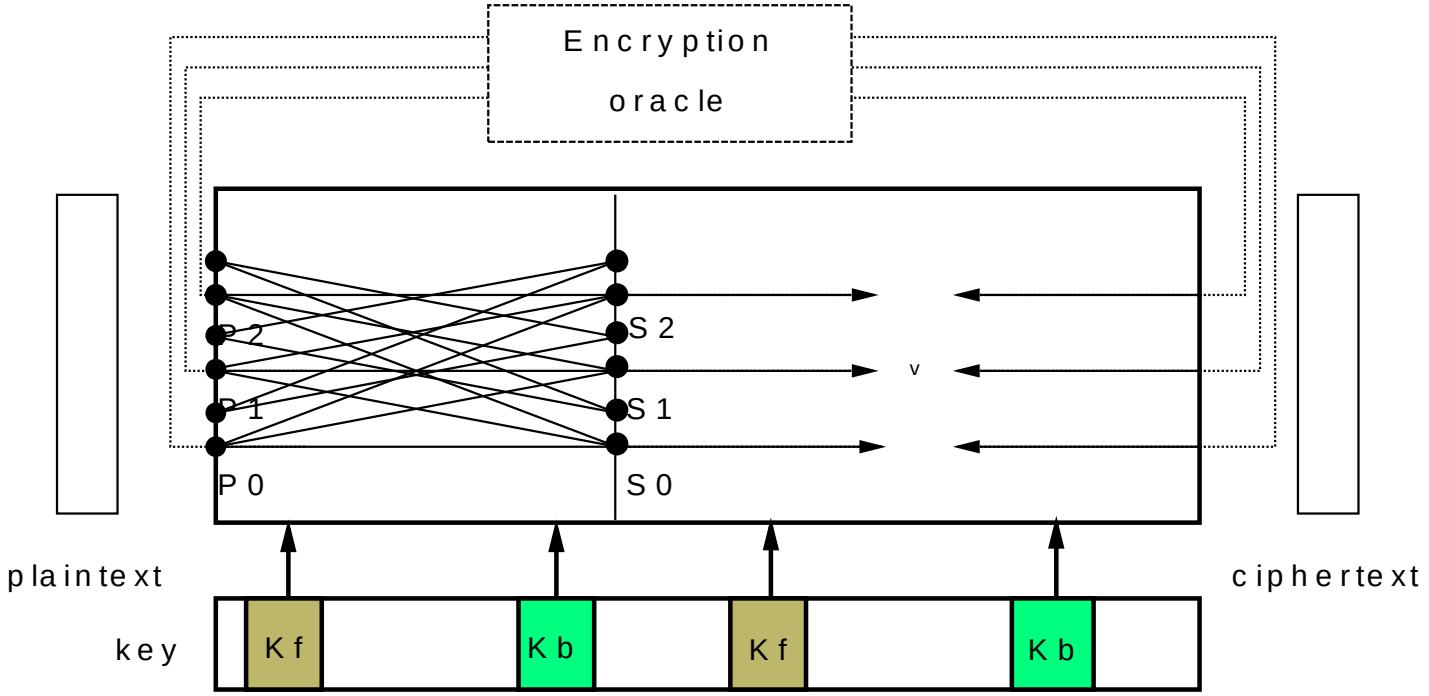
Biclique approach to MITM



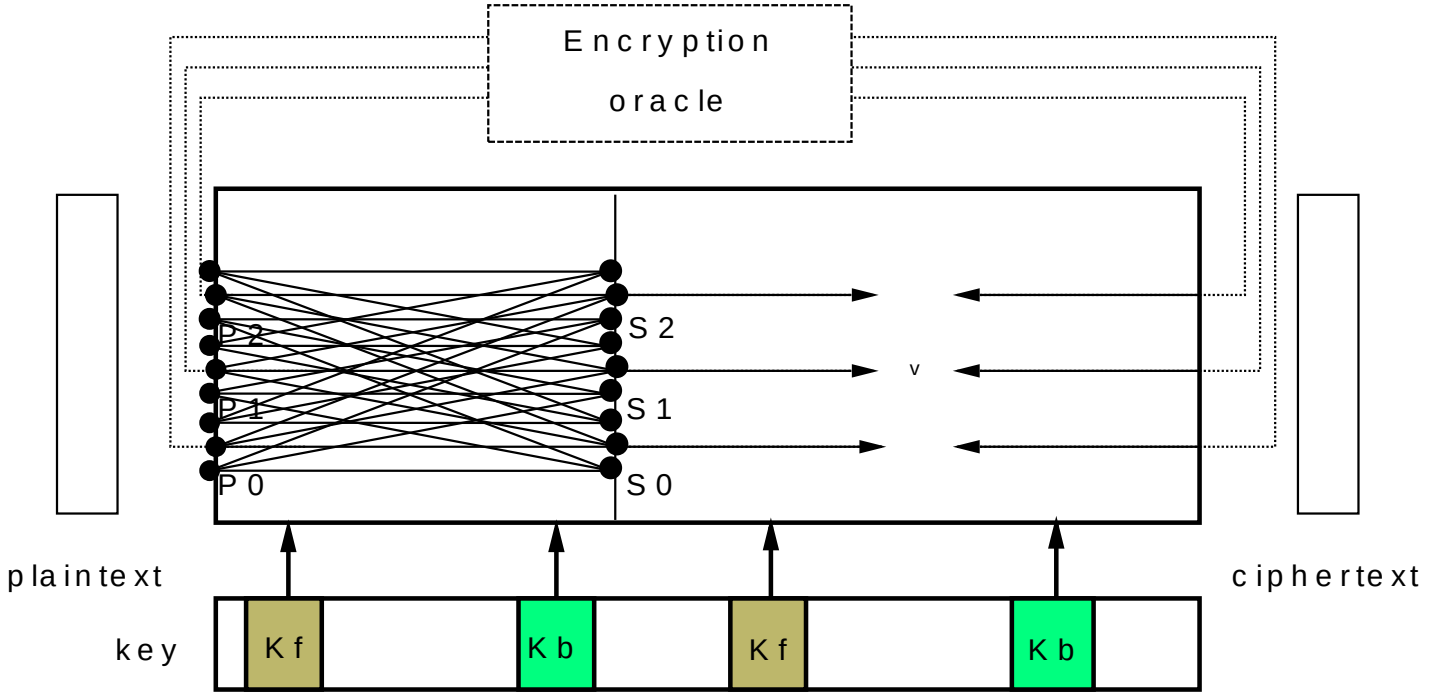
Biclique approach to MITM



Biclique approach to MITM

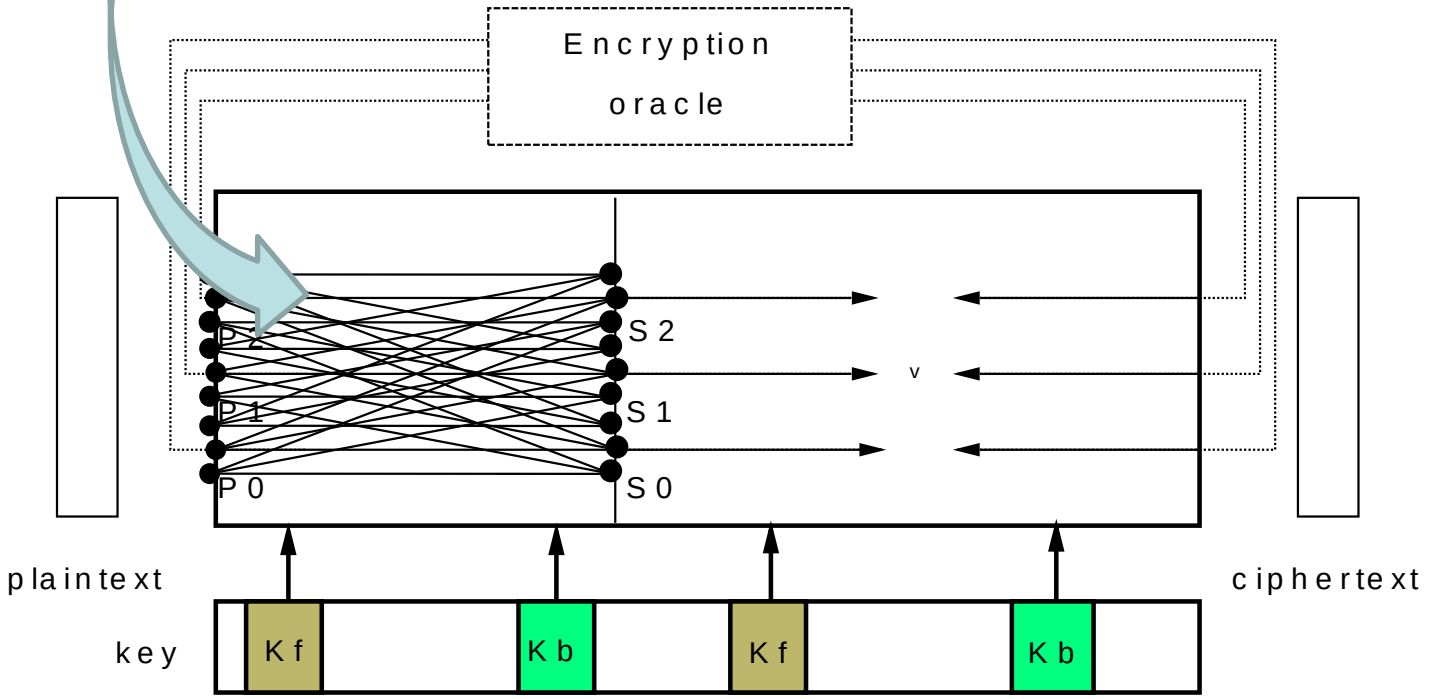


Biclique approach to MITM



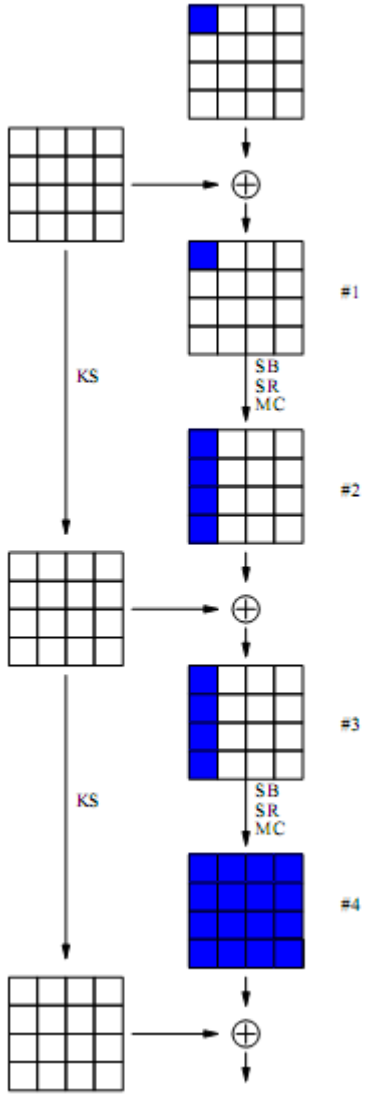
Biclique approach to MITM

- Use simple diffusion properties
- Rebound attack techniques
- Dedicated techniques

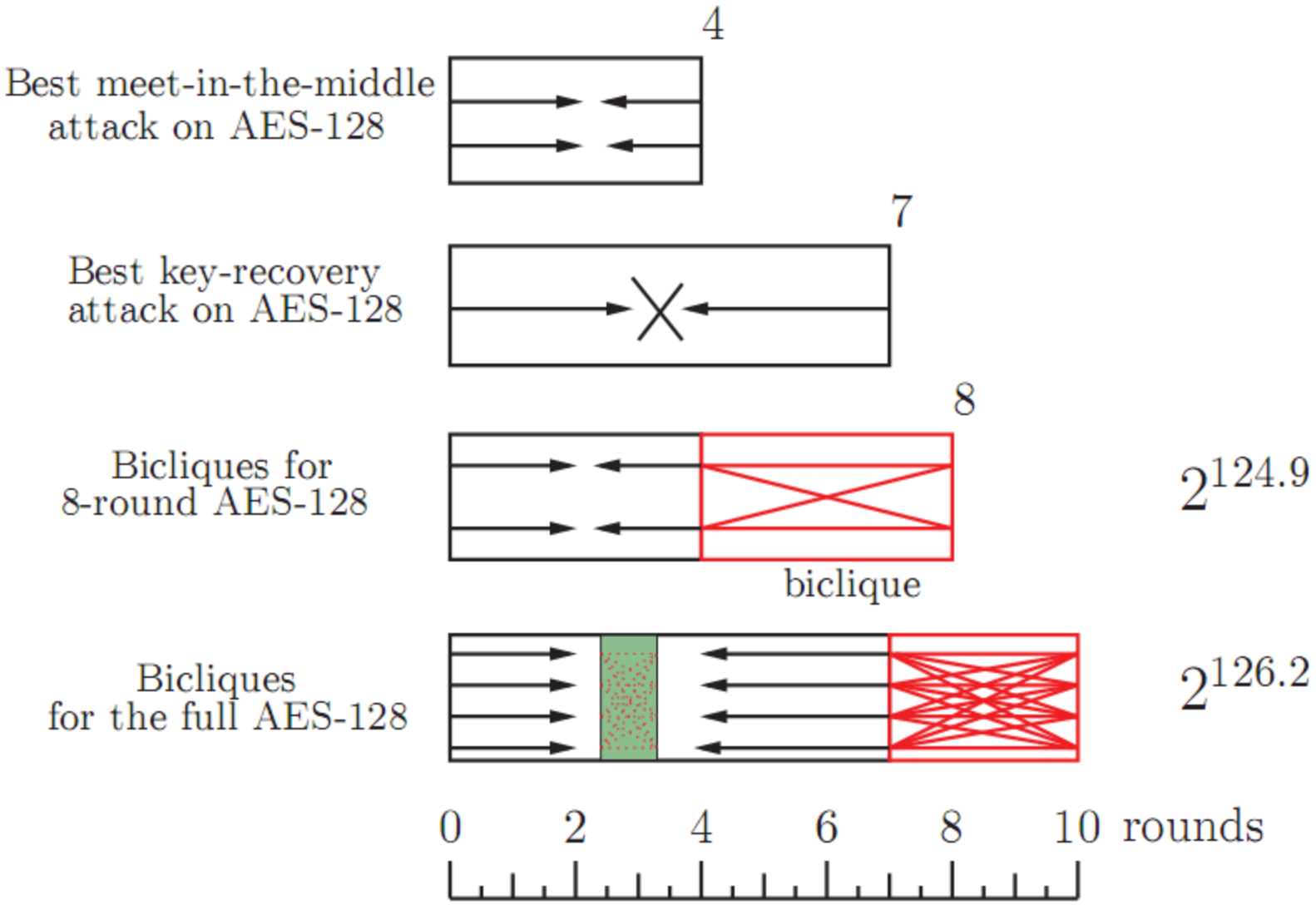


Security arguments for AES

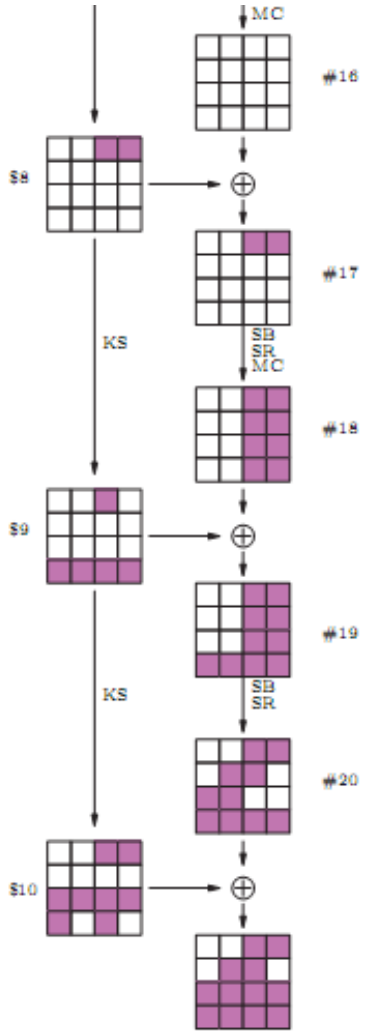
- Resistant against differential and linear attacks
  - Theorem: any 4-round trail has a least 25 active S-boxes
- Simple, clean and elegant



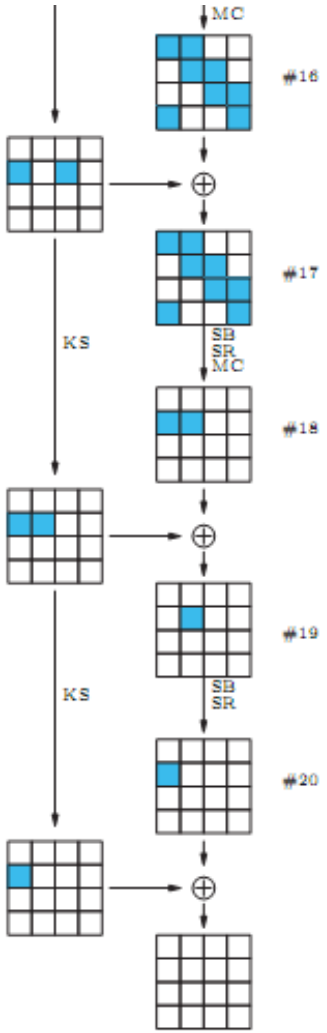
New key recovery for AES-128



2^8 dimension biclique for AES-128

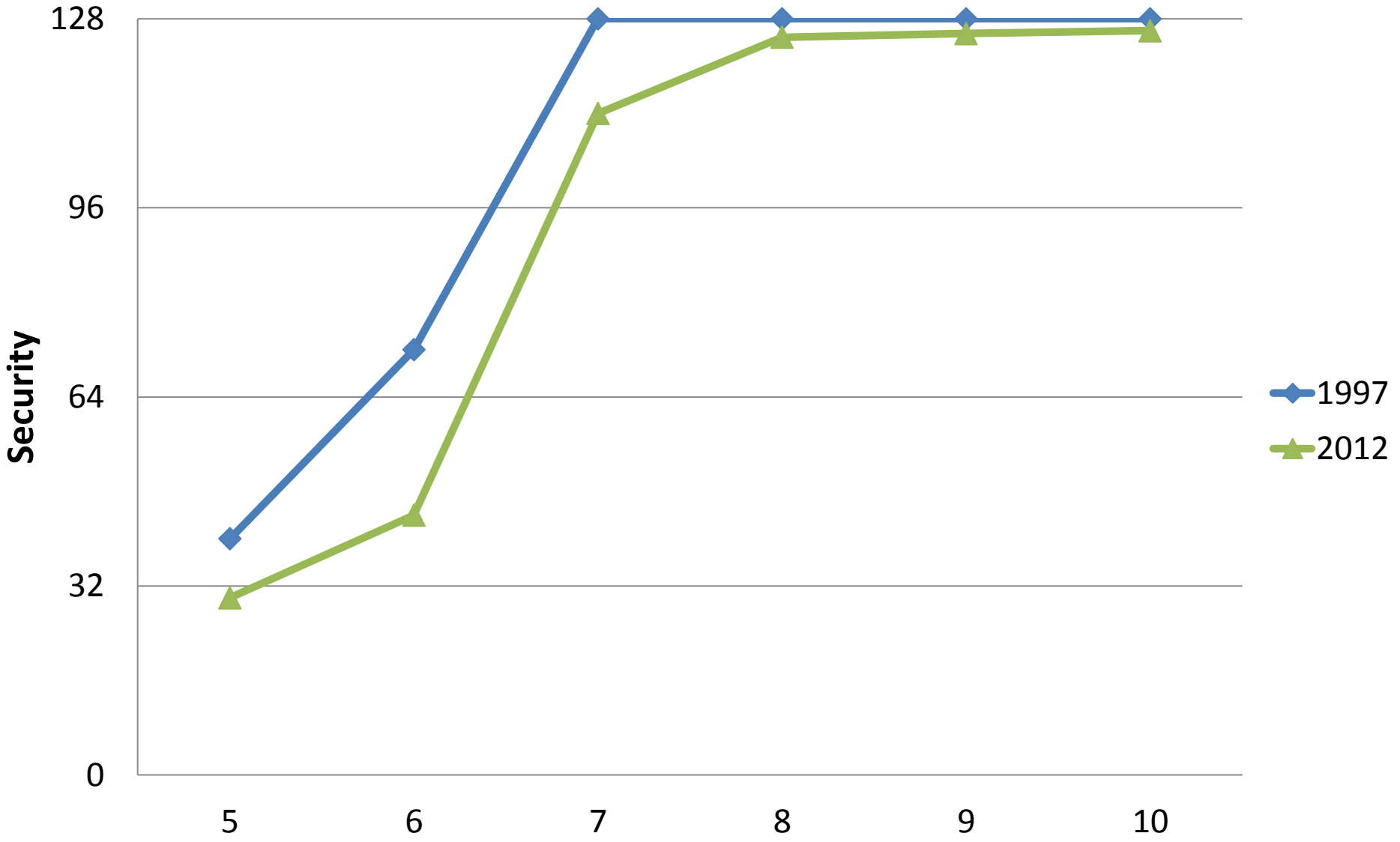


Biclique
Δ-differential

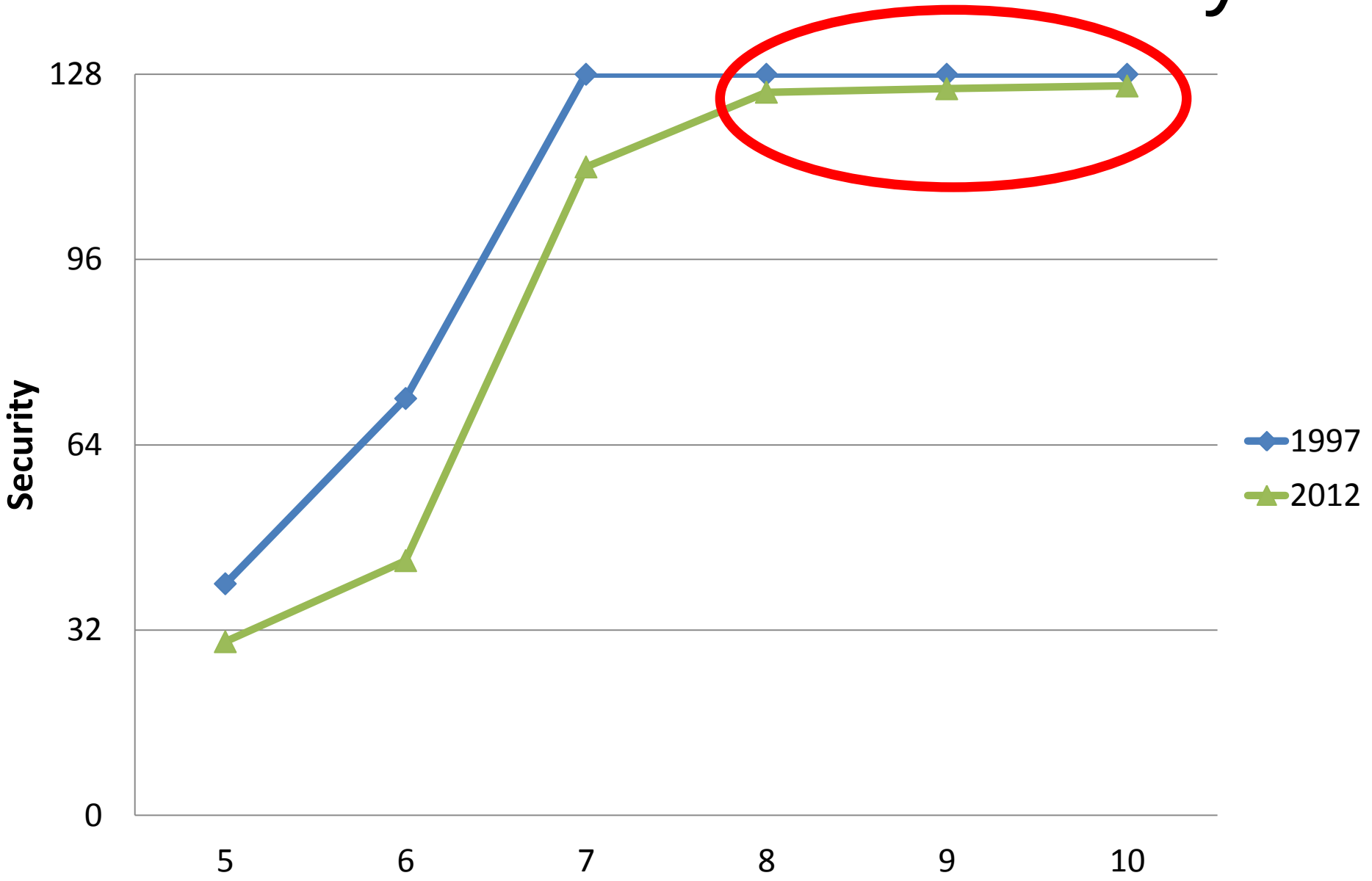


Biclique
∇-differential

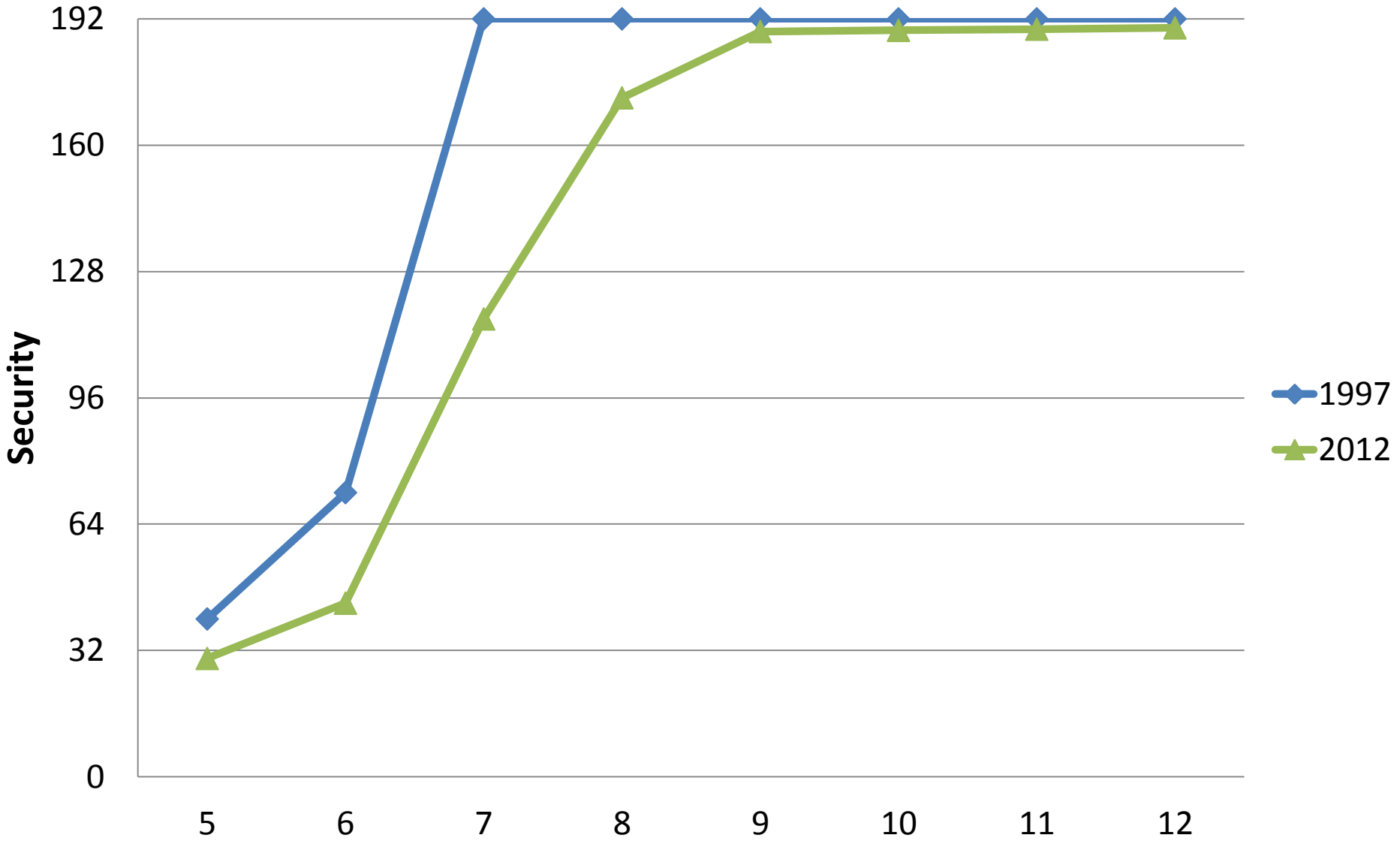
Evolution of AES-128 security



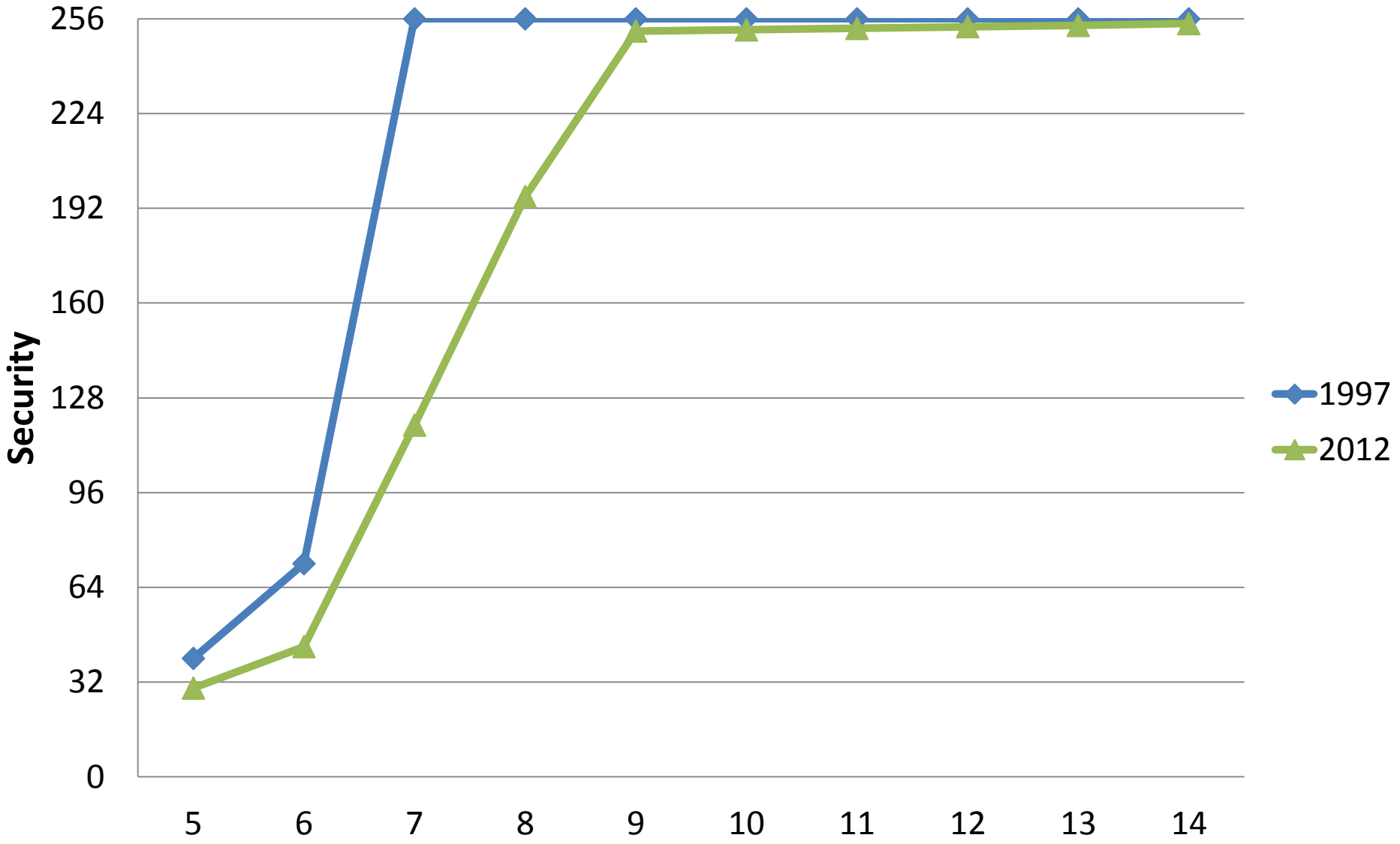
Evolution of AES-128 security



Evolution of AES-192 security



Evolution of AES-256 security



Conclusion on biclique idea

- Came from hash cryptanalysis
- Generic extension of MITM attacks
- **Can** give cryptanalytic results for more rounds than other techniques
- Biclique attacks **can** be million times faster than brute-force (see 5-round IDEA)

- Lesson learned: Expecting ideal behavior from a practical cipher can be too optimistic