Attacks on Advanced Encryption Standard: Results and Perspectives

Dmitry Khovratovich

Microsoft Research

29 February 2012

Advanced Encryption Standard

AES

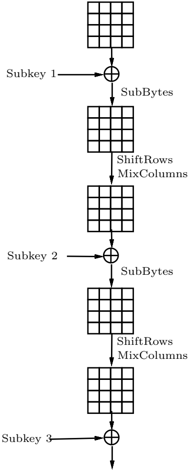
Algorithm

- Designed as *Rijndael* in 1997 by Daemen and Rijmen.
- 128/192/256-bit key.
- 10/12/14 rounds.

When selected as AES:

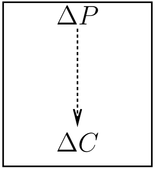
- Best practical attacks: 6 rounds.
- Best shortcut attack: 7 rounds.

2 rounds of AES:



Older methods

Probabilistic property:



Right pairs yield information about internal variables and hence the key.

Differential cryptanalysis (1990):

- Attack on DES with 2^{47} data.
- Many other ciphers broken.

Linear cryptanalysis (1993):

- Attack on DES in 2^{43} time.
- Verified but impractical.

Both properties activate few non-linear components with reasonably high total probability.

Wide trail design

AES was designed to withstand contemporary cryptanalysis:

- Lower bound on the number of active non-linear components;
- Upper bound on the probability of each active element;
- Differential and linear properties are worthless after 4 rounds.

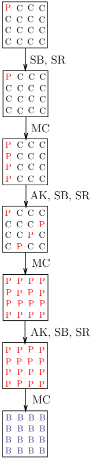
New attacks

Square (1997)

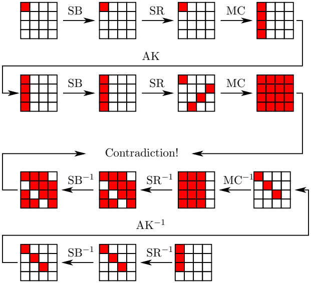
- Consider 256 plaintexts that vary in a single byte (P).
- This property preserves for two rounds (all bytes are P).
- The sum in every byte is zero after three rounds.

Was the most promising one, but:

- The main property has been extended by one round only (AES-128).
- Initial rounds are treated only a bit better.
- AES-128 reduced by 30% can be attacked.



Impossible differential (1998)



- Two deterministic properties meet each other.
- Transition in the middle is impossible.
- Limited by the length of deterministic properties.

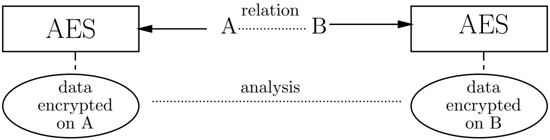
Related-key attacks

As the progress in standard attacks halted, some started to think that AES may serve as a universal primitive...

As the progress in standard attacks halted, some started to think that AES may serve as a universal primitive...

This proved to be wrong.

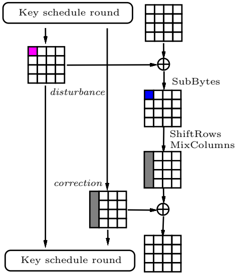
Related-key attacks



- Consider the difference between encryptions on unknown but related keys.
- Analyze the difference propagation.

Local collision in AES

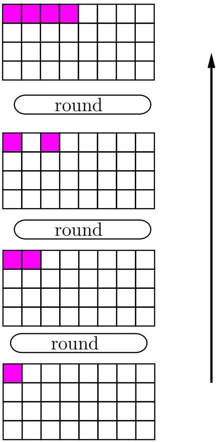
Main property exploited: local collision.



- Inject a difference in a key;
- Control the expansion;
- Cancel in the next injection.

Weak attacks

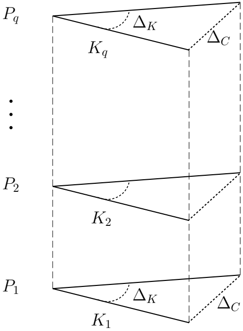
Slow diffusion in the key schedule



1. One-byte difference
2. Start from the last subkey
3. Every inverted round affects only one more byte.

Differential q-multicollision in AES

A set of q pairs (key, plaintext) that satisfy a modified trail.



Δ_K	0f070709 0e070709 0f070709 0e070709 371f1f21 00000000 371f1f21 00000000
Δ_{P_1}	a3**1f1f21 00000000** 19**1f1f21 00000000**
Δ_{P_2}	3a**1f1f21 00000000** db**1f1f21 00000000**
Δ_{P_3}	13**1f1f21 00000000** 7e**1f1f21 00000000**
Δ_{P_4}	fd**1f1f21 00000000** 06**1f1f21 00000000**
Δ_{P_5}	ab**1f1f21 00000000** db**1f1f21 00000000**
Δ_C	01000000 01000000 01000000 01000000

Boomerang attacks

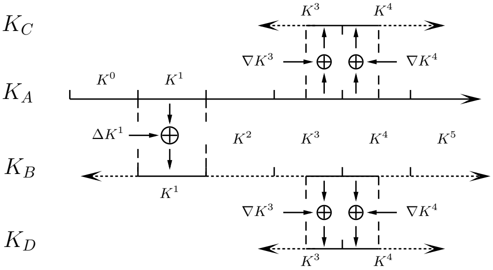
Related-key boomerang attack

First attack on the full AES-192/256:

1. Used the same idea as a distinguisher;
2. Encryption and decryption on four keys with the chosen relation;
3. Complexity 2^{100} and higher for the full key recovery.

Key relation

The key relation was quite controversial:

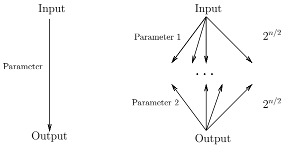


Similar relations are trivial, as every key can be recovered.

Meet-in-the-middle and bicliques

Basic

Basic meet-in-the-middle:

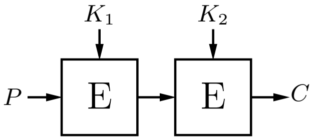


1. Target: find a parameter that converts input I to output O;
2. Split the parameter into two parts;
3. Compute all possible middle states;
4. Check for matching.

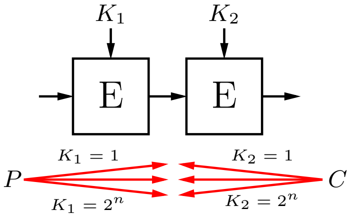
Complexity $2^{n/2}$.

Double-DES

Double-DES: 64-bit state, two 56-bit keys.



Cryptanalysis



- Obtain two plaintext/ciphertext pairs;
- Compute the middle state for 2^{56} first keys;
- Compute the middle state for 2^{56} second keys;
- Check for match.

Complexity 2^{56}.

Bicliques

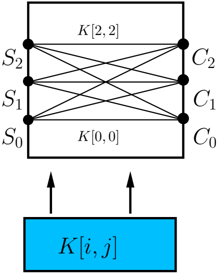
Biclique

Biclique of dimension d:

- 2^{2d} keys $K[i,j]$.
- 2^d states S_j;
- 2^d ciphertexts C_i.

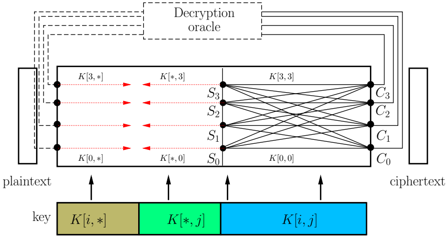
$$S_j \xrightarrow{K[i,j]} C_i.$$

Example with $d = 1.5$:



Attack

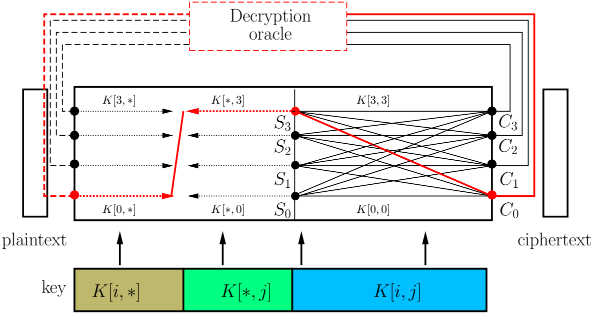
Suppose that the first part of the cipher can be splitted into tho parts using independent key bits:



1. Construct a biclique, fix states and ciphertexts;
2. Ask for decrypted ciphertexts;
3. Compute the matching state out of plaintexts;
4. Compute the matching state out of internal states;
5. Matching pair yields a candidate key.

Why it works

Suppose the key $K[0,3]$ is the right key.



$$S_j \xrightarrow{K[i,j]} C_i.$$

Attack parameters for AES-128

Dimension 1:

- Complexity $2^{n-\varepsilon}$;
- 5-round biclique;
- 3-round matching.

Attack parameters for AES-128

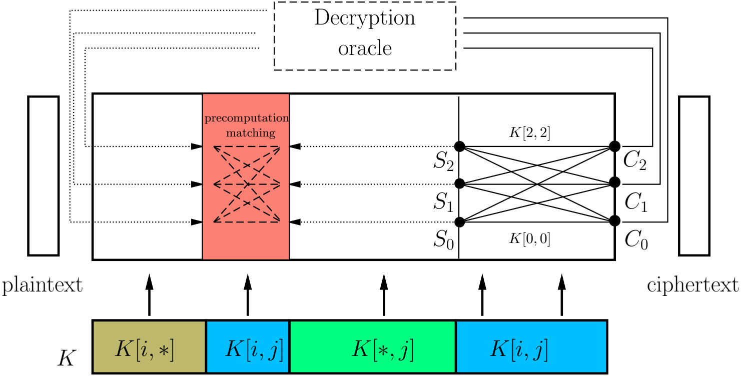
Dimension 1:

- Complexity $2^{n-\varepsilon}$;
- 5-round biclique;
- 3-round matching.

Dimension 8:

- Complexity 2^{n-8}.
- 3-round biclique;
- 3-round matching.

What is the overhead if we allow an exhaustive search in the matching part:



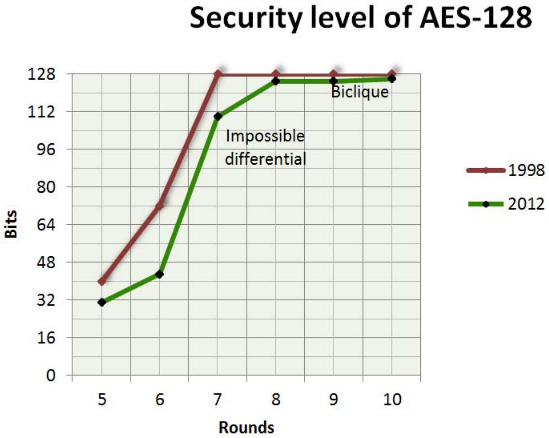
Only 1/5 of the full AES-192.

Results

	AES-128	AES-192	AES-256
8	$2^{125.4}$		
10	$2^{126.2}$		
12		$2^{189.7}$	
14			$2^{254.2}$

Future of AES

Progress in cryptanalysis



Any hope for improvements?

Full diffusion

Full diffusion takes 2 rounds in AES.

Natural limits:

- Short biclique length: one diffusion.
- Biclique matching: <2 full diffusions
- Impossible differential: 2 full diffusions.
- Square/multiset: <3 full diffusions.

Hence 3 full diffusions plus special treatment of the first and the last rounds if the attack allows.

Attack issues

Long bicliques:

- Low advantage, potentially many rounds.

Short bicliques:

- Limited rounds, brute-force elements.

Square/multiset:

- Properties on ≤ 4 rounds.

Impossible:

- Properties on ≤ 5 rounds.

Questions?