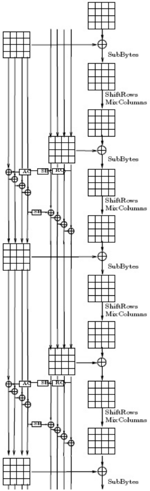
Distinguisher and Related-Key Attack on the Full AES-256

Alex Biryukov, Dmitry Khovratovich, Ivica Nikolić

University of Luxembourg

CRYPTO 2009
Santa Barbara
18 August 2009

AES-256



- 128-bit block;
- 256-bit key;
- 14 rounds;
- Approved for TOP SECRET in the U.S.

Cryptanalysis

Cryptanalysis timeline:

Year	Attack	Rounds	Authors
1998	Square	6	Daemen-Rijmen
2000	Square	8	Kelsey, Lucks et al.
2000	Related-key square	9	—
2005	Related-key rectangle	10	Biham et al.
2007	Known-key square	7	Knudsen-Rijmen

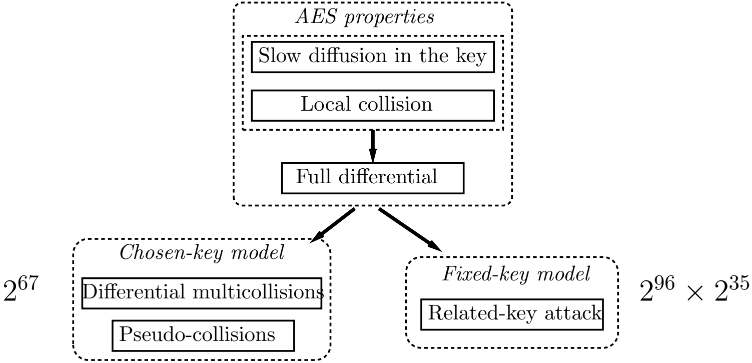
Cryptanalysis

Cryptanalysis timeline:

Year	Attack	Rounds	Authors
1998	Square	6	Daemen-Rijmen
2000	Square	8	Kelsey, Lucks et al.
2000	Related-key square	9	—
2005	**Related-key rectangle**	**10**	**Biham et al.**
2007	Known-key square	7	Knudsen-Rijmen

Best attack on 10 rounds: 2^6 related keys, 2^{114} data, 2^{173} time.

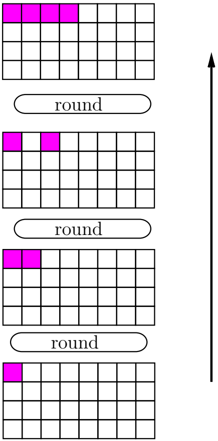
Outline of our paper



We show that AES is insecure in both models.

Differential Trail for the Full AES-256

Slow diffusion in the key schedule

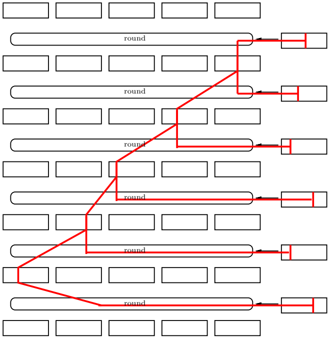


- One-byte difference
- Start from the last subkey
- Every inverted round affects only one more byte.

Idea of a local collision

SHA-0

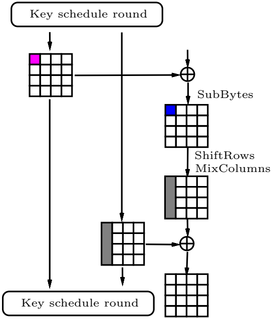
Difference from the message:



Probability 2^{-3}

AES

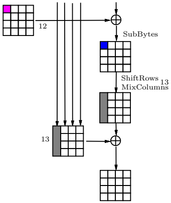
Difference from the key:



Probability 2^{-6}

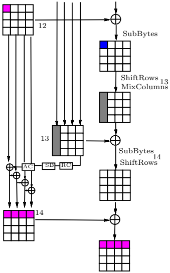
Construction: going backwards

Rounds	1
S-boxes in the state (🟦)	1
Probability	2^{-6}



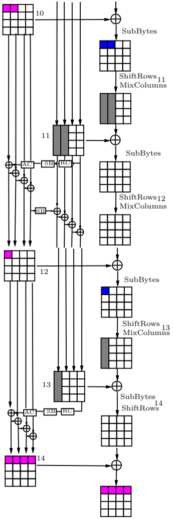
Construction: going backwards

Rounds	2
S-boxes in the state (🟦)	1
Probability	2^{-6}



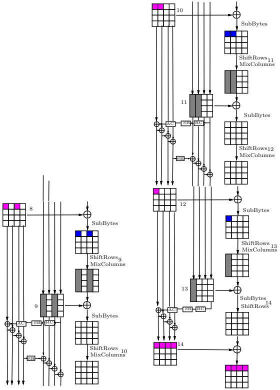
Construction: going backwards

Rounds	4
S-boxes in the state	3
Probability	2^{-18}



Construction: going backwards

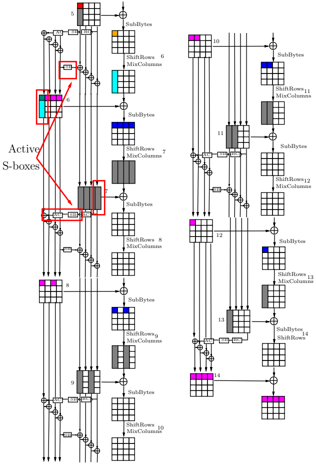
Rounds	6
S-boxes in the state	5
Probability	2^{-30}



Construction: going backwards

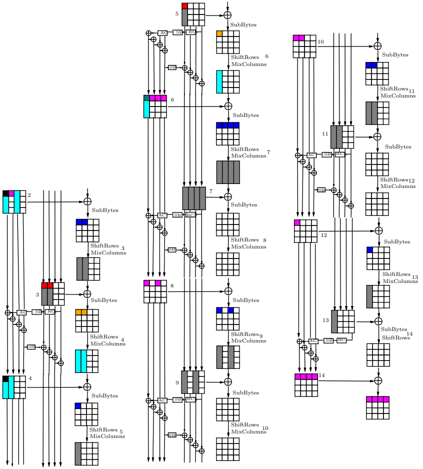
Rounds	9
S-boxes in the state	10
Probability	2^{-61}

- 5 active S-boxes in the key schedule;
- The trail is thus valid for 1 of 2^{35} key pairs.



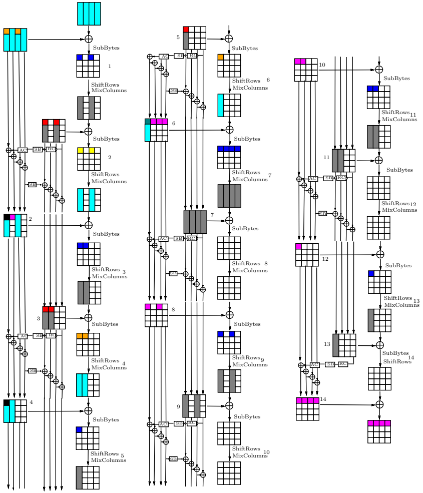
Construction: going backwards

Rounds	12
S-boxes in the state	14
Probability	2^{-87}
Key pairs	2^{35}



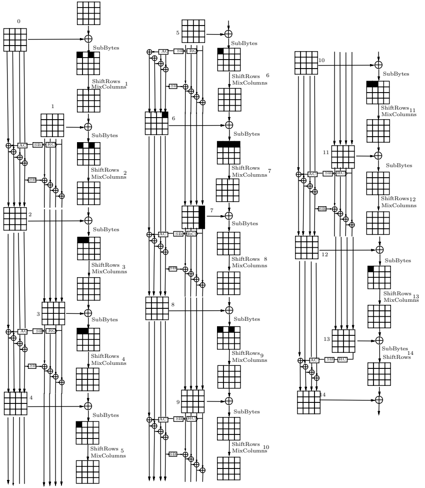
Construction: going backwards

Rounds	14 (full)
S-boxes in the state	19
Probability	2^{-119}
Key pairs	2^{35}



S-boxes

S-boxes in the state	19
S-boxes in the key	5



Attack directions

Trail is used in two models:

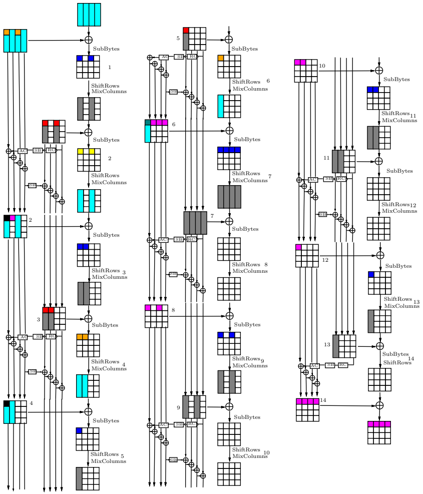
- Key is unknown and fixed (*fixed-key model*);
    - Find a secret key K.
- Key may be chosen (*chosen-key model*).
    - Find keys $\mathcal{K}$ and plaintexts $\mathcal{P}$ that satisfy special properties.

Fixed-key model

Related-key attack

Related-key attack

- K is unknown;
- Encrypt and decrypt on K and $K \oplus \Delta$;
- 1 of 2^{35} keys can be attacked.
- Complexity 2^{96} after we detect a right key pair.

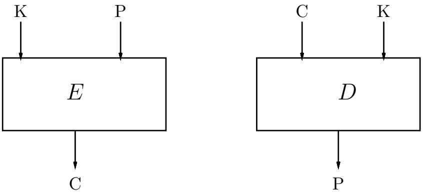


Chosen-key model

Chosen-key model

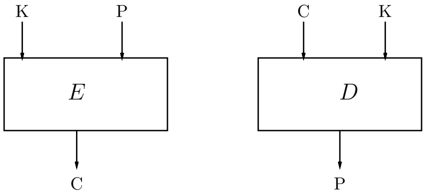
- AES is theoretically (2^{131}) insecure with a secret key.
- It is much less secure compared to an ideal cipher, which can be shown on a PC.

Ideal cipher



- Set of randomly chosen permutations.
- Can be modeled as two oracles.
- Used as a primitive in provably-secure constructions.

Ideal cipher

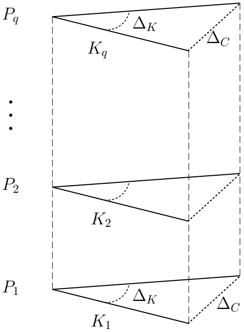


- Set of randomly chosen permutations.
- Can be modeled as two oracles.
- Used as a primitive in provably-secure constructions.

We show that AES should not be used in provably-secure constructions.

Differential q-multicollision

Introduce a new notion:

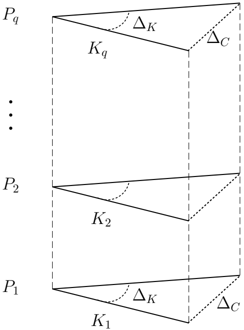


Definition. Differential q-multicollision:

$$F_{\Delta_K}(P,K) \overset{\text{def}}{=} E_K(P) \oplus E_{K\oplus\Delta_K}(P);$$
$$F(P_1,K_1) = F(P_2,K_2) = \cdots = F(P_q,K_q).$$

Differential q-multicollision

Introduce a new notion:



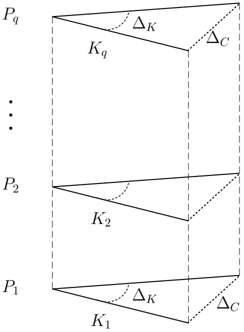
Definition. Differential q-multicollision:

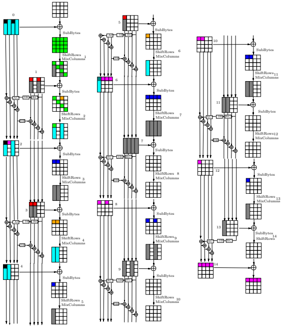
$$F_{\Delta_K}(P,K) \overset{\text{def}}{=} E_K(P) \oplus E_{K\oplus\Delta_K}(P);$$
$$F(P_1,K_1) = F(P_2,K_2) = \cdots = F(P_q,K_q).$$

Provably hard to find in an ideal cipher: $\gtrsim q \cdot 2^{\frac{q-1}{q+1}n}$.

Differential q-multicollision in AES

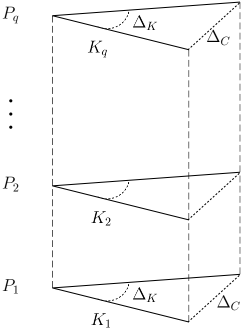
A set of q pairs (key, plaintext) that satisfy the trail.

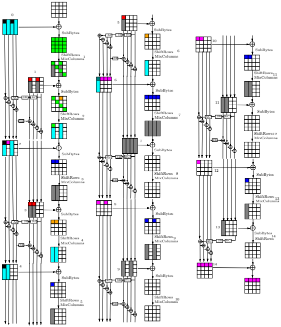




Differential *q*-multicollision in AES

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

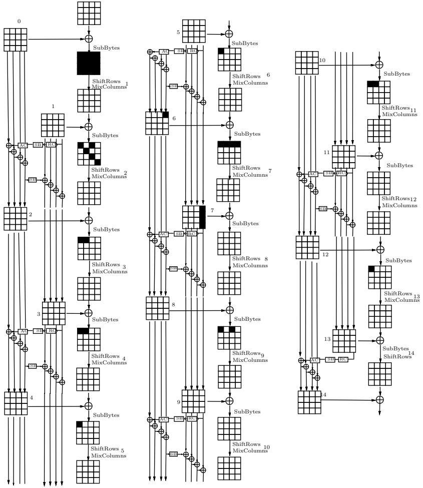




Can be found in $q \cdot 2^{67}$ with our *Triangulation Algorithm* (CT-RSA 2009).

Multicollision search

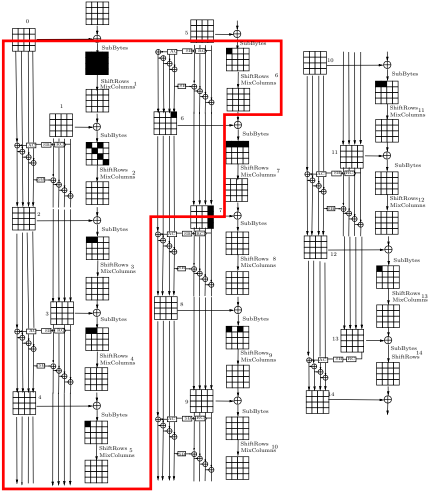
The trail has 41 active S-boxes.



Multicollision search

The trail has 41 active S-boxes.

1. Fix values of 30 active S-boxes.
2. Run the triangulation algorithm and derive a set of free variables.
3. Produce many pairs (P, K) and check for remaining S-boxes in 2^{67}.



Differential *q*-multicollision in AES

Practical distinguisher for 13 rounds (14 are similar):

Δ_K	0f070709 0e070709 0f070709 0e070709
	371f1f21 00000000 371f1f21 00000000

Differential q-multicollision in AES

Practical distinguisher for 13 rounds (14 are similar):

Δ_K	0f070709 0e070709 0f070709 0e070709 371f1f21 00000000 371f1f21 00000000
Δ_{P_1}	a3**1f1f21 00000000** 19**1f1f21 00000000**

Differential q-multicollision in AES

Practical distinguisher for 13 rounds (14 are similar):

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**

Differential q-multicollision in AES

Practical distinguisher for 13 rounds (14 are similar):

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**

Differential *q*-multicollision in AES

Practical distinguisher for 13 rounds (14 are similar):

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**

Differential q-multicollision in AES

Practical distinguisher for 13 rounds (14 are similar):

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**

Differential *q*-multicollision in AES

Practical distinguisher for 13 rounds (14 are similar):

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

Differential q-multicollision in AES

Practical distinguisher for 13 rounds (14 are similar):

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

- Lower bound for $q = 5$: 2^{75};
- Find 5-multicollision in a few hours on the PC;
- Try to find it for your favorite cipher.

Conclusion

Summary

- Differential trail on the full AES;
- Related-key attack in $2^{96} \cdot 2^{35}$;
- Practical insecurity in the chosen-key model.

See in the full paper

- All the trail details;
- Proof of the multicollision hardness;
- Insecurity of AES in the Davies-Meyer mode.

New attacks

New results?

Rump session today.

Details

Details on the related-key attack

User chooses a secret key pair with our relation.

Then for each key pair:

1. Relax two S-boxes and recover 80 bits of the key;

Details on the related-key attack

User chooses a secret key pair with our relation.

Then for each key pair:

1. Relax two S-boxes and recover 80 bits of the key;
2. Relax one more S-box and recover 64 bits of the key;

Details on the related-key attack

User chooses a secret key pair with our relation.

Then for each key pair:

1. Relax two S-boxes and recover 80 bits of the key;
2. Relax one more S-box and recover 64 bits of the key;
3. Exhaustive search on the other bits.

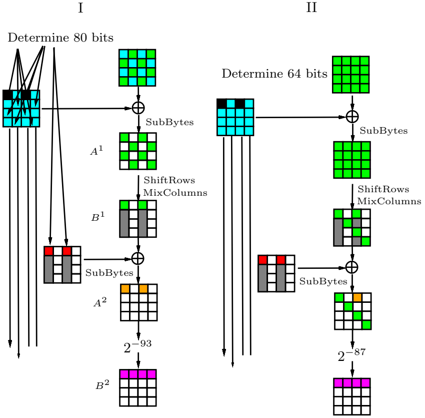
Details on the related-key attack

User chooses a secret key pair with our relation.

Then for each key pair:

1. Relax two S-boxes and recover 80 bits of the key;
2. Relax one more S-box and recover 64 bits of the key;
3. Exhaustive search on the other bits.

Works in 2^{96} time for a right key pair, 2^{131} in total.



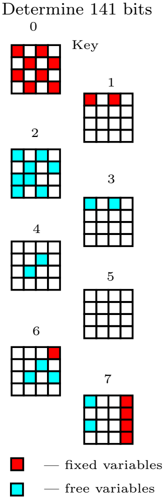
Alternative on the key recovery

Given: bytes of different subkeys.

Find: the key.

Tool: triangulation algorithm (CT-RSA 2009).

- Write the key schedule as a system of equations;
- Perform a Gaussian-like elimination;
- Try all values for free variables.


Determine 141 bits
0
Key
1
2
3
4
5
6
7
🟥 — fixed variables
🟦 — free variables