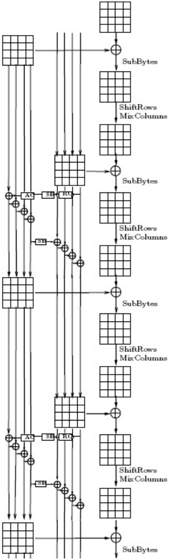
AES-256 is Not Ideal

Alex Biryukov, **Dmitry Khovratovich**, Ivica Nikolić

University of Luxembourg

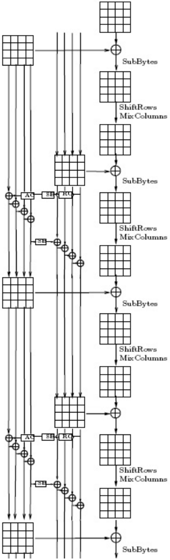
Eurocrypt 2009 Rump session
28 April 2009

AES-256



- 128-bit block;
- 256-bit key;
- Approved for TOP SECRET in the U.S.;
- Best attack on 10 (of 14) rounds: 2^6 related keys, 2^{114} data, 2^{173} time.

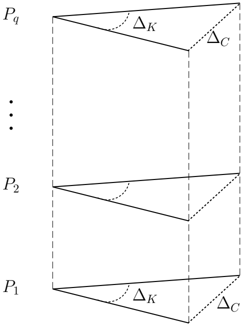
AES-256



- 128-bit block;
- 256-bit key;
- Approved for TOP SECRET in the U.S.;
- Best attack on 10 (of 14) rounds:
  2^6 related keys, 2^{114} data, 2^{173} time.

Secure?

NEW: Not as an ideal cipher

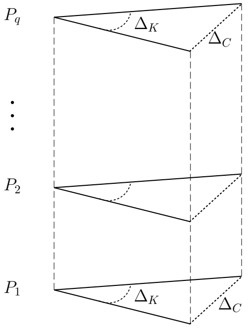


Definition. Differential q-multicollision:

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

NEW: Not as an ideal cipher

Differential q-multicollision:



Complexity:

- $\gtrsim q \cdot 2^n$ for an ideal cipher;
- $q \cdot 2^{67}$ for AES-256.

NEW: Not as an ideal cipher

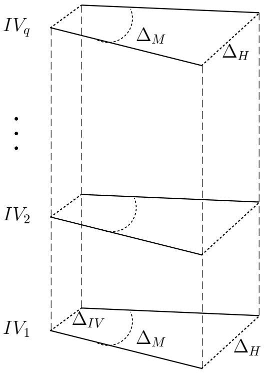
Practical distinguisher for 13 rounds (14 are similar):

Δ_K	0f070709 0e070709 0f070709 0e070709 $\ldots$
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

- Prove the lower bound for $q = 5$: 2^{75};
- Find 5-multicollision in few hours on the PC;

NEW: Not in the Davies-Meyer mode

q-pseudocollisions:



- Fixed ΔIV, ΔM, ΔH;
- $\approx q \cdot 2^n$ for an ideal cipher in DM;
- $q \cdot 2^{67}$ for AES-256.

NEW: Not in the related-key framework

Trail with 5 active S-boxes in the key schedule and 19 — in the state.

Recover 1 of 2^{35} related keys in:

- 2^{131} time;
- 2^{96} data for each key.

Summary

Questions? Work in progress