Key Recovery Attacks on 3-Round Even-Mansour (with Applications!)

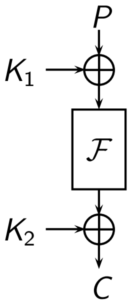
Itai Dinur, Orr Dunkelman, Nathan Keller, Adi Shamir

Computer Science Department
University of Haifa

28th May, 2013

The Even-Mansour Block Cipher

- Suggested by Even and Mansour in 1991, as a generalization of DESX.
- Main idea: Take an unkeyed random permutation, $\mathcal{F}$, and use pre-/post-whitening.
- Block size: n bits, Key size: 2n bits.



$$EM^{\mathcal{F}}_{K_1,K_2}(P) = \mathcal{F}(P \oplus K_1) \oplus K_2$$

Security of the Even-Mansour Scheme

- A simple attack that requires 2 plaintext/ciphertext pairs and 2^n time.
- Moreover, there is a **proof** that any attack that uses D plaintext/ciphertext pairs, and T queries to $\mathcal{F}$, has success rate of $O(DT/2^n)$.

Security of the Even-Mansour Scheme

- A simple attack that requires 2 plaintext/ciphertext pairs and 2^n time.
- Moreover, there is a **proof** that any attack that uses D plaintext/ciphertext pairs, and T queries to $\mathcal{F}$, has success rate of $O(DT/2^n)$.

D92 a differential attack that matches the bound (offers the complete tradeoff) in chosen plaintext settings.

BW00 a slide attack that matches the bound for $D = T = 2^{n/2}$ in known plaintext settings.

DKS11 a SlideX attack that matches the bound (offers the complete tradeoff) in known plaintext settings.

The Big Bang of EM-Based Constructions

- DKS11 Can we reduce the keying material? (answer: yes!)
- G+11 LED: 8-Round Iterated EM (1-Key) or 12-Round Iterated EM (2-Key).
- B+12 Iterative EM shown to be indistinguishable in time $\Omega(2^{2n/3})$.
- B+12 Introduced AES^2 $(=\mathrm{AES}_{c_2}(\mathrm{AES}_{c_1}(m \oplus K_1) \oplus K_2) \oplus K_3)$.
- LPS12 Improving [B+12] conjectures.
- S12 3-Round EM indistinguishable in time $\Omega(2^{3n/4})$.
- A+13 Iterative EM shown to be indifferentiable.
- NWW13 Attacks on 2-Round 1-Key EM.
- LS13 12-Round 1-Key iterated EM — indifferentiable from ideal cipher.
- G+13 Early versions of ZORRO (5-Round/3-Round Iterated EM).

Results on LED

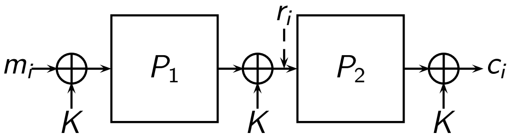
Reference	Cipher	Steps	Time	Data	Memory
[IS12]	LED-64	2	2^{56}	2^{8} CP	2^{11}
Our work	LED-64	3	$2^{60.2}$	2^{49} KP	2^{60}
[IS12]	LED-128	4	2^{112}	2^{16} CP	2^{19}
[M+12]	LED-128	4	2^{96}	2^{64} KP	2^{64}
[NWW13]	LED-128	4	2^{96}	2^{32} KP	2^{32}
[NWW13]	LED-128	6	$2^{124.4}$	2^{59} KP	2^{59}
Our work	LED-128	6	$2^{124.5}$	2^{45} KP	2^{60}
Our work	LED-128	8	$2^{123.8}$	2^{49} KP	2^{60}

Note that the in LED, each step is a 4-round unkeyed permutation. We use the steps notations to avoid confusion, in which case, LED-64 has 8 steps, and LED-128 has 12 steps.

Results on AES^2

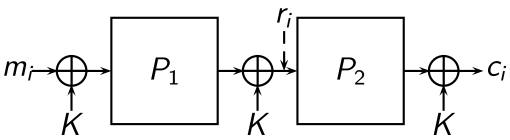
- $\text{AES}^2 = \text{AES}_{c_2}(\text{AES}_{c_1}(m \oplus K_1) \oplus K_2) \oplus K_3)$.
- A simple Meet-in-the-Middle attack exists (time complexity $2^{129.6}$ AES^2 evaluations, memory 2^{128} memory cells).
- Our attack takes:
  - Data: $2^{125.4}$ chosen plaintexts
  - Time: $2^{126.8}$ (7-fold improvement)
  - Memory: $2^{125.4}$ (6-fold improvement)
- Attack is based on large entries in the difference distribution table of AES_{c_1} (related to [M+12], assumes AES_{c_1} is a random permutation).

2-Round 1-Key Even-Mansour



- Let $P'_1(x) = x \oplus P_1(x)$ (a random function).
- XORing the input and output of $P_1(x)$ with the same value K, does not alter the outcome of the feed forward!
- Hence, if v is a frequent image of P'_1, then $\Pr[r_i = m_i \oplus v]$ is more frequent than other values.
- In other words, $P_2(m_i \oplus v) \oplus c_i$ is more likely to be K!

Our Attack (Variant of [NWW13])



- Find optimal v (and its probability $(t/2^n)$)
- Collect enough known plaintexts (roughly $2^n/t$)
- For each of them assume that v "happened", obtain candidate K, and try it.

Complexity: Preprocessing $\lambda \cdot 2^n$ (with similar memory).
Online data $O(2^n/t)$, online time $O(2^n/t)$, online memory 1.

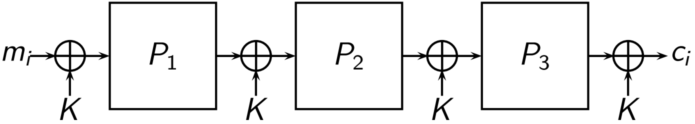
Improvements

- We offer two improvements:
  - Picking the inputs in the preprocessing as part of some affine subspace, allows immediate discarding of wrong values.
  - Using several values for v's (needs more online storage, reduces data complexity).

Improvements

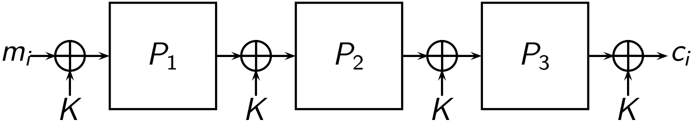
- We offer two improvements:
  - Picking the inputs in the preprocessing as part of some affine subspace, allows immediate discarding of wrong values.
  - Using several values for v's (needs more online storage, reduces data complexity).
- For 64-bit block: $2^{60.4}$ time (including pre-processing), $2^{58.7}$ known plaintexts.
- Collecting many v's: $2^{60.1}$ time, 2^{45} known plaintexts, and 2^{16} online memory.

3-Round 1-Key Even-Mansour



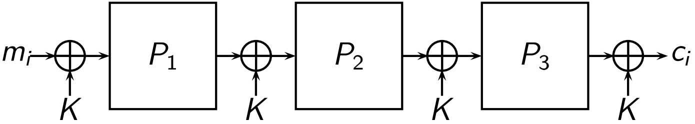
- Main problem — we still need to "skip" one more permutation!

3-Round 1-Key Even-Mansour



- Main problem — we still need to “skip” one more permutation!
- Main solution — precompute P'_3, and use it to find the key.

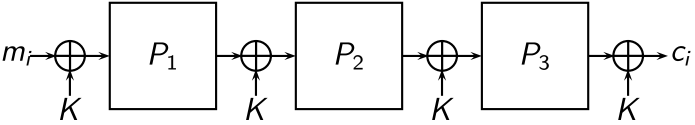
3-Round 1-Key Even-Mansour — Preprocessing



Preprocessing:

- Find optimal v for $P_1'(x) = x \oplus P_1(x)$ (with probability $t/2^n$).
- Evaluate $P_3'(x)$ on x's, and store the obtained values in a sorted list L_3 of $P_3'(x)$ along with $P_3(x)$.

3-Round 1-Key Even-Mansour — Online



Online:

- Ask for many plaintexts
- For any plaintext, assume that v happened in $P_1'(x)$ (i.e., $r_i = m_i \oplus v$).
- Apply $P_2(m_i \oplus v)$, and check whether $P_2(m_i \oplus v) \oplus c_i$ is in the list L_3.
- If so, obtain $P_3(x)$ from L_3, and check the key $K = P_3(x) \oplus c_i$.

Optimizations

- As before we can add optimizations which reduce the need to check wrong keys, and reduce the data complexity.
- For 64-bit blocks: $2^{60.2}$ time (including pre-processing), 2^{49} known plaintexts, and 2^{60} memory.

Summary & Conclusions

- Introduced new attacks on 2-round Even-Mansour (1-key/independent keys)
- Introduced new attacks on 3-round Even-Mansour (1-key)
- First attack on the full AES^2 (7-times faster than exhaustive search)
- Breaking 3/8 steps of LED-64
- Breaking 8/12 steps of LED-128 (improved from 6/12, with reduced complexities!)
- Better understanding of iterated Even-Mansour

Summary & Conclusions

- Introduced new attacks on 2-round Even-Mansour (1-key/independent keys)
- Introduced new attacks on 3-round Even-Mansour (1-key)
- First attack on the full AES^2 (7-times faster than exhaustive search)
- Breaking 3/8 steps of LED-64
- Breaking 8/12 steps of LED-128 (improved from 6/12, with reduced complexities!)
- Better understanding of iterated Even-Mansour
- **Does not go over all possible keys, applying a simpler operation than full encryption per guess.**

Questions?

$E\nu\chi\alpha\rho\iota\sigma\tau\omega$!

Thank you for your attention!

Paper to appear soon on eprint.