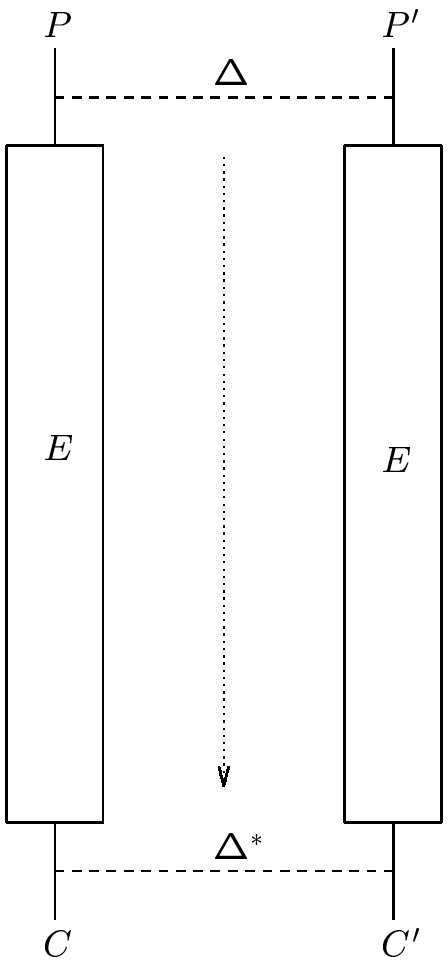
The boomerang attack

David Wagner
University of California, Berkeley

Organization

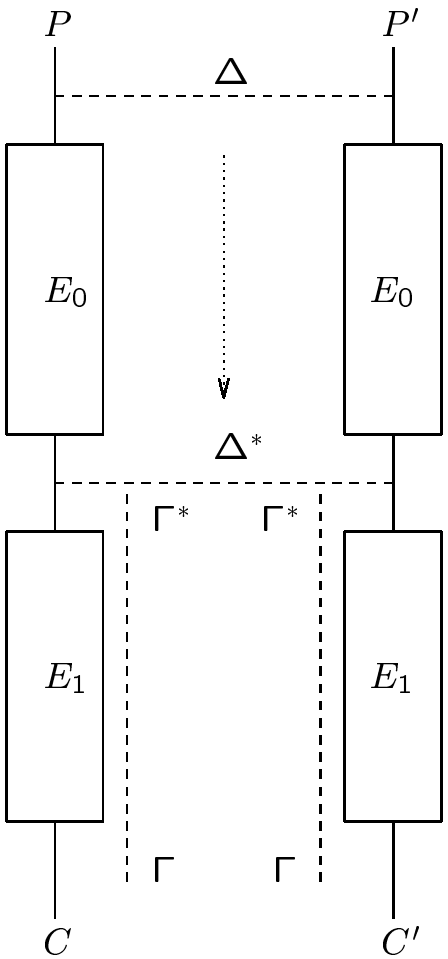
- Review: differential, differential-linear, and miss-in-the-middle attacks
- The boomerang
- Example application: COCONUT98, a decorrelated cipher
- The inside-out attack
- Exploiting asymmetries

Differential attack



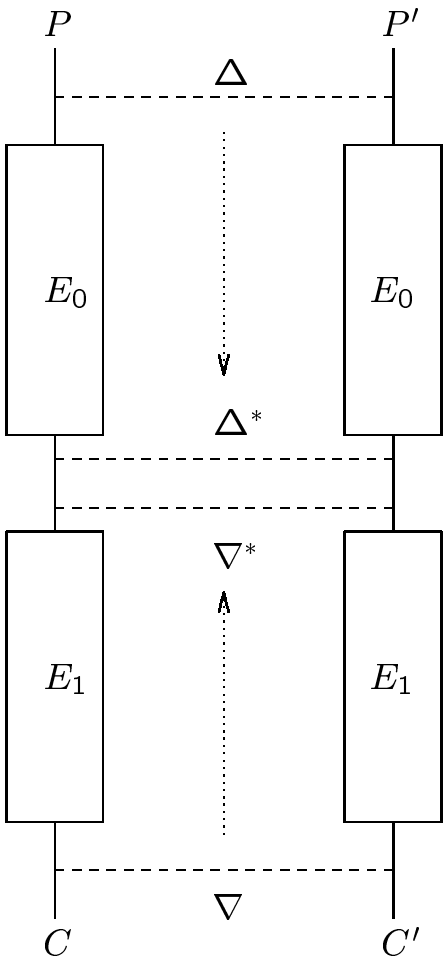
Uses: differential $\Delta \rightarrow \Delta^*$ for E.

Differential-linear attack



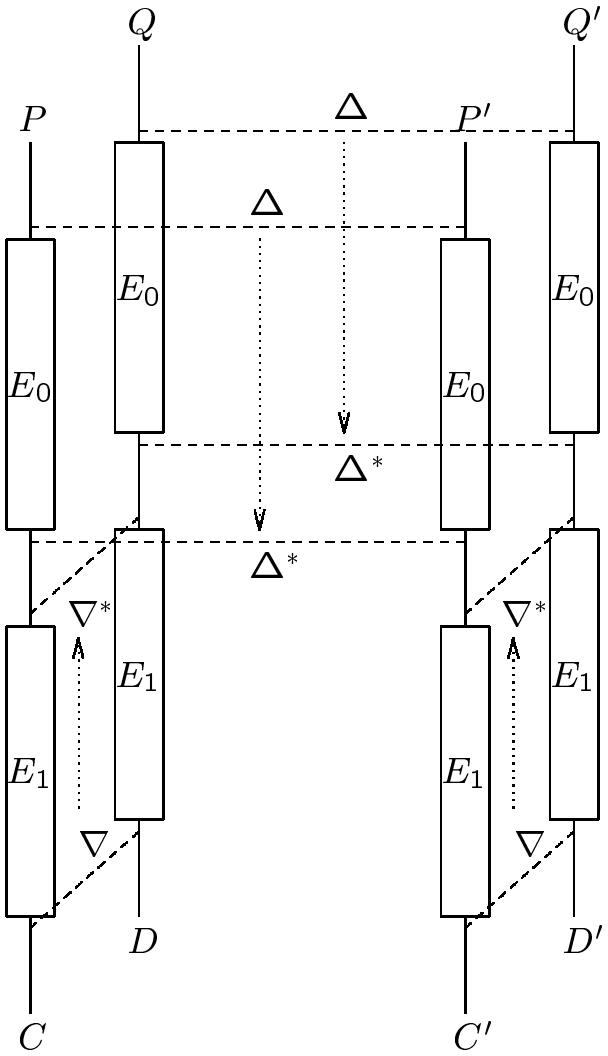
Uses: diff. $\Delta \to \Delta^*$ for E_0,
linear approx. $\Gamma \to \Gamma^*$ for E_1 (twice).

Miss-in-the-middle attack



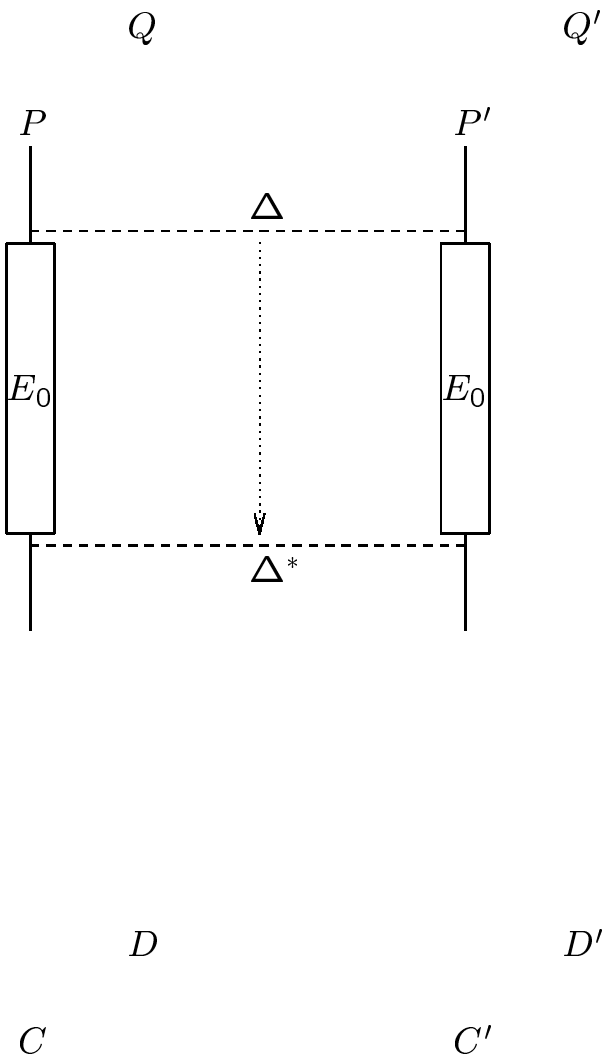
Uses: diff. $\Delta \to \Delta^*$ for E_0,
diff. $\nabla \to \nabla^*$ for E_1^{-1}.

Boomerang attack



Uses: diff. $\Delta \to \Delta^*$ for E_0,
diff. $\nabla \to \nabla^*$ for E_1^{-1} (twice),
diff. $\Delta^* \to \Delta$ for E_0^{-1}.

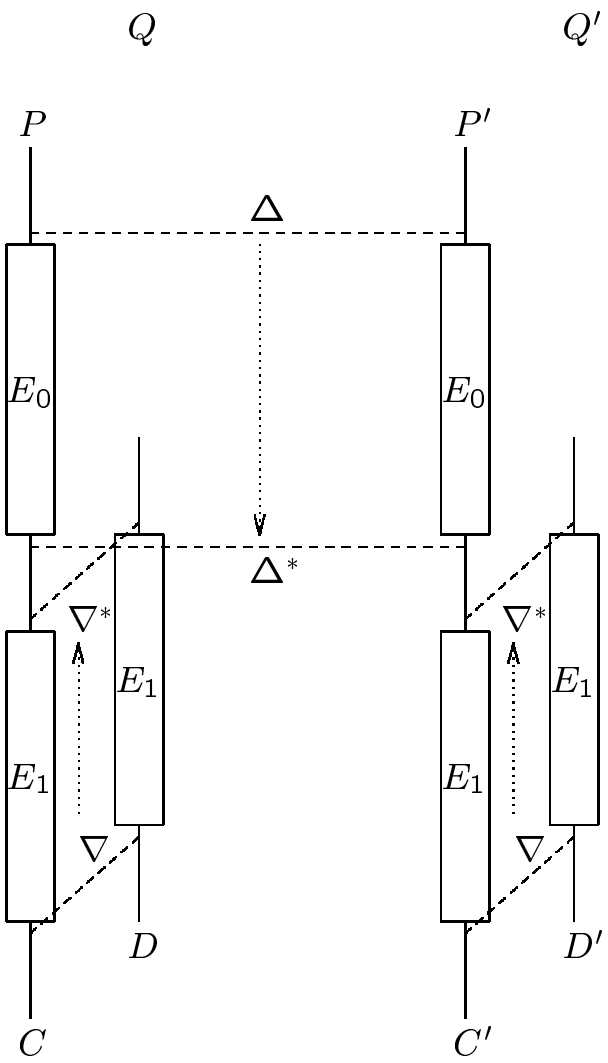
Slowly: step #1



Pick P, P' so that $P \oplus P' = \Delta$.

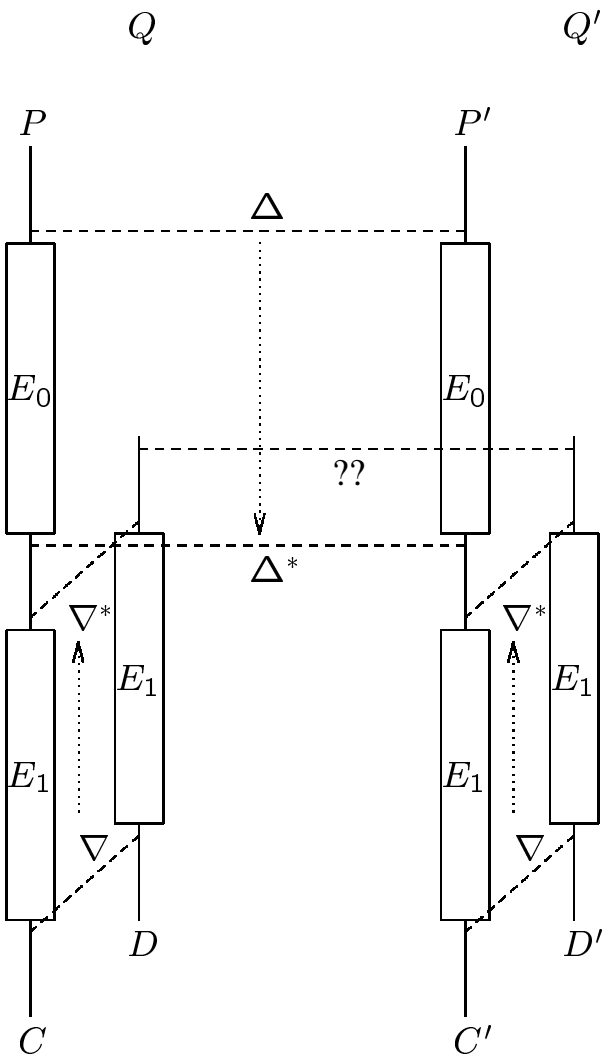
Encrypt. Use $\Delta \rightarrow \Delta^*$ for E_0.

Slowly: step #2



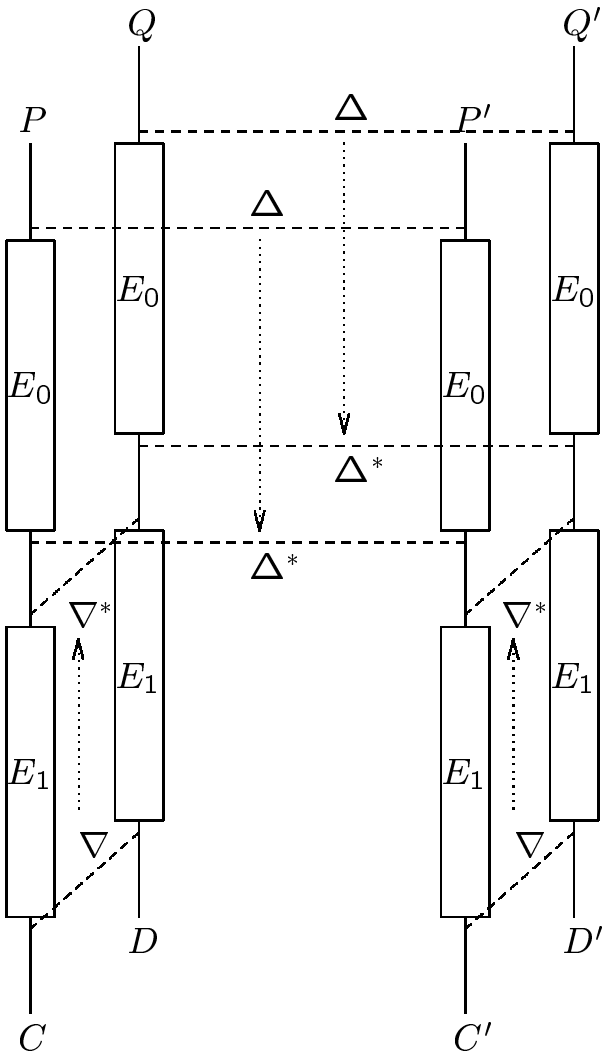
Pick D, D' so that $C \oplus D = C' \oplus D' = \nabla$.
Decrypt. Use $\nabla \to \nabla^*$ for E_1^{-1} twice.

Slowly: step #3



Note that $?? = \Delta^* \oplus \nabla^* \oplus \nabla^* = \Delta^*$, because of a quartet-like structure in the middle.

Slowly: step #4



Use $\Delta^* \to \Delta$ for E_1^{-1}.

COCONUT98

Application: COCONUT98, a decorrelated cipher.

COCONUT98 = $\Psi_1 \circ M \circ \Psi_0$,
where Ψ is a simple four-round Feistel and M is a decorrelation module $M(x) = \alpha x + \beta \in GF(2^{64})$.

Proven to be secure against the standard differential attack, using theory of decorrelation.

Breaking COCONUT98

Observation: There are good differentials for Ψ, Ψ^{-1}.

Idea: Let $E_0 = \Psi_0$, $E_1 = \Psi_1 \circ M$. Then there are good differentials for E_0, E_1^{-1}, E_0^{-1}.

Apply boomerang attack.

Result: Breakable with 2^{16} adaptive chosen-plaintext/ciphertext queries.

Lessons from COCONUT98

Decorrelation theorems must be interpreted with some care.

In general, it is not enough to ensure that there are no good differentials for the whole cipher; “differential-style” attacks may still be possible.

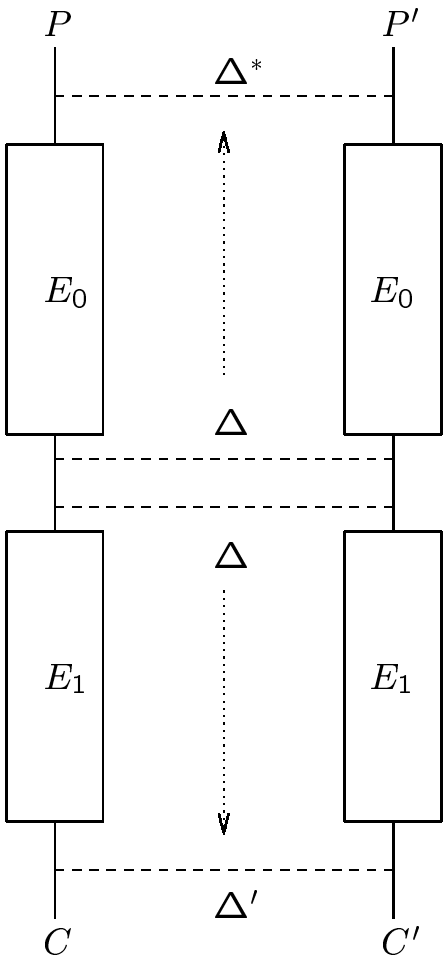
Should ensure that there are no good differentials for the first or last half of the cipher.

Other results

Can break 16 rounds of Khufu with 2^{18} adaptive chosen-plaintext/ciphertext queries and not much work.

Can break 16 rounds of CAST-256 with $2^{49.3}$ **known** texts and not much work, using the “inside-out attack”.

Inside-out attack



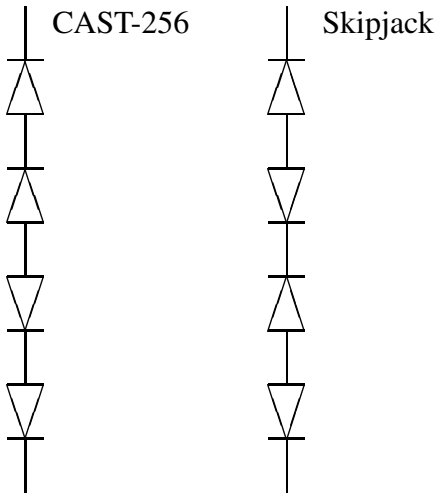
Uses: diff. $\Delta \to \Delta^*$ for E_0^{-1},
diff. $\Delta \to \Delta'$ for E_1.

Asymmetrical round functions

A-rounds have better diffusion in forward direction:

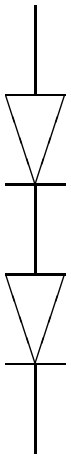
B-rounds have better diffusion in reverse direction:

Examples:

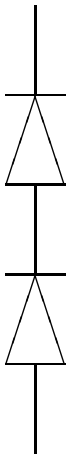


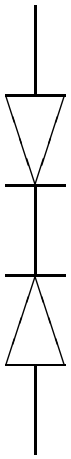
Exploiting asymmetry

Chosen-plaintext differential

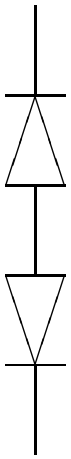


Chosen-ciphertext differential





Boomerang, miss-in-the-middle



Inside-out

Contributions

- New attacks on a decorrelated cipher.
  (Does not apply to DFC.)
- New results on Khufu, CAST-256.
- New techniques for exploiting asymmetrical round functions.
- It's all about drawing pretty pictures. . .