Boomerang Switch in Multiple Rounds

Application to AES Variants and Deoxys

Haoyang Wang, Thomas Peyrin

School of Physical and Mathematical Sciences,

Nanyang Technological University, Singapore

FSE 2019, Paris

March 26, 2019

Outline

- Background
- Boomerang Switch
- Attack on 10-round AES-256
- Application to Full-round AES-192 and reduced-round Deoxys-BC

Background

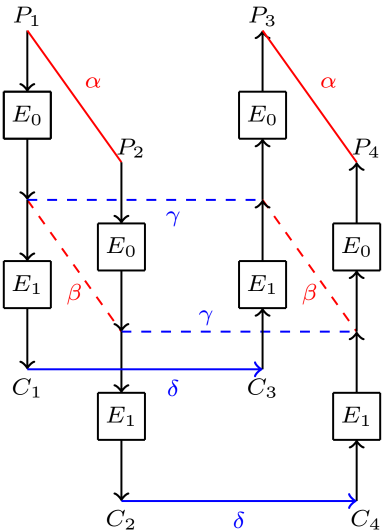
Boomerang Attack

Boomerang attack

- A cipher E is divided into two sub-ciphers:

$$E = E_1 \circ E_0$$

- E_0: $P[\alpha \rightarrow \beta] = p$
- E_1: $P[\gamma \rightarrow \delta] = q$
- The two trails are assumed to be independent.
- Distinguish probability: $Pr[E^{-1}(E(x) \oplus \delta) \oplus E^{-1}(E(x \oplus \alpha) \oplus \delta) = \alpha] = p^2q^2$



Dependency Between the Two Sub-Ciphers

- At the boundary of the two trails, dependency may exist.

Positive effect

- Middle round S-box trick [BDD03]
- Ladder switch [BK09]
- S-box switch [BK09]
- Feistel switch [BK09]

Negative effect

- Imcompatibility [Mer09]

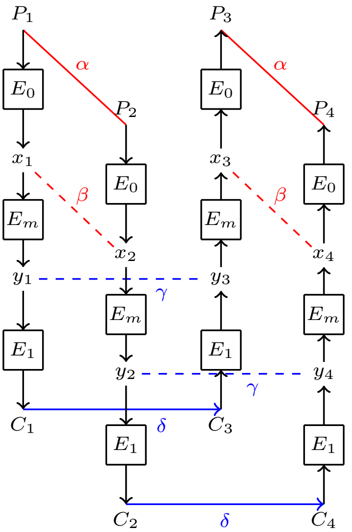
Sandwich Attack

Sandwich attack

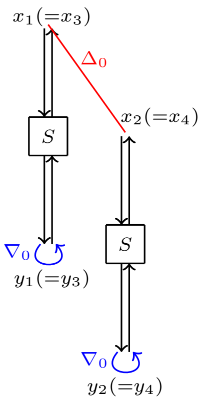
- E is further divided into three sub-ciphers:

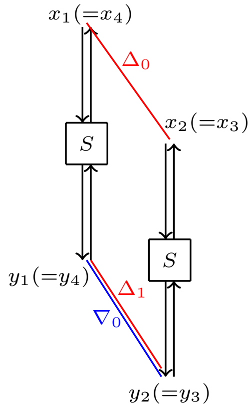
$$E = E_1 \circ E_m \circ E_0$$

- E_m contains the dependent parts of the two trails, with probability r
- $r = Pr[E_m^{-1}(E_m(x) \oplus \gamma) \oplus E_m^{-1}(E_m(x \oplus \beta) \oplus \gamma) = \beta]$
- Distinguish probability: p^2q^2r.



View of Boomerang Switch in Sandwich Attack





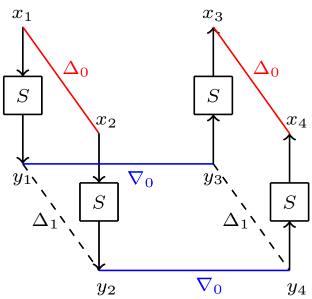
Ladder switch

1. $\nabla_0 = 0$
2. $y_3 = y_1$ and $y_4 = y_2$
3. $x_3 = x_1$ and $x_4 = x_2$
4. $r = 1$

Sbox switch

1. $\nabla_0 = \Delta_1$
2. $y_4 = y_1,\ y_3 = y_2$
3. $x_4 = x_1$ and $x_3 = x_2$
4. $r = pr[\Delta_0 \xrightarrow{Sbox} \Delta_1]$

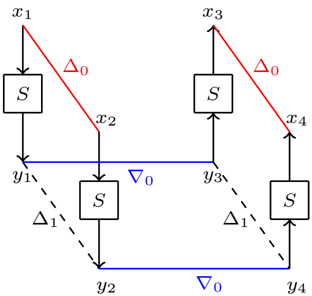
Boomerang Connectivity Table (BCT)



Construction

- Focus on a single S-box layer.
- Δ_0 and ∇_0 are taken into consideration.
- The entry for (Δ_0, ∇_0) is computed by $\#\{x \in \{0,1\}^n | S^{-1}(S(x) \oplus \nabla_0) \oplus S^{-1}(S(x \oplus \Delta_0) \oplus \nabla_0)\}$.

Boomerang Connectivity Table (BCT)



Advantages

- It covers the switching effect of ladder switch, S-box switch and incompatibility.
- New switching effect: Compared to S-box switch where $\nabla_0 = \Delta_1$, BCT does not require the value of Δ_1, which could lead to a higher switching probability.

Motivation

Questions

- Can we extend E_m to multiple rounds?
- If yes, can current switching techniques be applied to the multiple-round case?

Boomerang Switch

Determining the Number of Rounds in E_m

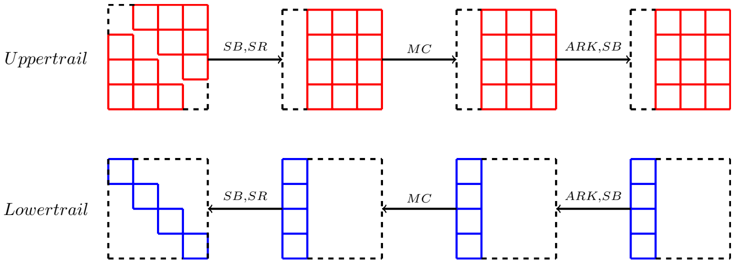


Figure: Parallel operations of truncated 2-round AES

The idea of ladder switch

The round function of a cipher can be divided into two independent parts, which can operate in parallel.

Extension

In E_m, if the forward diffusion of the active cells in the upper trail has no interaction with the backward diffusion of the active cells in the lower trail, a right quartet of E_m can be generated with probability 1.

Determining the Number of Rounds in E_m

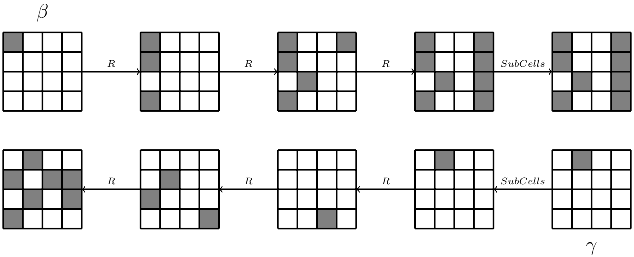


Figure: A 4-round E_m of SKINNY with probability 1

Observation

- For SKINNY [BJK+16], E_m can be at most four rounds with probability $r = 1$.
- E_m contains more rounds for those ciphers with slower diffusion layer.

Incompatibility in Multiple Rounds

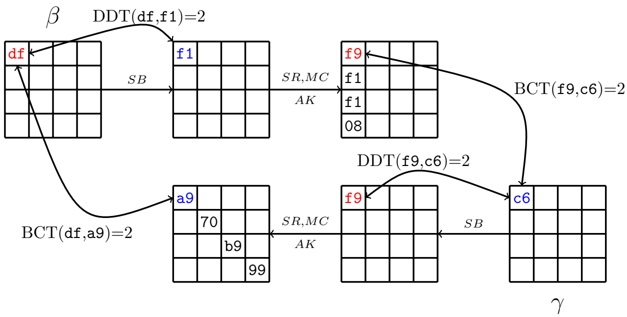
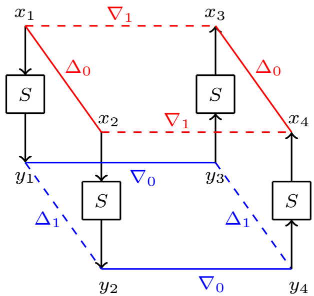


Figure: An incompatible 2-round E_m of AES

Deficiency of BCT

- BCT detects incompatibility while the entry is zero.
- The two trails are valid with probability 2^{-7} respectively: DDT(df,f1)=2, DDT(f9,c6)=2.
- For the two active S-boxes, the entries of BCT are non-zero: BCT(df,a9)=2, BCT(f9,c6)=2.
- However, this example is incompatible: BCT(df,a9) and DDT(df,f1) cannot be non-zero simultaneously.

Observation on S-box in the Boomerang Switch



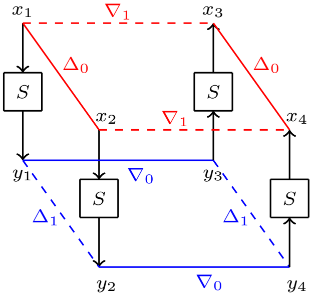
Lemma1

For any fixed Δ_0 and Δ_1, for which the DDT entry is $2l$, l being a nonzero integer, the maximum number of nontrivial values of ∇_0, for which a right quartet could be generated, is $2\binom{l}{2} + 1$.

Lemma2

For any fixed Δ_0 and ∇_0, for which the BCT entry is $2l$ and the DDT entry is $2l'$, l and l' being nonzero integers, the maximum number of choices of Δ_1, for which a right quartet could be generated, is $1 + (2l - 2l')/4$.

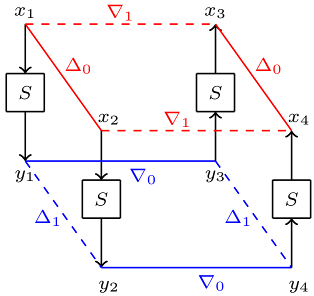
Boomerang Difference Table (BDT)



Construction

- A combination of BCT and DDT.
- The entry for $(\Delta_0, \Delta_1, \nabla_0)$ is defined by: $\#\{x \in \{0,1\}^n | S^{-1}(S(x) \oplus \nabla_0) \oplus S^{-1}(S(x \oplus \Delta_0) \oplus \nabla_0) = \Delta_0, S(x) \oplus S(x \oplus \Delta_0) = \Delta_1\}$, n is the S-box size.
- The time complexity for the construction is $O(2^{2n})$.

Boomerang Difference Table (BDT)



Properties

- $DDT(\Delta_0, \Delta_1) = BDT(\Delta_0, \Delta_1, 0) = BDT(\Delta_0, \Delta_1, \Delta_1)$
- $BCT(\Delta_0, \nabla_0) = \sum_{\Delta_1=0}^{2^n} BDT(\Delta_0, \Delta_1, \nabla_0)$
- $BDT(0, 0, \nabla_0) = 2^n$
- $(\Delta_0, \Delta_1, \nabla_0)$ is incompatible when the corresponding entry in BDT is 0.

Attack on 10-round AES-256

Attack model

Related-key attack

- The adversary chooses a relation between several keys, e.g., $K_2 = K_1 \oplus C$ and is given access to encryption/decryption oracles with these keys.

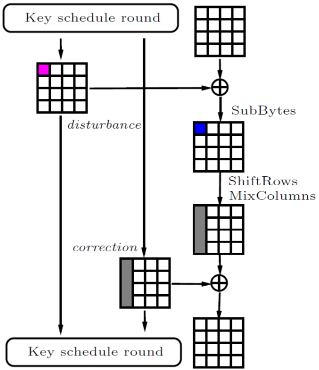
Related-subkey attack

- The adversary chooses a relation between subkeys, e.g., $K_2 = F^{-1}(F(K_1) \oplus C)$, where F represents the round function of key schedule.
- Advantage: easier to obtain a desired related-subkey difference in non-linear key schedule.
- Disadvantages: complex key access scheme, less practical and even too contrived for academic interest.

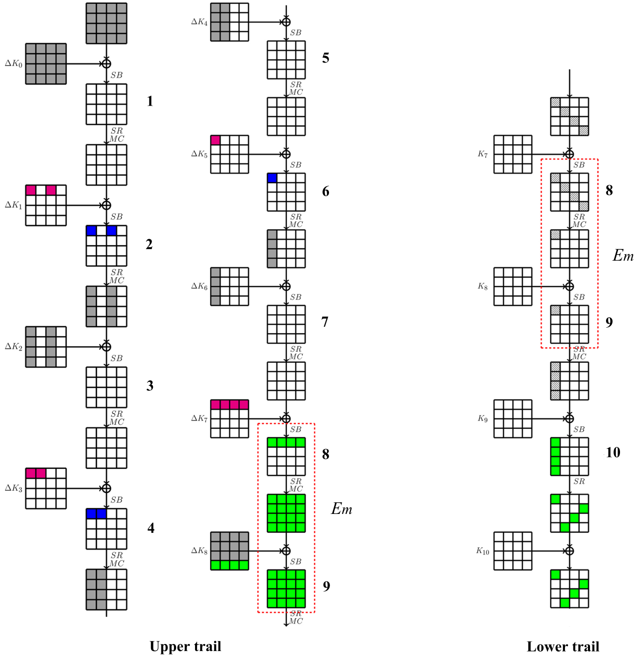
Overview of the Attack

Idea

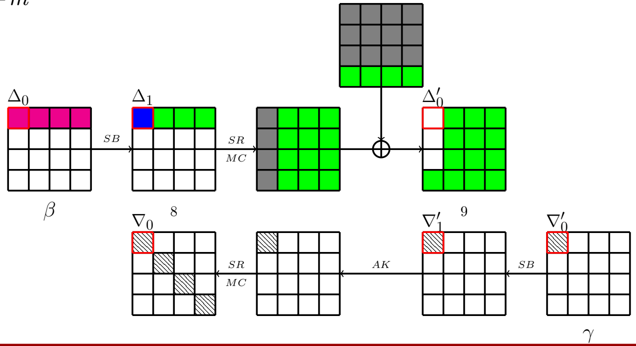
- We stick to the related-key attack. Since the key schedule of AES is non-linear, a related-key differential path is used for the upper trial while a single-key differential path is used for the lower trail.
- The local collision strategy is used for constructing the upper trail.
- Apply the boomerang switch in two rounds.



The 10-round Attack



The 2-round E_m



Analysis

- β and γ are fixed.
- For the S-box at (0,0) in round 8:
  - A fixed value Δ_1 is chosen so that there is no overlapped active cell in round 9.
  - With the fixed Δ_0 and Δ_1, choose the values of ∇_0 so that the BDT entries are non-zero, and the switching probability is obtained accordingly.
- For the S-box at (0,0) in round 9:
  - ∇'_1 is uniquely determined by ∇_0.
  - Since $\Delta'_0 = 0$, the switching probability can be evaluated by DDT with entry (∇'_1, ∇'_0)

Result

Scenario	# keys	Time	Data	Result	Reference
Key Diff.	64/256	2^{172}	2^{114}	Full key	[KHP07]/[BDK05]
Subkey Diff.	2	$2^{45}(2^{221})$	2^{44}	35 subkey bits (full key)	[BDK+10]
Key Diff.	2	2^{75}	2^{75}	Full key	this paper

Application to Full-round AES-192 and reduced-round Deoxys-BC

Overview of the Previous Attacks

- Full-round AES-192 [BN09]: the first related-key boomerang attack on full-round AES-192.
- Full-round AES-192 [BN10]: the upper trail is different than [BN09], and remains as the best attack.
- 10-round Deoxys-BC[CHP+17]: its distinguisher is built with the idea of 2-round boomerang switch.

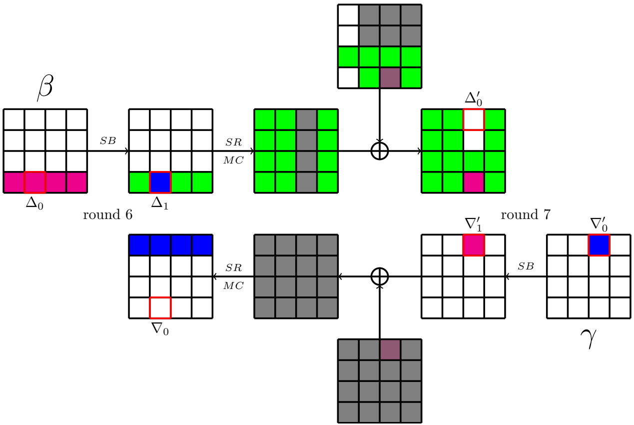
Improvement of the Attack [BN10]

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Idea

- The original attack [BN10] uses a similar idea of local collision. The boomerang switch is optimized in one round.
- With the help of BDT, we managed to extend the boomerang switch to 2-round by searching a new upper trail.

The 2-round E_m of the Improved Attack on [BN10]



Analysis

- No overlapped active S-box in the two S-box layer.
- However, specific values of Δ_1 and ∇'_1 are required.
- The switching probabilities of the corresponding two S-boxes are counted.

Results

Attacks	Improvement(Data&Time)
AES-192 [BN10]	$2^{1.3}$
AES-192 [BN09]	$2^{4.8}$
Deoxys-BC-256 [CHP+17]	$2^{1.6}$

Conclusion

- The slower is the diffusion in a cipher, the more rounds will be impacted by the switching effect.
- We introduced the BDT to easily evaluate the boomerang switch in multiple rounds.
- Improved attacks on 10-round AES-256, full-round AES-192 and reduced round Deoxys-BC-256.

THANK YOU!