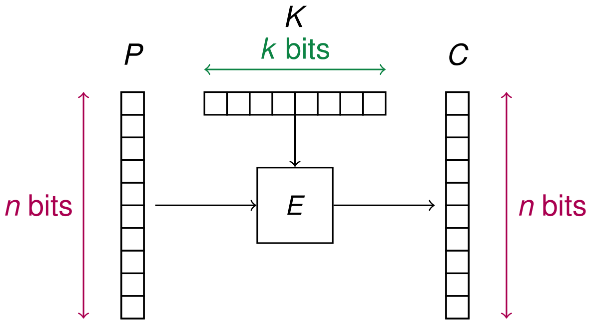
Truncated Boomerang Attacks and Application to AES-based Ciphers

Augustin Bariant, Gaëtan Leurent

INRIA, Paris

Journées C2 2023

Block Ciphers



$\forall K \in \{0,1\}^k$, $E_K : \{0,1\}^n \to \{0,1\}^n$ is a permutation.

- The most famous one: AES. [Daemen & Rijmen 1997]

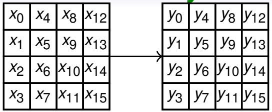
Modes of operation

Split messages in chunks of n bits and combine for a secure encryption.

The AES [Daemen & Rijmen, 1997]

- Selected by the NIST. [FIPS 197]
- States of 4x4 bytes.
- Key schedule not studied here.
- AES-128: 10 rounds.
- Security studied with cryptanalysis.

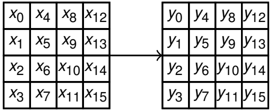
AddKey



rk: 16-byte round key

$y_i \leftarrow x_i + rk_i$

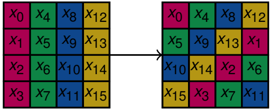
SubBytes



$S : \{0,1\}^8 \to \{0,1\}^8$

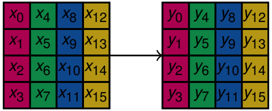
$y_i \leftarrow S(x_i)$

ShiftRows



$\text{Row}_i \leftarrow \text{Row}_i \lll i$

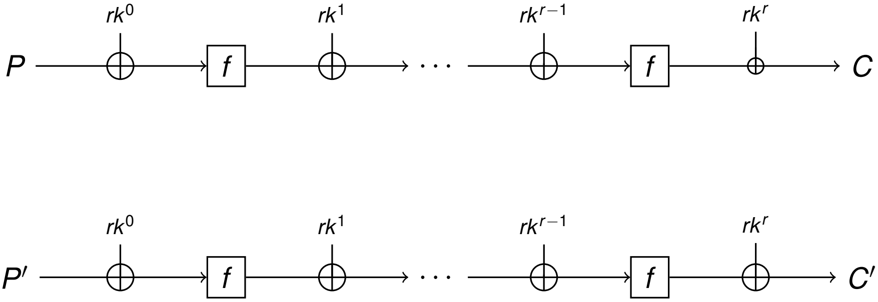
MixColumns



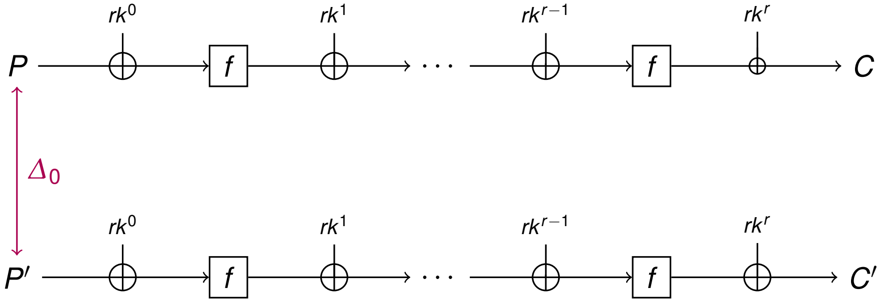
M: 4x4 matrix (MDS)

$\text{Col}_i \leftarrow M \times \text{Col}_i$

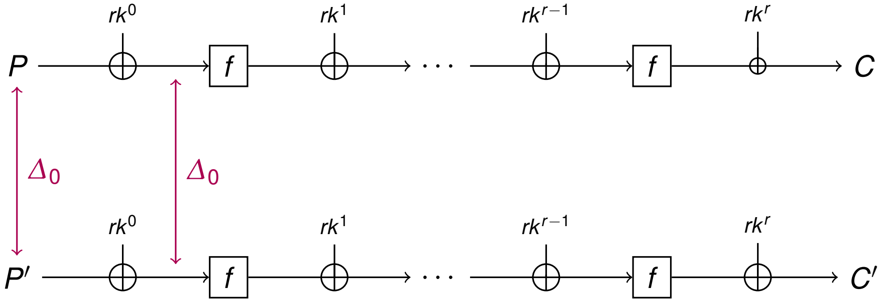
Differential cryptanalysis [Biham, ECS'91]



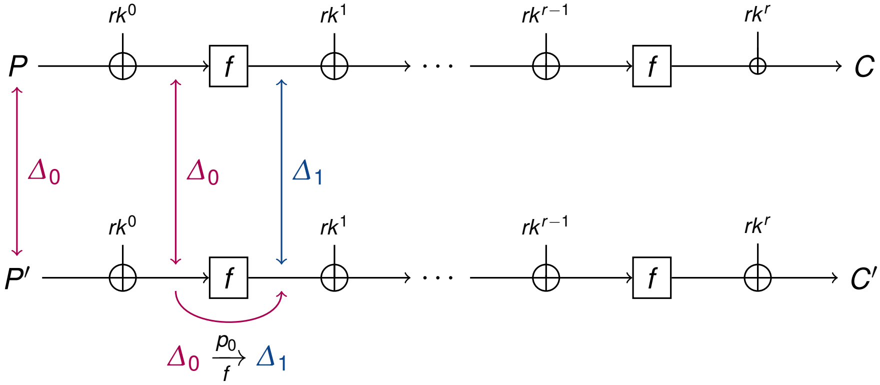
Differential cryptanalysis [Biham, ECS'91]



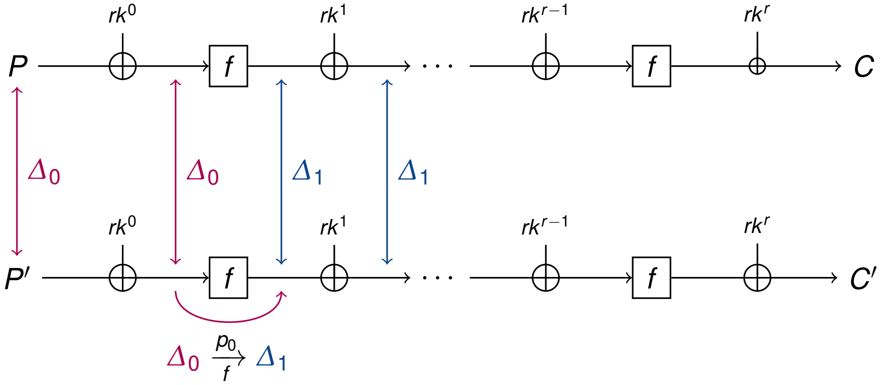
Differential cryptanalysis [Biham, ECS'91]



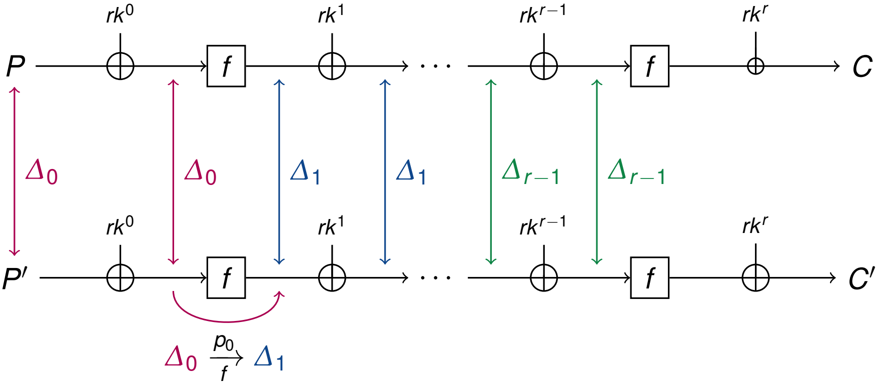
Differential cryptanalysis [Biham, ECS'91]



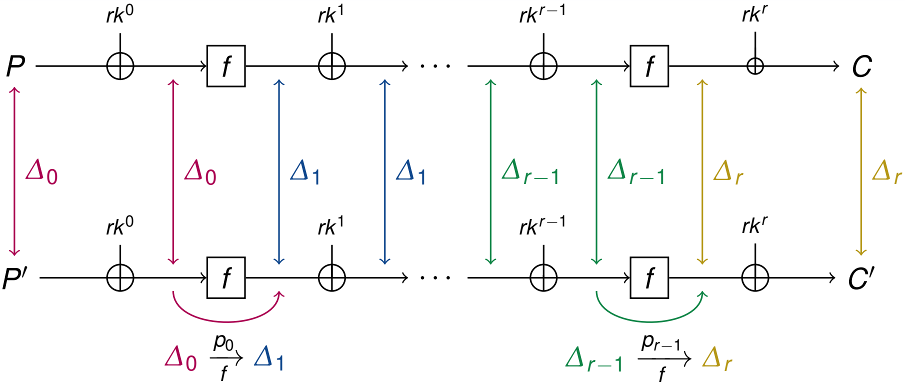
Differential cryptanalysis [Biham, ECS'91]



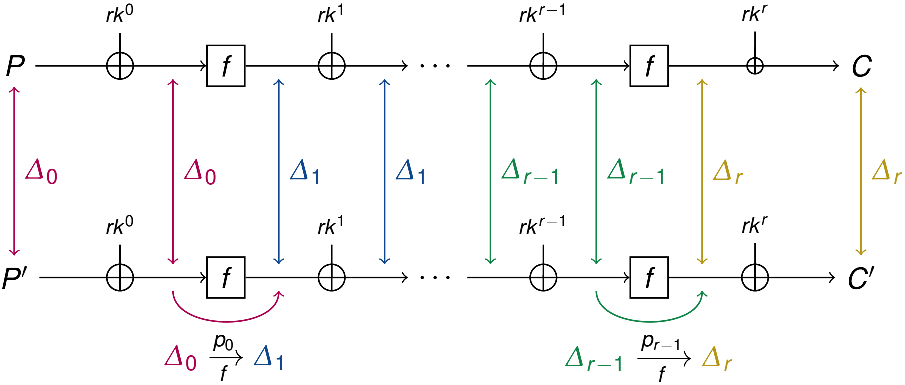
Differential cryptanalysis [Biham, ECS'91]



Differential cryptanalysis [Biham, ECS'91]

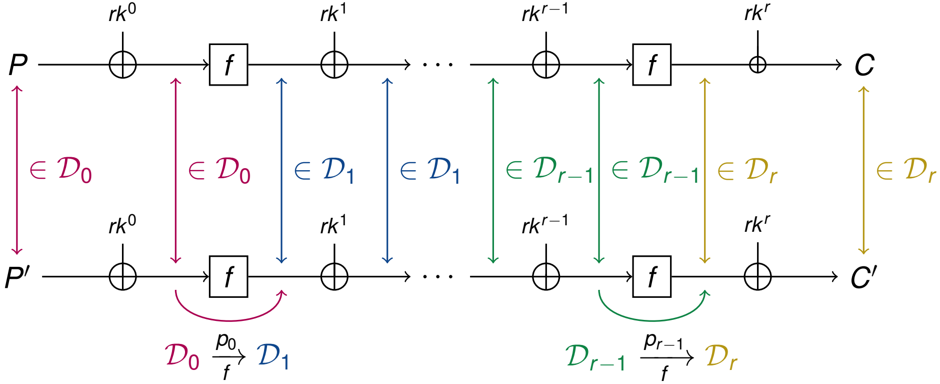


Differential cryptanalysis [Biham, ECS'91]



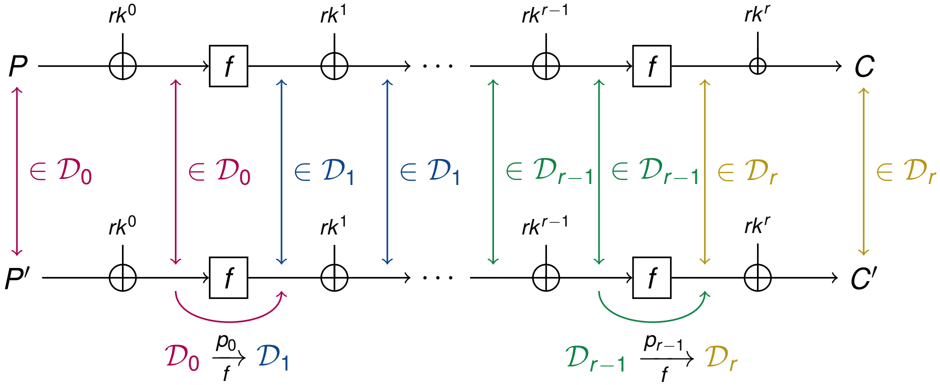
- $\Pr_{P \leftarrow \$} [E(P) + E(P \oplus \Delta_0) = \Delta_r] = p \approx \prod p_i$.
- Distinguisher if $p \gg 2^{-n}$.

Truncated differential cryptanalysis [Knudsen, FSE'94]



- $\mathcal{D}_i$ subspaces of $\mathbb{F}_2^n$.
- Trail probability $p \approx \prod p_i$.

Truncated differential cryptanalysis [Knudsen, FSE'94]



- $\mathcal{D}_i$ subspaces of $\mathbb{F}_2^n$.
- Trail probability $p \approx \prod p_i$.

Structures (if $\mathcal{D}_0$ is a vectorial subspace)

- Encrypt an affine space $P \oplus \mathcal{D}_0$.
- Look for $C, C' \in E(P \oplus \mathcal{D}_0)$ s.t. $C \oplus C' \in \mathcal{D}_r$.
- $|\mathcal{D}_0|$ encryptions but $|\mathcal{D}_0|^2/2$ pairs.

Truncated differentials: TLDR

- Thanks to sets of differences:
  - Capture multiple differentials → increased probability.
  - Structures → reduce complexity.

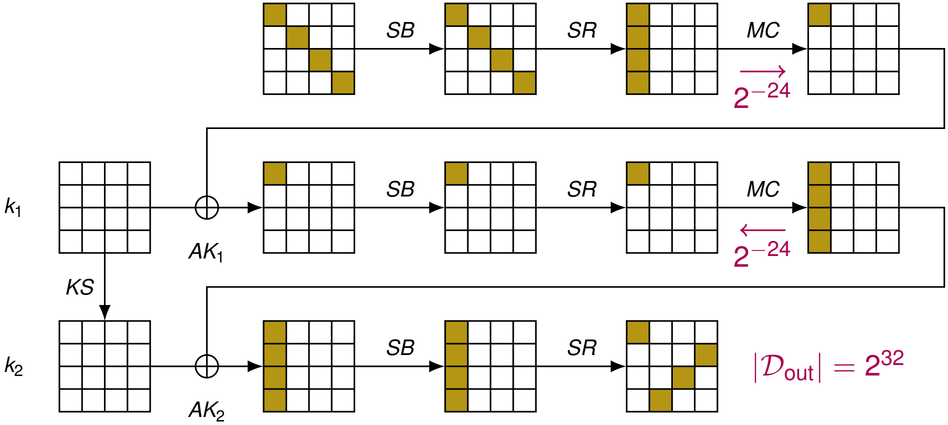
Notation

$$\mathcal{D}_{\text{in}} \overset{p}{\underset{f}{\longleftrightarrow}} \mathcal{D}_{\text{out}}$$

- Forward probability $\overrightarrow{p}$.
- Backward probability $\overleftarrow{p}$.

A Truncated differential of the AES

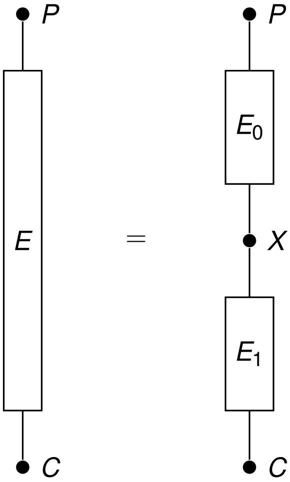
$|\mathcal{D}_{\text{in}}| = 2^{32}$



$|\mathcal{D}_{\text{out}}| = 2^{32}$

$\mathcal{D}_{\text{in}} \overset{p}{\underset{E}{\longleftrightarrow}} \mathcal{D}_{\text{out}}$ $\qquad \vec{p} = \overleftarrow{p} = 2^{-24}$

The Boomerang Attack [Wagner, FSE'99]

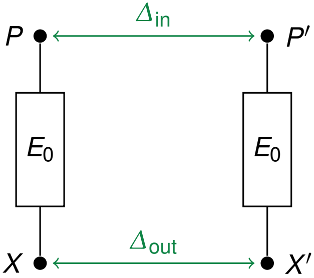


- Prerequisites for the attack:
  - $E = E_1 \circ E_0$
  - $\Delta_{in} \xrightarrow[E_0]{p} \Delta_{out}$
  - $\nabla_{in} \xrightarrow[E_1]{q} \nabla_{out}$

The Boomerang Attack

- Select a random P.
- Select P' s.t. $P \oplus P' = \Delta_{\text{in}}$.

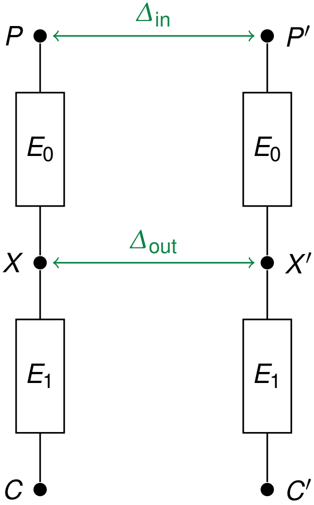
The Boomerang Attack



$$\Delta_{\text{in}} \xrightarrow[E_0]{p} \Delta_{\text{out}}$$

- Select a random P.
- Select P' s.t. $P \oplus P' = \Delta_{\text{in}}$.
- $\Pr[X \oplus X' = \Delta_{\text{out}}] = p$.

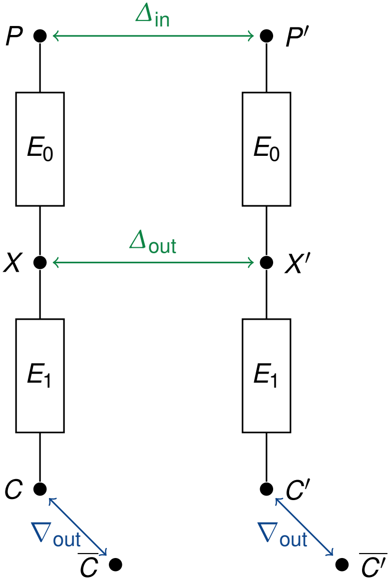
The Boomerang Attack



$$\Delta_{\text{in}} \xrightarrow[E_0]{p} \Delta_{\text{out}}$$

- Select a random P.
- Select P' s.t. $P \oplus P' = \Delta_{\text{in}}$.
- $\Pr[X \oplus X' = \Delta_{\text{out}}] = p$.

The Boomerang Attack

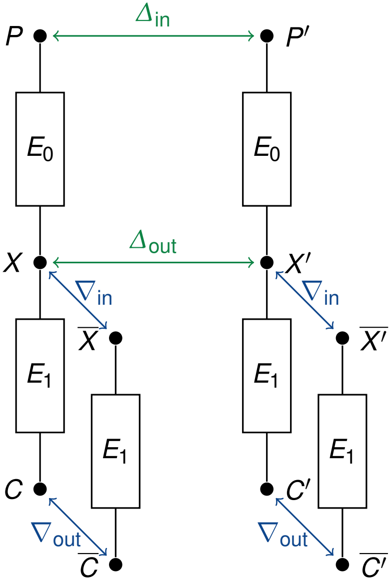


$$\Delta_{\text{in}} \xrightarrow[E_0]{p} \Delta_{\text{out}}$$

$$\nabla_{\text{in}} \xrightarrow[E_1]{q} \nabla_{\text{out}}$$

- Select a random P.
- Select P' s.t. $P \oplus P' = \Delta_{\text{in}}$.
- $\Pr[X \oplus X' = \Delta_{\text{out}}] = p$.
- Select $(\overline{C}, \overline{C'})$ s.t. $C \oplus \overline{C} = C' \oplus \overline{C'} = \nabla_{\text{out}}$.

The Boomerang Attack

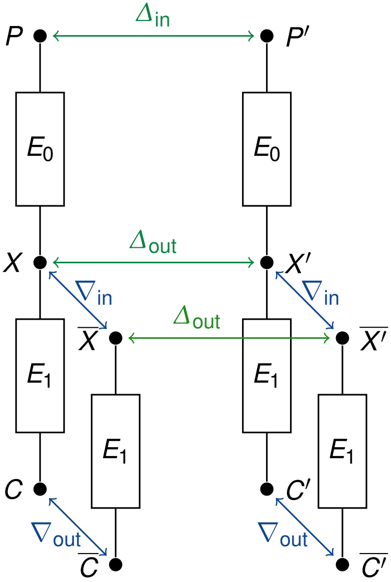


$$\Delta_{\text{in}} \xrightarrow[E_0]{p} \Delta_{\text{out}}$$

$$\nabla_{\text{in}} \xrightarrow[E_1]{q} \nabla_{\text{out}}$$

- Select a random P.
- Select P' s.t. $P \oplus P' = \Delta_{\text{in}}$.
- $\Pr[X \oplus X' = \Delta_{\text{out}}] = p$.
- Select $(\overline{C}, \overline{C'})$ s.t. $C \oplus \overline{C} = C' \oplus \overline{C'} = \nabla_{\text{out}}$.
- $\Pr[X \oplus \overline{X} = \nabla_{\text{in}}] = q$.
- $\Pr[X' \oplus \overline{X'} = \nabla_{\text{in}}] = q$.

The Boomerang Attack

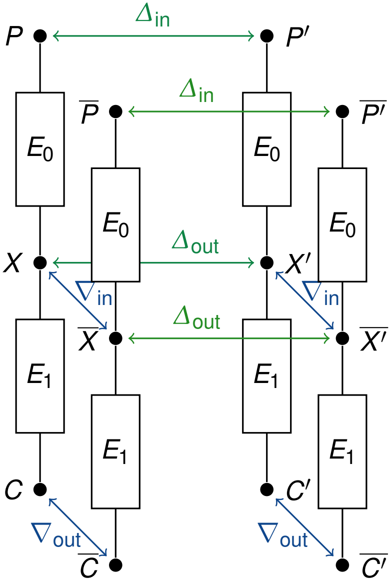


$\Delta_{in} \xrightarrow[E_0]{p} \Delta_{out}$

$\nabla_{in} \xrightarrow[E_1]{q} \nabla_{out}$

- Select a random P.
- Select P' s.t. $P \oplus P' = \Delta_{in}$.
- $\Pr[X \oplus X' = \Delta_{out}] = p$.
- Select $(\overline{C}, \overline{C'})$ s.t. $C \oplus \overline{C} = C' \oplus \overline{C'} = \nabla_{out}$.
- $\Pr[X \oplus \overline{X} = \nabla_{in}] = q$.
- $\Pr[X' \oplus \overline{X'} = \nabla_{in}] = q$.
- If this holds, then $\overline{X} \oplus \overline{X'} = \Delta_{out}$.

The Boomerang Attack

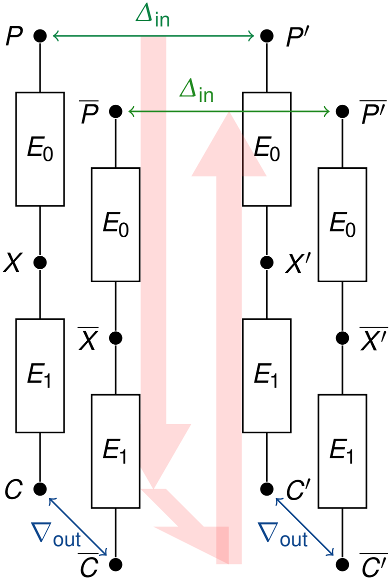


$$\Delta_{in} \xrightarrow[E_0]{p} \Delta_{out}$$

$$\nabla_{in} \xrightarrow[E_1]{q} \nabla_{out}$$

- Select a random P.
- Select P' s.t. $P \oplus P' = \Delta_{in}$.
- $\Pr[X \oplus X' = \Delta_{out}] = p$.
- Select $(\overline{C}, \overline{C'})$ s.t. $C \oplus \overline{C} = C' \oplus \overline{C'} = \nabla_{out}$.
- $\Pr[X \oplus \overline{X} = \nabla_{in}] = q$.
- $\Pr[X' \oplus \overline{X'} = \nabla_{in}] = q$.
- If this holds, then $\overline{X} \oplus \overline{X'} = \Delta_{out}$.
- $\Pr[\overline{P} \oplus \overline{P'} = \Delta_{in}] = p$.

The Boomerang Attack



$\Delta_{\text{in}} \xrightarrow[E_0]{p} \Delta_{\text{out}}$

$\nabla_{\text{in}} \xrightarrow[E_1]{q} \nabla_{\text{out}}$

- Select a random P.
- Select P' s.t. $P \oplus P' = \Delta_{\text{in}}$.
- $\Pr[X \oplus X' = \Delta_{\text{out}}] = p$.
- Select $(\overline{C}, \overline{C'})$ s.t. $C \oplus \overline{C} = C' \oplus \overline{C'} = \nabla_{\text{out}}$.
- $\Pr[X \oplus \overline{X} = \nabla_{\text{in}}] = q$.
- $\Pr[X' \oplus \overline{X'} = \nabla_{\text{in}}] = q$.
- If this holds, then $\overline{X} \oplus \overline{X'} = \Delta_{\text{out}}$.
- $\Pr[\overline{P} \oplus \overline{P'} = \Delta_{\text{in}}] = p$.

Total boomerang probability: $p^2 q^2$.

$p^2 q^2 \gg 2^{-n} \rightarrow$ Distinguisher

Our results

1. Analysis of boomerangs with truncated differentials. [Wagner, FSE'99]
2. Application: improved boomerang attack on 6-round AES.
3. Best attacks on several AES-based tweakable block ciphers:
   - TNT-AES. [Bao, Guo, Guo & Song, EC'20]
   - Kiasu-BC. [Jean, Nikolić & Peyrin, AC'14]
   - Deoxys-BC. [Jean, Nikolić & Peyrin, AC'14]

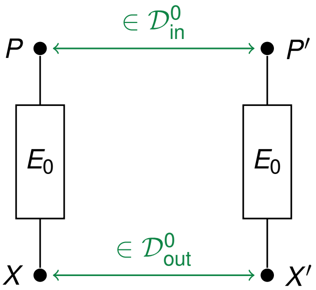
The Truncated Boomerang Framework [This work]

$$P \bullet \xleftrightarrow{\in \mathcal{D}^0_{\text{in}}} \bullet P'$$

- Pick a P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{\text{in}}$.

$$\mathcal{D}^0_{\text{in}} \xleftrightarrow[E_0]{p} \mathcal{D}^0_{\text{out}}$$

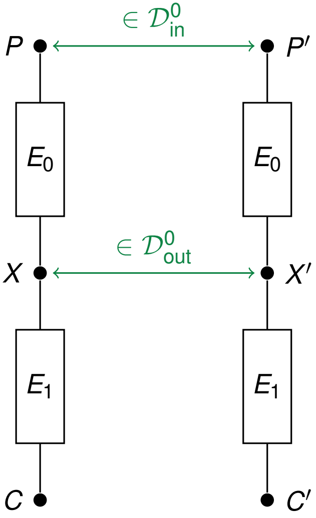
The Truncated Boomerang Framework [This work]



$\mathcal{D}^0_{in} \overset{p}{\underset{E_0}{\longleftrightarrow}} \mathcal{D}^0_{out}$

- Pick a P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{in}$.
- For $P, P' \in P_0 \oplus \mathcal{D}^0_{in}$, $\Pr[X \oplus X' \in \mathcal{D}^0_{out}] = \vec{p}$.

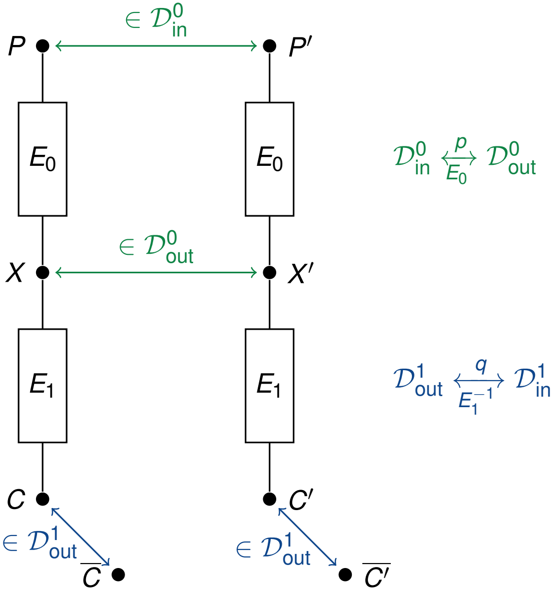
The Truncated Boomerang Framework [This work]



$$\mathcal{D}^0_{in} \overset{p}{\underset{E_0}{\longleftrightarrow}} \mathcal{D}^0_{out}$$

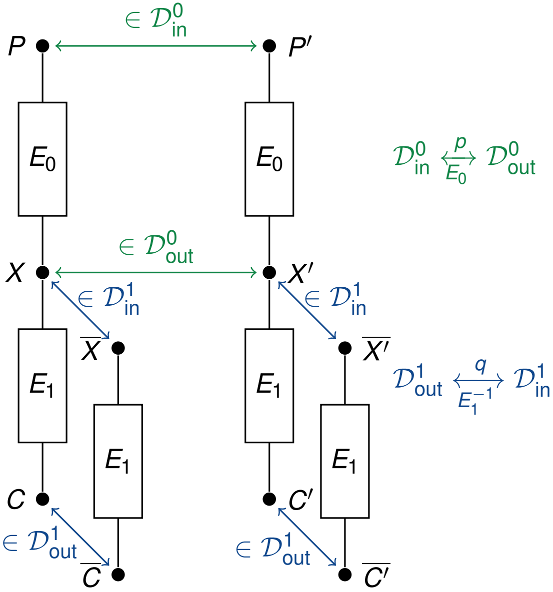
- Pick a P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{in}$.
- For $P, P' \in P_0 \oplus \mathcal{D}^0_{in}$, $\Pr[X \oplus X' \in \mathcal{D}^0_{out}] = \vec{p}$.

The Truncated Boomerang Framework [This work]



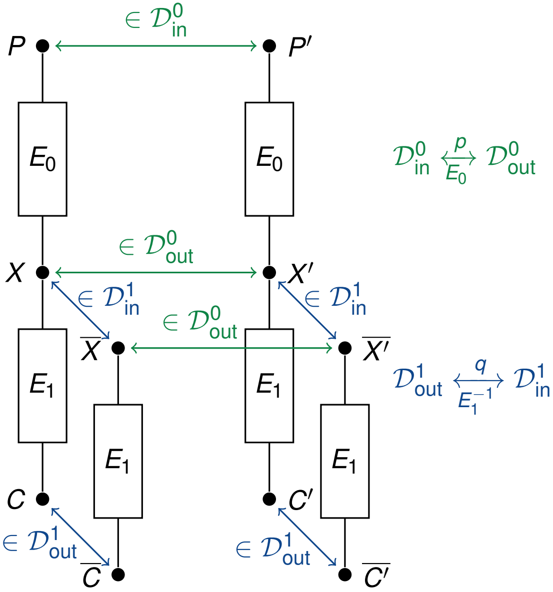
- Pick a P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{in}$.
- For $P, P' \in P_0 \oplus \mathcal{D}^0_{in}$, $\Pr[X \oplus X' \in \mathcal{D}^0_{out}] = \vec{p}$.
- For each $C \in E(P_0 \oplus \mathcal{D}^0_{in})$, decrypt a structure $C \oplus \mathcal{D}^1_{out}$.

The Truncated Boomerang Framework [This work]



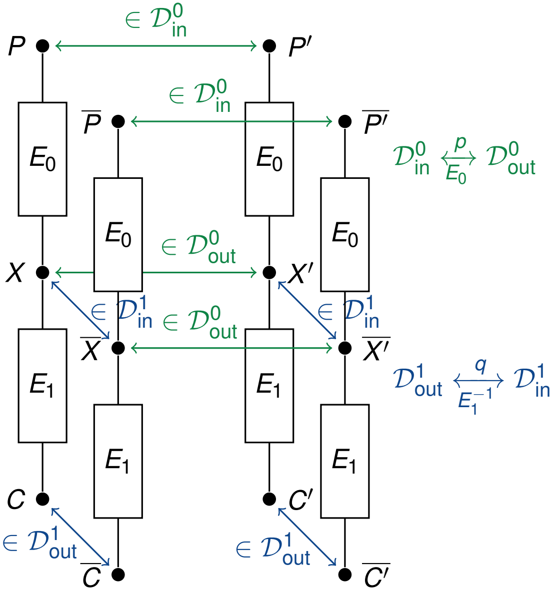
- Pick a P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{in}$.
- For $P, P' \in P_0 \oplus \mathcal{D}^0_{in}$, $\Pr[X \oplus X' \in \mathcal{D}^0_{out}] = \vec{p}$.
- For each $C \in E(P_0 \oplus \mathcal{D}^0_{in})$, decrypt a structure $C \oplus \mathcal{D}^1_{out}$.
- For $\overline{C} \in C \oplus \mathcal{D}^1_{out}$, $\Pr[X \oplus \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- For $\overline{C'} \in C' \oplus \mathcal{D}^1_{out}$, $\Pr[X' \oplus \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$.

The Truncated Boomerang Framework [This work]



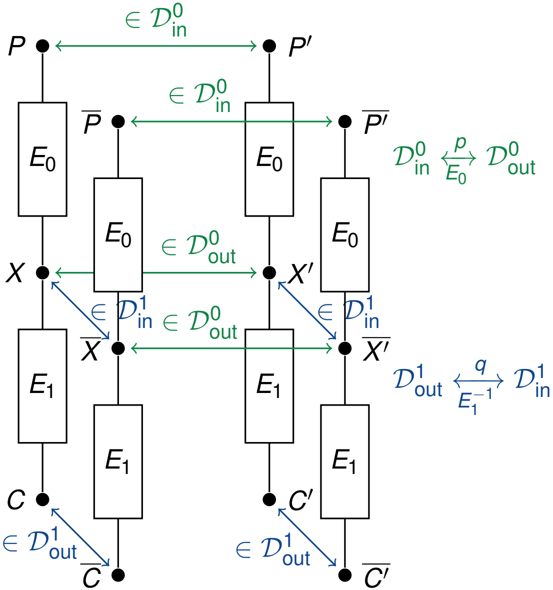
- Pick a P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{\text{in}}$.
- For $P, P' \in P_0 \oplus \mathcal{D}^0_{\text{in}}$, $\Pr[X \oplus X' \in \mathcal{D}^0_{\text{out}}] = \vec{p}$.
- For each $C \in E(P_0 \oplus \mathcal{D}^0_{\text{in}})$, decrypt a structure $C \oplus \mathcal{D}^1_{\text{out}}$.
- For $\overline{C} \in C \oplus \mathcal{D}^1_{\text{out}}$, $\Pr[X \oplus \overline{X} \in \mathcal{D}^1_{\text{in}}] = \overleftarrow{q}$
- For $\overline{C'} \in C' \oplus \mathcal{D}^1_{\text{out}}$, $\Pr[X' \oplus \overline{X'} \in \mathcal{D}^1_{\text{in}}] = \overleftarrow{q}$.
- $\Pr[\overline{X} \oplus \overline{X'} \in \mathcal{D}^0_{\text{out}}] = r \geq |\mathcal{D}^1_{\text{in}}|^{-1}$.

The Truncated Boomerang Framework [This work]



- Pick a P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{in}$.
- For $P, P' \in P_0 \oplus \mathcal{D}^0_{in}$, $\Pr[X \oplus X' \in \mathcal{D}^0_{out}] = \vec{p}$.
- For each $C \in E(P_0 \oplus \mathcal{D}^0_{in})$, decrypt a structure $C \oplus \mathcal{D}^1_{out}$.
- For $\overline{C} \in C \oplus \mathcal{D}^1_{out}$, $\Pr[X \oplus \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- For $\overline{C'} \in C' \oplus \mathcal{D}^1_{out}$, $\Pr[X' \oplus \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$.
- $\Pr[\overline{X} \oplus \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$.
- $\Pr[\overline{P} \oplus \overline{P'} \in \mathcal{D}^0_{in}] = \overleftarrow{p}$.

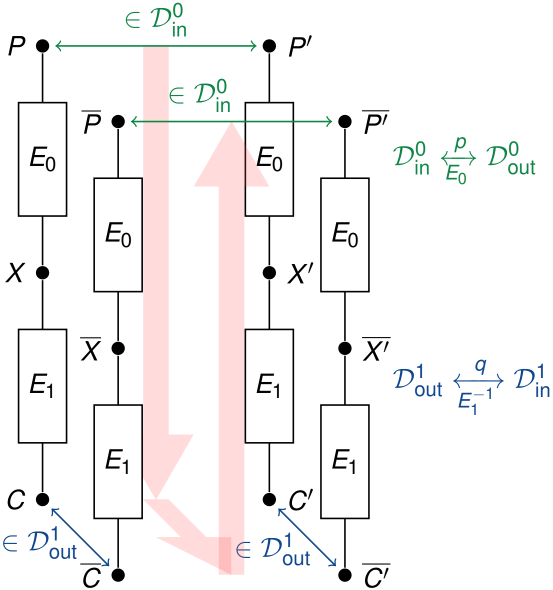
The Truncated Boomerang Framework [This work]



- Pick a P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{in}$.
- For $P, P' \in P_0 \oplus \mathcal{D}^0_{in}$, $\Pr[X \oplus X' \in \mathcal{D}^0_{out}] = \vec{p}$.
- For each $C \in E(P_0 \oplus \mathcal{D}^0_{in})$, decrypt a structure $C \oplus \mathcal{D}^1_{out}$.
- For $\overline{C} \in C \oplus \mathcal{D}^1_{out}$, $\Pr[X \oplus \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- For $\overline{C'} \in C' \oplus \mathcal{D}^1_{out}$, $\Pr[X' \oplus \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$.
- $\Pr[\overline{X} \oplus \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$.
- $\Pr[\overline{P} \oplus \overline{P'} \in \mathcal{D}^0_{in}] = \overleftarrow{p}$.

- Total probability: $p_b = \vec{p} \cdot \overleftarrow{q}^2 \cdot r \cdot \overleftarrow{p}$.

The Truncated Boomerang Framework [This work]



Summary

1. Select a random P_0 and encrypt a structure $P_0 \oplus \mathcal{D}^0_{in}$
2. For each $C \in E(P_0 \oplus \mathcal{D}^0_{in})$, decrypt a structure $C \oplus \mathcal{D}^1_{out}$.
3. Look for $\overline{P}, \overline{P'} \in E^{-1}(E(P_0 \oplus \mathcal{D}^0_{in}) \oplus \mathcal{D}^1_{out})$ s.t. $\overline{P} \oplus \overline{P'} \in \mathcal{D}^0_{in}$.
4. If needed, repeat with a new P_0.

- Total probability: $p_b = \vec{p} \cdot \overleftarrow{q}^2 \cdot r \cdot \overleftarrow{p}$.
- Random probability: $p_\$ = |\mathcal{D}^0_{in}| \cdot 2^{-n}$.
- Total structure size: $|\mathcal{D}^0_{in}||\mathcal{D}^1_{out}|$.

Distinguisher: Distinguishing property

- Boomerang probability $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$.
- Random probability $p_\$ = |\mathcal{D}^0_{\text{in}}| \cdot 2^{-n}$.

Distinguishing property

Probability that a quartet returns:

- Cipher E $\rightarrow p_\$ + p_b$.
- Random function $\rightarrow p_\$$.

Distinguisher: Analysis

- Signal to noise $\sigma = p_b / p_\$$.
- S structures of size $|\mathcal{D}^0_{\text{in}}| \cdot |\mathcal{D}^1_{\text{out}}|$.
- $Q = S \times |\mathcal{D}^0_{\text{in}}|^2 \cdot |\mathcal{D}^1_{\text{out}}|^2 / 2$ quartets.

Distinguisher: Analysis

- Signal to noise $\sigma = p_b / p_\$$.
- S structures of size $|\mathcal{D}^0_{\text{in}}| \cdot |\mathcal{D}^1_{\text{out}}|$.
- $Q = S \times |\mathcal{D}^0_{\text{in}}|^2 \cdot |\mathcal{D}^1_{\text{out}}|^2 / 2$ quartets.

If $\sigma \gg 1$

- A few good quartets are sufficient.
- $Q = \mathcal{O}(1/p_b)$ quartets needed.

If $\sigma \ll 1$

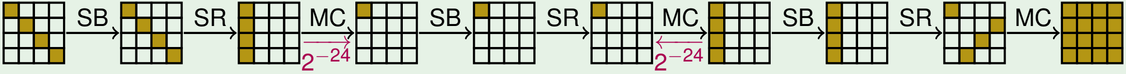
- More wrong quartets than good.
- $Q = \mathcal{O}(1/\sigma p_b)$ quartets needed.

- Time and data complexity:

$$T = D = \frac{2Q}{|\mathcal{D}^0_{\text{in}}| \cdot |\mathcal{D}^1_{\text{out}}|}$$

Example: 6-round AES distinguisher

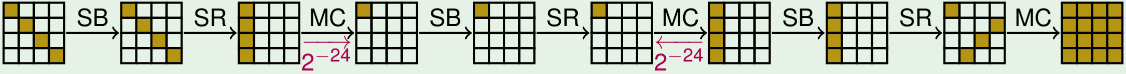
3-round AES truncated trail for E_0 and E_1



- $\vec{q} = \overleftarrow{q} = \vec{p} = \overleftarrow{p} = 2^{-24}$
- $|\mathcal{D}^0_{\text{out}}| = |\mathcal{D}^0_{\text{in}}| = |\mathcal{D}^1_{\text{out}}| = |\mathcal{D}^1_{\text{in}}| = 2^{32}$

Example: 6-round AES distinguisher

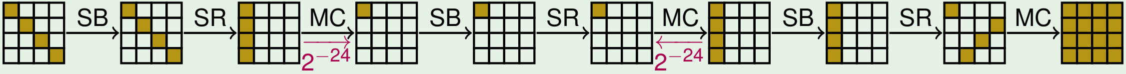
3-round AES truncated trail for E_0 and E_1



- $\vec{q} = \overleftarrow{q} = \vec{p} = \overleftarrow{p} = 2^{-24}$
- $r = |\mathcal{D}^1_{\text{in}}|^{-1} = 2^{-32}$
- $|\mathcal{D}^0_{\text{out}}| = |\mathcal{D}^0_{\text{in}}| = |\mathcal{D}^1_{\text{out}}| = |\mathcal{D}^1_{\text{in}}| = 2^{32}$

Example: 6-round AES distinguisher

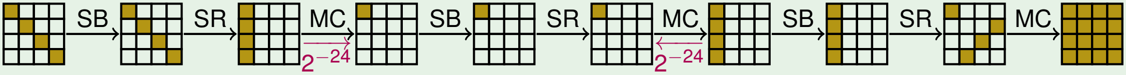
3-round AES truncated trail for E_0 and E_1



- $\overrightarrow{q} = \overleftarrow{q} = \overrightarrow{p} = \overleftarrow{p} = 2^{-24}$
- $r = |\mathcal{D}^1_{\text{in}}|^{-1} = 2^{-32}$
- $p_b = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r = 2^{-128}$
- $|\mathcal{D}^0_{\text{out}}| = |\mathcal{D}^0_{\text{in}}| = |\mathcal{D}^1_{\text{out}}| = |\mathcal{D}^1_{\text{in}}| = 2^{32}$

Example: 6-round AES distinguisher

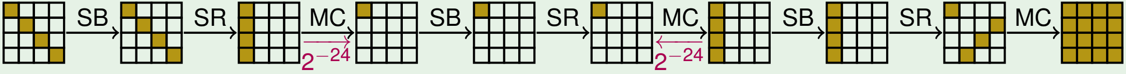
3-round AES truncated trail for E_0 and E_1



- $\vec{q} = \overleftarrow{q} = \vec{p} = \overleftarrow{p} = 2^{-24}$
- $r = |\mathcal{D}^1_{\text{in}}|^{-1} = 2^{-32}$
- $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r = 2^{-128}$
- $|\mathcal{D}^0_{\text{out}}| = |\mathcal{D}^0_{\text{in}}| = |\mathcal{D}^1_{\text{out}}| = |\mathcal{D}^1_{\text{in}}| = 2^{32}$
- $p_\$ = |\mathcal{D}^0_{\text{in}}| \cdot 2^{-n} = 2^{-96}$

Example: 6-round AES distinguisher

3-round AES truncated trail for E_0 and E_1

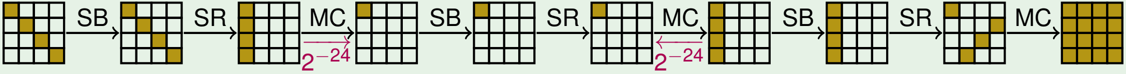


- $\vec{q} = \overleftarrow{q} = \vec{p} = \overleftarrow{p} = 2^{-24}$
- $r = |\mathcal{D}^1_{in}|^{-1} = 2^{-32}$
- $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r = 2^{-128}$
- $|\mathcal{D}^0_{out}| = |\mathcal{D}^0_{in}| = |\mathcal{D}^1_{out}| = |\mathcal{D}^1_{in}| = 2^{32}$
- $p_\$ = |\mathcal{D}^0_{in}| \cdot 2^{-n} = 2^{-96}$

$$\sigma = \frac{p_b}{p_\$} = 2^{-32} \ll 1$$

Example: 6-round AES distinguisher

3-round AES truncated trail for E_0 and E_1



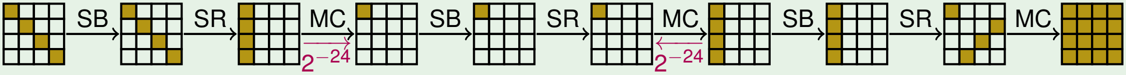
- $\vec{q} = \overleftarrow{q} = \vec{p} = \overleftarrow{p} = 2^{-24}$
- $r = |\mathcal{D}^1_{\text{in}}|^{-1} = 2^{-32}$
- $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r = 2^{-128}$
- $|\mathcal{D}^0_{\text{out}}| = |\mathcal{D}^0_{\text{in}}| = |\mathcal{D}^1_{\text{out}}| = |\mathcal{D}^1_{\text{in}}| = 2^{32}$
- $p_\$ = |\mathcal{D}^0_{\text{in}}| \cdot 2^{-n} = 2^{-96}$

$$\sigma = \frac{p_b}{p_\$} = 2^{-32} \ll 1$$

- Choose $Q = 2^{160}$ quartets.

Example: 6-round AES distinguisher

3-round AES truncated trail for E_0 and E_1



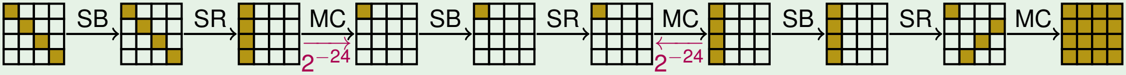
- $\overrightarrow{q} = \overleftarrow{q} = \overrightarrow{p} = \overleftarrow{p} = 2^{-24}$
- $r = |\mathcal{D}^1_{\text{in}}|^{-1} = 2^{-32}$
- $p_b = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r = 2^{-128}$
- $|\mathcal{D}^0_{\text{out}}| = |\mathcal{D}^0_{\text{in}}| = |\mathcal{D}^1_{\text{out}}| = |\mathcal{D}^1_{\text{in}}| = 2^{32}$
- $p_\$ = |\mathcal{D}^0_{\text{in}}| \cdot 2^{-n} = 2^{-96}$

$$\sigma = \frac{p_b}{p_\$} = 2^{-32} \ll 1$$

- Choose $Q = 2^{160}$ quartets.
- $Q \cdot p_b = 2^{32}$ good returning quartets.
- $Q \cdot p_\$ = 2^{64}$ wrong returning quartets.

Example: 6-round AES distinguisher

3-round AES truncated trail for E_0 and E_1



- $\overrightarrow{q} = \overleftarrow{q} = \overrightarrow{p} = \overleftarrow{p} = 2^{-24}$
- $r = |\mathcal{D}^1_{\text{in}}|^{-1} = 2^{-32}$
- $p_b = \overrightarrow{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r = 2^{-128}$
- $|\mathcal{D}^0_{\text{out}}| = |\mathcal{D}^0_{\text{in}}| = |\mathcal{D}^1_{\text{out}}| = |\mathcal{D}^1_{\text{in}}| = 2^{32}$
- $p_\$ = |\mathcal{D}^0_{\text{in}}| \cdot 2^{-n} = 2^{-96}$

$$\sigma = \frac{p_b}{p_\$} = 2^{-32} \ll 1$$

- Choose $Q = 2^{160}$ quartets.
- $Q \cdot p_b = 2^{32}$ good returning quartets.
- $Q \cdot p_\$ = 2^{64}$ wrong returning quartets.

Possible to detect signal from noise.

Example: 6-round AES distinguisher

Distinguisher

Throw $Q = 2^{160}$ quartets using structures of size $|\mathcal{D}^0_{\text{in}}||\mathcal{D}^1_{\text{out}}| = 2^{64}$:

- If $\approx 2^{64}$ quartets return $\rightarrow$ random function.
- If $> 2^{64} + 2^{31}$ quartets return $\rightarrow$ 6R AES.

$$T = D \approx \frac{Q}{|\mathcal{D}^0_{\text{in}}||\mathcal{D}^1_{\text{out}}|} = 2^{96}.$$

Including Key recovery

- Usual approach: add rounds before/after distinguisher.
- Our approach: same number of rounds, use key as extra distinguisher.

Including Key recovery

- Usual approach: add rounds before/after distinguisher.
- Our approach: same number of rounds, use key as extra distinguisher.
- Deduce key information from a returning quartet.
  - Example: $(P, P') \to (X, X')$ follows E_0 $\to$ only possible for certain keys.
  - Generalization: $(P, P', \overline{P}, \overline{P'})$ suggests ℓ candidates of κ key bits ($\ell \ll 2^\kappa$).

Including Key recovery

- Usual approach: add rounds before/after distinguisher.
- Our approach: same number of rounds, use key as extra distinguisher.
- Deduce key information from a returning quartet.
  - Example: $(P, P') \to (X, X')$ follows E_0 $\to$ only possible for certain keys.
  - Generalization: $(P, P', \overline{P}, \overline{P'})$ suggests ℓ candidates of κ key bits ($\ell \ll 2^\kappa$).

If $\sigma \gg 1$

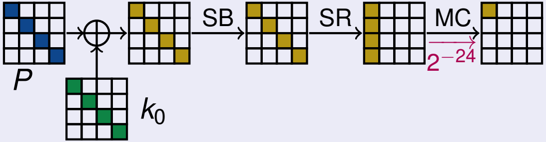
- Collect a few right quartets.
- For each quartet, recover ℓ candidates for κ key bits.
- Select the candidate suggested each time.

If $\sigma \ll 1$

- Initialize 2^κ key counters.
- Collect many quartets.
- For each quartet:
  - Increment ℓ key counters.
- Right key counter higher than random.

Example: 6-round AES boomerang

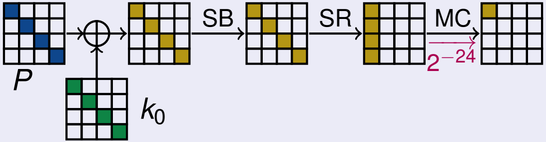
First round



- Diagonal of k_0 (32 bits):
  - $(P, P') \to 2^8$ candidates.
  - $(\overline{P}, \overline{P'}) \to 2^8$ candidates.
  - 2^{-16} candidates for both.

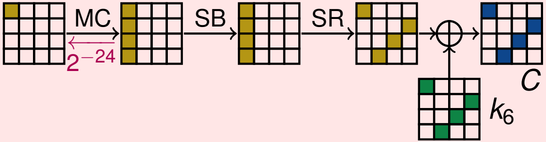
Example: 6-round AES boomerang

First round



- Diagonal of k_0 (32 bits):
  - $(P, P') \to 2^8$ candidates.
  - $(\overline{P}, \overline{P'}) \to 2^8$ candidates.
  - 2^{-16} candidates for both.

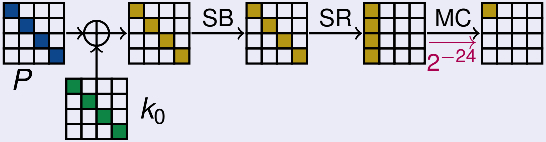
Last round



- Anti-diagonal of k_6 (32 bits):
  - $(C, \overline{C}) \to 2^8$ candidates.
  - $(C', \overline{C'}) \to 2^8$ candidates
  - 2^{-16} candidates for both.

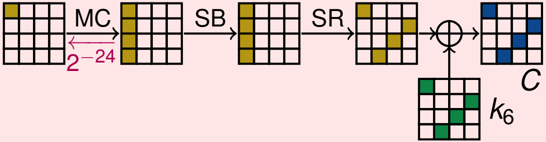
Example: 6-round AES boomerang

First round



- Diagonal of k_0 (32 bits):
  - $(P, P') \to 2^8$ candidates.
  - $(\overline{P}, \overline{P'}) \to 2^8$ candidates.
  - 2^{-16} candidates for both.

Last round

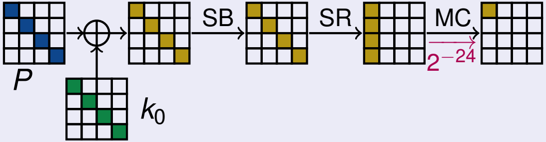


- Anti-diagonal of k_6 (32 bits):
  - $(C, \overline{C}) \to 2^8$ candidates.
  - $(C', \overline{C'}) \to 2^8$ candidates
  - 2^{-16} candidates for both.

- Total: $\ell = 2^{-32}$ candidates for $\kappa = 64$ bits of key.

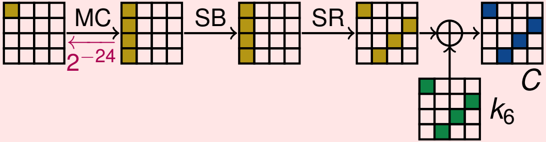
Example: 6-round AES boomerang

First round



- Diagonal of k_0 (32 bits):
  - $(P, P') \to 2^8$ candidates.
  - $(\overline{P}, \overline{P'}) \to 2^8$ candidates.
  - 2^{-16} candidates for both.

Last round



- Anti-diagonal of k_6 (32 bits):
  - $(C, \overline{C}) \to 2^8$ candidates.
  - $(C', \overline{C'}) \to 2^8$ candidates
  - 2^{-16} candidates for both.

- Total: $\ell = 2^{-32}$ candidates for $\kappa = 64$ bits of key.
- Random counter increased with probability $\frac{\ell}{2^\kappa} = 2^{-96}$.
- High probability of success with 4 right quartets ($D = T = 2^{67}$).

6-round AES results

	Type	Data		Time	Ref
Distinguishers	Yoyo	$2^{122.8}$	ACC	$2^{121.8}$	[AC:RonBarHel17]
	Exchange attack	$2^{88.2}$	CP	$2^{88.2}$	[AC:BarRon19]
	Exchange attack	2^{84}	ACC	2^{83}	[EPRINT:Bardeh19]
	Truncated differential	$2^{89.4}$	CP	$2^{96.5}$	[ToSC:BaoGuoLis20]
	Truncated boomerang	2^{87}	ACC	2^{87}	This work
Key-recovery	Square	2^{32}	CP	2^{71}	[FSE:DaeKnuRij97]
	Partial-sum	2^{32}	CP	2^{48}	[FSE:FKLSSWW00]
	Boomerang	2^{71}	ACC	2^{71}	[biryukov2004boomerang]
	Mixture	2^{26}	CP	2^{80}	[JC:BDKRS20]
	Retracing boomerang	2^{55}	ACC	2^{80}	[EC:DKRS20]
	Boomeyong	$2^{79.7}$	ACC	2^{78}	[ToSC:RahSahPau21]
	Truncated boomerang	2^{59}	ACC	2^{61}	This work

Conclusion

1. Analysis of truncated bommerang attacks.
2. Improving boomerangs on 6-round AES.
3. Applications
   - Best attack on KIASU-BC.
   - Best attacks on Deoxys-BC using MILP.
   - Distinguisher on full TNT-AES.

Thank you for your attention