Truncated Boomerang Attacks and Application to AES-based Ciphers

Augustin Bariant, Gaëtan Leurent

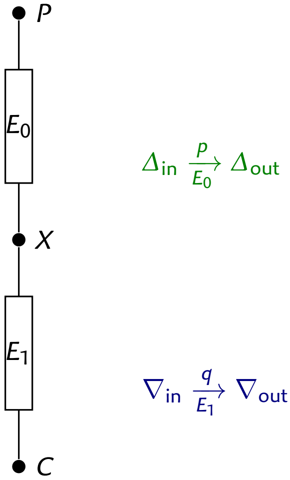
INRIA, Paris

Eurocrypt 2023

The AES

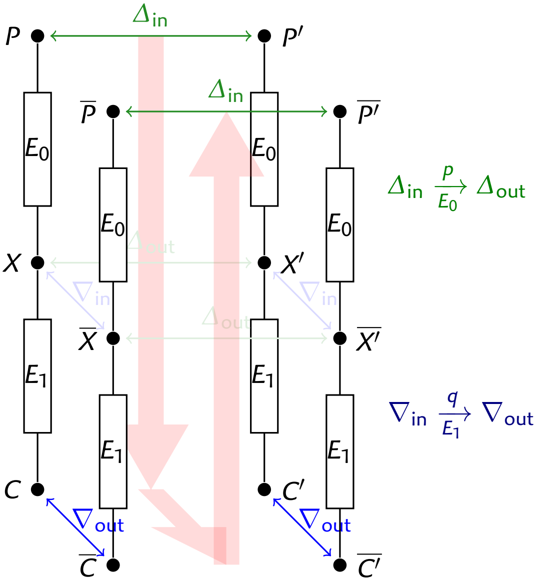
- AES is the most widely used block cipher today
  - Designed in 1999 [Daemen & Rijmen]
  - Selected by NIST [FIPS 197]
- Round function and reduced versions reused in many context
  - Hash function: Grøstl (SHA-3 finalist), LED, ECHO
  - Stream cipher: LEX
  - MACs: Alpha-MAC
  - Tweakable block ciphers: Deoxys (CAESAR portfolio), KIASU, TNT
  - AEAD: Aegis (CAESAR portfolio), Tiaoxin
- Need cryptanalysis to evaluate security
  - New and old attack techniques
  - Many recent results!

The Boomerang Attack [Wagner, FSE'99]



- Combine two short differentials instead of using a long one.
  - $E = E_1 \circ E_0$
  - $\Delta_{in} \xrightarrow[E_0]{p} \Delta_{out}$
  - $\nabla_{in} \xrightarrow[E_1]{q} \nabla_{out}$
- Uses an encryption oracle and decryption oracle
  - Adaptive attack
- Build quartets

Boomerang Quartet



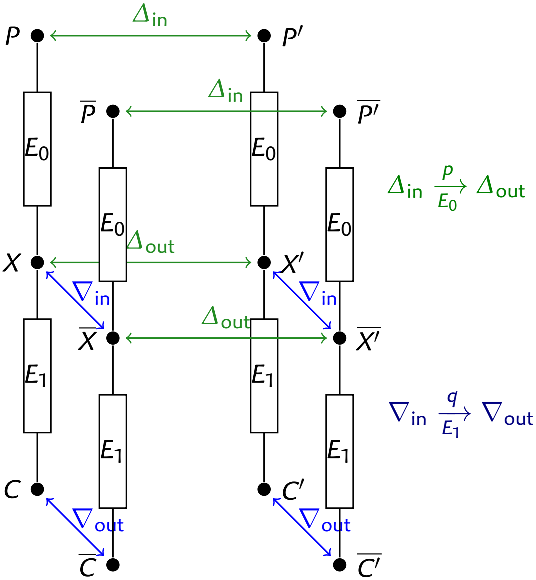
1. $P \leftarrow \$,\quad P' = P + \Delta_{in}$
2. $C = E(P),\quad C' = E(P')$
3. $\overline{C} = C + \nabla_{out},\ \overline{C'} = C' + \nabla_{out}$
4. $\overline{P} = E^{-1}(\overline{C}),\quad \overline{P'} = E^{-1}(\overline{C'})$
5. Check if $\overline{P} + \overline{P'} = \Delta_{in}$

Probability of returning: $p_b = p^2q^2$

- $\Pr[X + X' = \Delta_{out}] = p$
- $\Pr[X + \overline{X} = \nabla_{in}] = q$
- $\Pr[X' + \overline{X'} = \nabla_{in}] = q$
- If this holds, then $\overline{X} + \overline{X'} = \Delta_{out}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = p$

Distinguisher if $p_b \gg 2^{-n}$

Boomerang Quartet



1. $P \leftarrow \$, \quad P' = P + \Delta_{in}$
2. $C = E(P), \quad C' = E(P')$
3. $\overline{C} = C + \nabla_{out}, \quad \overline{C'} = C' + \nabla_{out}$
4. $\overline{P} = E^{-1}(\overline{C}), \quad \overline{P'} = E^{-1}(\overline{C'})$
5. Check if $\overline{P} + \overline{P'} = \Delta_{in}$

Probability of returning: $p_b = p^2 q^2$

- $\Pr[X + X' = \Delta_{out}] = p$
- $\Pr[X + \overline{X} = \nabla_{in}] = q$
- $\Pr[X' + \overline{X'} = \nabla_{in}] = q$
- If this holds, then $\overline{X} + \overline{X'} = \Delta_{out}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = p$

Distinguisher if $p_b \gg 2^{-n}$

Our results

1. Revisiting boomerang with truncated differentials — [Wagner, FSE'99]
   - Use of structures: plaintext ciphertext
   - Statistical distinguishers and key-recovery
   - Generic formula for complexity
2. Improving boomerang attack on 6-round AES — [Biryukov, AES'04]
   - Key-recovery with complexity 2^{61} (improved from 2^{71})
   - Key-recovery with secret S-Boxes
   - 6-round statistical distinguisher ("key-independent")
3. Best attacks on several AES-based tweakable block ciphers
   - KIASU — [Jean, Nikolić & Peyrin, AC'14]
   - TNT-AES — [Bao, Guo, Guo & Song, EC'20]
   - Deoxys — [Jean, Nikolić & Peyrin, AC'14]

Outline

Introduction

Truncated Boomerang Distinguisher

Truncated Boomerang Key-recovery

Applications

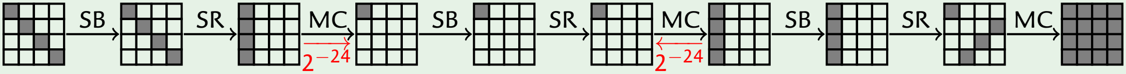
Conclusion

Truncated differential cryptanalysis

- Generalisation of differential cryptanalysis [Kundsen, FSE'94]
- Truncate information about differences, (e.g. active/inactive bytes)

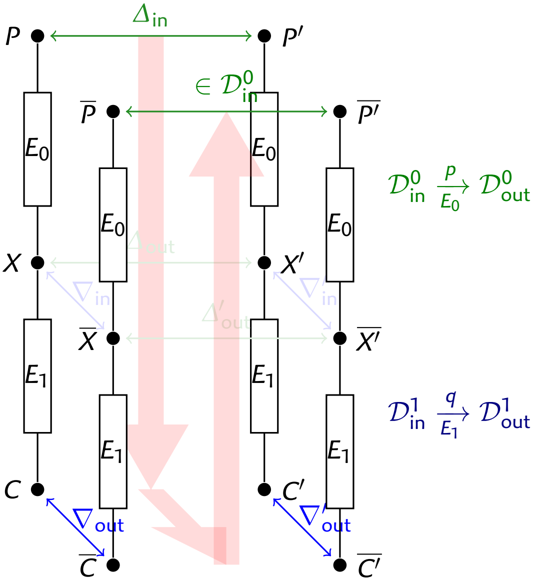
- Set of input/output differences: $\mathcal{D}_{\text{in}}$, $\mathcal{D}_{\text{out}}$
- $\vec{p} = \text{Avg}_{\Delta_{\text{in}} \in \mathcal{D}_{\text{in}}} \Pr\left[E(P) + E(P + \Delta_{\text{in}}) \in \mathcal{D}_{\text{out}}\right]$
- $\overleftarrow{p} = \text{Avg}_{\Delta_{\text{out}} \in \mathcal{D}_{\text{out}}} \Pr\left[E^{-1}(P) + E^{-1}(P + \Delta_{\text{out}}) \in \mathcal{D}_{\text{in}}\right]$
- $\frac{\vec{p}}{|\mathcal{D}_{\text{out}}|} = \frac{\overleftarrow{p}}{|\mathcal{D}_{\text{in}}|} = \text{Avg}_{\Delta_{\text{in}} \in \mathcal{D}_{\text{in}}, \Delta_{\text{out}} \in \mathcal{D}_{\text{out}}} \Pr\left[E(P) + E(P + \Delta_{\text{in}}) = \Delta_{\text{out}}\right]$

Example: 3-round AES truncated trail



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

Truncated Boomerang Quartet



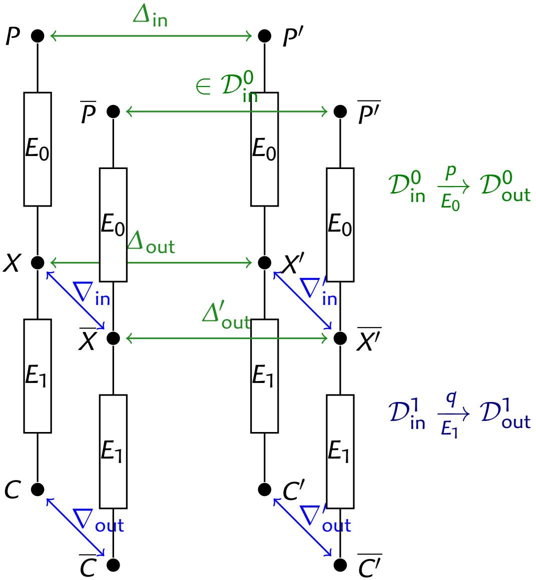
1. $P' = P + \Delta_{in}, \quad \Delta_{in} \in \mathcal{D}^0_{in}$
2. $\overline{C} = C + \nabla_{out}, \nabla_{out} \in \mathcal{D}^1_{out}$
3. $\overline{C'} = C' + \nabla'_{out}, \nabla'_{out} \in \mathcal{D}^1_{out}$
4. Check if $\overline{P} + \overline{P'} \in \mathcal{D}^0_{in}$

- Note: $\nabla_{out} \neq \nabla'_{out}$

Probability of returning: $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftrightarrow{q}^2 \cdot r$

- $\Pr[X + X' \in \mathcal{D}^0_{out}] = \vec{p}$
- $\Pr[X + \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[X' + \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[\overline{X} + \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = \overleftarrow{p}$

Truncated Boomerang Quartet



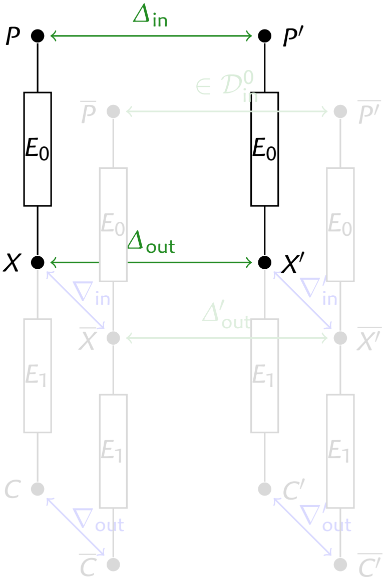
1. $P' = P + \Delta_{in}, \quad \Delta_{in} \in \mathcal{D}^0_{in}$
2. $\overline{C} = C + \nabla_{out}, \ \nabla_{out} \in \mathcal{D}^1_{out}$
3. $\overline{C'} = C' + \nabla'_{out}, \ \nabla'_{out} \in \mathcal{D}^1_{out}$
4. Check if $\overline{P} + \overline{P'} \in \mathcal{D}^0_{in}$

- Note: $\nabla_{out} \neq \nabla'_{out}$

Probability of returning: $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$

- $\Pr[X + X' \in \mathcal{D}^0_{out}] = \vec{p}$
- $\Pr[X + \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[X' + \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[\overline{X} + \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = \overleftarrow{p}$

Truncated Boomerang Quartet



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

$\mathcal{D}^1_{in} \xrightarrow[E_1]{q} \mathcal{D}^1_{out}$

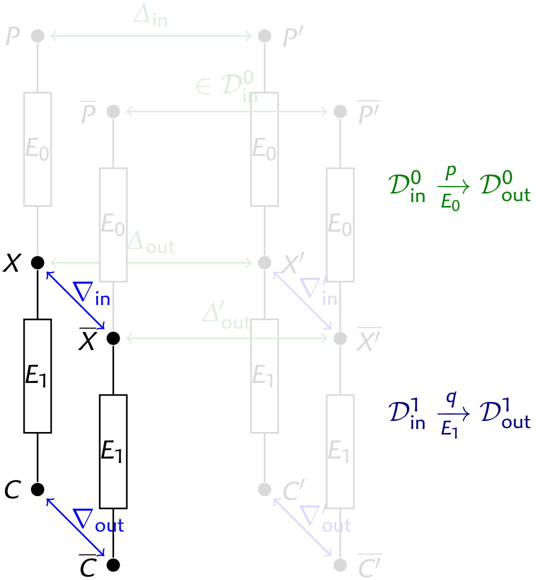
1. $P' = P + \Delta_{in}, \quad \Delta_{in} \in \mathcal{D}^0_{in}$
2. $\overline{C} = C + \nabla_{out}, \nabla_{out} \in \mathcal{D}^1_{out}$
3. $\overline{C'} = C' + \nabla'_{out}, \nabla'_{out} \in \mathcal{D}^1_{out}$
4. Check if $\overline{P} + \overline{P'} \in \mathcal{D}^0_{in}$

- Note: $\nabla_{out} \neq \nabla'_{out}$

Probability of returning: $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$

- $\Pr[X + X' \in \mathcal{D}^0_{out}] = \vec{p}$
- $\Pr[X + \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[X' + \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[\overline{X} + \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = \overleftarrow{p}$

Truncated Boomerang Quartet



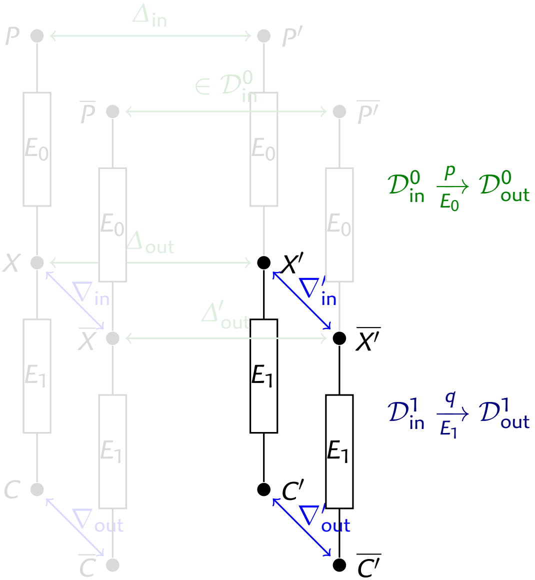
1. $P' = P + \Delta_{in}, \quad \Delta_{in} \in \mathcal{D}^0_{in}$
2. $\overline{C} = C + \nabla_{out}, \nabla_{out} \in \mathcal{D}^1_{out}$
3. $\overline{C'} = C' + \nabla'_{out}, \nabla'_{out} \in \mathcal{D}^1_{out}$
4. Check if $\overline{P} + \overline{P'} \in \mathcal{D}^0_{in}$

- Note: $\nabla_{out} \neq \nabla'_{out}$

Probability of returning: $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$

- $\Pr[X + X' \in \mathcal{D}^0_{out}] = \vec{p}$
- $\Pr[X + \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[X' + \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[\overline{X} + \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = \overleftarrow{p}$

Truncated Boomerang Quartet



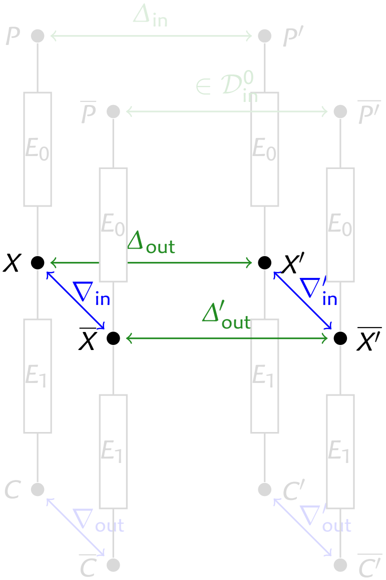
1. $P' = P + \Delta_{in}, \quad \Delta_{in} \in \mathcal{D}^0_{in}$
2. $\overline{C} = C + \nabla_{out}, \ \nabla_{out} \in \mathcal{D}^1_{out}$
3. $\overline{C'} = C' + \nabla'_{out}, \ \nabla'_{out} \in \mathcal{D}^1_{out}$
4. Check if $\overline{P} + \overline{P'} \in \mathcal{D}^0_{in}$

- Note: $\nabla_{out} \neq \nabla'_{out}$

Probability of returning: $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$

- $\Pr[X + X' \in \mathcal{D}^0_{out}] = \vec{p}$
- $\Pr[X + \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[X' + \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[\overline{X} + \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = \overleftarrow{p}$

Truncated Boomerang Quartet



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

$$\mathcal{D}^1_{in} \xrightarrow[E_1]{q} \mathcal{D}^1_{out}$$

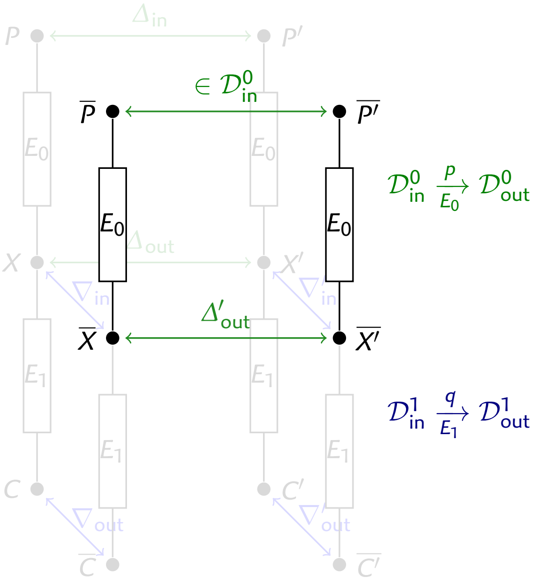
1. $P' = P + \Delta_{in}, \quad \Delta_{in} \in \mathcal{D}^0_{in}$
2. $\overline{C} = C + \nabla_{out}, \nabla_{out} \in \mathcal{D}^1_{out}$
3. $\overline{C'} = C' + \nabla'_{out}, \nabla'_{out} \in \mathcal{D}^1_{out}$
4. Check if $\overline{P} + \overline{P'} \in \mathcal{D}^0_{in}$

- Note: $\nabla_{out} \neq \nabla'_{out}$

Probability of returning: $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$

- $\Pr[X + X' \in \mathcal{D}^0_{out}] = \vec{p}$
- $\Pr[X + \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[X' + \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[\overline{X} + \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = \overleftarrow{p}$

Truncated Boomerang Quartet



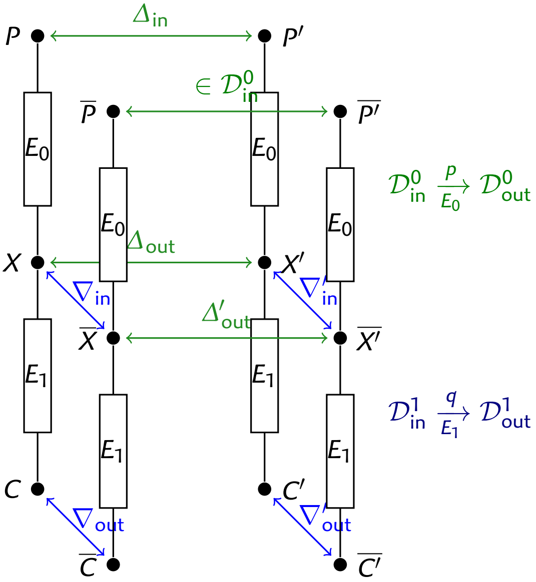
1. $P' = P + \Delta_{in}, \quad \Delta_{in} \in \mathcal{D}^0_{in}$
2. $\overline{C} = C + \nabla_{out}, \; \nabla_{out} \in \mathcal{D}^1_{out}$
3. $\overline{C'} = C' + \nabla'_{out}, \; \nabla'_{out} \in \mathcal{D}^1_{out}$
4. Check if $\overline{P} + \overline{P'} \in \mathcal{D}^0_{in}$

- Note: $\nabla_{out} \neq \nabla'_{out}$

Probability of returning: $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$

- $\Pr[X + X' \in \mathcal{D}^0_{out}] = \vec{p}$
- $\Pr[X + \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[X' + \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[\overline{X} + \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = \overleftarrow{p}$

Truncated Boomerang Quartet



1. $P' = P + \Delta_{in}, \quad \Delta_{in} \in \mathcal{D}^0_{in}$
2. $\overline{C} = C + \nabla_{out}, \ \nabla_{out} \in \mathcal{D}^1_{out}$
3. $\overline{C'} = C' + \nabla'_{out}, \ \nabla'_{out} \in \mathcal{D}^1_{out}$
4. Check if $\overline{P} + \overline{P'} \in \mathcal{D}^0_{in}$

- Note: $\nabla_{out} \neq \nabla'_{out}$

Probability of returning: $p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftarrow{q}^2 \cdot r$

- $\Pr[X + X' \in \mathcal{D}^0_{out}] = \vec{p}$
- $\Pr[X + \overline{X} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[X' + \overline{X'} \in \mathcal{D}^1_{in}] = \overleftarrow{q}$
- $\Pr[\overline{X} + \overline{X'} \in \mathcal{D}^0_{out}] = r \geq |\mathcal{D}^1_{in}|^{-1}$
- $\Pr[\overline{P} + \overline{P'} = \Delta_{in}] = \overleftarrow{p}$

Using structures

- Assuming $\mathcal{D}_{\text{in}}^0$ is a vector space

1. Start with a structure of plaintext
2. Build a structure for each ciphertext

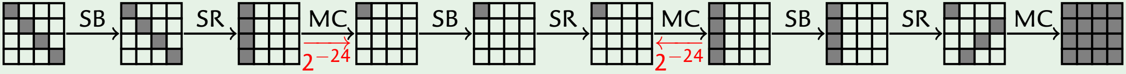
- Total structure size $|\mathcal{D}_{\text{in}}^0| \cdot |\mathcal{D}_{\text{out}}^1|$
  - $|\mathcal{D}_{\text{in}}^0|$ encryption queries
  - $|\mathcal{D}_{\text{in}}^0| \cdot |\mathcal{D}_{\text{out}}^1|$ decryption queries
- $|\mathcal{D}_{\text{in}}^0|^2 \cdot |\mathcal{D}_{\text{out}}^1|^2$ candidate quartets

Truncated Boomerang Distinguisher

1. Choose a random P_0
   - Define $P_i = P_0 + i$ for $i \in \mathcal{D}_{\text{in}}^0$
2. Query $C_i = E(P_i)$
   - Define $\overline{C_i^j} = C_i + j$ for $j \in \mathcal{D}_{\text{out}}^1$
3. Query $\overline{P_i^j} = E^{-1}(\overline{C_i^j})$
4. Count pairs with $\overline{P_i^j} + \overline{P_{i'}^{j'}} \in \mathcal{D}_{\text{in}}^0$
5. If needed, repeat with new P_0

Example: 6-round AES boomerang

3-round AES truncated trail for E_0 and E_1



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

- One structure has $|\mathcal{D}^0_{in}| \cdot |\mathcal{D}^1_{out}| = 2^{64}\ \overline{P}^j_i$
  - 2^{127} pairs: candidate quartets
  - $2^{127} \cdot p_b = 1/2$ good quartets
  - $2^{127} \cdot 2^{-96} = 2^{31}$ returning quartets: wrong quartets
- Most returning quartets are fake positive
- Detect signal with $\gg 2^{32}$ structures: $T = D = \mathcal{O}(2^{96})$

Analysis

- Starting from S structures of size $|\mathcal{D}^0_{\text{in}}| \cdot |\mathcal{D}^1_{\text{out}}|$
- $Q = S \times |\mathcal{D}^0_{\text{in}}|^2 \cdot |\mathcal{D}^1_{\text{out}}|^2$ candidate quartets

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

- $Q \cdot p_b$ good quartets
- $Q \cdot p_\$$ wrong 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

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

Outline

Key recovery

- Usual approach: add rounds before/after distinguisher
  - More rounds, higher complexity than distinguisher
- Our approach: extract key information from right pages
  - Same number of rounds, lower complexity than distinguisher
- Roughly equivalent, but easier to analyse with generic formulas

If $\sigma \gg 1$

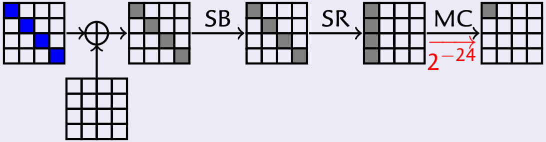
- Collect one good quartet
- (P, P') and $(\overline{P}, \overline{P'})$ follow E_0 trail
- $(C, \overline{C})$ and $(C', \overline{C'})$ follow E_1 trail
  - This is only true for a subset of keys
  - Recover ℓ candidates for a κ-bit key

If $\sigma \ll 1$

- Collect many quartets
- Assume quartets are good
- (P, P') and $(\overline{P}, \overline{P'})$ follow E_0 trail
- $(C, \overline{C})$ and $(C', \overline{C'})$ follow E_1 trail
  - This is only true for a subset of keys
  - Recover ℓ candidates for a κ-bit key
- Use counters for key candidates
- Right key suggested more frequently

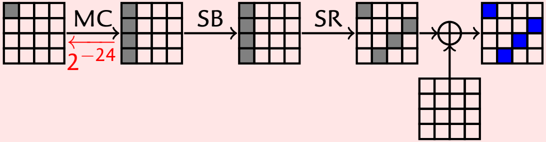
Example: 6-round AES boomerang

First round



- Plaintext is known
- Recover candidates for k_0 diagonal
  - Given (P, P'), 2^8 candidates
  - Given $(\overline{P}, \overline{P'})$, 2^8 candidates
  - 2^{-16} candidates in intersection

Last round



- Ciphertext is known
- Recover candidates for k_6 anti-diagonal
  - Given $(C, \overline{C})$, 2^8 candidates
  - Given $(C', \overline{C'})$, 2^8 candidates
  - 2^{-16} candidates in intersection

- On average $\ell = 2^{-32}$ candidates for $\kappa = 64$ bits of key
- With S structures: $S \times 2^{64}$ elements $\overline{P_i^j}$, $S \times 2^{127}$ pairs, $S \times 2^{31}$ returning quartets
  - $S \times 2^{31}$ fake positives $\rightarrow S \times 2^{31} \times 2^{-32} = S/2$ wrong keys suggestions
  - $S \times 1/2$ right quartet $\rightarrow S \times 1/2 \times 1 = S/2$ correct keys suggestions
- High probability of succes with 8 structures ($D = T = 2^{67}$)

Analysis

- Starting from S structures of size $|\mathcal{D}_{\text{in}}^0| \cdot |\mathcal{D}_{\text{out}}^1|$
- $Q = S \times |\mathcal{D}_{\text{in}}^0|^2 \cdot |\mathcal{D}_{\text{out}}^1|^2$ candidate quartets, $Q \cdot p_\$$ returning quartets
- $Q \cdot p_b$ good quartets
  - 1 suggestion for right key
  - ℓ suggestions for wrong key, $\ell \times 2^{-\kappa}$ hits for each
- $Q \cdot p_\$$ fake positives
  - ℓ suggestions for wrong key, $\ell \times 2^{-\kappa}$ hits for each
- Improved signal to noise $\tilde{\sigma} = p_b / p_\$ \times 2^\kappa / \ell$

If $\tilde{\sigma} \gg 1$

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

If $\tilde{\sigma} \ll 1$

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

- Time and data complexity

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

6-round AES results

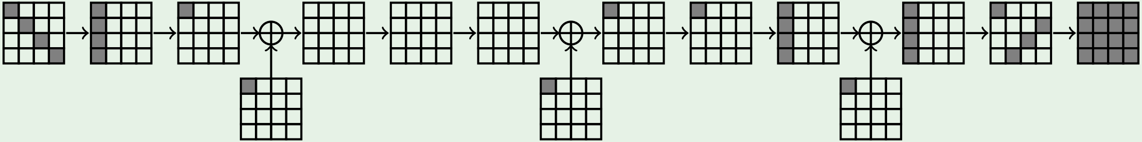
	Type	Data		Time	Ref
Distinguishers	Yoyo	$2^{122.8}$	ACC	$2^{121.8}$	[AC:RonBarHel17]
	Exchange attack	$2^{88.2}$	CP	$2^{88.2}$	[AC:BarRon19]
	Exchange attack	2^{84}	ACC	2^{83}	[EPRINT:Bardeh19]
	Truncated differential	$2^{89.4}$	CP	$2^{96.5}$	[ToSC:BaoGuoLis20]
	Truncated boomerang	2^{87}	ACC	2^{87}	New
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}	New
Secret S-Box KR	Square	2^{64}	CP	2^{90}	[FSE:TKKL15]
	Truncated boomerang	2^{94}	ACC	2^{94}	New

Outline

8-round boomerang on KIASU

- KIASU: AES-based tweakable block cipher [Jean, Nikolić & Peyrin, AC'14]
  - Tweak added on first 64 bits of state

4-round truncated trail for KIASU



$\vec{p} = 2^{-32}$ $\overleftarrow{p} = 2^{-32}$ $|\mathcal{D}^0_{\text{in}}| = 2^{32}$ $|\mathcal{D}^0_{\text{out}}| = 2^{32}$ $|\mathcal{D}^0_{\text{tw}}| = 2^{8}$

- Evaluate complexity with generic formula

$$p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftrightarrow{q}^2 \times |\mathcal{D}^1_{\text{in}}|^{-1} = 2^{-160} \qquad \tilde{\sigma} = 2^{32}$$

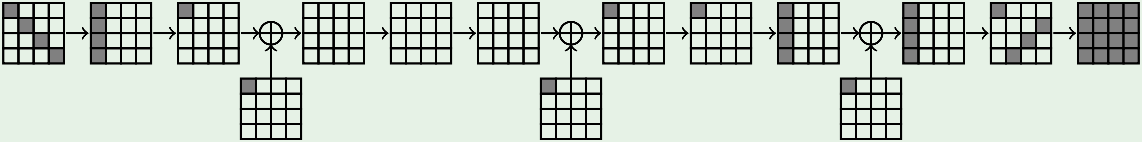
$$p_w = |\mathcal{D}^0_{\text{in}}| / 2^n \times \ell \times 2^{-\kappa} = 2^{-192} \qquad Q = \mathcal{O}(2^{160}) \qquad D = \mathcal{O}(2^{80})$$

- Previous best attack: boomerang with complexity 2^{103}

8-round boomerang on KIASU

- KIASU: AES-based tweakable block cipher [Jean, Nikolić & Peyrin, AC'14]
  - Tweak added on first 64 bits of state

4-round truncated trail for KIASU



$\vec{p} = 2^{-32}$ $\overleftarrow{p} = 2^{-32}$ $|\mathcal{D}^0_{\text{in}}| = 2^{32}$ $|\mathcal{D}^0_{\text{out}}| = 2^{32}$ $|\mathcal{D}^0_{\text{tw}}| = 2^{8}$

- Evaluate complexity with generic formula

$$p_b = \vec{p} \cdot \overleftarrow{p} \cdot \overleftrightarrow{q}^2 \times |\mathcal{D}^1_{\text{in}}|^{-1} = 2^{-160} \qquad \tilde{\sigma} = 2^{32}$$

$$p_w = |\mathcal{D}^0_{\text{in}}|/2^n \times \ell \times 2^{-\kappa} = 2^{-192} \qquad Q = \mathcal{O}(2^{160}) \qquad D = \mathcal{O}(2^{80})$$

- Previous best attack: boomerang with complexity 2^{103}

Deoxys

- AES-based Tweakable block cipher, CAESAR portfolio [Jean, Nikolić & Peyrin, AC'14]
- Best attacks: boomerangs built with MILP model
  - Key-recovery typically added afterwards

Our results

- MILP model with truncated boomerang framework (model truncated trails)
- Integrate key recovery: optimize data complexity (parameters given by trail)

		Previous				New		
Model	Rnd		Data	Time	Mem		Data	Time	Mem
RTK2	9	B	2^{98}	2^{112}	2^{17}	B	$2^{55.2}$	$2^{55.2}$	$2^{55.2}$
	10	B	$2^{98.4}$	$2^{109.1}$	2^{88}	B	$2^{94.2}$	$2^{95.2}$	$2^{94.2}$
	11	R	$2^{122.1}$	$2^{249.9}$	$2^{128.2}$	B	2^{129}	$2^{223.9}$	2^{129}
RTK3	11	B	2^{100}	2^{100}	2^{17}	B	$2^{32.7}$	$2^{32.7}$	$2^{32.7}$
	12	B	2^{98}	2^{98}	2^{64}	B	$2^{67.4}$	$2^{67.4}$	2^{65}
	13	R	$2^{125.2}$	$2^{186.7}$	2^{136}	B	$2^{126.7}$	$2^{170.2}$	$2^{126.7}$
	14	R	$2^{125.2}$	$2^{282.7}$	2^{136}	B	2^{129}	$2^{278.8}$	2^{129}

TNT-AES

- AES-based tweakable block cipher
- Uses 6-round AES as building block R
  - $\tilde{E} : T, P \mapsto R_2\big(T + R_1(T + R_0(P))\big)$
- Build boomerang quartets for middle layer using tweak differences
  - Only one usable return difference
  - No structures on ciphertext side
- First attack based on a 6-round distinguisher

Rounds	Type	Data		Time	Ref
∗-5-∗	Boomerang (dist.)	2^{126}	ACC	2^{126}	[EC:BGGS20]
5-∗-∗	Impossible differential (KR)	$2^{113.6}$	CP	$2^{113.6}$	[AC:GGLS20]
∗-∗-∗	Generic (dist.)	$2^{99.5}$	CP	$2^{99.5}$	[AC:GGLS20]
∗-5-∗	Truncated boomerang (dist.)	2^{76}	ACC	2^{76}	New
5-5-∗	Truncated boomerang (KR)	2^{87}	ACC	2^{87}	New
∗-6-∗	Truncated boomerang (dist.)	$2^{127.8}$	ACC	$2^{127.8}$	New

Conclusion

1. Analysis of truncated bommerang attacks
   - Use of structures
   - Generic formulas for data complexity
2. Revisiting boomerangs on 6-round AES
   - Competitive with recently proposed 6-round attacks
   - Statistical distinguisher (“key-independent”)
   - Key recovery
   - Key-recovery with secret S-Boxes
3. Applications
   - Best attack on KIASU
   - Marginal distinguisher on TNT-AES
   - First application of a 6-round distinguisher
4. Implementation as a MILP model
   - New results on Deoxys