Revisiting Differential-Linear Attacks via a Boomerang Perspective

Applications to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck, and SERPENT

Hosein Hadipour   Patrick Derbez   Maria Eichlseder

ASK 2024 - Kolkata, India

TU Graz
SCIENCE
PASSION
TECHNOLOGY

› hsn.hadipour@gmail.com

Research Gap and Our Contributions

Research Gap

- How to analytically estimate the correlation of DL distinguishers?
- How to (efficiently) find good DL distinguishers?

Contributions

- Generalizing the DLCT framework [Bar+19] for analytical correlation estimation.
- Introducing an efficient method to search for DL distinguishers applicable to:
  - Strongly aligned SPN primitives: AES, SKINNY
  - Weakly aligned SPN primitives: Ascon, SERPENT, KNOT, PRESENT
  - Feistel structures: CLEFIA, TWINE, LBlock, LBlock-s, WARP
  - AndRX designs: Simeck

Research Gap and Our Contributions

Research Gap

- How to analytically estimate the correlation of DL distinguishers?
- How to (efficiently) find good DL distinguishers?

Contributions

- Generalizing the `DLCT` framework [Bar+19] for analytical correlation estimation.
- Introducing an efficient method to search for DL distinguishers applicable to:
  - Strongly aligned SPN primitives: AES, SKINNY
  - Weakly aligned SPN primitives: Ascon, SERPENT, KNOT, PRESENT
  - Feistel structures: CLEFIA, TWINE, LBlock, LBlock-s, WARP
  - AndRX designs: Simeck

Outline

Background

Universal Bound for Data Complexity - I

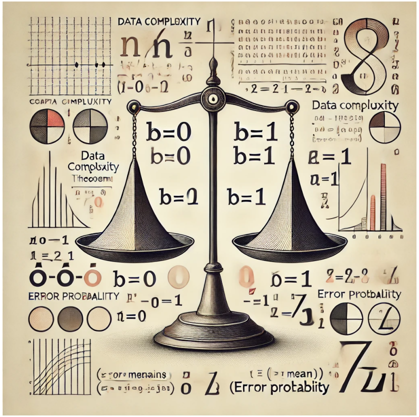
Theorem (Data Complexity)

Let X_0 and X_1 be two distributions. Given one sample from X_b, the distinguisher $\mathcal{D}$ outputs 1 with probability p if $b = 1$, and outputs 1 with probability q if $b = 0$. Assume that b is chosen uniformly at random from $\{0, 1\}$ and is fixed. Next, we run $\mathcal{D}$ on n samples, and output 1 if the sum of the outcomes is closer to $\mu_1 = np$, and 0 otherwise. If n satisfies the following inequality, then the error probability of the distinguisher is upper bounded by ε:

$$n \geq \max\left(\frac{2(3q+p)\ln\left(\frac{1}{\varepsilon}\right)}{(p-q)^2}, \frac{8p\ln\left(\frac{1}{\varepsilon}\right)}{(p-q)^2}\right).$$

Universal Bound for Data Complexity - II

- $n \geq \max\left(\frac{2(3q+p)\ln\left(\frac{1}{\varepsilon}\right)}{(p-q)^2}, \frac{8p\ln\left(\frac{1}{\varepsilon}\right)}{(p-q)^2}\right).$
- If $p \gg q$, then $p - q \approx p$ then $n \geq \frac{8\ln\left(\frac{1}{\varepsilon}\right)}{p}$.
- If $p = \frac{1}{2} + \frac{c}{2}, q = \frac{1}{2} + \frac{c'}{2}, c \gg c'$,
  and $c, c' \ll \frac{1}{2}$ then $n \geq \frac{8\ln\left(\frac{1}{\varepsilon}\right)}{c^2}$.



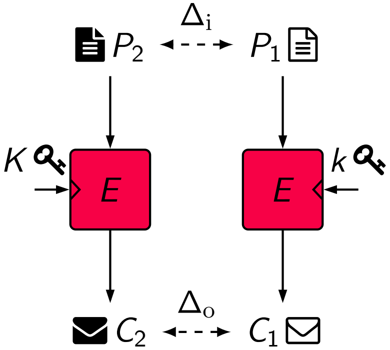
Generated using OpenAI's DALL·E.

Differential Attacks [BS90]

Input: $E_K, (\Delta_\mathrm{i}, \Delta_\mathrm{o}), N, p = \mathbb{P}(\Delta_\mathrm{i}, \Delta_\mathrm{o})$
Output: 0: **real** cipher, 1: **ideal** cipher

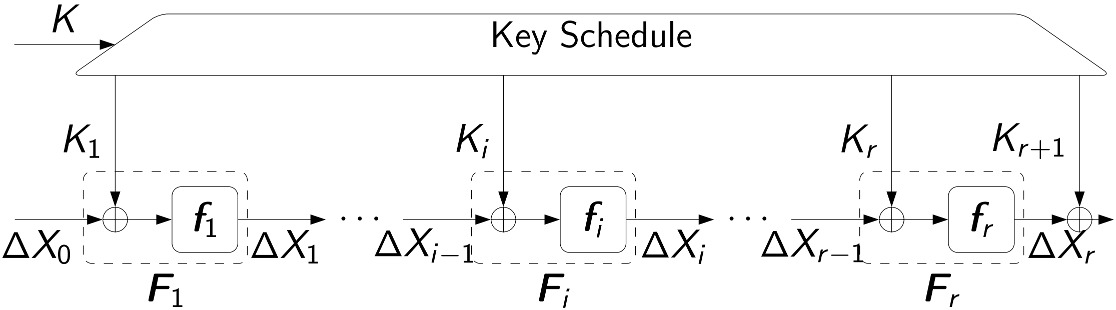
```
Initialize counter T with zero;
for i = 0, ..., N − 1 do
    P_1 ←$ F_2^n;
    C_1 ← E_K(P_1);
    P_2 ← P_1 ⊕ Δ_i;
    C_2 ← E_K(P_2);
    if C_1 ⊕ C_2 = Δ_o then
        T ← T + 1;
if T ~ N(μ = Np, σ^2 = Np(1 − p)) then
    return 0;                 // real cipher
else
    return 1;                 // ideal cipher
```

$N \approx \mathcal{O}(p^{-1})$.



$p = \mathbb{P}(\Delta_\mathrm{i} \to \Delta_\mathrm{o})$

Analyticl Estimation of Differential Probability



$$\mathbb{P}(\Delta X_r = \Delta_r \mid \Delta X_0 = \Delta_0) = \sum_{\Delta_1, \cdots, \Delta_{r-1}} \prod_{i=1}^{r} \mathbb{P}(f_i(X) \oplus f_i(X \oplus \Delta_{i-1}) = \Delta_i).$$

Difference Distribution Table (DDT) – I

We need a tool to handle the nonlinear operations

Differential Distribution Table (DDT)

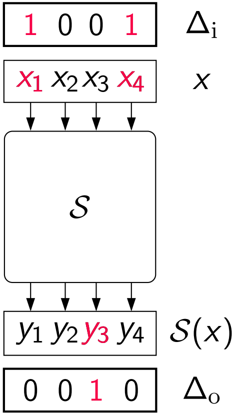
For a vectorial Boolean function $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, the DDT is a $2^n \times 2^m$ table whose rows correspond to the input difference Δ_i to S and whose columns correspond to the output difference Δ_o of S. The entry at index $(\Delta_\mathrm{i}, \Delta_\mathrm{o})$ is

$$\mathtt{DDT}(\Delta_\mathrm{i}, \Delta_\mathrm{o}) = |\{x \in \mathbb{F}_2^n : \ S(x) \oplus S(x \oplus \Delta_\mathrm{i}) = \Delta_\mathrm{o}\}|.$$

$$\mathbb{P}\left(\Delta_\mathrm{i}, \Delta_\mathrm{o}\right) = 2^{-n} \cdot \mathtt{DDT}\left(\Delta_\mathrm{i}, , \Delta_\mathrm{o}\right)$$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Difference Distribution Table (DDT) – II



$$\mathbb{P}(9, 2) = \frac{4}{16}$$

$\Delta_i \setminus \Delta_o$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
2	0	2	0	2	0	0	0	4	0	2	2	0	0	0	2	2
3	0	2	0	2	0	0	4	0	0	2	2	0	0	0	2	2
4	0	0	0	0	0	0	0	0	0	0	4	4	2	2	2	2
5	0	0	0	0	2	2	2	2	0	0	4	4	0	0	0	0
6	0	2	0	2	0	4	0	0	0	2	2	0	2	2	0	0
7	0	2	0	2	4	0	0	0	0	2	2	0	2	2	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4	4
9	0	4	4	0	0	0	0	0	0	4	0	4	0	0	0	0
a	0	0	2	2	2	0	0	2	4	0	0	0	0	2	0	2
b	0	0	2	2	0	2	2	0	4	0	0	0	2	0	2	0
c	0	4	4	0	2	2	2	2	0	0	0	0	0	0	0	0
d	0	0	0	0	2	2	2	2	0	4	0	4	0	0	0	0
e	0	0	2	2	0	2	2	0	4	0	0	0	0	2	0	2
f	0	0	2	2	2	0	0	2	4	0	0	0	2	0	2	0

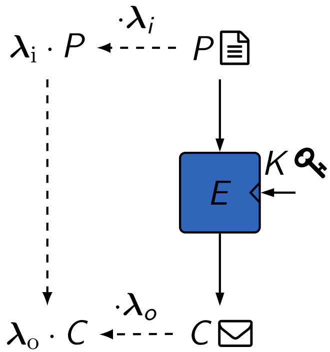
Linear Attacks [Mat93]

Input: E_K, Given N distinct plaintext-ciphertext pairs (P_i, C_i), $\boldsymbol{c} = \mathbb{C}(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}})$
Output: 0: **real** cipher, 1: **ideal** cipher

```
Initialize a counter list V[z] ← 0 for z ∈ {0,1};
for t = 0, ..., N − 1 do
    b1 ← λi · Pt;
    b2 ← λo · Ct;
    V[b1 ⊕ b2] ← V[b1 ⊕ b2] + 1;
if V[0] ~ N(μ0 = N(1+c)/2, σ0^2 = N(1−c^2)/4). then
    return 0;                  // real cipher
else
    return 1;                  // ideal cipher
```

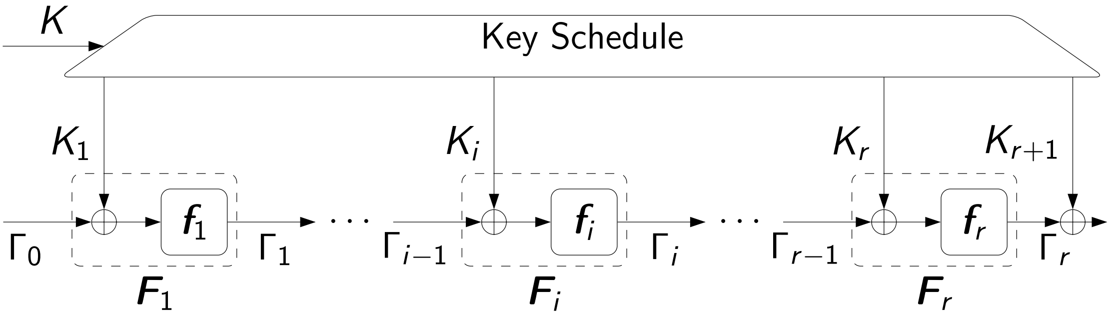
$$\text{if } V[0] \sim \mathcal{N}\left(\mu_0 = N\tfrac{1+\boldsymbol{c}}{2}, \sigma_0^2 = \tfrac{N(1-c^2)}{4}\right).$$

$$N = \mathcal{O}(\boldsymbol{c}^{-2}).$$



$\boldsymbol{c} = 2 \cdot \mathbb{P}(\boldsymbol{\lambda}_{\mathrm{i}} \cdot P \oplus \boldsymbol{\lambda}_{\mathrm{o}} \cdot C = 0) - 1$

Analyticl Estimation of Correlation



$$\mathbb{C}(\Gamma_0, \Gamma_{r+1}) \approx (-1)^{\mathtt{Sign}(\Gamma, K)} \prod_{i=1}^{r} \mathbb{C}_{f_i}(\Gamma_{i-1}, \Gamma_i), \ \mathtt{Sign}(\Gamma, K) = (-1)^{(\Gamma_0 \cdot K_1 \oplus \cdots \oplus \Gamma_r \cdot K_{r+1})}.$$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Linear Approximation Table (LAT) – I

We need a metric to measure the quality of a linear approximation.

Linear Approximation Table (LAT)

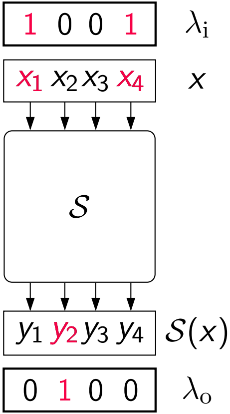
For a vectorial Boolean function $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, the LAT of S is a $2^n \times 2^m$ table whose rows correspond to the input mask λ_{i} to S and whose columns correspond to the output mask λ_{o} of S. The entry at index $(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}})$ is

$$\mathtt{LAT}(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}) = |\mathtt{LAT}_0(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}})| - |\mathtt{LAT}_1(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}})|,$$

where $\mathtt{LAT}_b(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}) = \{x \in \mathbb{F}_2^n : \ \lambda_{\mathrm{i}} \cdot x \oplus \lambda_{\mathrm{o}} \cdot S(x) = b\}$.

$$\mathbb{C}\left(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}\right) = 2^{-n} \cdot \mathtt{LAT}\left(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}\right)$$

Linear Approximation Table (LAT) – II



$$\mathbb{C}\,(9, 4) = \frac{8}{16}$$

$\lambda_i \setminus \lambda_o$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	4	-4	0	-8	-4	-4	0	0	4	-4	-8	0	4	4
2	0	0	0	0	0	0	0	0	0	8	8	0	0	8	-8	0
3	0	-8	4	4	0	0	-4	4	0	0	-4	4	-8	0	-4	-4
4	0	4	0	4	0	4	8	-4	0	4	0	4	-8	-4	0	4
5	0	4	-4	-8	0	-4	-4	0	0	4	-4	8	0	-4	-4	0
6	0	-4	8	4	0	-4	0	-4	0	4	0	4	8	-4	0	4
7	0	4	4	0	0	-4	4	-8	0	-4	-4	0	0	4	-4	-8
8	0	0	0	0	0	0	0	0	0	0	8	8	0	0	8	-8
9	0	0	-4	4	**8**	0	-4	-4	0	0	4	-4	0	-8	-4	-4
a	0	8	0	8	0	-8	0	8	0	0	0	0	0	0	0	0
b	0	0	-4	4	-8	0	-4	-4	0	8	-4	-4	0	0	4	-4
c	0	4	0	4	0	4	-8	-4	8	-4	0	4	0	4	0	4
d	0	4	4	0	-8	4	-4	0	-8	-4	4	0	0	-4	-4	0
e	0	4	8	-4	0	4	0	4	8	4	0	-4	0	-4	0	-4
f	0	-4	-4	0	-8	-4	4	0	8	-4	4	0	0	-4	-4	0

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Boomerang Distinguishers [Wag99]

Input: $E_K, (\Delta, \nabla), N, P = \mathbb{P}(P_3 \oplus P_4 = \Delta)$

Output: 0: **real** cipher, 1: **ideal** cipher

Initialize counter T with zero;

for $i = 0, \ldots, N-1$ **do**

  $P_1 \xleftarrow{\$} \mathbb{F}_2^n$; $P_2 = P_1 \oplus \Delta$;

  $C_1 \leftarrow E_K(P_1)$, $C_2 \leftarrow E_K(P_2)$;

  $C_3 \leftarrow C_1 \oplus \nabla$, $C_4 \leftarrow C_2 \oplus \nabla$;

  $P_3 \leftarrow D_K(C_3)$, $P_4 \leftarrow D_K(C_4)$;

  if $P_3 \oplus P_4 = \Delta$ **then**

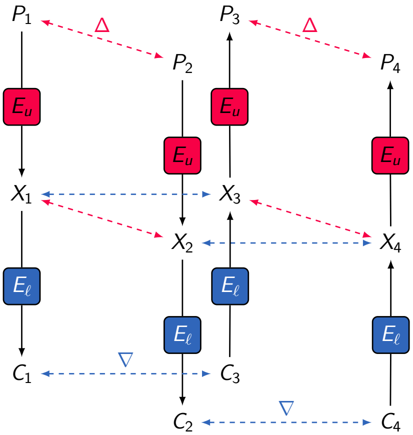
    $T \leftarrow T + 1$;

if $T \sim \mathcal{N}(\mu = NP, \sigma^2 = NP(1-P))$ **then**

  return 0; `// real cipher`

else

  return 1; `// ideal cipher`

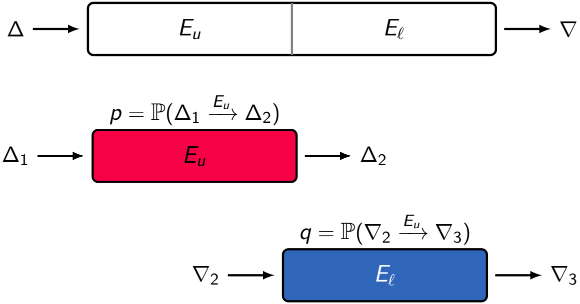


Probability of Boomerang Distinguishers [Wag99]

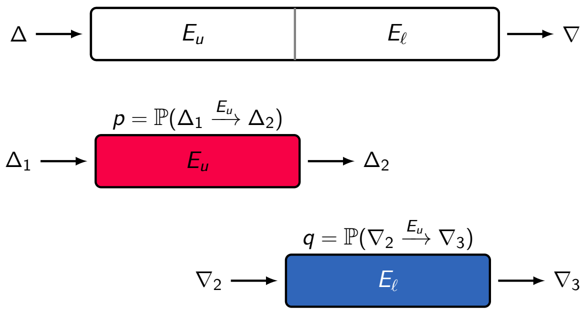
$$\Delta \longrightarrow \boxed{E : \mathbb{F}_2^n \to \mathbb{F}_2^n} \longrightarrow \nabla$$

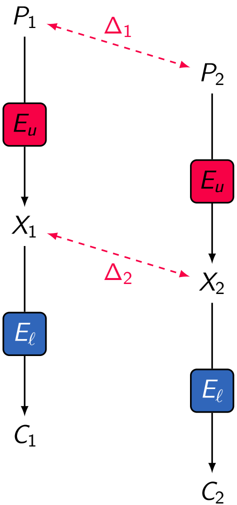
$$0 \lneq \mathbb{P}(\Delta \xrightarrow{E} \nabla) \lll 2^{-n}$$

Probability of Boomerang Distinguishers [Wag99]

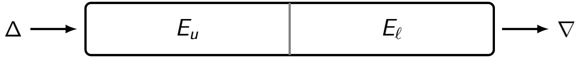


Probability of Boomerang Distinguishers [Wag99]



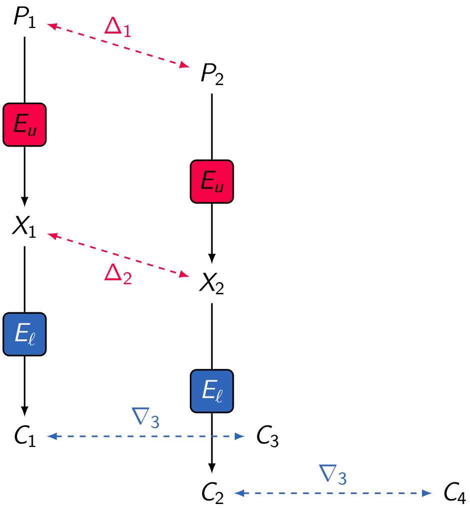


Probability of Boomerang Distinguishers [Wag99]

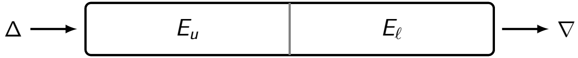


$p = \mathbb{P}(\Delta_1 \xrightarrow{E_u} \Delta_2)$

$q = \mathbb{P}(\nabla_2 \xrightarrow{E_u} \nabla_3)$

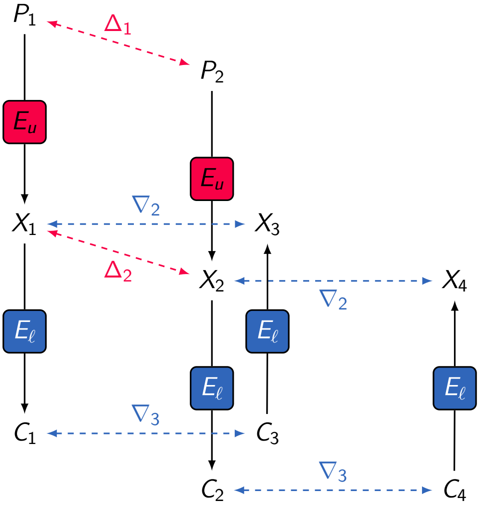


Probability of Boomerang Distinguishers [Wag99]

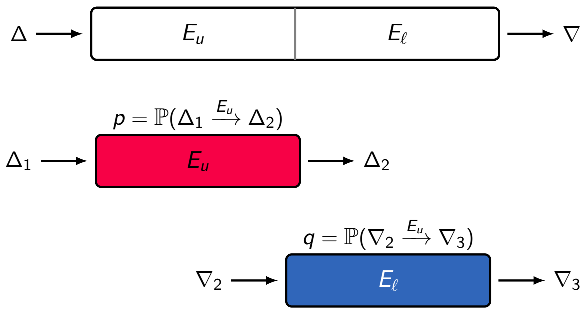


$p = \mathbb{P}(\Delta_1 \xrightarrow{E_u} \Delta_2)$

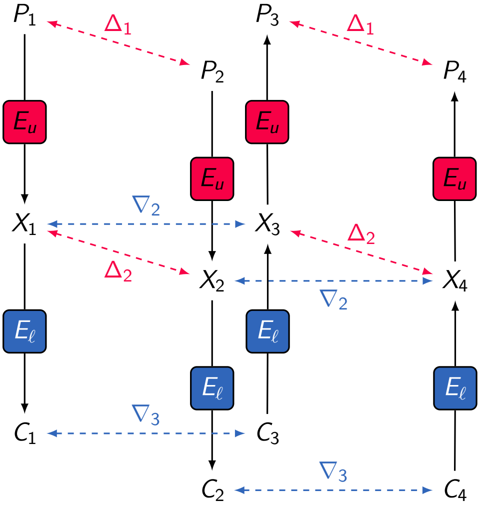
$q = \mathbb{P}(\nabla_2 \xrightarrow{E_\ell} \nabla_3)$



Probability of Boomerang Distinguishers [Wag99]

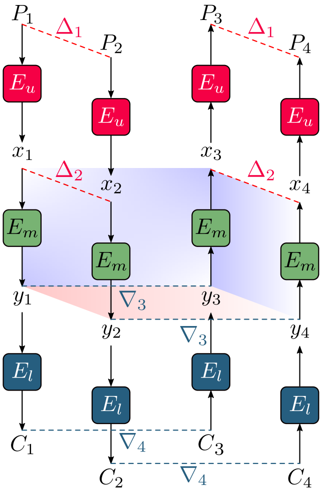


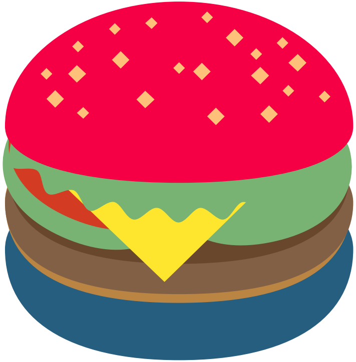
$$\mathbb{P}(P_3 \oplus P_4 = \Delta_1) = p^2 q^2$$



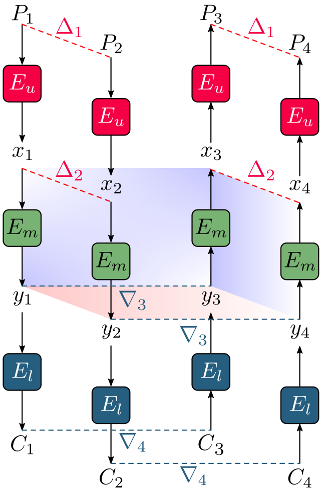
Hosein Hadipour, Patrick Derbez, Maria Eichlseder
ASK 2024 - Kolkata, India

Sandwiching the Differentials! [DKS10; DKS14]





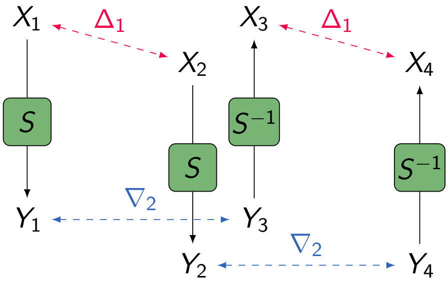
Sandwiching the Differentials! [DKS10; DKS14]

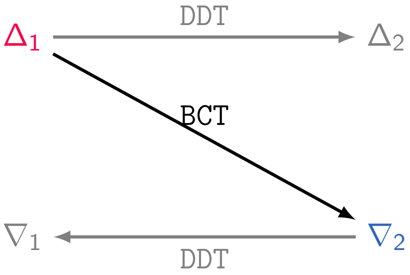


$$\mathbb{P}(P_3 \oplus P_4 = \Delta_1) \approx p^2 \times r \times q^2$$
$$r = \mathbb{P}(\Delta_2 \rightleftarrows \nabla_3)$$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Boomerang Connectivity Table (BCT) [Cid+18]

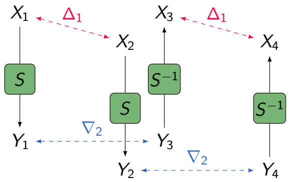


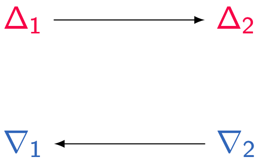


$$\mathtt{BCT}(\Delta_1, \nabla_2) \coloneqq \#\{X \in \mathbb{F}_2^n \mid S^{-1}(S(X) \oplus \nabla_2) \oplus S^{-1}(S(X \oplus \Delta_1) \oplus \nabla_2) = \Delta_1\}$$

$$\mathbb{P}(\Delta_1 \rightleftarrows \nabla_2) = 2^{-n} \cdot \mathtt{BCT}(\Delta_1, \nabla_2)$$

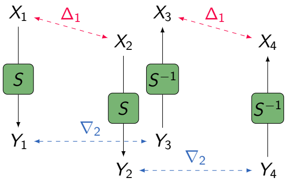
Generalized BCT Framework - I

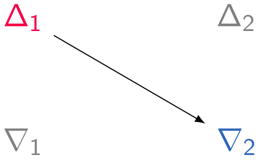




- $\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) = \{x : S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\}, \quad \mathtt{DDT}(\Delta_1, \Delta_2) = \#\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)$
- $\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) = \{x : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) = \Delta_1\}, \ \mathtt{BCT}(\Delta_1, \nabla_2) = \#\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2)$
- $\mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)\}$ [WP19]
- $\mathtt{LBCT}(\Delta_1, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [DDV20; SQH19]
- $\mathtt{EBCT}(\Delta_1, \Delta_2, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [Bou+20; DDV20]

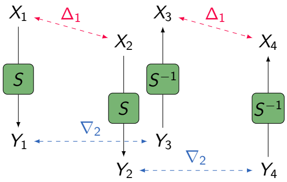
Generalized BCT Framework - I

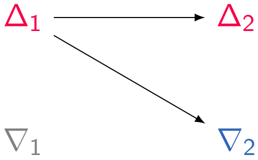




- $\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) = \{x : S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\}, \quad \mathtt{DDT}(\Delta_1, \Delta_2) = \#\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)$
- $\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) = \{x : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) = \Delta_1\}, \ \mathtt{BCT}(\Delta_1, \nabla_2) = \#\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2)$
- $\mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)\}$ [WP19]
- $\mathtt{LBCT}(\Delta_1, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [DDV20; SQH19]
- $\mathtt{EBCT}(\Delta_1, \Delta_2, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [Bou+20; DDV20]

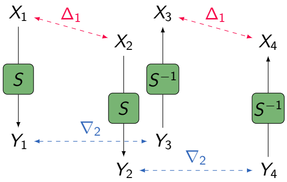
Generalized BCT Framework - I

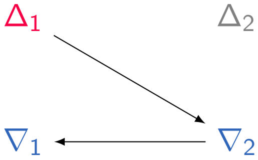




- $\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) = \{x : S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\}, \quad \mathtt{DDT}(\Delta_1, \Delta_2) = \#\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)$
- $\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) = \{x : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) = \Delta_1\}, \ \mathtt{BCT}(\Delta_1, \nabla_2) = \#\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2)$
- $\mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)\}$ [WP19]
- $\mathtt{LBCT}(\Delta_1, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [DDV20; SQH19]
- $\mathtt{EBCT}(\Delta_1, \Delta_2, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [Bou+20; DDV20]

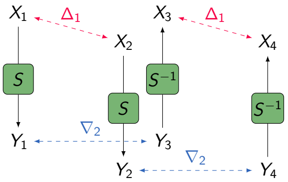
Generalized BCT Framework - I

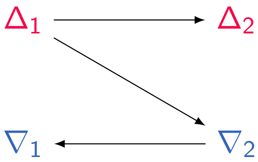




- $\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) = \{x : S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\}$, $\quad \mathtt{DDT}(\Delta_1, \Delta_2) = \#\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)$
- $\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) = \{x : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) = \Delta_1\}$, $\mathtt{BCT}(\Delta_1, \nabla_2) = \#\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2)$
- $\mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)\}$ [WP19]
- $\mathtt{LBCT}(\Delta_1, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [DDV20; SQH19]
- $\mathtt{EBCT}(\Delta_1, \Delta_2, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [Bou+20; DDV20]

Generalized BCT Framework - I





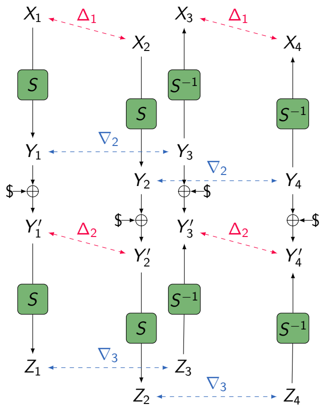
- $\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) = \{x : S(x) \oplus S(x \oplus \Delta_1) = \Delta_2\}, \quad \mathtt{DDT}(\Delta_1, \Delta_2) = \#\mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)$
- $\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) = \{x : S^{-1}(S(x) \oplus \nabla_2) \oplus S^{-1}(S(x \oplus \Delta_1) \oplus \nabla_2) = \Delta_1\}, \ \mathtt{BCT}(\Delta_1, \nabla_2) = \#\mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2)$
- $\mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2)\}$ [WP19]
- $\mathtt{LBCT}(\Delta_1, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [DDV20; SQH19]
- $\mathtt{EBCT}(\Delta_1, \Delta_2, \nabla_1, \nabla_2) = \#\{x : x \in \mathcal{X}_{\mathtt{BCT}}(\Delta_1, \nabla_2) \cap \mathcal{X}_{\mathtt{DDT}}(\Delta_1, \Delta_2) \cap \mathcal{X}_{\mathtt{DDT}}(\nabla_1, \nabla_2)\}$ [Bou+20; DDV20]

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Generalized BCT Framework (GBCT) - II

- Double Boomerang Connectivity Table ($\mathtt{DBCT}$) [HB21]

$$\begin{tikzcd} \Delta_1 \arrow[r] \arrow[dr] & \Delta_2 \arrow[dr] & \\ & \nabla_2^* \arrow[r] & \nabla_3 \end{tikzcd}$$



$\mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = \sum_{\nabla_2} \mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) \cdot \mathtt{LBCT}(\Delta_2, \nabla_2, \nabla_3)$

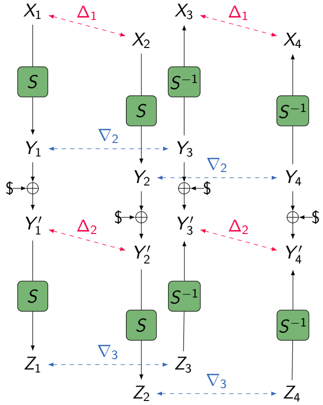
$\mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3) = \sum_{\Delta_2} \mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) \cdot \mathtt{LBCT}(\Delta_2, \nabla_2, \nabla_3).$

$\mathtt{DBCT}(\Delta_1, \nabla_3) = \sum_{\Delta_2} \mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = \sum_{\nabla_2} \mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3).$

Generalized BCT Framework (GBCT) - II

- Double Boomerang Connectivity Table (DBCT) [HB21]

$$\begin{tikzcd}
\Delta_1 \arrow[r] \arrow[dr] & \Delta_2^* \arrow[dr] & \\
& \nabla_2 \arrow[r] & \nabla_3
\end{tikzcd}$$

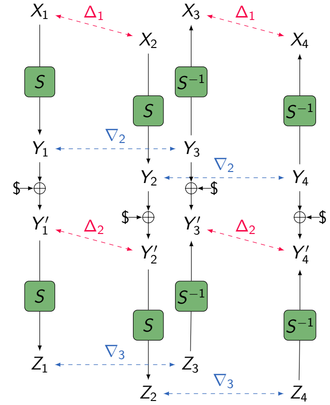


- $\mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = \sum_{\nabla_2} \mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) \cdot \mathtt{LBCT}(\Delta_2, \nabla_2, \nabla_3)$
- $\mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3) = \sum_{\Delta_2} \mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) \cdot \mathtt{LBCT}(\Delta_2, \nabla_2, \nabla_3).$
- $\mathtt{DBCT}(\Delta_1, \nabla_3) = \sum_{\Delta_2} \mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = \sum_{\nabla_2} \mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3).$

Generalized BCT Framework (GBCT) - II

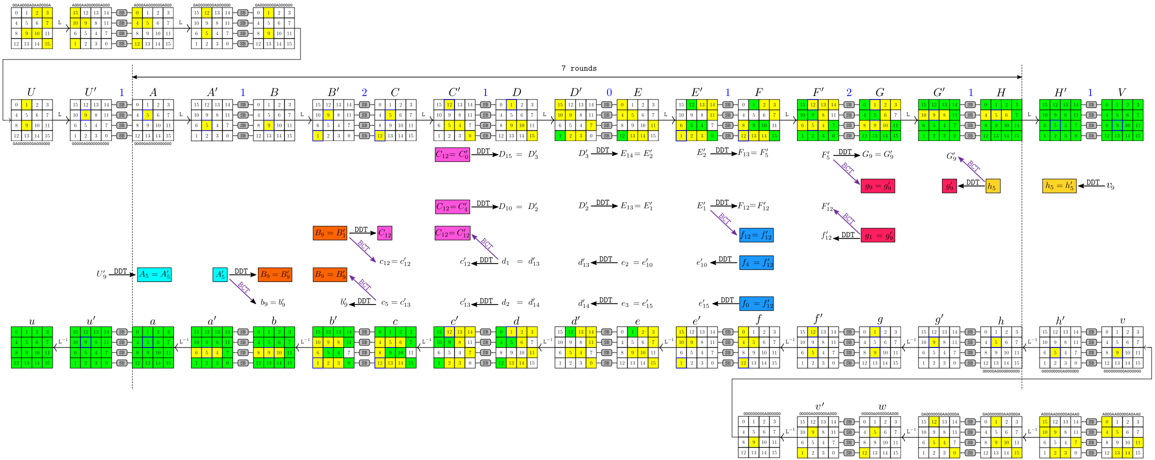
- Double Boomerang Connectivity Table ($\mathtt{DBCT}$) [HB21]

$$\begin{tikzcd} \Delta_1 \arrow[r] \arrow[dr] & \Delta_2^* \arrow[dr] & \\ & \nabla_2^* \arrow[r] & \nabla_3 \end{tikzcd}$$



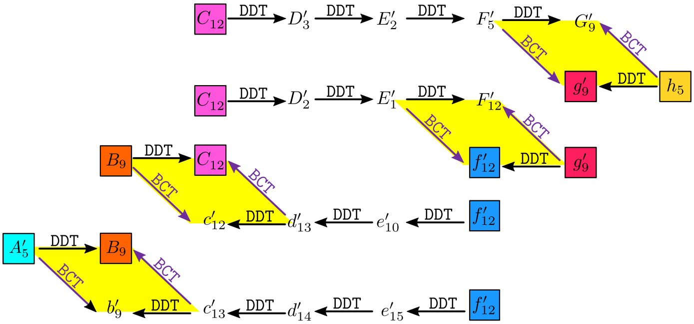
- ✓ $\mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = \sum_{\nabla_2} \mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) \cdot \mathtt{LBCT}(\Delta_2, \nabla_2, \nabla_3)$
- ✓ $\mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3) = \sum_{\Delta_2} \mathtt{UBCT}(\Delta_1, \Delta_2, \nabla_2) \cdot \mathtt{LBCT}(\Delta_2, \nabla_2, \nabla_3).$
- ✓ $\mathtt{DBCT}(\Delta_1, \nabla_3) = \sum_{\Delta_2} \mathtt{DBCT}^{\vdash}(\Delta_1, \Delta_2, \nabla_3) = \sum_{\nabla_2} \mathtt{DBCT}^{\dashv}(\Delta_1, \nabla_2, \nabla_3).$

Application of GBCT [HB21]



Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Application of GBCT [HB21]



$$\mathtt{DBCT}_{\text{total}} = \mathtt{DBCT}^{\vdash}(A_5, B_9, c_5) \cdot \mathtt{DBCT}^{\vdash}(B_9, C_{12}, d_1) \cdot \mathtt{DBCT}^{\dashv}(E'_1, f'_{12}, g'_9) \cdot \mathtt{DBCT}^{\dashv}(F'_5, g'_9, h_5)$$

$$\Pr_{\text{total}} = \Pr(d_1 \xleftarrow{2\ \mathtt{DDT}} f'_{12}) \cdot \Pr(c_5 \xleftarrow{3\ \mathtt{DDT}} f'_{12}) \cdot \Pr(C_{12} \xrightarrow{2\ \mathtt{DDT}} E'_1) \cdot \Pr(C_{12} \xrightarrow{3\ \mathtt{DDT}} F'_5)$$

$$r = 2^{-8\cdot n} \cdot \sum_{B_9} \sum_{C_{12}} \sum_{g'_9} \sum_{f'_{12}} \sum_{c_5} \sum_{d_1} \sum_{E'_1} \sum_{F'_5} \mathtt{DBCT}_{\text{total}} \cdot \Pr_{\text{total}}.$$

Differential-Linear (DL) Attack I [LH94]

Input: $E_K, (\Delta, \lambda), N, \boldsymbol{c} = \mathbb{C}(\Delta, \lambda)$

Output: 0: **real** cipher, 1: **ideal** cipher

Initialize a counter list $V[z] \leftarrow 0$ for $z \in \{0, 1\}$;

for $i = 0, \ldots, N-1$ **do**

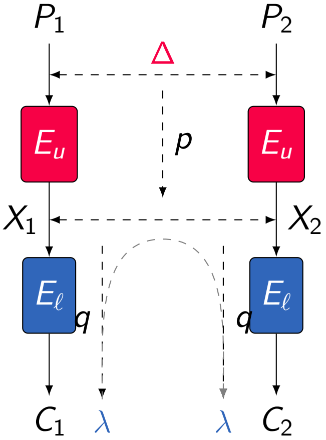
- $P_1 \xleftarrow{\$} \mathbb{F}_2^n$;
- $b_1 \leftarrow \lambda \cdot E_K(P_1)$;
- $P_2 \leftarrow P_1 \oplus \Delta$;
- $b_2 \leftarrow \lambda \cdot E_K(P_2)$;
- $V[b_1 \oplus b_2] \leftarrow V[b_1 \oplus b_2] + 1$;

if $V[0] \sim \mathcal{N}(\mu = N\frac{1+\boldsymbol{c}}{2}, \sigma^2 = N\frac{1-\boldsymbol{c}^2}{4})$ **then**

- **return** 0; `// real cipher`

else

- **return** 1; `// ideal cipher`

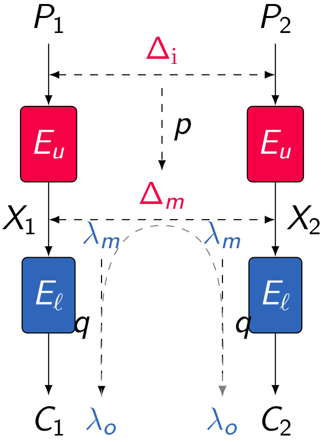


$\boldsymbol{c} = 2 \cdot \mathbb{P}(\boldsymbol{\lambda} \cdot C_1 \oplus \boldsymbol{\lambda} \cdot C_2 = 0) - 1$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder
ASK 2024 - Kolkata, India

Differential-Linear (DL) Attack II [LH94]

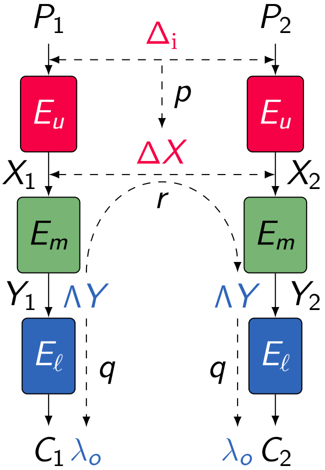
- $p = \mathbb{P}(\Delta_{\mathrm{i}} \xrightarrow{E_u} \Delta_m)$
- $q = \mathbb{C}(\lambda_m \xrightarrow{E_\ell} \lambda_{\mathrm{o}}) = 2 \cdot \mathbb{P}(\lambda_m \cdot X \oplus \lambda_{\mathrm{o}} \cdot E_\ell(X) = 0) - 1$
- Assumptions ($\Delta X = X_1 \oplus X_2$):
  1. E_u, and E_ℓ are statistically independent
  2. $\mathbb{P}\left(\lambda_m \cdot \Delta X = 0\right) = 1/2$ when $\Delta X \neq \Delta_m$
- $\mathcal{C} = \mathbb{C}\left(\lambda_{\mathrm{o}} \cdot \Delta C\right) \approx (-1)^{\lambda_m \cdot \Delta_m} \cdot pq^2 = \pm pq^2$
- Time/Data complexity: $\mathcal{O}(\mathcal{C}^{-2})$



Hosein Hadipour, Patrick Derbez, Maria Eichlseder
ASK 2024 - Kolkata, India

Sandwich Framework for DL Attack [BLN14; DKS14; Bar+19]

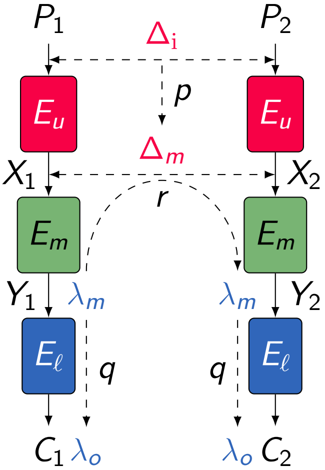
- $\mathbb{R}(\Delta X, \Lambda Y) = \mathbb{C}\,(\Lambda Y \cdot E_m(X) \oplus \Lambda Y \cdot E_m(X \oplus \Delta X))$
- $\mathbb{C}(\lambda_\mathrm{o} \cdot \Delta C) = \sum_{\Delta X, \Lambda Y} \mathbb{P}(\Delta_\mathrm{i}, \Delta X) \cdot \mathbb{R}(\Delta X, \Lambda Y) \cdot \mathbb{C}^2(\Lambda Y, \lambda_\mathrm{o})$
- $\mathbb{P}(\Delta_\mathrm{i} \xrightarrow{E_u} \Delta_m) = p$
- $\mathbb{R}(\Delta_m, \lambda_m) = r$
- $\mathbb{C}(\lambda_m \xrightarrow{E_\ell} \lambda_\mathrm{o}) = q$
- $\mathbb{C}(\lambda_\mathrm{o} \cdot \Delta C) \approx prq^2$



Hosein Hadipour, Patrick Derbez, Maria Eichlseder

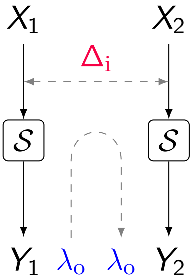
Sandwich Framework for DL Attack [BLN14; DKS14; Bar+19]

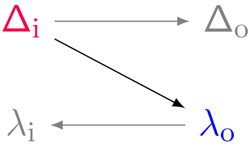
- $\mathbb{R}(\Delta X, \Lambda Y) = \mathbb{C}\left(\Lambda Y \cdot E_m(X) \oplus \Lambda Y \cdot E_m(X \oplus \Delta X)\right)$
- $\mathbb{C}(\lambda_{\mathrm{o}} \cdot \Delta C) = \sum_{\Delta X, \Lambda Y} \mathbb{P}(\Delta_{\mathrm{i}}, \Delta X) \cdot \mathbb{R}(\Delta X, \Lambda Y) \cdot \mathbb{C}^2(\Lambda Y, \lambda_{\mathrm{o}})$
- $\mathbb{P}(\Delta_{\mathrm{i}} \xrightarrow{E_u} \Delta_m) = p$
- $\mathbb{R}(\Delta_m, \lambda_m) = r$
- $\mathbb{C}(\lambda_m \xrightarrow{E_\ell} \lambda_{\mathrm{o}}) = q$
- $\mathbb{C}(\lambda_{\mathrm{o}} \cdot \Delta C) \approx prq^2$



Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Differential-Linear Connectivity Table (DLCT) [Bar+19]





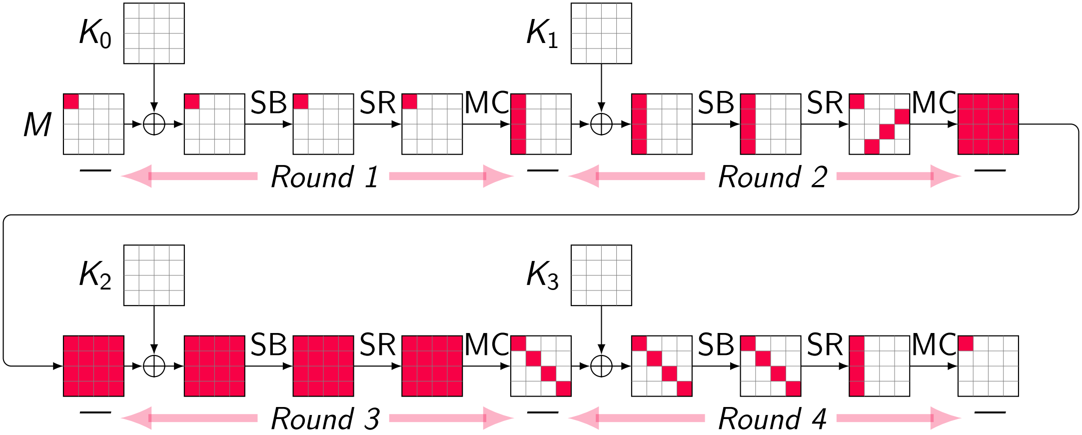
$$\mathtt{DLCT}_b(\Delta_i, \lambda_o) = \{x \in \mathbb{F}_2^n : \lambda_o \cdot S(x) \oplus \lambda_o \cdot S(x \oplus \Delta_i) = b\}$$

$$\mathtt{DLCT}(\Delta_i, \lambda_o) = |\mathtt{DLCT}_0(\Delta_i, \lambda_o)| - |\mathtt{DLCT}_1(\Delta_i, \lambda_o)|$$

$$\mathbb{C}_{\mathtt{DLCT}}(\Delta_i, \lambda_o) = 2^{-n} \cdot \mathtt{DLCT}(\Delta_i, \lambda_o)$$

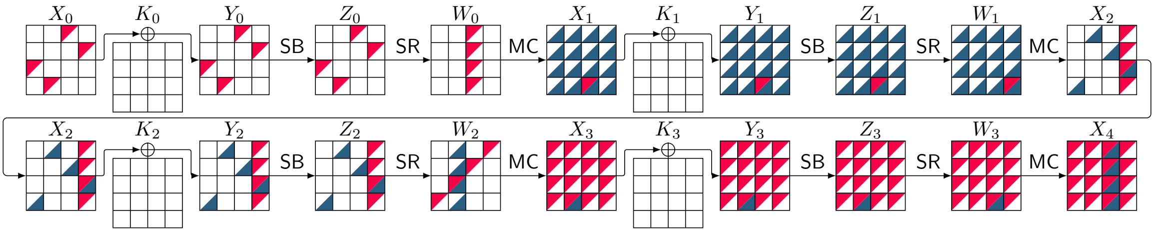
Hosein Hadipour, Patrick Derbez, Maria Eichlseder
ASK 2024 - Kolkata, India

Security of AES Against Differential/Linear Attacks



$$\mathbb{P}_{4\text{ rounds}} \leq 2^{-150},\ \mathbb{C}^2_{4\text{ rounds}} \leq 2^{-150}$$

A 4-round DL Distinguisher for AES



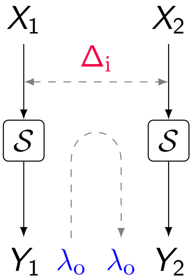
$r_u = 1, r_m = 3, r_\ell = 0,\ p = 2^{-24.00},\ r = 2^{-7.66}, q^2 = 1,\ \mathbb{C} = prq^2 = \mathbf{2^{-31.66}}$

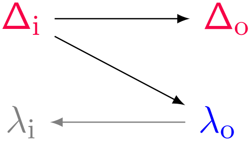
ΔX_0	00005200000000f58f000000007b0000	ΔX_1	0000000000000000000000000000b400
ΓX_4	0032000000ab00000066000000980000		-

$\mathbf{2^{63.32}}$ v.s. 2^{150}

Generalized DLCT Framework

Upper Differential-Linear Connectivity Table (UDLCT)



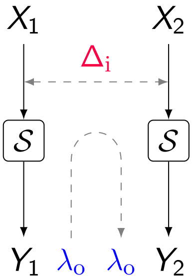


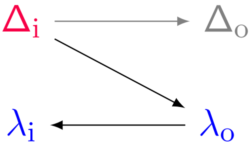
$$\mathtt{UDLCT}_b(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}}) = \{x \in \mathbb{F}_2^n : \ S(x) \oplus S(x \oplus \Delta_{\mathrm{i}}) = \Delta_{\mathrm{o}} \text{ and } \lambda_{\mathrm{o}} \cdot \Delta_{\mathrm{o}} = b\}$$

$$\mathtt{UDLCT}(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}}) = |\mathtt{UDLCT}_0(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}})| - |\mathtt{UDLCT}_1(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}})|$$

$$\mathbb{C}_{\mathtt{UDLCT}}\left(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}}\right) = 2^{-n} \cdot \mathtt{UDLCT}\left(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}}\right)$$

Lower Differential-Linear Connectivity Table (LDLCT)



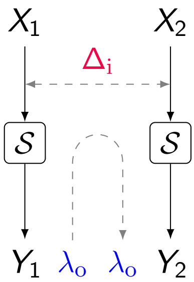


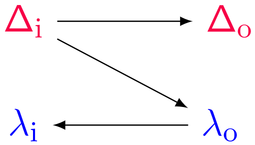
$$\mathtt{LDLCT}_b(\Delta_i, \lambda_i, \lambda_o) = \{x \in \mathbb{F}_2^n : \ \lambda_i \cdot \Delta_i \oplus \lambda_o \cdot S(x) \oplus \lambda_o \cdot S(x \oplus \Delta_i) = b\}$$

$$\mathtt{LDLCT}(\Delta_i, \lambda_i, \lambda_o) = |\mathtt{LDLCT}_0(\Delta_i, \lambda_i, \lambda_o)| - |\mathtt{LDLCT}_1(\Delta_i, \lambda_i, \lambda_o)|$$

$$\mathbb{C}_{\mathtt{LDLCT}}(\Delta_i, \lambda_i, \lambda_o) = 2^{-n} \cdot \mathtt{LDLCT}(\Delta_i, \lambda_i, \lambda_o)$$

Extended Differential-Linear Connectivity Table (EDLCT)





$$\mathtt{EDLCT}_b(\Delta_\mathrm{i}, \Delta_\mathrm{o}, \lambda_\mathrm{i}, \lambda_\mathrm{o}) = \{x \in \mathbb{F}_2^n : \ S(x) \oplus S(x \oplus \Delta_\mathrm{i}) = \Delta_\mathrm{o} \text{ and } \lambda_\mathrm{i} \cdot \Delta_\mathrm{i} \oplus \lambda_\mathrm{o} \cdot \Delta_\mathrm{o} = b\}$$

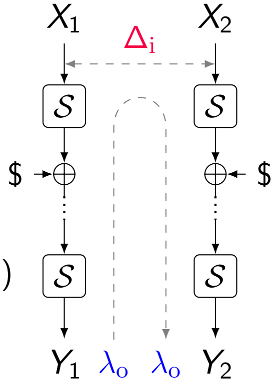
$$\mathtt{EDLCT}(\Delta_\mathrm{i}, \Delta_\mathrm{o}, \lambda_\mathrm{i}, \lambda_\mathrm{o}) = |\mathtt{EDLCT}_0(\Delta_\mathrm{i},\Delta_\mathrm{o},\lambda_\mathrm{i},\lambda_\mathrm{o})| - |\mathtt{EDLCT}_1(\Delta_\mathrm{i},\Delta_\mathrm{o},\lambda_\mathrm{i},\lambda_\mathrm{o})|$$

$$\mathbb{C}_{\mathtt{EDLCT}}(\Delta_\mathrm{i}, \Delta_\mathrm{o}, \lambda_\mathrm{i}, \lambda_\mathrm{o}) = 2^{-n} \cdot \mathtt{EDLCT}(\Delta_\mathrm{i}, \Delta_\mathrm{o}, \lambda_\mathrm{i}, \lambda_\mathrm{o})$$

Double Differential-Linear Connectivity Table (DDLCT)

$$
\begin{tikzcd}
\Delta_{\mathrm{i}} \arrow[r] \arrow[dr] & \Delta_m \arrow[r] \arrow[dr] & \Delta_{\mathrm{o}} \\
\lambda_{\mathrm{i}} \arrow[r] & \lambda_m \arrow[r] & \lambda_{\mathrm{o}}
\end{tikzcd}
$$

$$\mathtt{DDLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = 2^{-n} \cdot \sum_{\Delta_m} \sum_{\lambda_m} \mathtt{UDLCT}\left(\Delta_{\mathrm{i}}, \Delta_m, \lambda_m\right) \cdot \mathtt{LDLCT}\left(\Delta_m, \lambda_m, \lambda_{\mathrm{o}}\right)$$



Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Generalized DLCT Framework (GBCT)

- How to formulate the correaltion for more than 1 round?

$$\begin{tikzcd} \Delta_{\mathrm{i}} \arrow[r] \arrow[dr] & \Delta_{\mathrm{o}} \\ \lambda_{\mathrm{i}} \arrow[r] & \lambda_{\mathrm{o}} \end{tikzcd}$$

$\mathtt{DLCT}\left(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}\right)$

$$\begin{tikzcd} \Delta_{\mathrm{i}} \arrow[r] \arrow[dr] & \Delta_{\mathrm{o}} \\ \lambda_{\mathrm{i}} \arrow[r] & \lambda_{\mathrm{o}} \end{tikzcd}$$

$\mathtt{UDLCT}\left(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}}\right)$

$$\begin{tikzcd} \Delta_{\mathrm{i}} \arrow[r] \arrow[dr] & \Delta_{\mathrm{o}} \\ \lambda_{\mathrm{i}} \arrow[r] & \lambda_{\mathrm{o}} \end{tikzcd}$$

$\mathtt{LDLCT}\left(\Delta_{\mathrm{i}}, \lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}\right)$

$$\begin{tikzcd} \Delta_{\mathrm{i}} \arrow[r] \arrow[dr] & \Delta_{\mathrm{o}} \\ \lambda_{\mathrm{i}} \arrow[r] & \lambda_{\mathrm{o}} \end{tikzcd}$$

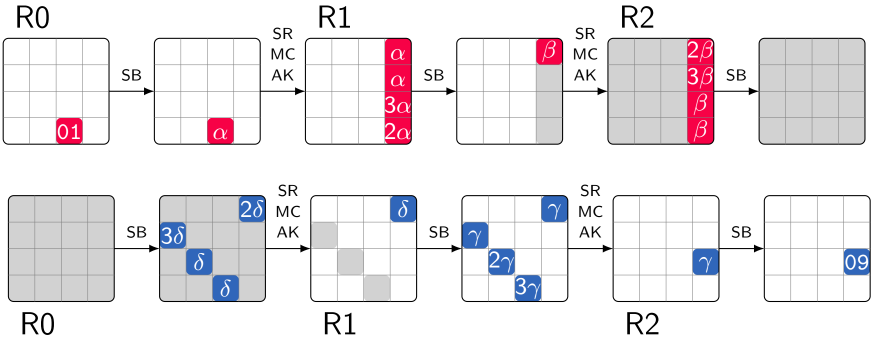
$\mathtt{EDLCT}\left(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}\right)$

$$\begin{tikzcd} \Delta_{\mathrm{i}} \arrow[r] \arrow[dr] & \Delta_{m} \arrow[r] \arrow[dr] & \Delta_{\mathrm{o}} \\ \lambda_{\mathrm{i}} \arrow[r] & \lambda_{m} \arrow[r] & \lambda_{\mathrm{o}} \end{tikzcd}$$

$\mathtt{DDLCT}\left(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}\right)$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

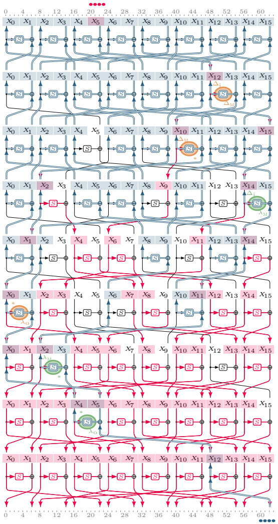
Application of the Generalized DLCT Tables - AES (– differential – linear)



$$\sum_{\alpha,\beta,\gamma,\delta} \mathbb{C}_{\mathtt{UDLCT}}(1,\alpha,\delta)\cdot\mathbb{C}_{\mathtt{EDLCT}}(\alpha,\beta,\delta,\gamma)\cdot\mathbb{C}_{\mathtt{LDLCT}}(\beta,\gamma,9) = -2^{-7.94}$$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Application of the Generalized DLCT Tables - TWINE (differential linear)



$$\mathbb{C}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = \sum_{\Delta_m} \mathbb{P}_{\mathtt{DDT}}(\Delta_{\mathrm{i}}, \Delta_m) \cdot \mathbb{C}_{\mathtt{DDLCT}}(\Delta_m, \lambda_{\mathrm{o}})$$

$$= \sum_{\lambda_m} \mathbb{C}_{\mathtt{DDLCT}}(\Delta_{\mathrm{i}}, \lambda_m) \cdot \mathbb{C}^2_{\mathtt{LAT}}(\lambda_m, \lambda_{\mathrm{o}}).$$

$$\mathbb{C}_{tot}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = \mathbb{C}^2(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}).$$

Input/Output Differences/Linear-mask	Formula	Exp. Correlation
$(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = (\mathtt{0xb4}, \mathtt{0x67})$	$-2^{-7.66}$	$-2^{-7.64}$
$(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = (\mathtt{0x02}, \mathtt{0x02})$	$-2^{-7.92}$	$-2^{-7.93}$
$(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = (\mathtt{0x55}, \mathtt{0x55})$	$-2^{-7.99}$	$-2^{-7.98}$
$(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = (\mathtt{0xbf}, \mathtt{0xef})$	$-2^{-8.05}$	$-2^{-8.06}$
$(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = (\mathtt{0xfe}, \mathtt{0x06})$	$-2^{-8.26}$	$-2^{-8.25}$
$(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = (\mathtt{0x4b}, \mathtt{0x1a})$	$-2^{-8.43}$	$-2^{-8.44}$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder
ASK 2024 - Kolkata, India

Differential-Linear Switches and Deterministic Trails

Cell-Wise and Bit-Wise Switches

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	4	0	a	7	b	e	1	d	9	f	6	8	5	2	c	3

$\Delta \setminus \lambda$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	0	0	0	-16	0	0	0	0	0	0	0	0	0	0	0
2	16	-8	-8	0	0	0	8	-8	0	-8	0	8	0	0	0	0
3	16	0	-8	-8	0	-8	8	0	0	0	0	0	0	-8	0	8
4	16	0	-8	0	0	0	-8	0	-16	0	8	0	0	0	8	0
5	16	0	-8	0	0	0	-8	0	0	0	8	0	-16	0	8	0
6	16	-8	8	-8	0	0	-8	0	0	-8	0	0	0	0	0	8
7	16	0	8	0	0	-8	-8	-8	0	0	0	8	0	-8	0	0
8	16	0	0	0	-16	0	0	0	-16	0	0	0	16	0	0	0
9	16	-8	0	-8	16	-8	0	-8	0	8	0	-8	0	8	0	-8
a	16	0	0	8	0	8	0	0	0	0	-8	0	0	-8	-8	-8
b	16	8	0	0	0	0	0	8	0	-8	-8	-8	0	0	-8	0
c	16	0	0	-8	0	0	0	-8	16	0	0	-8	0	0	0	-8
d	16	-8	0	0	0	-8	0	0	0	8	0	0	-16	8	0	0
e	16	0	0	0	0	8	0	8	0	0	-8	-8	0	-8	-8	0
f	16	8	0	8	0	0	0	0	0	-8	-8	0	0	0	-8	-8

- Cell-wise switches: $\mathtt{DLCT}(\Delta_{\mathrm{i}}, 0) = \mathtt{DLCT}(0, \lambda_{\mathrm{o}}) = 2^n$ for all $\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}$
- Bit-wise switches: $\mathtt{DLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = \pm 2^n$ for $\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}} \neq 0$
  - Example: $\mathbb{C}\,(9, 4) = \frac{16}{16}$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Deterministic Bit-Wise Differential Trails (Forward)

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	4	0	a	7	b	e	1	d	9	f	6	8	5	2	c	3

$\Delta_i \setminus \Delta_o$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
2	0	2	0	2	0	0	0	4	0	2	2	0	0	0	2	2
3	0	2	0	2	0	0	4	0	0	2	2	0	0	0	2	2
4	0	0	0	0	0	0	0	0	0	0	4	4	2	2	2	2
5	0	0	0	0	2	2	2	2	0	0	4	4	0	0	0	0
6	0	2	0	2	0	4	0	0	0	2	2	0	2	2	0	0
7	0	2	0	2	4	0	0	0	0	2	2	0	2	2	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	4	4	4	4
9	0	4	4	0	0	0	0	0	0	4	0	4	0	0	0	0
a	0	0	2	2	2	0	0	2	4	0	0	0	0	2	0	2
b	0	0	2	2	0	2	2	0	4	0	0	0	2	0	2	0
c	0	4	4	0	2	2	2	2	0	0	0	0	0	0	0	0
d	0	0	0	0	2	2	2	2	0	4	0	4	0	0	0	0
e	0	0	2	2	0	2	2	0	4	0	0	0	0	2	0	2
f	0	0	2	2	2	0	0	2	4	0	0	0	2	0	2	0

$$\Delta_i = (0,0,0,0) \xrightarrow{S} \Delta_o = (0,0,0,0)$$

$$\Delta_i = (0,0,0,1) \xrightarrow{S} \Delta_o = (?,1,?,?)$$

$$\Delta_i = (0,1,0,0) \xrightarrow{S} \Delta_o = (1,?,?,?)$$

$$\Delta_i = (1,0,0,0) \xrightarrow{S} \Delta_o = (1,1,?,?)$$

$$\Delta_i = (1,0,0,1) \xrightarrow{S} \Delta_o = (?,0,?,?)$$

$$\Delta_i = (1,1,0,0) \xrightarrow{S} \Delta_o = (0,?,?,?)$$

Deterministic Bit-Wise Linear Trails (Backward)

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	4	0	a	7	b	e	1	d	9	f	6	8	5	2	c	3

$\lambda_i \setminus \lambda_o$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	4	-4	0	-8	-4	-4	0	0	4	-4	-8	0	4	4
2	0	0	0	0	0	0	0	0	0	8	8	0	0	8	-8	0
3	0	-8	4	4	0	0	-4	4	0	0	-4	4	-8	0	-4	-4
4	0	4	0	4	0	4	8	-4	0	4	0	4	-8	-4	0	4
5	0	4	-4	-8	0	-4	-4	0	0	4	-4	8	0	-4	-4	0
6	0	-4	8	4	0	-4	0	-4	0	4	0	4	8	-4	0	4
7	0	4	4	0	0	-4	4	-8	0	-4	-4	0	0	4	-4	-8
8	0	0	0	0	0	0	0	0	0	0	8	8	0	0	8	-8
9	0	0	-4	4	8	0	-4	-4	0	0	4	-4	0	-8	-4	-4
a	0	8	0	8	0	-8	0	8	0	0	0	0	0	0	0	0
b	0	0	-4	4	-8	0	-4	-4	0	8	-4	-4	0	0	4	-4
c	0	4	0	4	0	4	-8	-4	8	-4	0	4	0	4	0	4
d	0	4	4	0	-8	4	-4	0	-8	-4	4	0	0	-4	-4	0
e	0	4	8	-4	0	4	0	4	8	4	0	-4	0	-4	0	-4
f	0	-4	-4	0	-8	-4	4	0	8	-4	4	0	0	-4	-4	0

$$\lambda_{\mathrm{i}} = (1, ?, ?, 1) \xleftarrow{S} \lambda_{\mathrm{o}} = (0, 1, 0, 0)$$

$$\lambda_{\mathrm{i}} = (1, 1, ?, ?) \xleftarrow{S} \lambda_{\mathrm{o}} = (1, 0, 0, 0)$$

$$\lambda_{\mathrm{i}} = (0, ?, ?, ?) \xleftarrow{S} \lambda_{\mathrm{o}} = (1, 1, 0, 0)$$

Bit-Wise Switches and Deterministic Trails

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$\mathcal{S}(x)$	4	0	a	7	b	e	1	d	9	f	6	8	5	2	c	3

$\Delta \setminus \lambda$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	0	0	0	-16	0	0	0	0	0	0	0	0	0	0	0
2	16	-8	-8	0	0	0	8	-8	0	-8	0	8	0	0	0	0
3	16	0	-8	-8	0	-8	8	0	0	0	0	0	0	-8	0	8
4	16	0	-8	0	0	0	-8	0	-16	0	8	0	0	0	8	0
5	16	0	-8	0	0	0	-8	0	0	0	8	0	-16	0	8	0
6	16	-8	8	-8	0	0	-8	0	0	-8	0	0	0	0	0	8
7	16	0	8	0	0	-8	-8	-8	0	0	0	8	0	-8	0	0
8	16	0	0	0	-16	0	0	0	-16	0	0	0	16	0	0	0
9	16	-8	0	-8	16	-8	0	-8	0	8	0	-8	0	8	0	-8
a	16	0	0	8	0	8	0	0	0	0	-8	0	0	-8	-8	-8
b	16	8	0	0	0	0	0	8	0	-8	-8	-8	0	0	-8	0
c	16	0	0	-8	0	0	0	-8	16	0	0	-8	0	0	0	-8
d	16	-8	0	0	0	-8	0	0	0	8	0	0	-16	8	0	0
e	16	0	0	0	0	8	0	8	0	0	-8	-8	0	-8	-8	0
f	16	8	0	8	0	0	0	0	0	-8	-8	0	0	0	-8	-8

$$\Delta_{\mathrm{i}} = (0,0,0,1) \xrightarrow{S} \Delta_{\mathrm{o}} = (?,1,?,?)$$

$$\Delta_{\mathrm{i}} = (0,1,0,0) \xrightarrow{S} \Delta_{\mathrm{o}} = (1,?,?,?)$$

$$\Delta_{\mathrm{i}} = (1,0,0,0) \xrightarrow{S} \Delta_{\mathrm{o}} = (1,1,?,?)$$

$$\Delta_{\mathrm{i}} = (1,0,0,1) \xrightarrow{S} \Delta_{\mathrm{o}} = (?,0,?,?)$$

$$\Delta_{\mathrm{i}} = (1,1,0,0) \xrightarrow{S} \Delta_{\mathrm{o}} = (0,?,?,?)$$

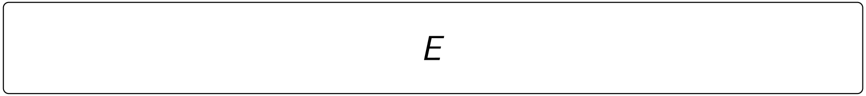
$$\lambda_{\mathrm{i}} = (1,?,?,1) \xleftarrow{S} \lambda_{\mathrm{o}} = (0,1,0,0)$$

$$\lambda_{\mathrm{i}} = (1,1,?,?) \xleftarrow{S} \lambda_{\mathrm{o}} = (1,0,0,0)$$

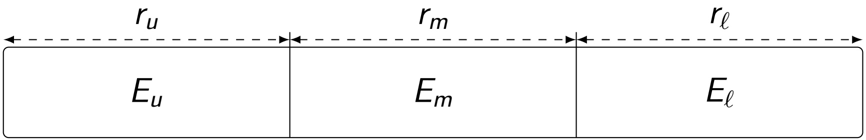
$$\lambda_{\mathrm{i}} = (0,?,?,?) \xleftarrow{S} \lambda_{\mathrm{o}} = (1,1,0,0)$$

Automatic Tools to Search for DL Distinguishers

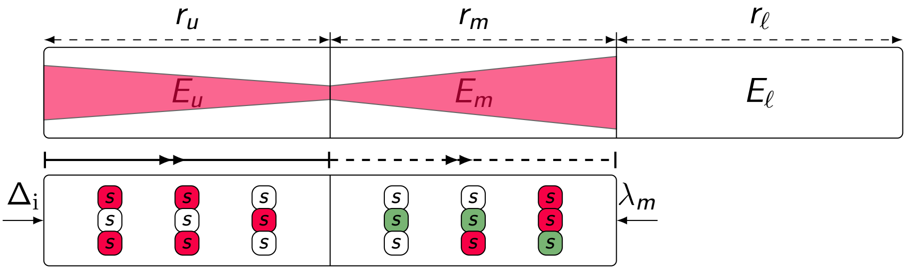
Overview of Our Method to Search for Distinguishers



Overview of Our Method to Search for Distinguishers

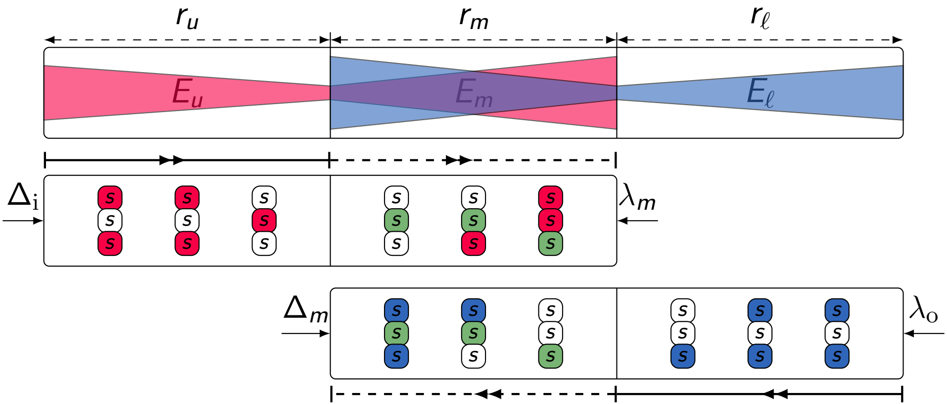


Overview of Our Method to Search for Distinguishers



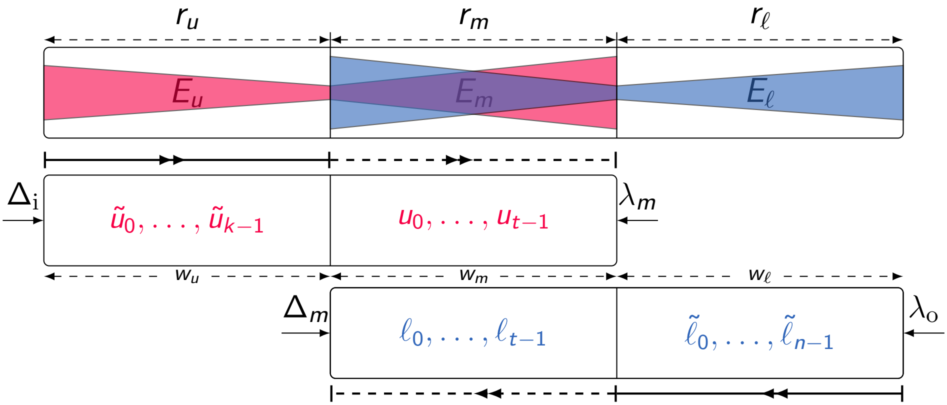
differentially active S-box   linearly active S-box   common active S-box

Overview of Our Method to Search for Distinguishers



differentially active S-box · linearly active S-box · common active S-box

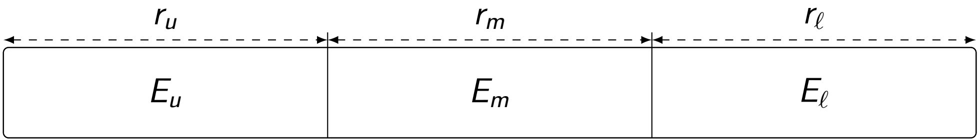
Overview of Our Method to Search for Distinguishers



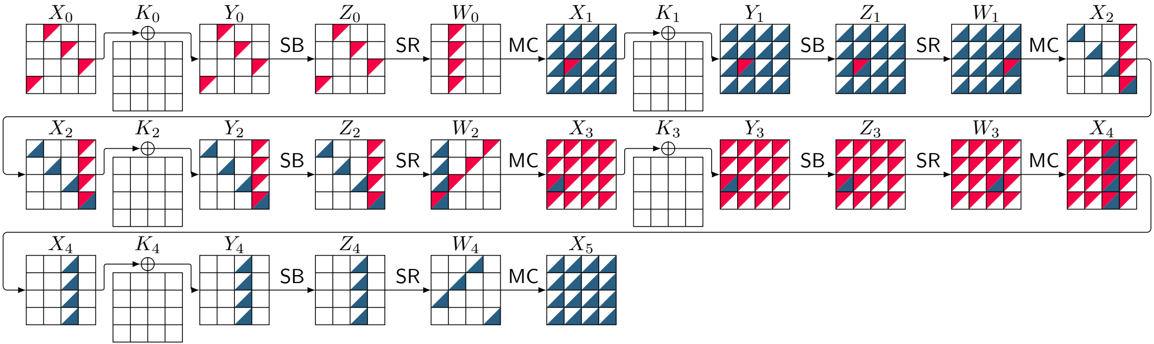
$$\min\left(\sum_{i=0}^{k-1} w_u \cdot \tilde{u}_i + \sum_{j=0}^{t-1} w_m \cdot \mathtt{bool2int}(\ell_j + u_j = 2) + \sum_{k=0}^{n-1} w_\ell \cdot \tilde{\ell}_k\right)$$

Usage of Our Tool

```
python3 attack.py -RU 6 -RM 10 -RL 6
```



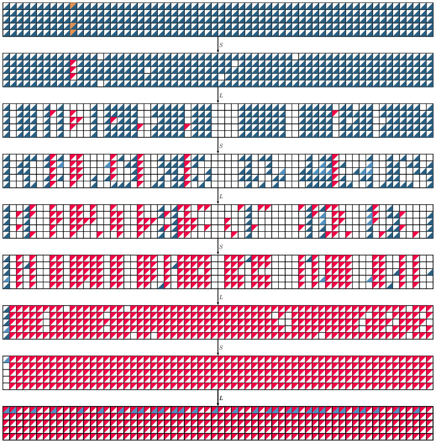
Results: A 5-round DL Distinguisher for AES



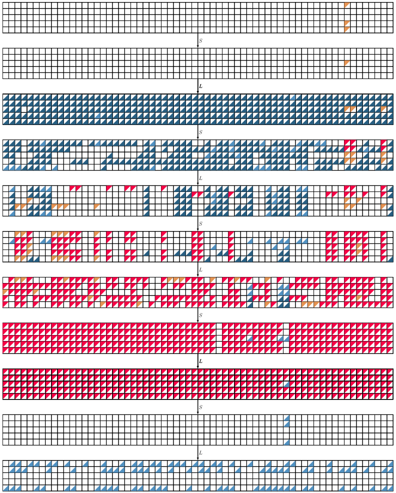
$r_0 = 1, r_m = 3, r_1 = 1,\ p = 2^{-24.00}, r = 2^{-7.66},\ q^2 = 2^{-24.00},\ prq^2 = 2^{-55.66}$

ΔX_0	`001c00000000e200000000dfb3000000`	ΔX_1	`0000000000000000f700000000000000`
ΓX_4	`00000000000000670000000000000000`	ΓX_5	`21d3814d93b1ef228e923507f67383fd`

Results: Application to Ascon-p(active difference unknown difference active mask unknown mask)



$\mathbb{C} = 1$



$\mathbb{C} = 2^{-4.33}$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Contributions and Future Works

Contributions and Future Works

- Contributions
  - We generalized the DLCT framework from one S-box layer to multiple rounds
  - We proposed an automatic tool for finding optimum DL distinguishers
  - We applied our tool to almost any design paradigm
- Future works
  - Extending the application of our tool to other primitives, e.g., ARX
  - Extending our tool to a unified model for finding complete attack (key recovery)

: https://github.com/hadipourh/DL

: https://ia.cr/2024/255

Bibliography I

[Bar+19] Achiya Bar-On et al. **DLCT: A New Tool for Differential-Linear Cryptanalysis**. EUROCRYPT 2019. Vol. 11476. LNCS. Springer, 2019, pp. 313–342. DOI: 10.1007/978-3-030-17653-2_11.

[BLN14] Céline Blondeau, Gregor Leander, and Kaisa Nyberg. **Differential-Linear Cryptanalysis Revisited**. FSE 2014. Ed. by Carlos Cid and Christian Rechberger. Vol. 8540. LNCS. Springer, 2014, pp. 411–430. DOI: 10.1007/978-3-662-46706-0_21.

[Bou+20] Hamid Boukerrou et al. **On the Feistel Counterpart of the Boomerang Connectivity Table Introduction and Analysis of the FBCT**. *IACR Trans. Symmetric Cryptol.* 2020.1 (2020), pp. 331–362. DOI: 10.13154/TOSC.V2020.I1.331-362.

Bibliography II

[BS90] Eli Biham and Adi Shamir. **Differential Cryptanalysis of DES-like Cryptosystems**. CRYPTO '90. Ed. by Alfred Menezes and Scott A. Vanstone. Vol. 537. LNCS. Springer, 1990, pp. 2–21. DOI: 10.1007/3-540-38424-3_1.

[Cid+18] Carlos Cid et al. **Boomerang Connectivity Table: A New Cryptanalysis Tool**. EUROCRYPT 2018. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10821. LNCS. Springer, 2018, pp. 683–714. DOI: 10.1007/978-3-319-78375-8_22.

[DDV20] Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. **Catching the Fastest Boomerangs Application to SKINNY**. *IACR Trans. Symmetric Cryptol.* 2020.4 (2020), pp. 104–129. DOI: 10.46586/TOSC.V2020.I4.104-129.

Bibliography III

[DIK08] Orr Dunkelman, Sebastiaan Indesteege, and Nathan Keller. **A Differential-Linear Attack on 12-Round Serpent**. INDOCRYPT 2008. Ed. by Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das. Vol. 5365. LNCS. Springer, 2008, pp. 308–321. DOI: 10.1007/978-3-540-89754-5_24.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. **A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony**. CRYPTO. Vol. 6223. LNCS. Springer, 2010, pp. 393–410. DOI: 10.1007/978-3-642-14623-7_21.

[DKS14] Orr Dunkelman, Nathan Keller, and Adi Shamir. **A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony**. *J. Cryptol.* 27.4 (2014), pp. 824–849. DOI: 10.1007/s00145-013-9154-9.

Bibliography IV

[HB21] Hosein Hadipour and Nasour Bagheri. **Improved Rectangle Attacks on SKINNY and CRAFT**. *IACR Trans. Symmetric Cryptol.* 2021.2 (2021), pp. 140–198. DOI: 10.46586/TOSC.V2021.I2.140-198.

[HNE22] Hosein Hadipour, Marcel Nageler, and Maria Eichlseder. **Throwing Boomerangs into Feistel Structures Application to CLEFIA, WARP, LBlock, LBlock-s and TWINE**. *IACR Trans. Symmetric Cryptol.* 2022.3 (2022), pp. 271–302. DOI: 10.46586/TOSC.V2022.I3.271-302.

[LH94] Susan K. Langford and Martin E. Hellman. **Differential-Linear Cryptanalysis**. CRYPTO '94. Vol. 839. Springer, 1994, pp. 17–25. DOI: 10.1007/3-540-48658-5_3.

Bibliography V

[Mat93] Mitsuru Matsui. **Linear Cryptanalysis Method for DES Cipher**. EUROCRYPT '93. Ed. by Tor Helleseth. Vol. 765. LNCS. Springer, 1993, pp. 386–397. DOI: 10.1007/3-540-48285-7_33.

[SQH19] Ling Song, Xianrui Qin, and Lei Hu. **Boomerang Connectivity Table Revisited. Application to SKINNY and AES**. *IACR Trans. Symmetric Cryptol.* 2019.1 (2019), pp. 118–141. DOI: 10.13154/TOSC.V2019.I1.118-141. URL: https://doi.org/10.13154/tosc.v2019.i1.118-141.

[Wag99] David A. Wagner. **The Boomerang Attack**. FSE. Vol. 1636. LNCS. Springer, 1999, pp. 156–170. DOI: 10.1007/3-540-48519-8_12.

[WP19] Haoyang Wang and Thomas Peyrin. **Boomerang Switch in Multiple Rounds. Application to AES Variants and Deoxys**. *IACR Trans. Symmetric Cryptol.* 2019.1 (2019), pp. 142–169. DOI: 10.13154/TOSC.V2019.I1.142-169.

Bibliography VI

[ZWH24] Yanyan Zhou, Senpeng Wang, and Bin Hu. **MILP/MIQCP-Based Fully Automatic Method of Searching for Differential-Linear Distinguishers for SIMON-Like Ciphers**. *IET Information Security* 2024 (2024). DOI: 10.1049/2024/8315115.

Properties of Generalized DLCT Tables - I

- $\mathtt{DLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = \sum_{\Delta_{\mathrm{o}}} \mathtt{UDLCT}(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}})$
- $\mathtt{UDLCT}(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{o}}) = (-1)^{\Delta_{\mathrm{o}} \cdot \lambda_{\mathrm{o}}} \mathtt{DDT}(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}})$
- $\mathtt{LDLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}) = (-1)^{\Delta_{\mathrm{i}} \cdot \lambda_{\mathrm{i}}} \mathtt{DLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}})$
- $\mathtt{EDLCT}(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}) = (-1)^{\lambda_{\mathrm{i}} \cdot \Delta_{\mathrm{i}} \oplus \lambda_{\mathrm{o}} \cdot \Delta_{\mathrm{o}}} \mathtt{DDT}(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}})$
- $\mathtt{LDLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}) = \sum_{\Delta_{\mathrm{o}}} \mathtt{EDLCT}(\Delta_{\mathrm{i}}, \Delta_{\mathrm{o}}, \lambda_{\mathrm{i}}, \lambda_{\mathrm{o}})$
- $\sum_{\Delta_{\mathrm{i}}} \mathtt{LDLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{i}}, \lambda_{\mathrm{o}}) = \mathtt{LAT}^2(\lambda_{\mathrm{i}}, \lambda_{\mathrm{o}})$

Properties of Generalized $\texttt{DLCT}$ Tables - II

- $\texttt{DDLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) = 2^{-n} \cdot \sum_{\Delta_m} \sum_{\lambda_m} \texttt{UDLCT}\left(\Delta_{\mathrm{i}}, \Delta_m, \lambda_m\right) \cdot \texttt{LDLCT}\left(\Delta_m, \lambda_m, \lambda_{\mathrm{o}}\right)$

$$\begin{aligned}\texttt{DDLCT}(\Delta_{\mathrm{i}}, \lambda_{\mathrm{o}}) &= \sum_{\Delta_m} \texttt{DDT}(\Delta_{\mathrm{i}}, \Delta_m) \cdot \texttt{DLCT}(\Delta_m, \lambda_{\mathrm{o}}) \\ &= 2^{-n} \sum_{\lambda_m} \texttt{DLCT}(\Delta_{\mathrm{i}}, \lambda_m) \cdot \texttt{LAT}^2(\lambda_m, \lambda_{\mathrm{o}}).\end{aligned}$$

Hosein Hadipour, Patrick Derbez, Maria Eichlseder

Results: Distinguishers for up to 17 Rounds of TWINE

- Comparing the data complexity of best boomerang and DL distinguishers

# Rounds	Boomerang [HNE22]	Differential-Linear	Gain
5	1	1	1
7	$2^{3.20}$	1	$2^{3.20}$
13	$2^{34.32}$	$2^{27.16}$	$2^{7.16}$
14	$2^{42.25}$	$2^{31.28}$	$2^{10.97}$
15	$2^{51.03}$	$2^{38.98}$	$2^{12.05}$
16	$2^{58.04}$	$2^{47.28}$	$2^{10.76}$
17	-	$2^{59.24}$	-

Results: Distinguishers for up to 17 Rounds of LBlock

- Comparing the data complexity of best boomerang and DL distinguishers

# Rounds	Boomerang [HNE22]	Differential-Linear	Gain
5	1	1	1
7	$2^{2.97}$	1	$2^{2.97}$
13	$2^{30.28}$	$2^{23.78}$	$2^{6.50}$
14	$2^{38.86}$	$2^{30.34}$	$2^{8.52}$
15	$2^{46.90}$	$2^{38.26}$	$2^{8.64}$
16	$2^{57.16}$	$2^{46.26}$	$2^{10.90}$
17	-	$2^{58.30}$	-

Results: Distinguishers for up to 8 Rounds of CLEFIA

- Comparing the data complexity of best boomerang and DL distinguishers

# Rounds	Boomerang [HNE22]	Differential-Linear	Gain
3	1	1	1
4	$2^{6.32}$	1	$2^{6.32}$
5	$2^{12.26}$	$2^{5.36}$	$2^{6.90}$
6	$2^{22.45}$	$2^{14.14}$	$2^{8.31}$
7	$2^{32.67}$	$2^{23.50}$	$2^{9.17}$
8	$2^{76.03}$	$2^{66.86}$	$2^{9.17}$

Results: Application to SERPENT

- 💻: Experimentally verified

Cipher	#R	$\mathbb{C}$	💻	Ref.
SERPENT	3	$\mathbf{2^{-0.68}}$	✓	This work
	4	$2^{-12.75}$		[DIK08]
	4	$\mathbf{2^{-5.54}}$	✓	This work
	5	$2^{-16.75}$		[DIK08]
	5	$\mathbf{2^{-11.10}}$	✓	This work
	8	$2^{-39.18}$		This work
	9	$2^{-56.50}$		[DIK08]
	9	$\mathbf{2^{-50.95}}$		This work

Results: Application to Simeck

- 💻: Experimentally verified

Cipher	#R	$\mathbb{C}$	💻	Ref.
Simeck-32	7	$\mathbf{1}$	✓	This work
	14	$2^{-16.63}$		[ZWH24]
	14	$\mathbf{2^{-13.92}}$	✓	This work

Cipher	#R	$\mathbb{C}$	💻	Ref.
Simeck-48	8	$\mathbf{1}$	✓	This work
	17	$2^{-22.37}$		[ZWH24]
	17	$\mathbf{2^{-13.89}}$	✓	This work
	18	$2^{-24.75}$		[ZWH24]
	18	$\mathbf{2^{-15.89}}$		This work
	19	$\mathbf{2^{-17.89}}$		This work
	20	$\mathbf{2^{-21.89}}$		This work

Cipher	#R	$\mathbb{C}$	💻	Ref.
Simeck-64	10	$\mathbf{1}$	✓	This work
	24	$2^{-38.13}$		[ZWH24]
	24	$\mathbf{2^{-25.14}}$		This work
	25	$2^{-41.04}$		[ZWH24]
	25	$\mathbf{2^{-27.14}}$		This work
	26	$\mathbf{2^{-30.35}}$		This work