Round-Based Approximation of (Higher-Order) Differential-Linear Correlation

A Geometric Approach Perspective

Kai Hu[1], Zhongfeng Niu[2], and Meiqin Wang[1]

1. Shandong University
2. Nanyang Technological University

November 6, 2025@ Gelrecrypt, Nijmegen

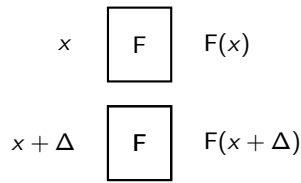
Background Knowledge

Differential-linear attacks [LH94]

- Differential-linear distinguisher for $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$:

$$\mathrm{DL}[\Delta \xrightarrow{F} \lambda] = \mathrm{Cor}[\lambda^\top (F(x) + F(x+\Delta)) = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} (-1)^{v^\top D_\Delta F(x)}$$

where $D_\Delta F(x) = F(x) + F(x+\Delta)$



Question: How to approximate $\mathrm{DL}[\Delta \xrightarrow{F} \lambda]$?

Existing approximation methods (1)

- Classical 2-phase approximation [LH94]: $\mathsf{F} = \mathsf{F}_1 \circ \mathsf{F}_0, \quad \mathsf{D}[\Delta \xrightarrow{\mathsf{F}_0} \Delta'] = p, \quad \mathsf{Cor}[\lambda' \xrightarrow{\mathsf{F}_1} \lambda] = \varepsilon$

$$\mathsf{DL}[\Delta \xrightarrow{\mathsf{F}} \lambda] = \pm p\varepsilon^2$$

  Two assumptions:
  1. Independence between F_0 and F_1
  2. When $\Delta \xrightarrow{\mathsf{F}_0} \Delta'$ does NOT happen with $1 - p$ probability, the correlation is 0

- Classical 3-phase refinement [DSK08]: $\mathsf{F} = \mathsf{F}_2 \circ \mathsf{F}_1 \circ \mathsf{F}_0, \quad \mathsf{D}[\Delta \xrightarrow{\mathsf{F}_0} \Delta'] = p, \quad \mathsf{Cor}[\lambda' \xrightarrow{\mathsf{F}_2} \lambda] = \varepsilon$
  Experiments for F_1: $\mathsf{Cor}[\Delta' \xrightarrow{\mathsf{F}_1} \lambda'] = c$

$$\mathsf{DL}[\Delta \xrightarrow{\mathsf{F}} \lambda] = pc\varepsilon^2$$

- Closed formula, removing Assumption 2 [BLN14]: $\mathsf{F} = \mathsf{F}_1 \circ \mathsf{F}_0$

$$\mathsf{DL}[\Delta \xrightarrow{\mathsf{F}} \lambda] = \sum_{\lambda'} \mathsf{DL}[\Delta \xrightarrow{\mathsf{F}_0} \lambda']\mathsf{Cor}[\lambda' \xrightarrow{\mathsf{F}_1} \lambda]$$

Existing approximation methods (2)

- Differential-linear connectivity table (DLCT) [BDK+19]:
  $\mathsf{F} = \mathsf{F}_2 \circ \mathsf{F}_1 \circ \mathsf{F}_0, \quad \mathsf{D}[\Delta \xrightarrow{\mathsf{F}_0} \Delta'] = p, \quad \mathsf{Cor}[\lambda' \xrightarrow{\mathsf{F}_2} \lambda] = \varepsilon$
  DLCT for F_1 (1 layer of S-boxes): $\mathsf{Cor}[\Delta' \xrightarrow{\mathsf{F}_1} \lambda'] = DLCT[\Delta', \lambda']$

$$\mathsf{DL}[\Delta \xrightarrow{\mathsf{F}} \lambda] = p \cdot DLCT[\Delta', \lambda'] \cdot \varepsilon^2$$

- Algebraic transition form (ATF) [LLL21]: denote $f(x) := \lambda^\top \mathsf{F}(x)$

$$\lambda^\top(\mathsf{F}(x) + \mathsf{F}(x+\Delta)) = f(x) + f(x+\Delta) = \sum_{u \in \mathbb{F}_2} f(x + u \cdot \Delta) = \mathsf{Coe}_f(u)$$

$$\mathsf{DL}[\Delta \xrightarrow{\mathsf{F}} \lambda] := \mathsf{Cor}[\lambda^\top(\mathsf{F}(x) + \mathsf{F}(x+\Delta))] = \mathsf{Cor}[\mathsf{Coe}_f(u)]$$

F is iterative: $\mathsf{F} = \mathsf{F}_{r-1} \circ \mathsf{F}_{r-2} \circ \cdots \mathsf{F}_0$

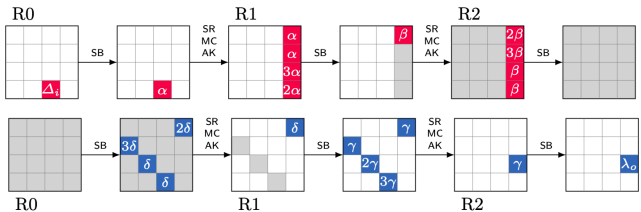
$$x + u\Delta \xrightarrow{\mathsf{F}_0} \alpha_1 + u\beta_1 \xrightarrow{\mathsf{F}_1} \cdots\cdots \xrightarrow{\mathsf{F}_{r-1}} \alpha_r + u\beta_r$$

Approximate the bias of bits of α_i and β_i according to [ANFs]

Existing approximation methods (3)

- Generalized differential-linear connectivity table (DLCT) [HDE+24]:
  Using a boomerang way, different tables are constructed to cover more middle rounds

$$\mathrm{DL}[\Delta_i \to \lambda_o] = \sum_{\alpha,\beta,\gamma,\delta} \mathrm{Cor}_{\mathrm{UDLCT}}(\Delta_i, \alpha, \delta) \cdot \mathrm{Cor}_{\mathrm{EDLCT}}(\alpha, \beta, \delta, \gamma) \cdot \mathrm{Cor}_{\mathrm{LDLCT}}(\beta, \gamma, \lambda_o)$$



(The picture was copied from [HDE+24])

- Truncated differential table (TDT) [PZW+24]: trace the propagation of truncated differentials

Geometric approach [Bey21]

A meta-approach that enables systematically thinking about various cryptanalytic methods

- Free vector space: Regarding elements in $\mathbb{F}_2^n$ as basis vectors, where u is denoted by δ_u. We can construct a vector space:

$$\mathbb{R}[\mathbb{F}_2^n] = \left\{ \sum_u k_u \delta_u, k_u \in \mathbb{R}, u \in \mathbb{F}_2^n \right\} \quad (\mathbb{R} \text{ is the field of real numbers})$$

- Obtain a linear extension function (pushforward) from any (nonlinear) function
  For $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$, we define T^F as

$$\mathsf{T}^\mathsf{F} : \mathbb{R}[\mathbb{F}_2^n] \to \mathbb{R}[\mathbb{F}_2^n]; \quad \sum_u k_u \delta_u \mapsto \sum_u k_u \delta_{\mathsf{F}(u)}$$

  Nonlinear F can be embedded into a much larger linear map T^F

Transition matrix and change-of-basis [Bey21]

- $\mathsf{T}^{\mathsf{F}} : \mathbb{R}[\mathbb{F}_2^n] \to \mathbb{R}[\mathbb{F}_2^n]$ is a linear map. Fixing bases for the input/output spaces, we will get a matrix w.r.t the bases
- Regard $(\delta_u, u \in \mathbb{F}_2^n)$ as the standard basis for the input and output spaces, the corresponding transition matrix has elements as

$$\mathsf{T}^{\mathsf{F}}[v,u] = \delta_v^\top \mathsf{T}^{\mathsf{F}}(\delta_u) = \delta_v(\mathsf{F}(u)) \quad \left(\delta_u(x) := \begin{cases} 1, & u = x \\ 0, & \text{otherwise} \end{cases}\right)$$

- Choose another basis $(\beta_u, u \in \mathbb{F}_2^n)$ satisfying $(\delta_u, u \in \mathbb{F}_2^n) = (\beta_u, u \in \mathbb{F}_2^n) \cdot \mathsf{H}$

$$\mathsf{C}^{\mathsf{F}} = \mathsf{H}\ \mathsf{T}^{\mathsf{F}}\ \mathsf{H}^{-1}$$

  When H is the Walsh-Hadamard matrix, $(\beta_u, u \in \mathbb{F}_2^n)$ is called the linear basis. C^{F} is called the correlation matrix [DGV94].
- The coordinate of C^{F} is

$$\mathsf{C}^{\mathsf{F}}[v,u] = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{u^\top x + v^\top \mathsf{F}(x)}$$

d-wise form of a function

Definition (d-wise form of a function [HZC+25])

The d-wise form of a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as

$$\mathsf{F}^{\times d} : \mathbb{F}_2^{n \times d} \to \mathbb{F}_2^{n \times d}$$
$$(x, \theta_1, \theta_2, \ldots, \theta_{d-1}) \mapsto (\mathsf{F}(x), \mathsf{D}_{\theta_1}\mathsf{F}(x), \ldots, \mathsf{D}_{\theta_{d-1}}\mathsf{F}(x))$$

$\mathsf{D}_\theta\mathsf{F}(x)$ is the derivative of F in the direction of θ at the point x, i.e., $\mathsf{D}_\theta\mathsf{F}(x) = \mathsf{F}(x) + \mathsf{F}(x + \theta)$.

Correlation matrix of $\mathsf{F}^{\times d}$:

$$\mathsf{C}^{\mathsf{F}^{\times d}} = \left(\bigotimes_{i=0}^{d-1} \mathsf{H}\right) \cdot \mathsf{T}^{\mathsf{F}^{\times d}} \cdot \left(\bigotimes_{i=0}^{d-1} \mathsf{H}\right)^{-1} = \left(\bigotimes_{i=0}^{d-1} \mathsf{H}\right) \cdot \mathsf{T}^{\mathsf{F}^{\times d}} \cdot \left(\bigotimes_{i=0}^{d-1} \mathsf{H}^{-1}\right)$$

$\bigotimes$: Kronecker/tensor product

d-wise form of a function

Definition (d-wise form of a function [HZC+25])

The d-wise form of a function $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as

$$\mathsf{F}^{\times d} : \mathbb{F}_2^{n \times d} \to \mathbb{F}_2^{n \times d}$$
$$(x, \theta_1, \theta_2, \ldots, \theta_{d-1}) \mapsto (\mathsf{F}(x), \mathsf{D}_{\theta_1}\mathsf{F}(x), \ldots, \mathsf{D}_{\theta_{d-1}}\mathsf{F}(x))$$

$\mathsf{D}_\theta\mathsf{F}(x)$ is the derivative of F in the direction of θ at the point x, i.e., $\mathsf{D}_\theta\mathsf{F}(x) = \mathsf{F}(x) + \mathsf{F}(x+\theta)$.

Correlation matrix of $\mathsf{F}^{\times d}$:

$$\mathsf{C}^{\mathsf{F}^{\times d}} = \left(\bigotimes_{i=0}^{d-1} \mathsf{H}\right) \cdot \mathsf{T}^{\mathsf{F}^{\times d}} \cdot \left(\bigotimes_{i=0}^{d-1} \mathsf{H}\right)^{-1} = \left(\bigotimes_{i=0}^{d-1} \mathsf{H}\right) \cdot \mathsf{T}^{\mathsf{F}^{\times d}} \cdot \left(\bigotimes_{i=0}^{d-1} \mathsf{H}^{-1}\right)$$

$\bigotimes$: Kronecker/tensor product

Remark. The d-wise form was called d-th order form [HZC+25]. But "order" has been used in higher-order differential attacks, so we change its name since this work.

Properties of correlation matrix

Theorem ([DGV94, Bey21])

The correlation matrix has the following properties

(1) *For* $F = F_{r-1} \circ F_{r-2} \circ \cdots \circ F_0$

$$C^F = \prod_{i=0}^{r-1} C^{F_i}$$

(2) *For* $F = \underbrace{f \,||\, f \,||\, \cdots \,||\, f}_{t}$

$$C^F = \bigotimes_{i=0}^{t-1} C^f$$

A Geometric Approach Viewpoint on DL

DL correlation and correlation vector

Definition (Correlation vector of a multiset)

The correlation vector of a multiset $\mathbb{S}$ whose values are taken from $\mathbb{F}_2^n$ is a vector $\mathrm{CV}(\mathbb{S}) \in \mathbb{R}^{2^n}$ whose u-th coordinate is

$$\mathrm{CV}(\mathbb{S})[u] = \frac{1}{|\mathbb{S}|} \sum_{x \in \mathbb{S}} (-1)^{u^\top x}$$

Remark: There are similar things before defined for Boolean functions

New perspective on DL correlation of $\mathrm{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ from the geometric approach:

- Consider $\mathrm{F}^{\times 2} : (x, \Delta) \mapsto (\mathrm{F}(x), \mathrm{D}_\Delta \mathrm{F}(x))$
- Input multiset: $\mathbb{P} = \mathbb{F}_2^n \times \{\Delta\}$, output multiset: $\mathbb{C} := \mathrm{F}^{\times 2}(\mathbb{P})$
- $\mathrm{DL}[\Delta \xrightarrow{\mathrm{F}} \lambda]$ is the $(0, \lambda)$-coordinate of $\mathrm{CV}(\mathbb{C})$:

$$\mathrm{CV}(\mathbb{C})[(0,\lambda)] = 2^{-n} \sum_{\mathrm{F}(x), \mathrm{D}_\Delta \mathrm{F}(x)} (-1)^{(0,\lambda)^\top (\mathrm{F}(x), \mathrm{D}_\Delta \mathrm{F}(x))} = 2^{-n} \sum_{x \in \mathbb{F}_2^n, \Delta \in \{\Delta\}} (-1)^{\lambda^\top \mathrm{D}_\Delta \mathrm{F}(x)} = \mathrm{DL}[\Delta \xrightarrow{\mathrm{F}} \lambda]$$

DL correlation and correlation vector

Definition (Correlation vector of a multiset)

The correlation vector of a multiset $\mathbb{S}$ whose values are taken from $\mathbb{F}_2^n$ is a vector $\mathrm{CV}(\mathbb{S}) \in \mathbb{R}^{2^n}$ whose u-th coordinate is

$$\mathrm{CV}(\mathbb{S})[u] = \frac{1}{|\mathbb{S}|} \sum_{x \in \mathbb{S}} (-1)^{u^\top x}$$

Remark: There are similar things before defined for Boolean functions

New perspective on DL correlation of $\mathrm{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ from the geometric approach:

- Consider $\mathrm{F}^{\times 2} : (x, \Delta) \mapsto (\mathrm{F}(x), \mathrm{D}_\Delta \mathrm{F}(x))$
- Input multiset: $\mathbb{P} = \mathbb{F}_2^n \times \{\Delta\}$, output multiset: $\mathbb{C} := \mathrm{F}^{\times 2}(\mathbb{P})$
- $\mathrm{DL}[\Delta \xrightarrow{\mathrm{F}} \lambda]$ is the $(0, \lambda)$-coordinate of $\mathrm{CV}(\mathbb{C})$:

$$\mathrm{CV}(\mathbb{C})[(0,\lambda)] = 2^{-n} \sum_{\mathrm{F}(x), \mathrm{D}_\Delta \mathrm{F}(x)} (-1)^{(0,\lambda)^\top (\mathrm{F}(x), \mathrm{D}_\Delta \mathrm{F}(x))} = 2^{-n} \sum_{x \in \mathbb{F}_2^n, \Delta \in \{\Delta\}} (-1)^{\lambda^\top \mathrm{D}_\Delta \mathrm{F}(x)} = \mathrm{DL}[\Delta \xrightarrow{\mathrm{F}} \lambda]$$

- Question: how to approximate $\mathrm{CV}(\mathbb{C})[(0,\lambda)]$?

How to approximate $\mathrm{CV}(\mathbb{C})[(0, \lambda)]$?

Lemma (Correlation vector propagation, [DVG94, Bey21])

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, *and* $\mathbb{C} = F(\mathbb{P})$

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^F \cdot \mathrm{CV}(\mathbb{P})$$

Similarly for $\mathrm{F}^{\times 2}$*:* $\mathrm{CV}(\mathbb{C}') = \mathrm{C}^{F^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}')$.

How to approximate $\mathrm{CV}(\mathbb{C})[(0, \lambda)]$?

Lemma (Correlation vector propagation, [DVG94, Bey21])

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, *and* $\mathbb{C} = F(\mathbb{P})$

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^F \cdot \mathrm{CV}(\mathbb{P})$$

Similarly for $\mathrm{F}^{\times 2}$: $\mathrm{CV}(\mathbb{C}') = \mathrm{C}^{F^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}')$.

$\mathrm{F}^{\times 2}$ is composite

$$\mathrm{F}^{\times 2} = \mathrm{F}_{r-1}^{\times 2} \circ \mathrm{F}_{r-2}^{\times 2} \circ \cdots \circ \mathrm{F}_0^{\times 2}$$

How to approximate $\mathrm{CV}(\mathbb{C})[(0,\lambda)]$?

Lemma (Correlation vector propagation, [DVG94, Bey21])

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, *and* $\mathbb{C} = F(\mathbb{P})$

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^F \cdot \mathrm{CV}(\mathbb{P})$$

Similarly for $\mathrm{F}^{\times 2}$: $\mathrm{CV}(\mathbb{C}') = \mathrm{C}^{F^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}')$.

$\mathrm{F}^{\times 2}$ is composite

$$\mathrm{F}^{\times 2} = \mathrm{F}_{r-1}^{\times 2} \circ \mathrm{F}_{r-2}^{\times 2} \circ \cdots \circ \mathrm{F}_0^{\times 2}$$

According to the correlation matrix/geometric approach theories,

$$\mathrm{C}^{\mathrm{F}^{\times 2}} = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}$$

Therefore,

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}(\mathbb{P})$$

How to approximate $\mathrm{CV}(\mathbb{C})[(0,\lambda)]$?

Lemma (Correlation vector propagation, [DVG94, Bey21])

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, *and* $\mathbb{C} = F(\mathbb{P})$

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^F \cdot \mathrm{CV}(\mathbb{P})$$

Similarly for $\mathrm{F}^{\times 2}$: $\mathrm{CV}(\mathbb{C}') = \mathrm{C}^{F^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}')$.

$\mathrm{F}^{\times 2}$ is composite

$$\mathrm{F}^{\times 2} = \mathrm{F}_{r-1}^{\times 2} \circ \mathrm{F}_{r-2}^{\times 2} \circ \cdots \circ \mathrm{F}_0^{\times 2}$$

According to the correlation matrix/geometric approach theories,

$$\mathrm{C}^{\mathrm{F}^{\times 2}} = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}$$

Therefore,

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}(\mathbb{P})$$

For an SPN cipher $\mathrm{F}_i = \mathrm{L} \circ \mathrm{S}$. Let $\gamma_{i+1} = \mathrm{C}^{\mathrm{S}^{\times 2}} \sigma_i$, and $\sigma_i = \mathrm{C}^{\mathrm{L}^{\times 2}} \gamma_i$

$$\mathrm{CV}(\mathbb{P}) = \sigma_0$$

How to approximate $\mathrm{CV}(\mathbb{C})[(0,\lambda)]$?

Lemma (Correlation vector propagation, [DVG94, Bey21])

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, *and* $\mathbb{C} = F(\mathbb{P})$

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^F \cdot \mathrm{CV}(\mathbb{P})$$

Similarly for $\mathrm{F}^{\times 2}$: $\mathrm{CV}(\mathbb{C}') = \mathrm{C}^{F^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}')$.

$\mathrm{F}^{\times 2}$ is composite

$$\mathrm{F}^{\times 2} = \mathrm{F}_{r-1}^{\times 2} \circ \mathrm{F}_{r-2}^{\times 2} \circ \cdots \circ \mathrm{F}_0^{\times 2}$$

According to the correlation matrix/geometric approach theories,

$$\mathrm{C}^{\mathrm{F}^{\times 2}} = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}$$

Therefore,

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}(\mathbb{P})$$

For an SPN cipher $\mathrm{F}_i = \mathrm{L} \circ \mathrm{S}$. Let $\gamma_{i+1} = \mathrm{C}^{\mathrm{S}^{\times 2}} \sigma_i$, and $\sigma_i = \mathrm{C}^{\mathrm{L}^{\times 2}} \gamma_i$

$$\mathrm{CV}(\mathbb{P}) = \sigma_0 \underbrace{\xrightarrow{\mathrm{C}^{\mathrm{S}^{\times 2}}}}_{\approx} \gamma_1$$

How to approximate $\mathrm{CV}(\mathbb{C})[(0,\lambda)]$?

Lemma (Correlation vector propagation, [DVG94, Bey21])

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, *and* $\mathbb{C} = F(\mathbb{P})$

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^F \cdot \mathrm{CV}(\mathbb{P})$$

Similarly for $\mathrm{F}^{\times 2}$: $\mathrm{CV}(\mathbb{C}') = \mathrm{C}^{F^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}')$.

$\mathrm{F}^{\times 2}$ is composite

$$\mathrm{F}^{\times 2} = \mathrm{F}_{r-1}^{\times 2} \circ \mathrm{F}_{r-2}^{\times 2} \circ \cdots \circ \mathrm{F}_0^{\times 2}$$

According to the correlation matrix/geometric approach theories,

$$\mathrm{C}^{\mathrm{F}^{\times 2}} = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}$$

Therefore,

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}(\mathbb{P})$$

For an SPN cipher $\mathrm{F}_i = \mathrm{L} \circ \mathrm{S}$. Let $\gamma_{i+1} = \mathrm{C}^{\mathrm{S}^{\times 2}} \sigma_i$, and $\sigma_i = \mathrm{C}^{\mathrm{L}^{\times 2}} \gamma_i$

$$\mathrm{CV}(\mathbb{P}) = \sigma_0 \underbrace{\xrightarrow{\mathrm{C}^{\mathrm{S}^{\times 2}}}}_{\approx} \gamma_1 \underbrace{\xrightarrow{\mathrm{C}^{\mathrm{L}^{\times 2}}}}_{\approx} \sigma_1$$

How to approximate $\mathrm{CV}(\mathbb{C})[(0,\lambda)]$?

Lemma (Correlation vector propagation, [DVG94, Bey21])

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, *and* $\mathbb{C} = F(\mathbb{P})$

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^F \cdot \mathrm{CV}(\mathbb{P})$$

Similarly for $\mathrm{F}^{\times 2}$*:* $\mathrm{CV}(\mathbb{C}') = \mathrm{C}^{F^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}')$.

$\mathrm{F}^{\times 2}$ is composite

$$\mathrm{F}^{\times 2} = \mathrm{F}_{r-1}^{\times 2} \circ \mathrm{F}_{r-2}^{\times 2} \circ \cdots \circ \mathrm{F}_0^{\times 2}$$

According to the correlation matrix/geometric approach theories,

$$\mathrm{C}^{\mathrm{F}^{\times 2}} = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}$$

Therefore,

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}(\mathbb{P})$$

For an SPN cipher $\mathrm{F}_i = \mathrm{L} \circ \mathrm{S}$. Let $\gamma_{i+1} = \mathrm{C}^{\mathrm{S}^{\times 2}} \sigma_i$, and $\sigma_i = \mathrm{C}^{\mathrm{L}^{\times 2}} \gamma_i$

$$\mathrm{CV}(\mathbb{P}) = \sigma_0 \underbrace{\xrightarrow{\mathrm{C}^{\mathrm{S}^{\times 2}}}}_{\approx} \gamma_1 \underbrace{\xrightarrow{\mathrm{C}^{\mathrm{L}^{\times 2}}}}_{\approx} \sigma_1 \underbrace{\rightarrow}_{\approx} \cdots \underbrace{\rightarrow}_{\approx} \sigma_{r-1}$$

How to approximate $\mathrm{CV}(\mathbb{C})[(0,\lambda)]$?

Lemma (Correlation vector propagation, [DVG94, Bey21])

Consider $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, *and* $\mathbb{C} = F(\mathbb{P})$

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^F \cdot \mathrm{CV}(\mathbb{P})$$

Similarly for $\mathrm{F}^{\times 2}$: $\mathrm{CV}(\mathbb{C}') = \mathrm{C}^{F^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}')$.

$\mathrm{F}^{\times 2}$ is composite

$$\mathrm{F}^{\times 2} = \mathrm{F}_{r-1}^{\times 2} \circ \mathrm{F}_{r-2}^{\times 2} \circ \cdots \circ \mathrm{F}_0^{\times 2}$$

According to the correlation matrix/geometric approach theories,

$$\mathrm{C}^{\mathrm{F}^{\times 2}} = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}$$

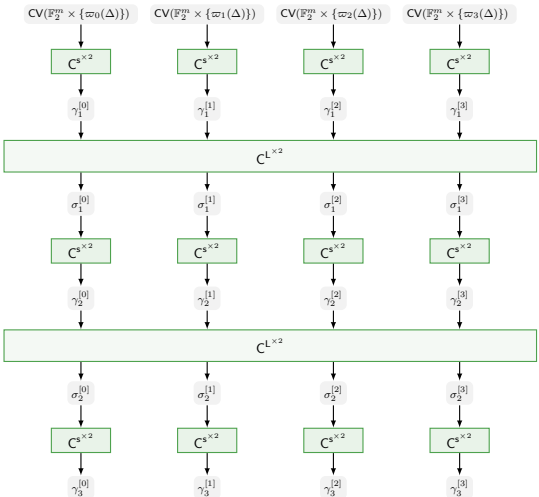
Therefore,

$$\mathrm{CV}(\mathbb{C}) = \mathrm{C}^{\mathrm{F}_{r-1}^{\times 2}} \cdot \mathrm{C}^{\mathrm{F}_{r-2}^{\times 2}} \cdots \mathrm{C}^{\mathrm{F}_0^{\times 2}}(\mathbb{P})$$

For an SPN cipher $\mathrm{F}_i = \mathrm{L} \circ \mathrm{S}$. Let $\gamma_{i+1} = \mathrm{C}^{\mathrm{S}^{\times 2}} \sigma_i$, and $\sigma_i = \mathrm{C}^{\mathrm{L}^{\times 2}} \gamma_i$

$$\mathrm{CV}(\mathbb{P}) = \sigma_0 \underbrace{\xrightarrow{\mathrm{C}^{\mathrm{S}^{\times 2}}}}_{\approx} \gamma_1 \underbrace{\xrightarrow{\mathrm{C}^{\mathrm{L}^{\times 2}}}}_{\approx} \sigma_1 \underbrace{\rightarrow}_{\approx} \cdots \underbrace{\rightarrow}_{\approx} \sigma_{r-1} \underbrace{\xrightarrow{\mathrm{C}^{\mathrm{S}^{\times 2}}}}_{\approx} \gamma_r = \mathrm{CV}(\mathbb{C})$$

Visualization for the round-based approximation



Global setting:

- S-box size: m
- block size: $n = mt$

Prepare for the plaintext vector σ_0

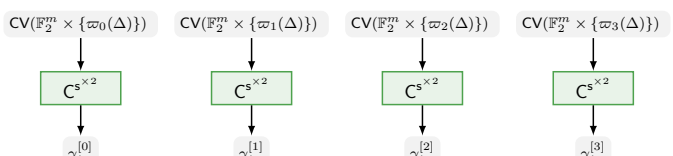
- The plaintext multiset: $\mathbb{P} = \mathbb{F}_2^n \times \{\Delta\} = \prod_{i=0}^{t-1}(\mathbb{F}_2^m \times \varpi_i(\Delta))$.

  Projection map: For $v = (v_0, v_1, \ldots, v_{t-1}) \in \mathbb{F}_2^{mt}$, $\quad \varpi_i : \mathbb{F}_2^{mt} \to \mathbb{F}_2^m$; $\quad v \mapsto v_i$.

- Compute the correlation vector

$$\mathsf{CV}(\mathbb{P}) = \bigotimes_{i=0}^{t-1} \mathsf{CV}(\mathbb{F}_2^m \times \varpi_i(\Delta))$$

- Complexity: $\mathcal{O}(t \times 2^m)$



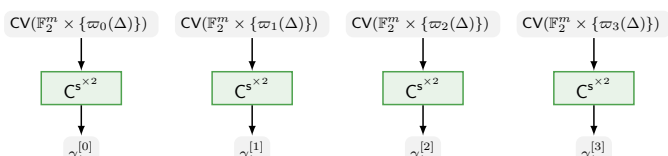
Approximation for the first nonlinear layer $\mathbf{S} = \underbrace{\mathbf{s}||\mathbf{s}||\cdots||\mathbf{s}||\mathbf{s}}_{t}$

- Compute the first nonlinear layer:

$$\gamma_1 = \mathrm{C}^{\mathrm{S}^{\times 2}} \cdot \mathrm{CV}(\mathbb{P}) = \mathrm{C}^{\mathrm{S}^{\times 2}} \sigma_0 := \mathrm{C}^{\mathrm{S}^{\times 2}} \cdot \bigotimes_{i=0}^{t-1} \sigma_0^{[i]} = \bigotimes_{i=0}^{t-1} \mathrm{C}^{\mathrm{s}^{\times 2}} \cdot \bigotimes_{i=0}^{t-1} \sigma_0^{[i]} = \bigotimes_{i=0}^{t-1} \mathrm{C}^{\mathrm{s}^{\times 2}} \cdot \sigma_0^{[i]}$$

  Raw complexity: $\mathcal{O}(t \times 2^{4m})$

- A fast algorithm can reduce the time complexity to $\mathcal{O}(t \times 2^{3m})$



Approximation for the first linear layer: L

- Cannot handle the linear layer efficiently:

$$\sigma_1 = \mathsf{C}^{\mathsf{L}^{\times 2}} \cdot \gamma_1 = \mathsf{C}^{\mathsf{L}^{\times 2}} \cdot \bigotimes_{i=0}^{t-1} \gamma_1^{[i]}$$

  Because $\mathsf{C}^{\mathsf{L}^{\times 2}}$ cannot be decomposed into small matrices aligned to S-boxes

Approximation for the first linear layer: L

- Cannot handle the linear layer efficiently:

$$\sigma_1 = \mathsf{C}^{\mathsf{L}^{\times 2}} \cdot \gamma_1 = \mathsf{C}^{\mathsf{L}^{\times 2}} \cdot \bigotimes_{i=0}^{t-1} \gamma_1^{[i]}$$

  Because $\mathsf{C}^{\mathsf{L}^{\times 2}}$ cannot be decomposed into small matrices aligned to S-boxes
- However, $\sigma_1[(v_0, v_1)] = \gamma_1[(\mathsf{L}^{\times 2})^\top (v_0, v_1)] = \gamma_1[(\mathsf{L}^\top v_0, \mathsf{L}^\top v_1)]$

$$= \prod_{j=0}^{t-1} \gamma_1^{[j]}[(\varpi_j(\mathsf{L}^\top v_0), \varpi_j(\mathsf{L}^\top v_1))]$$

Approximation for the first linear layer: L

- Cannot handle the linear layer efficiently:

$$\sigma_1 = \mathsf{C}^{\mathsf{L}^{\times 2}} \cdot \gamma_1 = \mathsf{C}^{\mathsf{L}^{\times 2}} \cdot \bigotimes_{i=0}^{t-1} \gamma_1^{[i]}$$

  Because $\mathsf{C}^{\mathsf{L}^{\times 2}}$ cannot be decomposed into small matrices aligned to S-boxes

- However, $\sigma_1[(v_0, v_1)] = \gamma_1[(\mathsf{L}^{\times 2})^\top (v_0, v_1)] = \gamma_1[(\mathsf{L}^\top v_0, \mathsf{L}^\top v_1)]$

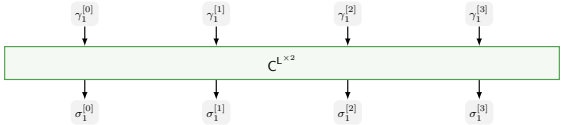
$$= \prod_{j=0}^{t-1} \gamma_1^{[j]}[(\varpi_j(\mathsf{L}^\top v_0), \varpi_j(\mathsf{L}^\top v_1))]$$

- Compute coordinates corresponding with S-boxes

$$\mathbb{I} = \left\{ \sigma_1[\tau_i(w)] : w \in \mathbb{F}_2^{2m}, 0 \le i < t \right\}$$

  Inclusion map: $\tau_i : \mathbb{F}_2^m \to \mathbb{F}_2^{mt}; \quad v \mapsto (0, \ldots, v, \ldots, 0)$

- Complexity: $\mathcal{O}(t \times 2^{2m})$



What about the remaining coordinates of σ_1?

Assumption (Piling-up assumption)

For any $v \in \mathbb{F}_2^{2m \times t}$,

$$\varphi[v] \approx \prod_{i=0}^{t-1} \varphi[\tau_i(\varpi_i(v))]$$

Given any coordinate $v = (v_0, v_1, \ldots, v_{t-1})$

$$\sigma_1[(v_0, v_1, \ldots, v_{t-1})] \approx \prod_{i=0}^{t-1} \sigma_1^{[i]}[v_i]$$

Do not need to store the whole σ_1!

What about the remaining coordinates of σ_1?

Assumption (Piling-up assumption)

For any $v \in \mathbb{F}_2^{2m \times t}$,

$$\varphi[v] \approx \prod_{i=0}^{t-1} \varphi[\tau_i(\varpi_i(v))]$$

Given any coordinate $v = (v_0, v_1, \ldots, v_{t-1})$

$$\sigma_1[(v_0, v_1, \ldots, v_{t-1})] \approx \prod_{i=0}^{t-1} \sigma_1^{[i]}[v_i]$$

Do not need to store the whole σ_1!

Remark. This assumption holds if we assume that the S-boxes in a round are all independent.

Influence of key-XORs: fixed-key setting

- k is a constant, and the 2-wise form of the key-XOR K is

$$\mathsf{K}_k^{\times 2} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x, \theta) \to (x + k, \theta)$$

- The correlation matrix of $\mathsf{K}_k^{\times 2}$ has the element

$$\begin{aligned} \mathsf{C}^{\mathsf{K}_k^{\times 2}}[(v_0, v_1)(u_0, u_1)] &= 2^{-2n} \sum_{x \in \mathbb{F}_2^n, \theta \in \mathbb{F}_2^n} (-1)^{u_0^\top x + u_1^\top \theta + v_0^\top (x+k) + v_1^\top \theta} \\ &= (-1)^{v_0^\top k} \left(2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{(u_0^\top + v_0^\top)x} \right) \left(2^{-n} \sum_{\theta \in \mathbb{F}_2^n} (-1)^{(u_1^\top + v_1^\top)\theta} \right) \\ &= (-1)^{v_0^\top k} \delta(u_0 + v_0)\delta(u_1 + v_1). \end{aligned}$$

- Let $\varphi = \mathsf{C}^{\mathsf{K}_k^{\times 2}} \sigma$, then

$$\varphi[(v_0, v_1)] = \sum_{u_0 \in \mathbb{F}_2^n, u_1 \in \mathbb{F}_2^n} (-1)^{v_0^\top k} \delta(v_0 + u_0)\delta(v_1 + u_1)\sigma[(u_0, u_1)] = (-1)^{v_0^\top k} \sigma[(v_0, v_1)].$$

Conclusion: the key values only influence the sign

Influence of key-XORs: average-key setting

- k is a uniform and independent input

$$\mathsf{K}^{\times 2} : \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n; (x, \theta, k) \to (x + k, \theta).$$

- The correlation matrix of K has the elements as

$$\begin{aligned} \mathsf{C}^{\mathsf{K}^{\times 2}}[(v_0, v_1), (u_0, u_1, u_k)] &= 2^{-3n} \sum_{x \in \mathbb{F}_2^n, \theta \in \mathbb{F}_2^n, k \in \mathbb{F}_2^n} (-1)^{u_0^\top x + u_1^\top \theta + u_k^\top k + v_0^\top (x+k) + v_1^\top \theta} \\ &= \delta(v_0 + u_k)\delta(v_0 + u_0)\delta(v_1 + u_1). \end{aligned}$$

- Let $\varphi = \mathsf{C}^{\mathsf{K}^{\times 2}}\sigma$. σ' and σ'' are the correlation vectors of the data path and key, respectively

$$\varphi[(v_0, v_1)] = \sigma'[(v_0, v_1)] \cdot \sigma''[v_0].$$

  Under the assumption that k is uniform,

$$\sigma''[v_0] = 2^{-n} \sum_{k \in \mathbb{F}_2^n} (-1)^{v_0^\top k} = \begin{cases} 1, & v_0 = 0, \\ 0, & v_0 \neq 0. \end{cases}$$

  Consequently,

$$\varphi[(v_0, v_1)] = \begin{cases} 0, & v_0 \neq 0, \\ \sigma'[(v_0, v_1)], & v_0 = 0. \end{cases}$$

Conclusion: the key has no influence

DL Application Results to S-box Ciphers

Application to Ascon

Target	Rounds	Exp. Cor.	Th. Cor.	Method	Ref.
Ascon-128 init.	4	2^{-1}	2^{-5}	DLCT	[BDK+19]
			$2^{-1.36}$	ATF	[LLL, C21]
			$2^{-1.09}$	HATF	[HPT+23]
			2^{-1}	TDT	[PZW+24]
			$\mathbf{2^{-1}}$	**Round-based**	[Ours]
Ascon-128	5	$2^{-8.94}$	$2^{-9.1}$	TDT	[PZW+24]
			$\mathbf{2^{-8.94}}$	**Round-based**	[Ours]
		$2^{-7.94}$	$\mathbf{2^{-7.94}}$	**Round-based**	[Ours]
Ascon-128a init.	6 ★	–	$\mathbf{2^{-23.89}}$	**Round-based**	[Ours]
Ascon-p	5	$2^{-4.33}$	$2^{-4.0}$	GDLCT	[HDE24]
			$\mathbf{2^{-4.21}}$	**Round-based**	[Ours]
		$2^{-7.61}$	$2^{-6.83}$	GDLCT	[HDE24]
			$\mathbf{2^{-7.58}}$	**Round-based**	[Ours]
	6 ★		$\mathbf{2^{-21.89}}$	**Round-based**	[Ours]

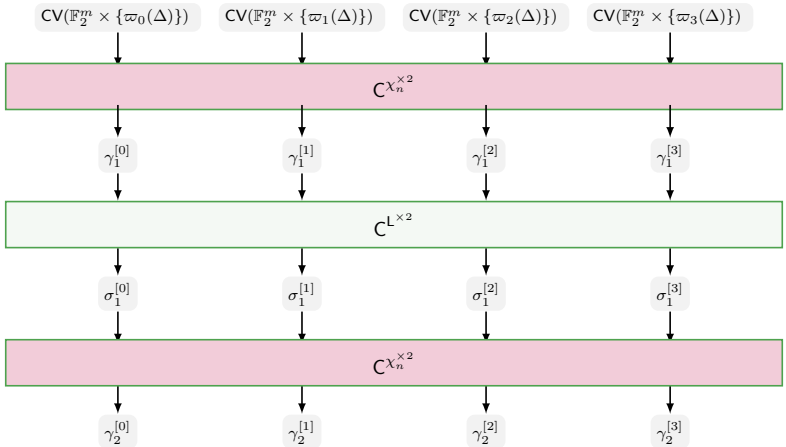
★ means we find DL distinguishers for more rounds

Application to Present

Target	Rounds	Exp. Cor.	Th. Cor.	Method	Ref.
Present	10	$2^{-12.94}$	$2^{-13.97}$	GDLCT	[HDE24]
			$2^{-13.03}$	**Round-based**	[Ours]
	13		$2^{-27.01}$	GDLCT	[HDE24]
			$\mathbf{2^{-22.43}}$	**Round-based**	[Ours]
	17 ★		$\mathbf{2^{-28.85}}$	**Round-based**	[Ours]
	18 ★		$\mathbf{2^{-31.46}}$	**Round-based**	[Ours]

Round-Based Approximation for χ-Based Ciphers

Visualization for the round-based approximation for Chi ciphers



Chi, Chi$^{\times 2}$ and their correlations

- Chi function [Dae95]

$$\chi_n : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x[0], x[1], \ldots, x[n-1]) \mapsto (y[0], y[1], \ldots, y[n-1]), \quad y[i] = x[i] + (x[i+1]+1)x[i+2]$$

- Auxiliary function g_n

$$g_n : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x[0], x[1], \ldots, x_[n-1]) \mapsto (y[0], y[1], \ldots, y[n-1]), \quad y[i] = (x[i]+1)x[i+1]$$

Chi, Chi$^{\times 2}$ and their correlations

- Chi function [Dae95]

$$\chi_n : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x[0], x[1], \ldots, x[n-1]) \mapsto (y[0], y[1], \ldots, y[n-1]), \quad y[i] = x[i] + (x[i+1]+1)x[i+2]$$

- Auxiliary function g_n

$$g_n : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x[0], x[1], \ldots, x_[n-1]) \mapsto (y[0], y[1], \ldots, y[n-1]), \quad y[i] = (x[i]+1)x[i+1]$$

- $\chi_n(x) = x + (g_n(x) \lll 1)$

$$C^{\chi_n}[v, u] := \mathrm{Cor}[u^\top x + v^\top \chi_n(x)]$$

Chi, Chi$^{\times 2}$ and their correlations

- Chi function [Dae95]

$$\chi_n : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x[0], x[1], \ldots, x[n-1]) \mapsto (y[0], y[1], \ldots, y[n-1]), \quad y[i] = x[i] + (x[i+1]+1)x[i+2]$$

- Auxiliary function g_n

$$g_n : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x[0], x[1], \ldots, x_[n-1]) \mapsto (y[0], y[1], \ldots, y[n-1]), \quad y[i] = (x[i]+1)x[i+1]$$

- $\chi_n(x) = x + (g_n(x) \lll 1)$

$$\mathrm{C}^{\chi_n}[v, u] := \mathrm{Cor}[u^\top x + v^\top \chi_n(x)] = \mathrm{Cor}[(u^\top + v^\top)x + (v \ggg 1)^\top g_n(x)] = \mathrm{C}^{g_n}[v \ggg 1, v + u]$$

Chi, Chi$^{\times 2}$ and their correlations

- Chi function [Dae95]

$$\chi_n : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x[0], x[1], \ldots, x[n-1]) \mapsto (y[0], y[1], \ldots, y[n-1]), \quad y[i] = x[i] + (x[i+1]+1)x[i+2]$$

- Auxiliary function g_n

$$g_n : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (x[0], x[1], \ldots, x_[n-1]) \mapsto (y[0], y[1], \ldots, y[n-1]), \quad y[i] = (x[i]+1)x[i+1]$$

- $\chi_n(x) = x + (g_n(x) \lll 1)$

$$\mathrm{C}^{\chi_n}[v, u] := \mathrm{Cor}[u^\top x + v^\top \chi_n(x)] = \mathrm{Cor}[(u^\top + v^\top)x + (v \ggg 1)^\top g_n(x)] = \mathrm{C}^{g_n}[v \ggg 1, v + u]$$

- The coordinate of $\mathrm{C}^{\chi_n^{\times 2}}$ can be computed by

$$\begin{aligned} \mathrm{C}^{\chi_n^{\times 2}}[(v_0, v_1), (u_0, u_1)] &= \mathrm{C}^{\chi_n}[v_0, u_0] \cdot \mathrm{C}^{\chi_n}[v_0 + v_1, u_0 + u_1] \quad ([HZC + 25]) \\ &= \mathrm{C}^{g_n}[v_0 \ggg 1, v_0 + u_0] \cdot \mathrm{C}^{g_n}[(v_0 + v_1) \ggg 1, v_0 + v_1 + u_0 + u_1] \end{aligned}$$

- To compute $\gamma = \mathrm{C}^{\chi_n^{\times 2}}\sigma$, we need $\mathrm{C}^{g_n}[v, u]$

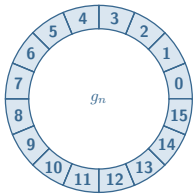
Break the circle of g_n

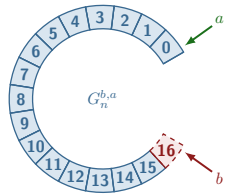
Definition ($G_n^{a,b}$)

We define

$$G_n^{b,a} : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad y = G_n(x)$$

where $y[i] = (x[i] + 1)x[i + 1], 0 \leq i < n$ and $x[0] = a, x[n] = b$.





Proposition (Correlation of $C^{G_n^{b,a}}$)

$$C^{g_n}[v, u] = C^{G_n^{0,0}}[v, u] + C^{G_n^{1,1}}[v, u].$$

Chaining property of $C^{G_n^{a,b}}$ coordinates

Proposition

Let $n > 1$, $v'' = v||v', u'' = u||u' \in \mathbb{F}_2^{n+1}$ where $u', v' \in \mathbb{F}_2$. From $C^{G_n^{b,a}}[v, u]$ we can get $C^{G_n^{b,a}}[v'', u'']$ from the following formula,

$$C^{G_{n+1}^{b,a}}[v'', u''] = \frac{1}{2} \sum_{c \in \mathbb{F}_2} (-1)^{u'c + v'(c+1)b} C^{G_n^{c,a}}[v, u]$$

Lemma

For the four possible values of $v', u', a, b \in \mathbb{F}_2$, we define a matrix $M_{v',u'}$ whose (b, a)-coordinate is $M_{v',u'}[b, a] = \frac{1}{2}(-1)^{ua+v(a+1)b}$. According to the four possibilities of (v', u'), we obtain four matrices:

$$M_{0,0} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, M_{0,1} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}, M_{1,0} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, M_{1,1} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$$

$C^{G_n^{b,a}}[v, u]$ can be computed as

$$C^{G_n^{b,a}}[v, u] = e_b^\top \left(\prod_{i=0}^{n-1} M_{v[i],u[i]} \right) e_a$$

where $e_0 = [1, 0]^\top$ and $e_1 = [0, 1]^\top$

Obtain $C^{\chi_n^{\times 2}}$

Theorem

Denote $e_0 = [1, 0]^\top$ *and* $e_1 = [0, 1]^\top$. *The coordinate of* $C^{\chi^{\times 2}}$ *can be computed as*

$$C^{\chi_n^{\times 2}}[(v_0, v_1), (u_0, u_1)] = \sum_{i=0}^{1} \sum_{i'=0}^{1} (e_i \otimes e_{i'})^\top \prod_{j=0}^{n-1} \left(M^{\otimes}_{v_0, v_1, u_0, u_1, j} \right) (e_i \otimes e_{i'}),$$

where $M^{\otimes}_{v_0, v_1, u_0, u_1, j} = M_{((v_0+v_1) \ggg 1)[j], (u_0+u_1+v_0+v_1)[j]} \otimes M_{(v_1 \ggg 1)[j], (u_1+v_1)[j]}$.

Approximate $\gamma[(v_0, v_1)]$

- Let $\gamma = C^{\chi_n^{\times 2}}\sigma$. Assume $\mathbb{J} = \left\{\sigma[\tau_i(w)] : w \in \mathbb{F}_2^2, i = 0, \ldots, n-1\right\}$ is known, we want to compute

$$\mathbb{I} = \left\{\gamma[\tau_i(w)] : w \in \mathbb{F}_2^2, i = 0, \ldots, n-1\right\} \text{ (a bit-level approximation)}$$

Approximate $\gamma[(v_0, v_1)]$

- Let $\gamma = \mathsf{C}^{\chi_n^{\times 2}}\sigma$. Assume $\mathbb{J} = \left\{\sigma[\tau_i(w)] : w \in \mathbb{F}_2^2, i = 0, \ldots, n-1\right\}$ is known, we want to compute

$$\mathbb{I} = \left\{\gamma[\tau_i(w)] : w \in \mathbb{F}_2^2, i = 0, \ldots, n-1\right\} \text{ (a bit-level approximation)}$$

- Assume $\sigma[(u_0, u_1)] = \prod_{i=0}^{t-1} \sigma^{[i]}[(\varpi_i(u_0), \varpi(u_1))]$

$$\begin{aligned}
\gamma[(v_0, v_1)] &= \sum_{(u_0,u_1)\in\mathbb{F}_2^{2n}} \mathsf{C}^{\chi_2^{\times 2}}[(v_0, v_1), (u_0, u_1)] \cdot \sigma[(u_0, u_1)] \\
&= \sum_{(u_0,u_1)\in\mathbb{F}_2^{2n}} \sum_{i=0}^{1}\sum_{i'=0}^{1} (e_i \otimes e_{i'})^\top \prod_{j=0}^{n-1} M^{\otimes}_{v_0,v_1,u_0,u_1,j} \cdot (e_i \otimes e_{i'}) \cdot \sigma[(u_0, u_1)] \\
&= \sum_{i=0}^{1}\sum_{i'=0}^{1} (e_i \otimes e_{i'})^\top \sum_{(u_0,u_1)\in\mathbb{F}_2^{2n}} \prod_{j=0}^{n-1} M^{\otimes}_{v_0,v_1,u_0,u_1,j} \prod_{j=0}^{n-1} \sigma^{[j]}[(\varpi_j(u_0), \varpi(u_1))] \cdot (e_i \otimes e_{i'}) \\
&= \sum_{i=0}^{1}\sum_{i'=0}^{1} (e_i \otimes e_{i'})^\top \sum_{(u_0,u_1)\in\mathbb{F}_2^{2n}} \prod_{j=0}^{n-1} (\sigma^{[j]}[(\varpi_j(u_0), \varpi_j(u_1))] M^{\otimes}_{v_0,v_1,u_0,u_1,j}) \cdot (e_i \otimes e_{i'}) \\
&= \sum_{i=0}^{1}\sum_{i'=0}^{1} (e_i \otimes e_{i'})^\top \prod_{j=0}^{n-1} \sum_{u_0[j],u_1[j]\in\mathbb{F}_2} (\sigma^{[j]}[\varpi_j((u_0, u_1))] M^{\otimes}_{v_0,v_1,u_0,u_1,j}) \cdot (e_i \otimes e_{i'}).
\end{aligned}$$

DL Application Results to Chi Ciphers

Application to Subterranean-2.0 and Koala-p

Target	Rounds	Exp. Cor.	Th. Cor.	Method	Ref.
Subterranean-2.0	5 ★	$-2^{-7.88}$	$\mathbf{-2^{-7.98}}$	**Round-based**	[Ours]
	6 ★		$\mathbf{2^{-20.09}}$	**Round-based**	[Ours]
Koala-p	5 ★	$2^{-6.73}$	$\mathbf{2^{-6.87}}$	**Round-based**	[Ours]
	6 ★		$\mathbf{2^{-21.42}}$	**Round-based**	[Ours]

Higher-Order Differential-Linear Attacks

Round-based approximation for 2^d-wise form

- d-th Higher-order differential linear (HDL) attacks

$$\mathrm{HDL}[\boldsymbol{\Delta} \xrightarrow{\mathsf{F}} \lambda] = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda \cdot \sum_{\boldsymbol{w} \in \mathbb{F}_2^d \setminus \{0\}} \mathrm{D}_{\langle \boldsymbol{w}, \boldsymbol{\Delta} \rangle} \mathsf{F}(x)}$$

  $\boldsymbol{\Delta} = (\Delta_0, \Delta_1, \ldots, \Delta_{d-1})$ is d linearly-independent vectors
- Higher-order algebraic transition form [HPT+23] is the only method to approximate a non-deterministic HDL correlation
- Let $\boldsymbol{v} = (0, \underbrace{\lambda, \ldots, \lambda}_{2^d - 1 \text{ times}}) \in \mathbb{F}_2^{n \times 2^d}$

$$\begin{aligned}
\mathrm{CV}(\mathbb{C})[\boldsymbol{v}] &= \sum_{\boldsymbol{u}} \mathsf{C}^{\mathsf{F}^{2^d}}[\boldsymbol{v}, \boldsymbol{u}] \cdot \mathrm{CV}(\mathbb{P})[\boldsymbol{u}] = 2^{-n} \sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda \sum_{\boldsymbol{u} \in \mathbb{F}_2^d \setminus \{0\}} \mathrm{D}_{\langle \boldsymbol{u}, \boldsymbol{\Delta} \rangle} \mathsf{F}(x)} \\
&= \mathrm{CV}(\mathbb{C})[0, \underbrace{\lambda, \ldots, \lambda}_{2^d - 1 \text{ times}}] \\
&= \mathrm{HDL}[\boldsymbol{\Delta} \xrightarrow{\mathsf{F}} \lambda]
\end{aligned}$$

- Round-based approximation

$$\mathrm{CV}(\mathbb{P}) = \sigma_0 \xrightarrow{\mathsf{C}^{\mathsf{S} \times 2^d}} \gamma_1 \xrightarrow{\mathsf{C}^{\mathsf{L} \times 2^d}} \sigma_1 \to \cdots \to \sigma_{r-1} \xrightarrow{\mathsf{C}^{\mathsf{S} \times 2^d}} \gamma_r = \mathrm{CV}(\mathbb{C}).$$

Correlation propagation for $\chi_n^{\times 2^d}$

$$\gamma[\boldsymbol{v}] = \sum_{\boldsymbol{u}} \mathrm{C}^{\chi_n^{\times 2^d}}[\boldsymbol{v}, \boldsymbol{u}] \cdot \sigma[\boldsymbol{u}]$$

$$= \sum_{i^{(0)}=0}^{1} \cdots \sum_{i^{(2^d-1)}=0}^{1} \left(\bigotimes_{j=0}^{2^d-1} e_{i^{(j)}}^{\top} \right) \left(\sum_{u_0,\ldots,u_{2^d-1} \in \mathbb{F}_2^n} \prod_{j=0}^{n-1} \sigma[\tau_j(\varpi_j(\boldsymbol{u}))] \bigotimes_{k=0}^{2^d-1} M_{\lambda_0^{(k)}[j], \lambda_1^{(k)}[j]} \right) \left(\bigotimes_{j=0}^{2^d-1} e_{i^{(j)}} \right)$$

$$= \sum_{i^{(0)}=0}^{1} \cdots \sum_{i^{(2^d-1)}=0}^{1} \left(\bigotimes_{j=0}^{2^d-1} e_{i^{(j)}}^{\top} \right) \left(\prod_{j=0}^{n-1} \sum_{u_0[j],\ldots,u_{2^d-1}[j] \in \mathbb{F}_2} \sigma[\tau_j(\varpi_j(\boldsymbol{u}))] \bigotimes_{k=0}^{2^d-1} M_{\lambda_0^{(k)}[j], \lambda_1^{(k)}[j]} \right) \left(\bigotimes_{j=0}^{2^d-1} e_{i^{(j)}} \right)$$

HDL Application Results

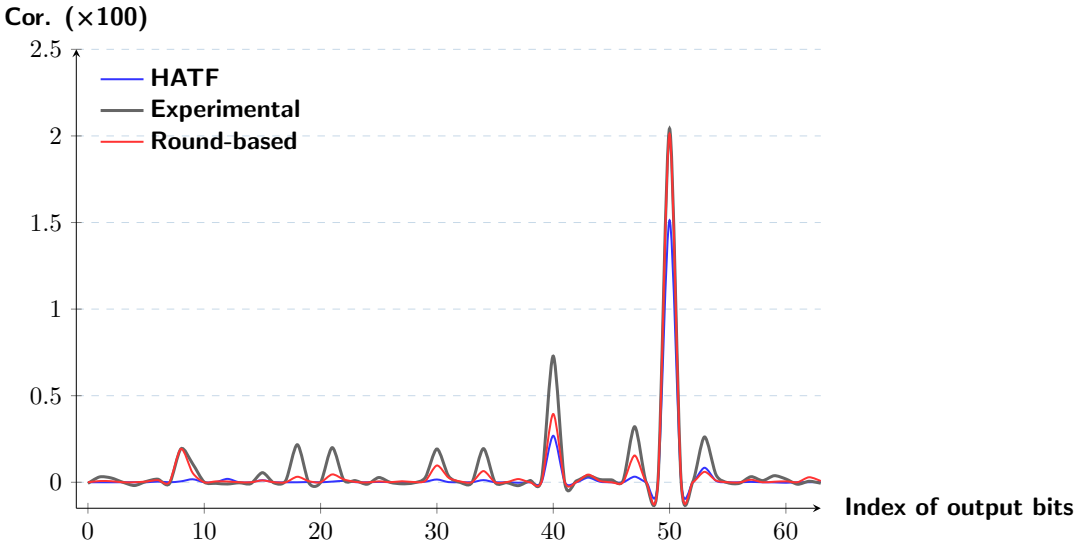
Applications to second-order DL distinguishers

Target	Rounds	Exp. Cor.	Th. Cor.	Method	Ref.
Second-order differential-linear distinguisher					
Ascon-128 init.	5	$2^{-5.60}$	$2^{-6.05}$	HATF	[HPT+23]
			$2^{-5.63}$	**Round-based**	[Ours]
	6 ★		**$2^{-45.35}$**	**Round-based**	[Ours]
Subterranean-2.0	5 ★	$2^{-6.05}$	**$2^{-6.05}$**	**Round-based**	[Ours]
	7 ★		**$2^{-90.99}$**	**Round-based**	[Ours]
	8 ★ (full)		**$2^{-63.84}$**	**Round-based**	[Ours]
Koala-p	5 ★	$2^{-5.89}$	**$2^{-6.09}$**	**Round-based**	[Ours]
	7 ★		**$2^{-86.24}$**	**Round-based**	[Ours]
	8 ★ (full)		**$2^{-63.75}$**	**Round-based**	[Ours]

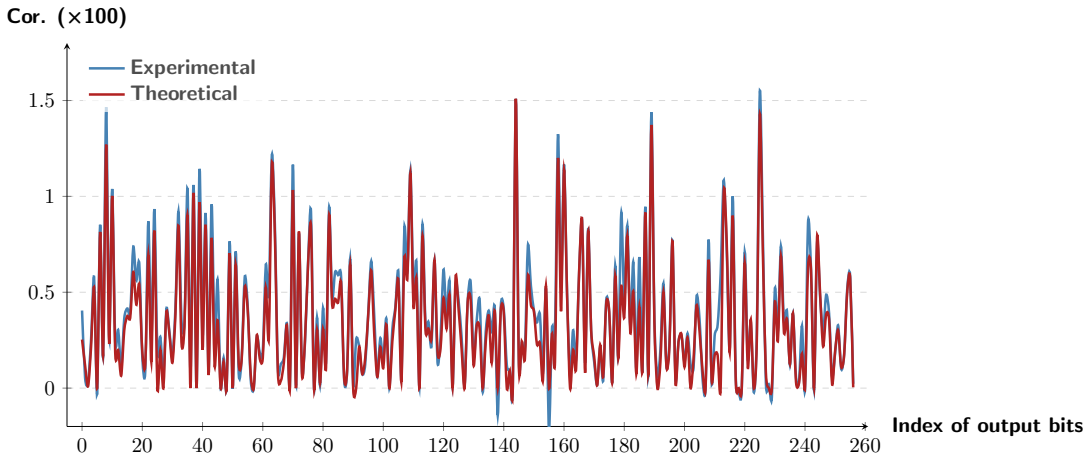
A possible explanation for counter-intuitive 7-round and 8-round correlations

$$\gamma_r[(0, \underbrace{\lambda, \ldots, \lambda}_{2^d-1})] \text{ is NOT ONLY from } \gamma_{r-1}[(0, \underbrace{\lambda, \ldots, \lambda}_{2^d-1})] \text{ when } d > 1$$

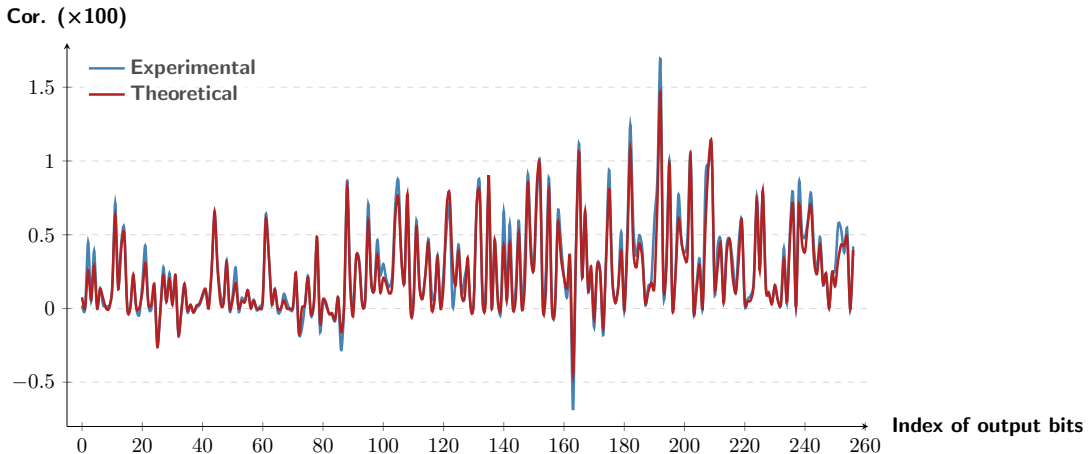
Precision of Second-Order HDL Correlation for 5-Round Ascon



Precision of Second-Order HDL Correlation for 5-Round Subterranean-2.0



Precision of Second-Order HDL Correlation for 5-Round Koala-p



Classification of DL Approximation Methods

Classification

- Quasidifferential basis for input, 2-wise linear basis for output

$$\text{Task: to approximate } \mathrm{Q}^{\mathrm{F}}[(0,\lambda),(0,\Delta)]$$

- According to change-of-basis timing:
  - At the beginning: the current method [Ours], ATF [LLL21]
  - In the middle: classical 2-phase [LH94], 3-phase method, DLCT [BDK+19], generalized DLCT [HDE+24]
  - At the last: truncated differential table [PZW+24]
- According to the approximation method
  - Round-based: ATF [LLL21], the current method [Ours], TDT [PZW+24]

$$\mathrm{Q}^{\mathrm{F}}[(0,\lambda),(0,\Delta)] = \lambda^{\top} \cdot \mathrm{M}_{r-1} \cdot \mathrm{M}_{r-2} \cdots \mathrm{M}_0 \cdot \sigma_0$$

  - Trail-based: classical 2-phase [LH94], 3-phase method, DLCT [BDK+19], generalized DLCT [HDE+24]

$$\mathrm{Q}^{\mathrm{F}}[(0,\lambda),(0,\Delta)] = \sum_{(0,\Delta)=v_0,v_1,v_2,\ldots,v_{r-1},v_r=(0,\lambda)} \prod_{j=0}^{r-1} \omega_{v_{i+1},v_i}$$

Classification

- Quasidifferential basis for input, 2-wise linear basis for output

$$\text{Task: to approximate } \mathrm{Q}^{\mathrm{F}}[(0,\lambda),(0,\Delta)]$$

- According to change-of-basis timing:
  - At the beginning: the current method [Ours], ATF [LLL21]
  - In the middle: classical 2-phase [LH94], 3-phase method, DLCT [BDK+19], generalized DLCT [HDE+24]
  - At the last: truncated differential table [PZW+24]
- According to the approximation method
  - Round-based: ATF [LLL21], the current method [Ours], TDT [PZW+24]

$$\mathrm{Q}^{\mathrm{F}}[(0,\lambda),(0,\Delta)] = \lambda^{\top} \cdot \mathrm{M}_{r-1} \cdot \mathrm{M}_{r-2} \cdots \mathrm{M}_0 \cdot \sigma_0$$

  - Trail-based: classical 2-phase [LH94], 3-phase method, DLCT [BDK+19], generalized DLCT [HDE+24]

$$\mathrm{Q}^{\mathrm{F}}[(0,\lambda),(0,\Delta)] = \sum_{(0,\Delta)=v_0,v_1,v_2,\ldots,v_{r-1},v_r=(0,\lambda)} \prod_{j=0}^{r-1} \omega_{v_{i+1},v_i}$$

Thank you for your attention!

Reference

- [LH94] Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis
- [DIK08] Dunkelman O., Indesteege S., Keller N.: A Differential-Linear Attack on 12-Round Serpent
- [BLN14] Blondeau, C., Leander, G., Nyberg, K.: Differential-linear cryptanalysis revisited
- [BDK+19] Bar-On, A., Dunkelman, O., Keller, N., Weizman, A.: DLCT: A new tool for differential-linear cryptanalysis
- [LLL21] Liu, M., Lu, X., Lin, D.: Differential-linear cryptanalysis from an algebraic perspective
- [HDE24] Hadipour, H., Derbez, P., Eichlseder, M.: Revisiting differential-linear attacks via a boomerang perspective with application to AES, ASCON, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBLOCK, SIMECK, and SERPENT
- [PZW+24] Peng, T., Zhang, W., Weng, J., Ding, T.: New approaches for estimating the bias of differential-linear distinguishers
- [Bey21] Beyne, T.: A geometric approach to linear cryptanalysis
- [DGV94] Daemen, J., Govaerts, R., Vandewalle, J.: Correlation matrices
- [HZC+25] Hu, K., Zhang, C., Chang, C., Zhang, J., Wang, M., Peyrin, T.: Unlocking mix-basis potential: Geometric approach for combined attacks
- [Dae95] J. Daemen. Cipher and hash function design, strategies based on linear and differential cryptanalysis
- [HPT+23] Hu, K., Peyrin, T., Tan, Q.Q., Yap, T.: Revisiting higher-order differential-linear attacks from an algebraic perspective