# Revisiting Higher-Order Differential(-Linear) Attacks from an Algebraic Perspective

## Applications to Ascon

Kai Hu and Thomas Peyrin

SPMS, Nanyang Technological University, Singapore

Virtual NIST Lightweight Cryptography Workshop
May 10, 2022

# Outline

# Outline

# Results in This Work for ASCON

● Permutation (black-box model) ◆ Permutation (non-black-box model)
■ Initialization ▲ Encryption (Nonce-Misuse Scenario)

| **Type** | **Round** | **Data** (log) | **Time** (log) | **Method** | Reference |
|---|---|---|---|---|---|
| Distinguisher | 4 | 3 | 3 | HD ● | Ours |
| | | 2 | 2 | HDL ▲ ■ | Ours |
| | 5 | 13 | 13 | HDL ■ | Ours |
| | | 6 | 6 | HD ● | Ours |
| | 6 | 12 | 12 | HD ● | Ours |
| | | 7 | 7 | Zero-Sum ◆ | Ours |
| | 7 | 23 | 23 | HD ● | Ours |
| | 8 | 46 | 46 | HD ● | Ours |
| | | 13 | 13 | Zero-Sum ◆ | Ours |
| | 11 | 48 | 48 | Zero-Sum ◆ | Ours |
| | 12 | 55 | 55 | Zero-Sum ◆ | Ours |
| Key-Recovery | 5 | 23 | 23 | Cond. HDL | Ours |
| | 6 | 74 | 74 | Cond. HDL | Ours |

# Outline

# Higher-Order Differential-Linear Analysis

- Higher-Order differential (HD) was Proposed by Lai in 1994
  - Given $l$ linearly independent values $\mathbf{\Delta}_I = (\Delta_0, \Delta_1, \ldots, \Delta_{l-1})$, the $l$-th order HD of $E$ is

$$p = \Pr\left[\bigoplus_{x \in X \oplus \mathcal{L}(\mathbf{\Delta}_I)} E(x) = \Delta_O\right]$$

- Higher-Order Differential-Linear (HDL) cryptanalysis was proposed by Biham, Dunkelman and Keller in 2005
  - A generalization of differential-linear attack
  - The bias of an HDL approximation is $\varepsilon$ as follows,

$$\Pr\left[\lambda_O \cdot \left(\bigoplus_{x \in X \oplus \mathcal{L}(\mathbf{\Delta}_I)} E(x)\right) = 0\right] = \frac{1}{2} + \varepsilon.$$

# Higher-Order Differential-Linear Analysis

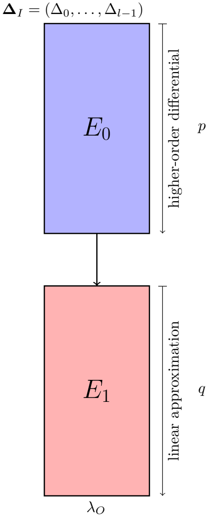
- Higher-Order differential (HD) was Proposed by Lai in 1994
  - Given $l$ linearly independent values $\boldsymbol{\Delta}_I = (\Delta_0, \Delta_1, \ldots, \Delta_{l-1})$, the $l$-th order HD of $E$ is

$$p = \Pr\left[\bigoplus_{x \in X \oplus \mathcal{L}(\boldsymbol{\Delta}_I)} E(x) = \Delta_O\right]$$

- Higher-Order Differential-Linear (HDL) cryptanalysis was proposed by Biham, Dunkelman and Keller in 2005
  - A generalization of differential-linear attack
  - The bias of an HDL approximation is $\varepsilon$ as follows,

$$\Pr\left[\lambda_O \cdot \left(\bigoplus_{x \in X \oplus \mathcal{L}(\boldsymbol{\Delta}_I)} E(x)\right) = 0\right] = \frac{1}{2} + \varepsilon.$$

# Two Sub-Ciphers Strategy for HDL



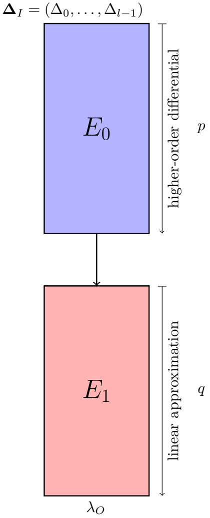

$$\mathrm{PR}\left[\lambda_O \cdot \left(\bigoplus_{x \in X \oplus \mathcal{L}(\boldsymbol{\Delta}_I)} E(x)\right) = 0\right] = \frac{1}{2} + \varepsilon.$$

- Process:
  - Find an $l$-th order HD with probability $p$ for $E_0$
  - Find a linear approximation (LA) with bias $q$ for $E_1$
  - The bias of the corresponding HDL approximation for $E$ is estimated as

$$\varepsilon = 2^{2^l - 1} p q^{2^l}$$

- In practice, $l$ is usually large, so $\varepsilon$ is exponentially small when $q \neq \frac{1}{2}$
- IDEA has a weak-key LA with bias $\frac{1}{2}$, so vulnerable to HDL attack: the only application thus far
- Generally speaking, applications of HDL were limited

# Two Sub-Ciphers Strategy for HDL



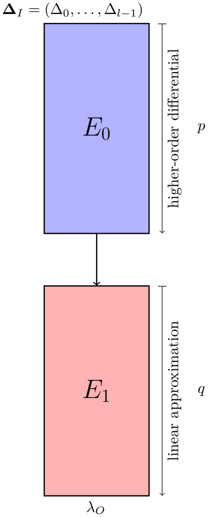

$\mathrm{PR}\left[\lambda_O \cdot \left(\bigoplus_{x \in X \oplus \mathcal{L}(\mathbf{\Delta}_I)} E(x)\right) = 0\right] = \frac{1}{2} + \varepsilon.$

- Process:
  - Find an $l$-th order HD with probability $p$ for $E_0$
  - Find a linear approximation (LA) with bias $q$ for $E_1$
  - The bias of the corresponding HDL approximation for $E$ is estimated as

$$\varepsilon = 2^{2^l - 1} p q^{2^l}$$

- In practice, $l$ is usually large, so $\varepsilon$ is exponentially small when $q \neq \frac{1}{2}$
- IDEA has a weak-key LA with bias $\frac{1}{2}$, so vulnerable to HDL attack: the only application thus far
- Generally speaking, applications of HDL were limited

# Two Sub-Ciphers Strategy for HDL



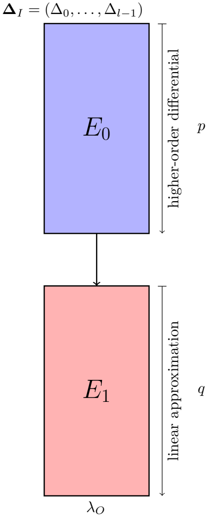

$$\mathrm{PR}\left[\lambda_O \cdot \left(\bigoplus_{x \in X \oplus \mathcal{L}(\boldsymbol{\Delta}_I)} E(x)\right) = 0\right] = \frac{1}{2} + \varepsilon.$$

- Process:
  - Find an $l$-th order HD with probability $p$ for $E_0$
  - Find a linear approximation (LA) with bias $q$ for $E_1$
  - The bias of the corresponding HDL approximation for $E$ is estimated as

$$\varepsilon = 2^{2^l - 1} p q^{2^l}$$

- In practice, $l$ is usually large, so $\varepsilon$ is exponentially small when $q \neq \frac{1}{2}$
- IDEA has a weak-key LA with bias $\frac{1}{2}$, so vulnerable to HDL attack: the only application thus far
- Generally speaking, applications of HDL were limited

# Two Sub-Ciphers Strategy for HDL




$$\mathrm{PR}\left[\lambda_O \cdot \left(\bigoplus_{x \in X \oplus \mathcal{L}(\mathbf{\Delta}_I)} E(x)\right) = 0\right] = \frac{1}{2} + \varepsilon.$$

- Process:
  - Find an $l$-th order HD with probability $p$ for $E_0$
  - Find a linear approximation (LA) with bias $q$ for $E_1$
  - The bias of the corresponding HDL approximation for $E$ is estimated as

$$\varepsilon = 2^{2^l - 1} p q^{2^l}$$

- In practice, $l$ is usually large, so $\varepsilon$ is exponentially small when $q \neq \frac{1}{2}$
- IDEA has a weak-key LA with bias $\frac{1}{2}$, so vulnerable to HDL attack: the only application thus far
- Generally speaking, applications of HDL were limited

# Algebraic Perspective on Differential

- Proposed by Liu, Lu, and Lin at CRYPTO 2021 [LLL21]
- A new method to evaluate the bias of the differential-linear approximation $(\Delta_I, \lambda_O)$ from an algebraic viewpoint

**Example**

Let $f(x_1, x_2, x_3) = x_1 \oplus x_2x_3 \oplus x_3$ and $\Delta = (1, 1, 0)$. On one hand, the derivation of $f$ with respect to $\Delta$ is

$$\begin{aligned} \mathcal{D}_\Delta(f) &= f(X) \oplus f(X \oplus \Delta) = f(x_1, x_2, x_3) \oplus f(x_1 \oplus 1, x_2 \oplus 1, x_3) \\ &= (x_1 \oplus x_2x_3 \oplus x_3) \oplus ((x_1 \oplus 1)x_3 \oplus x_3) = x_3 \oplus 1 \end{aligned}$$

We introduce an auxiliary Boolean function with an auxiliary variable $x$,

$$\begin{aligned} f_\Delta = f([x_1, x_2, x_3] \oplus x[1, 1, 0]) &= (x_1 \oplus x) \oplus (x_2 \oplus x)x_3 \oplus x_3 \\ &= (x_3 \oplus 1)x \oplus x_1 \oplus x_2x_3 \oplus x_3 \end{aligned}$$

# Outline

# Algebraic Perspective on HDL

## Example

Let $f(x_1,x_2,x_3) = x_1x_2x_3 \oplus x_1 \oplus x_2x_3 \oplus x_3$, $\Delta_1 = (1,1,0)$, $\Delta_2 = (0,1,1)$. On one hand, the 2nd higher-order derivation of $f$ with respect to $(\Delta_1,\Delta_2)$ is

$$\begin{aligned}\mathcal{D}_\Delta(f) &= f(X) \oplus f(X \oplus \Delta_1) \oplus f(X \oplus \Delta_2) \oplus f(X \oplus \Delta_1 \oplus \Delta_1)\\ &= f(x_1,x_2,x_3) \oplus f(x_1 \oplus 1, x_2 \oplus 1, x_3) \oplus f(x_1, x_2 \oplus 1, x_3 \oplus 1) \oplus f(x_1 \oplus 1, x_2 \oplus, x_3 \oplus 1)\\ &= x_1 \oplus x_2 \oplus x_3 \oplus 1\end{aligned}$$

We introduce an auxiliary Boolean function with 2 auxiliary variables $u, v$,

$$\begin{aligned}f_\Delta &= f([x_1,x_2,x_3] \oplus u\Delta_0 \oplus v\Delta_2)\\ &= (x_1 \oplus x_2 \oplus x_3 \oplus 1)uv \oplus (x_1x_3 \oplus x_2x_3 \oplus 1)u\\ &\oplus (x_1x_2 \oplus x_1x_3 \oplus x_1 \oplus x_2 \oplus x_3)v \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1\end{aligned}$$

$u\Delta_0 = u[1,1,0] = [u,u,0], v\Delta_1 = v[0,1,1] = [0,v,v]$

# Algebraic Perspective on HD/HDL

- With an $l$-th order difference $\boldsymbol{\Delta} = (\Delta_0, \Delta_1, \ldots, \Delta_{l-1})$, the $l$-th order differential of $f$ is

$$\mathcal{D}_{\boldsymbol{\Delta}} f(X) = \bigoplus_{a \in X \oplus \mathcal{L}(\boldsymbol{\Delta})} f(a), \quad \mathcal{L}(\boldsymbol{\Delta}) \text{ is the linear span of } \boldsymbol{\Delta}$$

- We are operating a $l$-dimensional affine space $\mathbb{A}^l = X \oplus \mathcal{L}(\boldsymbol{\Delta})$. Find a bijective mapping:

$$\mathcal{M}^l : \mathbb{F}_2^l \to \mathbb{A}^l$$
$$(x_0, x_1, \ldots, x_{l-1}) \mapsto X \oplus x_0\Delta_0 \oplus x_1\Delta_1 \oplus \cdots \oplus x_{n-1}\Delta_{l-1} = X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T$$

$\mathbb{A}^l$ and $\mathbb{F}_2^l$ are transformed mutually. $\bigoplus_{a \in X \oplus \mathcal{L}(\boldsymbol{\Delta})} f(a) = \bigoplus_{x \in \mathbb{F}_2^n} f(\mathcal{M}^l(x))$

**Proposition (Algebraic-Perspective on HD/HDL)**

*Given $f$ and an $l$-th order difference $\boldsymbol{\Delta}$,* $\mathcal{D}_{\boldsymbol{\Delta}} f = D_{\boldsymbol{x}} f_{\boldsymbol{\Delta}} = \mathsf{Coe}\left(\boldsymbol{x}, f(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T)\right)$

We call $f(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T)$ Differential Supporting Function (DSF), denoted by $\mathrm{DSF}_{f,X,\boldsymbol{\Delta}}$

# Algebraic Perspective on HD/HDL

- With an $l$-th order difference $\boldsymbol{\Delta} = (\Delta_0, \Delta_1, \ldots, \Delta_{l-1})$, the $l$-th order differential of $f$ is

$$\mathcal{D}_{\boldsymbol{\Delta}} f(X) = \bigoplus_{a \in X \oplus \mathcal{L}(\boldsymbol{\Delta})} f(a), \quad \mathcal{L}(\boldsymbol{\Delta}) \text{ is the linear span of } \boldsymbol{\Delta}$$

- We are operating a $l$-dimensional affine space $\mathbb{A}^l = X \oplus \mathcal{L}(\boldsymbol{\Delta})$. Find a bijective mapping:

$$\mathcal{M}^l : \mathbb{F}_2^l \rightarrow \mathbb{A}^l$$
$$(x_0, x_1, \ldots, x_{l-1}) \mapsto X \oplus x_0\Delta_0 \oplus x_1\Delta_1 \oplus \cdots \oplus x_{n-1}\Delta_{l-1} = X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T$$

$\mathbb{A}^l$ and $\mathbb{F}_2^l$ are transformed mutually. $\bigoplus_{a \in X \oplus \mathcal{L}(\boldsymbol{\Delta})} f(a) = \bigoplus_{x \in \mathbb{F}_2^n} f(\mathcal{M}^l(x))$

**Proposition (Algebraic-Perspective on HD/HDL)**

*Given $f$ and an $l$-th order difference $\boldsymbol{\Delta}$, $\mathcal{D}_{\boldsymbol{\Delta}} f = D_{\boldsymbol{x}} f_{\boldsymbol{\Delta}} = \mathsf{Coe}\left(\boldsymbol{x}, f(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T)\right)$*

We call $f(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T)$ Differential Supporting Function (DSF), denoted by $\mathrm{DSF}_{f,X,\boldsymbol{\Delta}}$

# Algebraic Perspective on HD/HDL

- With an $l$-th order difference $\boldsymbol{\Delta} = (\Delta_0, \Delta_1, \ldots, \Delta_{l-1})$, the $l$-th order differential of $f$ is

$$\mathcal{D}_{\boldsymbol{\Delta}} f(X) = \bigoplus_{a \in X \oplus \mathcal{L}(\boldsymbol{\Delta})} f(a), \quad \mathcal{L}(\boldsymbol{\Delta}) \text{ is the linear span of } \boldsymbol{\Delta}$$

- We are operating a $l$-dimensional affine space $\mathbb{A}^l = X \oplus \mathcal{L}(\boldsymbol{\Delta})$. Find a bijective mapping:

$$\mathcal{M}^l : \mathbb{F}_2^l \to \mathbb{A}^l$$

$$(x_0, x_1, \ldots, x_{l-1}) \mapsto X \oplus x_0\Delta_0 \oplus x_1\Delta_1 \oplus \cdots \oplus x_{n-1}\Delta_{l-1} = X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T$$

$\mathbb{A}^l$ and $\mathbb{F}_2^l$ are transformed mutually. $\bigoplus_{a \in X \oplus \mathcal{L}(\boldsymbol{\Delta})} f(a) = \bigoplus_{x \in \mathbb{F}_2^n} f(\mathcal{M}^l(x))$

## Proposition (Algebraic-Perspective on HD/HDL)

*Given $f$ and an $l$-th order difference $\boldsymbol{\Delta}$,* $\mathcal{D}_{\boldsymbol{\Delta}} f = D_{\boldsymbol{x}} f_{\boldsymbol{\Delta}} = \mathsf{Coe}\left(\boldsymbol{x}, f(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T)\right)$

We call $f(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T)$ Differential Supporting Function (DSF), denoted by $\mathrm{DSF}_{f,X,\boldsymbol{\Delta}}$

# Algebraic Perspective on HD/HDL

- With an $l$-th order difference $\boldsymbol{\Delta} = (\Delta_0, \Delta_1, \ldots, \Delta_{l-1})$, the $l$-th order differential of $f$ is

$$\mathcal{D}_{\boldsymbol{\Delta}} f(X) = \bigoplus_{a \in X \oplus \mathcal{L}(\boldsymbol{\Delta})} f(a), \quad \mathcal{L}(\boldsymbol{\Delta}) \text{ is the linear span of } \boldsymbol{\Delta}$$

- We are operating a $l$-dimensional affine space $\mathbb{A}^l = X \oplus \mathcal{L}(\boldsymbol{\Delta})$. Find a bijective mapping:

$$\mathcal{M}^l : \mathbb{F}_2^l \to \mathbb{A}^l$$
$$(x_0, x_1, \ldots, x_{l-1}) \mapsto X \oplus x_0\Delta_0 \oplus x_1\Delta_1 \oplus \cdots \oplus x_{n-1}\Delta_{l-1} = X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T$$

$\mathbb{A}^l$ and $\mathbb{F}_2^l$ are transformed mutually. $\bigoplus_{a \in X \oplus \mathcal{L}(\boldsymbol{\Delta})} f(a) = \bigoplus_{x \in \mathbb{F}_2^n} f(\mathcal{M}^l(x))$

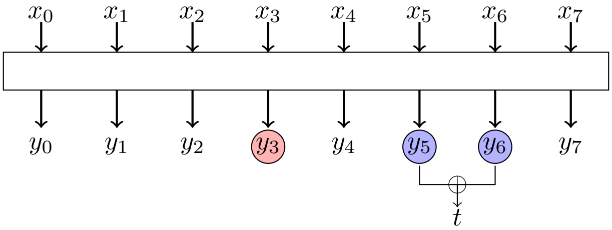
## Proposition (Algebraic-Perspective on HD/HDL)

*Given $f$ and an $l$-th order difference $\boldsymbol{\Delta}$,* $\mathcal{D}_{\boldsymbol{\Delta}} f = D_{\boldsymbol{x}} f_{\boldsymbol{\Delta}} = \mathsf{Coe}\left(\boldsymbol{x}, f(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T)\right)$

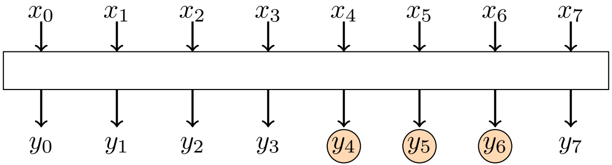
We call $f(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T)$ Differential Supporting Function (DSF), denoted by $\mathrm{DSF}_{f,X,\boldsymbol{\Delta}}$

# Difference between HD and HDL

HDL: we study one output Boolean function or a linear combination of several output bits




HD: we study several (greater than 1) output Boolean functions simultaneously



# Outline

# HD Cryptanalysis on ASCON Permutation

## Notations for ASCON permutation

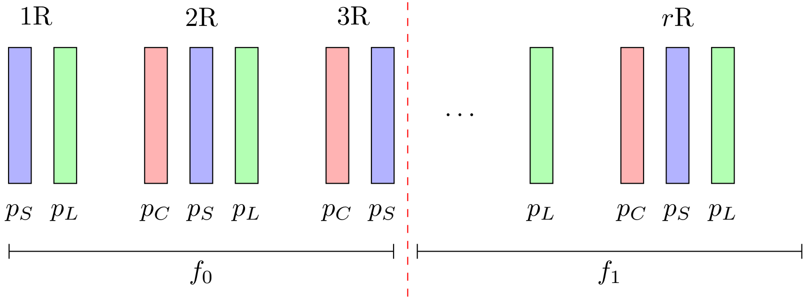
- $S^r$ : the output state after $r$ rounds. $S^0$ is the input of the whole permutation. $S^{r.5}$ is the output of $r+1$ rounds without the last diffusion layer
- $S^r[i]$ : the $i$-th word(row) of $S^r$
- $S^r[i][j]$ : the $j$-th bit of $S^r[i]$
- $p_C$ : the operation of *addition of constants*
- $p_S$ : the operation of *substitution layer*
- $p_L$ : the operation of *diffusion layer*

## HD Cryptanalysis on Ascon Permutation

### Idea

Find a proper combination $(X, \boldsymbol{\Delta})$ to simplify the DSF $(f(\boldsymbol{X} \oplus \boldsymbol{x}\boldsymbol{\Delta}^T))$ *s.t.*, $\deg(\mathrm{DSF}_{f,X,\boldsymbol{\Delta}}) < \dim(\boldsymbol{\Delta})$

### Divide the permutation into two parts (without the first $p_C$)




$f_0$ : calculate the exact ANFs (symbolical computation)

$f_1$ : estimate the upper bound on the degrees of outputs

# Degree Matrix Transition of the Ascon Permutation

## Definition (Degree Matrix of $S^r$)

The algebraic degrees of the bits in the state $S^r$ are called a degree matrix of $S^r$, denoted by

$$\mathrm{DM}(S^r) = (\deg(S^r[i][j]), 0 \le i < 5, 0 \le j < 64)\,.$$

## Degree Matrix Transition over $p_S$

$$y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1x_0 + x_1 + x_0 \qquad d_0' = \max(d_4 + d_1, d_3, d_2 + d_1, d_2, d_2 + d_0, d_1, d_0)$$

$$y_1 = x_4 + x_3x_2 + x_3x_1 + \cdots \qquad d_1' = \max(d_4, d_3 + d_2, d_3 + d_1, \ldots)$$

$$y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1 \qquad d_2' = \max(d_4 + d_3, d_4, d_2, d_1, 0)$$

$$y_3 = x_4x_0 + x_4 + x_3x_0 + x_3 + x_2 + x_1 + x_0 \qquad d_3' = \max(d_4 + d_0, d_4, d_3 + d_0, d_3, d_2, d_1, d_0)$$

$$y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1 \qquad d_4' = \max(d_4 + d_1, d_4, d_3, d_1 + d_0, d_1)$$

# Degree Matrix Transition of the Ascon Permutation

## Degree Matrix Transition over $p_L$

$$
\begin{aligned}
y_0 &\leftarrow \Sigma_0(x_0) = x_0 + (x_0 \ggg 19) + (x_0 \ggg 28) \\
y_1 &\leftarrow \Sigma_1(x_1) = x_1 + (x_1 \ggg 61) + (x_1 \ggg 39) \\
y_2 &\leftarrow \Sigma_2(x_2) = x_2 + (x_2 \ggg 1) + (x_2 \ggg 6) \\
y_3 &\leftarrow \Sigma_3(x_3) = x_3 + (x_3 \ggg 10) + (x_3 \ggg 17) \\
y_4 &\leftarrow \Sigma_4(x_4) = x_4 + (x_4 \ggg 7) + (x_4 \ggg 41)
\end{aligned}
$$

$$
\begin{aligned}
d'_{0,j} &= \max(d_{0,j+0}, d_{0,j-19 \bmod 64}, d_{0,j-28 \bmod 64}) \\
d'_{1,j} &= \max(d_{1,j+0}, d_{1,j-61 \bmod 64}, d_{1,j-39 \bmod 64}) \\
d'_{2,j} &= \max(d_{2,j+0}, d_{2,j-1 \bmod 64}, d_{2,j-6 \bmod 64}) \\
d'_{3,j} &= \max(d_{3,j+0}, d_{3,j-10 \bmod 64}, d_{3,j-17 \bmod 64}) \\
d'_{4,j} &= \max(d_{4,j+0}, d_{4,j-7 \bmod 64}, d_{4,j-41 \bmod 64})
\end{aligned}
$$

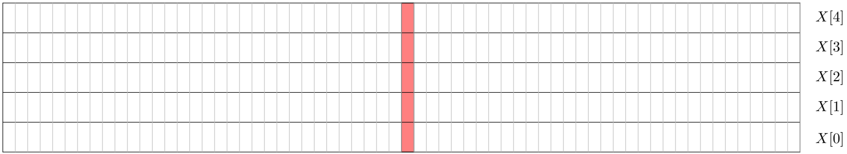
# HD Cryptanalysis on Ascon Permutation

## Method to choose $X$ and $\boldsymbol{\Delta}$

- Exhausting all $X$ and $\boldsymbol{\Delta}$ is impossible
- Note that the first operation of $f_0$ is $p_S$. We inject 1st order difference into each Sbox, totally 64-th order HD

$$p_S(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T) = \mathcal{S}(\bar{X} \oplus x_0\bar{\Delta})||\mathcal{S}(\bar{X} \oplus x_1\bar{\Delta})|| \cdots ||\mathcal{S}(\bar{X} \oplus x_{63}\bar{\Delta}),$$

$$\bar{X} \oplus \boldsymbol{x}_i\bar{\Delta}^T$$




- Since $\bar{X} \in \mathbb{F}_2^5$, $\bar{\Delta} \in \mathbb{F}_2^5 \backslash \{0\}$, we have $32 \times 31 = 992$ choices

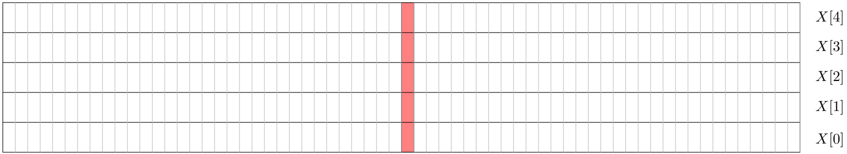
# HD Cryptanalysis on ASCON Permutation

## Method to choose $X$ and $\boldsymbol{\Delta}$

- Exhausting all $X$ and $\boldsymbol{\Delta}$ is impossible
- Note that the first operation of $f_0$ is $p_S$. We inject 1st order difference into each Sbox, totally 64-th order HD

$$p_S(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T) = \mathcal{S}(\bar{X} \oplus x_0\bar{\Delta})||\mathcal{S}(\bar{X} \oplus x_1\bar{\Delta})||\cdots||\mathcal{S}(X \oplus x_{63}\bar{\Delta}),$$

$$\bar{X} \oplus \boldsymbol{x}_i\bar{\Delta}^T$$




- Since $\bar{X} \in \mathbb{F}_2^5$, $\bar{\Delta} \in \mathbb{F}_2^5 \backslash \{0\}$, we have $32 \times 31 = 992$ choices

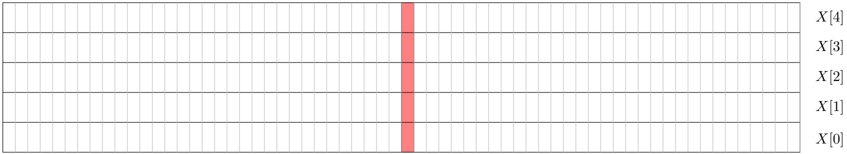
# HD Cryptanalysis on Ascon Permutation

## Method to choose $X$ and $\boldsymbol{\Delta}$

- Exhausting all $X$ and $\boldsymbol{\Delta}$ is impossible
- Note that the first operation of $f_0$ is $p_S$. We inject 1st order difference into each Sbox, totally 64-th order HD

$$p_S(X \oplus \boldsymbol{x}\boldsymbol{\Delta}^T) = \mathcal{S}(\bar{X} \oplus x_0\bar{\Delta})||\mathcal{S}(\bar{X} \oplus x_1\bar{\Delta})||\cdots||\mathcal{S}(X \oplus x_{63}\bar{\Delta}),$$

$\bar{X} \oplus \boldsymbol{x}_i\bar{\Delta}^T$




- Since $\bar{X} \in \mathbb{F}_2^5$, $\bar{\Delta} \in \mathbb{F}_2^5 \backslash \{0\}$, we have $32 \times 31 = 992$ choices

# HD Distinguishers for ASCON Permutation

With an exhaustive search, we find 8 optimal combinations:

$$(\bar{X}, \bar{\Delta}) \in \left\{ \begin{array}{l} (\texttt{0x6}, \texttt{0x13}), (\texttt{0xa}, \texttt{0x13}), (\texttt{0xc}, \texttt{0x17}), (\texttt{0xf}, \texttt{0x18}), \\ (\texttt{0x15}, \texttt{0x13}), (\texttt{0x17}, \texttt{0x18}), (\texttt{0x19}, \texttt{0x13}), (\texttt{0x1b}, \texttt{0x17}) \end{array} \right\}$$

$$[0,0,1,1,0]^{\mathrm{T}} \oplus x[1,0,0,1,1]^{\mathrm{T}} = [x,0,1,1 \oplus x, x]^{\mathrm{T}}$$

| **Round $r$** | **Upper bounds on the algebraic degree** | | | | |
|---|---|---|---|---|---|
| | $S^r[0]$ | $S^r[1]$ | $S^r[2]$ | $S^r[3]$ | $S^r[4]$ |
| 4 | 3 | 3 | 2 | 2 | 3 |
| 5 | 6 | 5 | 5 | 6 | 6 |
| 6 | 11 | 11 | 12 | 12 | 11 |
| 7 | 23 | 24 | 23 | 23 | 22 |
| 8 | 47 | 47 | 45 | 46 | 47 |

# Zero-Sum Distinguisher for Full Ascon Permutation

- Apply a similar method to inverse Ascon permutation (including an extra $p_C$), we obtain 2 optimal combinations:

$$(\bar{X}, \bar{\boldsymbol{\Delta}}) \in \{(\texttt{0xf}, \texttt{0x18}), (\texttt{0x17}, \texttt{0x18})\}$$

| **Round** $r$ | **Upper bounds on the algebraic degree** | | | | |
|---|---|---|---|---|---|
| | $S[0]$ | $S[1]$ | $S[2]$ | $S[3]$ | $S[4]$ |
| 1 | 2 | 1 | 2 | 0 | 2 |
| 2 | 4 | 6 | 6 | 6 | 6 |
| 3 | 18 | 16 | 18 | 18 | 18 |
| 4 | 54 | 54 | 54 | 54 | 54 |

- Since $(\texttt{0xf}, \texttt{0x18}), (\texttt{0x17}, \texttt{0x18})$ are also optimal for the forward Ascon permutation, we obtain zero-sum distinguishers:
- **12 R**: $2^{55}$ calls, **11 R**: $2^{48}$ calls, **8 R**: $2^{13}$ calls, **6 R**: $2^{7}$ calls

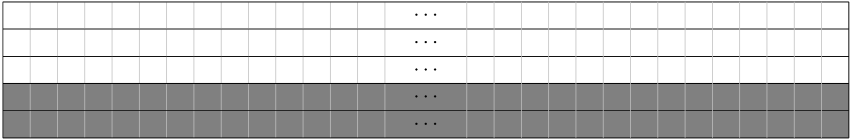
# Impact of these Zero-Sum Distinguishers

- Zero-sum distinguishers represent some non-ideal property of the target permutation
- Although these zero-sum distinguishers require low complexities, their actual impact on the security of the Ascon AEAD and Hash are very likely non-existent or at best not clear
- Advantage of the zero-sum distinguisher for Ascon permutation and a perfect permutation is very small, usually falling under a factor of 2

# Outline

# HDL Cryptanalysis on Ascon Initialization

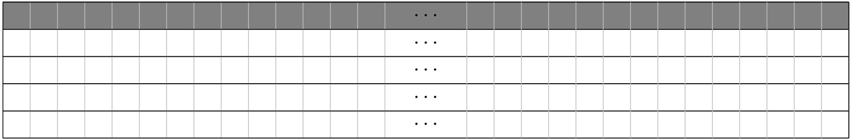
- For initialization, we can only access $S^0[3]$ and $S^0[4]$, thus $\bar{X} \in \{0, 1, 2, 3\}$ and $\bar{\Delta} \in \{1, 2, 3\}$



- Focus on the 2nd order HDL. We choose 2 different positions $(i_0, i_1)$ to impose differences, IV are set as specification, other positions are filled with free variables
- When $(i_0, i_1) = (0, 60)$, $(\bar{X}, \bar{\Delta}) = (\texttt{0x0}, \texttt{0x3})$, we have $\deg(S^{3.5}[50]) \leq 1$
- 1 sample (4 texts) is enough to distinguish the 4 rounds of Ascon initialization

# HDL Cryptanalysis on Ascon Encryption

- For encryption, we can only access $S^0[0]$, thus $\bar{X} \in \{\texttt{0}, \texttt{0x10}\}$ and $\bar{\Delta} \in \{\texttt{0x10}\}$



- Focus on the 2nd order HDL. We choose 2 different positions $(i_0, i_1)$ to impose differences, other positions are filled with free variables
- When $(i_0, i_1) = (0, 22)$, $(\bar{X}, \bar{\Delta}) = (\texttt{0x0}, \texttt{0x10})$, we have $\deg(S^{3.5}[50]) \leq 1$
- 1 sample (4 texts) is enough to distinguish the 4 rounds of Ascon encryption under the nonce-misuse scenario

# Outline

# Practical Distinguishers for Ascon Initialization

## Observation

HD attacks on a Boolean function is equivalent to cube attacks on its DSF.

We can apply cube testers to DSF, then convert it back to a HD distinguisher.

Input of each sbox: $[0, 0, 0, 0, 0] \oplus x[0, 0, 0, 1, 1]^T$

Table: Practical HDL Distinguishers for 5-Round Ascon Initialization

| **Order** | **Input/Output Mask** | **Bias**$(-\log)$ | **Con. Bias**$(-\log)$ |
|---|---|---|---|
| 3 | `(0,24,33)/51` | 6.52 | 3.56 |
| 4 | `(0,9,15,41)/27` | 6.44 | 2.14 |
| 5 | `(0,9,24,51,55)/18` | 5.31 | 2.02 |
| 6 | `(1,12,18,22,21,52)/49` | 4.88 | 1.89 |
| 7 | `(10,13,21,31,49,55,61)/28` | 4.03 | 1 |
| 8 | `(0,3,10,11,26,28,31,55)/60` | 2.46 | 1 |
| 9 | `(8,13,14,16,21,25,39,42,46)/12` | 1.76 | 1 |
| 10 | `(4,14,23,27,35,39,41,49,51,55)/0` | 1.09 | 1 |
| 11 | `(19,24,33,35,36,48,54,57,59,62,63)/27` | 1.04 | 1 |

# Summary

- Algebraic perspective on the HDL cryptanalysis
- Efficient HD or zero-sum distinguishers on Ascon permutation, initialization and encryption
- Practical HDL distinguishers for Ascon
- The key-recovery attack based on the conditional HDL is given in our paper

Thanks for your attention!

# Summary

- Algebraic perspective on the HDL cryptanalysis
- Efficient HD or zero-sum distinguishers on Ascon permutation, initialization and encryption
- Practical HDL distinguishers for Ascon
- The key-recovery attack based on the conditional HDL is given in our paper

Thanks for your attention!

# Reference


[LLL21] Meicheng Liu, Xiaojuan Lu, and Dongdai Lin. Differential-Linear Cryptanalysis from an Algebraic Perspective. CRYPTO 2021

[RHSS21] Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun. Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon. FSE 2021

[DEMS15] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Cryptanalysis of Ascon. CT-RSA 2015

[LDW17] Zheng Li, Xiaoyang Dong, and Xiaoyun Wang. Conditional Cube Attack on Round-Reduced ASCON. IACR Trans. Symmetric Cryptol., 2017(1)