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

Results in This Work

Introduction to HD/HDL

Algebraic Perspective on HD/HDL

HD Cryptanalysis on Ascon Permutation

HDL Cryptanalysis on Ascon Initialization and Encryption

Practical HDL Distinguishers Based on Cube Testers
Outline

Results in This Work

Introduction to HD/HDL

Algebraic Perspective on HD/HDL

HD Cryptanalysis on ASCON Permutation

HDL Cryptanalysis on ASCON Initialization and Encryption

Practical HDL Distinguishers Based on Cube Testers
## Results in This Work for Ascon

- **Permutation (black-box model)**
- **Permutation (non-black-box model)**
- **Initialization**
- **Encryption (Nonce-Misuse Scenario)**

<table>
<thead>
<tr>
<th>Type</th>
<th>Round</th>
<th>Data (log)</th>
<th>Time (log)</th>
<th>Method</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinguisher</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>HD ●</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>13</td>
<td>13</td>
<td>HDL ▲ ●</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>12</td>
<td>12</td>
<td>HD ●</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>23</td>
<td>23</td>
<td>HD ●</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>46</td>
<td>46</td>
<td>HD ●</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>48</td>
<td>48</td>
<td>Zero-Sum</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>55</td>
<td>55</td>
<td>Zero-Sum</td>
<td>Ours</td>
</tr>
<tr>
<td>Key-Recovery</td>
<td>5</td>
<td>23</td>
<td>23</td>
<td>Cond. HDL</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>74</td>
<td>74</td>
<td>Cond. HDL</td>
<td>Ours</td>
</tr>
</tbody>
</table>

Comparisons with existing results can be found in our paper.
Outline

Results in This Work

Introduction to HD/HDL

Algebraic Perspective on HD/HDL

HD Cryptanalysis on ASCON Permutation

HDL Cryptanalysis on ASCON Initialization and Encryption

Practical HDL Distinguishers Based on Cube Testers
Higher-Order Differential-Linear Analysis

Higher-Order differential (HD) was Proposed by Lai in 1994

- Given \( l \) linearly independent values \( \Delta_I = (\Delta_0, \Delta_1, \ldots, \Delta_{l-1}) \), the \( l \)-th order HD of \( E \) is

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

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,

\[
\Pr \left[ \lambda_O \cdot \left( \bigoplus_{x \in X \oplus \mathcal{L}(\Delta_I)} E(x) \right) = 0 \right] = \frac{1}{2} + \varepsilon.
\]
Higher-Order Differential-Linear Analysis

- Higher-Order differential (HD) was Proposed by Lai in 1994
  - Given $l$ linearly independent values $\Delta_I = (\Delta_0, \Delta_1, \ldots, \Delta_{l-1})$, the $l$-th order HD of $E$ is
    \[
    p = \Pr \left[ \bigoplus_{x \in X \oplus \mathcal{L}(\Delta_I)} E(x) = \Delta_O \right]
    \]

- 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,
    \[
    \Pr \left[ \lambda_O \cdot \left( \bigoplus_{x \in X \oplus \mathcal{L}(\Delta_I)} E(x) \right) = 0 \right] = \frac{1}{2} + \varepsilon.
    \]
Two Sub-Ciphers Strategy for HDL

\[ \Delta_l = (\Delta_0, \ldots, \Delta_{l-1}) \]

- **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
    \[ \varepsilon = 2^{2^l-1}pq^{2^l} \]

- 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

\[ \text{PR} \left[ \lambda_0 \cdot \left( \bigoplus_{x \in X} \Theta_{\Delta_l} E(x) \right) = 0 \right] = \frac{1}{2} + \varepsilon. \]
Two Sub-Ciphers Strategy for HDL

\[ \Delta_i = (\Delta_0, \ldots, \Delta_{l-1}) \]

\[ E_0 \]

\[ p \]

\[ E_1 \]

\[ q \]

\[ \lambda_0 \]

- **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
    \[ \varepsilon = 2^{2^l - 1}pq^2 \]

- **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

\[ \Delta_l = (\Delta_0, \ldots, \Delta_{l-1}) \]

\[ E_0 \]

\[ p \]

higher-order differential

\[ \lambda_0 \]

\[ E_1 \]

\[ q \]

linear approximation

\[ PR \left[ \lambda_0 \cdot \left( \bigoplus_{x \in X} \delta_{E_1}(\Delta_l) E(x) \right) = 0 \right] = \frac{1}{2} + \varepsilon. \]

- **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
  \[ \varepsilon = 2^{2^l-1} pq^{2^l} \]

- 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

\[ \Delta_l = (\Delta_0, \ldots, \Delta_{l-1}) \]

\[ \varepsilon = 2^{2^l - 1}pq^{2^l} \]

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

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

\[
D_\Delta(f) = f(X) \oplus f(X \oplus \Delta) = f(x_1, x_2, x_3) \oplus f(x_1 \oplus 1, x_2 \oplus 1, x_3) \\
= (x_1 \oplus x_2 x_3 \oplus x_3) \oplus ((x_1 \oplus 1)x_3 \oplus x_3) = x_3 \oplus 1
\]

We introduce an auxiliary Boolean function with an auxiliary variable \(x\),

\[
f_\Delta = f([x_1, x_2, x_3] \oplus x[1, 1, 0]) = (x_1 \oplus x) \oplus (x_2 \oplus x)x_3 \oplus x_3 \\
= (x_3 \oplus 1)x \oplus x_1 \oplus x_2 x_3 \oplus x_3
\]
Outline

Results in This Work

Introduction to HD/HDL

Algebraic Perspective on HD/HDL

HD Cryptanalysis on ASCON Permutation

HDL Cryptanalysis on ASCON Initialization and Encryption

Practical HDL Distinguishers Based on Cube Testers
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

$$D_{\Delta}(f) = f(X) \oplus f(X \oplus \Delta_1) \oplus f(X \oplus \Delta_2) \oplus f(X \oplus \Delta_1 \oplus \Delta_1)$$
$$= f(x_1, x_2, x_3) \oplus f(x_1 \oplus 1, x_2 \oplus 1, x_3) \oplus f(x_1, x_2 \oplus 1, x_3 \oplus 1) \oplus f(x_1 \oplus 1, x_2 \oplus, x_3 \oplus 1)$$
$$= x_1 \oplus x_2 \oplus x_3 \oplus 1$$

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

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

$$u\Delta_0 = u[1, 1, 0] = [u, u, 0], v\Delta_1 = v[0, 1, 1] = [0, v, v]$$
Algebraic Perspective on HD/HDL

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

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

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

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

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

$\mathbb{A}^l$ and $\mathbb{F}_2^l$ are transformed mutually.

$$\bigoplus_{a \in X \oplus \mathcal{L}(\Delta)} f(a) = \bigoplus_{x \in \mathbb{F}_2^l} f(\mathcal{M}^l(x))$$

Proposition (Algebraic-Perspective on HD/HDL)

Given $f$ and an $l$-th order difference $\Delta$, $D_{\Delta}f = D_xf_\Delta = \text{Coe}(x, f(X \oplus x \Delta^T))$

We call $f(X \oplus x \Delta^T)$ Differential Supporting Function (DSF), denoted by $\text{DSF}_{f, X, \Delta}$
Algebraic Perspective on HD/HDL

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

\[
D_{\Delta} f(X) = \bigoplus_{a \in X \oplus \mathcal{L}(\Delta)} f(a), \quad \mathcal{L}(\Delta) \text{ is the linear span of } \Delta
\]

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

\[
\mathcal{M}^l : \mathbb{F}_2^l \rightarrow \mathbb{A}^l
\]

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

\(\mathbb{A}^l\) and \(\mathbb{F}_2^l\) are transformed mutually.

\[
\bigoplus_{a \in X \oplus \mathcal{L}(\Delta)} f(a) = \bigoplus_{x \in \mathbb{F}_2^n} f(\mathcal{M}^l(x))
\]

Proposition (Algebraic-Perspective on HD/HDL)

Given \(f\) and an \(l\)-th order difference \(\Delta\), \(D_{\Delta} f = D_X f_{\Delta} = \text{Coe} (x, f(X \oplus x \Delta^T))\)

We call \(f(X \oplus x \Delta^T)\) Differential Supporting Function (DSF), denoted by \(\text{DSF}_{f,X,\Delta}\)
Algebraic Perspective on HD/HDL

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

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

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

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

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

$\mathbb{A}^l$ and $\mathbb{F}_2^l$ are transformed mutually.

$$\bigoplus_{a \in X \oplus \mathcal{L}(\Delta)} f(a) = \bigoplus_{x \in \mathbb{F}_2^n} f(\mathcal{M}^l(x))$$

Proposition (Algebraic-Perspective on HD/HDL)

Given $f$ and an $l$-th order difference $\Delta$, $D_{\Delta} f = D_x f_{\Delta} = \text{Coe}(x, f(X \oplus x \Delta^T))$

We call $f(X \oplus x \Delta^T)$ Differential Supporting Function (DSF), denoted by $\text{DSF}_{f, x, \Delta}$
Algebraic Perspective on HD/HDL

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

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

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

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

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

$\mathbb{A}^l$ and $\mathbb{F}_2^l$ are transformed mutually.

$$\bigoplus_{a \in X \oplus \mathcal{L}(\Delta)} f(a) = \bigoplus_{x \in \mathbb{F}_2^n} f(\mathcal{M}^l(x))$$

Proposition (Algebraic-Perspective on HD/HDL)

*Given $f$ and an $l$-th order difference $\Delta$, $D_{\Delta} f = D_x f \Delta = \text{Coe}\,(x, f(X \oplus x \Delta^T))$*

We call $f(X \oplus x \Delta^T)$ Differential Supporting Function (DSF), denoted by $\text{DSF}_f, x, \Delta$
**Difference between HD and HDL**

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

```
<table>
<thead>
<tr>
<th>x0</th>
<th>x1</th>
<th>x2</th>
<th>x3</th>
<th>x4</th>
<th>x5</th>
<th>x6</th>
<th>x7</th>
</tr>
</thead>
<tbody>
<tr>
<td>y0</td>
<td>y1</td>
<td>y2</td>
<td>y3</td>
<td>y4</td>
<td>y5</td>
<td>y6</td>
<td>y7</td>
</tr>
</tbody>
</table>
```

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

```
<table>
<thead>
<tr>
<th>x0</th>
<th>x1</th>
<th>x2</th>
<th>x3</th>
<th>x4</th>
<th>x5</th>
<th>x6</th>
<th>x7</th>
</tr>
</thead>
<tbody>
<tr>
<td>y0</td>
<td>y1</td>
<td>y2</td>
<td>y3</td>
<td>y4</td>
<td>y5</td>
<td>y6</td>
<td>y7</td>
</tr>
</tbody>
</table>
```
Outline

Results in This Work

Introduction to HD/HDL

Algebraic Perspective on HD/HDL

**HD Cryptanalysis on AsCON Permutation**

HDL Cryptanalysis on AsCON Initialization and Encryption

Practical HDL Distinguishers Based on Cube Testers
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 \((X, \Delta)\) to simplify the DSF \(f(X \oplus x\Delta^T)\) s.t.,
\[\text{deg}(\text{DSF}_{f,X,\Delta}) < \text{dim}(\Delta)\]

Divide the permutation into two parts (without the first \(p_C\))

\[f_0 : \text{calculate the exact ANFs (symbolical computation)}\]

\[f_1 : \text{estimate the upper bound on the degrees of outputs}\]
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

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

Degree Matrix Transition over $p_S$

\[
\begin{align*}
y_0 &= x_4x_1 + x_3 + x_2x_1 + x_2 + x_1x_0 + x_1 + x_0 \\
y_1 &= x_4 + x_3x_2 + x_3x_1 + \\
y_2 &= x_4x_3 + x_4 + x_2 + x_1 + 1 \\
y_3 &= x_4x_0 + x_4 + x_3x_0 + x_3 + x_2 + x_1 + x_0 \\
y_4 &= x_4x_1 + x_4 + x_3 + x_1x_0 + x_1
\end{align*}
\]

\[
\begin{align*}
d_0' &= \max(d_4 + d_1, d_3, d_2 + d_1, d_2, d_2 + d_0, d_1, d_0) \\
d_1' &= \max(d_4, d_3 + d_2, d_3 + d_1, \ldots) \\
d_2' &= \max(d_4 + d_3, d_4, d_2, d_1, 0) \\
d_3' &= \max(d_4 + d_0, d_4, d_3 + d_0, d_3, d_2, d_1, d_0) \\
d_4' &= \max(d_4 + d_1, d_4, d_3, d_1 + d_0, d_1)
\end{align*}
\]
Degree Matrix Transition of the Ascon Permutation

Degree Matrix Transition over $p_L$

\[
y_0 \leftarrow \Sigma_0(x_0) = x_0 + (x_0 \gg 19) + (x_0 \gg 28)
\]
\[
y_1 \leftarrow \Sigma_1(x_1) = x_1 + (x_1 \gg 61) + (x_1 \gg 39)
\]
\[
y_2 \leftarrow \Sigma_2(x_2) = x_2 + (x_2 \gg 1) + (x_2 \gg 6)
\]
\[
y_3 \leftarrow \Sigma_3(x_3) = x_3 + (x_3 \gg 10) + (x_3 \gg 17)
\]
\[
y_4 \leftarrow \Sigma_4(x_4) = x_4 + (x_4 \gg 7) + (x_4 \gg 41)
\]
\[
d'_{0,j} = \max(d_{0,j} + 0, d_{0,j} - 19 \mod 64, d_{0,j} - 28 \mod 64)
\]
\[
d'_{1,j} = \max(d_{1,j} + 0, d_{1,j} - 61 \mod 64, d_{1,j} - 39 \mod 64)
\]
\[
d'_{2,j} = \max(d_{2,j} + 0, d_{2,j} - 1 \mod 64, d_{2,j} - 6 \mod 64)
\]
\[
d'_{3,j} = \max(d_{3,j} + 0, d_{3,j} - 10 \mod 64, d_{3,j} - 17 \mod 64)
\]
\[
d'_{4,j} = \max(d_{4,j} + 0, d_{4,j} - 7 \mod 64, d_{4,j} - 41 \mod 64)
\]
HD Cryptanalysis on Ascon Permutation

Method to choose $X$ and $\Delta$

- Exhausting all $X$ and $\Delta$ 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

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

$$\bar{X} \oplus x_i\bar{\Delta}^T$$

- Since $\bar{X} \in \mathbb{F}_2^5$, $\bar{\Delta} \in \mathbb{F}_2^5\setminus\{0\}$, we have $32 \times 31 = 992$ choices
HD Cryptanalysis on Ascon Permutation

Method to choose $X$ and $\Delta$

- Exhausting all $X$ and $\Delta$ 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

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

$$\bar{X} \oplus x_i\bar{\Delta}^T$$

- Since $\bar{X} \in \mathbb{F}_2^5$, $\bar{\Delta} \in \mathbb{F}_2^5 \setminus \{0\}$, we have $32 \times 31 = 992$ choices
HD Cryptanalysis on Ascon Permutation

Method to choose $X$ and $\Delta$

- Exhausting all $X$ and $\Delta$ 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

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

$\bar{X} \oplus x_i\bar{\Delta}^T$

- Since $\bar{X} \in \mathbb{F}_2^5$, $\bar{\Delta} \in \mathbb{F}_2^5\setminus\{0\}$, we have $32 \times 31 = 992$ choices
HD Distinguishers for Ascon Permutation

With an exhaustive search, we find 8 optimal combinations:

\[
(\tilde{X}, \tilde{\Delta}) \in \left\{ (0x6, 0x13), (0xa, 0x13), (0xc, 0x17), (0xf, 0x18),
(0x15, 0x13), (0x17, 0x18), (0x19, 0x13), (0x1b, 0x17) \right\}
\]

\[
[0, 0, 1, 1, 0]^T \oplus x[1, 0, 0, 1, 1]^T = [x, 0, 1, 1 \oplus x, x]^T
\]

<table>
<thead>
<tr>
<th>Round $r$</th>
<th>Upper bounds on the algebraic degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>23</td>
</tr>
<tr>
<td>8</td>
<td>47</td>
</tr>
</tbody>
</table>
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:

$$\left(\vec{X}, \vec{\Delta}\right) \in \{(0xf, 0x18), (0x17, 0x18)\}$$

<table>
<thead>
<tr>
<th>Round $r$</th>
<th>Upper bounds on the algebraic degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
</tr>
<tr>
<td>4</td>
<td>54</td>
</tr>
</tbody>
</table>

- Since $(0xf, 0x18), (0x17, 0x18)$ 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

Results in This Work

Introduction to HD/HDL

Algebraic Perspective on HD/HDL

HD Cryptanalysis on Ascon Permutation

HDL Cryptanalysis on Ascon Initialization and Encryption

Practical HDL Distinguishers Based on Cube Testers
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 $\bar{\Delta} \in \{1, 2, 3\}$

  ![Diagram showing HDL values]

- 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 $(i_0, i_1) = (0, 60)$, $(\bar{X}, \bar{\Delta}) = (0x0, 0x3)$, 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 $\bar{X} \in \{0, 0x10\}$ and $\bar{\Delta} \in \{0x10\}$

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

- 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 $(i_0, i_1) = (0, 22)$, $(\bar{X}, \bar{\Delta}) = (0x0, 0x10)$, we have $\text{deg}(S^{3.5}[50]) \leq 1$

- 1 sample (4 texts) is enough to distinguish the 4 rounds of Ascon encryption under the nonce-misuse scenario
Outline

Results in This Work

Introduction to HD/HDL

Algebraic Perspective on HD/HDL

HD Cryptanalysis on ASCON Permutation

HDL Cryptanalysis on ASCON Initialization and Encryption

Practical HDL Distinguishers Based on Cube Testers
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

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


