Block Cipher Cryptanalysis

Mahavir Jhawar
Ashoka University
Consider an $S$-box $S: \{0,1\}^m \rightarrow \{0,1\}^n$.

For any $x' \in \{0,1\}^m$, $y' \in \{0,1\}^n$, define $\text{DDT}[x',y'] = |\{x \in \{0,1\}^m | S(x) \oplus S(x \oplus x') = y'\}|$.

For any $x' \in \{0,1\}^m$, define $\Delta[x'] = \{(x,x \oplus x') \in \{0,1\}^m \times \{0,1\}^m | x \oplus x' = x'\}$.

Clearly, $|\Delta[x']| = 2^m$.

Alternatively, $\text{DDT}[x',y'] = |\{(x,x') \in \Delta[x'] | S(x) \oplus S(x') = y'\}|$.
Notations

- Consider an $S$-box $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$. 

- For any $x' \in \{0, 1\}^m$, $y' \in \{0, 1\}^n$, define $\operatorname{DDT}[x', y'] = |\{ x \in \{0, 1\}^m | S(x) \oplus S(x \oplus x') = y' \}|$.

- For any $x' \in \{0, 1\}^m$, define $\Delta[x'] = \{(x, x) \in \{0, 1\}^m \times \{0, 1\}^m | x \oplus x = x'\}$.

- Clearly, $\|\Delta[x']\| = 2^m$.

- Alternatively, $\operatorname{DDT}[x', y'] = |\{ (x, x) \in \Delta[x'] | S(x) \oplus S(x') = y' \}|$. 


Notations

- Consider an $S$-box $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$.
- For any $x' \in \{0, 1\}^m$, $y' \in \{0, 1\}^n$, define
Notations

• Consider an $S$-box $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$.

• For any $x' \in \{0, 1\}^m$, $y' \in \{0, 1\}^n$, define

$$\text{DDT}[x', y'] = |\{x \in \{0, 1\}^m \mid S(x) \oplus S(x \oplus x') = y'\}|$$

• For any $x' \in \{0, 1\}^m$, define

$$\Delta[x'] = \{(x, x^*) \in \{0, 1\}^m \times \{0, 1\}^m \mid x \oplus x^* = x'\}$$

.
Notations

• Consider an $S$-box $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$.

• For any $x' \in \{0, 1\}^m$, $y' \in \{0, 1\}^n$, define

$$\text{DDT}[x', y'] = |\{x \in \{0, 1\}^m \mid S(x) \oplus S(x \oplus x') = y'\}|$$

• For any $x' \in \{0, 1\}^m$, define

$$\Delta[x'] = \{(x, x^*) \in \{0, 1\}^m \times \{0, 1\}^m \mid x \oplus x^* = x'\}$$

• Clearly, $\Delta[x'] = \{(x, x \oplus x') \mid x \in \{0, 1\}^m\}$. 
Notations

- Consider an $S$-box $S : \{0, 1\}^m \to \{0, 1\}^n$.
- For any $x' \in \{0, 1\}^m$, $y' \in \{0, 1\}^n$, define
  \[
  \text{DDT}[x', y'] = |\{x \in \{0, 1\}^m \mid S(x) \oplus S(x \oplus x') = y'\}|
  \]
- For any $x' \in \{0, 1\}^m$, define
  \[
  \Delta[x'] = \{(x, x^*) \in \{0, 1\}^m \times \{0, 1\}^m \mid x \oplus x^* = x'\}
  \]
  Clearly, \[
  \Delta[x'] = \{(x, x \oplus x') \mid x \in \{0, 1\}^m\}.
  \]
  \[
  |\Delta[x']| = 2^m.
  \]
Consider an $S$-box $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$.

For any $x' \in \{0, 1\}^m$, $y' \in \{0, 1\}^n$, define

$$DDT[x', y'] = |\{x \in \{0, 1\}^m \mid S(x) \oplus S(x \oplus x') = y'\}|$$

For any $x' \in \{0, 1\}^m$, define

$$\Delta[x'] = \{(x, x^*) \in \{0, 1\}^m \times \{0, 1\}^m \mid x \oplus x^* = x'\}$$

Clearly, $\Delta[x'] = \{(x, x \oplus x') \mid x \in \{0, 1\}^m\}$.

$|\Delta[x']| = 2^m$.

Alternatively,

$$DDT[x', y'] = |\{(x, x^*) \in \Delta[x'] \mid S(x) \oplus S(x^*) = y'\}|$$
Difference Distribution Table of $S$-boxes

- Define difference distribution table (DDT) of $S$ to be a $2^m \times 2^n$ matrix with $\text{DDT}[x',y']$ as its $(x',y')$ entry.

- Consider the following example $S$: 

$$
\begin{array}{c|cccc}
 & 00 & 01 & 10 & 11 \\
\hline
00 & 4 & 0 & 0 & 0 \\
01 & 2 & 2 & 0 & 0 \\
10 & 0 & 0 & 2 & 2 \\
11 & 0 & 0 & 2 & 2 \\
\end{array}
$$

Table: An $S$-box and its DDT
Difference Distribution Table of $S$-boxes

- Define difference distribution table (DDT) of $S$ to be a $2^m \times 2^n$ matrix with $\text{DDT}[x', y']$ as its $(x', y')$ entry.
Difference Distribution Table of $S$-boxes

- Define difference distribution table (DDT) of $S$ to be a $2^m \times 2^n$ matrix with $DDT[x',y']$ as its $(x',y')$ entry.
- Consider the following example $S: \{0,1\}^2 \rightarrow \{0,1\}^2$

<table>
<thead>
<tr>
<th>$x'$</th>
<th>$y'$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Table**: An $S$ box and its $DDT$
DDT of Keyed S-box

For $S$:

$\{0, 1\}^m \rightarrow \{0, 1\}^n$ and any fixed key $K \in \{0, 1\}^m$, define keyed $S$-box $S_K$ as:

$S_K(x) = S(K \oplus x)$, $x \in \{0, 1\}^m$.

Claim: $\text{DDT}_S = \text{DDT}_{S_K}$.

For our previous $S$:

$\{0, 1\}^2 \rightarrow \{0, 1\}^2$ and a fixed $K = 10 \in \{0, 1\}^2$, consider $S_{10}$:

- $S_{10}(00) = S(10) = 11$
- $S_{10}(01) = S(11) = 10$
- $S_{10}(10) = S(00) = 00$
- $S_{10}(11) = S(01) = 00$

<table>
<thead>
<tr>
<th>$x'$</th>
<th>$y'$</th>
<th>$00$</th>
<th>$01$</th>
<th>$10$</th>
<th>$11$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$00$</td>
<td>$00$</td>
<td>$2$</td>
<td>$2$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$01$</td>
<td>$01$</td>
<td>$4$</td>
<td>$0$</td>
<td>$0$</td>
<td>$0$</td>
</tr>
<tr>
<td>$10$</td>
<td>$10$</td>
<td>$0$</td>
<td>$2$</td>
<td>$2$</td>
<td>$2$</td>
</tr>
<tr>
<td>$11$</td>
<td>$11$</td>
<td>$0$</td>
<td>$2$</td>
<td>$2$</td>
<td>$2$</td>
</tr>
</tbody>
</table>

Table: $S$-box $S_{10}$ and its DDT $\text{DDT}_{S_{10}}$.

Clearly, $\text{DDT}_S = \text{DDT}_{S_{10}}$. 
DDT of Keyed S-box

• For $S : \{0, 1\}^m \to \{0, 1\}^n$ and any fixed key $K \in \{0, 1\}^m$, define keyed S-box $S^k$ as:

\[
S^K(x) = S(x \oplus K), \quad x \in \{0, 1\}^m.
\]
DDT of Keyed $S$-box

- For $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$ and any fixed key $K \in \{0, 1\}^m$, define keyed $S$-box $S^K$ as:

\[ S^K(x) = S(K \oplus x), \quad x \in \{0, 1\}^m. \]
DDT of Keyed $S$-box

- For $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$ and any fixed key $K \in \{0, 1\}^m$, define keyed $S$-box $S^K$ as:

$$S^K(x) = S(K \oplus x), \ x \in \{0, 1\}^m.$$ 

- **Claim**: $\text{DDT}_S = \text{DDT}_{S^K}$. 

Table: $S$-box $S_{10}$ and its DDT
DDT of Keyed $S$-box

- For $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$ and any fixed key $K \in \{0, 1\}^m$, define keyed $S$-box $S^K$ as:
  \[
  S^K(x) = S(K \oplus x), \ x \in \{0, 1\}^m.
  \]

- **Claim:** $\text{DDT}_S = \text{DDT}_{S^K}$.
- For our previous $S : \{0, 1\}^2 \rightarrow \{0, 1\}^2$ and a fixed $K = 10 \in \{0, 1\}^2$, consider $S^{10}$
**DDT of Keyed S-box**

- For $S : \{0, 1\}^m \to \{0, 1\}^n$ and any fixed key $K \in \{0, 1\}^m$, define keyed S-box $S^K$ as:

  $$S^K(x) = S(K \oplus x), \; x \in \{0, 1\}^m.$$ 

- **Claim:** $\text{DDT}_S = \text{DDT}_{S^K}$.
- For our previous $S : \{0, 1\}^2 \to \{0, 1\}^2$ and a fixed $K = 10 \in \{0, 1\}^2$, consider $S^{10}$

<table>
<thead>
<tr>
<th>$S^{10}$ : ${0, 1}^2 \to {0, 1}^2$</th>
<th>$x' \backslash y'$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S^{10}(00) = S(10) = 11$</td>
<td>00</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$S^{10}(01) = S(11) = 10$</td>
<td>01</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$S^{10}(10) = S(00) = 00$</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$S^{10}(11) = S(01) = 00$</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Table:** S box $S^{10}$ and its $\text{DDT}_{S^{10}}$

- Clearly, $\text{DDT}_S = \text{DDT}_{S^{10}}$
A Conditional Probability Distribution
A Conditional Probability Distribution

• For a random $K \in 0, 1^2$, consider $S^K$
A Conditional Probability Distribution

- For a random $K \in \{0,1\}^2$, consider $S^K$

<table>
<thead>
<tr>
<th>$S^K: {0,1}^2 \rightarrow {0,1}^2$</th>
<th>$x'\backslash y'$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S^K(00) = S(K \oplus 00)$</td>
<td>00</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$S^K(01) = S(K \oplus 01)$</td>
<td>01</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$S^K(10) = S(K \oplus 10)$</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$S^K(11) = S(K \oplus 11)$</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table: $S$ box $S^K$ and its $DDT_{S^K}$
A Conditional Probability Distribution

• For a random $K \in \{0, 1\}^2$, consider $S^K$

<table>
<thead>
<tr>
<th>$S^K: {0, 1}^2 \to {0, 1}^2$</th>
<th>$x' \backslash y'$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S^K(00) = S(K \oplus 00)$</td>
<td>00</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$S^K(01) = S(K \oplus 01)$</td>
<td>01</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$S^K(10) = S(K \oplus 10)$</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$S^K(11) = S(K \oplus 11)$</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table: $S$ box $S^K$ and its $DDT_{S^K}$

• Suppose $(x, x^*) \in \Delta[10]$. Then, for an unknown $K \in \{0, 1\}^2$,  
  $\mathbb{P}[S^K(x) \oplus S^K(x^*) = 01]$
A Conditional Probability Distribution

- For a random $K \in \{0, 1\}^2$, consider $S^K$

<table>
<thead>
<tr>
<th>$S^K$</th>
<th>${0, 1}^2 \rightarrow {0, 1}^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S^K(00)$</td>
<td>$S(K \oplus 00)$</td>
</tr>
<tr>
<td>$S^K(01)$</td>
<td>$S(K \oplus 01)$</td>
</tr>
<tr>
<td>$S^K(10)$</td>
<td>$S(K \oplus 10)$</td>
</tr>
<tr>
<td>$S^K(11)$</td>
<td>$S(K \oplus 11)$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$x' \backslash y'$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Table:** S box $S^K$ and its $DDT_{S^K}$

- Suppose $(x, x^*) \in \Delta[10]$. Then, for an unknown $K \in \{0, 1\}^2$,  
  - $\Pr[S^K(x) \oplus S^K(x^*) = 01] = 0$
A Conditional Probability Distribution

• For a random \( K \in \{0,1\}^2 \), consider \( S^K \)

\[
S^K : \{0,1\}^2 \rightarrow \{0,1\}^2
\]

\[
\begin{align*}
S^K(00) &= S(K \oplus 00) \\
S^K(01) &= S(K \oplus 01) \\
S^K(10) &= S(K \oplus 10) \\
S^K(11) &= S(K \oplus 11)
\end{align*}
\]

<table>
<thead>
<tr>
<th>( x' \backslash y' )</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table: S box \( S^K \) and its \( DDT_{S^K} \)

• Suppose \((x, x^*) \in \Delta[10]\). Then, for an unknown \( K \in \{0,1\}^2 \),
  • \( P[S^K(x) \oplus S^K(x^*) = 01] = 0 \)
  • \( P[S^K(x) \oplus S^K(x^*) = 10] \)
A Conditional Probability Distribution

- For a random $K \in \{0, 1\}^2$, consider $S^K$

<table>
<thead>
<tr>
<th>$S^K : {0, 1}^2 \rightarrow {0, 1}^2$</th>
<th>$x'\backslash y'$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S^K(00) = S(K \oplus 00)$</td>
<td>00</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$S^K(01) = S(K \oplus 01)$</td>
<td>01</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$S^K(10) = S(K \oplus 10)$</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$S^K(11) = S(K \oplus 11)$</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table: $S$ box $S^K$ and its $DDT_{S^K}$

- Suppose $(x, x^*) \in \Delta[10]$. Then, for an unknown $K \in \{0, 1\}^2$,
  - $P[S^K(x) \oplus S^K(x^*) = 01] = 0$
  - $P[S^K(x) \oplus S^K(x^*) = 10] = \frac{2}{2^2}$
A Conditional Probability Distribution

• For a random \( K \in \{0, 1\}^2 \), consider \( S^K \)

\[
\begin{array}{c|cc}
S^K : \{0, 1\}^2 & \rightarrow & \{0, 1\}^2 \\
\hline
S^K(00) = S(K \oplus 00) & \quad & \quad \\
S^K(01) = S(K \oplus 01) & \quad & \quad \\
S^K(10) = S(K \oplus 10) & \quad & \quad \\
S^K(11) = S(K \oplus 11) & \quad & \quad \\
\end{array}
\]

\[
\begin{array}{c|cccc}
& 00 & 01 & 10 & 11 \\
\hline
00 & 4 & 0 & 0 & 0 \\
01 & 2 & 2 & 0 & 0 \\
10 & 0 & 0 & 2 & 2 \\
11 & 0 & 0 & 2 & 2 \\
\end{array}
\]

Table: \( S \) box \( S^K \) and its \( DDT_{S^K} \)

• Suppose \( (x, x^*) \in \Delta[10] \). Then, for an unknown \( K \in \{0, 1\}^2 \),
  • \( \mathbb{P}[S^K(x) \oplus S^K(x^*) = 01] = 0 \)
  • \( \mathbb{P}[S^K(x) \oplus S^K(x^*) = 10] = \frac{2}{2^2} \)

• In general, for any \( x' \in \{0, 1\}^m, y' \in \{0, 1\}^n \)
A Conditional Probability Distribution

• For a random $K \in \{0, 1\}^2$, consider $S^K$

$$
\begin{array}{|c|c|}
\hline
S^K &: \{0, 1\}^2 \rightarrow \{0, 1\}^2 \\
\hline
S^K(00) &= S(K \oplus 00) \\
S^K(01) &= S(K \oplus 01) \\
S^K(10) &= S(K \oplus 10) \\
S^K(11) &= S(K \oplus 11) \\
\hline
\end{array}
$$

<table>
<thead>
<tr>
<th>$x' \backslash y'$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>01</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table: $S$ box $S^K$ and its $DDT_{S^K}$

• Suppose $(x, x^*) \in \Delta[10]$. Then, for an unknown $K \in \{0, 1\}^2$

• $\mathbb{P}[S^K(x) \oplus S^K(x^*) = 01] = 0$
• $\mathbb{P}[S^K(x) \oplus S^K(x^*) = 10] = \frac{2}{2^2}$

• In general, for any $x' \in \{0, 1\}^m$, $y' \in \{0, 1\}^n$

\[
\mathbb{P}\left[ S^K(x) \oplus S^K(x^*) = y' \mid (x, x^*) \in \Delta[x'] \right] = \frac{DDT[x', y']}{{2^m}}
\]

, where the probability is computed over distribution of $K$. 
A Parallel Combination of $S$-boxes

Consider the following two $S$-boxes:

$S_1$: \{
0, 1
\} \rightarrow \{
0, 1
\}

\begin{align*}
00 & \rightarrow 00 \\
01 & \rightarrow 00 \\
10 & \rightarrow 11 \\
11 & \rightarrow 10
\end{align*}

$S_2$: \{
0, 1
\} \rightarrow \{
0, 1
\}

\begin{align*}
00 & \rightarrow 10 \\
01 & \rightarrow 01 \\
10 & \rightarrow 11 \\
11 & \rightarrow 11
\end{align*}

For random keys $K_1, K_2 \in \{0, 1\}^2$ consider:

$S_{K_1}^1$: \{
0, 1
\} \rightarrow \{
0, 1
\}

\begin{align*}
S_{K_1}^1(00) &= S(K_1 \oplus 00) \\
S_{K_1}^1(01) &= S(K_1 \oplus 01) \\
S_{K_1}^1(10) &= S(K_1 \oplus 10) \\
S_{K_1}^1(11) &= S(K_1 \oplus 11)
\end{align*}

$S_{K_2}^2$: \{
0, 1
\} \rightarrow \{
0, 1
\}

\begin{align*}
S_{K_2}^2(00) &= S(K_2 \oplus 00) \\
S_{K_2}^2(01) &= S(K_2 \oplus 01) \\
S_{K_2}^2(10) &= S(K_2 \oplus 10) \\
S_{K_2}^2(11) &= S(K_2 \oplus 11)
\end{align*}
A Parallel Combination of $S$-boxes

- Consider the following two $S$-boxes:

<table>
<thead>
<tr>
<th>$S_1$ : ${0, 1}^2 \rightarrow {0, 1}^2$</th>
<th>$S_2$ : ${0, 1}^2 \rightarrow {0, 1}^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 $\rightarrow$ 00</td>
<td>00 $\rightarrow$ 10</td>
</tr>
<tr>
<td>01 $\rightarrow$ 00</td>
<td>01 $\rightarrow$ 01</td>
</tr>
<tr>
<td>10 $\rightarrow$ 11</td>
<td>10 $\rightarrow$ 11</td>
</tr>
<tr>
<td>11 $\rightarrow$ 10</td>
<td>11 $\rightarrow$ 11</td>
</tr>
</tbody>
</table>
A Parallel Combination of $S$-boxes

- Consider the following two $S$-boxes:

<table>
<thead>
<tr>
<th>$S_1$ : ${0, 1}^2 \rightarrow {0, 1}^2$</th>
<th>$S_2$ : ${0, 1}^2 \rightarrow {0, 1}^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 → 00</td>
<td>00 → 10</td>
</tr>
<tr>
<td>01 → 00</td>
<td>01 → 01</td>
</tr>
<tr>
<td>10 → 11</td>
<td>10 → 11</td>
</tr>
<tr>
<td>11 → 10</td>
<td>11 → 11</td>
</tr>
</tbody>
</table>

- For random keys $K_1, K_2 \in \{0, 1\}^2$ consider:

<table>
<thead>
<tr>
<th>$S_{K_1}^1$ : ${0, 1}^2 \rightarrow {0, 1}^2$</th>
<th>$S_{K_2}^2$ : ${0, 1}^2 \rightarrow {0, 1}^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_{K_1}^1(00) = S(K_1 \oplus 00)$</td>
<td>$S_{K_2}^2(00) = S(K_2 \oplus 00)$</td>
</tr>
<tr>
<td>$S_{K_1}^1(01) = S(K_1 \oplus 01)$</td>
<td>$S_{K_2}^2(01) = S(K_2 \oplus 01)$</td>
</tr>
<tr>
<td>$S_{K_1}^1(10) = S(K_1 \oplus 10)$</td>
<td>$S_{K_2}^2(10) = S(K_2 \oplus 10)$</td>
</tr>
<tr>
<td>$S_{K_1}^1(11) = S(K_1 \oplus 11)$</td>
<td>$S_{K_2}^2(11) = S(K_2 \oplus 11)$</td>
</tr>
</tbody>
</table>
A Parallel Combination of S-boxes

Define an S-box $S$: 

$$S : \{0, 1\}^4 \rightarrow \{0, 1\}^4$$

as follows: for $x \in \{0, 1\}^4$, write $x = x_L || x_R$ with $x_L, x_R \in \{0, 1\}^2$ and define $S(x) = S(x_L || x_R) = S_1(x_L) || S_2(x_R)$.

Then, for a random key $K \in \{0, 1\}^4$, the keyed $S_K$ works as follows:

$$S_K(x) = S(K \oplus x) = S(K_L \oplus x_L || K_R \oplus x_R) = S_1(K_L \oplus x_L) || S_2(K_R \oplus x_R)$$
A Parallel Combination of S-boxes

• Define an S-box $S : \{0, 1\}^4 \rightarrow \{0, 1\}^4$ as follows: for $x \in \{0, 1\}^4$, write $x = x_L || x_R$ with $x_L, x_R \in \{0, 1\}^2$ and define
A Parallel Combination of S-boxes

- Define an S-box $S : \{0, 1\}^4 \rightarrow \{0, 1\}^4$ as follows: for $x \in \{0, 1\}^4$, write $x = x_L || x_R$ with $x_L, x_R \in \{0, 1\}^2$ and define

$$S(x) = S(x_L || x_R) = S_1(x_L) || S_2(x_R)$$
A Parallel Combination of $S$-boxes

- Define an $S$-box $S : \{0, 1\}^4 \rightarrow \{0, 1\}^4$ as follows: for $x \in \{0, 1\}^4$, write $x = x_L \| x_R$ with $x_L, x_R \in \{0, 1\}^2$ and define

$$S(x) = S(x_L \| x_R) = S_1(x_L) \| S_2(x_R)$$

- Then, for a random key $K \in \{0, 1\}^4$, the keyed $S^K$ works as follows:
A Parallel Combination of $S$-boxes

- Define an $S$-box $S : \{0, 1\}^4 \rightarrow \{0, 1\}^4$ as follows: for $x \in \{0, 1\}^4$, write $x = x_L \parallel x_R$ with $x_L, x_R \in \{0, 1\}^2$ and define

$$S(x) = S(x_L \parallel x_R) = S_1(x_L) \parallel S_2(x_R)$$

- Then, for a random key $K \in \{0, 1\}^4$, the keyed $S^K$ works as follows:

$$S^K(x) = S(K \oplus x) = S(K_L \oplus x_L \parallel K_R \oplus x_R) = S_1(K_L \oplus x_L) \parallel S_2(K_R \oplus x_R) = S_1^K(x_L) \parallel S_2^K(x_R)$$
A Parallel Combination of $S$-boxes

Claim:
The DDT $S_K$ is a $2^4 \times 2^4$ matrix and its entries are given by:

For $x', y' \in \{0, 1\}^4$,

$$\text{DDT}_{S_K}[x', y'] = \text{DDT}_{S_{K_1}}[x'_L, y'_L] \times \text{DDT}_{S_{K_2}}[x'_R, y'_R]$$

Consequently, for any $x' \in \{0, 1\}^4$, $y' \in \{0, 1\}^4$,

$$P[S_K(x) \oplus S_K(x^*)] = \text{DDT}_{S_K}[x', y']$$

$$= \text{DDT}_{S_{K_1}}[x'_L, y'_L] \times \text{DDT}_{S_{K_2}}[x'_R, y'_R]$$

$$= \text{DDT}_{S_{K_1}}[x'_L, y'_L] \times \text{DDT}_{S_{K_2}}[x'_R, y'_R]$$
A Parallel Combination of $S$-boxes

- **Claim:** The $\text{DDT}_{SK}$ is a $2^4 \times 2^4$ matrix and its entries are given by:
A Parallel Combination of S-boxes

- **Claim:** The $\text{DDT}_{S^K}$ is a $2^4 \times 2^4$ matrix and its entries are given by: For $x', y' \in \{0, 1\}^4$,

$$\text{DDT}_{S^K}[x', y'] = \text{DDT}_{S^K_{1L}}[x'_L, y'_L] \times \text{DDT}_{S^K_{2R}}[x'_R, y'_R]$$
A Parallel Combination of $S$-boxes

- **Claim:** The $DDT_{S^K}$ is a $2^4 \times 2^4$ matrix and its entries are given by: For $x', y' \in \{0, 1\}^4$,

$$DDT_{S^K}[x', y'] = DDT_{S^K_L}[x'_L, y'_L] \times DDT_{S^K_R}[x'_R, y'_R]$$

- Consequently, for any $x' \in \{0, 1\}^4$, $y' \in \{0, 1\}^4$

$$P[S^K(x) \oplus S^K(x^*) = y' \mid (x, x^*) \in \Delta[x']] = DDT_{S^K}[x', y']$$

$$= \frac{DDT_{S^K_L}[x'_L, y'_L] \times DDT_{S^K_R}[x'_R, y'_R]}{2^4}$$

$$= \frac{DDT_{S^K_L}[x'_L, y'_L]}{2^2} \times \frac{DDT_{S^K_R}[x'_R, y'_R]}{2^2}$$
A Iterative Combination of $S$-boxes

Consider the previously defined $S$-boxes $S_1, S_2$.

For random keys $K_1, K_2 \in \{0, 1\}^2$, define $S$-box $S(K_2, K_1)$:

For $x \in \{0, 1\}^2$, $S(K_2, K_1)(x) = S_{K_2}(S_{K_1}(x))$.

For $x', y', z' \in \{0, 1\}^2$, consider $\text{DDT} S_{K_1}[x', y']$ and $\text{DDT} S_{K_2}[y', z']$.

For any $x, x^* \in \Delta[x']$, compute $P[S_{K_1}(x) \oplus S_{K_1}(x^*) = y' \land S(K_2, K_1)(x) \oplus S(K_2, K_1)(x^*) = z']$.

If $K_1$ and $K_2$ are independent, then the above is $P[S_{K_1}(x) \oplus S_{K_1}(x^*) = y'] \times P[S(K_2, K_1)(x) \oplus S(K_2, K_1)(x^*) = z']$.
A Iterative Combination of $S$-boxes

- Consider the previously defined $S$-boxes $S_1, S_2$. 

For random keys $K_1, K_2 \in \{0, 1\}^2$, define $S$-box $S(K_2, K_1)$:

For $x \in \{0, 1\}^2$, $S(K_2, K_1)(x) = S_{K_2}(S_{K_1}(x))$.

For $x', y', z' \in \{0, 1\}^2$, consider DDT $S_{K_1}[-x', y']$, and $S_{K_2}[-y', z']$.

For any $x, x' \in \Delta[-x']$, compute $P[S_{K_1}(x) \oplus S_{K_1}(x') = y' \wedge S(K_2, K_1)(x) \oplus S(K_2, K_1)(x') = z']$.

If $K_1$ and $K_2$ are independent, then the above is $P[S_{K_1}(x) \oplus S_{K_1}(x') = y'] \times P[S(K_2, K_1)(x) \oplus S(K_2, K_1)(x') = z']$. 
A Iterative Combination of $S$-boxes

- Consider the previously defined $S$-boxes $S_1, S_2$.
- For random keys $K_1, K_2 \in \{0, 1\}^2$, define $S$-box $S^{(K_2,K_1)} : \{0, 1\}^2 \rightarrow \{0, 1\}^2$ as follows:

  \[
  S^{(K_2,K_1)}(x) = S^{K_2}(S^{K_1}(x)).
  \]

- If $K_1$ and $K_2$ are independent, then the above is

  \[
  P[S^{K_1}(x) \oplus S^{K_1}(x^*) = y'] \times P[S^{(K_2,K_1)}(x) \oplus S^{(K_2,K_1)}(x^*) = z']
  \]
A Iterative Combination of $S$-boxes

- Consider the previously defined $S$-boxes $S_1, S_2$.
- For random keys $K_1, K_2 \in \{0, 1\}^2$, define $S$-box $S^{(K_2,K_1)} : \{0, 1\}^2 \rightarrow \{0, 1\}^2$ as follows: For $x \in \{0, 1\}^2$,
  \[ S^{(K_2,K_1)}(x) = S^{K_2}(S^{K_1}(x)). \]
A Iterative Combination of $S$-boxes

- Consider the previously defined $S$-boxes $S_1, S_2$.
- For random keys $K_1, K_2 \in \{0, 1\}^2$, define $S$-box $S^{(K_2, K_1)} : \{0, 1\}^2 \to \{0, 1\}^2$ as follows: For $x \in \{0, 1\}^2$,
  \[ S^{(K_2, K_1)}(x) = S^{K_2}(S^{K_1}(x)). \]

- For $x', y', z' \in \{0, 1\}^2$, consider $\text{DDT}_{S^{K_1}}[x', y']$, and $\text{DDT}_{S^{K_2}}[y', z']$
A Iterative Combination of S-boxes

- Consider the previously defined S-boxes $S_1, S_2$.
- For random keys $K_1, K_2 \in \{0, 1\}^2$, define S-box $S^{(K_2, K_1)} : \{0, 1\}^2 \rightarrow \{0, 1\}^2$ as follows: For $x \in \{0, 1\}^2$,
  \[
  S^{(K_2, K_1)}(x) = S^{K_2}(S^{K_1}(x)).
  \]

- For $x', y', z' \in \{0, 1\}^2$, consider $\text{DDT}_{S^{K_1}}[x', y']$, and $\text{DDT}_{S^{K_2}}[y', z']$
- For any $x, x^* \in \Delta[x']$, compute
  \[
  \mathbb{P}[S^{K_1}(x) \oplus S^{K_1}(x^*) = y' \land S^{(K_2, K_1)}(x) \oplus S^{(K_2, K_1)}(x^*) = z']
  \]
A Iterative Combination of $S$-boxes

- Consider the previously defined $S$-boxes $S_1, S_2$.

- For random keys $K_1, K_2 \in \{0, 1\}^2$, define $S$-box $S^{(K_2,K_1)} : \{0, 1\}^2 \rightarrow \{0, 1\}^2$ as follows: For $x \in \{0, 1\}^2$,
  \[ S^{(K_2,K_1)}(x) = S^{K_2}(S^{K_1}(x)). \]

- For $x', y', z' \in \{0, 1\}^2$, consider $\text{DDT}_{S^{K_1}}[x', y']$, and $\text{DDT}_{S^{K_2}}[y', z']$

- For any $x, x^* \in \Delta[x']$, compute
  \[ \mathbb{P}[S^{K_1}(x) \oplus S^{K_1}(x^*) = y' \land S^{(K_2,K_1)}(x) \oplus S^{(K_2,K_1)}(x^*) = z'] \]

- If $K_1$ and $K_2$ are independent, then the above is $=$
  \[ \mathbb{P}[S^{K_1}(x) \oplus S^{K_1}(x^*) = y'] \times \mathbb{P}[S^{(K_2,K_1)}(x) \oplus S^{(K_2,K_1)}(x^*) = z'] \]
Characteristics and Differentials

\[ (K_2, K_1) [x', y', z'] \] is called the characteristic of \( S (K_2, K_1) \).

\[ P[ Char S (K_2, K_1) [x', y', z'] ] \] denotes the probability with which \( Char S (K_2, K_1) [x', y', z'] \) holds true.

We now define Differentials \( Diff \) of \( S (K_2, K_1) \):

For \( x', z' \), the probability that causes the differential \( Diff S (K_2, K_1) [x', z'] \) is given by

\[ P[ Diff S (K_2, K_1) [x', z'] ] = \sum_{y' \in \{0, 1\}^2} P[ Char S (K_2, K_1) [x', y', z'] ] \]

Finally, our discussion so far applies to

- Parallel composition of \( r (r > 2) \) many \( S \)-boxes
- Sequential composition of \( r (r > 2) \) many \( S \)-boxes
Characteristics and Differentials

- $\text{Char}_{S(K_2,K_1)}[x',y',z']$ is called the characteristic of $S(K_2,K_1)$.

- We now define Differentials $\text{Diff}$ of $S(K_2,K_1)$.

- For $x',z'$, the probability that causes the differential $\text{Diff}_{S(K_2,K_1)}[x',z']$ is given by $P[\text{Diff}_{S(K_2,K_1)}[x',z']] = \sum_{y' \in \{0,1\}^2} P[\text{Char}_{S(K_2,K_1)}[x',y',z']]$.

- Finally, our discussion so far applies to parallel composition of $r (r > 2)$ many $S$-boxes and sequential composition of $r (r > 2)$ many $S$-boxes.
Characteristics and Differentials

• $\text{Char}_{S(K_2,K_1)}[x', y', z']$ is called the characteristic of $S(K_2,K_1)$.

• $\mathbb{P}[\text{Char}_{S(K_2,K_1)}[x', y', z']]$ denotes the probability with which the $\text{Char}_{S(K_2,K_1)}[x', y', z']$ holds true.
Characteristics and Differentials

- \( \text{Char}_{S(K_2,K_1)}[x', y', z'] \) is called the characteristic of \( S(K_2,K_1) \).
- \( \mathbb{P}[\text{Char}_{S(K_2,K_1)}[x', y', z']] \) denotes the probability with which the \( \text{Char}_{S(K_2,K_1)}[x', y', z'] \) holds true.
- We now define Differentials Diff of \( S(K_2,K_1) \)
Characteristics and Differentials

- \( \text{Char}_{S(K_2,K_1)}[x',y',z'] \) is called the characteristic of \( S(K_2,K_1) \).
- \( \mathbb{P}[\text{Char}_{S(K_2,K_1)}[x',y',z']] \) denotes the probability with which the \( \text{Char}_{S(K_2,K_1)}[x',y',z'] \) holds true.
- We now define Differentials \( \text{Diff} \) of \( S(K_2,K_1) \).
- For \( x',z' \), the probability that causes the differential \( \text{Diff}_{S(K_2,K_1)}[x',z'] \) is given by

\[
\mathbb{P}[\text{Diff}_{S(K_2,K_1)}[x',z']] = \sum_{y' \in \{0,1\}^2} \mathbb{P}[\text{Char}_{S(K_2,K_1)}[x',y',z']]
\]
Characteristics and Differentials

- $\text{Char}_{S(K_2,K_1)}[x', y', z']$ is called the characteristic of $S(K_2,K_1)$.
- $\mathbb{P}[\text{Char}_{S(K_2,K_1)}[x', y', z']]$ denotes the probability with which the $\text{Char}_{S(K_2,K_1)}[x', y', z']$ holds true.
- We now define Differentials $\text{Diff}$ of $S(K_2,K_1)$
- For $x', z'$, the probability that causes the differential $\text{Diff}_{S(K_2,K_1)}[x', z']$ is given by

$$
\mathbb{P}[\text{Diff}_{S(K_2,K_1)}[x', z']] = \sum_{y' \in \{0,1\}^2} \mathbb{P}[\text{Char}_{S(K_2,K_1)}[x', y', z']]
$$

- Finally, our discussion so far applies to
  - Parallel composition of $r(>2)$ many $S$-boxes
Characteristics and Differentials

- $\text{Char}_{S(K_2,K_1)}[x', y', z']$ is called the characteristic of $S(K_2,K_1)$.
- $\mathbb{P}[\text{Char}_{S(K_2,K_1)}[x', y', z']]$ denotes the probability with which the $\text{Char}_{S(K_2,K_1)}[x', y', z']$ holds true.
- We now define Differentials $\text{Diff}$ of $S(K_2,K_1)$.
- For $x', z'$, the probability that causes the differential $\text{Diff}_{S(K_2,K_1)}[x', z']$ is given by
  \[ \mathbb{P}[\text{Diff}_{S(K_2,K_1)}[x', z']] = \sum_{y' \in \{0,1\}^2} \mathbb{P}[\text{Char}_{S(K_2,K_1)}[x', y', z']] \]

- Finally, our discussion so far applies to
  - Parallel composition of $r(>2)$ many $S$-boxes
  - Sequential composition of $r(>2)$ many $S$-boxes
The $F$-functions: Let us add linear components to $S$-boxes

- Consider an (affine) expansion function $E$: \[ \{0, 1\}^{32} \rightarrow \{0, 1\}^{48} \]
- Consider a permutation $P$: \[ \{1, 2, ..., 32\} \rightarrow \{1, 2, ..., 32\} \]
- Consider 8 many $S$-boxes $S_i$: \[ \{0, 1\}^6 \rightarrow \{0, 1\}^4 \], $1 \leq i \leq 8$
- Define a function $F$: \[ \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32} \]
  - Input: $x \in \{0, 1\}^{32}$, $K \in \{0, 1\}^{48}$
  - Compute $B = E(x) \oplus K$
  - Write $B = B_1 || B_2 || B_3 || B_4 || B_5 || B_6 || B_7 || B_8$, $B_i \in \{0, 1\}^6$
  - Compute $C_i = S_i(B_i)$
  - Write $D = C_1 || C_2 || C_3 || C_4 || C_5 || C_6 || C_7 || C_8$
  - Write $D = d_1 d_2 \ldots d_{32}$, $d_i \in \{0, 1\}$
  - Compute $y = d_1 P(1) d_2 P(2) \ldots d_{32} P(32)$
- Output: $F(x, K) = y$. 
The \( F \)-functions: Let us add linear components to \( S \)-boxes

- The \( F \)-function of DES
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4$, $1 \leq i \leq 8$
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function
  $$E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4$, $1 \leq i \leq 8$
- Define a function $F : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$ as follows
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4$, $1 \leq i \leq 8$
- Define a function $F : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$ as follows
  - **Input:** $x \in \{0, 1\}^{32}$, $K \in \{0, 1\}^{48}$
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4$, $1 \leq i \leq 8$
- Define a function $F : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$ as follows
  - **Input:** $x \in \{0, 1\}^{32}$, $K \in \{0, 1\}^{48}$
  - Compute $B = E(x) \oplus K$
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \to \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \to \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^6 \to \{0, 1\}^4$, $1 \leq i \leq 8$
- Define a function $F : \{0, 1\}^{32} \times \{0, 1\}^{48} \to \{0, 1\}^{32}$ as follows
  - **Input:** $x \in \{0, 1\}^{32}$, $K \in \{0, 1\}^{48}$
  - Compute $B = E(x) \oplus K$
  - Write $B = B_1\|B_2\|B_3\|B_4\|B_5\|B_6\|B_7\|B_8$, $B_i \in \{0, 1\}^6$
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4$, $1 \leq i \leq 8$
- Define a function $F : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$ as follows
  - **Input:** $x \in \{0, 1\}^{32}$, $K \in \{0, 1\}^{48}$
  - Compute $B = E(x) \oplus K$
  - Write $B = B_1|B_2|B_3|B_4|B_5|B_6|B_7|B_8$, $B_i \in \{0, 1\}^6$
  - Compute $C_i = S_i(B_i)$
  - Output: $F(x, K) = y$
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^{6} \rightarrow \{0, 1\}^{4}$, $1 \leq i \leq 8$
- Define a function $F : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$ as follows
  - **Input:** $x \in \{0, 1\}^{32}$, $K \in \{0, 1\}^{48}$
  - Compute $B = E(x) \oplus K$
  - Write $B = B_1 || B_2 || B_3 || B_4 || B_5 || B_6 || B_7 || B_8$, $B_i \in \{0, 1\}^{6}$
  - Compute $C_i = S_i(B_i)$
  - Write $D = C_1 || C_2 || C_3 || C_4 || C_5 || C_6 || C_7 || C_8$
  - Output: $F(x, K) = y$. 
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^{6} \rightarrow \{0, 1\}^{4}$, $1 \leq i \leq 8$
- Define a function $F : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$ as follows
  - **Input:** $x \in \{0, 1\}^{32}$, $K \in \{0, 1\}^{48}$
  - Compute $B = E(x) \oplus K$
  - Write $B = B_1||B_2||B_3||B_4||B_5||B_6||B_7||B_8$, $B_i \in \{0, 1\}^{6}$
  - Compute $C_i = S_i(B_i)$
  - Write $D = C_1||C_2||C_3||C_4||C_5||C_6||C_7||C_8$
  - Write $D = d_1d_1\ldots d_{32}$, $d_i \in \{0, 1\}$
  - Output: $F(x, K) = y$. 
The \( F \)-functions: Let us add linear components to \( S \)-boxes

- The \( F \)-function of DES
- Consider an (affine) expansion function 
  \( E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48} \)
- Consider a permutation \( P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\} \)
- Consider 8 many \( S \)-boxes \( S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4 \), \( 1 \leq i \leq 8 \)
- Define a function \( F : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32} \) as follows
  - **Input:** \( x \in \{0, 1\}^{32}, K \in \{0, 1\}^{48} \)
  - Compute \( B = E(x) \oplus K \)
  - Write \( B = B_1||B_2||B_3||B_4||B_5||B_6||B_7||B_8, \ B_i \in \{0, 1\}^6 \)
  - Compute \( C_i = S_i(B_i) \)
  - Write \( D = C_1||C_2||C_3||C_4||C_5||C_6||C_7||C_8 \)
  - Write \( D = d_1d_1\ldots d_{32}, \ d_i \in \{0, 1\} \)
  - Compute \( y = d_{P(1)}d_{P(2)}\ldots d_{P(32)} \)
The $F$-functions: Let us add linear components to $S$-boxes

- The $F$-function of DES
- Consider an (affine) expansion function $E : \{0, 1\}^{32} \rightarrow \{0, 1\}^{48}$
- Consider a permutation $P : \{1, 2, \ldots, 32\} \rightarrow \{1, 2, \ldots, 32\}$
- Consider 8 many $S$-boxes $S_i : \{0, 1\}^6 \rightarrow \{0, 1\}^4$, $1 \leq i \leq 8$
- Define a function $F : \{0, 1\}^{32} \times \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$ as follows
  - **Input:** $x \in \{0, 1\}^{32}$, $K \in \{0, 1\}^{48}$
  - Compute $B = E(x) \oplus K$
  - Write $B = B_1||B_2||B_3||B_4||B_5||B_6||B_7||B_8$, $B_i \in \{0, 1\}^6$
  - Compute $C_i = S_i(B_i)$
  - Write $D = C_1||C_2||C_3||C_4||C_5||C_6||C_7||C_8$
  - Write $D = d_1d_1\ldots d_{32}$, $d_i \in \{0, 1\}$
  - Compute $y = d_{P(1)}d_{P(2)}\ldots d_{P(32)}$
  - **Output:** $F(x, K) = y$. 
The $F$-function of DES
The $F$-function of DES
Computing the probability that $x' \rightarrow y'$ under $F$
Computing the probability that $x' \rightarrow y'$ under $F$

- Goal is to compute the following: For $x', y' \in \{0, 1\}^{32}$,
Computing the probability that $x' \rightarrow y'$ under $F$

- Goal is to compute the following: For $x', y' \in \{0, 1\}^{32}$,

\[
P[F(x) \oplus F(x^*) = y' \mid (x, x^*) \in \Delta[x']] \]

• Finally, the probability can also be computed under $F$-iterations!!
Computing the probability that $x' \rightarrow y'$ under $F$

- Goal is to compute the following: For $x', y' \in \{0, 1\}^{32}$,

$$\Pr[F(x) \oplus F(x^*) = y' \mid (x, x^*) \in \Delta[x']]$$

- The following will help:

Finally, the probability can also be computed under $F$-iterations!!
Computing the probability that $x' \rightarrow y'$ under $F$

- Goal is to compute the following: For $x', y' \in \{0, 1\}^{32}$,

$$\mathbb{P}[F(x) \oplus F(x^*) = y' \mid (x, x^*) \in \Delta[x']]$$

- The following will help:
  - For $x, x^* \in \{0, 1\}^{32}$, $E(x) \oplus E(x^*) = E(x \oplus x^*)$
Computing the probability that $x' \rightarrow y'$ under $F$

- Goal is to compute the following: For $x', y' \in \{0, 1\}^{32}$,

$$P[F(x) \oplus F(x^*) = y' \mid (x, x^*) \in \Delta[x']]$$

- The following will help:
  - For $x, x^* \in \{0, 1\}^{32}$, $E(x) \oplus E(x^*) = E(x \oplus x^*)$
  - For $y, y^* \in \{0, 1\}^{32}$, $P(y) \oplus P(y^*) = P(y \oplus y^*)$
Computing the probability that $x' \rightarrow y'$ under $F$

- Goal is to compute the following: For $x', y' \in \{0, 1\}^{32}$,

$$\mathbb{P}[F(x) \oplus F(x^*) = y' \mid (x, x^*) \in \Delta[x']]$$

- The following will help:
  - For $x, x^* \in \{0, 1\}^{32}$, $E(x) \oplus E(x^*) = E(x \oplus x^*)$
  - For $y, y^* \in \{0, 1\}^{32}$, $P(y) \oplus P(y^*) = P(y \oplus y^*)$

- Therefore,

$$\mathbb{P}[F(x) \oplus F(x^*) = y' \mid (x, x^*) \in \Delta[x']] = \mathbb{P}[S^K(E(x)) \oplus S^K(E(x^*)) = P^{-1}(y') \mid (E(x), E(x^*)) \in \Delta[E(x')]],$$

where

$$S^K(E(x)) = S(K \oplus E(x)) = S_1(B_1) || \cdots || S_8(B_8)$$
Computing the probability that $x' \rightarrow y'$ under $F$

- Goal is to compute the following: For $x', y' \in \{0, 1\}^{32}$,

$$\mathbb{P}[F(x) \oplus F(x^*) = y' \mid (x, x^*) \in \Delta[x']]$$

- The following will help:
  - For $x, x^* \in \{0, 1\}^{32}$, $E(x) \oplus E(x^*) = E(x \oplus x^*)$
  - For $y, y^* \in \{0, 1\}^{32}$, $P(y) \oplus P(y^*) = P(y \oplus y^*)$

- Therefore,

$$\mathbb{P}[F(x) \oplus F(x^*) = y' \mid (x, x^*) \in \Delta[x']] = \mathbb{P}[S^K(E(x)) \oplus S^K(E(x^*)) = P^{-1}(y') \mid (E(x), E(x^*)) \in \Delta[E(x')]]$$

  , where

$$S^K(E(x)) = S(K \oplus E(x)) = S_1(B_1) \| \cdots \| S_8(B_8)$$

- Finally, the probability can also be computed under $F$-iterations !!
Feistel Cipher

• Consider a function $F: \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n$.

• Using $F$, define a function $g: \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n \times \{0, 1\}^n$:

$$g(x, y, z) = (y, F(y, z) \oplus x)$$

• For a positive integer $r$, a tuple $(K_1, \ldots, K_r) \in (\{0, 1\}^m)^r$ define $g(r)(K_1, \ldots, K_r): \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$:

$$g(r)(K_1, \ldots, K_r)(x, y) = g(\cdots g(g(x, y, K_1), K_2), K_r)$$

• Then $g(r)(K_1, \ldots, K_r)$ is called a Feistel cipher with

  • block size $2n$
  • with $r$ rounds and
  • with $r$ sub keys $(K_1, \ldots, K_r)$.
Feistel Cipher

- Consider a function $F : \{0, 1\}^n \times \{0, 1\}^m \to \{0, 1\}^n$. 

- Using $F$, define a function $g : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}^n \times \{0, 1\}^n$:
  
  $$g(x, y, z) = (y, F(y, z) \oplus x)$$

- For a positive integer $r$, a tuple $(K_1, \ldots, K_r) \in (\{0, 1\}^m)^r$ define $g^r(K_1, \ldots, K_r)$:
  
  $$g^r(x, y) = g(\cdots g(g(x, y, K_1), K_2), K_r)$$

- Then $g^r(K_1, \ldots, K_r)$ is called a Feistel cipher with
  - block size $2^n$
  - with $r$ rounds and
  - with $r$ sub keys $(K_1, \ldots, K_r)$.
Feistel Cipher

- Consider a function \( F : \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n \).
- Using \( F \), define a function
  \[
g : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n \times \{0, 1\}^n
  \]
  \[
g(x, y, z) = (y, F(y, z) \oplus x).
  \]
Feistel Cipher

- Consider a function $F : \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n$.
- Using $F$, define a function
  
  \[ g : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n \times \{0, 1\}^n \]
  
  \[ g(x, y, z) = (y, F(y, z) \oplus x). \]

- For a positive integer $r$, a tuple $(K_1, \ldots, K_r) \in (\{0, 1\}^m)^r$ define $g^{(r)}_{(K_1, \ldots, K_r)} : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$

  \[ g^{(r)}_{(K_1, \ldots, K_r)}(x, y) = g \left( \cdots g(g(x, y, K_1), K_2), K_r \right) \]
Feistel Cipher

• Consider a function $F : \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n$.

• Using $F$, define a function
g : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n \times \{0, 1\}^n

\[ g(x, y, z) = (y, F(y, z) \oplus x). \]

• For a positive integer $r$, a tuple $(K_1, \ldots, K_r) \in (\{0, 1\}^m)^r$
define $g_{(K_1, \ldots, K_r)}^{(r)} : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$

\[ g_{(K_1, \ldots, K_r)}^{(r)}(x, y) = g \left( \cdots g \left( g(x, y, K_1), K_2 \right), K_r \right) \]

• Then $g_{(K_1, \ldots, K_r)}^{(r)}$ is called a Feistel cipher with
Feistel Cipher

- Consider a function $F : \{0, 1\}^n \times \{0, 1\}^m \to \{0, 1\}^n$.
- Using $F$, define a function
  
  $g : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^m \to \{0, 1\}^n \times \{0, 1\}^n$

  $g(x, y, z) = (y, F(y, z) \oplus x)$.

- For a positive integer $r$, a tuple $(K_1, \ldots, K_r) \in (\{0, 1\}^m)^r$
  define $g^{(r)}_{(K_1, \ldots, K_r)} : \{0, 1\}^{2n} \to \{0, 1\}^{2n}$

  $g^{(r)}_{(K_1, \ldots, K_r)}(x, y) = g\left( \cdots g(g(x, y, K_1), K_2), K_r \right)$

- Then $g^{(r)}_{(K_1, \ldots, K_r)}$ is called a Feistel cipher with
  - block size $2n$
Feistel Cipher

- Consider a function $F : \{0, 1\}^n \times \{0, 1\}^m \to \{0, 1\}^n$.
- Using $F$, define a function
  
  $g : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^m \to \{0, 1\}^n \times \{0, 1\}^n$

  $g(x, y, z) = (y, F(y, z) \oplus x)$.

- For a positive integer $r$, a tuple $(K_1, \ldots, K_r) \in (\{0, 1\}^m)^r$
  define $g^{(r)}_{(K_1, \ldots, K_r)} : \{0, 1\}^{2n} \to \{0, 1\}^{2n}$

  $g^{(r)}_{(K_1, \ldots, K_r)}(x, y) = g \left( \cdots g \left( g(x, y, K_1), K_2 \right), K_r \right)$

- Then $g^{(r)}_{(K_1, \ldots, K_r)}$ is called a Feistel cipher with
  - block size $2n$
  - with $r$ rounds and
Feistel Cipher

• Consider a function $F : \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n$.

• Using $F$, define a function
  
  $g : \{0, 1\}^n \times \{0, 1\}^n \times \{0, 1\}^m \rightarrow \{0, 1\}^n \times \{0, 1\}^n$

  $g(x, y, z) = (y, F(y, z) \oplus x)$.

• For a positive integer $r$, a tuple $(K_1, \ldots, K_r) \in (\{0, 1\}^m)^r$

  define $g_{(K_1, \ldots, K_r)}^{(r)} : \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$

  $g_{(K_1, \ldots, K_r)}^{(r)}(x, y) = g \left( \cdots g \left( g(x, y, K_1), K_2 \right), K_r \right)$

• Then $g_{(K_1, \ldots, K_r)}^{(r)}$ is called a Feistel cipher with
  
  • block size $2n$
  • with $r$ rounds and
  • with $r$ sub keys $(K_1, \ldots, K_r)$
Feistel Cipher

- A pictorial description!!

- For input $x \in \{0, 1\}^n$, write $x = L_0 || R_0$

- The cipher proceeds through the $r$-rounds as follows:

  - Rounds Left Half Right Half
  - $0 \quad L_0 \quad R_0$
  - $1 \quad L_1 = R_0 \quad R_1 = L_0 \oplus F(R_0, K_1)$
  - $2 \quad L_2 = R_1 \quad R_2 = L_1 \oplus F(R_1, K_2)$
  - $\vdots$
  - $r \quad L_r = R_{r-1} \quad R_r = L_{r-1} \oplus F(R_{r-1}, K_r)$

- Finally, the ciphertext is set to $C = R_r || L_r$.

- $F$ function: The core of a Feistel Cipher.

- Different $F$ function instantiates different Feistel Ciphers.
Feistel Cipher

• A pictorial description !!
• For input $x \in \{0, 1\}^{2n}$, write $x = L_0 || R_0$
Feistel Cipher

- A pictorial description !!
- For input $x \in \{0, 1\}^{2n}$, write $x = L_0 || R_0$
- The cipher proceeds through the $r$-rounds as follows
Feistel Cipher

- A pictorial description !!
- For input $x \in \{0, 1\}^{2n}$, write $x = L_0 || R_0$
- The cipher proceeds through the $r$-rounds as follows

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Left Half</th>
<th>Right Half</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$L_0$</td>
<td>$R_0$</td>
</tr>
<tr>
<td>1</td>
<td>$L_1 = R_0$</td>
<td>$R_1 = L_0 \oplus F(R_0, K_1)$</td>
</tr>
<tr>
<td>2</td>
<td>$L_2 = R_1$</td>
<td>$R_2 = L_1 \oplus F(R_1, K_2)$</td>
</tr>
<tr>
<td>3</td>
<td>$L_3 = R_2$</td>
<td>$R_3 = L_2 \oplus F(R_2, K_3)$</td>
</tr>
<tr>
<td>:</td>
<td>:</td>
<td>:</td>
</tr>
<tr>
<td>$r$</td>
<td>$L_r = R_{r-1}$</td>
<td>$R_r = L_{r-1} \oplus F(R_{r-1}, K_r)$</td>
</tr>
</tbody>
</table>

- $F$ function: The core of a Feistel Cipher
- Different $F$ function instantiates different Feistel Ciphers
Feistel Cipher

- A pictorial description !
- For input $x \in \{0, 1\}^{2n}$, write $x = L_0 || R_0$
- The cipher proceeds through the $r$-rounds as follows

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Left Half</th>
<th>Right Half</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$L_0$</td>
<td>$R_0$</td>
</tr>
<tr>
<td>1</td>
<td>$L_1 = R_0$</td>
<td>$R_1 = L_0 \oplus F(R_0, K_1)$</td>
</tr>
<tr>
<td>2</td>
<td>$L_2 = R_1$</td>
<td>$R_2 = L_1 \oplus F(R_1, K_2)$</td>
</tr>
<tr>
<td>3</td>
<td>$L_3 = R_2$</td>
<td>$R_3 = L_2 \oplus F(R_2, K_3)$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$r$</td>
<td>$L_r = R_{r-1}$</td>
<td>$R_r = L_{r-1} \oplus F(R_{r-1}, K_r)$</td>
</tr>
</tbody>
</table>

- Finally, the ciphertext is set to $C = R_r || L_r$. 
Feistel Cipher

• A pictorial description !!
• For input $x \in \{0, 1\}^{2n}$, write $x = L_0||R_0$
• The cipher proceeds through the $r$-rounds as follows

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Left Half</th>
<th>Right Half</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$L_0$</td>
<td>$R_0$</td>
</tr>
<tr>
<td>1</td>
<td>$L_1 = R_0$</td>
<td>$R_1 = L_0 \oplus F(R_0, K_1)$</td>
</tr>
<tr>
<td>2</td>
<td>$L_2 = R_1$</td>
<td>$R_2 = L_1 \oplus F(R_1, K_2)$</td>
</tr>
<tr>
<td>3</td>
<td>$L_3 = R_2$</td>
<td>$R_3 = L_2 \oplus F(R_2, K_3)$</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>$r$</td>
<td>$L_r = R_{r-1}$</td>
<td>$R_r = L_{r-1} \oplus F(R_{r-1}, K_r)$</td>
</tr>
</tbody>
</table>

• Finally, the ciphertext is set to $C = R_r||L_r$.
• $F$ function: The core of a Feistel Cipher
Feistel Cipher

- A pictorial description !!
- For input $x \in \{0, 1\}^{2n}$, write $x = L_0 || R_0$
- The cipher proceeds through the $r$-rounds as follows

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Left Half</th>
<th>Right Half</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$L_0$</td>
<td>$R_0$</td>
</tr>
<tr>
<td>1</td>
<td>$L_1 = R_0$</td>
<td>$R_1 = L_0 \oplus F(R_0, K_1)$</td>
</tr>
<tr>
<td>2</td>
<td>$L_2 = R_1$</td>
<td>$R_2 = L_1 \oplus F(R_1, K_2)$</td>
</tr>
<tr>
<td>3</td>
<td>$L_3 = R_2$</td>
<td>$R_3 = L_2 \oplus F(R_2, K_3)$</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$r$</td>
<td>$L_r = R_{r-1}$</td>
<td>$R_r = L_{r-1} \oplus F(R_{r-1}, K_r)$</td>
</tr>
</tbody>
</table>

- Finally, the ciphertext is set to $C = R_r || L_r$.
- $F$ function: The core of a Feistel Cipher
- Different $F$ function instantiates different Feistel Ciphers
Computing $\mathbb{P}[x' \rightarrow y']$ for the Fiestel Cipher itself

\[\begin{aligned}
L_0 &= R_0 \\
R_1 &= L_0 \oplus F(R_0, K_1) \\
L_1 &= R_1 \\
R_2 &= L_1 \oplus F(R_1, K_2) \\
L_2 &= R_2 \\
R_3 &= L_2 \oplus F(R_2, K_3) \\
L_3 &= R_3 \\
R_4 &= L_3 \oplus F(R_3, K_4)
\end{aligned}\]
Computing $\mathbb{P}[x' \rightarrow y']$ for the Fiestel Cipher itself

- It proceeds as follows:

<table>
<thead>
<tr>
<th></th>
<th>Input</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_0$</td>
<td>$R_0$</td>
<td>$[0, x_1']$</td>
</tr>
<tr>
<td>$L_1 = R_0$</td>
<td>$R_1 = L_0 \oplus F(R_0, K_1)$</td>
<td>$[x_1', y_1']$</td>
</tr>
<tr>
<td>$L_2 = R_1$</td>
<td>$R_2 = L_1 \oplus F(R_1, K_2)$</td>
<td>$[y_1', x_1' + y_2']$</td>
</tr>
<tr>
<td>$L_3 = R_2$</td>
<td>$R_3 = L_2 \oplus F(R_2, K_3)$</td>
<td>$[x_1' + y_2', y_1' + y_3']$</td>
</tr>
<tr>
<td>$L_4 = R_3$</td>
<td>$R_4 = L_3 \oplus F(R_3, K_4)$</td>
<td>$[y_1' + y_3', x_1' + y_2' + y_4']$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Computing $\mathbb{P}[x' \rightarrow y']$ for the Fiestel Cipher itself

• It proceeds as follows:

<table>
<thead>
<tr>
<th></th>
<th>Input</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_0$</td>
<td>$R_0$</td>
<td>$[0, x'_1]$</td>
</tr>
<tr>
<td>$L_1 = R_0$</td>
<td>$R_1 = L_0 \oplus F(R_0, K_1)$</td>
<td>$[x'_1, y'_1]$</td>
</tr>
<tr>
<td>$L_2 = R_1$</td>
<td>$R_2 = L_1 \oplus F(R_1, K_2)$</td>
<td>$[y'_1, x'_1 + y'_2]$</td>
</tr>
<tr>
<td>$L_3 = R_2$</td>
<td>$R_3 = L_2 \oplus F(R_2, K_3)$</td>
<td>$[x'_1 + y'_2, y'_1 + y'_3]$</td>
</tr>
<tr>
<td>$L_4 = R_3$</td>
<td>$R_4 = L_3 \oplus F(R_3, K_4)$</td>
<td>$[y'_1 + y'_3, x'_1 + y'_2 + y'_4]$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
</tbody>
</table>

• In particular, we are looking at the following probability trail:

$\mathbb{P}[0||x'_1 \rightarrow x'_1||y'_1]; \mathbb{P}[x'_1||y'_1 \rightarrow y'_1||x'_1 + y'_2]; \mathbb{P}[y'_1||x'_1 + y'_2 \rightarrow x'_1 + y'_2||y'_1 + y'_3]; \cdots$
Differential Attack

Suppose one founds a high-probability \((r - 1)\)-round characteristic/differential \([0]|\rightarrow x_1 \rightarrow x_{r - 1}||y_1\rightarrow r - 1\]

Consider Input Difference

\[L_0 R_0 [0, x_1] \ldots \ldots \ldots \]

\[L_r = R_{r - 1} R_{r - 1} = L_{r - 1} \oplus F(R_{r - 1} \oplus K_{r - 1})\]
Differential Attack

- Suppose one finds a high-probability \((r - 1)\)-round characteristic/differential \([0\|x' \rightarrow x'_{r-1}\|y'_{r-1}]\).
Differential Attack

- Suppose one founds a high-probability \((r - 1)\)-round characteristic/differential \([0||x' \rightarrow x'_{r-1}||y'_{r-1}]\)
- Consider

<table>
<thead>
<tr>
<th>Input</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>(L_0)</td>
<td>(R_0)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>(L_{r-1})</td>
<td>(R_{r-1})</td>
</tr>
</tbody>
</table>

\[
L_r = R_{r-1} \quad R_r = L_{r-1} \oplus F(R_{r-1} \oplus K_r)
\]
The round probabilities of characteristics only depend on \( F \)-function:

\[
S_{K}(E(x)) = S(E(x) \oplus K)
\]

In general, let us denote this \( S_{K} \) function for DES-type cipher by \( f \):

\[
\{0, 1\}^{m} \rightarrow \{0, 1\}^{n}
\]

Define \( p_{\text{max}} = \max_{\beta \neq 0} P[f(x) \oplus f(x^*) = \beta | (x, x^*) \in \Delta[\alpha]] \)

**Theorem**

It is assumed that in a DES-like cipher with \( f \):

\[
\{0, 1\}^{m} \rightarrow \{0, 1\}^{n}
\]

the inputs to \( f \) at each round are independent and uniformly random. Then the probability of an \( r \)-round \((r \geq 4)\) differential is \( \leq 2p_{\text{max}}^{2} \).
• The round probabilities of characteristics only depend on $F$-function

In particular, it depends on $S_K$: $\{0,1\}^{48} \rightarrow \{0,1\}^{32}$

$\text{DES-type cipher}$

- Define $p_{\text{max}} = \max_{\beta \neq 0} P[f(x) \oplus f(x^*) = \beta | (x, x^*) \in \Delta[\alpha]]$

Theorem: It is assumed that in a DES-like cipher with $f$: $\{0,1\}^m \rightarrow \{0,1\}^n$ the inputs to $f$ at each round are independent and uniformly random. Then the probability of an $r$-round ($r \geq 4$) differential is $\leq 2p_{\text{max}}^2$. 
Provable Security Flavor Against Differential Attacks

- The round probabilities of characteristics only depends on $F$-function.
- In particular, it depends on $S^K : \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$
  
  \[
  S^K(E(x)) = S(E(x) \oplus K)
  \]
Provable Security Flavor Against Differential Attacks

- The round probabilities of characteristics only depends on $F$-function
- In particular, it depends on $S^K : \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$
  $(S^K(E(x)) = S(E(x) \oplus K))$
- In general, let us denote this ($S^K$ function for DES-type cipher) by $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$
Provable Security Flavor Against Differential Attacks

- The round probabilities of characteristics only depends on $F$-function
- In particular, it depends on $S^K : \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$
  \[ (S^K(E(x))) = S(E(x) \oplus K) \]
- In general, let us denote this ($S^K$ function for DES-type cipher) by $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$
- Define
  \[ p_{\text{max}} = \max_{\beta} \max_{\alpha \neq 0} \mathbb{P}[f(x) \oplus f(x^*) = \beta \mid (x, x^*) \in \Delta[\alpha]] \]
The round probabilities of characteristics only depends on $F$-function

In particular, it depends on $S^K : \{0, 1\}^{48} \rightarrow \{0, 1\}^{32}$

$(S^K(E(x))) = S(E(x) \oplus K))$

In general, let us denote this ($S^K$ function for DES-type cipher) by $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$

Define

$$p_{\text{max}} = \max_\beta \max_\alpha \neq 0 \Pr[f(x) \oplus f(x^*) = \beta \mid (x, x^*) \in \Delta[\alpha]]$$

**Theorem**

*It is assumed that in a DES-like cipher with $f : \{0, 1\}^m \rightarrow \{0, 1\}^n$ the inputs to $f$ at each round are independent and uniformly random. Then the probability of an $r$-round ($r \geq 4$) differential is $\leq 2p_{\text{max}}^2$.***
Truncated Differential

- Cipher presumably secure against differential attack - but vulnerable to truncated differential
- Consider $S: \mathbb{GF}(2^n) \rightarrow \mathbb{GF}(2^n)$ defined by $x \rightarrow x - 1$
- For $n$ odd, $S$ is 2-uniform
- Consider $S_K: \mathbb{GF}(2^n) \rightarrow \mathbb{GF}(2^n)$ defined by $S_K(x) = (x \oplus K) - 1$
- Plug $S_K$ in a Fiestel cipher as an $F$-function.
- Differential attack will fail due to low-probability differentials.
- But, the cipher can be attacked using truncated differentials.
Truncated Differential

- Cipher presumably secure against differential attack - but vulnerable to truncated differential
- Consider $S : GF(2^n) \rightarrow GF(2^n)$ defined by $x \rightarrow x^{-1}$
- For $n$ odd, $S$ is 2-uniform
- Consider $S^K : GF(2^n) \rightarrow GF(2^n)$ defined by $S^K(x) = (x \oplus K)^{-1}$
- Plug $S^K$ in a Fiestel cipher as an $F$-function.
- Differential attach will fail due to low-probability differentials.
- But, the cipher can be attacked using truncated differentials.
Impossible Differential Cryptanalysis

Differential cryptanalysis considers characteristics/differentials with high probabilities.

- Uses them to distinguish the correct unknown key from the wrong keys.

- When a correct key is used to decrypt the last round of many ciphertext pairs, it is expected that the difference predicted by differential appears frequently.

- When a wrong key is used, the difference occurs less frequently.

Impossible Differential:

- A differential that predicts that a certain difference should not occur (with probability zero).

- Hence, if a ciphertext pair decrypted to this pair under some trail key, then certainly this trial key is not the correct key.

- This is a sieving attack which finds the correct key by elimination all the other keys which lead to contradictions.
Impossible Differential Cryptanalysis

- Differential cryptanalysis considers characteristics/differentials with high probabilities

- Impossible Differential: a differential that predicts that certain difference should not occur (with probability zero)

- Hence, if a ciphertext pair decrypted to this pair under some trial key, then certainly this trial key is not the correct key.

- This is a sieving attack which finds the correct key by elimination all the other keys which lead to contradictions.
Impossible Differential Cryptanalysis

- Differential cryptanalysis considers characteristics/differentials with high probabilities.
- Uses them to distinguish the correct unknown key from the wrong keys.
- When a correct key is used to decrypt the last round of many ciphertext pairs, it is expected that the difference predicted by differential appears frequently.
- When a wrong key is used, the difference occurs less frequently.
- Impossible Differential: a differential that predicts that certain difference should not occur (with probability zero).
- Hence, if a ciphertext pair decrypted to this pair under some trial key, then certainly this trial key is not the correct key.
- This is a sieving attack which finds the correct key by eliminating all the other keys which lead to contradictions.
Impossible Differential Cryptanalysis

- Differential cryptanalysis considers characteristics/differentials with high probabilities
- uses them to distinguish the correct unknown key from the wrong keys
- when a correct key is used to decrypt last round of many ciphertext pairs, it is expected that the difference predicted by differential appears frequently
Impossible Differential Cryptanalysis

- Differential cryptanalysis considers characteristics/differentials with high probabilities
- uses them to distinguish the correct unknown key from the wrong keys
- when a correct key is used to decrypt last round of many ciphertext pairs, it is expected that the difference predicted by differential appears frequently
- when a wrong key is used the difference occurs less frequently
Impossible Differential Cryptanalysis

- Differential cryptanalysis considers characteristics/differentials with high probabilities.
- Uses them to distinguish the correct unknown key from the wrong keys.
- When a correct key is used to decrypt last round of many ciphertext pairs, it is expected that the difference predicted by differential appears frequently.
- When a wrong key is used the difference occurs less frequently.
- **Impossible Differential**: a differential that predicts that certain difference should not occur (with probability zero).
Impossible Differential Cryptanalysis

- Differential cryptanalysis considers characteristics/differentials with high probabilities
- uses them to distinguish the correct unknown key from the wrong keys
- when a correct key is used to decrypt last round of many ciphertext pairs, it is expected that the difference predicted by differential appears frequently
- when a wrong key is used the difference occurs less frequently
- **Impossible Differential**: a differential that predicts that certain difference should not occur (with probability zero)
- Hence, if a ciphertext pair decrypted to this pair under some trail key, then certainly this trial key is not the correct key.
Impossible Differential Cryptanalysis

- Differential cryptanalysis considers characteristics/differentials with high probabilities
- uses them to distinguish the correct unknown key from the wrong keys
- when a correct key is used to decrypt last round of many ciphertext pairs, it is expected that the difference predicted by differential appears frequently
- when a wrong key is used the difference occurs less frequently
- **Impossible Differential**: a differential that predicts that certain difference should not occur (with probability zero)
- Hence, if a ciphertext pair decrypted to this pair under some trail key, then certainly this trial key is not the correct key.
- This is a sieving attack which finds the correct key by elimination all the other keys which lead to contradictions.
Skipjack

- Skipjack supports a 64-bit block size and a 80-bit key
- It is an iterated cipher with 32 rounds
- The underlying primitives/algorithms for Skipjack are
  - The transformation $G : \{0, 1\}^{32} \times \{0, 1\}^{16} \rightarrow \{0, 1\}^{16}$ consists of a 4 round Feistel structure whose internal function $F : \{0, 1\}^{8} \rightarrow \{0, 1\}^{8}$ is an $8 \times 8$ S-box.
- **Key Schedule**

<table>
<thead>
<tr>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K \in {0, 1}^{80}$</td>
</tr>
<tr>
<td>Write $K = B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8 B_9 B_{10}$, $B_i \in {0, 1}^8$</td>
</tr>
<tr>
<td>$K_1 = B_1 B_2 B_3 B_4$</td>
</tr>
<tr>
<td>$K_2 = B_5 B_6 B_7 B_8$</td>
</tr>
<tr>
<td>$K_3 = B_9 B_{10} B_{11} B_{12}$</td>
</tr>
<tr>
<td>\vdots</td>
</tr>
<tr>
<td>Output: 32 round keys: $K_i \in {0, 1}^{32}$, $1 \leq i \leq 32$</td>
</tr>
</tbody>
</table>
Skipjack

- The underlying primitives/algorithms for Skipjack are
  - **Rule A**

  **Input:** \( w^k \in \{0, 1\}^{64}, \text{ where } 1 \leq k \leq 32 \)

  Write \( w^k = w^k_1 || w^k_2 || w^k_3 || w^k_4 \)

  Compute \( w^{k+1}_1 \leftarrow G(K^k, w^k_1) \oplus w^k_4 \oplus \text{counter}^k \)

  \( w^{k+1}_2 \leftarrow G(K^k, w^k_1), \ w^{k+1}_3 \leftarrow w^k_2, \ w^{k+1}_4 \leftarrow w^k_3 \)

  **Output:** \( w^{k+1} = w^{k+1}_1 || w^{k+1}_2 || w^{k+1}_3 || w^{k+1}_4 \)

  - **Rule B**

  **Input:** \( w^k \in \{0, 1\}^{64}, \text{ where } 1 \leq k \leq 32 \)

  Write \( w^k = w^k_1 || w^k_2 || w^k_3 || w^k_4 \)

  Compute \( w^{k+1}_1 \leftarrow w^k_4, \ w^{k+1}_2 \leftarrow G(K^k, w^k_1) \)

  \( w^{k+1}_3 \leftarrow w^k_1 \oplus w^k_2 \oplus \text{counter}^k, \ w^{k+1}_4 \leftarrow w^k_3 \)

  **Output:** \( w^{k+1} = w^{k+1}_1 || w^{k+1}_2 || w^{k+1}_3 || w^{k+1}_4 \)

- Skipjack encryption of a plaintext is obtained by applying
  - eight rounds of Rule A; followed by eight rounds of Rule B; followed by another eight rounds of Rule A; followed by another eight rounds of Rule B
### A 24-round Differential with Probability Zero

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Input Difference</th>
<th>Output Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>( \Delta^I_5 = (0, a, 0, 0) )</td>
<td>( \Delta^O_{16} = (c, d, e, 0) )</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>( \Delta^I_{17} = (f, g, 0, h) )</td>
<td>( \Delta^O_{17} = (f, g, 0, h) )</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>( \Delta^O_{28} = (b, 0, 0, 0) )</td>
<td>( \Delta^O_{28} = (b, 0, 0, 0) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Miss-in-the-middle Attack

• Consider a cipher $E$ as a cascade, such that $E = E_1 \circ E_0$ s.t.
  • for $E_0$ there exists a differential $(\alpha \rightarrow \beta)$ with prob. 1 and
  • for $E_1$ there exists a differential $(\gamma \rightarrow \delta)$ with prob. 1 and
  • $\beta \neq \gamma$

This leads to an impossible differential: $(\alpha \rightarrow \delta)$

• Application: Distinguisher
  • Choose pairs of plaintexts $(P_1, P_2)$ such that $P_1 \oplus P_2 = \alpha$.
  • Obtain ciphertexts $(C_1, C_2)$ of $(P_1, P_2)$.
  • Check whether $C_1 \oplus C_2 = \delta$

• Application: Key Recovery
  • Guess the last round subkey
  • If the guessed cause impossible differentials, then they are discarded.
Thank You !!