Aalto University
School of Science

Improbable Differential from Impossible Differential : On the Validity of the Model

Céline Blondeau

Aalto University, Finland

Indocrypt 2013, *Mumbai*

Outline

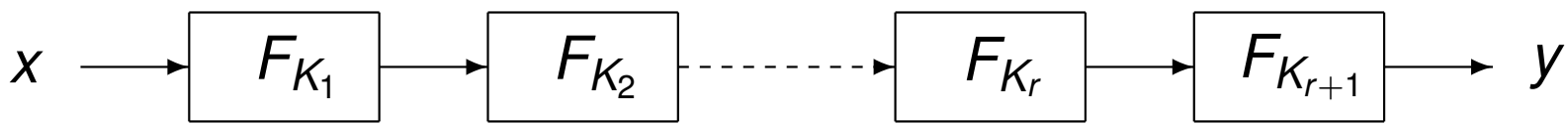
Outline

Block Cipher

Block cipher :

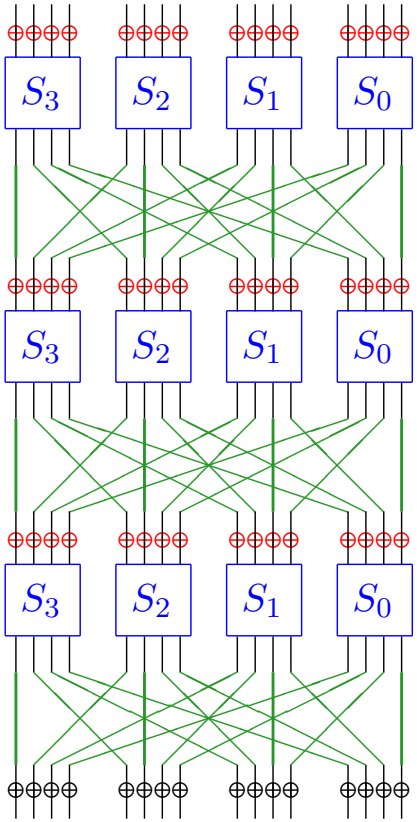
$$\begin{array}{rccc} E_K & : & \mathbb{F}_2^n & \rightarrow & \mathbb{F}_2^n \\ & & x & \mapsto & y \end{array}$$

Iterative block cipher :



Block cipher : SPN Example

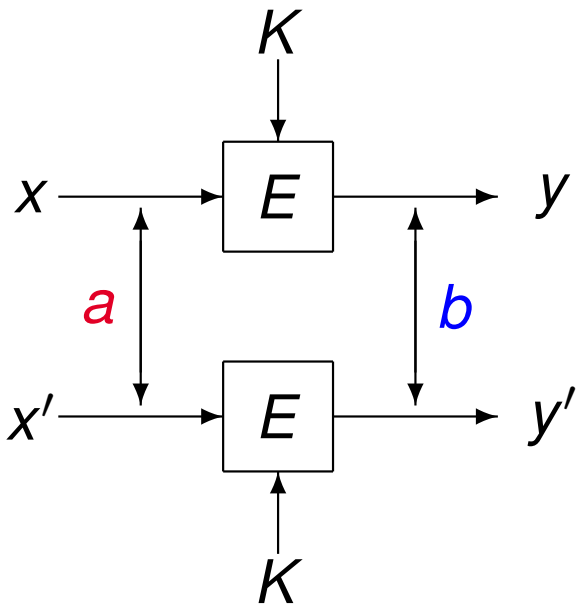
PRESENT [BKL+07]



Round function F :

- Key addition
- Linear layer
- Non-linear layer

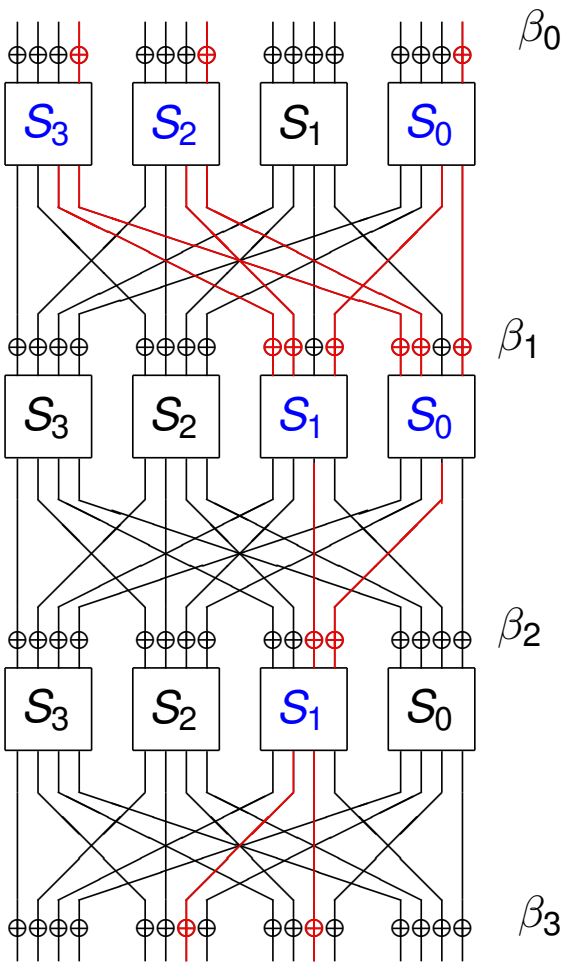
Differential Cryptanalysis [Biham Shamir 90]



Differential : pair of input and output difference (a, b)

Differential probability : $p = P_{\mathbf{x},\mathbf{K}}[\, E_K(X) \oplus E_K(X \oplus a) = b \,]$

Computing Differential Probabilities



Differential trail :

Sequence of all intermediate differences

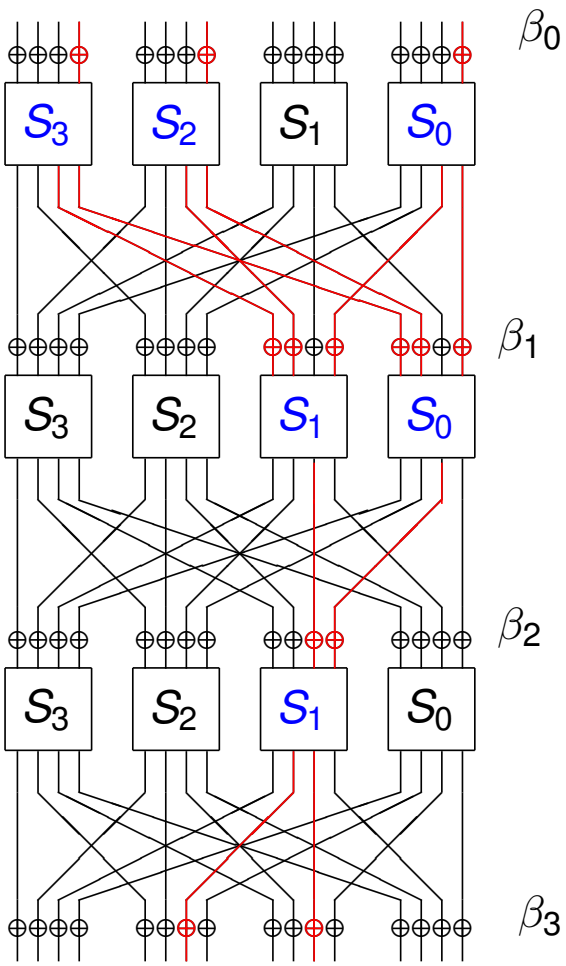
$$(\beta_0, \beta_1, \cdots \beta_r)$$

Probability of a differential trail :

Assuming a Markov cipher and independent round-key, we have

$$P\left[(\beta_0, \beta_1, \cdots \beta_r)\right] = \prod_{i<r} P[\beta_i \rightarrow \beta_{i+1}]$$

Computing Differential Probabilities



Expected differential probability :

Sum of the probability of trails with input difference a and output difference b

$$p = P[\, a \to b \,] = \sum_{\beta} P[(a, \beta_1, \cdots \beta_{r-1}, b)]$$

If p significantly larger than the uniform probability p_U,
we have a distinguisher,
which can often be converted to a key-recovery attack

Truncated Differential [Knudsen 94]

Truncated differential : pair (A, B) where

$A \subset \mathbb{F}_2^n \setminus \{0\}$ is a set of input differences,
$B \subset \mathbb{F}_2^n \setminus \{0\}$ is a set of output differences

Truncated Differential [Knudsen 94]

Truncated differential : pair (A, B) where

$A \subset \mathbb{F}_2^n \setminus \{0\}$ is a set of input differences,
$B \subset \mathbb{F}_2^n \setminus \{0\}$ is a set of output differences

$$\sum_{b \in \mathbb{F}_2^n} P[a \to b] = 1 \text{ and } \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^n} P[a \to b] = 2^n$$

Truncated Differential [Knudsen 94]

Truncated differential : pair (A, B) where

$A \subset \mathbb{F}_2^n \setminus \{0\}$ is a set of input differences,
$B \subset \mathbb{F}_2^n \setminus \{0\}$ is a set of output differences

$$\sum_{b \in \mathbb{F}_2^n} P[a \to b] = 1 \text{ and } \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^n} P[a \to b] = 2^n$$

Expected probability of the truncated differential (A, B) :

$$p = P[A \to B] = \frac{1}{|A|} \sum_{a \in A} \sum_{b \in B} P[a \to b]$$

Probability is averaged over the input differences

Complexity of a Distinguishing Attack

Expected probability : $p = P[A \rightarrow B]$

Uniform probability : $p_U = \frac{|B|}{2^n - 1} \approx \frac{|B|}{2^n}$

Assume p is close to p_U : $p = p_U + \varepsilon$, with $\varepsilon > 0$

Data complexity : Number of plaintexts required to distinguish the cipher E from a random permutation

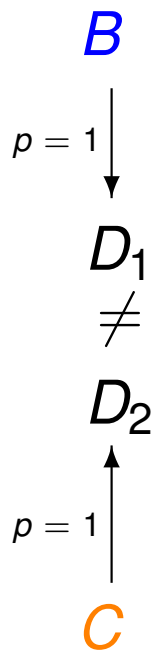
$$N = \gamma \cdot \frac{p_U}{(p_U - p)^2} = \gamma \cdot \frac{p_U}{\varepsilon^2},$$

where γ depends of $|A|$, the false-alarm and non-detection error probabilities [Selçuk 07], [Blondeau et al 09]

Impossible differential [Knudsen 98]

Impossible differential :

Truncated differential (B, C) with probability $p = P[B \to C] = 0$



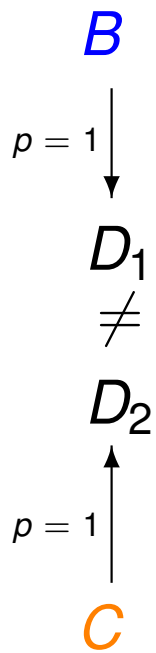
Distinguisher :

Based on a mismatch between two deterministic truncated differentials

Impossible differential [Knudsen 98]

Impossible differential :

Truncated differential (B, C) with probability $p = P[B \to C] = 0$



Distinguisher :

Based on a mismatch between two deterministic truncated differentials

Outline

Improbable Differential Distinguisher

Improbable differential :

Truncated differential (A, C) with $p < p_U$

Assume p close to p_U : $p = p_U + \varepsilon$ with $\varepsilon < 0$

Data complexity : (as in the truncated case)

$$N = \gamma \cdot \frac{p_U}{\varepsilon^2}$$

Example : [Borst et al 97] and [Knudsen et al 99]

Improbable Differential Distinguisher

Improbable differential :

Truncated differential (A, C) with $p < p_U$

Assume p close to p_U : $p = p_U + \varepsilon$ with $\varepsilon < 0$

Data complexity : (as in the truncated case)

$$N = \gamma \cdot \frac{p_U}{\varepsilon^2}$$

Example : [Borst et al 97] and [Knudsen et al 99]

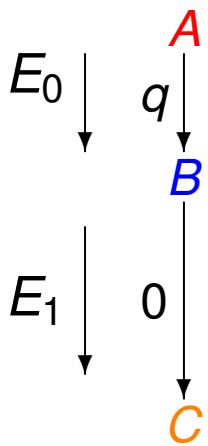
But : Difficulty of finding distinguishers

Idea : [Tezcan 10] and [Mala et al 10]
To derive improbable distinguishers from impossible ones

Improbable from Impossible

Distinguisher on E is derived from :

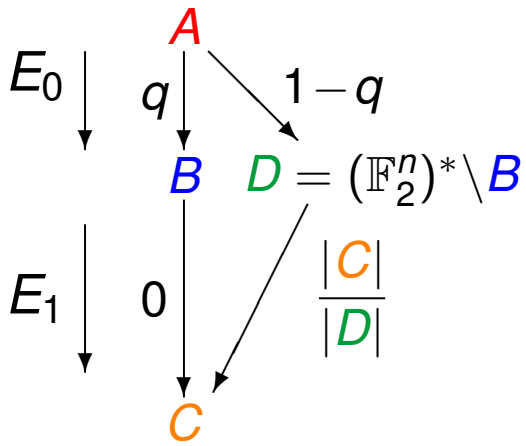
- a truncated differential (A, B) over E_0,
- an impossible differential (B, C) over E_1



Improbable from Impossible

Distinguisher on E is derived from :

- a truncated differential (A, B) over E_0,
- an impossible differential (B, C) over E_1

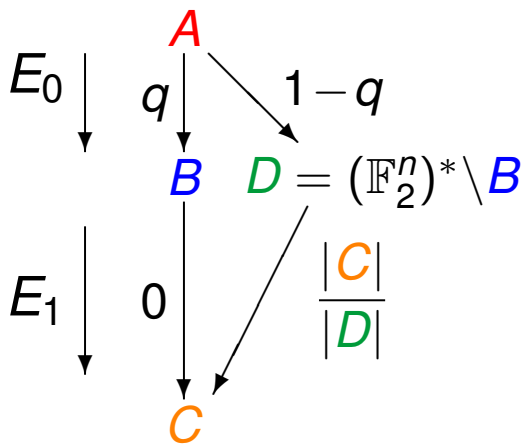


- $D = (\mathbb{F}_2^n)^* \setminus B$, $\quad \frac{|C|}{|D|} \leq 1$

Improbable from Impossible

Distinguisher on E is derived from :

- a truncated differential (A, B) over E_0,
- an impossible differential (B, C) over E_1

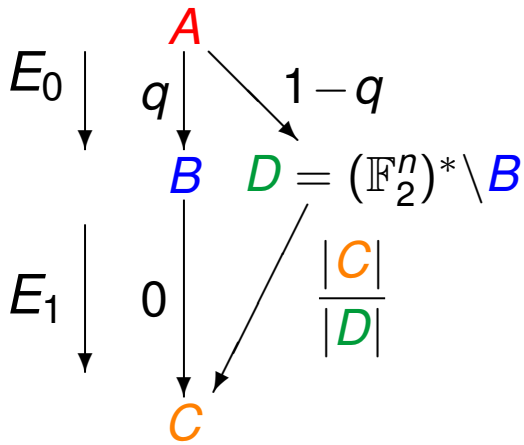


- $D = (\mathbb{F}_2^n)^* \setminus B$, $\quad \frac{|C|}{|D|} \leq 1$
- If $P[A \to B] = q$ then $P[A \to D] = 1 - q$
- If $P[B \to C] = 0$ then $P[D \to C] = \frac{|C|}{|D|}$

Improbable from Impossible

Distinguisher on E is derived from :

- a truncated differential (A, B) over E_0,
- an impossible differential (B, C) over E_1



- $D = (\mathbb{F}_2^n)^* \setminus B$, $\quad \frac{|C|}{|D|} \leq 1$
- If $P[A \to B] = q$ then $P[A \to D] = 1 - q$
- If $P[B \to C] = 0$ then $P[D \to C] = \frac{|C|}{|D|}$

Claim :

$$P[A \to C] = P[A \to D] \cdot P[D \to C] = (1 - q) \cdot \frac{|C|}{|D|}$$

Improbable from Impossible

Uniform probability :

$$p_U = \frac{|C|}{2^n}$$

Claim :

$$P[A \to C] = (1 - q) \cdot \frac{|C|}{|D|}$$

Often $|D| \approx 2^n$ and as in [Tezcan 10], it is assumed that :

$$P[A \to C] \approx (1 - q) \cdot p_U = p_U + \varepsilon,$$

with $\varepsilon = -q \cdot p_U < 0$

Analyzing the Model

For differential distinguishers :

- To compute the probability of a differential trail
  - Markov assumption is assumed correct when averaging over the keys
- If we do not sum over all trails, we get
  - an underestimate of the probability
  - and an overestimate of data complexity N

For such improbable differential distinguishers :

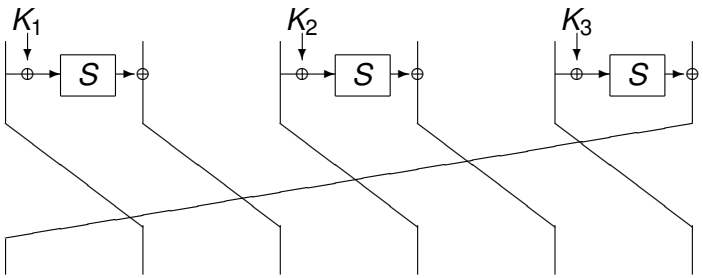
- What is happening in practice? and why?

We denote by p_E the experimental probability

Example 1

- 24-bit generalized Feistel

Round function



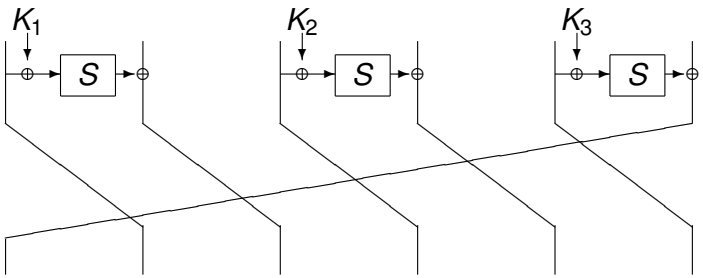
Improbable distinguisher

$$
\begin{array}{lcccccc}
A: & \mathrm{X} & \mathrm{Y} & 0 & 0 & 0 & 0 \\
 & \text{1 round} & \Downarrow & q = 2^{-3.91} & & & \\
B: & 0 & \mathrm{X} & 0 & 0 & 0 & 0 \\
 & \text{10 rounds} & \Downarrow & \textit{Impossible} & & & \\
C: & 0 & 0 & 0 & \mathrm{Z} & 0 & 0
\end{array}
$$

Example 1

- 24-bit generalized Feistel

Round function



Improbable distinguisher

$$
\begin{array}{lcccccc}
A: & X & Y & 0 & 0 & 0 & 0 \\
 & \text{1 round} & & \Downarrow & q = 2^{-3.91} & & \\
B: & 0 & X & 0 & 0 & 0 & 0 \\
 & \text{10 rounds} & & \Downarrow & \textit{Impossible} & & \\
C: & 0 & 0 & 0 & Z & 0 & 0
\end{array}
$$

p	p_E	p_U
$2^{-20.10}$	$2^{-19.94}$	2^{-20}

$X, Y \in \{0x1, \ldots, 0xF\}$

In this case :

$p_E > p$ and even $p_E > p_U$

The differential is not improbable!!!

Improbable Differential on PRESENT

[Tezcan 13] : Notion of “undisturbed bits” to find impossible distinguishers on SPN ciphers

Improbable distinguishers on reduced-round PRESENT :

- $\mathcal{A}$: 3 rounds truncated + 6 rounds impossible (unpublished)
- $\mathcal{B}$: 5 rounds truncated + 5 rounds impossible [Tezcan 13]

Improbable Differential on PRESENT

[Tezcan 13] : Notion of "undisturbed bits" to find impossible distinguishers on SPN ciphers

Improbable distinguishers on reduced-round PRESENT :

- $\mathcal{A}$: 3 rounds truncated + 6 rounds impossible (unpublished)
- $\mathcal{B}$: 5 rounds truncated + 5 rounds impossible [Tezcan 13]

Experiments :

- On 3 rounds truncated + 5 rounds impossible of $\mathcal{A}$:

$$q = 2^{-12} \qquad p_U = 2^{-13}$$
$$p = 2^{-13.00035} \qquad p_E = 2^{-12.97}$$
$$p \leq p_U \leq p_E$$

Experiments on PRESENT

- On 1 round truncated + 4 rounds impossible of $\mathcal{B}$:

$$q = 2^{-4} \qquad p_U = 2^{-13.20}$$
$$p = 2^{-13.29} \qquad p_E = 2^{-13.31}$$

p_E close to p

Experiments on PRESENT

- On 1 round truncated + 4 rounds impossible of $\mathcal{B}$:

$$q = 2^{-4} \qquad p_U = 2^{-13.20}$$
$$p = 2^{-13.29} \qquad p_E = 2^{-13.31}$$

p_E close to p

- On 1 round truncated + 5 rounds impossible of $\mathcal{B}$:

$$q = 2^{-4} \qquad p_U = 2^{-16} \qquad p_E \leq p \leq p_U$$
$$p = 2^{-16.09} \qquad p_E = 2^{-16.49} \qquad \text{All } p_E \leq 2^{-16.34}$$

Experiments on PRESENT

- On 1 round truncated + 4 rounds impossible of $\mathcal{B}$:

$$q = 2^{-4} \qquad p_U = 2^{-13.20}$$
$$p = 2^{-13.29} \qquad p_E = 2^{-13.31}$$

p_E close to p

- On 1 round truncated + 5 rounds impossible of $\mathcal{B}$:

$$q = 2^{-4} \qquad p_U = 2^{-16} \qquad p_E \leq p \leq p_U$$
$$p = 2^{-16.09} \qquad p_E = 2^{-16.49} \qquad \text{All } p_E \leq 2^{-16.34}$$

- On 2 rounds truncated + 5 rounds impossible of $\mathcal{B}$:

$$q = 2^{-8} \qquad p_U = 2^{-16}$$
$$p = 2^{-16.006} \qquad p_E = 2^{-16.0073}$$

p_E close to p

Conclusion on the Experiments

Observation :

- The experimental probabilities can be different from the expected ones
- We can find under/over-estimate

Conclusion on the Experiments

Observation :

- The experimental probabilities can be different from the expected ones
- We can find under/over-estimate

Question :

- Can we safely multiply truncated differential probabilities?
- For simplicity, in the following explanation, the role of the key is omitted

Multiplying Truncated Differential Probability 1/2

$$p = P[A \xrightarrow{E} C] = \frac{1}{|A|} \sum_{a \in A} P_{\mathbf{X},\mathbf{K}} \left[E_K(X) \oplus E_K(X \oplus a) \in C \right]$$

Description :

- $E = E_1 \circ E_0$,
- a truncated differential (A, D) over E_0,
- a truncated differential (D, C) over E_1

Is it true that $P[A \xrightarrow{E} C] = P[A \xrightarrow{E_0} D] \cdot P[D \xrightarrow{E_1} C]$?

In general : NO

Multiplying Truncated Differential Probability 2/2

$$
\begin{aligned}
p &= \frac{1}{|A|} \sum_{a \in A} \sum_{c \in C} P[a \xrightarrow{E} c] \\
&\geq \frac{1}{|A|} \sum_{a \in A} \sum_{d \in D} \sum_{c \in C} P[a \xrightarrow{E_0} d] \cdot P[d \xrightarrow{E_1} c]
\end{aligned}
$$

Assuming that $\forall d \in D$, $P[d \overset{E_1}{\mapsto} C]$ are equal[1], we obtain

$$
\begin{aligned}
p &\geq \frac{|C|}{|D|} \frac{1}{|a|} \sum_{a \in A} \sum_{d \in D} P[a \xrightarrow{E_0} d] \\
&\geq P[A \xrightarrow{E_0} D] \cdot P[D \xrightarrow{E_1} C]
\end{aligned}
$$

[1] Assumption can be done for the other part of the cipher

Explanation Continue by Hand...

- What happens if the assumption is not satisfied?

Example $|D = 2|$

Explanation Continue by Hand...

- What happens if the assumption is not satisfied?

Example $|D = 2|$

$P[A \to d]$ \ $P[d \to C]$	$1/16$	$3/16$
$2/16$	$2/256$	-
$6/16$	-	$18/256$

$$P[A \to D] \cdot P[D \to C] = (\frac{2}{16} + \frac{6}{16}) \times \frac{1}{2}(\frac{1}{16} + \frac{3}{16}) = \frac{16}{256}$$

$$\leq$$

$$\sum_d P[A \to d] \cdot P[d \to C] = \frac{2}{256} + \frac{18}{256} = \frac{20}{256}$$

Explanation Continue by Hand...

- What happens if the assumption is not satisfied?

Example $|D = 2|$

$P[A \to d]$ \ $P[d \to C]$	$1/16$	$3/16$
$6/16$	$6/256$	-
$2/16$	-	$6/256$

$$P[A \to D] \cdot P[D \to C] = (\frac{2}{16} + \frac{6}{16}) \times \frac{1}{2}(\frac{1}{16} + \frac{3}{16}) = \frac{16}{256}$$

$$\geq$$

$$\sum_d P[A \to d] \cdot P[d \to C] = \frac{6}{256} + \frac{6}{256} = \frac{12}{256}$$

Explanation Continue by Hand...

- What happens if the assumption is not satisfied?

Example $|D = 2|$ (same probabilities)

$P[A \to d]$ \ $P[d \to C]$	$2/16$	$2/16$
$2/16$	$4/256$	-
$6/16$	-	$12/256$

$$P[A \to D] \cdot P[D \to C] = (\frac{2}{16} + \frac{6}{16}) \times \frac{1}{2}(\frac{2}{16} + \frac{2}{16}) = \frac{16}{256}$$

$$=$$

$$\sum_d P[A \to d] \cdot P[d \to C] = \frac{4}{256} + \frac{12}{256} = \frac{16}{256}$$

Summary of the Explanation

$$p \geq \frac{1}{|A|} \sum_{a \in A} \sum_{d \in D} \sum_{c \in C} P[a \xrightarrow{E_0} d] \cdot P[d \xrightarrow{E_1} c]$$

Assuming that $\forall d \in D$, $P[d \xrightarrow{E_1} C]$ or $P[A \xrightarrow{E_0} d]$ are equal,

$$p \geq P[A \xrightarrow{E_0} D] \cdot P[D \xrightarrow{E_1} C]$$

Summary of the Explanation

$$p \geq \frac{1}{|A|} \sum_{a \in A} \sum_{d \in D} \sum_{c \in C} P[a \xrightarrow{E_0} d] \cdot P[d \xrightarrow{E_1} c]$$

Assuming that $\forall d \in D$, $P[d \xrightarrow{E_1} C]$ or $P[A \xrightarrow{E_0} d]$ are equal,

$$p \geq P[A \xrightarrow{E_0} D] \cdot P[D \xrightarrow{E_1} C]$$

For truncated distinguisher :

We do not know if

$$P[A \xrightarrow{E_0} D] \cdot P[D \xrightarrow{E_1} C]$$

is an under/over-estimate of

$$\frac{1}{|A|} \sum_{a \in A} \sum_{d \in D} \sum_{c \in C} P[a \xrightarrow{E_0} d] \cdot P[d \xrightarrow{E_1} c]$$

Summary of the Explanation

$$p = \frac{1}{|A|} \sum_{a \in A} \sum_{d \in D} \sum_{c \in C} P[a \xrightarrow{E_0} d] \cdot P[d \xrightarrow{E_1} c]$$

Assuming that $\forall d \in D$, $P[d \xrightarrow{E_1} C]$ or $P[A \xrightarrow{E_0} d]$ are equal,

$$p = P[A \xrightarrow{E_0} D] \cdot P[D \xrightarrow{E_1} C]$$

For improbable distinguisher :

- "$\geq$" is "$=$"
- $|D|$ is close to 2^n
- $P[A \xrightarrow{E_0} D] \cdot P[D \xrightarrow{E_1} C]$ is not an under/over-estimate of $P[A \xrightarrow{E} C]$

Conclusion

- Improbable differential can be used for cryptanalytic purposes
- Tezcan and Mala et al proposed to derive improbable distinguishers from impossible ones
- We show based on experiments that the model is not completely correct