Aalto University
School of Science

Differential-Linear Cryptanalysis Revisited

Céline Blondeau[1] and Gregor Leander[2] and **Kaisa Nyberg**[1]

[1] Aalto University School of Science, Finland
[2] Ruhr Universität Bochum, Germany

4 March 2014

FSE London

Outline

Introduction

The Setting and Previous Work

Computing the Bias

Estimating the Bias

Multidimensional Differential-Linear Cryptanalysis

Conclusion

Outline

Introduction

The Setting and Previous Work

Computing the Bias

Estimating the Bias

Multidimensional Differential-Linear Cryptanalysis

Conclusion

Motivation

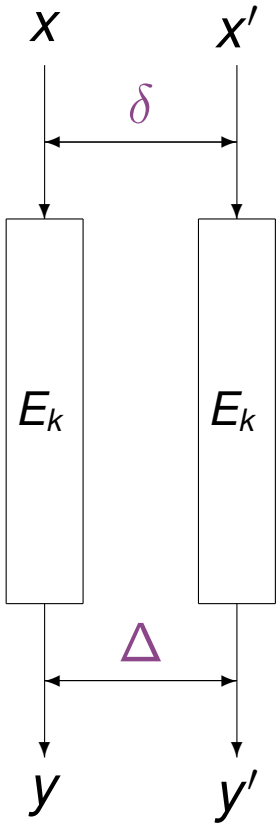
Differential-linear cryptanalysis has been quite successful attacking block ciphers, in particular, Serpent

Although it seems to work, it is rather ad hoc and its foundations have not been well studied

We know by now that differential and linear cryptanalysis are closely linked - what does it mean for differential-linear cryptanalysis?

Differential Cryptanalysis [Murphy 90][Biham Shamir 90]

Difference between plaintext and ciphertext pairs



Input difference : δ
Output Difference : Δ

Differential Probability :

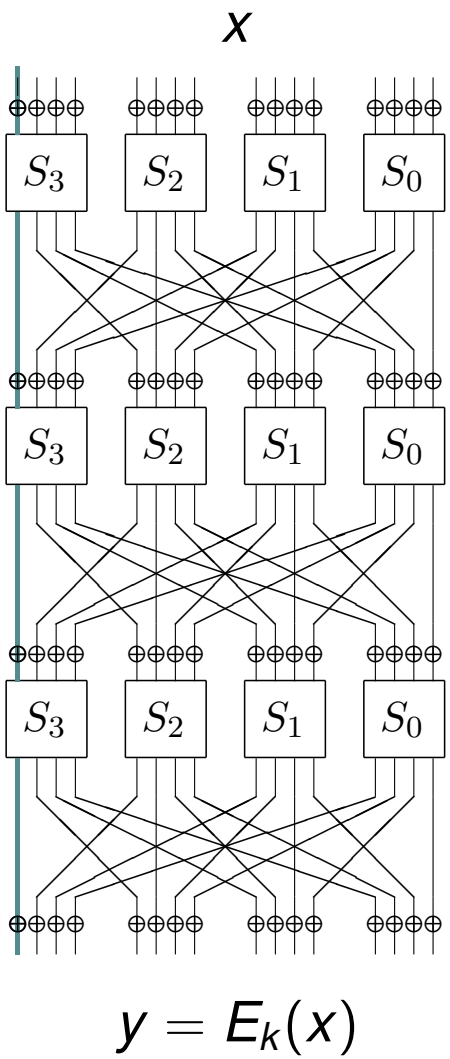
$$\Pr[\delta \rightarrow \Delta] \quad = \quad \Pr_x[\, E_k(x) \oplus E_k(x \oplus \delta) = \Delta]$$

Truncated Differential (TD) [Knudsen 94] :

$$\Pr[U^{\perp} \rightarrow V^{\perp}] = \frac{1}{|U^{\perp}|} \sum_{\delta \in U^{\perp}} \sum_{\Delta \in V^{\perp}} \Pr[\delta \rightarrow \Delta]$$

Linear Cryptanalysis [Tardy Gilbert 91] [Matsui 93]

Linear relation involving plaintext and ciphertext bits



Input mask : u
Output mask : v

Correlation :

$$c_{u,v} = 2 \cdot \Pr_x[u \cdot x + v \cdot E_k(x) = 0] - 1$$

Capacity of a multidimensional linear approximation : [Hermelin et al. 08]

$$c_{U,V} = \sum_{u \in U \setminus \{0\}} \sum_{v \in V \setminus \{0\}} c_{u,v}^2$$

Outline

Introduction

The Setting and Previous Work

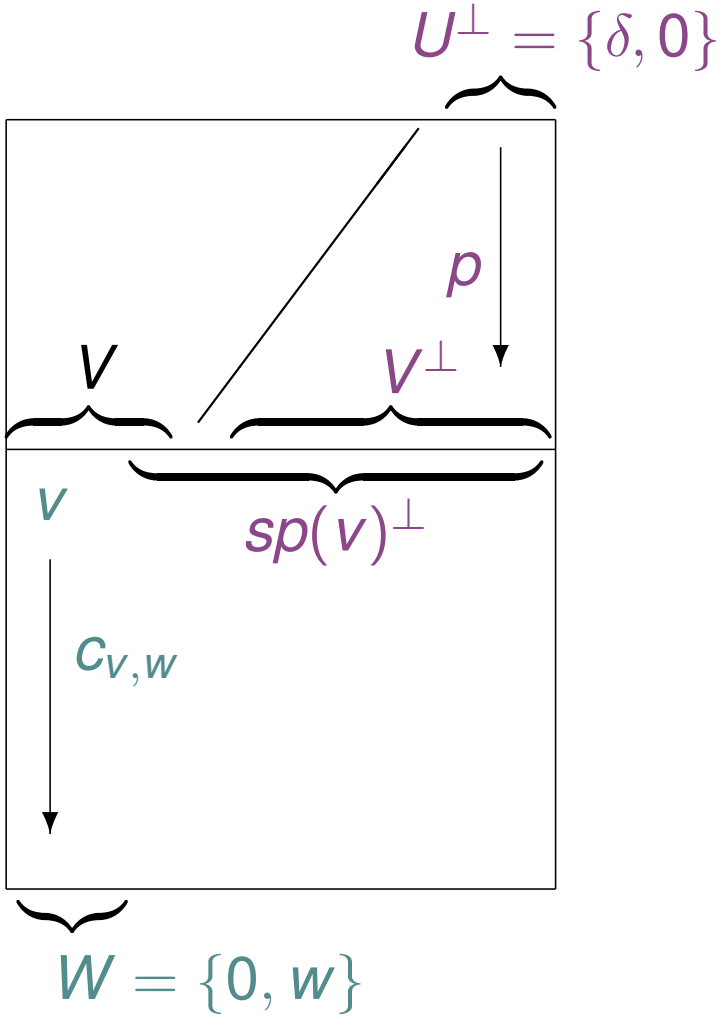
Computing the Bias

Estimating the Bias

Multidimensional Differential-Linear Cryptanalysis

Conclusion

Differential-Linear Cryptanalysis: The Setting



- $E = E_1 \circ E_0$
- V is a subspace of the intermediate layer
- Strong truncated differential $(\delta, V^\perp)$ over E_0

$$p = \Pr[\delta \xrightarrow{E_0} V^\perp]$$

- Strong linear approximation (v, w) over E_1, where $v \in V$

$$c_{v,w} = 2 \cdot \Pr[v \cdot y + w \cdot E_1(y) = 0] - 1$$

Differential-Linear Relation: The Bias?

In differential-linear cryptanalysis, we want to compute this bias:

$$\mathcal{E}_{\delta,w} = \Pr[w \cdot (E(x+\delta) + E(x)) = 0] - \frac{1}{2}$$

Approach used in the literature:

$$\begin{aligned} w \cdot (E(x+\delta) + E(x)) &= v \cdot E_0(x+\delta) + w \cdot E(x+\delta) \\ &+ v \cdot (E_0(x+\delta) + E_0(x)) \\ &+ v \cdot E_0(x) + w \cdot E(x) \end{aligned}$$

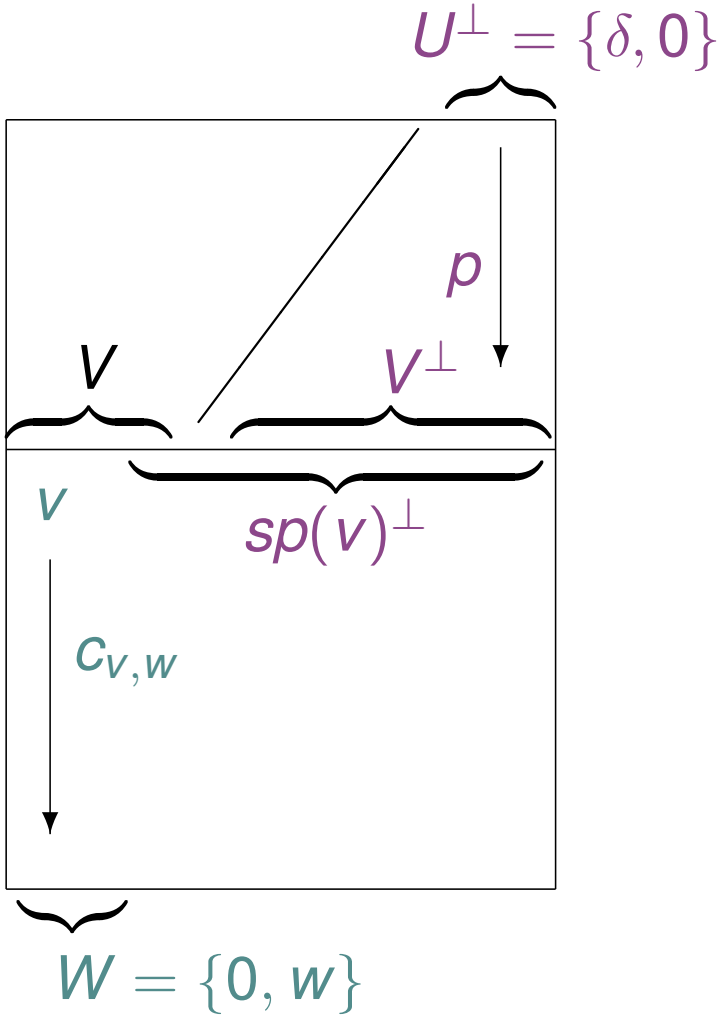
The Piling-up lemma gives

$$\mathcal{E}_{\delta,w} = \varepsilon_{\delta,v} c_{v,w}^2,$$

where

$$\varepsilon_{\delta,v} = \Pr[v \cdot (E_0(x+\delta) + E_0(x)) = 0] - \frac{1}{2} = \Pr[\delta \xrightarrow{E_0} sp(v)^{\perp}] - \frac{1}{2}$$

Previous Work



$$\mathcal{E}_{\delta,w} = \varepsilon_{\delta,v} c_{v,w}^2$$

[Langford and Hellman 94]

$$p = 1 \text{ and } \mathcal{E}_{\delta,w} = \frac{1}{2} c_{v,w}^2$$

[Biham et al 02]

Problem: $p < 1$ known, $\varepsilon_{\delta,v}$ not known

Assumption: outside $V^\perp$ the parities of $v \cdot \Delta$ balanced. They get $\varepsilon_{\delta,v} \approx \frac{p}{2}$

[Lu 12]

Observes that this estimate fails if $V^\perp = sp(v)^\perp$, and restricts to this case

Example: Estimate may fail also if $V^\perp \neq sp(v)^\perp$

$$
\begin{aligned}
V &= \{(0,0,0,\ldots,0),(0,1,0,\ldots,0),(1,0,0,\ldots,0),(1,1,0,\ldots,0)\} \\
V^\perp &= \{(0,0,*,\ldots,*)\} \\
v &= (1,1,0,\ldots,0) \\
sp(v)^\perp &= \{(0,0,*,\ldots,*),(1,1,*,\ldots,*)\}
\end{aligned}
$$

Assume

$$p = \frac{1}{2} \quad \text{and} \quad \Pr[\delta \to (1,1,*,\ldots,*)] = 0$$

Then $\Pr[v \cdot (E_0(x+\delta) + E_0(x)) = 0] = \frac{1}{2}$, that is $\varepsilon_{\delta,v} = 0$

The assumption of Biham et al. gives $\varepsilon_{\delta,v} \approx \frac{1}{4}$

Linear approximations with more than one intermediate mask v must be considered

Outline

Introduction

The Setting and Previous Work

Computing the Bias

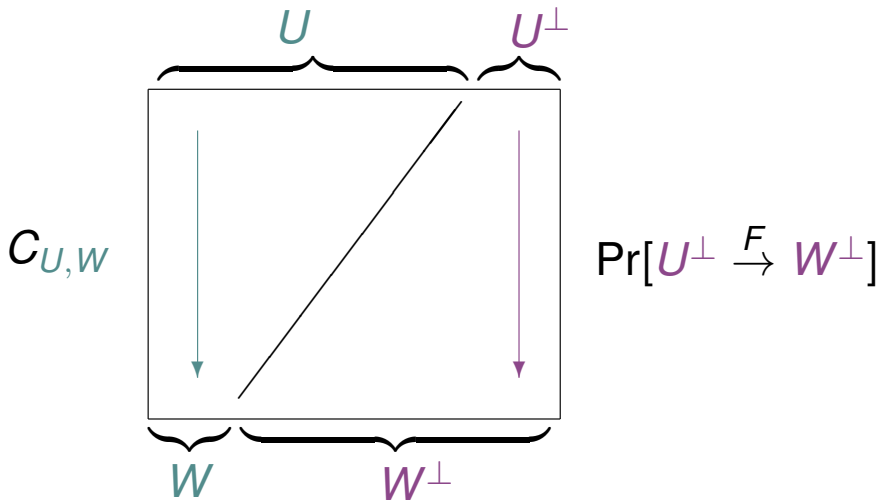
Estimating the Bias

Multidimensional Differential-Linear Cryptanalysis

Conclusion

Differential and Linear Cryptanalysis: The Link

[Chabaud Vaudenay 94] [Blondeau Nyberg 13, 14]



multidim. linear $\quad \frac{1}{|W|}(C_{U,W}+1)$

trunc. differential $\quad \Pr[U^\perp \xrightarrow{F} W^\perp]$

differential-linear $\quad \frac{1}{|U^\perp|}\sum_{\delta\in U^\perp} \Pr[w\cdot(F(x+\delta)+F(x))=0, \text{ for all } w\in W]$

Differential-Linear Relation: The Bias

Assumption : E_0 and E_1 are independent

Result : For all $\delta \in \mathbb{F}_2^n \setminus \{0\}$ and $w \in \mathbb{F}_2^n \setminus \{0\}$

$$\mathcal{E}_{\delta,w} = \sum_{v \in \mathbb{F}_2^n} \varepsilon_{\delta,v} c_{v,w}^2.$$

The ideas of the proof:

- Round-independence
- Splitting

$$\Pr[\delta \xrightarrow{E} sp(w)^{\perp}] = \sum_{\Delta \in \mathbb{F}_2^n} \Pr[\delta \xrightarrow{E_0} \Delta] \Pr[\Delta \xrightarrow{E_1} sp(w)^{\perp}]$$

- Link between linear and differential cryptanalysis

Outline

Introduction

The Setting and Previous Work

Computing the Bias

Estimating the Bias

Multidimensional Differential-Linear Cryptanalysis

Conclusion

Restricting to a Part of the Intermediate Layer

$$\mathcal{E}_{\delta,w} = \sum_{v \in \mathbb{F}_2^n} \varepsilon_{\delta,v} c_{v,w}^2$$

- Impossible to compute in practice for all intermediates masks
- Cover only a part V of the intermediate layer

$$\hat{\mathcal{E}}_{\delta,w} = \sum_{v \in V} \varepsilon_{\delta,v} c_{v,w}^2$$

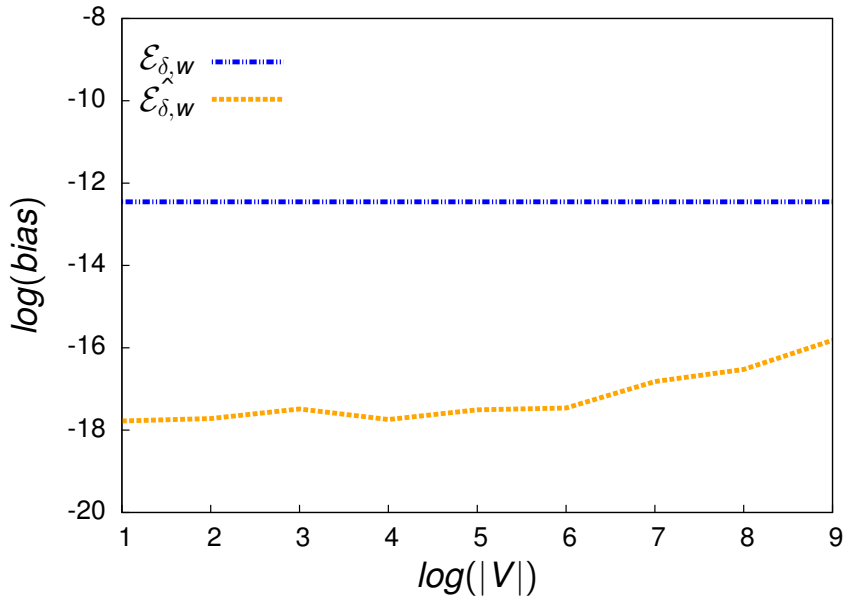
Assumption: For our selected set V we have

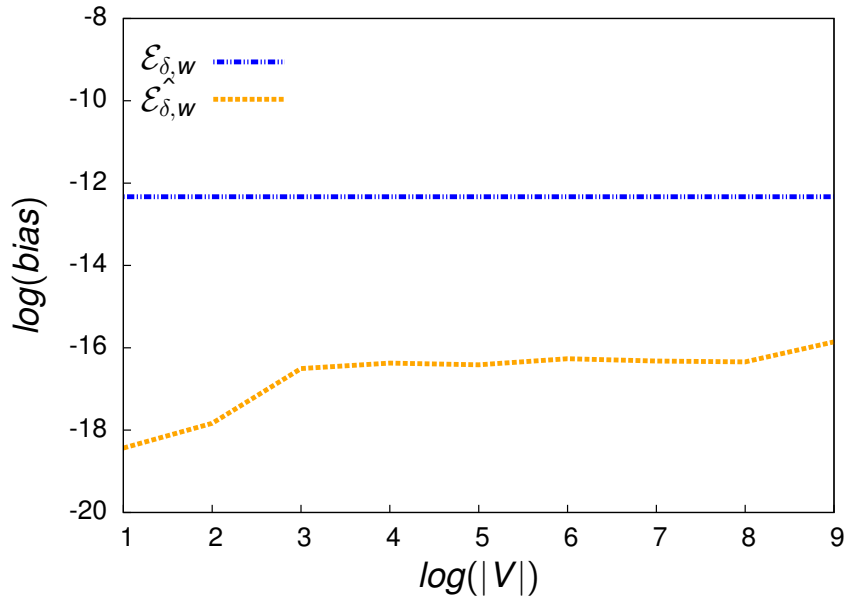
$$\left|\hat{\mathcal{E}}_{\delta,w}\right| \leq \left|\mathcal{E}_{\delta,w}\right|$$

- Then we can derive an upperbound to the data complexity
- Is this assumption true in practice?

Experiments on SmallPRESENT-[8]

- Comparison between
  - The exact bias
  - The bias computed when taking only a subset of the intermediate linear mask





- The assumption is verified on these experiments:
  the estimate $|\hat{\mathcal{E}}_{\delta,w}|$ is an underestimate of the absolute bias $|\mathcal{E}_{\delta,w}|$

A Lower Bound to $\mathcal{E}_{\delta,w} > 0$

$$\mathcal{E}_{\delta,w} = \sum_{v \in \mathbb{F}_2^n} \varepsilon_{\delta,v} c_{v,w}^2 = \sum_{v \in \mathbb{F}_2^n} \left(\varepsilon_{\delta,v} + \frac{1}{2} \right) c_{v,w}^2 - \frac{1}{2}$$

Then the following quantity increases with V

$$\sum_{v \in V} \left(\varepsilon_{\delta,v} + \frac{1}{2} \right) c_{v,w}^2 - \frac{1}{2} = \hat{\mathcal{E}}_{\delta,w} - \frac{1}{2} \left(1 - \sum_{v \in V} c_{v,w}^2 \right)$$

and is less than or equal to $\mathcal{E}_{\delta,w}$. As soon as it is positive, it gives a lower bound to $\mathcal{E}_{\delta,w}$.

Works if $\mathcal{E}_{\delta,w}$ is positive.

Multiplying Truncated Differentials

$$\hat{\mathcal{E}}_{\delta,w} = \sum_{v \in V} \varepsilon_{\delta,v} c^2_{v,w}$$

Question:

Do we need to know the quantities $\varepsilon_{\delta,v}$ and $c^2_{v,w}$ for all $v \in V$?

Multiplying Truncated Differentials

$$\hat{\mathcal{E}}_{\delta,w} = \sum_{v \in V} \varepsilon_{\delta,v} c_{v,w}^2$$

Question:

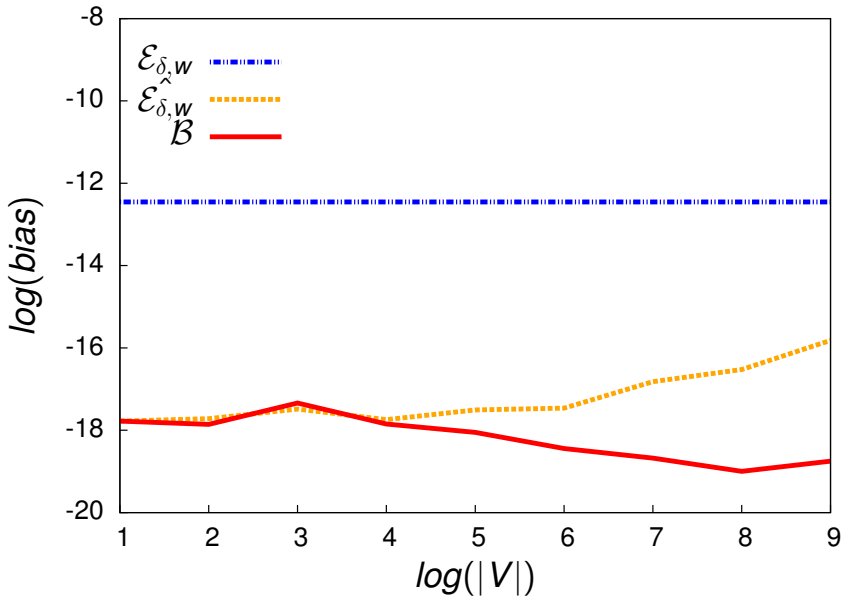
Do we need to know the quantities $\varepsilon_{\delta,v}$ and $c_{v,w}^2$ for all $v \in V$?

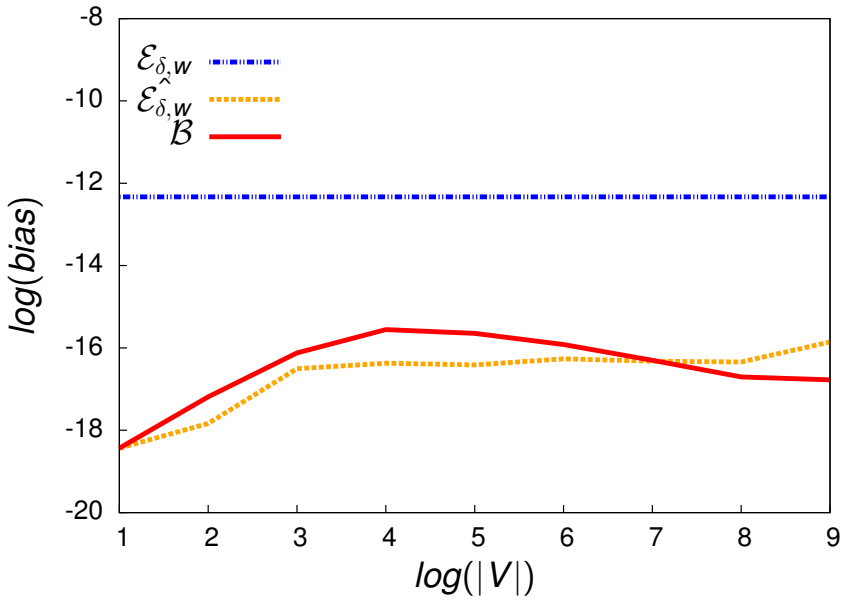
- $\varepsilon_{\delta,V} = \Pr[\delta \xrightarrow{E_0} V^\perp] - \frac{1}{|V|}$
- $C_{V,w} = \sum_{v \in V, v \neq 0} c_{v,w}^2$

Assumption: For all $\Delta \notin V^\perp$, the probabilities $\mathbf{P}[\delta \xrightarrow{E_0} \Delta]$ are equal

Result: $\hat{\mathcal{E}}_{\delta,w} = \underbrace{\frac{1}{2} \frac{|V|}{|V|-1} \varepsilon_{\delta,V} C_{V,w}}_{=\mathcal{B}}$

More Experiments





- Multiplication of truncated differentials instead of differentials does not give an underestimate or an overestimate of $\hat{\mathcal{E}}_{\delta,w}$
- In this example, $\mathcal{B}$ would work because it is sufficiently close to $\hat{\mathcal{E}}_{\delta,w}$ which is an underestimate of the true bias $\mathcal{E}_{\delta,w}$
- [Blondeau 13] This phenomenon of multiplication of truncated differentials may ruin the estimates in sensitive situations such as improbable differentials

Outline

Introduction

The Setting and Previous Work

Computing the Bias

Estimating the Bias

Multidimensional Differential-Linear Cryptanalysis

Conclusion

Multidimensional Differential-Linear Cryptanalysis

- All input differences in $U^\perp$
- All output masks in W

Given for all $v \in \mathbb{F}_2^n, v \neq 0$

- $\varepsilon_{U,v} = \Pr[U^\perp \setminus \{0\} \xrightarrow{E_0} sp(v)^\perp] - 1/2$
- $C_{v,W} = \sum_{w \in W, w \neq 0} \mathbf{cor}^2(v \cdot y + w \cdot E_1(y))$

Then

$$\mathcal{E}_{U,W} = \Pr[U^\perp \setminus \{0\} \xrightarrow{E} W^\perp] - \frac{1}{|W|} = \frac{2}{|W|} \sum_{v \in \mathbb{F}_2^n, v \neq 0} \varepsilon_{U,v} C_{v,W}$$

- The results about intermediate space V apply also here
- Multiplication of truncated differentials is even more shaky

Outline

Introduction

The Setting and Previous Work

Computing the Bias

Estimating the Bias

Multidimensional Differential-Linear Cryptanalysis

Conclusion

Conclusion

- We analyze the previous approaches to the differential-linear cryptanalysis
- Using the links between differential and linear cryptanalysis, we derive an exact formula for the bias $\mathcal{E}_{\delta,w}$ of a differential-linear approximation
- Under some clear assumptions, we explain how this bias can be estimated in practice
- It seems that positive biases are easier to estimate
- We generalize the results to the case of many input differences and output masks