Aalto University
School of Science

New Links Between Differential and Linear Cryptanalysis

Céline Blondeau and Kaisa Nyberg

Tuesday, May 28, 2013

EUROCRYPT, *Athens*

Outline

Outline

- Statistical Cryptanalysis
  - Statistical Attack
  - Differential and Linear Cryptanalysis
- Links between Statistical Attacks
  - Recent Links
  - Zero Correlation Linear and Impossible Differential
- Computing Differential Probabilities using Linear Correlations
  - Methodology
  - Experiment on PRESENT

Statistical Attacks

LINEAR CONTEXT | **DIFFERENTIAL CONTEXT**

Linear Cryptanalysis [Tardy, Gilbert 92] [Matsui 93]

Differential Cryptanalysis [Biham, Shamir 90]

Differential-Linear Cryptanalysis [Langford, Hellman 94]

Truncated Differential Cryptanalysis [Knudsen 94]

Higher Order Differential cryptanalysis [Lai 94] [Knudsen 94]

Square Attack, Integral ··· [Daemen, Rijmen, Knudsen 97]

Statistical Saturation [Collard, Standaert 09]

Zero Correlation [Bogdanov, Rijmen 11]

Impossible Differential Cryptanalysis [Biham, Biryukov, Shamir 99]

Multiple Linear Cryptanalysis [Biryukov, de Cannière, Quisquater 04]

Multiple Differential Cryptanalysis [Albrecht, Leander 12] [Blondeau, Gérard, Nyberg 12]

Multidimensional Linear Cryptanalysis [Cho, Hermelin, Nyberg 08]

. . . . . .

. . . . . .

Link Between Statistical Attacks

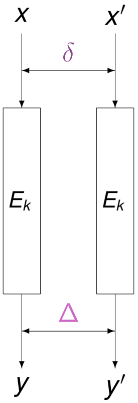
Too many statistical attacks!!!

Aim:

- Understanding the attacks and their relations
- Helping designers and cryptanalysts to concentrate on important attacks

Differential Cryptanalysis

Difference between plaintext and ciphertext pairs



Input difference δ

Output Difference Δ

Differential Probability:

$$\mathbf{P}[\delta \to \Delta] \quad = \quad P_x[\ E_k(x) \oplus E_k(x \ \oplus \ \delta) = \Delta]$$

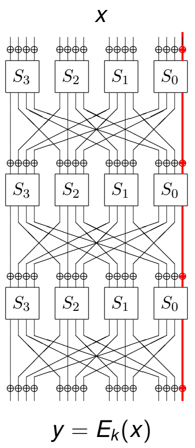
Truncated Output Differences:

Set of output differences: $\Delta \in W$

$$\mathbf{P}[\delta \to W] = \sum_{\Delta \in W} P[\delta \to \Delta]$$

Linear Cryptanalysis

Linear relation involving plaintext, key and ciphertext bits.



Input mask a

Key mask κ

Output mask b

Bias:

$$\varepsilon = 2^{-n}\#\{x \in \mathbb{F}_2^n |\ a \cdot x \oplus \kappa \cdot k \oplus b \cdot y = 0\} - \frac{1}{2}$$

Correction: $\mathbf{cor}_x(a, b) = 2\varepsilon$

Multidimensional linear approximation:

Set of masks $(a, b) \in A \times B$

Capacity: $\sum_{a \in A} \sum_{b \in B} \mathbf{cor}_x^2(a, b)$

Estimation of Differential Probability or Correlation

Methods to catch significant trails:

- Dominant trails: By hand
- Branch and Bound algorithm
- Transition matrices

Observation:

- For some ciphers like PRESENT, it is easier to estimate linear correlations than differential probabilities

Idea:

- Use linear correlations to compute differential probabilities

Link between Differential Probability and Correlation

[Chabaud Vaudenay 94]

Let $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^m} (-1)^{a\cdot\delta \oplus b\cdot\Delta} \mathbf{cor}_x^2(a, b)$$

Link between Differential Probability and Correlation

[Chabaud Vaudenay 94]

Let $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^m} (-1)^{a \cdot \delta \oplus b \cdot \Delta} \mathbf{cor}_x^2(a, b)$$

- Used for theory (almost bent $\Rightarrow$ APN)
- Not really used for cryptanalysis

Link between Differential Probability and Correlation

[Chabaud Vaudenay 94]

Let $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^m} (-1)^{a \cdot \delta \oplus b \cdot \Delta} \mathbf{cor}_x^2 (a, b)$$

- Used for theory (almost bent $\Rightarrow$ APN)
- Not really used for cryptanalysis

Our contribution:

- New links between statistical attacks
- New method to compute differential probabilities

Outline

Recent Links

[Leander 11] :

Statistical Saturation $\Leftrightarrow$ Multidimensional Linear

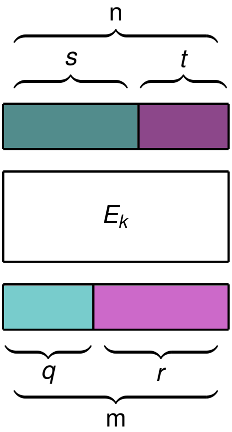
[Bogdanov *et al* 12] :

Integral $\Leftrightarrow$ Zero Correlation Linear

Proofs can be done using Fundamental Theorem [Nyberg 94]:

$$2^{-s} \sum_{x \in \mathbb{F}_2^s} \sum_{b \in \mathbb{F}_2^q \setminus \{0\}} \mathbf{cor}_x^2(0, b) = \sum_{a \in \mathbb{F}_2^s} \sum_{b \in \mathbb{F}_2^q \setminus \{0\}} \mathbf{cor}_x^2(a, b)$$

New Extended Link : Splitting the Spaces



Split the input and output spaces

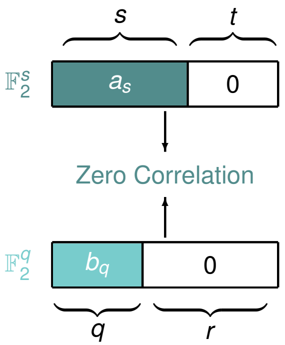
Left is active in:

the multidimensional linear context

Right is active in:

the truncated differential context

Zero Correlation Linear

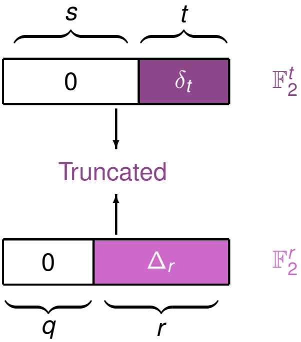


Zero Correlation Linear :

$$\mathbf{cor}_x((a_s, 0), (b_q, 0)) = 0$$

for all $(a_s, b_q) \in \mathbb{F}_2^s \times \mathbb{F}_2^q \neq (0, 0)$

Truncated Differential

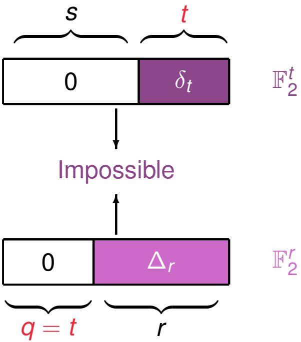


Using the Chabaud-Vaudenay's link:

Truncated Differential:

$$\sum_{\delta_t \in \mathbb{F}_2^t} \sum_{\Delta_r \in \mathbb{F}_2^r} \mathbf{P}\left[(0, \delta_t) \to (0, \Delta_r)\right] = 2^{t-q}$$

Impossible Differential



Using the Chabaud-Vaudenay's link:

Truncated Differential:

$$\sum_{\delta_t \in \mathbb{F}_2^t} \sum_{\Delta_r \in \mathbb{F}_2^r} \mathbf{P}\left[(0, \delta_t) \to (0, \Delta_r)\right] = 2^{t-q}$$

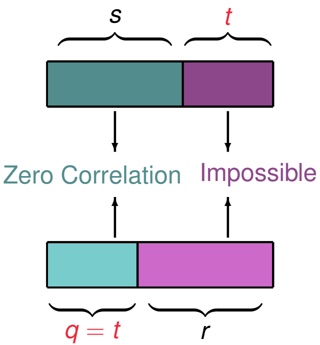
If t=q and $\delta_t \neq 0$

Impossible Differential:

$$\mathbf{P}\left[(0, \delta_t) \to (0, \Delta_r)\right] = 0$$

for all $(\delta_t, \Delta_r) \in \mathbb{F}_2^t \times \mathbb{F}_2^r \neq (0, 0)$

Zero Correlation Linear and Impossible Differential



If $t = q$

Zero Correlation Linear Distinguisher

is equivalent to

Impossible Differential Distinguisher

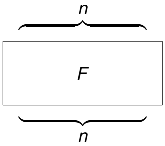
Outline

Statistical Cryptanalysis
- Statistical Attack
- Differential and Linear Cryptanalysis

Links between Statistical Attacks
- Recent Links
- Zero Correlation Linear and Impossible Differential

Computing Differential Probabilities using Linear Correlations
- Methodology
- Experiment on PRESENT

Computation



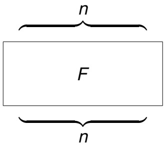
Chabaud-Vaudenay's link:

$$\mathbf{P}[\delta \xrightarrow{F} \Delta] = 2^{-n} \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^n} (-1)^{a \cdot \delta \oplus b \cdot \Delta} \mathbf{cor}_x^2(a, b)$$

Complexity: Computation of 2^{2n} correlations!!!

$\Rightarrow$ Impossible in practice

Computation



Chabaud-Vaudenay's link:

$$\mathbf{P}[\delta \xrightarrow{F} \Delta] = 2^{-n} \sum_{a \in \mathbb{F}_2^n} \sum_{b \in \mathbb{F}_2^n} (-1)^{a \cdot \delta \oplus b \cdot \Delta} \mathbf{cor}_x^2(a, b)$$

Complexity: Computation of 2^{2n} correlations!!!

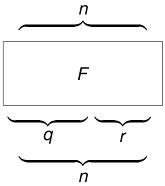
$\Rightarrow$ Impossible in practice

How to reduce the complexity:

- Using truncated output difference
  $\Rightarrow$ Reduce the output space

- Assuming δ of small weight
  $\Rightarrow$ Reduce the input space

Truncated Output Difference

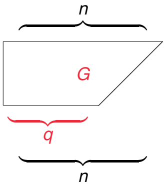


Setting:

- Affine space $\Delta_q \oplus \mathbb{F}_2^r$
- Let G be projection of F

$$\mathbf{P}[\delta \xrightarrow{F} (\Delta_q \oplus \mathbb{F}_2^r)] = \mathbf{P}[\delta \xrightarrow{\color{red}{G}} \Delta_q]$$

Truncated Output Difference

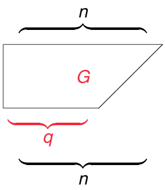


Setting:

- Affine space $\Delta_q \oplus \mathbb{F}_2^r$
- Let G be projection of F

$$\mathbf{P}[\delta \xrightarrow{F} (\Delta_q \oplus \mathbb{F}_2^r)] = \mathbf{P}[\delta \xrightarrow{G} \Delta_q]$$

Truncated Output Difference



Setting:

- Affine space $\Delta_q \oplus \mathbb{F}_2^r$
- Let G be projection of F

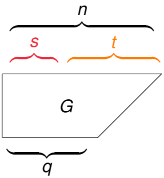
$$\mathbf{P}[\delta \xrightarrow{F} (\Delta_q \oplus \mathbb{F}_2^r)] = \mathbf{P}[\delta \xrightarrow{G} \Delta_q]$$

Link:

$$\mathbf{P}[\delta \xrightarrow{G} \Delta_q] = 2^{-q} \sum_{a \in \mathbb{F}_2^n} \sum_{b_q \in \mathbb{F}_2^q} (-1)^{a \cdot \delta \oplus b_q \cdot \Delta_q} \mathbf{cor}_x^2(a, b_q)$$

Complexity: Computation of 2^{n+q} correlations

Assuming δ of Small Weight

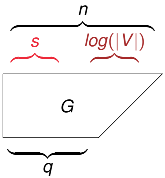


Assumption: $\delta = (\delta_s, \delta_t) \in \mathbb{F}_2^s \times \mathbb{F}_2^t$ with $\delta_t = 0$

Fundamental Theorem:

$$\sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot \delta} \mathbf{cor}_x^2(a, b_q) = 2^{-t} \sum_{x_t \in \mathbb{F}_2^t} \sum_{a_s \in \mathbb{F}_2^s} (-1)^{a_s \cdot \delta_s} \mathbf{cor}_{x_s}^2(a_s, b_q)$$

Assuming δ of Small Weight



Assumption: $\delta = (\delta_s, \delta_t) \in \mathbb{F}_2^s \times \mathbb{F}_2^t$ with $\delta_t = 0$

Fundamental Theorem:

$$\sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot \delta} \mathbf{cor}_x^2(a, b_q) = 2^{-t} \sum_{x_t \in \mathbb{F}_2^t} \sum_{a_s \in \mathbb{F}_2^s} (-1)^{a_s \cdot \delta_s} \mathbf{cor}_{x_s}^2(a_s, b_q)$$

Approximation:

$$\sum_{a \in \mathbb{F}_2^n} (-1)^{a \cdot \delta} \mathbf{cor}_x^2(a, b_q) \approx \frac{1}{|V|} \sum_{x_t \in V} \sum_{a_s \in \mathbb{F}_2^s} (-1)^{a_s \cdot \delta_s} \mathbf{cor}_{x_s}^2(a_s, b_q)$$

Method of Computation

Estimated Truncated Differential Probability:

$$\mathbf{P}[\delta \overset{G}{\to} \Delta_q] \approx \frac{2^{-q}}{|V|} \sum_{x_t \in V} \sum_{a_s \in \mathbb{F}_2^s} \sum_{b_q \in \mathbb{F}_2^q} (-1)^{a_s \cdot \delta_s \oplus b_q \cdot \Delta_q} \mathbf{cor}^2_{x_s}(a_s, b_q)$$

Complexity: Computation of $2^{s+q}|V|$ correlations

Accuracy: Depends on the choice of s and V

Setting of Experiments on PRESENT

PRESENT:

- Single-bit linear trails are dominant
- Computation of correlations using transition matrices as for instance in [Cho 10]

Setting of Experiments on PRESENT

PRESENT:

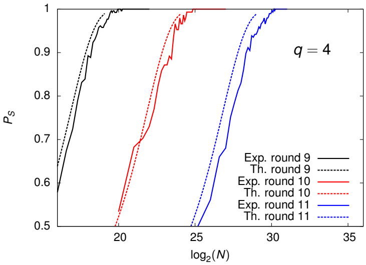
- Single-bit linear trails are dominant
- Computation of correlations using transition matrices
  as for instance in [Cho 10]

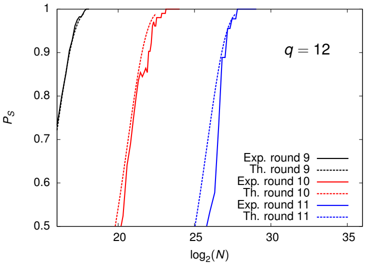
Setting:

- Truncated differential distribution cryptanalysis
  Using *LLR* statistical test [Blondeau Gérard Nyberg 12]
- Partition of the output difference space $\mathbb{F}_2^n = \cup \ \Delta_q^{(j)} \oplus \mathbb{F}_2^r$
- Estimation of all the $p_j = \mathbf{P}[\delta \overset{G}{\to} \Delta_q^{(j)}]$
  $\Rightarrow$ Need to compute the correlations only once
  $\Rightarrow$ We obtain a distribution

Truncated Differential Distribution Cryptanalysis

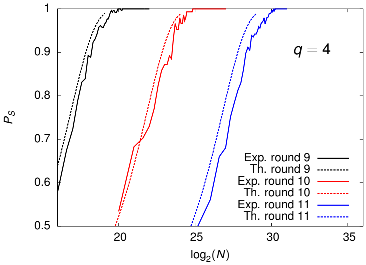
Experiments on PRESENT :

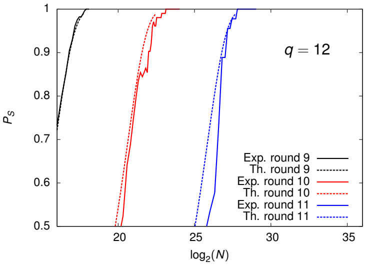




Truncated Differential Distribution Cryptanalysis

Experiments on PRESENT :





Cryptanalysis:

- On 19 rounds

Previously:

- Multiple differential cryptanalysis: 18 rounds
- Multidimensional linear cryptanalysis: 26 rounds

Conclusion

Extending the link of Chabaud and Vaudenay we provide:

- New links between statistical attacks

  Zero Correlation Linear $\Leftrightarrow$ Impossible Differential

- New method to compute differential probabilities

  $\Rightarrow$ Using correlations

- Instantiation of the technique on PRESENT