On the Data Complexity of Statistical Attacks against Block Ciphers

Céline Blondeau and Benoît Gérard

INRIA project-team SECRET, France

WCC - May the 14th 2009

Outline

Outline

Statistical attacks against block ciphers

Some known statistical cryptanalyses:

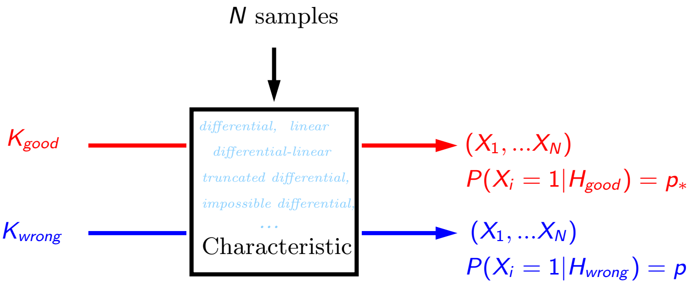
- linear cryptanalysis [Matsui 93];
- differential cryptanalysis [Biham Shamir 91];
- higher order differential cryptanalysis [Knudsen 94];
- impossible differential cryptanalysis [Biham Biryukov Shamir 99];
- ...

Using a characteristic to distinguish from random

Let χ be some characteristic on a given cipher.

- If the sub-key guess is correct : χ occurs with probability p_*.
- If the sub-key guess is not correct : χ occurs with probability p.

$$X_i = \begin{cases} 1 \text{ if } \chi \text{ occurs in sample } i, \\ 0 \text{ otherwise.} \end{cases}$$



Distinguisher

Neyman-Pearson (optimal) test:

Accept a candidate K if

$$\frac{P(X_1, X_2, \ldots, X_N | H_{\text{good}})}{P(X_1, X_2, \ldots, X_N | H_{\text{wrong}})} > t.$$

This (likelihood) ratio only depends on $S_N = \sum_{i=1}^{N} X_i$, p_* and p and is increasing in S_N.

Thus, the acceptance condition becomes, for some threshold $0 < T < N$,

$$\boxed{S_N > T}$$

- $S_{N,p_*} = \sum_{i=1}^{N} X_i$ follows a binomial law of parameters (N, p_*).
- $S_{N,p} = \sum_{i=1}^{N} X_i$ follows a binomial law of parameters (N, p).

Error probabilities

Two kinds of errors can be made:

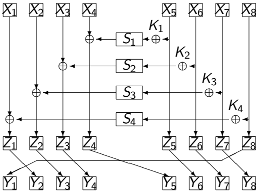
- **Non-detection error probability** $P(S_{N,p_*} < T)$;
- **False alarm error probability** $P(S_{N,p} \geq T)$.

The **non-detection error probability** corresponds to the success probability of the cryptanalysis.

The **false alarm error probability** is the expected ratio of kept candidates and thus influences the time complexity of the cryptanalysis.

Aim: Finding N minimal and the corresponding T such that $P(S_{N,p_*} < T) \leq \alpha$ and $P(S_{N,p} \geq T) \leq \beta$ for given values of α and β.

Motivation



Generalized Feistel Network [Nyberg 96] with:

- 10 rounds;
- 4 S-boxes.

Truncated differential path: $p_* = 1.18 \cdot 2^{-16}$ and $p = 2^{-16}$

Differential path: $p_* = 1.53 \cdot 2^{-27}$ and $p = 2^{-32}$

Question:

Which couple of parameters gives the best cryptanalysis ???

Outline

1. Introduction
2. Algorithm to find the data complexity
3. A problem: Approximation of the involved binomial tails
4. A formula to approximate the Data Complexity
5. Asymptotic behavior for some statistical attacks

An algorithm for finding N (1/2)

- For a fixed $\tau = T/N$, error probabilities decrease when N increases.
- For a fixed N, non-detection error increases with τ.
- For a fixed N, false alarm error decreases when τ increases.

Problem

N and T are integers $\Rightarrow$ restrictions on τ.

Solution

Approximations of probabilities (G_{nd} and G_{fa}) that:

- allow non integers values for N and T;
- have the expected properties.

An algorithm for finding N (2/2)

Input: (α, β) and (p_*, p)
Output: N and τ the minimum number of samples and the corresponding relative threshold to reach error probabilities less than (α, β).

$\tau_{\min} \leftarrow p$ and $\tau_{\max} \leftarrow p_*$.
repeat

$\quad \tau \leftarrow \dfrac{\tau_{\min} + \tau_{\max}}{2}$.

$\quad$ Compute $N_{\rm nd}$ such that $\forall N > N_{\rm nd},\ G_{\rm nd}(N, \tau) \leq \alpha$.

$\quad$ Compute $N_{\rm fa}$ such that $\forall N > N_{\rm fa},\ G_{\rm fa}(N, \tau) \leq \beta$.

$\quad$ **if** $N_{\rm nd} > N_{\rm fa}$ **then** $\tau_{\max} = \tau$ **else** $\tau_{\min} = \tau$

until $N_{\rm nd} = N_{\rm fa}$.
return N and τ.

Number of required samples N for differential and truncated-differential cryptanalyses

Answer to the question:

In that case, truncated differential is better than differential.

α	β	$\log(N)$ (differential)	$\log(N)$ (truncated differential)
0.5	0.001	27.35	24.31
0.5	10^{-10}	29.25	26.37
0.01	0.001	29.43	25.94
0.01	10^{-10}	30.54	27.29

Differential: $p_* = 1.53 \cdot 2^{-27}$ and $p = 2^{-32}$

Truncated differential: $p_* = 1.18 \cdot 2^{-16}$ and $p = 2^{-16}$

Outline

1. Introduction
2. Algorithm to find the data complexity
3. A problem: Approximation of the involved binomial tails
4. A formula to approximate the Data Complexity
5. Asymptotic behavior for some statistical attacks

Gaussian approximation of the binomial tail

$$P\left[S_{N,p} \leq N\tau\right] \simeq \int_{-\infty}^{\tau} \frac{1}{\sqrt{2\pi N p(1-p)}} \cdot e^{-\frac{N(x-p)^2}{2p(1-p)}}\, dx$$

Classically used in linear cryptanalysis:

- [Matsui 93,94];
- [Gilbert 97];
- [Junod 01,03,05];
- [Selçuk 08]
- ...

But ...

... not valid everywhere. For instance, when $N \cdot p$ is too small as in differential cryptanalysis [Selçuk 08].

Poisson approximation of the binomial tail

$$P\left[S_{N,p} \leq N\tau\right] \simeq \sum_{k=0}^{\lfloor N\tau \rfloor} e^{-Np} \cdot \frac{(Np)^k}{k!}$$

Implicitly used in differential cryptanalysis:

- [Biham Shamir 91,93];
- [Gilbert 97];
- [Selçuk 08]
- ...

But ...

... not valid everywhere. For instance, when $N \cdot p$ is too big as in linear cryptanalysis.

A good approximation of the binomial tail

We recall the binomial tail:

$$P\left[S_{N,p} \leq N\tau\right] = \sum_{k=0}^{\lfloor N\tau \rfloor} \binom{n}{k} p^k (1-p)^{n-k}$$

Approximation found, for instance, in [Arriata, Gordon 89]:

$$P(S_{N,p_*} \leq N\tau) \underset{N\to\infty}{\sim} \frac{p_*\sqrt{1-\tau}}{(p_* - \tau)\sqrt{2\pi N\tau}} \cdot 2^{-N\cdot D(\tau||p_*)}.$$

Where the Kullback-Leibler divergence is defined by:

$$D\left(p||q\right) = p\log_2\left(\frac{p}{q}\right) + (1-p)\log_2\left(\frac{1-p}{1-q}\right).$$

Experimental results

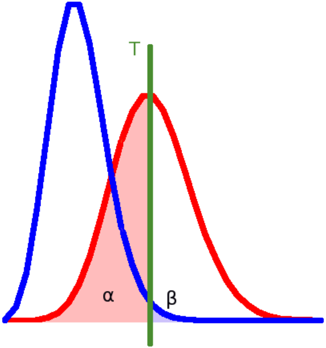
		Exact	Poisson	Gaussian	Ours
Lin Crypt: $p = 0.5$ $p_* = 0.5 + 2^{-10}$	β	$\mathbf{8.12 \cdot 10^{-5}}$	$3.84 \cdot 10^{-3}$	$\mathbf{8.12 \cdot 10^{-5}}$	$8.62 \cdot 10^{-5}$
	α	$\mathbf{2.97 \cdot 10^{-2}}$	$9.14 \cdot 10^{-2}$	$\mathbf{2.97 \cdot 10^{-2}}$	$3.58 \cdot 10^{-2}$
Diff Crypt: $p = 2^{-27}$ $p_* = 2^{-20}$	β	$\mathbf{2.03 \cdot 10^{-3}}$	$\mathbf{2.03 \cdot 10^{-3}}$	$8.84 \cdot 10^{-5}$	$1.97 \cdot 10^{-3}$
	α	$\mathbf{3.27 \cdot 10^{-3}}$	$\mathbf{3.27 \cdot 10^{-3}}$	$6.66 \cdot 10^{-3}$	$3.33 \cdot 10^{-3}$
Trunc Diff(1): $p = 2^{-4}$ $p_* = 1.01 \cdot 2^{-4}$	β	$\mathbf{9.29 \cdot 10^{-5}}$	$1.46 \cdot 10^{-4}$	$9.23 \cdot 10^{-5}$	$9.90 \cdot 10^{-5}$
	α	$\mathbf{9.80 \cdot 10^{-5}}$	$1.55 \cdot 10^{-4}$	$9.89 \cdot 10^{-5}$	$1.04 \cdot 10^{-4}$
Trunc Diff(2): $p = 2^{-15}$ $p_* = 1.5 \cdot 2^{-15}$	β	$\mathbf{5.05 \cdot 10^{-5}}$	$\mathbf{5.06 \cdot 10^{-5}}$	$3.17 \cdot 10^{-5}$	$5.34 \cdot 10^{-5}$
	α	$\mathbf{4.37 \cdot 10^{-4}}$	$\mathbf{4.38 \cdot 10^{-4}}$	$5.45 \cdot 10^{-4}$	$4.67 \cdot 10^{-4}$

These values are given for $N = 2^{23}$ and $\tau = \dfrac{p_* + p}{2}$.

Outline

Approximation of the data complexity (1)

Aim: Finding a simple formula to estimate the data complexity.



Fixing T simplifies the problem.

So we take $T = Np_*$ what implies $\alpha \simeq 50\ \%$.

Approximation of the data complexity (2)

$$\boxed{N' = -\frac{1}{D\left(p_*||p\right)}\left[\log\left(\frac{\lambda\beta}{\sqrt{D\left(p_*||p\right)}}\right) + 0.5\log\left(-\log(\lambda\beta)\right)\right],}$$

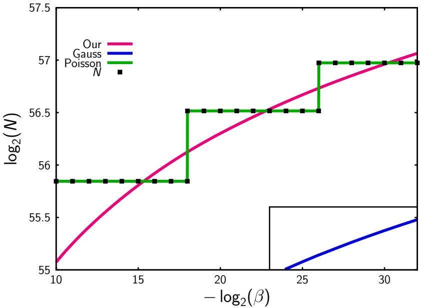
where $\lambda = \frac{(p_* - p)\sqrt{2\pi(1-p_*)}}{(1-p)\sqrt{p_*}}$.

$$\boxed{N' \leq N_\infty \leq N'\left[1 + \frac{(\theta - 1)\log(\theta)}{\log(N')}\right],}$$

with $\theta = \left[1 + \frac{1}{2\log(\lambda\beta)}\log\left(-\frac{\log(\lambda\beta)}{D(p_*||p)}\right)\right]^{-1}$.

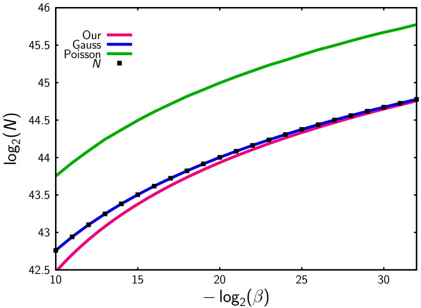
This is a good approximation of N when β tends to 0.

Experimental results (1)



Differential cryptanalysis of DES

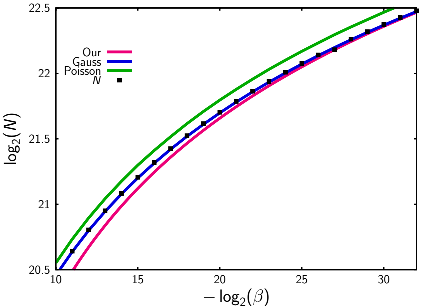
$p_* = 1.87 \cdot 2^{-56},\ p = 2^{-64}$



Linear cryptanalysis of DES

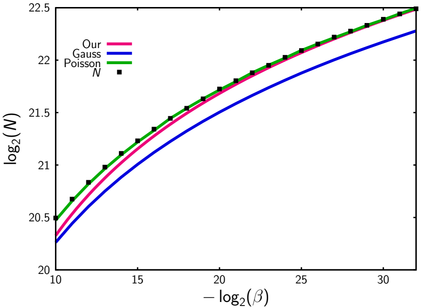
$p_* = 0.5 + 1.19 \cdot 2^{-21},\ p = 0.5$

Experimental results (2)



Truncated differential (1)

$p_* = 1.01 \cdot 2^{-4}$, $p = 2^{-4}$



Truncated differential (2)

$p_* = 1.5 \cdot 2^{-15}$, $p = 2^{-15}$

Outline

Simplified formula for the data complexity

Recall that:

$$N' = -\frac{1}{D\left(p_* || p\right)}\left[\log\left(\frac{\lambda\beta}{\sqrt{D\left(p_* || p\right)}}\right) + 0.5\log\left(-\log(\lambda\beta)\right)\right],$$

Using Taylor series, $\log(2\sqrt{\pi D\left(p_* || p\right)})$ is a good estimate of $\log(\lambda)$.

$$\boxed{N'' = -\frac{\log(2\sqrt{\pi}\beta)}{D\left(p_* || p\right)}.}$$

So comparing the data complexity of two statistical cryptanalyses boils down to comparing the Kullback Leibler divergences of those cryptanalyses.

Behavior of the data complexity for some statistical attacks

Attack	Parameters		Classical results	$\frac{1}{D(p_* \| \| p)}$
Linear	$p = 0.5$	$p_* - p \ll p$	$\frac{1}{(p_* - p)^2}$	$\frac{1}{2(p_* - p)^2}$
Differential	$p_* \ll 1$	$p_* \gg p$	$\frac{1}{p_*}$	$\frac{1}{p_* \log_2(p_*/p) - p_*}$
Differential-linear	$p = 0.5$	$p_* - p \ll p$	$\frac{1}{(p_* - p)^2}$	$\frac{1}{2(p_* - p)^2}$
Truncated differential	$p_* \ll 1$	$p_* - p \ll p$	unknown	$\frac{2p}{(p_* - p)^2}$
Impossible differential	$p_* = 0$	$p \ll 1$	implicitly : $\frac{1}{p}$	$\frac{1}{p}$
k-th order differential	$p_* = 1$	$p \ll 1$	1	$-\frac{1}{\log_2 p}$

Conclusions

We were interested in the Data Complexity of statistical attacks.
This work provides:

- an algorithm to accurately compute the DC;
- an asymptotic formula of the DC;
- the asymptotic behavior of the DC.

Perspectives:

- Key ranking.
- Using an approximation that catches the lattice behavior of the considered random variables.
- Generalizing this work to other distributions than Bernoulli.