Data complexity and success probability of statisticals cryptanalysis

Céline Blondeau

SECRET-Project-Team, INRIA, France

Joint work with Benoît Gérard and Jean-Pierre Tillich

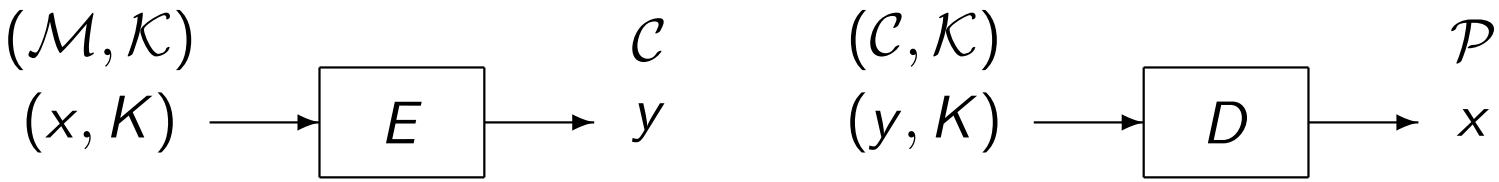
Outline

Outline

Context

We focus on *symmetric cryptography*.

Block Cipher



$$E_K = F_{K_{r+1}} \circ F_{K_r} \cdots \circ F_{K_1}$$

Statistical attack: Use a biased behavior of the cipher in order to find information of the key.

Last round attack: Find information on the last round subkey K_{r+1}.

History

- differential cryptanalysis [Biham Shamir 1990];
- linear cryptanalysis [Matsui 1993];
- truncated differential cryptanalysis [Knudsen 1994];
- higher order differential cryptanalysis [Knudsen 1994];
- impossible differential cryptanalysis [Biham Biryukov Shamir 1999];
- ...

History

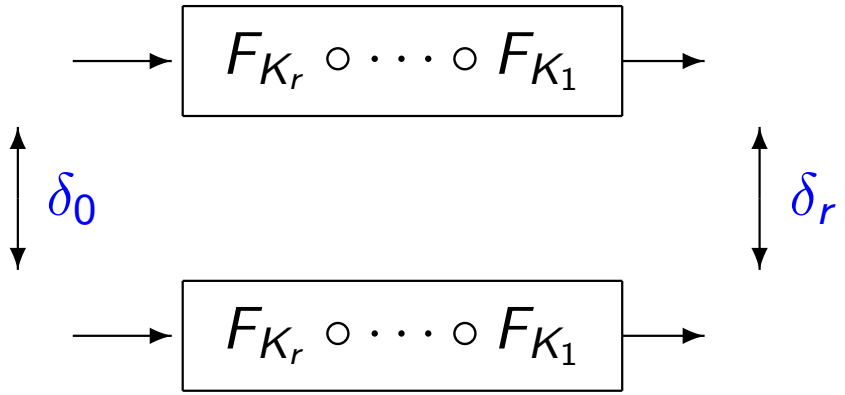
- differential cryptanalysis [Biham Shamir 1990];
- linear cryptanalysis [Matsui 1993];
- truncated differential cryptanalysis [Knudsen 1994];
- higher order differential cryptanalysis [Knudsen 1994];
- impossible differential cryptanalysis [Biham Biryukov Shamir 1999];
- ...
- Multiple linear cryptanalysis[Matsui 1993]
- Multidimensional linear cryptanalysis[Cho Hermelin Nyberg 2008]

History

- differential cryptanalysis [Biham Shamir 1990];
- linear cryptanalysis [Matsui 1993];
- truncated differential cryptanalysis [Knudsen 1994];
- higher order differential cryptanalysis [Knudsen 1994];
- impossible differential cryptanalysis [Biham Biryukov Shamir 1999];
- ...
- Multiple linear cryptanalysis[Matsui 1993]
- Multidimensional linear cryptanalysis[Cho Hermelin Nyberg 2008]
- Multiple differential cryptanalysis

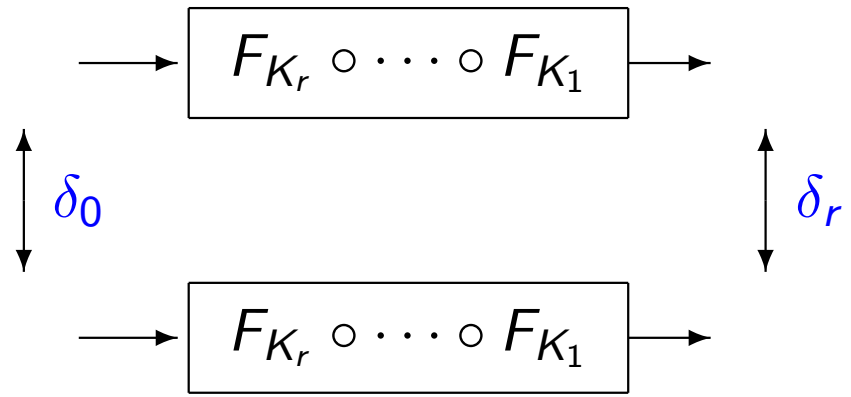
Differential cryptanalysis [Biham-Shamir 1990]

Differential



Differential cryptanalysis [Biham-Shamir 1990]

Differential

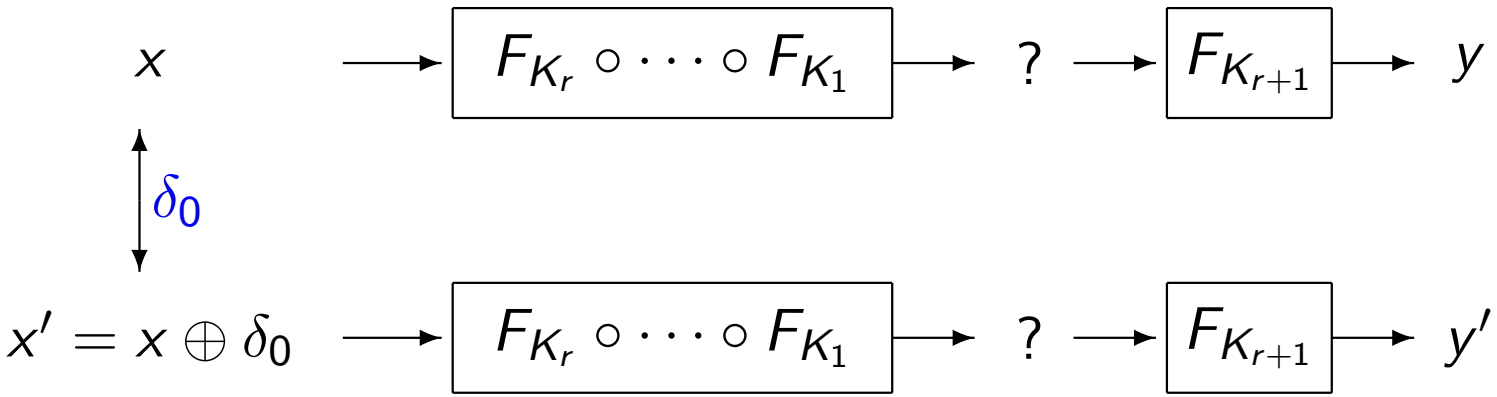


Differential probability

$$\Pr\left[\delta_0 \to \delta_r\right] \stackrel{\text{def}}{=} \Pr_{\mathbf{X},\mathbf{K}}\left[F_K^r(x) \oplus F_K^r(x \oplus \delta_0) = \delta_r\right].$$

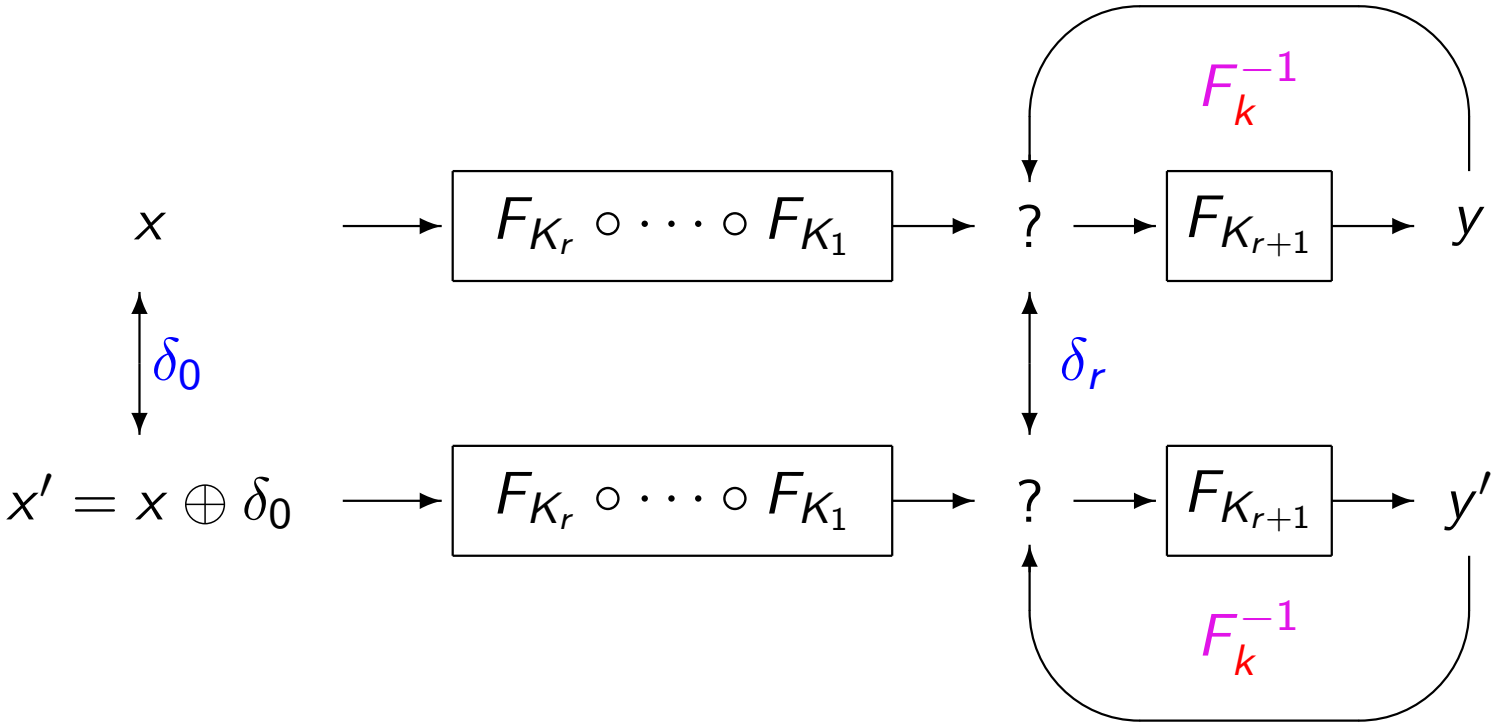
Differential cryptanalysis [Biham-Shamir 1990]

Differential cryptanalysis



Differential cryptanalysis [Biham-Shamir 1990]

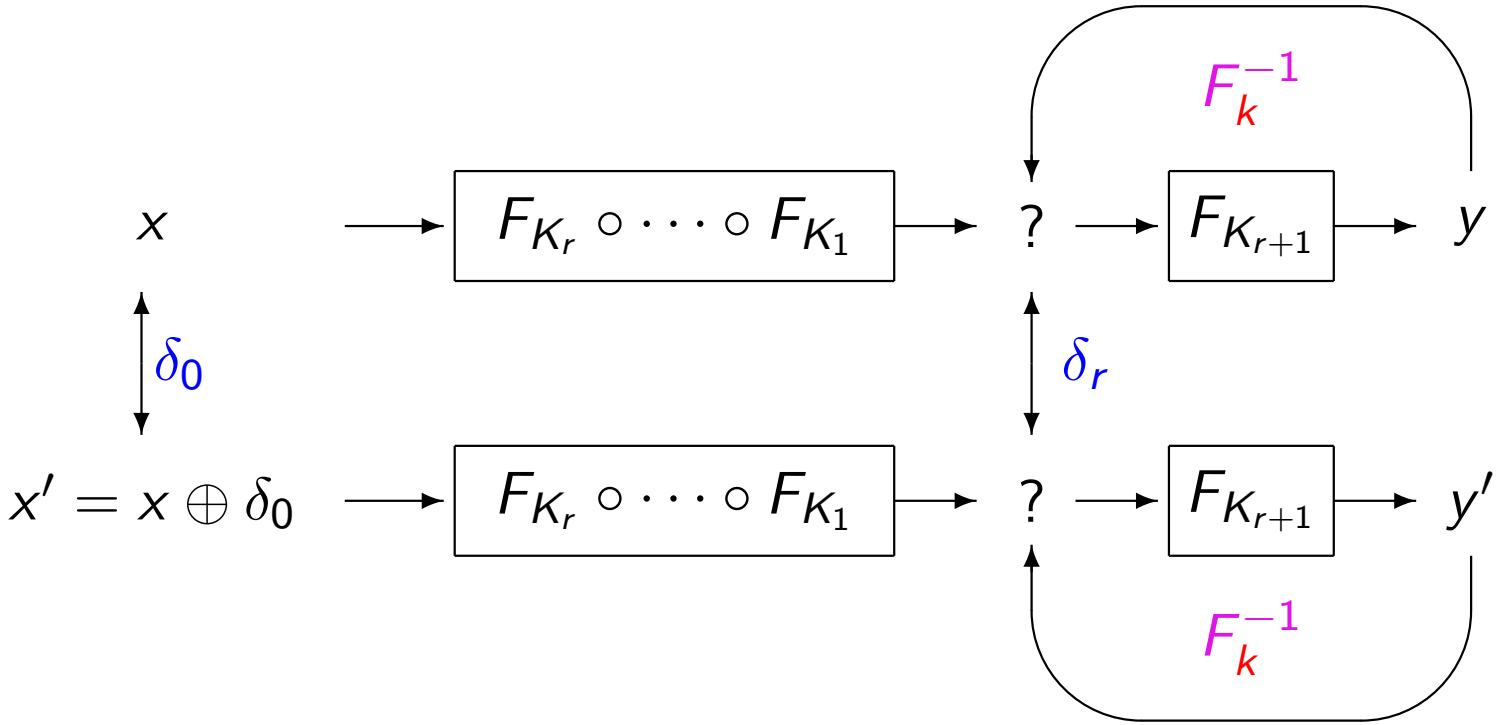
Last round attack



k: last round candidate

Differential cryptanalysis [Biham-Shamir 1990]

Last round attack



Basic Principle:

For each last-round subkey candidate k, compute

$$C(k) = \#\{(y, y') \text{ such that } F_k^{-1}(y) \oplus F_k^{-1}(y') = \delta_r\}$$

Differential cryptanalysis (2)

$$C_x(k) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ if } F_k^{-1}(y) \oplus F_k^{-1}(y') = \delta_r, \\ 0 \text{ otherwise.} \end{cases}$$

$$C(k) \stackrel{\text{def}}{=} \sum_x C_x(k).$$

Wrong key randomization hypothesis

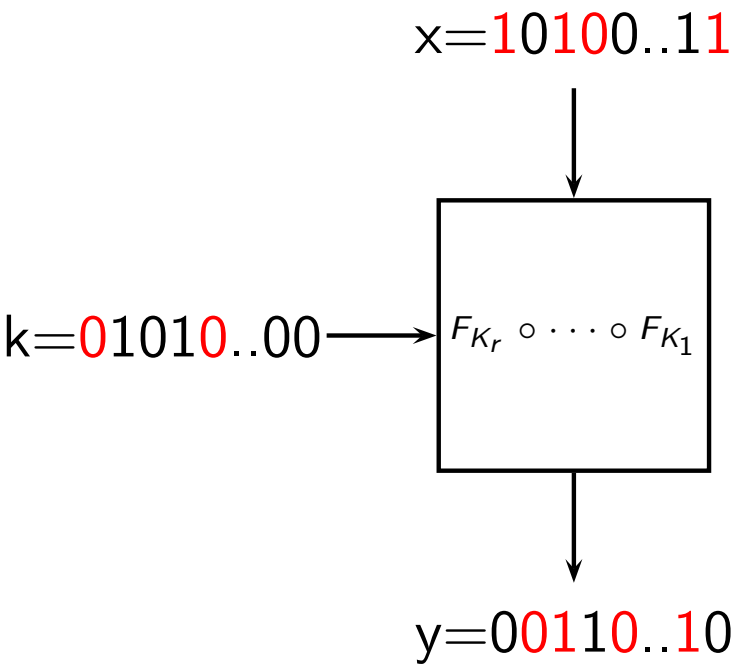
$$\Pr_{\mathbf{x}}\left[F_k^{-1}(y) \oplus F_k^{-1}(y') = \delta_r\right] = \begin{cases} p_* \text{ if } k = K_{r+1}, \\ p \text{ if } k \neq K_{r+1}. \end{cases}$$

Counter

$C_x(k)$ follows a Bernoulli distribution of parameter p_* or p.

$\Rightarrow$ $C(k)$ follows a Binomial distribution.

Linear Cryptanalysis



Approximation of the form:

$$\pi_I(x) \oplus \pi_K(K) = \pi_O(y)$$

Probability of the linear approximation:

$$\frac{1}{2} + \varepsilon \text{ with } \varepsilon \text{ small.}$$

Linear cryptanalysis (Matsui Algorithm 2)

$$C_x(k) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ if } \pi_O(F_k^{-1}(y)) + \pi_I(x) + \pi_K(k) = 0 \\ 0 \text{ otherwise.} \end{cases}$$

$$C(k) \stackrel{\text{def}}{=} \sum_x C_x(k).$$

Hypothesis

$$\Pr_{\mathbf{x}}\left[\pi_O(F_k^{-1}(y)) + \pi_I(x) + \pi_K(k)\right] = \begin{cases} p_* = \frac{1}{2} + \varepsilon \text{ if } k = K_{r+1}, \\ p = \frac{1}{2} \quad \text{if } k \neq K_{r+1}. \end{cases}$$

Counters

$C_x(k)$ follows a Bernoulli distribution of parameter p_* or p.

$\Rightarrow$ $C(k)$ follows a Binomial distribution.

Statistical attacks: the phases

1. Distillation phase: some statistic Σ is extracted from the available data

$$(\Sigma \text{ correspond to some counter } C(k))$$

2. Analysis phase: from Σ, the likelihood of each possible subkey is computed and a list $\mathcal{L}$ of the likeliest keys is suggested

$$(\text{Sort the counter})$$

3. Search phase: for each subkey in $\mathcal{L}$, all the possible corresponding master keys are exhaustively tried until the good one is found.

Problematic

Important quantities in statistical cryptanalysis:

- Data Complexity :

  N: Number of elementary unit

- P_S: Success Probability
- n: Number of last round candidate
- $\ell = \#\mathcal{L}$: Size of the list of kept keys (exhaustive search)

Aim: Evaluate the data complexity, the success probability and relate both quantities.

Problem: Hard to do with binomial law.

Previous work: differential cryptanalysis

Poisson Approximation of Binomial Tails

$$P\left[C(k) \leq T\right] \simeq \sum_{i=0}^{T} e^{-Np} \cdot \frac{(Np)^i}{i!}$$

Implicitly used in differential cryptanalysis:

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

But ...

... not accurate for some pN. For instance, when pN is too big as in linear cryptanalysis.

Previous work: Linear Cryptanalysis

Gaussian Approximation of Binomial Tails

$$P\left[C(k) \leq T\right] \simeq \int_{-\infty}^{T/N} \frac{1}{\sqrt{2\pi Np(1-p)}} \cdot e^{-\frac{N(x-p)^2}{2p(1-p)}} dx$$

Classically used in linear cryptanalysis:

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

But...

... not accurate for some pN. For instance, when pN is too small as in differential cryptanalysis [Selçuk 08].

Simple statistical attack

Large variation of p_* and p depending of the attack.

Attacks	p	p_*
Differential cryptanalysis	2^{-m}	λp with big λ
Truncated differential cryptanalysis	2^{-t}	λp with small λ
Impossible differential cryptanalysis	2^{-t}	0
Higher order differential cryptanalysis	2^{-t}	1
Linear cryptanalysis	$1/2$	$1/2 + \varepsilon$
Differential Linear cryptanalysis	$1/2$	$1/2 + \varepsilon$

$\Rightarrow$ Counters follows a binomial law.

Good Approximation of Binomial Tails

Binomial tail:

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

Theorem

$$P(C(k) \leq N\tau) \underset{N\to\infty}{\sim} \frac{p\sqrt{1-\tau}}{(p-\tau)\sqrt{2\pi N\tau}} \cdot 2^{-N\cdot Kull(\tau||p)}.$$

Where the *Kullback-Leibler divergence* is defined by:

$$Kull(p||q) \stackrel{\text{def}}{=} p\log_2\left(\frac{p}{q}\right) + (1-p)\log_2\left(\frac{1-p}{1-q}\right).$$

Comparison

		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	$\mathbf{9.29 \cdot 10^{-5}}$	$1.46 \cdot 10^{-4}$	$\mathbf{9.23 \cdot 10^{-5}}$	$9.90 \cdot 10^{-5}$
	α	$\mathbf{9.80 \cdot 10^{-5}}$	$1.55 \cdot 10^{-4}$	$\mathbf{9.89 \cdot 10^{-5}}$	$1.04 \cdot 10^{-4}$
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	$\mathbf{4.37 \cdot 10^{-4}}$	$\mathbf{4.38 \cdot 10^{-4}}$	$5.45 \cdot 10^{-4}$	$4.67 \cdot 10^{-4}$

Outline

Paradigm

Fixed threshold (T)

$$\mathcal{L} = \{k_i, C(k_i) > T\}.$$

- $\alpha \stackrel{\text{def}}{=} \Pr[K_{r+1} \notin \mathcal{L}]$.
- $\beta \stackrel{\text{def}}{=} \Pr[k \neq K_{r+1}, k \in \mathcal{L}]$.

Fixed size of list (ℓ)

$$\ell \stackrel{\text{def}}{=} \#\mathcal{L},$$
$$k \in \mathcal{L}, k' \notin \mathcal{L} \Rightarrow C(k) > C(k')$$

- $P_S \stackrel{\text{def}}{=} \Pr[K_{r+1} \in \mathcal{L}]$.
- ℓ/n: ratio of kept keys.

Paradigm

Fixed threshold (T)

$$\mathcal{L} = \{k_i, C(k_i) > T\}.$$

- $\alpha \stackrel{\text{def}}{=} \Pr[K_{r+1} \notin \mathcal{L}]$.
- $\beta \stackrel{\text{def}}{=} \Pr[k \neq K_{r+1}, k \in \mathcal{L}]$.

$\Rightarrow$ Data complexity

Fixed size of list (ℓ)

$$\ell \stackrel{\text{def}}{=} \#\mathcal{L},$$
$$k \in \mathcal{L}, k' \notin \mathcal{L} \Rightarrow C(k) > C(k')$$

- $P_S \stackrel{\text{def}}{=} \Pr[K_{r+1} \in \mathcal{L}]$.
- ℓ/n: ratio of kept keys.

$\Rightarrow$ Success probability

Fixed threshold method

Neyman-Pearson (optimal) test:

Accept a candidate k if

$$\frac{P(C_{x_1}(k), C_{x_2}(k), \ldots, C_{x_N}(k)|k = K_{r+1})}{P(C_{x_1}(k), C_{x_2}(k), \ldots, C_{x_N}(k)|k \neq K_{r+1})} > t.$$

This (likelihood) ratio only depends on $C(k) = \sum_{i=1}^{N} C_{x_i}(k)$, p_* and p and is increasing in $C(k)$. Thus, the acceptance condition becomes, for some threshold $0 < T < N$,

$$\text{If } C(k) \geq T \text{ then } k \in \mathcal{L} \text{ else } k \notin \mathcal{L}$$

Error probabilities

- **Non-detection error probability**

$$P(K_{r+1} \notin \mathcal{L}) = P(C(K_{r+1}) < T) \underset{N\to\infty}{\sim} \frac{p_* \sqrt{1-\tau}}{(p_* - \tau)\sqrt{2\pi N \tau}} 2^{-N\ Kull(\tau||p_*)};$$

- **False alarm error probability** $k \neq K_{r+1}$

$$P(k \in \mathcal{L}) = P(C(k) \geq T) \underset{N\to\infty}{\sim} \frac{(1-p)\sqrt{\tau}}{(\tau - p)\sqrt{2\pi N(1-\tau)}} 2^{-N\ Kull(\tau||p)}.$$

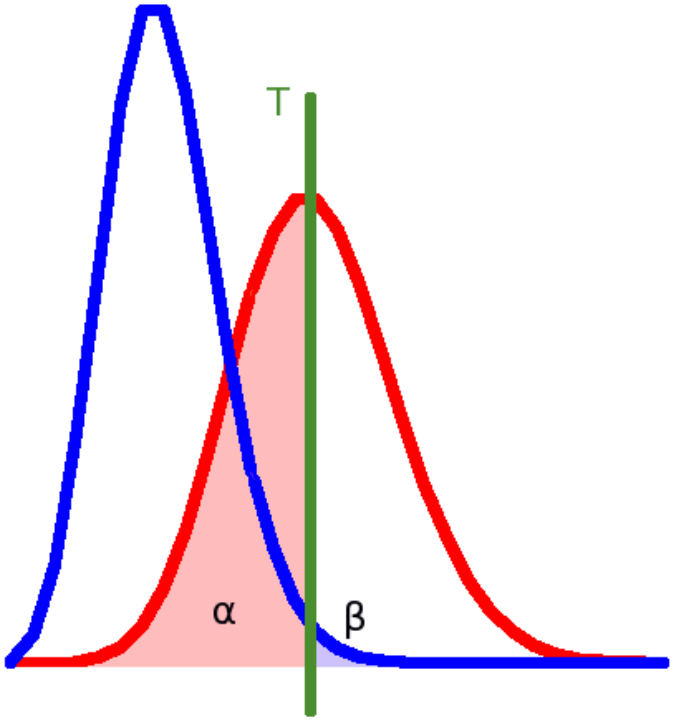
$$\tau \stackrel{\text{def}}{=} T/N\text{: Relative threshold}$$

Aim

Finding N minimal such that it exists T such that $P(C(K_{r+1}) < T) \leq \alpha$ and $P(C(k) \geq T,\ k \neq K_{r+1}) \leq \beta$ for given values of α and β.

Approximation of the data complexity (1)

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



Fixing $\tau = p_*$ simplifies the problem.

Thus α is close to 50%.

Approximation of the data complexity (2)

$$\beta = \frac{(1-p)\sqrt{p_*}}{(p_*-p)\sqrt{2\pi N(1-p_*)}} 2^{-N\ Kull(p_*||p)}.$$

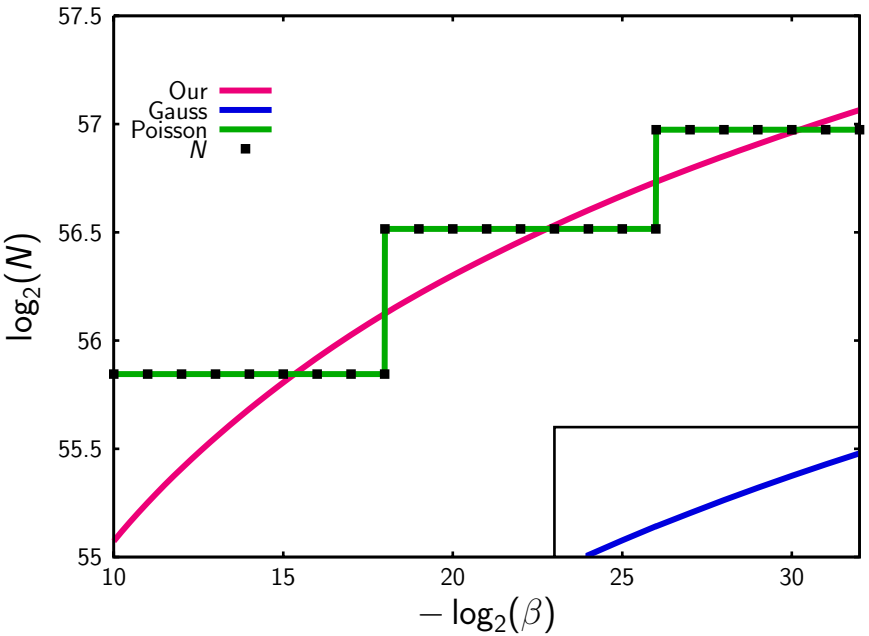
$$N = f(N) = -\frac{\log(\lambda\beta\sqrt{N})}{Kull(p_*||p)} \qquad \text{where } \lambda = \frac{(p_*-p)\sqrt{2\pi(1-p_*)}}{(1-p)\sqrt{p_*}}.$$

$$N_{i+1} = f(N_i),\ N_1 = \frac{1}{Kull(p_*||p)}$$

Theorem

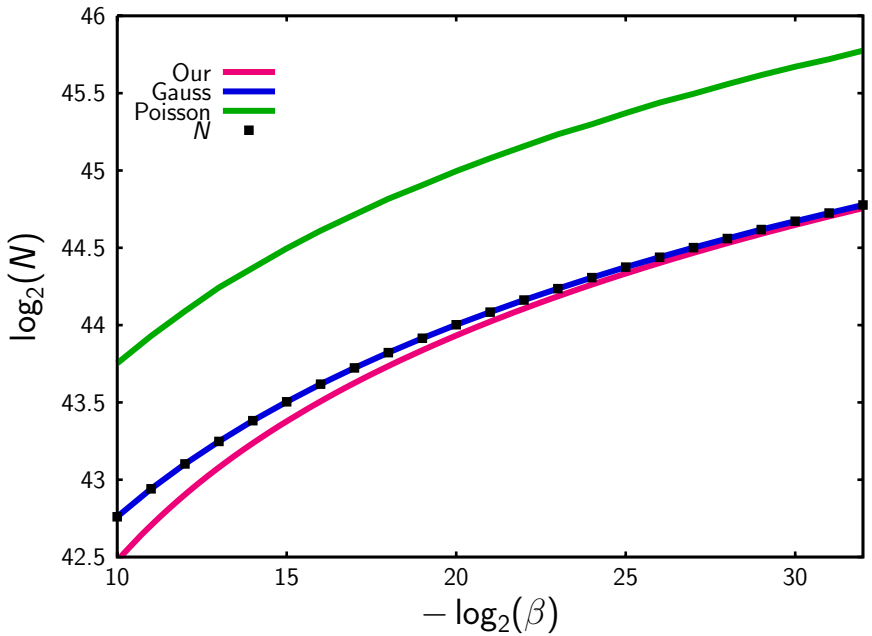
$$N_2 = N' = -\frac{1}{Kull(p_*||p)}\left[\log\left(\frac{\lambda\beta}{\sqrt{Kull(p_*||p)}}\right) + 0.5\log\left(-\log(\lambda\beta)\right)\right]$$

Experimental results (1)



Differential cryptanalysis of DES

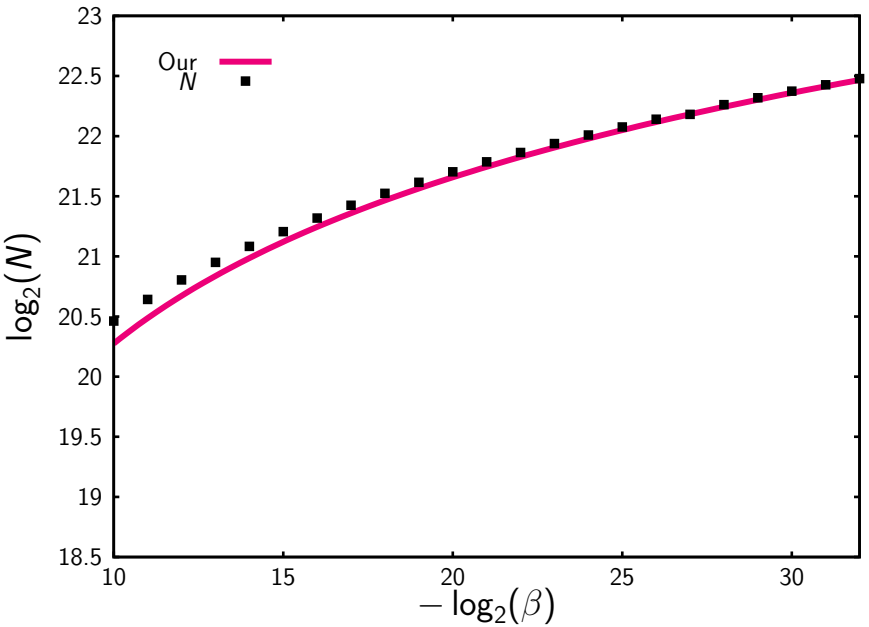
$p_* = 1.87 \cdot 2^{-56}$, $p = 2^{-64}$



Linear cryptanalysis of DES

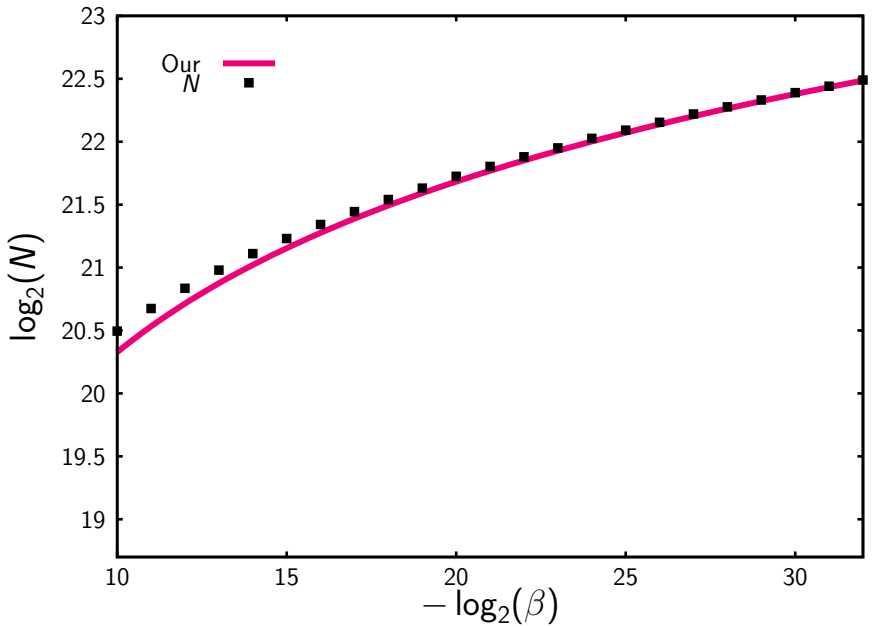
$p_* = 0.5 + 1.19 \cdot 2^{-21}$, $p = 0.5$

Experimental results (2)



Truncated differential (1)

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



Truncated differential (2)

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

Simplified formula for the data complexity

Recall that:

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

Using Taylor series, $\frac{1}{\sqrt{Kull(p_*||p)}} \approx \frac{2\sqrt{\pi}}{\lambda}$.

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

Behavior of the data complexity for statistical attacks (1)

Attack	Classical results	$\frac{1}{Kull(p_* \| \| p)}$
Linear	$\frac{1}{2(p_* - p)^2}$	$\frac{1}{2(p_* - p)^2}$
Differential	$\frac{1}{p_*}$	$\frac{1}{p_* \log_2(p_*/p) - p_*}$
Differential-linear	$\frac{1}{2(p_* - p)^2}$	$\frac{1}{2(p_* - p)^2}$

Behavior of the data complexity for statistical attacks (2)

Attack	Classical results	$\frac{1}{Kull(p_* \| \| p)}$
Truncated differential	unknown	$\frac{2p}{(p_* - p)^2}$
Impossible differential	implicitly: $\frac{1}{p}$	$\frac{1}{p}$
k-th order differential	1	$-\frac{1}{\log_2 p}$

Success probability (order statistics)

We have n possible candidates:

- $k_0 = K_{r+1}$, the correct one;
- $k_1, \ldots, k_{n-1}$.

For all random variables, $C(k_j) \sim \begin{cases} \mathcal{B}(N, p_*) \text{ if } j = 0, \\ \mathcal{B}(N, p) \text{ if } j \neq 0. \end{cases}$

$$P_s = P(K_{r+1} \in \mathcal{L})$$

Order statistic tools

We want to keep a list $\mathcal{L}$ of size ℓ which contains the most likely candidates.

$$\forall k \notin \mathcal{L}, \quad \forall k' \in \mathcal{L} \qquad C(k) < C(k')$$

We sort $C(k_1), \ldots, C(k_{n-1})$ in decreasing order $\rightarrow D(k_1), \ldots D(k_{n-1})$.

$$P_S = P[K_{r+1} \in \mathcal{L}] = P[D(k_\ell) < C(K_{r+1})].$$

Success probability

Without approximation:

$$C(K_{r+1}) \sim \mathcal{B}(N, p_*), \qquad k \neq K_{r+1} \quad C(k) \sim \mathcal{B}(N, p).$$

Let G be the be the cumultative function of the binomial law.

$$P_S \approx \sum_{i=G^{-1}(1-(\ell-1)/(n-2))}^{N} P[C(K_{r+1}) = i].$$

Where

$$G^{-1}(y) \stackrel{\text{def}}{=} \min_{x \in \mathbb{N}} \{P[C(k \neq K_{r+1}) \leq x] \geq y\}.$$

Comparison

[Selçuk 08]: Using a normal approximation:

$$P_S \approx P(\widetilde{C}(K_{r+1}) > \tau) \quad \text{where} \quad P(\widetilde{C}(k) < \tau) = 1 - \frac{\ell}{n}.$$

Without approximation:

$$P_S \approx P(C(K_{r+1}) > \tau) \quad \text{where} \quad P(C(k) < \tau) = 1 - \frac{\ell - 1}{n - 2}.$$

Experimental results and comparison with Selçuk

Type of cryptanalysis	Parameters $N = 2^{48}$ $2^{n_K} = 2^{20}$	Experimental results	Ours	Selçuk
Linear	$\ell = 2^{15}$	**86.81**	86.81	86.81
Linear	$\ell = 2^{10}$	**45.33**	45.33	45.33
Differential	$\ell = 2^{15}$	**82.57**	82.47	90.50
Differential	$\ell = 2^{10}$	**82.50**	82.47	90.50

Linear: $p = 0.5$ and $p_* = 0.5 + 1.49 \cdot 2^{-24}$

Differential: $p = 2^{-64}$ and $p_* = 2^{-47.2}$

Outline

Previous works

Previous works using many differentials:

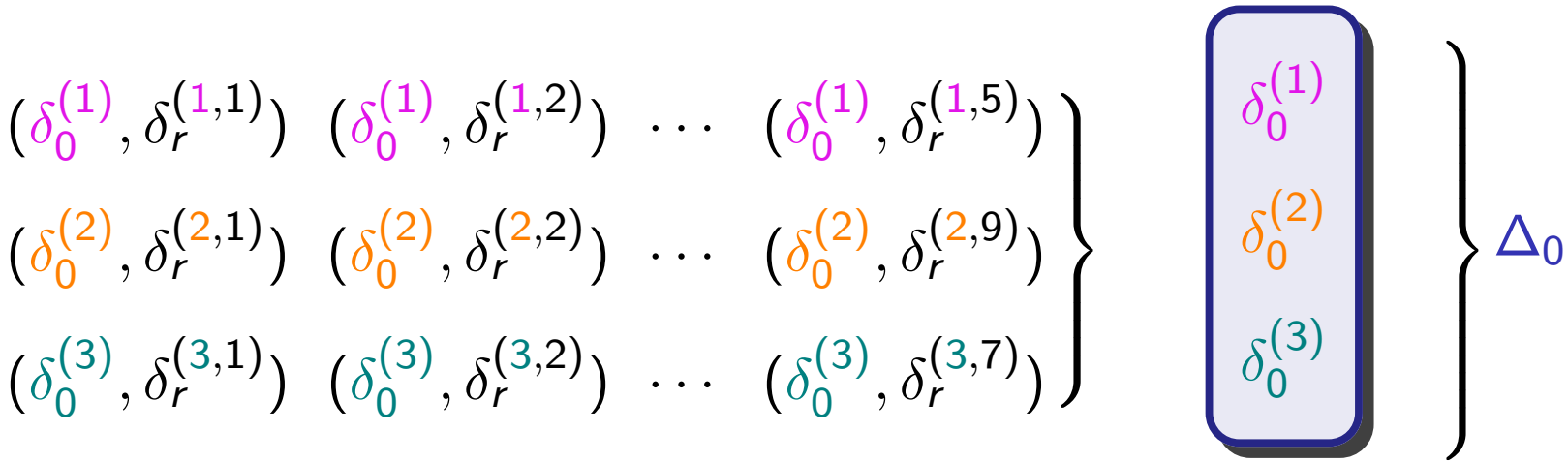
[Biham Shamir 1990]
Collection of differentials with same output difference.

[Knudsen 1994]
Collection of differentials with same input difference.

[Sugita et al. 2000]
Same set of output differences for each input difference.

Multiple differential cryptanalysis

Collection of differentials



Multiple differential cryptanalysis

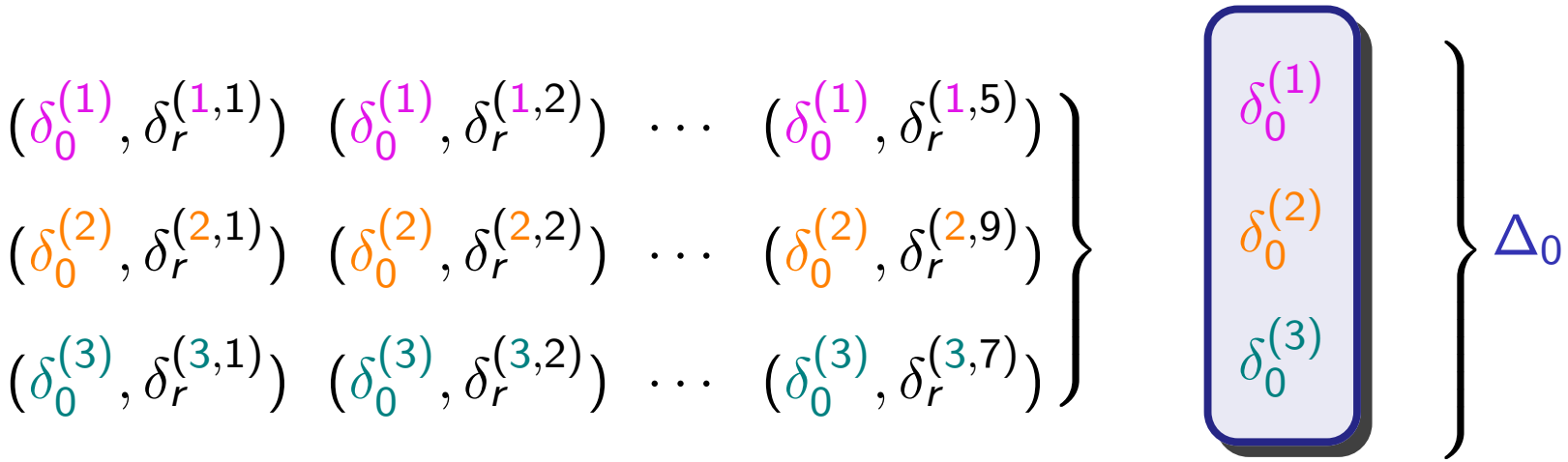
Collection of differentials

$$\left.\begin{array}{llll} (\delta_0^{(1)}, \delta_r^{(1,1)}) & (\delta_0^{(1)}, \delta_r^{(1,2)}) & \cdots & (\delta_0^{(1)}, \delta_r^{(1,5)}) \\ (\delta_0^{(2)}, \delta_r^{(2,1)}) & (\delta_0^{(2)}, \delta_r^{(2,2)}) & \cdots & (\delta_0^{(2)}, \delta_r^{(2,9)}) \\ (\delta_0^{(3)}, \delta_r^{(3,1)}) & (\delta_0^{(3)}, \delta_r^{(3,2)}) & \cdots & (\delta_0^{(3)}, \delta_r^{(3,7)}) \end{array}\right\} \quad \left.\begin{array}{l} \delta_0^{(1)} \\ \delta_0^{(2)} \\ \delta_0^{(3)} \end{array}\right\} \Delta_0$$

$p_*^{(i,j)}$: Probability of the differential $(\delta_0^{(i)}, \delta_r^{(i,j)})$

Multiple differential cryptanalysis

Collection of differentials



$p_*^{(i,j)}$: Probability of the differential $(\delta_0^{(i)}, \delta_r^{(i,j)})$

$\Delta_r^{(i)}$: Set of output differences for the i-th input difference.

Δ_0: Set of input differences.

The counters

$$C_x^{(i)}(k) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ if } F_k^{-1}\big(E_{K_*}(x)\big) \oplus F_k^{-1}\big(E_{K_*}(x \oplus \delta_0^{(i)})\big) \in \Delta_r^{(i)}, \\ 0. \end{cases}$$

$$C_x(k) \stackrel{\text{def}}{=} \sum_{i=1}^{\#\Delta_0} C_x^{(i)}(k) \qquad \text{and} \qquad C(k) \stackrel{\text{def}}{=} \sum_x C_x(k).$$

$C_x^{(i)}(k)$ follows a Bernoulli distribution of parameter $p_*^{(i)}$ or $p^{(i)}$ where

$$p_*^{(i)} = \sum_{j=1}^{\#\Delta_r^{(i)}} p_*^{(i,j)} \quad \text{and} \quad p^{(i)} = \#\Delta_r^{(i)} \cdot 2^{-m}.$$

What is the distribution of $C(k)$?

Poisson approximation

[Le Cam 1960]:

Let $C_x^{(i)}(k)$ be some independent Bernoulli random variables with probability $p^{(i)}$. Then $C_x(k) \stackrel{\text{def}}{=} \sum_{i=1}^{\#\Delta_0} C_x^{(i)}(k)$ follows a distribution close to a Poisson distribution of parameters $\lambda = \sum_{i=1}^{\#\Delta_0} p^{(i)}$.

$$C(K_{r+1}) \underset{approx}{\sim} \mathcal{P}\left(N \sum_{i=0}^{\#\Delta_0} p_*^{(i)}\right) \quad , \quad C(k) \underset{approx}{\sim} \mathcal{P}\left(N \sum_{i=0}^{\#\Delta_0} p^{(i)}\right).$$

The cumulative function $G_{\mathcal{P}}$ is not a good estimate for the tails of the distribution of the counters !!!

Tails of the cumulative functions

$$p_* \stackrel{\text{def}}{=} \frac{\sum_i p_*^{(i)}}{\#\Delta_0} \quad \text{and} \quad p \stackrel{\text{def}}{=} \frac{\sum_i p^{(i)}}{\#\Delta_0}$$

Using [Gallager 1968]:

$$G_-(\tau, q) \stackrel{\text{def}}{=} \Pr\left[C(k) \leq \tau \#\Delta_0 N\right] \approx e^{-\#\Delta_0 \cdot N \cdot Kull(\tau||q)} \cdot \left[\frac{q\sqrt{(1-\tau)}}{(q-\tau)\sqrt{2\pi\tau\#\Delta_0 N}} + \frac{1}{\sqrt{8\pi\tau\#\Delta_0 N}}\right]$$

Where $q = p_*$ or p.

$$Kull(\tau||q) = \tau \log\left(\frac{\tau}{q}\right) + (1-\tau)\log\left(\frac{1-\tau}{1-q}\right).$$

Data complexity

Before, the data complexity is computed by approximating one tail of binomial cumulative function with:

$$1 - e^{-N \cdot Kull(\tau||p))} \frac{(1-p)\sqrt{\tau}}{(\tau-p)\sqrt{2\pi N(1-\tau)}}.$$

Data complexity

Here one tail of the cumulative function of the counters is:

$$G_+(\tau, p) \approx 1 - e^{-\#\Delta_0 N \cdot Kull(\tau||p))} \left[\frac{(1-p)\sqrt{\tau}}{(\tau - p)\sqrt{2\pi N(1-\tau)}} + \frac{1}{\sqrt{8\pi \#\Delta_0 N \tau}} \right].$$

Data complexity

Here one tail of the cumulative function of the counters is:

$$G_+(\tau, p) \approx 1 - e^{-\#\Delta_0 N \cdot Kull(\tau||p))} \left[\frac{(1-p)\sqrt{\tau}}{(\tau-p)\sqrt{2\pi N(1-\tau)}} + \frac{1}{\sqrt{8\pi \#\Delta_0 N\tau}} \right].$$

With similar arguments, the data complexity is

$$N \approx -2 \cdot \frac{\ln(2\sqrt{\pi}\ell/n)}{\#\Delta_0 Kull(p_*||p)}.$$

Where:

- n: Number of subkey,
- ℓ: Size of the list of kept candidates.

Success probability

Success probability:

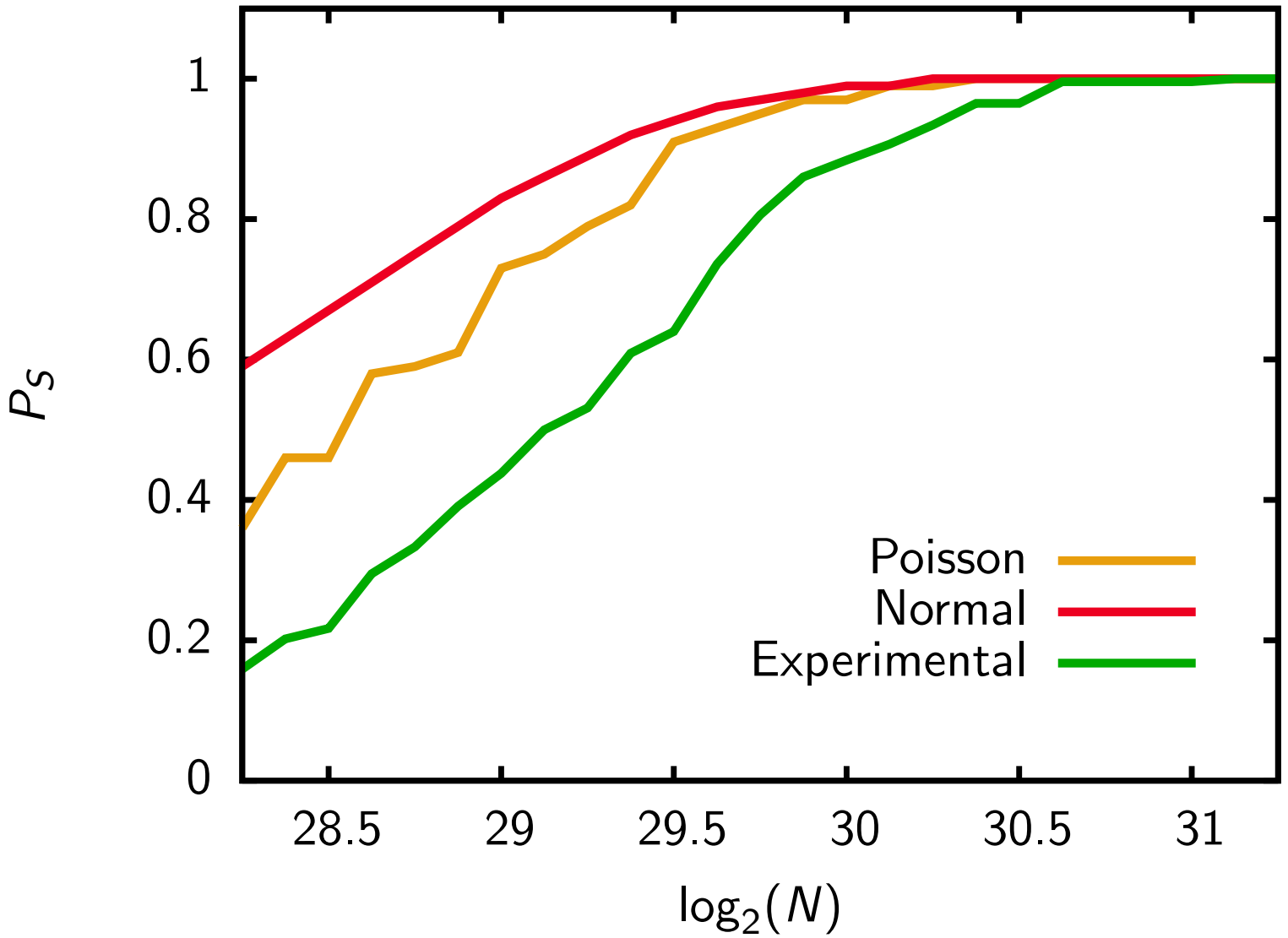
$$P_s \approx 1 - G_* \left[G^{-1} \left(1 - \frac{\ell - 1}{n - 2} \right) - 1 \right],$$

where G and G_* are the cumulative functions of the distribution of the random variables.

For G and G_* we can take:

- Normal distribution ([Selçuk2007])
- Poisson distribution (First Idea)

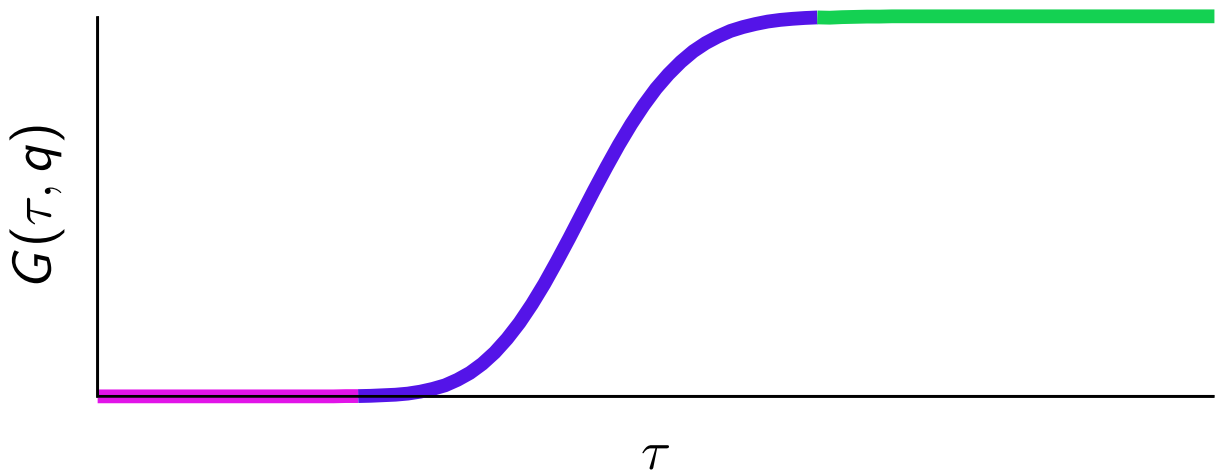
Experiments on SMALLPRESENT-[8]



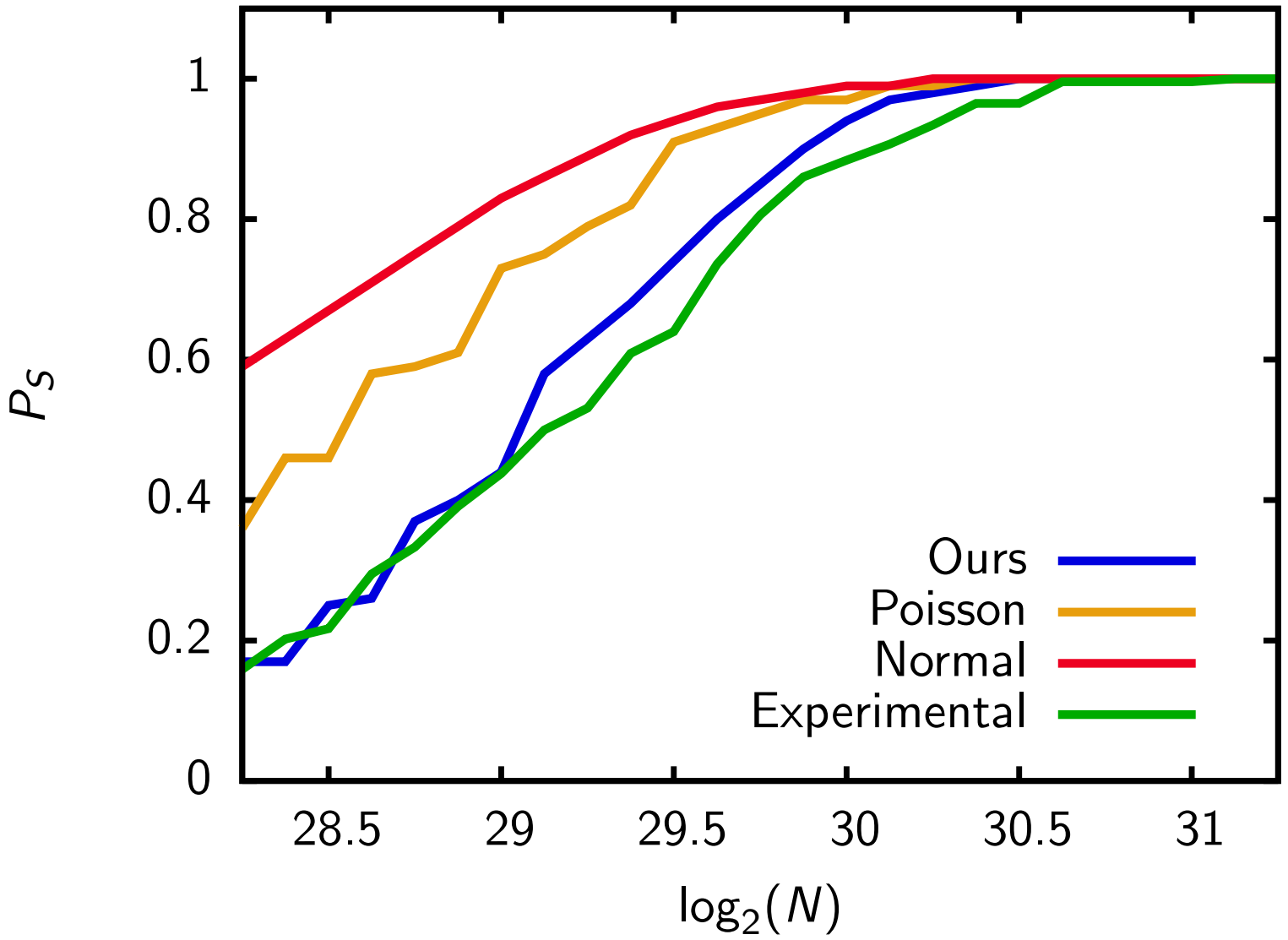
Distribution of the counters

We use the following estimate for the cumulative function of the $C(k)$'s:

$$G(x,q) = \begin{cases} G_-(x,q) \text{ if } x < q - 3\cdot\sqrt{q/N}, \\ G_+(x,q) \text{ if } x > q + 3\cdot\sqrt{q/N}, \\ G_{\mathcal{P}}(x,q) \text{ otherwise.} \end{cases} \qquad \begin{array}{l} G_*(x) = G(x,p_*) \\ G(x) = G(x,p) \end{array}$$



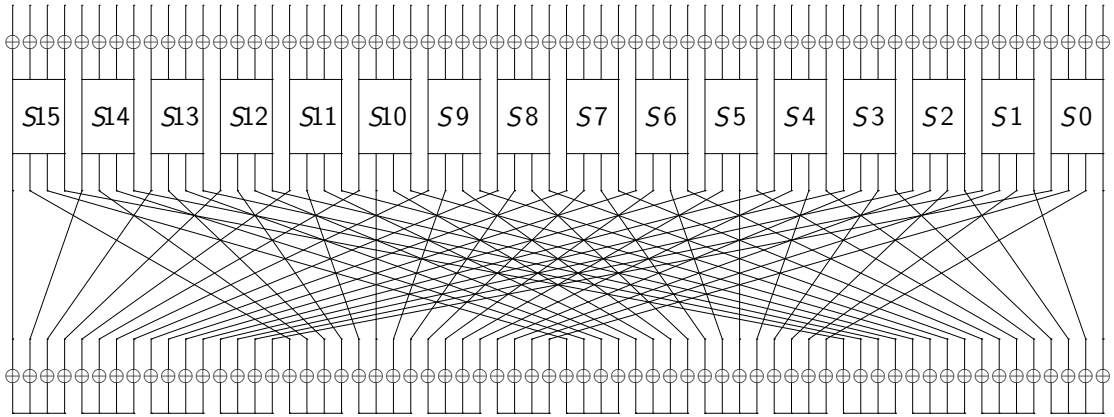
Experiments on SMALLPRESENT-[8]



PRESENT [Bogdanov et al. 2007]

PRESENT:

- Plaintext: 64 bits
- Key: 80 bits
- Rounds: 31



Multidimensional linear attack [Cho 2010]:

- Rounds: 26
- Data complexity: $2^{64.0}$
- Time complexity: $2^{72.0}$
- Memory complexity: $2^{32.0}$

Differential Attack [Wang 2008]:

- Rounds: 16
- Data complexity: $2^{64.0}$
- Time complexity: $2^{64.0}$
- Memory complexity: $2^{32.0}$

Attack on PRESENT

Setting:

- Differentials on 16 rounds $\Rightarrow$ attack on 18 rounds.
- $\#\Delta_0 = 16, \quad \#\Delta_r^{(i)} = 33, \quad \#\Delta_{sieve} \approx 2^{32}$.
- $p_* = 2^{-58.52}$ and $p = 2^{-58.96}$.

Attack:

N	ℓ	P_S	time complexity
2^{60}	2^{51}	76%	$2^{79.00}$
2^{62}	2^{47}	81%	$2^{75.04}$
2^{64}	2^{36}	94%	$2^{71.72}$

Conclusions

Conclusions

We have computed accurate formulas of the:

- Data complexity and success probability of simple statistical attacks;
- Data complexity and success probability of multiple differential cryptanalysis.

Perspectives

- Apply multiple differential cryptanalysis on other block ciphers.
- Improve multiple differential cryptanalysis.