# Statistical cryptanalyses of symmetric-key algorithms

Benoît Gérard

supervised by Jean-Pierre Tillich

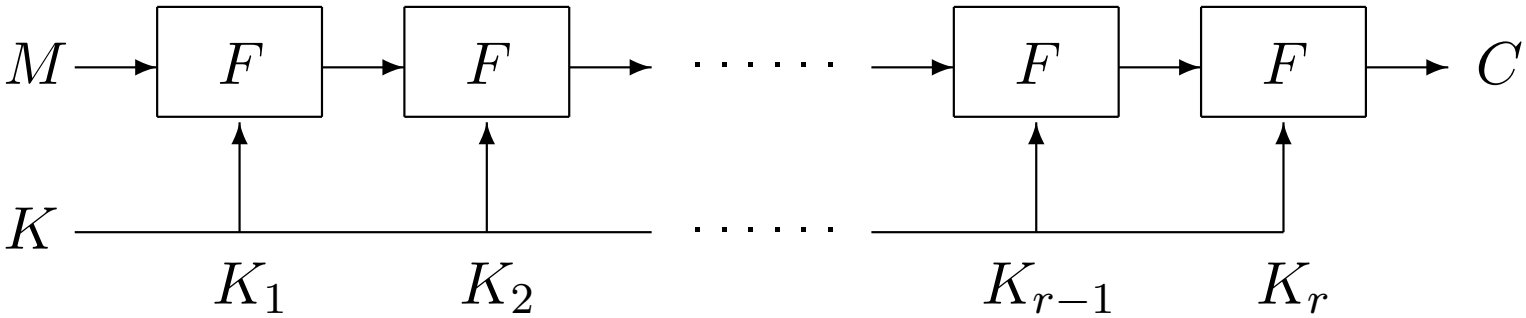


Thesis defense

-

December 9, 2010

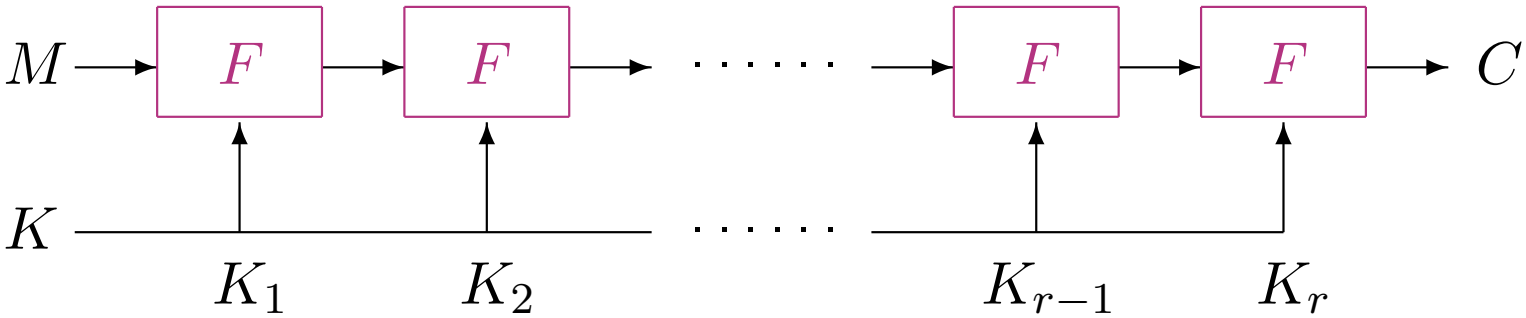
# Iterative block ciphers




- $K$: master key.
- $F$: round function.
- $K_i$: round sub-keys.

$$\begin{aligned} E_K : \mathbb{F}_2^s &\rightarrow \mathbb{F}_2^s \\ M &\mapsto C = E_K(M) = F_{K_r} \circ \cdots \circ F_{K_1}(M). \end{aligned}$$

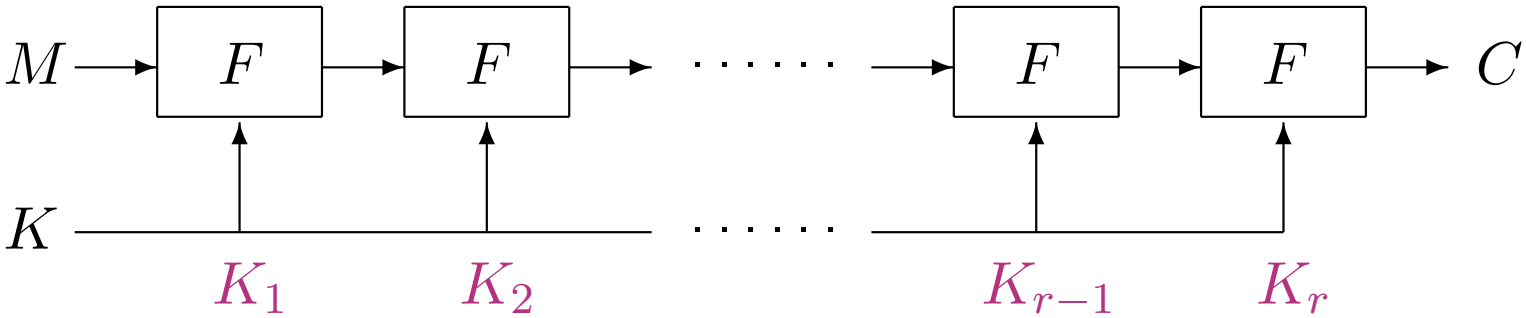
# Iterative block ciphers




- $K$: master key.
- $F$: round function.
- $K_i$: round sub-keys.

$$\begin{aligned} E_K : \mathbb{F}_2^s &\rightarrow \mathbb{F}_2^s \\ M &\mapsto C = E_K(M) = F_{K_r} \circ \cdots \circ F_{K_1}(M). \end{aligned}$$

# Iterative block ciphers

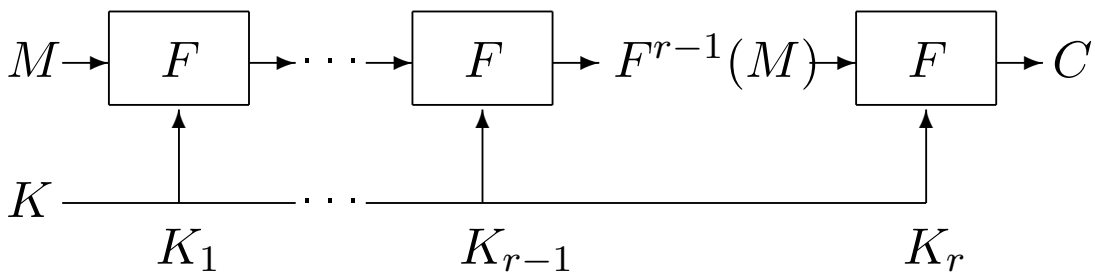



- $K$: master key.
- $F$: round function.
- $K_i$: round sub-keys.

$$\begin{aligned} E_K : \mathbb{F}_2^s &\to \mathbb{F}_2^s \\ M &\mapsto C = E_K(M) = F_{K_r} \circ \cdots \circ F_{K_1}(M). \end{aligned}$$

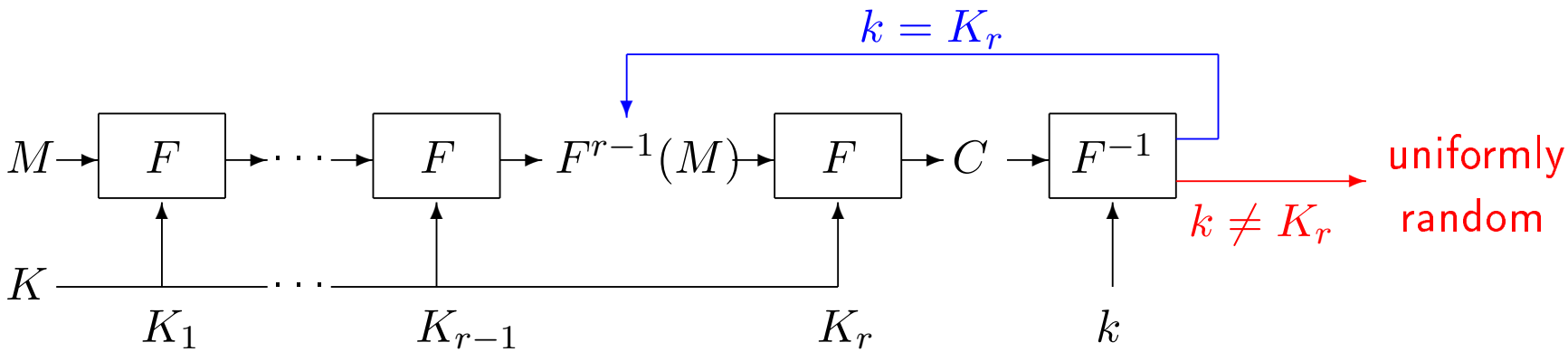
# Last round attack

1. Find a non-ideal behavior of $r-1$ rounds of the cipher.



# Last round attack

1. Find a non-ideal behavior of $r-1$ rounds of the cipher.
2. For every possible candidate $k$ for $K_r$
   - Decipher ciphertexts by one round $F$ using $k$.
   - Generate the corresponding statistic (generally a counter).
3. Order the candidates regarding their likelihood.
4. Test all the master keys that correspond to the best candidate and so on ...




Wrong key randomization hypothesis (W.K.R.H.).

# Statistical cryptanalyses: notation

- $N$ is the number of samples available to the attacker.
- $k^*$ is the correct value of the subkey we are interested in.
- $n_{key}$ the number of bits of $k^*$.
- $\Sigma_k$ is the counter extracted from samples for a candidate $k$.

Concerning the time complexity.

- Only stop when the key is recovered.
- Keeping a list $\mathcal{L}$ of the likeliest candidates for the final search.

$$P_S \stackrel{\text{def}}{=} \Pr\left[k^* \in \mathcal{L}\right].$$

- Defining a criterion to determine candidates to keep.
- Fixing the size of the list $\ell = |\mathcal{L}|$.

# Issues

Analyzing the efficiency of a statistical cryptanalysis.

- data complexity: $N$.
- success probability: $P_S$.
- time complexity: related to $\ell$.
- Each quantity is determined by the two others.

One would like to quantify the tradeoff between them *i.e.*

- Expressing $P_S$ as a function of $N$ and $\ell$.
- Expressing $N$ as a function of $P_S$ and $\ell$.

# Summary

# Model

- A non-ideal statistical behavior of the cipher has been found: statistical characteristic.
- From this characteristic and the samples, one is able to compute a counter $\Sigma_k$ for each candidate.

**Model**

$$\Sigma_k \sim \begin{cases} \mathcal{B}in\,(N, p_*) & \text{if } k = k^*, \\ \mathcal{B}in\,(N, p) & \text{otherwise.} \end{cases}$$

# Linear cryptanalysis: Matsui's Algorithm 2

- Non-ideal behavior:

$$\Pr_{M,K}\left[\langle \pi, M\rangle \oplus \langle \gamma, F_K^{r-1}(M)\rangle = 0\right] = \frac{1}{2} + \varepsilon.$$

$$p_* = \frac{1}{2} + \varepsilon \quad \text{and} \quad p = \frac{1}{2}.$$

- Statistics extracted from $N$ known plaintext/ciphertext pairs $(m^i, c^i)$:

$$\Sigma_k = \sum_{i=1}^{N} \langle \pi, m^i\rangle \oplus \langle \gamma, F_k^{-1}(c^i)\rangle.$$

- Criterion for ordering candidates:

$$\left|\frac{\Sigma_k}{N} - \frac{1}{2}\right|.$$

# Analysis

Typical values for a 64-bit cipher ($s = 64$):

$$p_* = \frac{1}{2} + 2^{-32} \quad \text{and} \quad p = \frac{1}{2}.$$

In this domain, the Gaussian approximation for the binomial distribution is tight.

- ✓ In [Matsui 1993]: $N = \mathcal{O}\left(1/\varepsilon^2\right)$.
- ✓ In [Junod 2001]: a precise formula for the distribution of the rank of $k^*$.
- ✓ In [Selçuk 2008]:

$$P_S \approx \Phi\left(2\sqrt{N}|\varepsilon| + \Phi^{-1}\left(1 - \frac{\ell}{2^{n_{key}+1}}\right)\right).$$

# Differential cryptanalysis

- Non-ideal behavior:

$$\Pr_{M,K}\left[F_K^{r-1}(M) \oplus F_K^{r-1}(M \oplus \delta_1) = \delta_2\right] = p_*.$$

$$p_* > 2^{-s} \quad \text{and} \quad p = \frac{1}{2^s - 1} \approx 2^{-s}.$$

- Statistics extracted from $N$ ciphertexts $(c_1^i, c_2^i)$ corresponding to chosen plaintexts $(m_1^i, m_2^i)$ with difference $\delta_1$:

$$\Sigma_k^i = \begin{cases} 1 & \text{if } F_k^{-1}(c_1^i) \oplus F_k^{-1}(c_2^i) = \delta_2 \\ 0 & \text{otherwise.} \end{cases}$$

- Criterion for ordering candidates:

$$\Sigma_k = \sum_{i=1}^{N} \Sigma_k^i.$$

# Analysis

Typical values for $s = 64$:

$$p_* = 2^{-60} \quad \text{and} \quad p = 2^{-64}.$$

In this domain, the Poisson approximation for the binomial distribution is tight.

✓ [Biham, Shamir 1990]: for $p_*$ sufficiently larger than $2^{-s}$,

$$N = \mathcal{O}\left(1/p_*\right).$$

x In [Selçuk 2008],

$$P_S \approx \Phi\left(\frac{\sqrt{Np_*^2/p} - \Phi^{-1}(1 - \frac{\ell}{2^{n_{key}}})}{\sqrt{1 + p_*/p}}\right).$$

# Truncated differential cryptanalysis

- Non-ideal behavior:

$$\Pr_{M,K}\left[F_K^{r-1}(M) \oplus F_K^{r-1}(M \oplus \delta) \in \Delta_2 \middle| \, \delta \in \Delta_1\right] = p_*.$$

$$p_* > |\Delta_2| \cdot 2^{-s} \quad \text{and} \quad p = \frac{|\Delta_2|}{2^s - 1} \approx |\Delta_2| \cdot 2^{-s}.$$

- Statistics extracted from $N$ ciphertexts $(c_1^i, c_2^i)$ corresponding to chosen plaintexts $(m_1^i, m_2^i)$ with difference in $\Delta_1$:

$$\Sigma_k^i = \begin{cases} 1 & \text{if } F_k^{-1}(c_1^i) \oplus F_k^{-1}(c_2^i) \in \Delta_2 \\ 0 & \text{otherwise.} \end{cases}$$

- Criterion for ordering candidates:

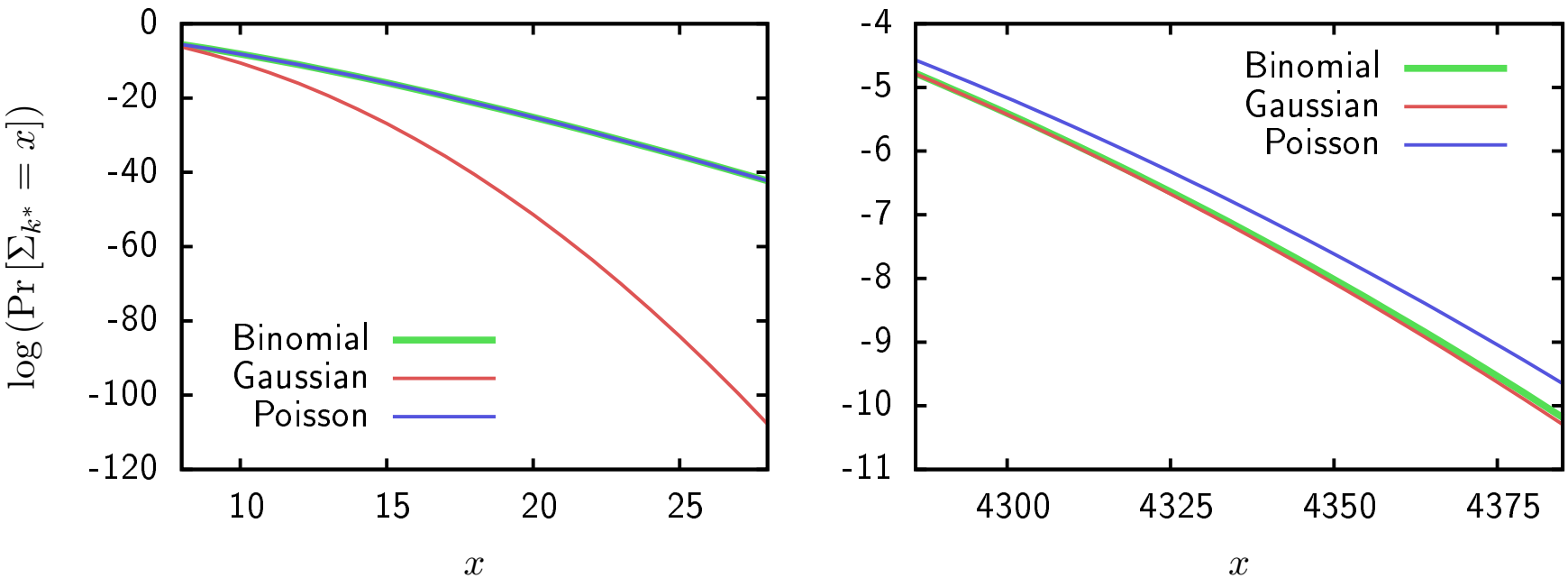
$$\Sigma_k = \sum_{i=1}^{N} \Sigma_k^i.$$

# Analysis

No typical values for probabilities since it depends on $|\Delta_2|$.

$$\left(2^{-60}, 2^{-64}\right) \quad , \quad \left(2^{-15.8}, 2^{-16}\right) \quad , \quad \left(0.5 + 2^{-32}, 0.5\right).$$

Both the Poisson and the Gaussian approximations may not be valid.

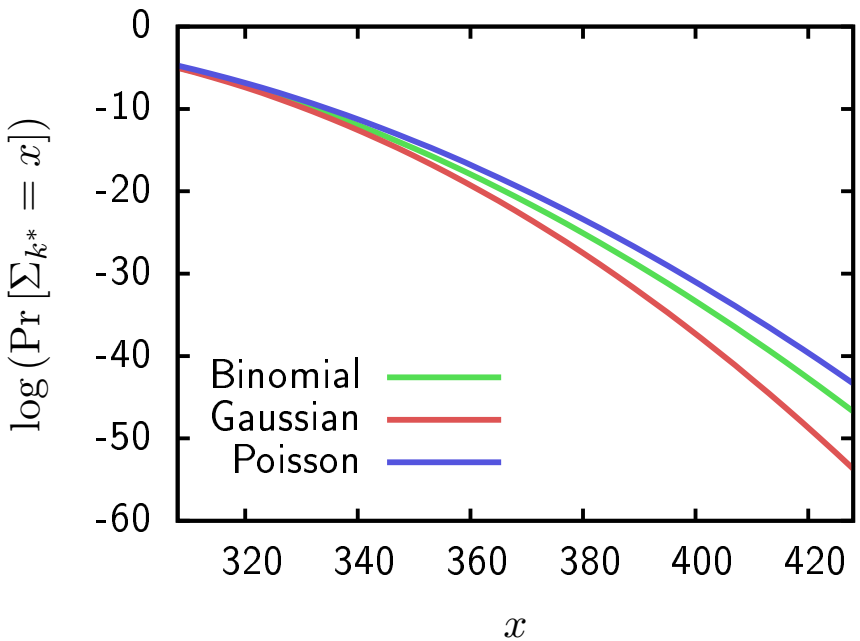


# Analysis

No typical values for probabilities since it depends on $|\Delta_2|$.

$$\left(2^{-60}, 2^{-64}\right) \quad , \quad \left(2^{-15.8}, 2^{-16}\right) \quad , \quad \left(0.5 + 2^{-32}, 0.5\right).$$

Both the Poisson and the Gaussian approximations may not be valid.



# Approximating the tails of the binomial distribution

## Main tool (folklore)

Supposing that $\Sigma_k \sim \mathcal{B}in\,(N,p)$, then, for $\tau < p$,

$$\Pr\left[\Sigma_k \leq \tau N\right] \underset{N\to\infty}{\sim} \frac{p\sqrt{1-\tau}}{(p-\tau)\sqrt{2\pi N\tau}} \cdot e^{-ND(\tau||p)},$$

and, for $\tau > p$,

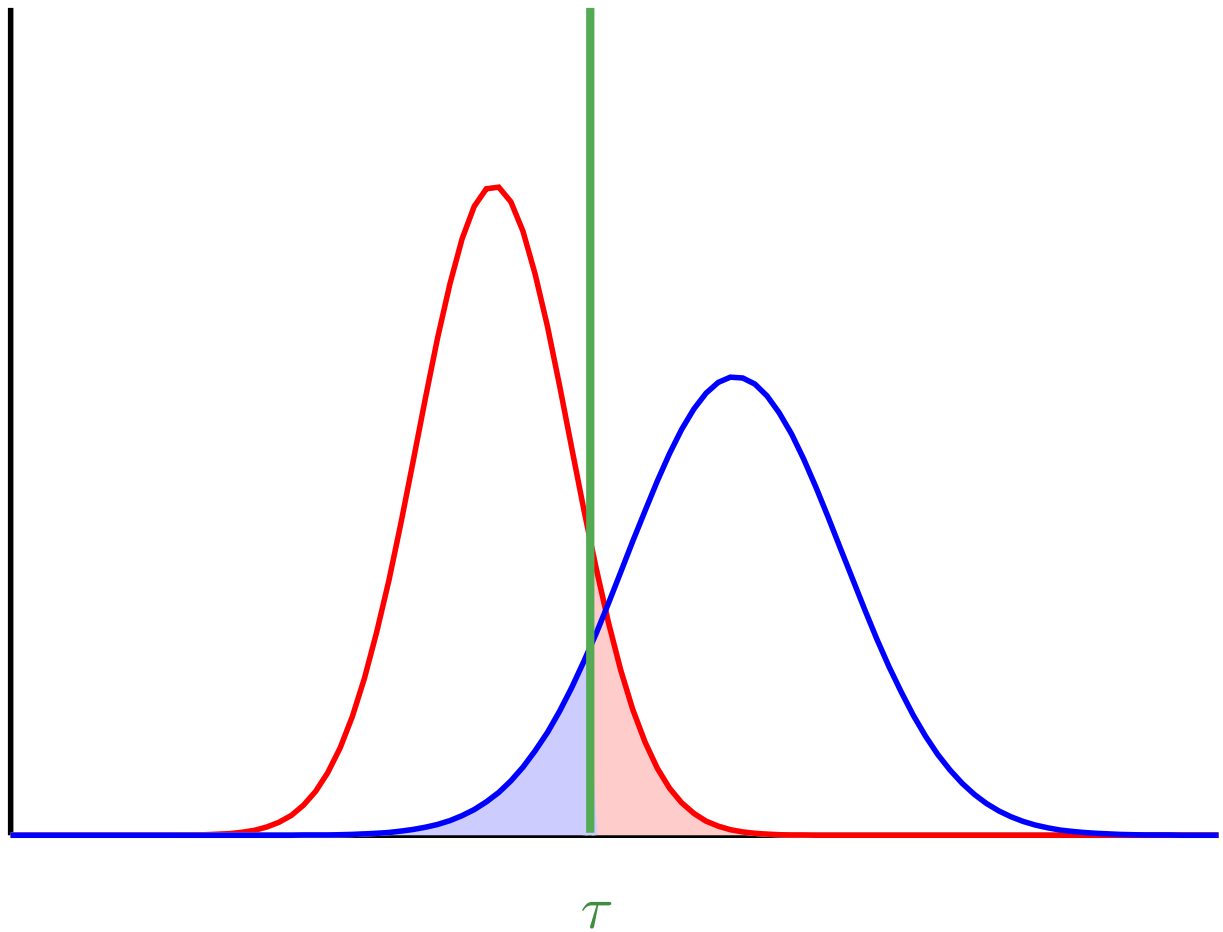
$$\Pr\left[\Sigma_k \geq \tau N\right] \underset{N\to\infty}{\sim} \frac{(1-p)\sqrt{\tau}}{(\tau-p)\sqrt{2\pi N(1-\tau)}} \cdot e^{-ND(\tau||p)}.$$

The Kullback-Leibler divergence:

$$D\,(a||b) \stackrel{\text{def}}{=} a \cdot \ln\left(\frac{a}{b}\right) + (1-a) \cdot \ln\left(\frac{1-a}{1-b}\right).$$

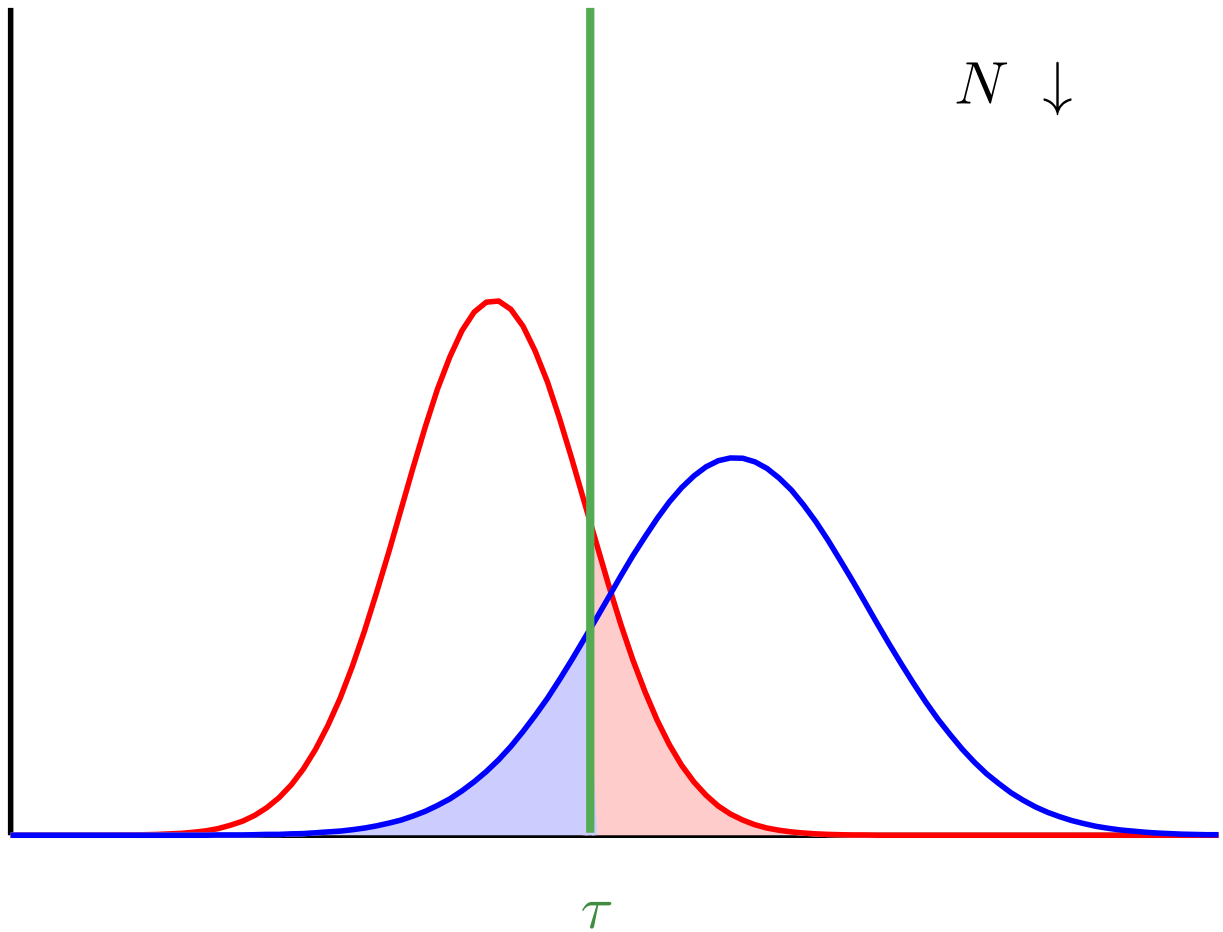
# Data complexity (1/2)

$$\Pr\left[\Sigma_{k^*} < \tau\, N\right] \leq \alpha \quad , \quad \Pr\left[\Sigma_k \geq \tau\, N\right] \leq \beta.$$



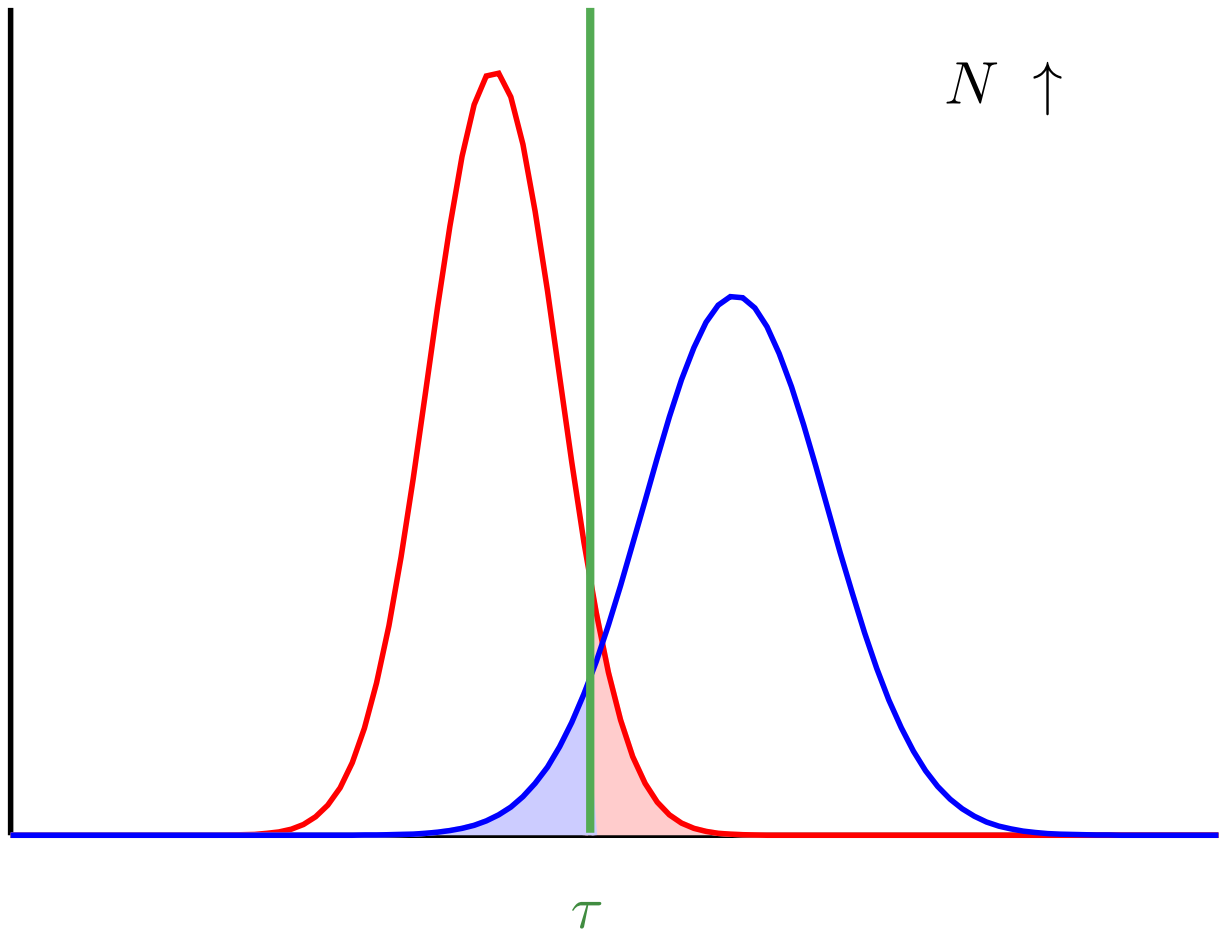
# Data complexity (1/2)

$$\Pr\left[\Sigma_{k^*} < \tau\, N\right] \leq \alpha \quad , \quad \Pr\left[\Sigma_k \geq \tau\, N\right] \leq \beta.$$



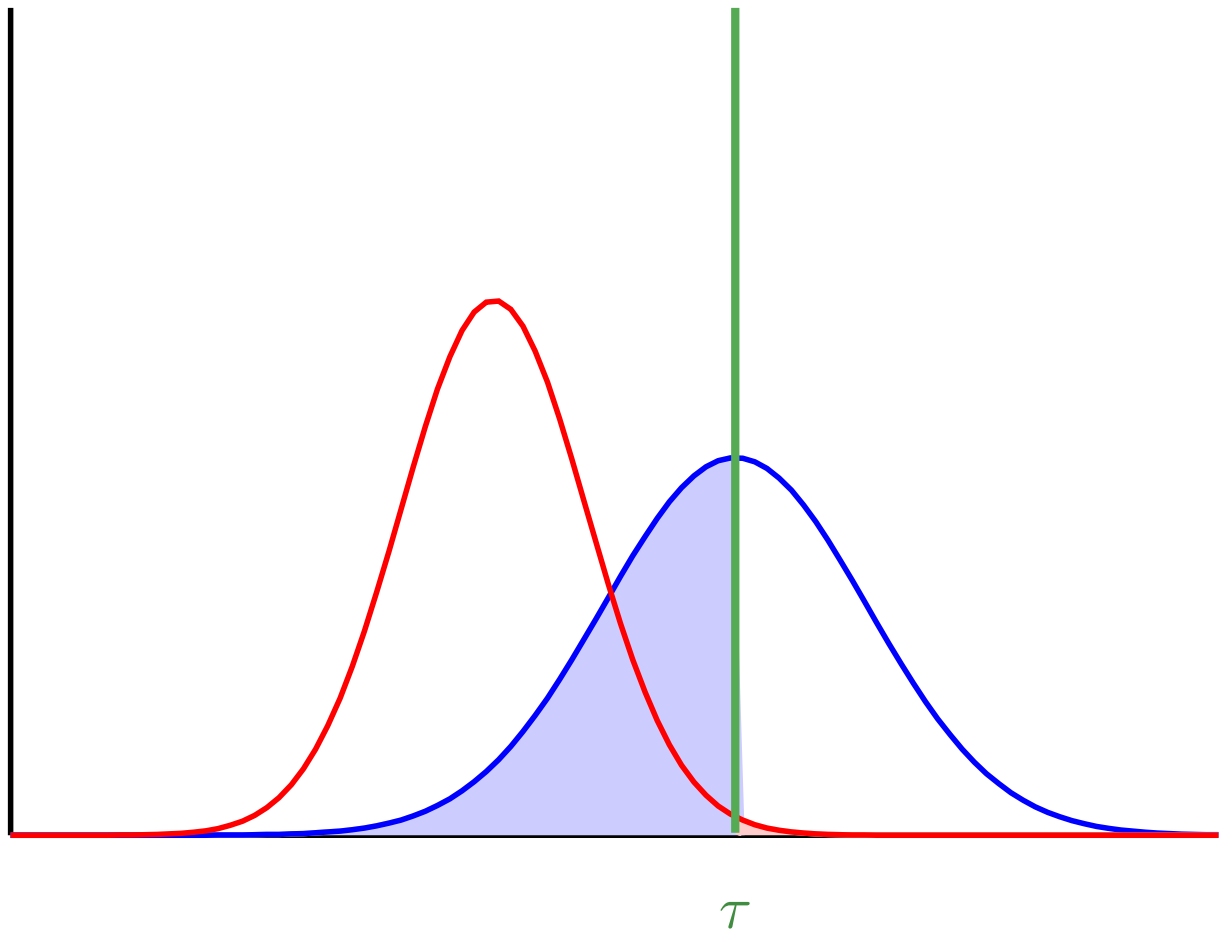
# Data complexity (1/2)

$$\Pr\left[\Sigma_{k^*} < \tau\, N\right] \leq \alpha \quad , \quad \Pr\left[\Sigma_k \geq \tau\, N\right] \leq \beta.$$



# Data complexity (1/2)

$$\Pr\left[\Sigma_{k^*} < \tau\, N\right] \leq \alpha \quad , \quad \Pr\left[\Sigma_k \geq \tau\, N\right] \leq \beta.$$



# Data complexity (2/2)

## Estimates for N [Blondeau, G. 2009]

Two estimates for the data complexity of a simple statistical cryptanalysis with success probability close to 0.5 are

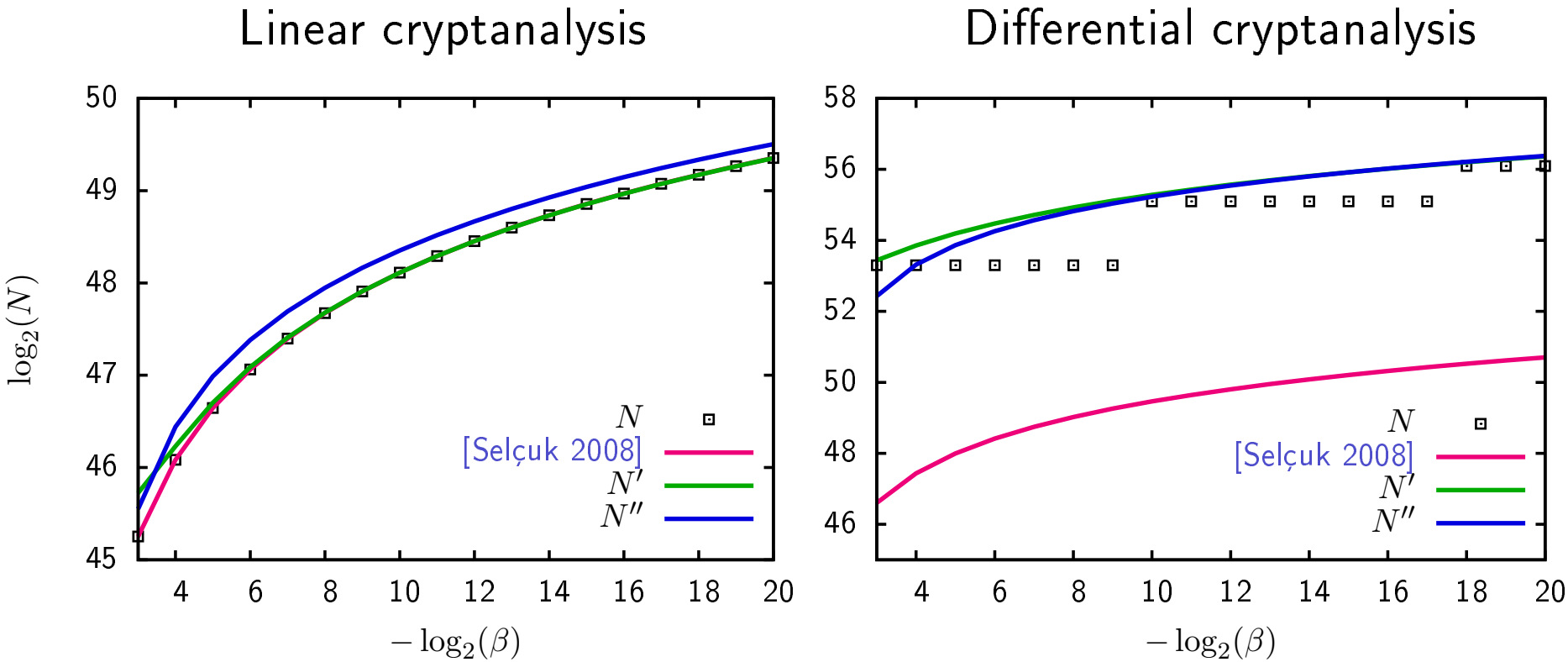
$$N' \stackrel{\text{def}}{=} -\frac{1}{D\left(p_*||p\right)}\left[\ln\left(\frac{\lambda\,\beta}{\sqrt{D\left(p_*||p\right)}}\right)+\frac{1}{2}\ln\left(-\ln\left(\frac{\lambda\,\beta}{\sqrt{D\left(p_*||p\right)}}\right)\right)\right],$$

and

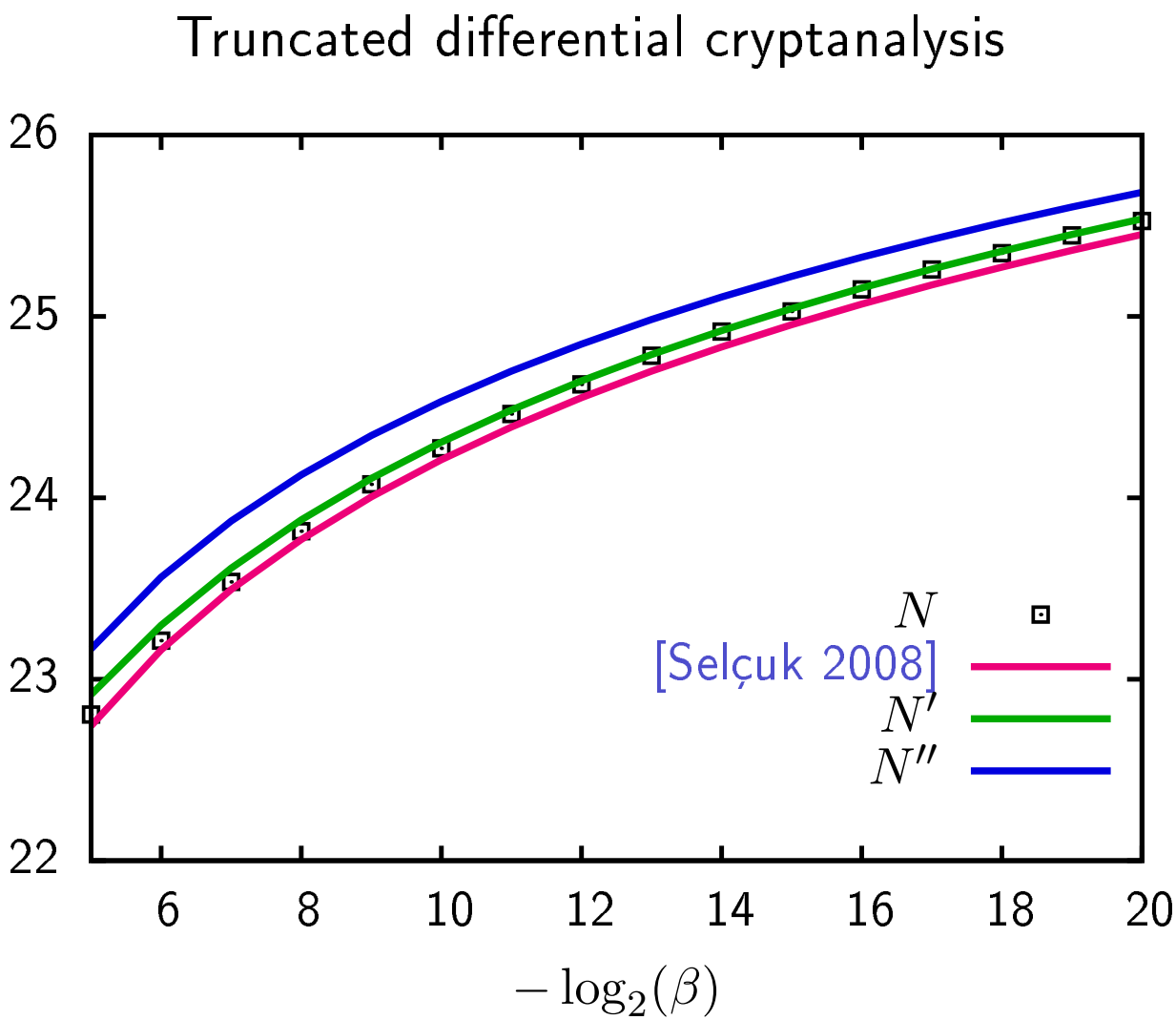
$$N'' \stackrel{\text{def}}{=} -\frac{\ln\left(2\sqrt{\pi}\beta\right)}{D\left(p_*||p\right)}.$$

Bounds on error made using $N'$ and $N''$ guarantee their accuracy.

# Empirical accuracy of the estimates



# Empirical accuracy of the estimates



# Fixing the list size

We gave estimates of $N$

- for $P_S = 1 - \alpha \approx 0.5$,
- function of $\beta$: proportion of kept candidates.

Now, we fix the list size $|\mathcal{L}| = \ell$.

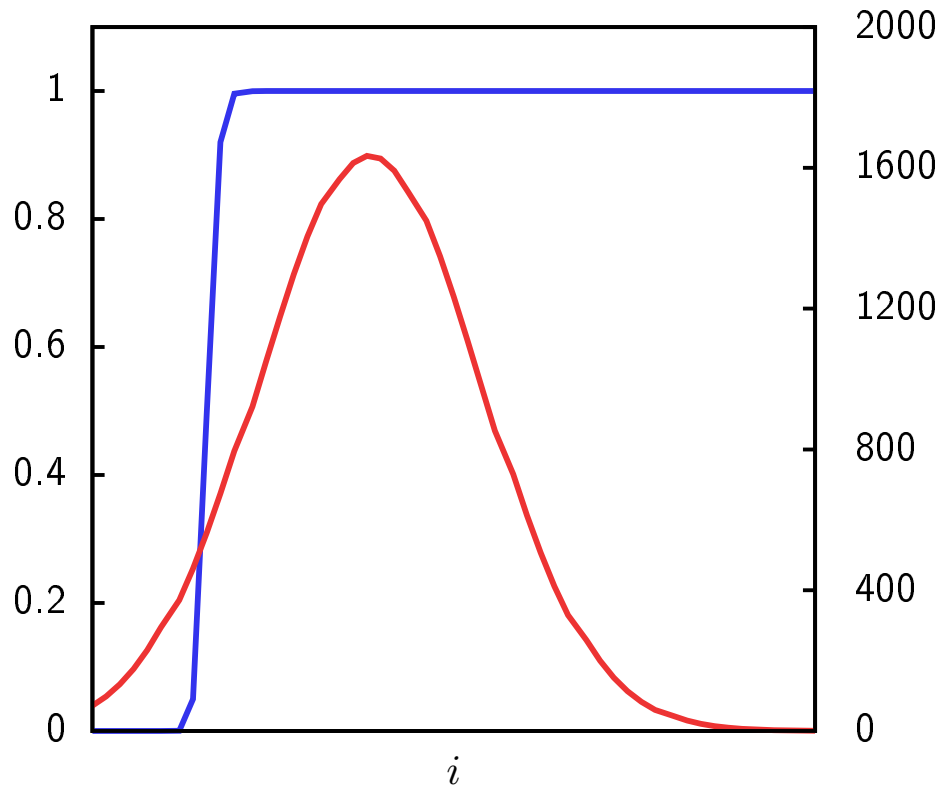
- Expressing $P_S$ as a function of $N$ and $\ell$.

$$P_S = \sum_{i=0}^{N} \Pr\left[\Sigma_{k^*} = i\right] \cdot B_{n-\ell,\ell}(G(i)),$$

where $G$ is the cumulative distribution function of $\Sigma_{k \neq k^*}$.

# Success Probability (1/2)

$$P_S = \sum_{i=0}^{N} \Pr\left[\Sigma_{k^*} = i\right] \cdot B_{n-\ell,\ell}(G(i)).$$



# Success Probability (2/2)

**Theorem [Blondeau, G., Tillich 2009]**

If $G^{-1}$ denotes the inverse cumulative distribution function of the counters $\Sigma_k$ for $k \neq k^*$, then,

$$P_S \approx \sum_{i=G^{-1}(t_0)}^{N} \Pr\left[\Sigma_{k^*} = i\right],$$

with $t_0 \stackrel{\text{def}}{=} 1 - \frac{\ell-1}{2^{n_{key}}-2}$.

Formula in [Selçuk 2008]:

$$\int_{\Phi_w^{-1}\left(1-\frac{\ell}{2^{n_{key}}}\right)}^{\infty} \varphi_r(x)\, dx.$$

# Multiple differential cryptanalysis

Multiple cryptanalyses: extracting more information using several characteristics.

$$\Pr_{M,K}\left[F_K^{r-1}(M) \oplus F_K^{r-1}(M \oplus \delta_1^j) = \delta_2^j\right] = p_*^j.$$

Here the counters are

$$\Sigma_k^j \stackrel{\text{def}}{=} \#\left\{(m_1, m_2 = m_1 \oplus \delta_1^j, c_1, c_2), F_k^{-1}(c_1) \oplus F_k^{-1}(c_2) = \delta_2^j\right\},$$

$$\Sigma_k \stackrel{\text{def}}{=} \sum_j \Sigma_k^j.$$

**Main difficulty**

$$\Sigma_k^j \sim \mathcal{B}in\left(N, p_*^j\right) \text{ with } p_*^{j_1} \neq p_*^{j_2}.$$

# Analyzing multiple differential cryptanalysis

Main issue: estimating the distribution of a sum of binomial variables.

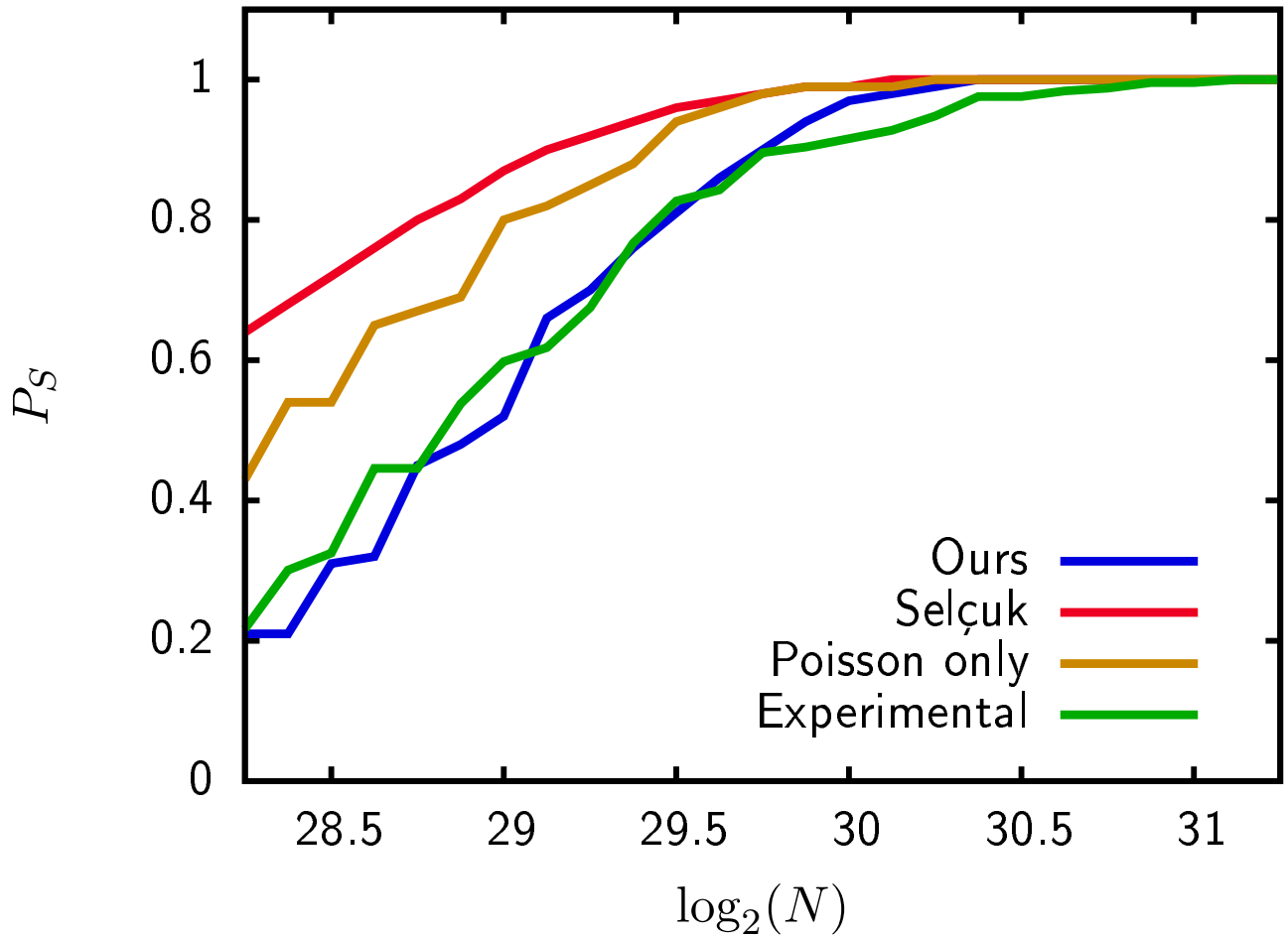
- x In literature, Selçuk's formula is used.
- x Using Poisson approximation, the behavior of counters for large deviations is not caught.

*Use another approximation for the tails.*

**Main tool**

Generalization of the formula used in the case of binomial tails for approximating the tails of the distribution of a sum of i.i.d. variables.

# Experimental results



# Proposed attack on 18-round PRESENT

Improvements from [Wang 2008]

- Use of differentials with different output differences.
- Better estimation of differential probabilities.
- Specific analysis that do not use Gaussian approximation.

| | Data | Time | Version | Rounds | Type |
|---|---|---|---|---|---|
| [Wang08] | $2^{64.0}$ | $2^{64.0}$ | 80 | 16 | (multi.) diff. |
| [OVTK09] | $2^{63.0}$ | $2^{104.0}$ | 128 | 17 | related keys |
| submitted | $2^{62.0}$ | $2^{75.0}$ | 80 | 18 | multi. diff. |
| [AlbCid09] | $2^{62.0}$ | $2^{113.0}$ | 128 | 19 | alg. diff. |
| [ColSta09] | $2^{57.0}$ | $2^{57.0}$ | 80 | 24 | stat. sat. |
| [Cho10] | $2^{64.0}$ | $2^{72.0}$ | 80 | 26 | multi. lin. |

# Advantage and gain

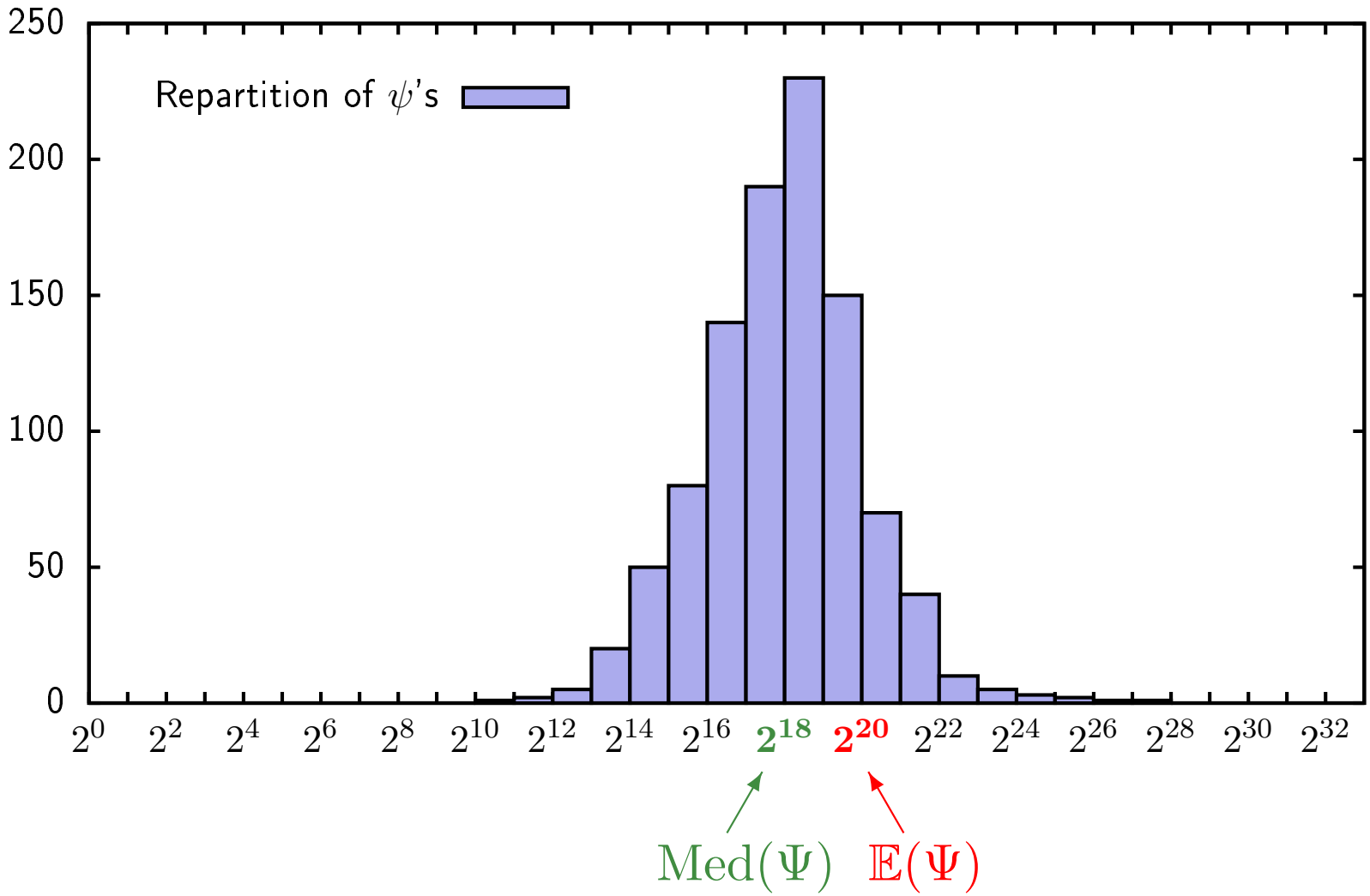
- $\Psi$: random variable corresponding to the rank of $k^*$ among the $2^{n_{key}}$ candidates.
- Advantage:

$$a \stackrel{\text{def}}{=} -\log_2 \left( \frac{\text{Med}(\Psi)}{2^{n_{key}}} \right).$$

- Gain:

$$\Gamma \stackrel{\text{def}}{=} -\log_2 \left( \frac{2\,\mathbb{E}(\Psi) - 1}{2^{n_{key}}} \right).$$

# Advantage vs gain (1/2)



# Advantage vs gain (2/2)

Gain:

- x provides pessimistic results;
- ✓ $\mathbb{E}(\Psi)$ can be easily estimated.

Advantage:

- ✓ provides non-pessimistic results;
- x estimating $\mathrm{Med}(\Psi)$ may not be easy.

# Advantage vs gain (2/2)

Gain:

- x provides pessimistic results;
- ✓ $\mathbb{E}(\Psi)$ can be easily estimated.

Advantage:

- ✓ provides non-pessimistic results;
- x estimating $\mathrm{Med}(\Psi)$ may not be easy.

**Remark on previous example**

- $\mathrm{Med}(\Psi) = 2^{18.05}$;
- $\mathbb{E}(\Psi) = 2^{19.99}$;
- $\mathbb{E}(\log_2(\Psi)) = 17.96$.

# Some definition

An alternative quantity to look at is entropy.

$$\begin{aligned} \mathcal{H}(X) &\stackrel{\text{def}}{=} \mathbb{E}_X \log_2 (\Pr[X]), \\ \mathcal{H}(X|Y) &\stackrel{\text{def}}{=} \mathbb{E}_{X,Y} \log_2 (\Pr[X|Y]), \end{aligned}$$

- $Y$: the variable containing the statistics.
- $K'$: the sub-key to recover.
- $\mathcal{H}(K'|Y)$: quantify the uncertainty on the key knowing samples.

**Heuristic**

Taking a list of size $\ell = 2^{\mathcal{H}(K'|Y)}$ leads to a success probability greater than $0.5$.

# Links between entropy and advantage

$$a \stackrel{\text{def}}{=} -\log_2\left(\frac{\text{Med}(\Psi)}{2^{n_{key}}}\right) \quad \textit{similar to} \quad ? = -\log_2\left(\frac{2^{\mathcal{H}(K'|Y)}}{2^{n_{key}}}\right).$$

# Links between entropy and advantage

$$a \stackrel{\text{def}}{=} -\log_2\left(\frac{\text{Med}(\Psi)}{2^{n_{key}}}\right) \quad \textit{similar to} \quad \mathcal{I}(K';Y) = -\log_2\left(\frac{2^{\mathcal{H}(K'|Y)}}{2^{n_{key}}}\right).$$

$$\mathcal{I}(K';Y) \stackrel{\text{def}}{=} \mathcal{H}(K') - \mathcal{H}(K'|Y).$$

**Formula for $\mathcal{I}(K';Y)$**

$$\mathcal{I}(K';Y) = \sum_{k'}\sum_{y} \Pr\left[K'=k', Y=y\right] \log_2\left(\frac{\Pr\left[K'=k', Y=y\right]}{\Pr\left[K'=k'\right]\Pr\left[Y=y\right]}\right),$$

# Estimating $\mathcal{I}(K';Y)$

*Bounding mutual information by a sum of quantities easier to compute.*

The probability function of a variable $A$ is $g(A)$.

**Main tool**

If

$$g(Y|K') = \prod_j g(Y_j|K'_j),$$

then,

$$\mathcal{I}(K';Y) \leq \sum_j \mathcal{I}(K'_j;Y_j).$$

# Application to multiple linear cryptanalysis (1/3)

Here the variables are decomposed regarding approximations.

$$\Pr_{M,K}\left[\langle \pi_j, M\rangle \oplus \langle \gamma_j, C\rangle = \langle \kappa_j, K\rangle\right] = \frac{1}{2} + \varepsilon_j.$$

Counters are

$$\Sigma_j \stackrel{\text{def}}{=} \sum_{i=1}^{N} \langle \pi_j, m^i\rangle \oplus \langle \gamma_j, c^i\rangle.$$

Then, we use the bound with

$$Y_j \stackrel{\text{def}}{=} \frac{N - 2\Sigma_j}{2N\varepsilon_j} \quad \text{and} \quad K'_j \stackrel{\text{def}}{=} \langle \kappa_j, K\rangle.$$

$$Y_j = (-1)^{K'_j} + B_j \text{ with } B_j \sim \mathcal{N}\left(0, \frac{1}{4N\varepsilon_j^2}\right).$$

# Application to multiple linear cryptanalysis (2/3)

$$g(Y|K') = \prod_j g(Y_j|K'_j) \iff \text{approximations are independent.}$$

Then,

$$\mathcal{I}(K'_j; Y_j) \leq \mathrm{Cap}(\sigma_j^2),$$

where $\mathrm{Cap}(\sigma_j^2)$ is the capacity of the Gaussian channel with noise variance $\sigma_j^2 \stackrel{\text{def}}{=} 1/4N\varepsilon_j^2$.

$$\mathcal{I}(K'; Y) \leq \sum_j \mathrm{Cap}\left(\sigma_j^2\right) \approx \frac{2N \sum_j \varepsilon_j^2}{\ln 2} + \mathcal{O}\left(\sum_j \varepsilon_j^4\right).$$

# Application to multiple linear cryptanalysis (3/3)

**Theorem**

For $\ell = 1$, if

$$\sum_j \mathrm{Cap}\left(\sigma_j^2\right) > n_{key},$$

then the success probability tends to 1 with the number of approximations.

In this case, we obtain the following estimates for $N$:

x Gain $\rightarrow N \approx \dfrac{n_{key}+1}{\sum_j \varepsilon_j^2}$.

✓ Entropy $\rightarrow N \approx \dfrac{n_{key}}{2\sum_j \varepsilon_j^2}$.

# Application to Matsui's Algorithm 2

The decomposition is done among possible values for $k^*$.

$$\mathcal{I}(K';Y) \leq \int_{\mathbb{R}^+} f^1(y) \log_2 \left( \frac{f^1(y)}{f(y)} \right) + (2^{n_{key}} - 1) f^0(y) \log_2 \left( \frac{f^0(y)}{f(y)} \right) \, dy.$$

Using this bound, we can explain observations in [Junod 2001]:

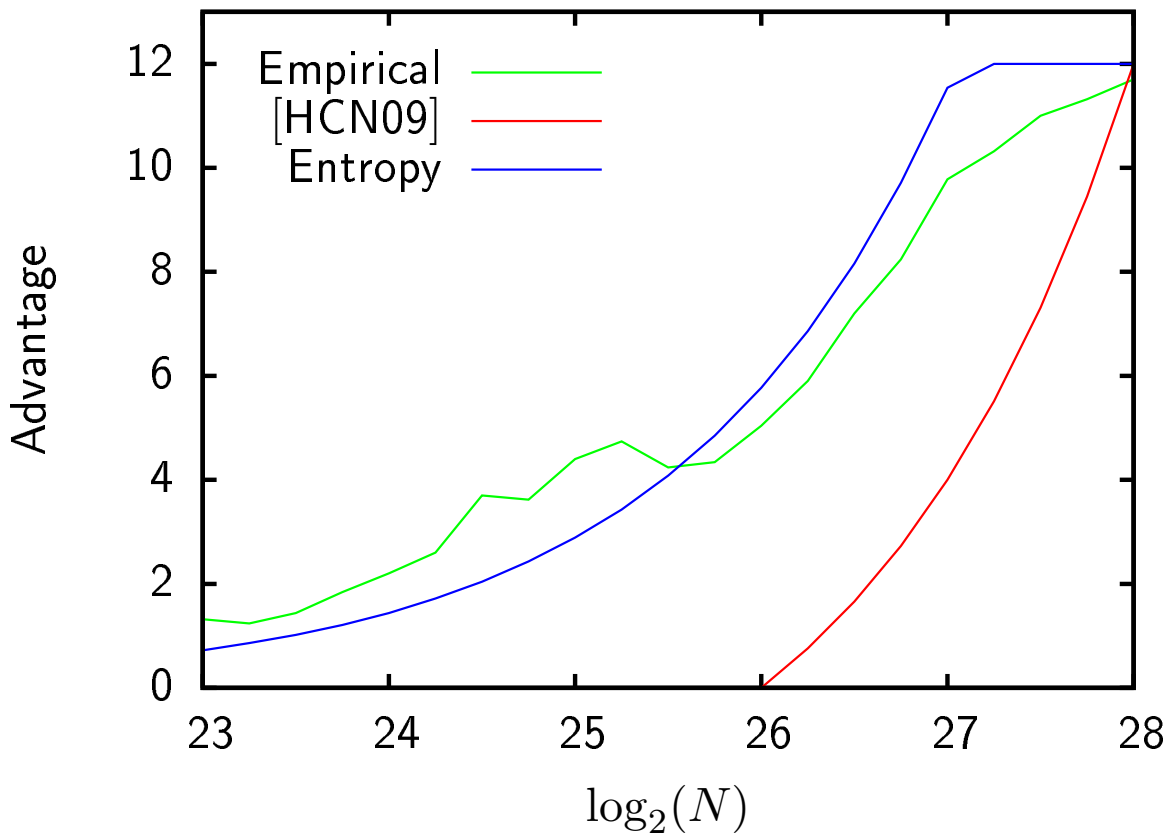
*Experimental time complexity is $2^{41}$ while the theoretical complexity obtained considering the expected rank of the key is $2^{43}$.*

Applying the bound on mutual information leads to a time complexity of $2^{41}$.

# Application to multidimensional linear cryptanalysis

We easily obtain the following bound as a function of $\mathcal{H}(\Sigma_{k^*})$ the entropy of the counter corresponding to the correct candidate,

$$\mathcal{I}(K';Y) \leq \sum_{j=1}^{N} \mathcal{I}(K;Y_j) \leq N \cdot (d - \mathcal{H}(\Sigma_{k^*})).$$




- Attack presented by Hermelin, Nyberg and Cho at FSE 2009.
- For 4 base approximations and the LLR method.
- Data provided by authors.

# Other works and perspectives

Some other works:

- experiments on the use of a linear decoding algorithm for recovering the key in multiple linear cryptanalysis;
- implementation of a multiple linear cryptanalysis on DES.
- experiments on differential cryptanalysis [Blondeau, G. 2010].

Perspectives:

- Other way for handling multiple attacks.
- Application of entropy approach to other cryptanalyses.
- Bounding the success rate when taking $\ell = 2^{\mathcal{H}(K'|Y)}$.

# Entropy in multidimensional linear cryptanalysis (1/2)

For $d$ base approximations

$$\Pr_{M,K}\left[\langle \pi_j, M\rangle \oplus \langle \gamma_j, C\rangle = 0\right] = \frac{1}{2} + \varepsilon_j.$$

$$Y_k^i \stackrel{\text{def}}{=} \begin{pmatrix} \langle \pi_1, m^i\rangle \oplus \langle \gamma_1, F_k^{-1}(c^i)\rangle \\ \vdots \\ \langle \pi_d, m^i\rangle \oplus \langle \gamma_d, F_k^{-1}(c^i)\rangle \end{pmatrix}.$$

- For $k = k^*$, the distribution of $Y_{k^*}^i$ is $\mathbf{p}_*$.
- For $k \neq k^*$, the distribution of $Y_{k^*}^i$ is uniform on $\mathbb{F}_2^s$.

$$\mathcal{I}(K';Y) \leq \sum_{i=1}^{N} \sum_{k \in \mathbb{F}_2^{n_{key}}} \mathcal{I}(K';Y_k^i).$$

# Entropy in multidimensional linear cryptanalysis (2/2)

$$\mathcal{I}(K';Y) \leq \sum_{i=1}^{N} \sum_{k \in \mathbb{F}_2^{n_{key}}} \mathcal{I}(K';Y_k^i).$$

$$\mathcal{I}(K';Y_k^i) = \mathcal{H}(Y_k^i) - \mathcal{H}(Y_k^i|K').$$

**Final result**

$$\mathcal{I}(K';Y) \leq N \cdot (d - \mathcal{H}(\mathbf{p}_*)).$$

# Entropy in multidimensional linear cryptanalysis (2/2)

$$\mathcal{I}(K';Y) \leq \sum_{i=1}^{N} \sum_{k \in \mathbb{F}_2^{n_{key}}} \mathcal{H}(Y_k^i) - \mathcal{H}(Y_k^i|K').$$

$$\sum_{k \in \mathbb{F}_2^{n_{key}}} \mathcal{H}(Y_k^i|K') = \mathcal{H}(\mathbf{p}_*) + (2^{n_{key}} - 1) \cdot d.$$

$$\sum_{k \in \mathbb{F}_2^{n_{key}}} \mathcal{H}(Y_k^i) = 2^{n_{key}} \cdot d.$$

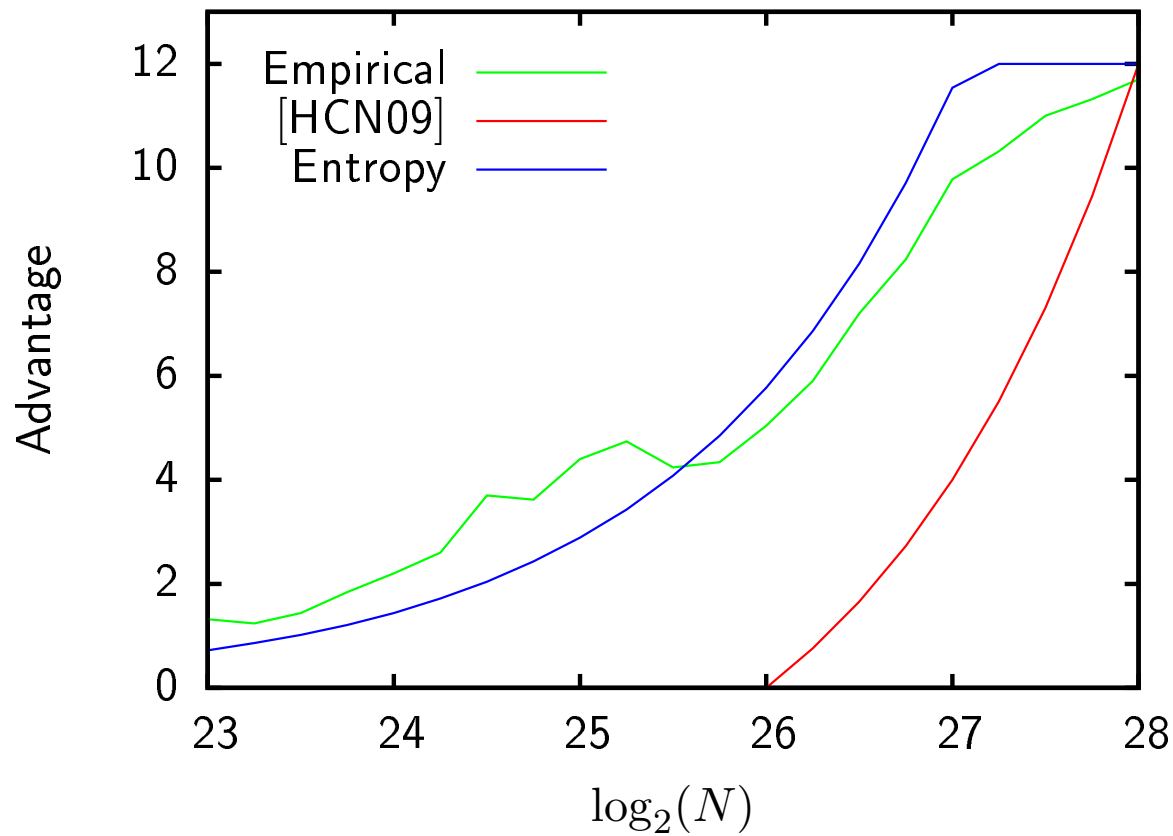
**Final result**

$$\mathcal{I}(K';Y) \leq N \cdot (d - \mathcal{H}(\mathbf{p}_*)).$$

# Application to multidimensional linear cryptanalysis

Formula used from [Hermelin, Cho, Nyberg 2009]:

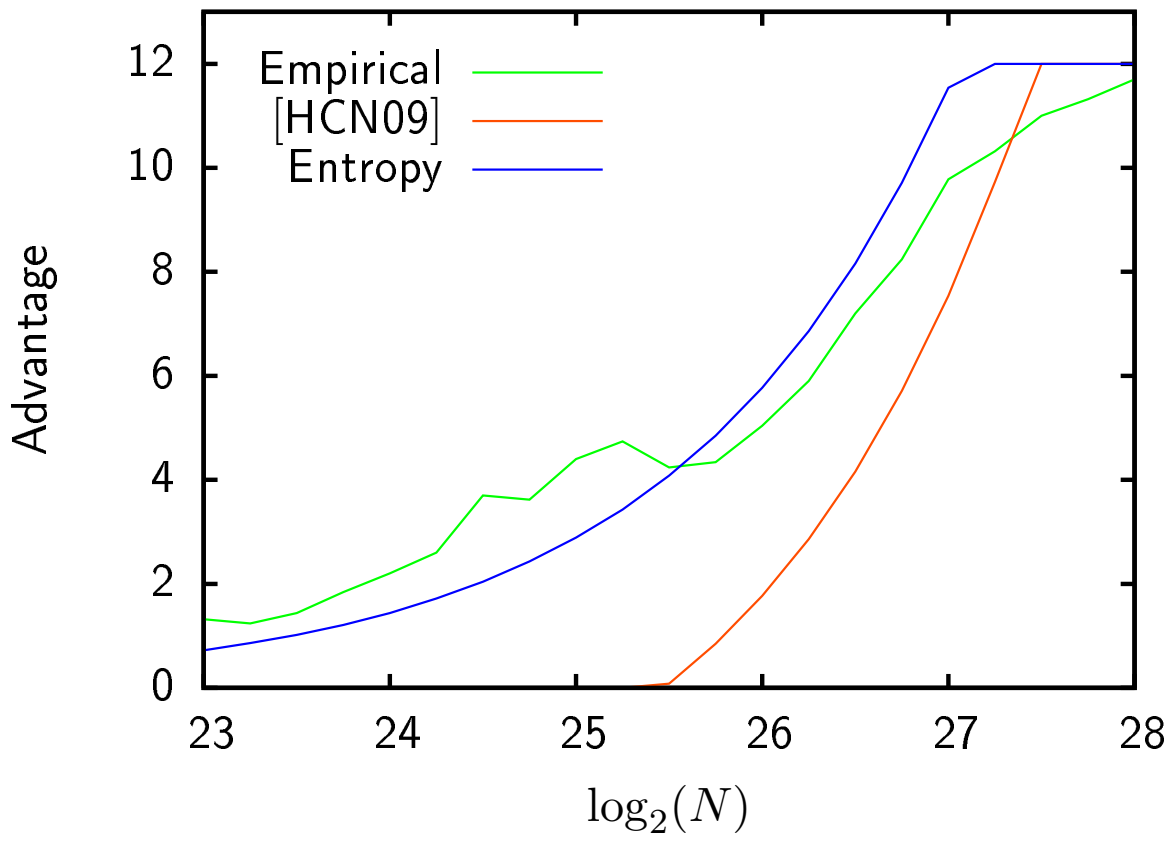
$$a_{\mathrm{LLR}} \approx \frac{NC(p)}{2} - m.$$



# Application to multidimensional linear cryptanalysis

Formula used from [Hermelin, Cho, Nyberg 2009]:

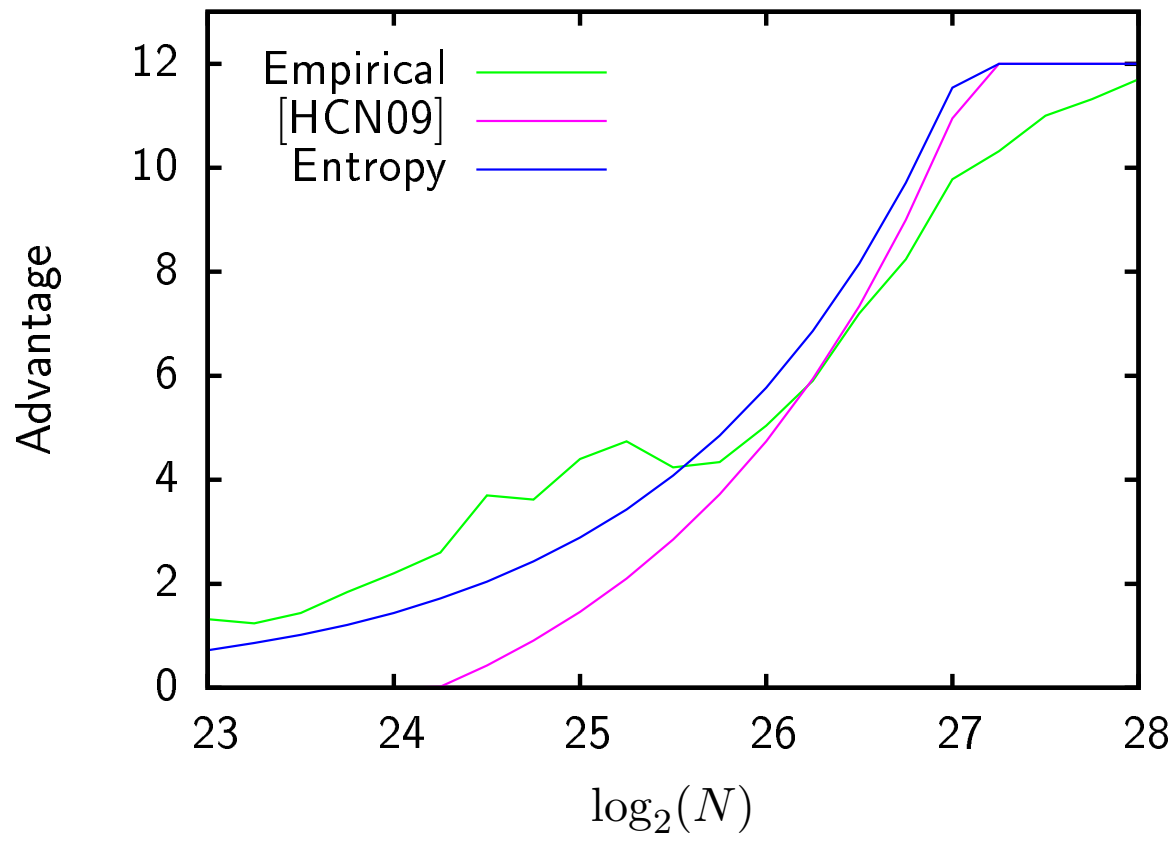
$$a_{\text{LLR}} \approx \frac{NC(p)}{2\ln(2)} - m.$$



# Application to multidimensional linear cryptanalysis

Formula used from [Hermelin, Cho, Nyberg 2009]:

$$a_{\text{LLR}} \approx -\log_2 \Phi\left(-\sqrt{NC(p)}\right) - m.$$



# Application to multidimensional linear cryptanalysis

Formula used from [Hermelin, Cho, Nyberg 2009]:

$$a_{\text{LLR}} \approx -\log_2 \left[ 1 - \Phi\left( \sqrt{NC(p)} \right)^{2^m} \right].$$