Multiple Differential Cryptanalysis: Theory and Practice

Céline Blondeau, Benoît Gérard

SECRET-Project-Team, INRIA, France

FSE, February 14th, 2011

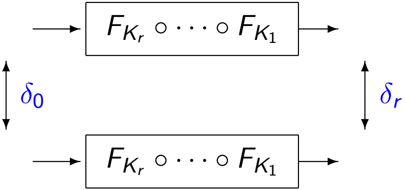
Outline

1. Multiple differential cryptanalysis
2. Data complexity and success probability
3. Attack on PRESENT

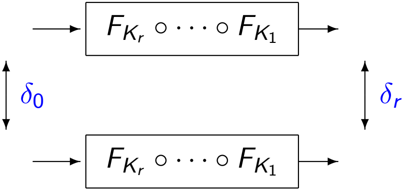
Outline

Differential cryptanalysis [Biham-Shamir 1990]

Differential



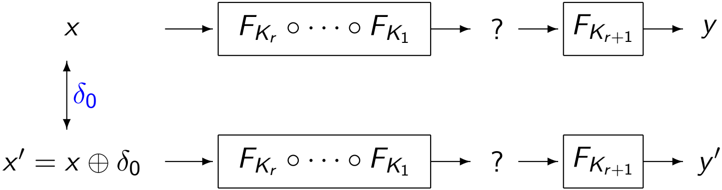
Differential



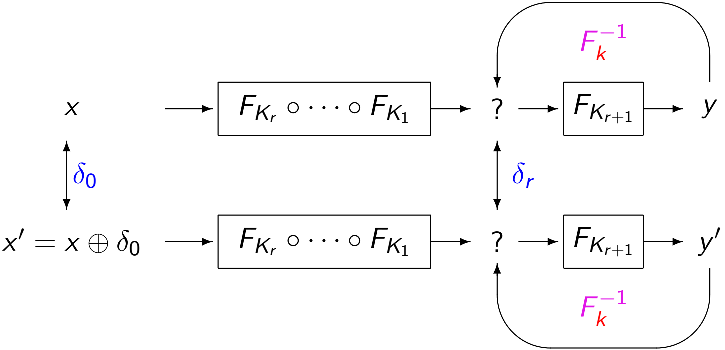
Differential probability

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

Differential cryptanalysis

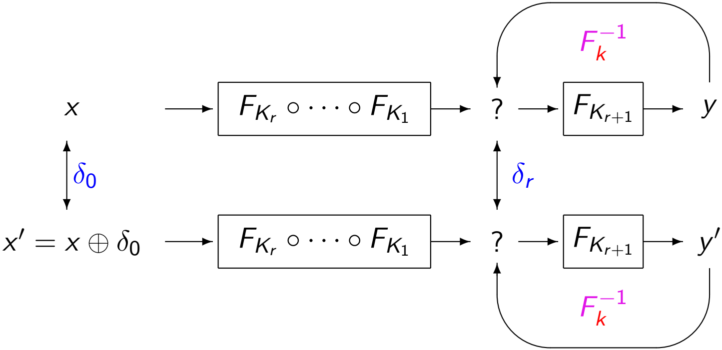


Last round attack



Differential cryptanalysis [Biham-Shamir 1990]

Last round attack



Basic Principle:

For each last-round subkey candidate k, compute

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

Wrong Key Randomization Hypothesis

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

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

Hypothesis

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

Counters

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

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

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.

Collection of differentials

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

Multiple differential cryptanalysis

Collection of differentials

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

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

Multiple differential cryptanalysis

Collection of differentials

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

$p_*^{(i,j)}$: 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

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

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

$C_x^{(i)}(k)$ 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 $C(k)$?

Outline

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]:

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

Where $q = p_*$ or p.

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

Data complexity

In [Blondeau-Gérard-Tillich-2010], the data complexity is computed by approximating one tail of binomial cumulative function with:

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

Data complexity

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

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

Data complexity

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

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

With similar arguments, the data complexity is

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

Where:

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

Success probability

Success probability:

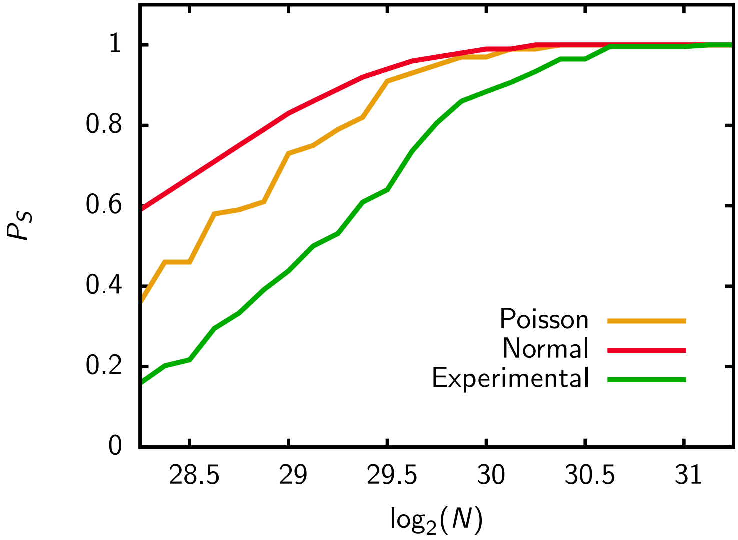
$$P_s \approx 1 - G_* \left[G^{-1} \left(1 - \frac{\ell - 1}{2^n - 2} \right) - 1 \right],$$

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]

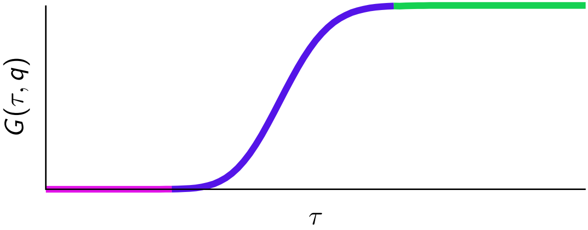


Distribution of the counters

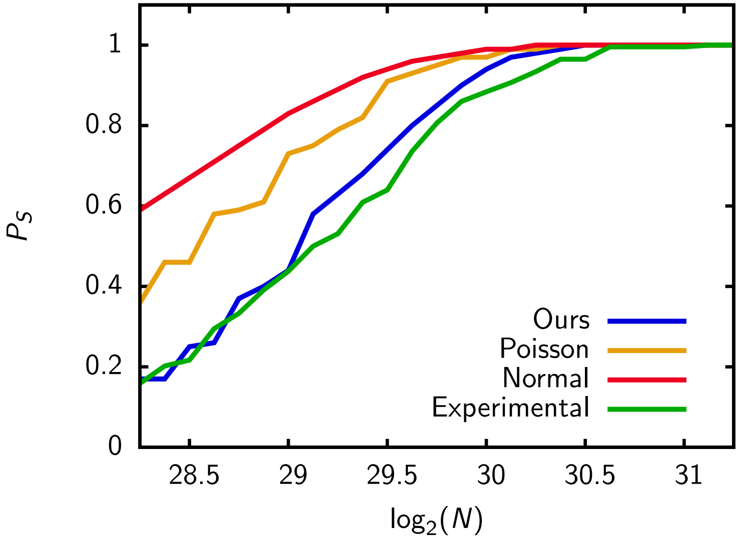
We use the following estimate for the cumulative function of the $C(k)$'s:

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

$$G_*(x) = G(x, p_*)$$
$$G(x) = G(x, p)$$



Experiments on SMALLPRESENT-[8]

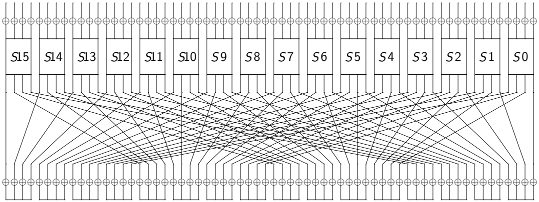


Outline

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 analysed the distribution of the counter when the sum of the simple random variables is taken.

  $\Rightarrow$ Formula of the data complexity
  $\Rightarrow$ Formula of the success probability

Perspectives:

- Study complexities of multiple differential cryptanalysis by using other statistical tests.