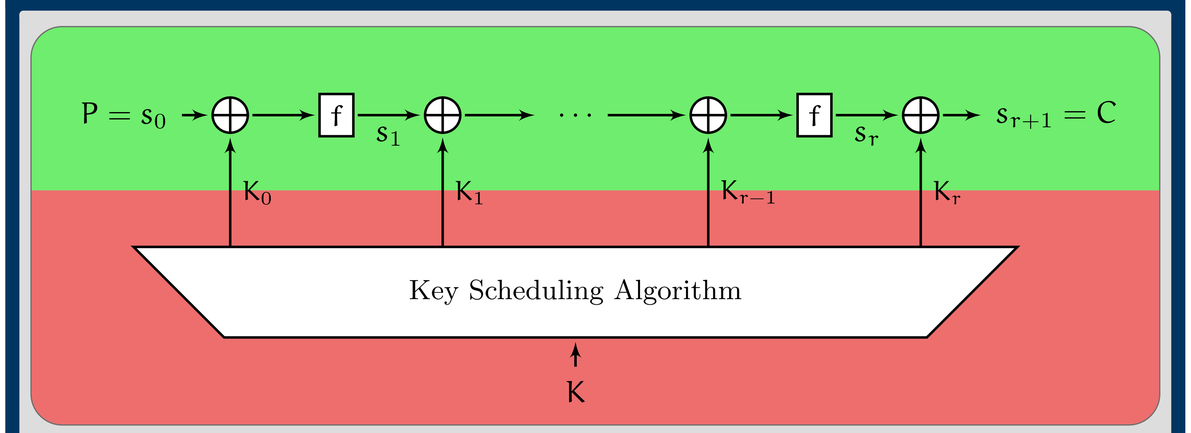
On the Design of Key Schedules

Friedrich Wiemer
1. Advisor: Prof. Dr. Gregor Leander 2. Advisor: Prof. Dr. Alexander May

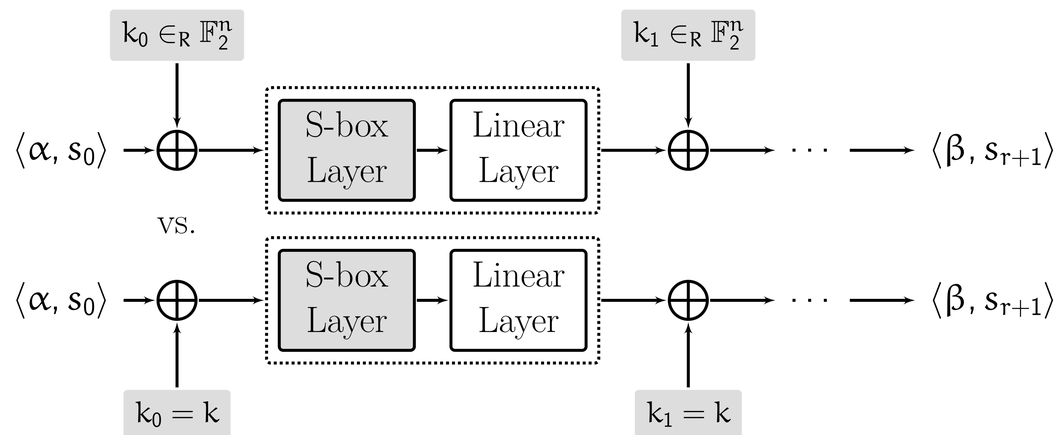
Design of Block Ciphers



Problem

- Abdelraheem et al. (2012), cf. Fig. 1:
  PRESENT with const. round keys is weaker than with indp. round keys.
- How do different S-boxes influence this behaviour?
- Interesting candidate: R_1, cf. Fig. 2.
- Its convergence distribution fulfills *Tchebysheff's inequality tightly.*

Experimental Setup



What is the distribution of

$$\Pr[\langle \alpha, s_0 \rangle = \langle \beta, s_{r+1} \rangle]$$

over k and the choice of the S-box?

We cannot hope to prove better bounds than Tchebysheff in general for resistence against linear cryptanalysis.

Experimental Results

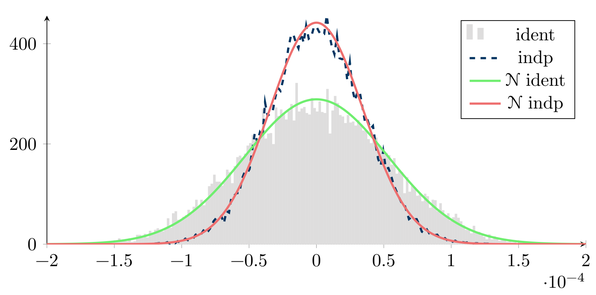


Figure 1: Standard PRESENT.

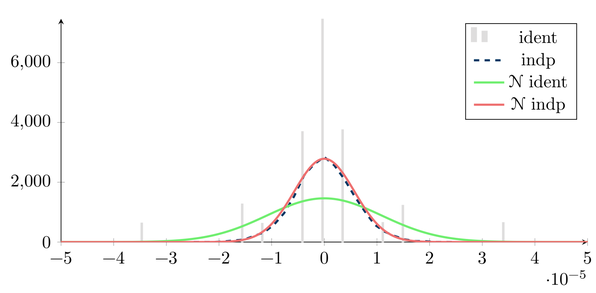


Figure 2: PRESENT with R_1 S-box.

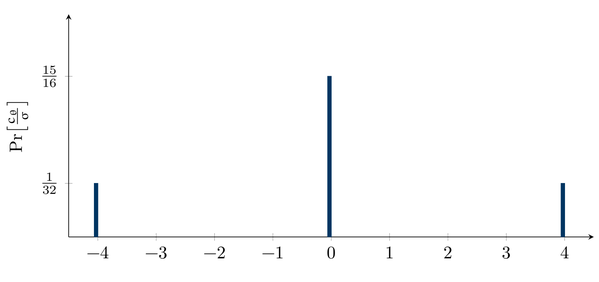


Figure 3: Convergence distribution.

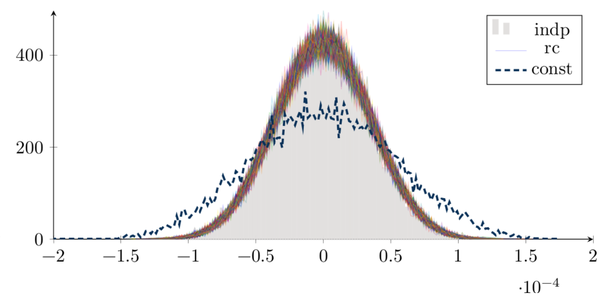


Figure 4: Influence of round constants.

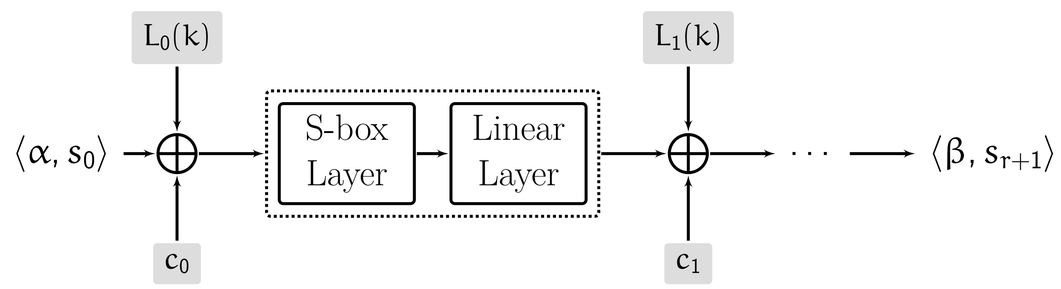
How to Design a Key Schedule:

Typically, a design uses round constants to avoid slide attacks, etc., and break symmetries in the round function.

To design a good key schedule against linear cryptanalysis, it is on average sufficient to choose any linear key schedule L_i and fix randomly chosen round constants c_i.

$$\mathbb{E}_{\mathsf{c}}\left(\mathrm{Var}\left(\widehat{\mathsf{E}_{\mathsf{k}}}(\alpha,\beta)\right)\right) = 2^{-n(r+1)} \sum_{\mathsf{c}} \mathbb{F}_2^{-\ell} \sum_{\mathsf{k}\in\mathbb{F}_2^{\ell}} \widehat{\mathsf{E}_{\mathsf{k}}}(\alpha,\beta)^2 = 2^{2n} \sum_{\substack{\gamma \\ \gamma_0=\alpha,\gamma_r=\beta}} \mathsf{C}_\gamma^2$$

Round Constants



Background

Linear Cryptanalysis

For a block cipher $\mathsf{E}_{\mathsf{k}} : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we need to find good *input/output masks* $(\alpha,\beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$, s. t. $\langle \alpha, x \rangle = \langle \beta, \mathsf{E}_{\mathsf{k}}(x) \rangle$ holds for many x. The Fourier coefficient $\widehat{\mathsf{E}_{\mathsf{k}}}$ at the point (α,β) is $\widehat{\mathsf{E}_{\mathsf{k}}}(\alpha,\beta) := \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle \alpha,x\rangle + \langle \beta, \mathsf{E}_{\mathsf{k}}(x)\rangle}$.

PRESENT (Bogdanov et al. 2007)

- lightweight block cipher
- one bit trails dominate (Ohkuma 2009)
- SPN with 64 bit blocks
- 4 bit S-box
- Bitpermutation

Acknowledgements

This work was supported by the DFG Research Training Group GRK 1817 UbiCrypt.

References

[1] T. Kranz, G. Leander, and F. Wiemer. "Linear Cryptanalysis: On Key Schedules and Tweakable Block Ciphers". In submission.

DFG Deutsche Forschungsgemeinschaft
RUHR UNIVERSITÄT BOCHUM
RUB
hgi Horst Görtz Institute for IT-Security
UbiCrypt Cryptography in Ubiquitous Computing