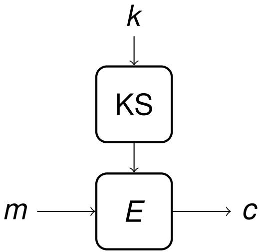
Linear Cryptanalysis: Key Schedules and Tweakable Block Ciphers

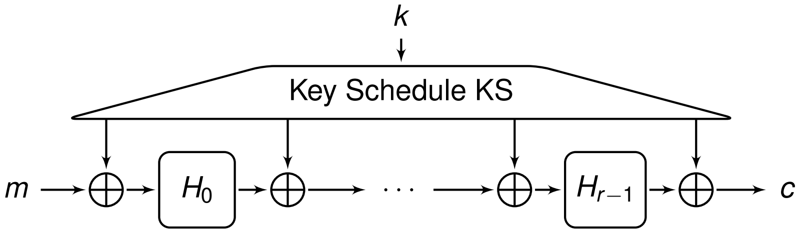
Thorsten Kranz, Gregor Leander, Friedrich Wiemer

Horst Görtz Institute for IT Security, Ruhr University Bochum

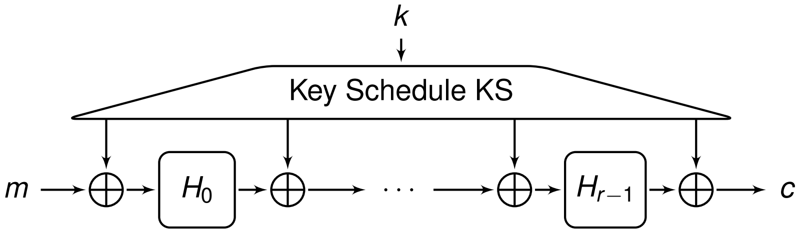
Block Cipher Design



Block Cipher Design



Block Cipher Design



How does the key schedule influence statistical attacks?

Linear Cryptanalysis

For $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\alpha, \gamma \in \mathbb{F}_2^n$

Bias of a linear approximation

$$\Pr_x[\langle \gamma, E_k(x) \rangle = \langle \alpha, x \rangle] = \frac{1}{2} + \epsilon_{E_k}(\alpha, \gamma)$$

Goal: Find (α, γ) such that $|\epsilon_{E_k}(\alpha, \gamma)|$ is large.

Linear Cryptanalysis

For $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\alpha, \gamma \in \mathbb{F}_2^n$

Bias of a linear approximation

$$\Pr_x[\langle \gamma, E_k(x) \rangle = \langle \alpha, x \rangle] = \frac{1}{2} + \epsilon_{E_k}(\alpha, \gamma)$$

Goal: Find (α, γ) such that $|\epsilon_{E_k}(\alpha, \gamma)|$ is large.

Fourier Coefficient

$$\widehat{E_k}(\alpha, \gamma) = 2^{n+1} \epsilon_{E_k}(\alpha, \gamma)$$

Linear Cryptanalysis

For $E_k : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\alpha, \gamma \in \mathbb{F}_2^n$

Bias of a linear approximation

$$\Pr_x[\langle \gamma, E_k(x) \rangle = \langle \alpha, x \rangle] = \frac{1}{2} + \epsilon_{E_k}(\alpha, \gamma)$$

Goal: Find (α, γ) such that $|\epsilon_{E_k}(\alpha, \gamma)|$ is large.

Fourier Coefficient

$$\widehat{E_k}(\alpha, \gamma) = 2^{n+1} \epsilon_{E_k}(\alpha, \gamma)$$

How does the key schedule influence the Fourier coefficient?

Outline

Outline

Experiments with one bit trails

- We cannot compute the exact Fourier coefficient

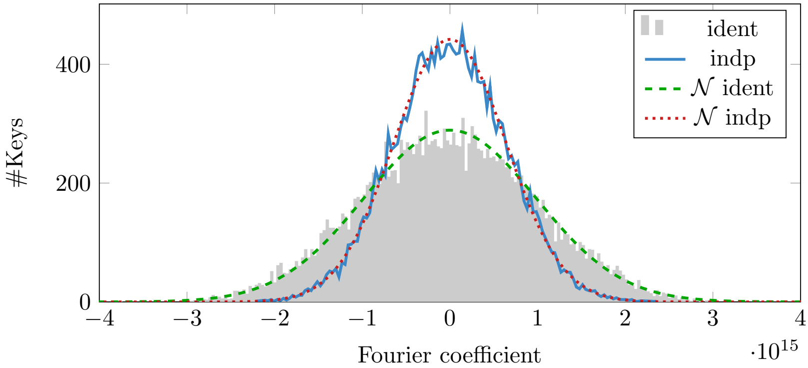
[1] Ohkuma. Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis, SAC 2008.

Experiments with one bit trails

- We cannot compute the exact Fourier coefficient
- For round-reduced PRESENT, it is enough to look at the one bit trails [1]

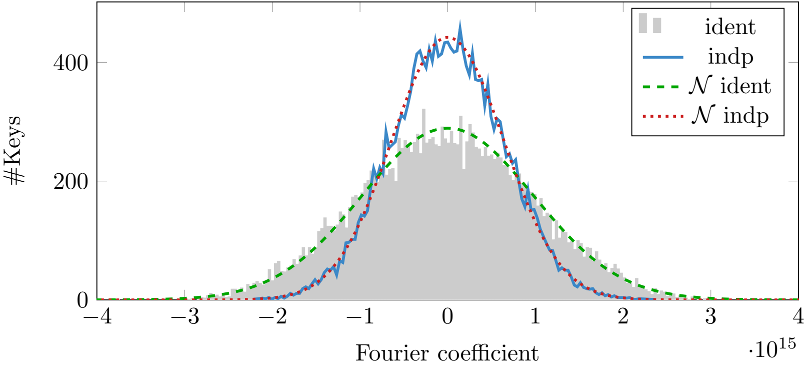
[1] Ohkuma. Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis, SAC 2008.

Round-reduced PRESENT: Identical round keys cause greater variance [2]



[2] Abdelraheem *et al*. On the Distribution of Linear Biases: Three Instructive Examples, CRYPTO 2012.

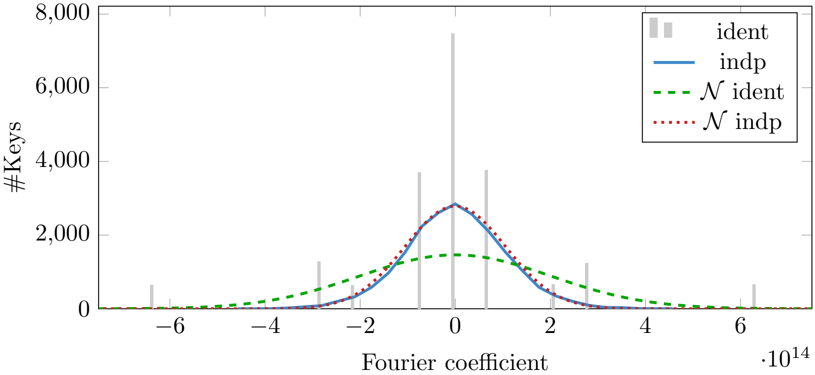
Round-reduced PRESENT: Identical round keys cause greater variance [2]



Greater variance, but still a normal distribution.

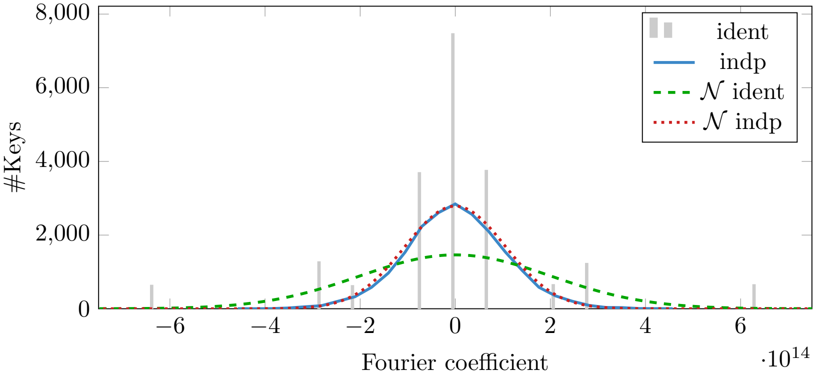
[2] Abdelraheem *et al*. On the Distribution of Linear Biases: Three Instructive Examples, CRYPTO 2012.

Round-reduced PRESENT with *Serpent-type* S-box



Horst Görtz Institute for IT-Security

Round-reduced PRESENT with *Serpent-type* S-box



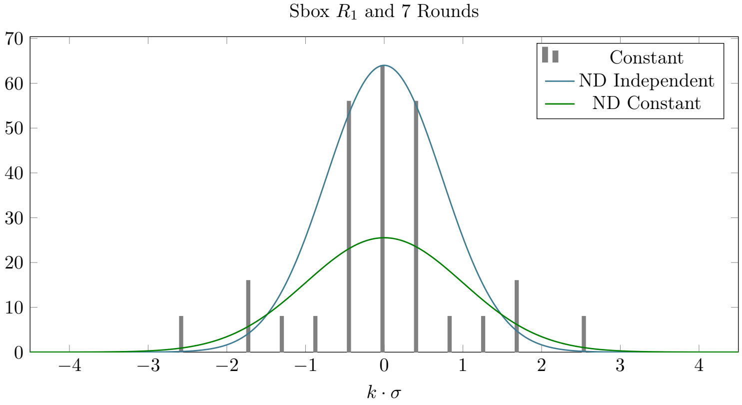
Not a normal distribution any more!

Horst Görtz Institute for IT-Security

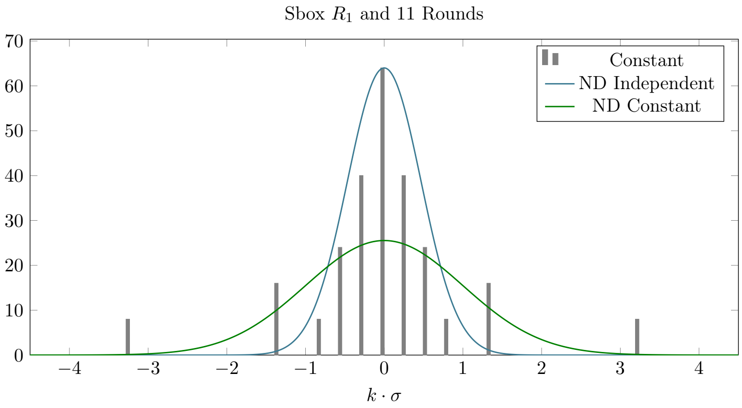
Number of weak keys is substantially increased

- 3% outliers with $|x - \mu| > 3\sigma$
- Factor of 10 higher than what we expect from normal distribution
- Factor of 2^{20} higher than what we expect from independent round keys

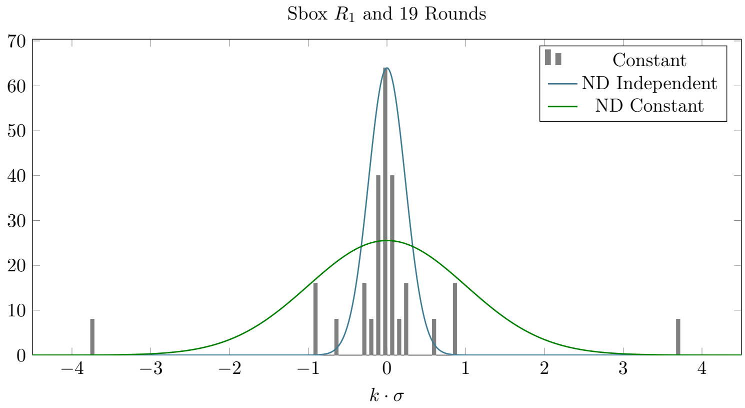
Increasing the number of rounds



Increasing the number of rounds

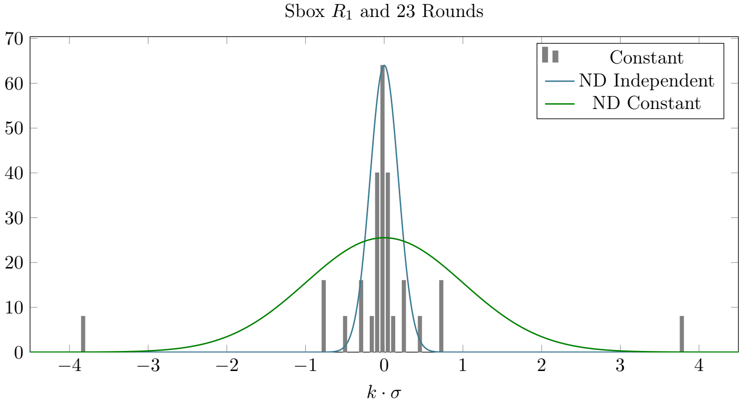


Increasing the number of rounds

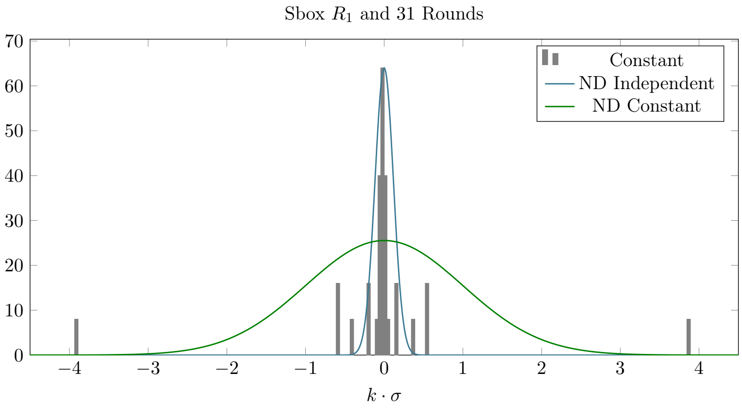


Horst Görtz Institute for IT-Security

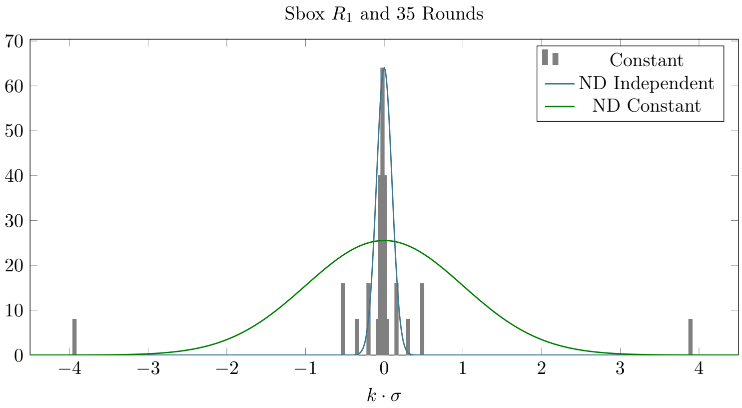
Increasing the number of rounds



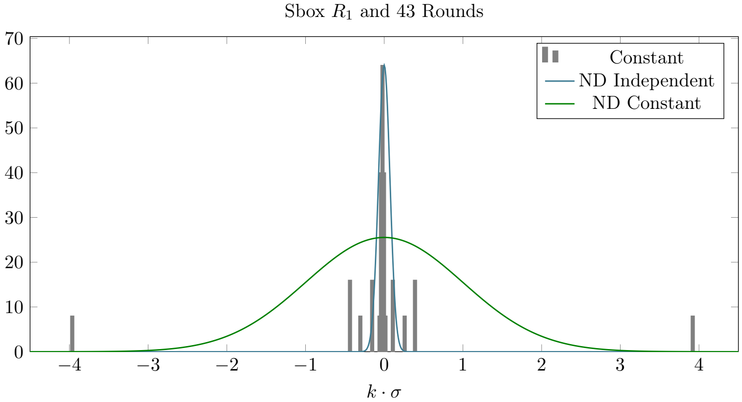
Increasing the number of rounds



Increasing the number of rounds

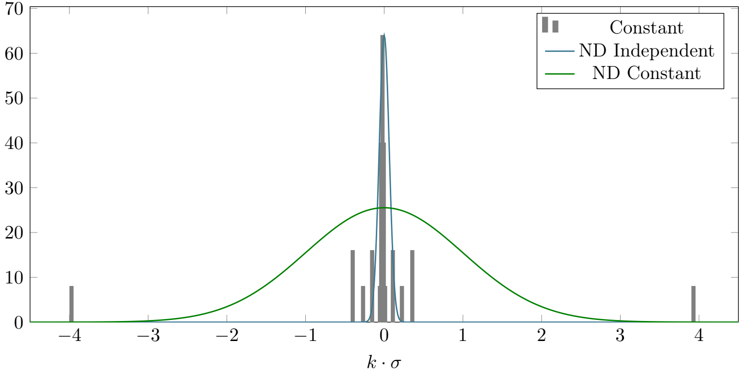


Increasing the number of rounds

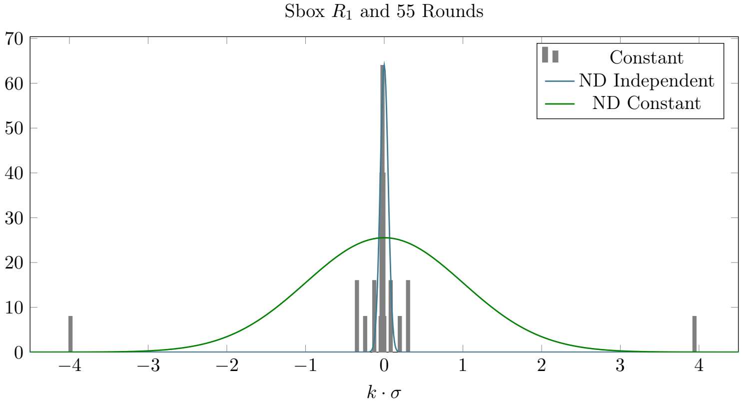


Increasing the number of rounds

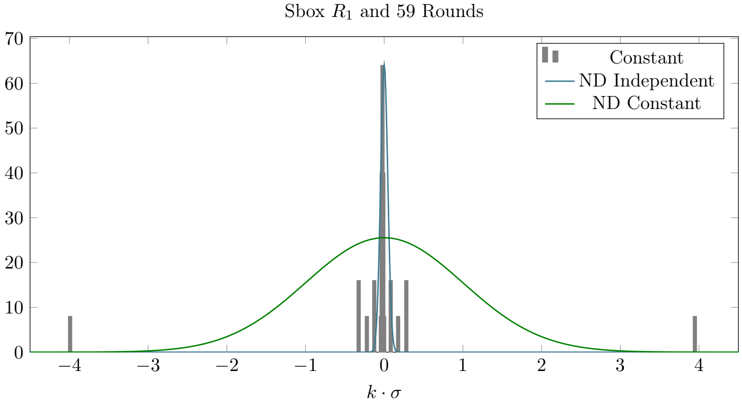
Sbox R_1 and 47 Rounds



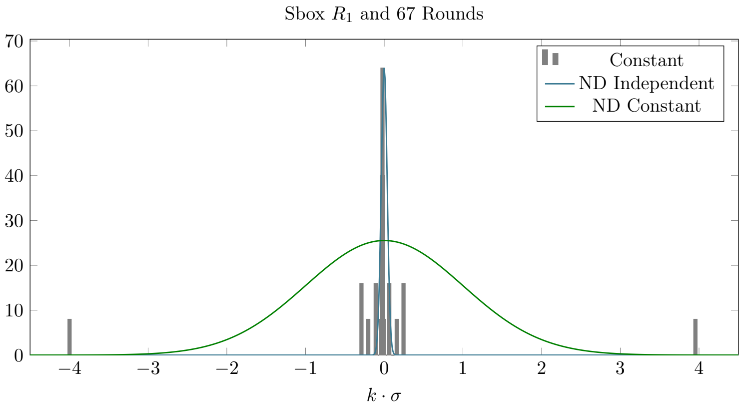
Increasing the number of rounds



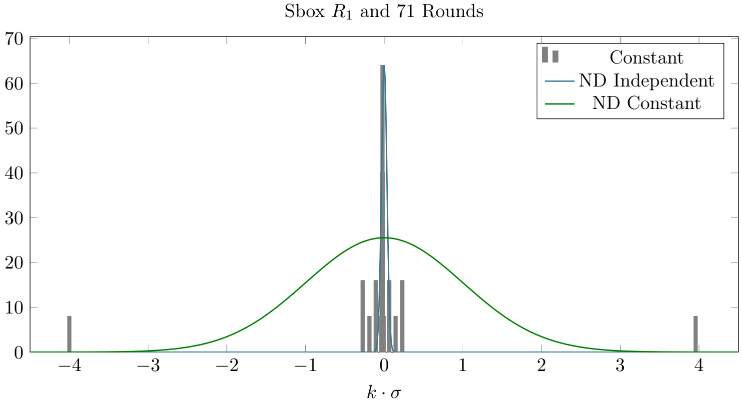
Increasing the number of rounds



Increasing the number of rounds

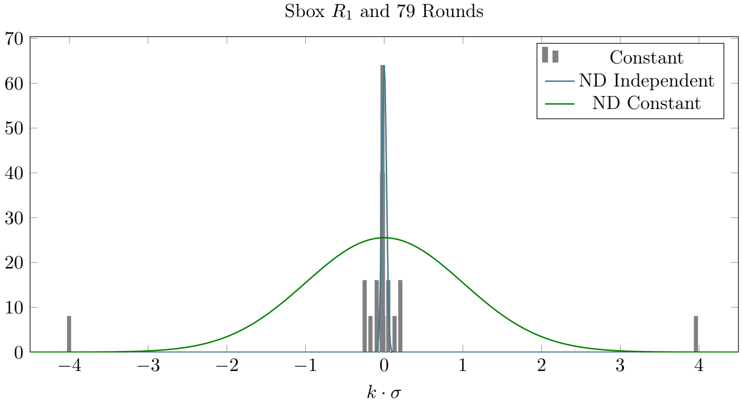


Increasing the number of rounds

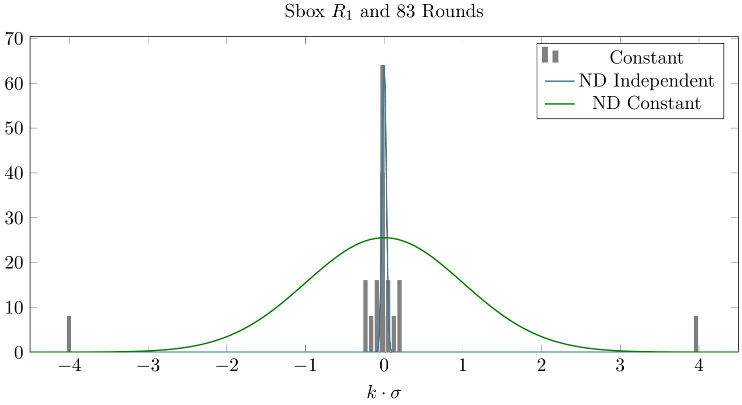


Horst Görtz Institute for IT-Security

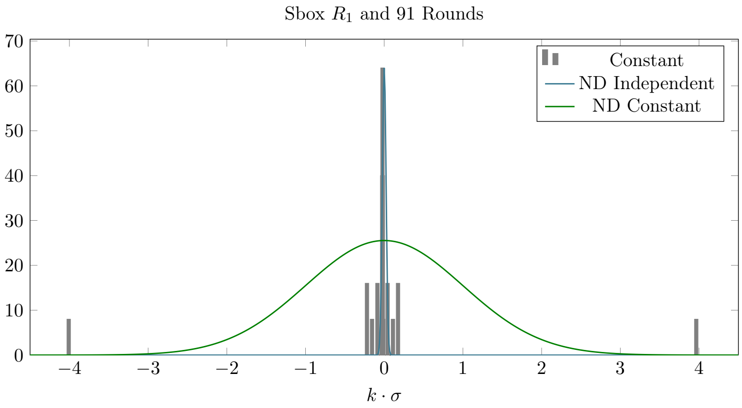
Increasing the number of rounds



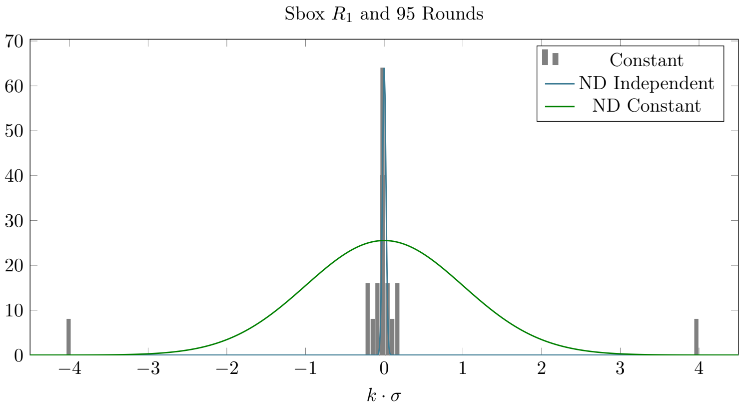
Increasing the number of rounds



Increasing the number of rounds



Increasing the number of rounds



Worst case for increasing number of rounds

For increasing number of rounds, the distribution of 1 bit trails converges to

$$\widehat{E_k}(\alpha,\gamma) \sim \begin{cases} -4\sigma & \text{with probability } \frac{1}{32} \\ 0 & \text{with probability } \frac{15}{16} \\ 4\sigma & \text{with probability } \frac{1}{32} \end{cases}$$

This distribution fulfills Tchebysheff's bound with equality:

$$\Pr\left[|\widehat{E_k}|(\alpha,\gamma) \geq 4 \cdot \sigma\right] = \left(\frac{1}{32} + \frac{1}{32}\right) = \frac{1}{4^2}$$

Outline

Key Schedule Design

- Hypothesis of Independent Round Keys wrong.
  Instead: *Key Schedule*
- Often a linear function.
- Using round constants.

Sound Design:
Linear Key Schedule with Random Constants

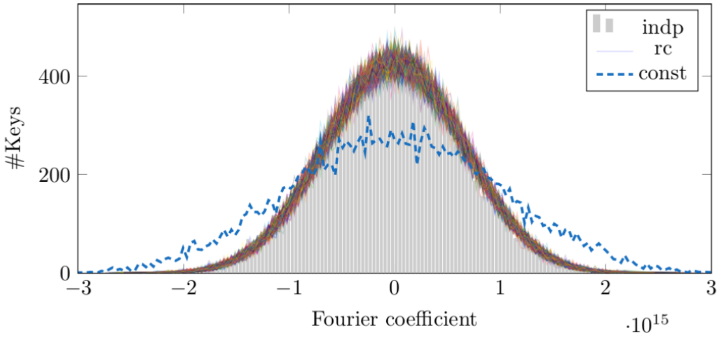
Variance of Fourier Coefficients (over the keys)

For a linear key schedule, the average variance over all constants is equal to the variance for independent round keys.

Choosing Random Constants

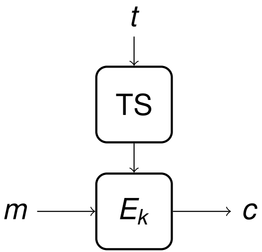
Choosing any linear key schedule and random round constants is on average as good as having independent round keys (in terms of the variance of the distribution).

Experiments:
Linear Key Schedule with Random Constants



Outline

Tweakable Block Ciphers



New attack vector:
also consider tweak input for linear cryptanalysis.

Input mask is $(\alpha, \beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$.

Tweaks do not introduce new linear trails

Observation

Tweaking a block cipher with a linear key schedule does not introduce any new linear trails.

Design Consequences

Protecting a tweakable block cipher against linear cryptanalysis can be done in the same way as in the non-tweakable case.

Application: Design of SKINNY

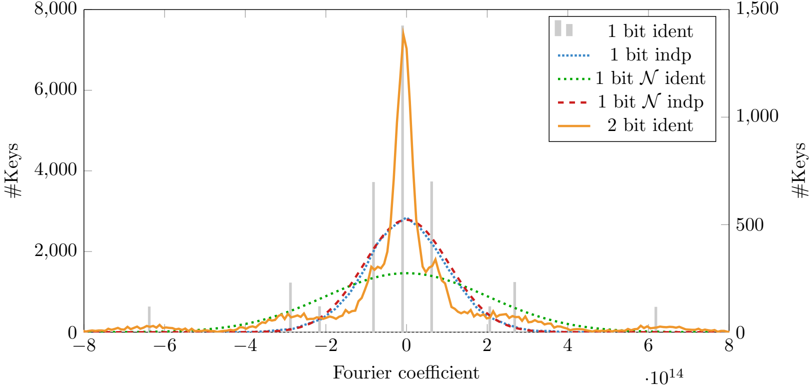
Table: Lower bounds on the number of active Sboxes in SKINNY.

Model	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
SK	75	82	88	92	96	102	108	(114)	(116)	(124)	(132)	(138)	(136)	(148)	(158)
TK1	54	59	62	66	70	75	79	83	85	88	95	102	(108)	(112)	(120)
TK2	40	43	47	52	57	59	64	67	72	75	82	85	88	92	96
TK3	27	31	35	43	45	48	51	55	58	60	65	72	77	81	85
SK Lin	70	76	80	85	90	96	102	107	(110)	(118)	(122)	(128)	(136)	(141)	(143)

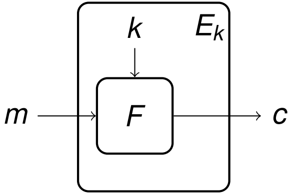
Any Questions?

Any Questions?

Round-reduced PRESENT with *Serpent-type* S-box



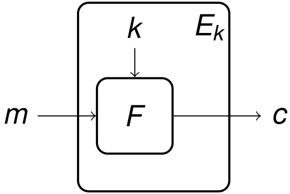
Fourier coefficient of $E_k(x) = F(x, k)$



$$2^m \widehat{E_k}(\alpha, \gamma) = \sum_{\beta \in \mathbb{F}_2^m} (-1)^{\langle \beta, k \rangle} \widehat{F}((\alpha, \beta), \gamma)$$

$$\widehat{F}((\alpha, \beta), \gamma) = \sum_{k \in \mathbb{F}_2^m} (-1)^{\langle \beta, k \rangle} \widehat{E_k}(\alpha, \gamma)$$

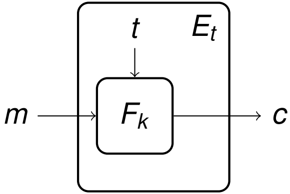
Fourier coefficient of $E_k(x) = F(x, k)$



$$2^m \widehat{E_k}(\alpha, \gamma) = \sum_{\beta \in \mathbb{F}_2^m} (-1)^{\langle \beta, k \rangle} \widehat{F}((\alpha, \beta), \gamma)$$

$$\widehat{F}((\alpha, \beta), \gamma) = \sum_{k \in \mathbb{F}_2^m} (-1)^{\langle \beta, k \rangle} \widehat{E_k}(\alpha, \gamma)$$

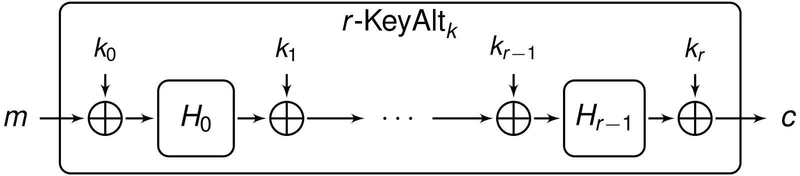
Fourier coefficient of $E_t(x) = F(x, t)$



$$2^m \widehat{E}_t(\alpha, \gamma) = \sum_{\beta \in \mathbb{F}_2^m} (-1)^{\langle \beta, t \rangle} \widehat{F_k}((\alpha, \beta), \gamma)$$

$$\widehat{F_k}((\alpha, \beta), \gamma) = \sum_{t \in \mathbb{F}_2^m} (-1)^{\langle \beta, t \rangle} \widehat{E}_t(\alpha, \gamma)$$

Linear Hull for key-alternating cipher



Linear Hull Theorem

$$r\text{-}\widehat{\text{KeyAlt}}_k(\alpha, \gamma) = 2^n \sum_{\substack{\theta \\ \theta_0 = \alpha, \theta_r = \gamma}} (-1)^{\langle \theta, k \rangle} C_\theta$$

where $\theta \in \mathbb{F}_2^{(r+1)n}$ and $C_\theta = 2^n \prod_{i=0}^{r-1} \widehat{H}_i(\theta_i, \theta_{i+1})$

Tweaks do not introduce new linear trails

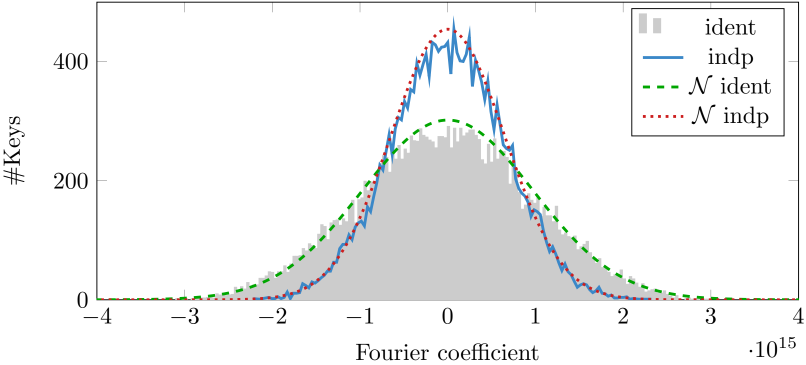
Let r-TweakAlt^L be a tweak-alternating and key-alternating block cipher with linear key-schedule L

$$\widehat{r\text{-TweakAlt}^L}((\alpha,\beta),\gamma) = 2^{(r+2)n} \sum_{\substack{\theta \\ L^T(\theta)=\beta \\ \theta_0=\alpha, \theta_r=\gamma}} (-1)^{\langle \theta, k\rangle} C_\theta$$

Design Consequences

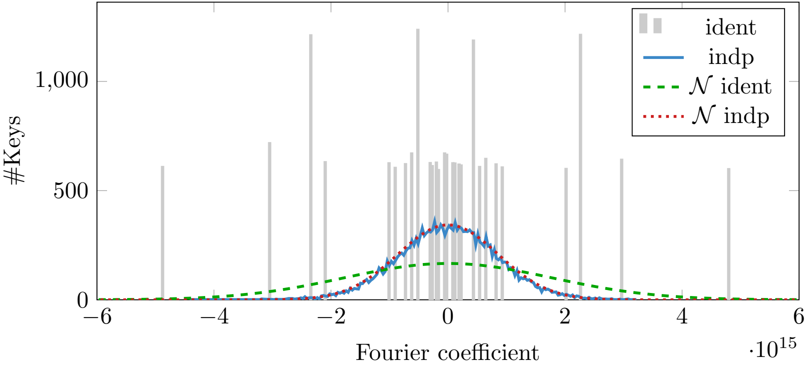
Protecting a tweakable block cipher against linear cryptanalysis can be done in the same way as in the non-tweakable case.

Round-reduced PRESENT with S-box R_0

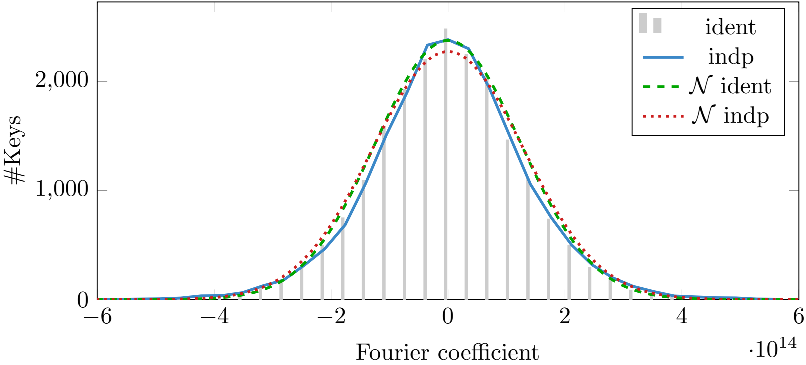


Horst Görtz Institute for IT-Security

Round-reduced PRESENT with S-box R_2



Round-reduced PRESENT with S-box R_3



Round-reduced PRESENT with S-box R_5