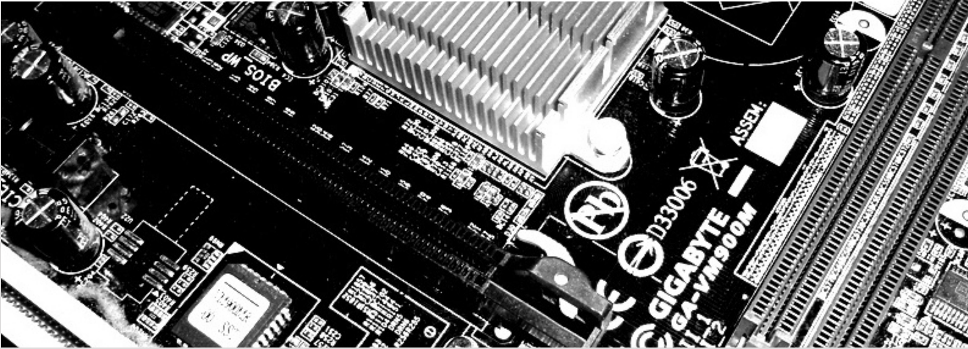
RUHR-UNIVERSITÄT BOCHUM

On the Influence of the Key Scheduling on Linear Approximations

6. April 2016

CITS Oberseminar

Friedrich Wiemer

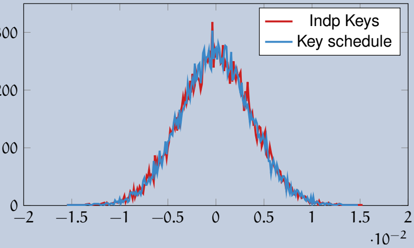


Outline

Assumptions made in Block Cipher Designs

Motivation

Independent Round Keys and Key Schedule Behaviour



Hypothesis of Stochastic Equivalence

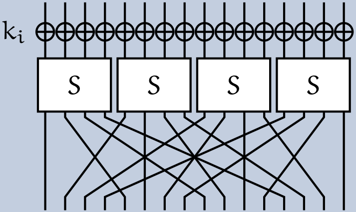
Cipher behaves the same when instantiated with

- independent round keys, or
- round keys generated by key schedule.

SMALLPRESENT

Introduction

SMALLPRESENT-[4]



- SPN
- PRESENT's 4 bit S-box
- Blocksize is $4 \cdot n$
- last round omits permutation

- standard PRESENT: $n = 16$

4 bit S-boxes

Introduction

RUB

Representatives of Serpent-type Equivalence Classes

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$R_0(x)$	0	3	5	6	7	10	11	12	13	4	14	9	8	1	2	15
$R_1(x)$	0	3	5	8	6	9	10	7	11	12	14	2	1	15	13	4
$R_2(x)$	0	3	5	8	6	9	11	2	13	4	14	1	10	15	7	12
$\vdots$									$\dots$							$\vdots$

- all 4 bit S-boxes are classified
- 16 *optimal* and 20 *Serpent-type* equivalence classes

Linear Cryptanalysis (LC)

Introduction

- invented by Matsui 1993–1994
- broke DES
- together with Differential Cryptanalysis (DC) most used attack on block ciphers

- advanced techniques: multidimensional LC, zero-correlation LC, . . .
- links to DC

Image: `http://www.isce2009.ryukoku.ac.jp/eng/keynote_address.html`

Linear Approximations

Introduction

- We want to linear approximate a function $\mathrm{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Linear Approximations

Introduction

- We want to linear approximate a function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$

Dot-Product

$$\langle \alpha, x \rangle = \bigoplus_{i=0}^{n-1} \alpha_i x_i$$

Linear Approximations

Introduction

RUB

- We want to linear approximate a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Dot-Product

$$\langle \alpha, x \rangle = \bigoplus_{i=0}^{n-1} \alpha_i x_i$$

Mask

Let $\alpha, \beta, x \in \mathbb{F}_2^n$ and

$$\langle \alpha, x \rangle = \langle \beta, F(x) \rangle \tag{1}$$

- We say α is an *input mask* and β is an *output mask*.
- Equation 1 does not hold for every input/output masks.

Linear Approximations

Introduction

- We want to linear approximate a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$

Dot-Product

$$\langle \alpha, x \rangle = \bigoplus_{i=0}^{n-1} \alpha_i x_i$$

Mask

Let $\alpha, \beta, x \in \mathbb{F}_2^n$ and

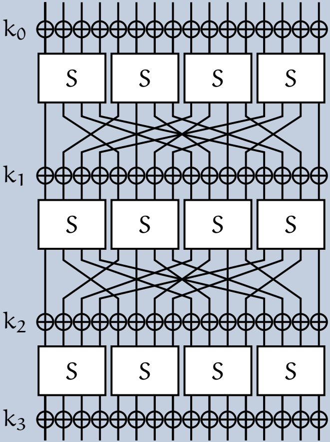
$$\langle \alpha, x \rangle = \langle \beta, F(x) \rangle \qquad (1)$$

- We say α is an *input mask* and β is an *output mask*.
- Equation 1 does not hold for every input/output masks.
- It is *correlated*, i.e., $\Pr[\langle \alpha, x \rangle = \langle \beta, F(x) \rangle] = \frac{c(\alpha,\beta)-1}{2}$.

LC Example: SMALLPRESENT

Introduction

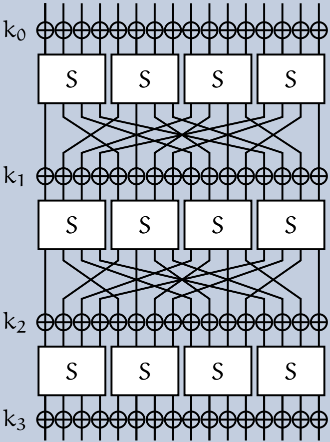
SMALLPRESENT-[4] over 3 Rounds



LC Example: SMALLPRESENT

Introduction

SMALLPRESENT-[4] over 3 Rounds



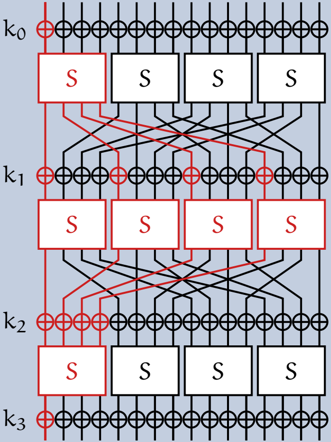
Basically approximate:

- the S-box
- the linear layer

LC Example: SMALLPRESENT

Introduction

SMALLPRESENT-[4] over 3 Rounds



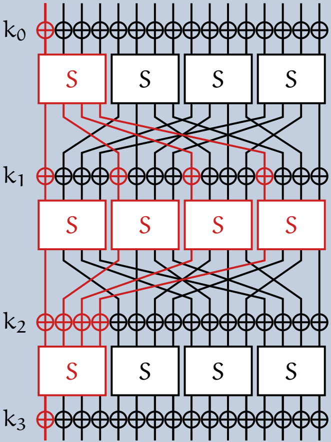
Basically approximate:

- the S-box
- the linear layer

LC Example: SMALLPRESENT

Introduction

SMALLPRESENT-[4] over 3 Rounds



Basically approximate:

- the S-box
- the linear layer

- the linear layer ‘is easy’
- for the S-boxes use *Linear Approximation Table (LAT)*

LC Example: SMALLPRESENT

Introduction

LAT

$\beta \backslash \alpha$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1					−8		−8						−8		8
2		4	4	−4	−4			4	−4		8		8	−4	−4
3		4	4	4	−4	−8		−4	4	−8				−4	4
4		−4	4	−4	−4		8	−4	−4		−8			−4	
5		−4	4	−4	4			4	4	−8		8		4	
6			−8			−8			−8			8			−4
7			8	8					−8					8	−4
8		4	−4			−4	4	−4	4			−4	4	8	−4
9	8	−4	−4			4	−4	−4	−4	−8		−4	4		4
10		8		4	4	4	−4				−8	4	4	−4	8
11	−8			−4	−4	4	−4	−8				4	4	4	
12				−4	−4	−4	−4	8			−8	−4	4	4	4
13	8	8		−4	−4	4	4					4	−4	4	4
14		4	4	−8	8	−4	−4	−4	−4			−4	−4		
15	8	4	−4	4	4			8		4	−4	−4	−4		

Linear Hull

Introduction

- Our example exhibits more than one trail for $(\alpha, \beta) = (15, 15)$
- Key dependency

Linear Hull

Introduction

- Our example exhibits more than one trail for $(\alpha, \beta) = (15, 15)$
- Key dependency

Linear Hull

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher over r rounds,
and $E : \mathbb{F}_2^m \to (\mathbb{F}_2^n)^{r+1}$ a key schedule. The *linear hull* $c_F^k(\alpha, \beta)$ is

$$c_F^k(\alpha, \beta) := \sum_{\theta | \theta_0 = \alpha, \theta_r = \beta} (-1)^{\langle \theta, E(k) \rangle} c_\theta$$

Distributions

Introduction

- Attack complexity of linear cryptanalysis is proportional to $(c_\theta)^{-2}$.

Distributions

Introduction

- Attack complexity of linear cryptanalysis is proportional to $(c_\theta)^{-2}$.

- We assume the *Hypothesis of Stochastic equivalence*.
- Thus, distribution of linear biases follows a normal distribution.
- Its width is defined by the variance.

Distributions

Introduction

- Attack complexity of linear cryptanalysis is proportional to $(c_\theta)^{-2}$.

- We assume the *Hypothesis of Stochastic equivalence*.
- Thus, distribution of linear biases follows a normal distribution.
- Its width is defined by the variance.

- What happens with different key schedules?

SMALLPRESENT variants

Experiments

Independent Round Keys

$$k = (k_0, \ldots, k_r) \in (\mathbb{F}_2^n)^{r+1}$$

$$\begin{array}{ccc} k_0 & \longrightarrow & k_0 \\ k_1 & \longrightarrow & k_1 \\ \vdots & & \\ k_r & \longrightarrow & k_r \end{array}$$

Constant Round Keys

$$k \in \mathbb{F}_2^n$$

$$\begin{array}{ccc} k & \longrightarrow & k_0 \\ k & \longrightarrow & k_1 \\ \vdots & & \\ k & \longrightarrow & k_r \end{array}$$

S-boxes

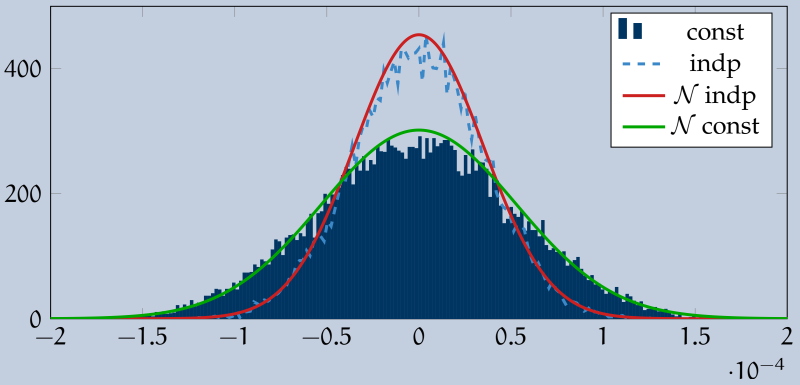
choose $S \in \{R_0, \ldots, R_{19}\}$

Distributions

Results

RUB

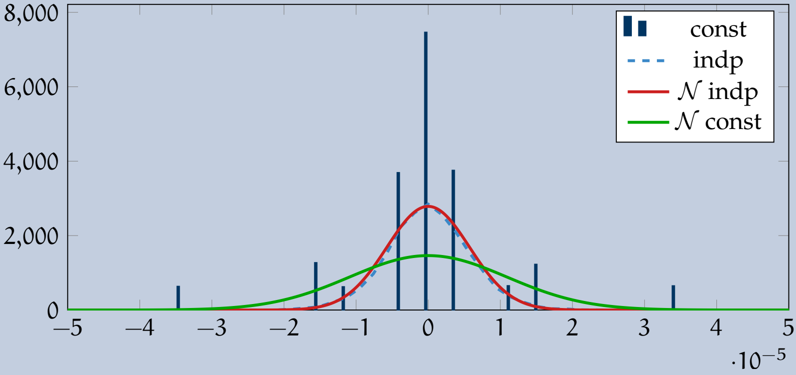
SMALLPRESENT-[16] with $\mathcal{R}_0$, 10 rounds



Distributions

Results

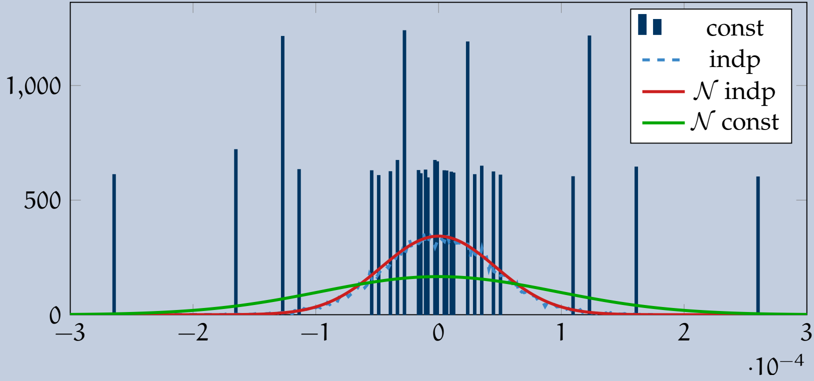
SMALLPRESENT-[16] with R_1, 10 rounds



Distributions

Results

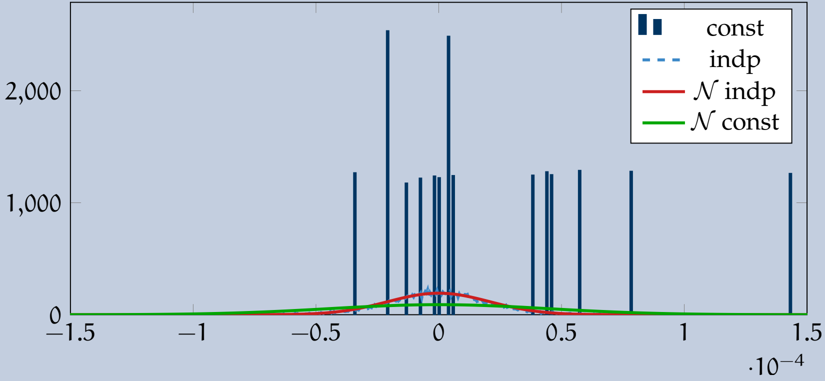
SMALLPRESENT-[16] with R_2, 10 rounds



Distributions

Results

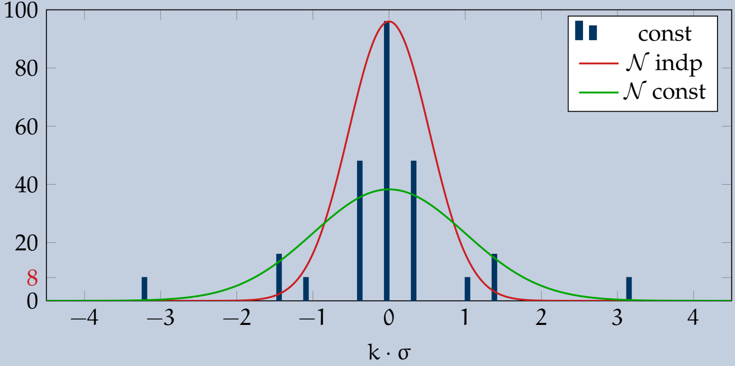
SmallPresent-[16] with $\mathcal{R}_2$, 11 rounds



More Distributions for R_1

Results

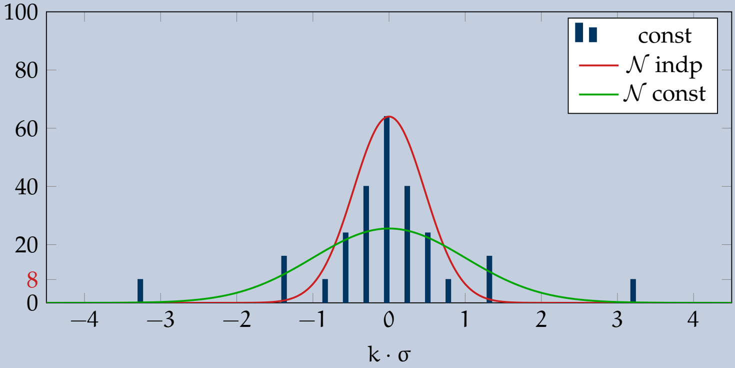
SMALLPRESENT-[16] with R_1, 10 rounds



More Distributions for $\mathcal{R}_1$

Results

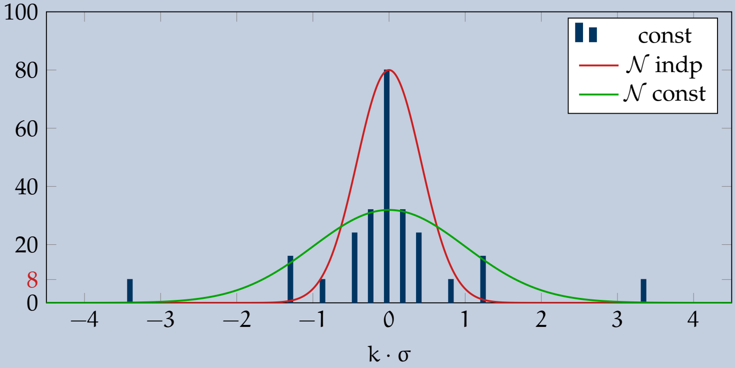
SMALLPRESENT-[16] with $\mathcal{R}_1$, 11 rounds



More Distributions for R_1

Results

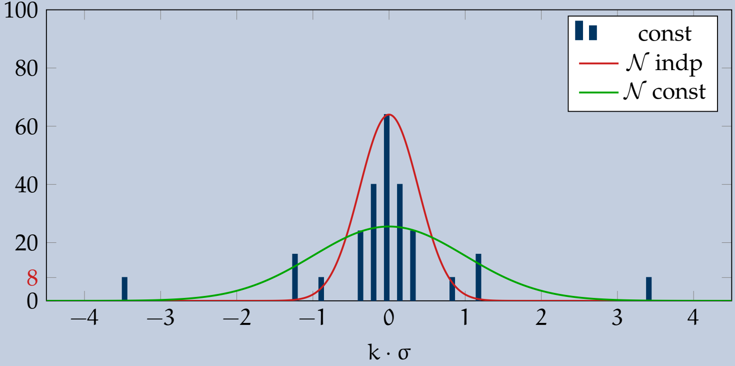
SMALLPRESENT-[16] with R_1, 12 rounds



More Distributions for $\mathcal{R}_1$

Results

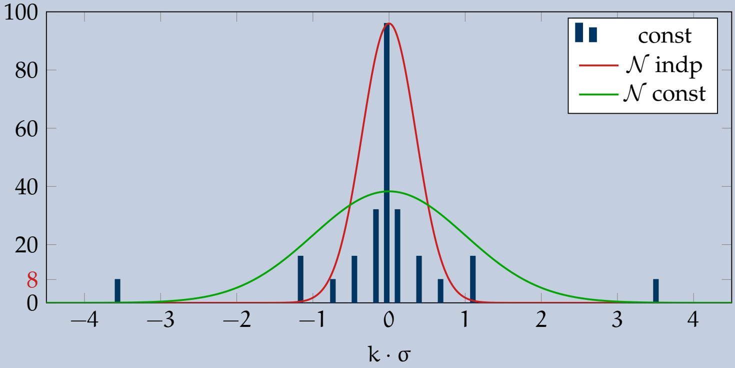
SMALLPRESENT-[16] with $\mathcal{R}_1$, 13 rounds



More Distributions for R_1

Results

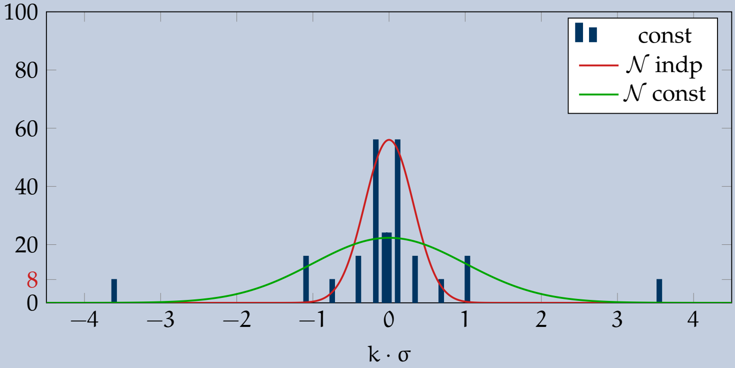
SMALLPRESENT-[16] with R_1, 14 rounds



More Distributions for R_1

Results

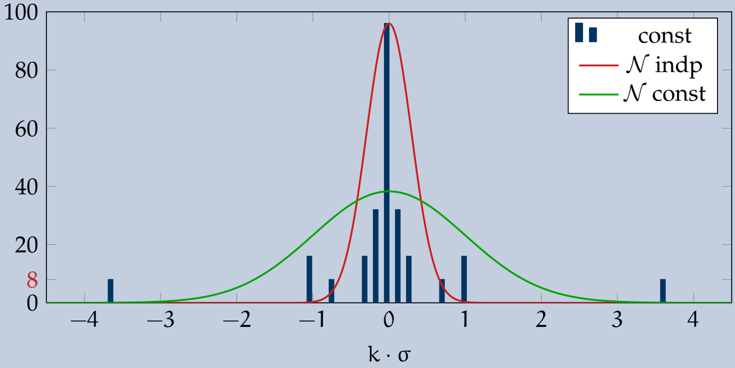
SmallPresent-[16] with R_1, 15 rounds



More Distributions for R_1

Results

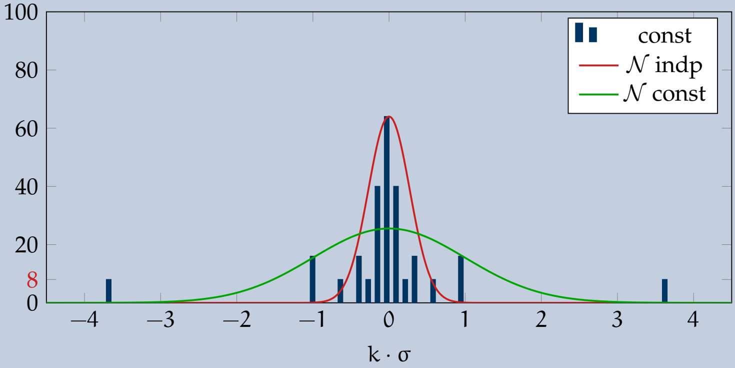
SMALLPRESENT-[16] with R_1, 16 rounds



More Distributions for R_1

Results

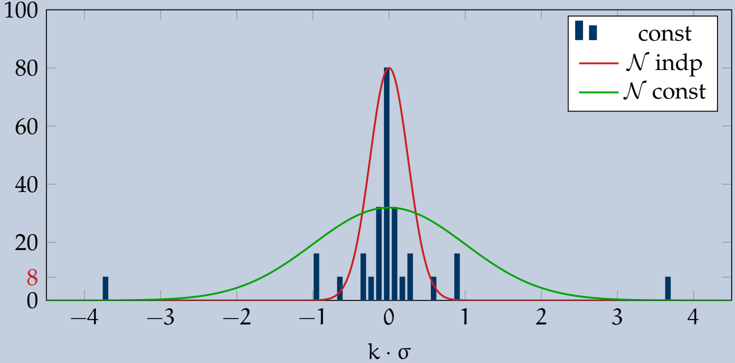
SMALLPRESENT-[16] with R_1, 17 rounds



More Distributions for R_1

Results

SMALLPRESENT-[16] with R_1, 18 rounds

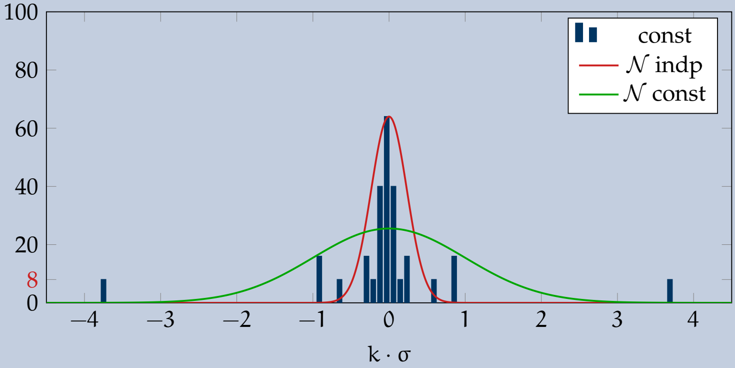


More Distributions for R_1

Results

RUB

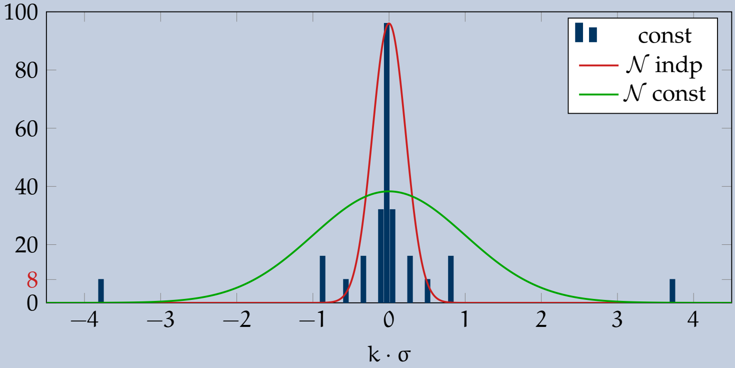
SMALLPRESENT-[16] with R_1, 19 rounds



More Distributions for R_1

Results

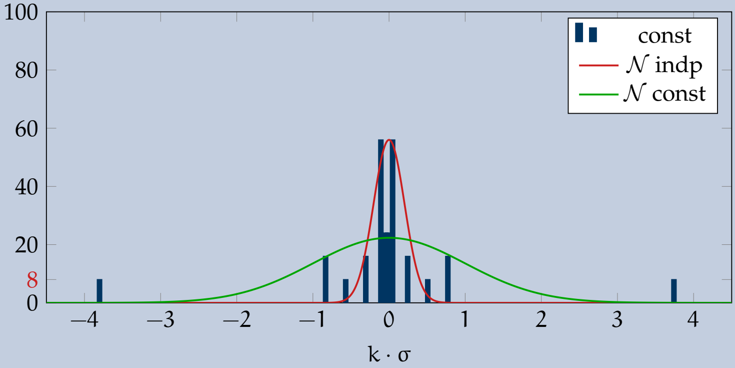
SMALLPRESENT-[16] with R_1, 20 rounds



More Distributions for R_1

Results

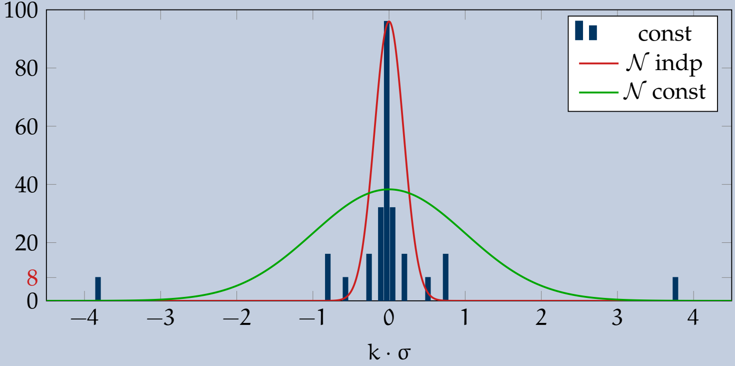
SMALLPRESENT-[16] with R_1, 21 rounds



More Distributions for R_1

Results

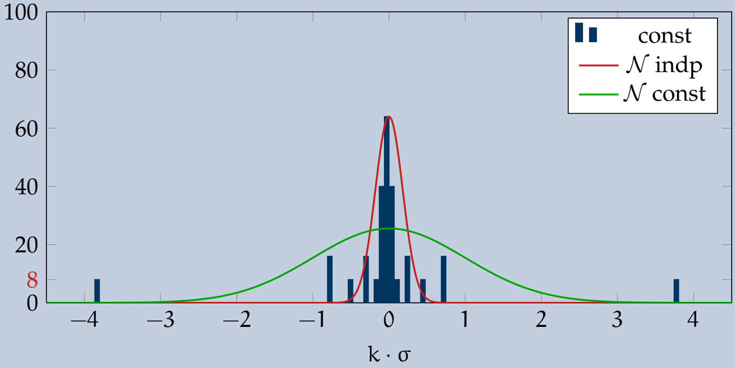
SMALLPRESENT-[16] with R_1, 22 rounds



More Distributions for R_1

Results

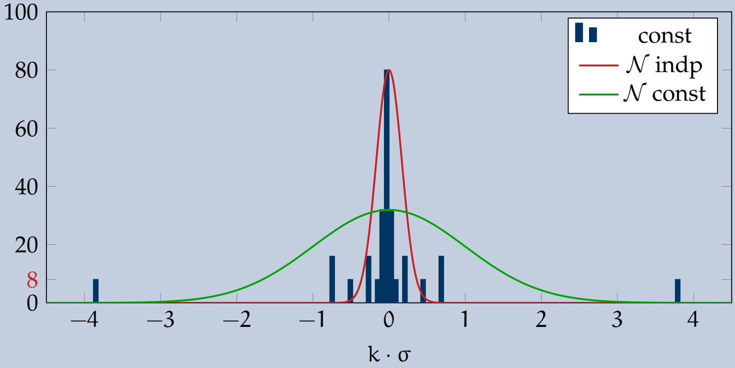
SMALLPRESENT-[16] with R_1, 23 rounds



More Distributions for R_1

Results

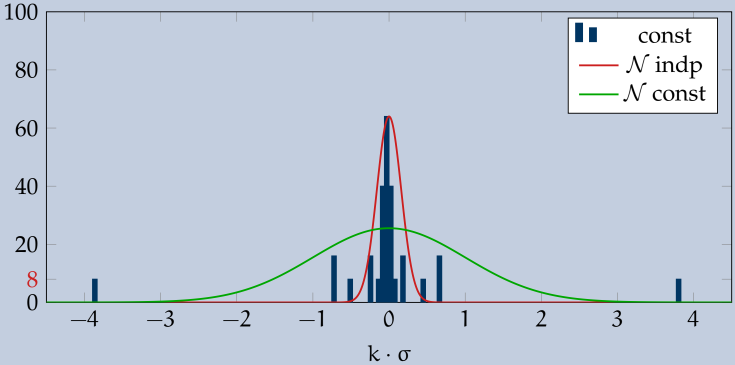
SMALLPRESENT-[16] with R_1, 24 rounds



More Distributions for R_1

Results

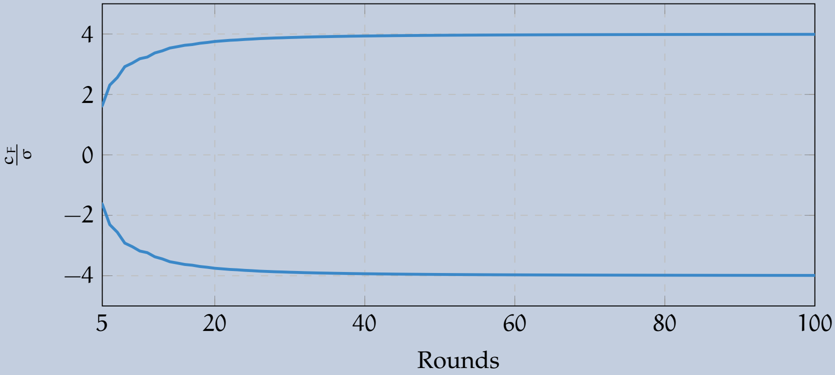
SmallPresent-[16] with R_1, 25 rounds



Behaviour over more rounds

Results

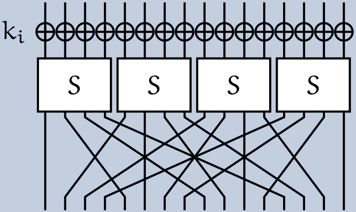
Min/Max correlation with S-box R_1, normalised to standard deviations



Induced Graph

Results

SmallPresent-[4]

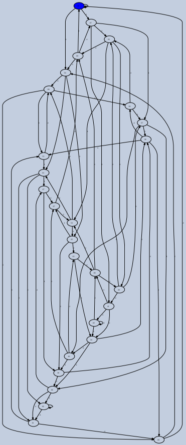


- adjacency matrix from ciphers round function
- each bit is a vertex
- each non-zero entry in the LAT is an edge

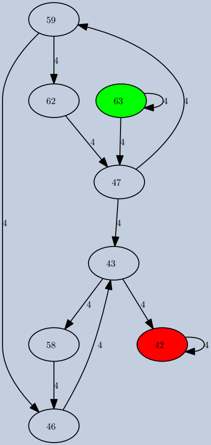
Induced Graph

Results

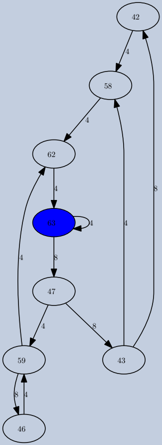
S-box R_0



S-box R_1



S-box R_2



A new (un-) secure PRESENT variant

Future Work

Proposal

- PRESENT with $\mathcal{R}_2$ as S-box
- 31 encryption rounds
- Constant key schedule

A new (un-) secure PRESENT variant

Future Work

Proposal

- PRESENT with $\mathcal{R}_2$ as S-box
- 31 encryption rounds
- Constant key schedule

Problem: Constant key schedule is suspicious

- Slide attacks
- Wider distribution is known

Future Work

Invariant Subspaces (Inv. Subs) in Key Schedules

- Invariant subspaces can be equivalent to constant round keys.
- Can we construct functions with specific Inv. Subs?
- Is there an unsuspicious key schedule with an Inv. Sub?

Future Work

Invariant Subspaces (Inv. Subs) in Key Schedules

- Invariant subspaces can be equivalent to constant round keys.
- Can we construct functions with specific Inv. Subs?
- Is there an unsuspicious key schedule with an Inv. Sub?

Hypothesis of Stochastic Equivalence

- Find an explanation for observed behaviour.

Future Work

Invariant Subspaces (Inv. Subs) in Key Schedules

- Invariant subspaces can be equivalent to constant round keys.
- Can we construct functions with specific Inv. Subs?
- Is there an unsuspicious key schedule with an Inv. Sub?

Hypothesis of Stochastic Equivalence

- Find an explanation for observed behaviour.

Hypothesis of Wrong Key Randomisation

- Scrutinise wrong key behaviour.

Questions?

Thank you for your attention!

Mainboard & Questionmark Images: flickr