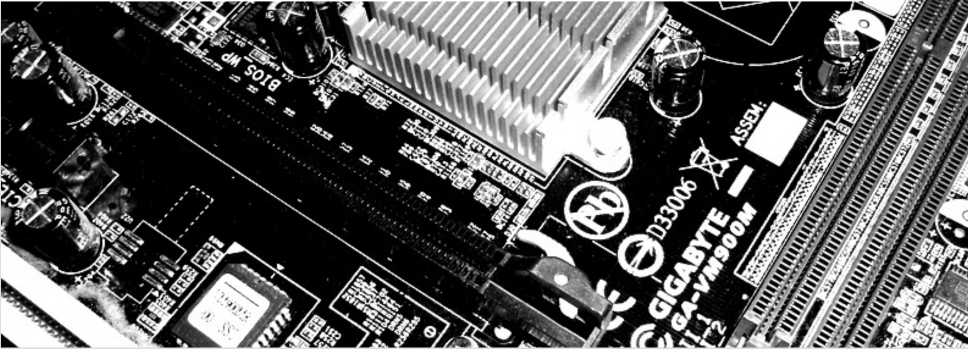
RUHR-UNIVERSITÄT BOCHUM

Distribution of Linear Biases in PRESENT

16. July 2015

EMSEC/SHA Seminar
Horst Görtz Institute for IT-Security
Ruhr University Bochum

Friedrich Wiemer



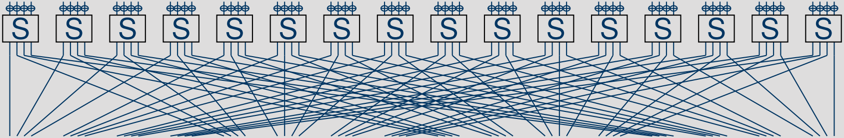
Outline

Introduction to Linear Cryptanalysis

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

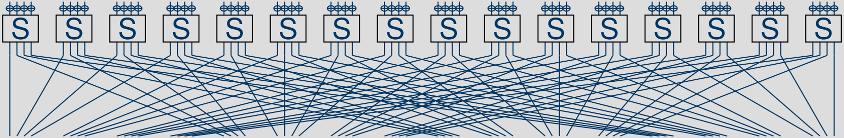
Image: http://www.isce2009.ryukoku.ac.jp/eng/keynote_address.html

PRESENT



- Let $F_{k_i} : \mathbb{F}_2^{64} \rightarrow \mathbb{F}_2^{64}$ be the round function that xor's the key k_i and applies the substitution and permutation layer.

PRESENT



- Let $F_{k_i} : \mathbb{F}_2^{64} \rightarrow \mathbb{F}_2^{64}$ be the round function that xor's the key k_i and applies the substitution and permutation layer.
- Can we approximate this function?

Linear Approximations

Dot-Product, Masks and Linear Bias

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

Linear Approximations

Dot-Product, Masks and Linear Bias

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

Dot-Product

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

Linear Approximations

Dot-Product, Masks and Linear Bias

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

Dot-Product

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

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

Dot-Product, Masks and Linear Bias

- 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

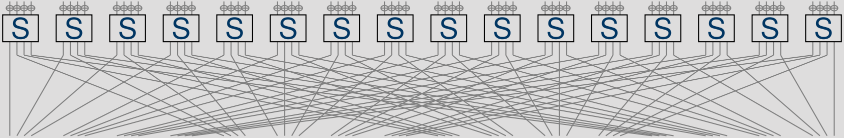
Let $\alpha, \beta, x \in \mathbb{F}_2^n$ and

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

- 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 *biased*, i.e., $\Pr[\langle \alpha, x \rangle = \langle \beta, F(x) \rangle] = \frac{1}{2} - \varepsilon(\alpha, \beta)$.

PRESENT

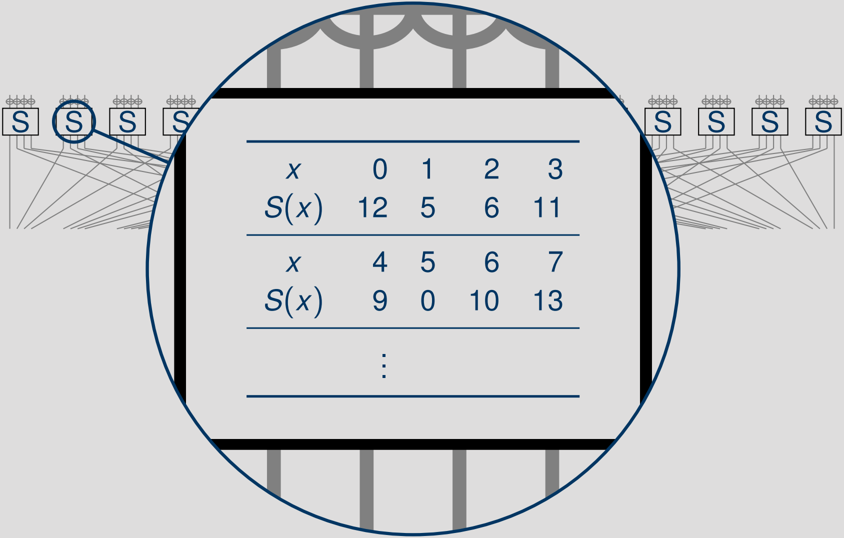
S-box and Linear Approximation Table



- The only difficult part of F_{k_i} is the (non-linear) substitution layer.

PRESENT

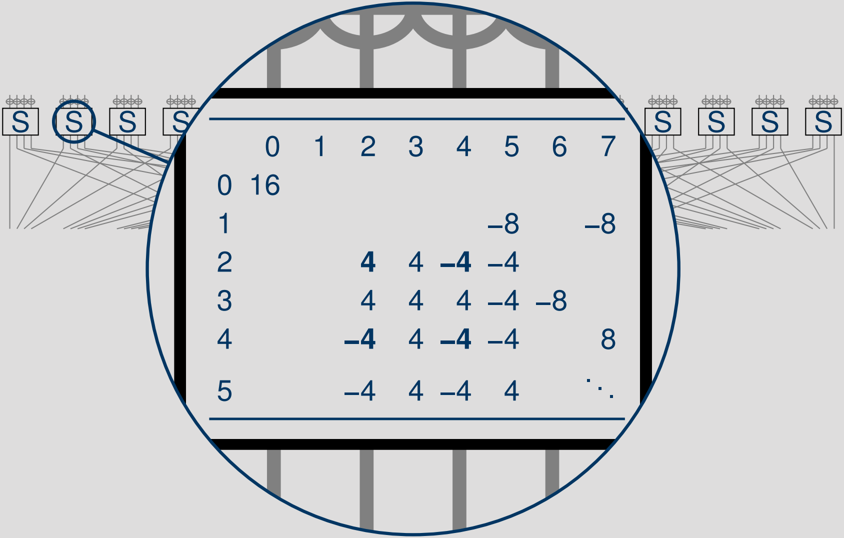
S-box and Linear Approximation Table



x	0	1	2	3
$S(x)$	12	5	6	11
x	4	5	6	7
$S(x)$	9	0	10	13
	⋮			

PRESENT

S-box and Linear Approximation Table



	0	1	2	3	4	5	6	7
0	16							
1						−8		−8
2			**4**	4	**−4**	−4		
3			4	4	4	−4	−8	
4			**−4**	4	**−4**	−4		8
5			−4	4	−4	4		⋱

Distributions

RUB

- Attack complexity of linear cryptanalysis is proportional to $\frac{1}{\varepsilon^2}$.
- In experiments, we observe a key dependency of the linear bias.

Distributions

- Attack complexity of linear cryptanalysis is proportional to $\frac{1}{\varepsilon^2}$.
- In experiments, we observe a key dependency of the linear bias.

- The distribution of linear biases follows a normal distribution.
- Its width is defined by the variance.

Distributions

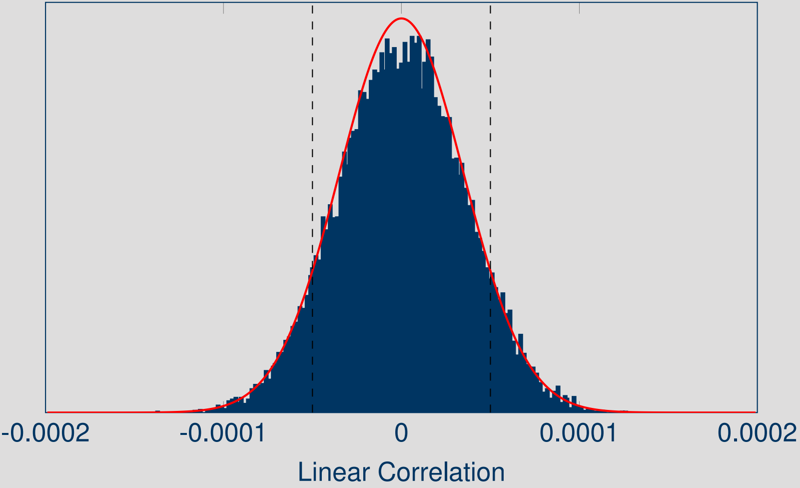
- Attack complexity of linear cryptanalysis is proportional to $\frac{1}{\varepsilon^2}$.
- In experiments, we observe a key dependency of the linear bias.

- The distribution of linear biases follows a normal distribution.
- Its width is defined by the variance.

- What happens with different key-schedules?

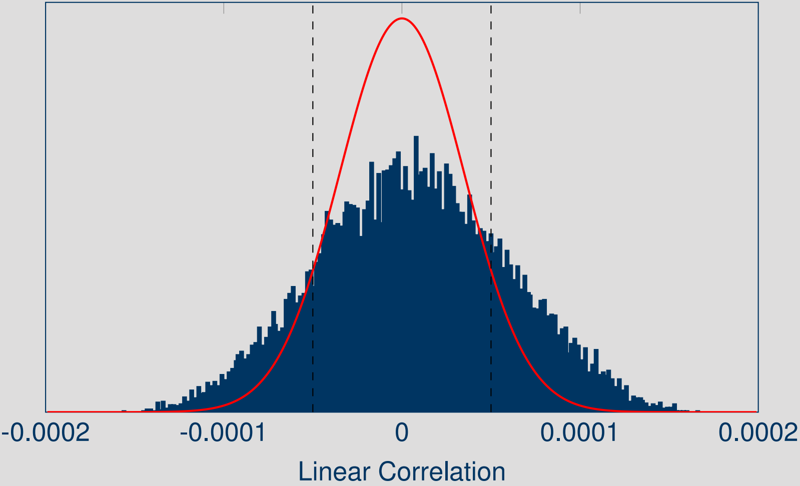
Distributions

Independent Round Keys



Distributions

Constant Round Keys



Questions?

Thank you for your attention!

Mainboard & Questionmark Images: flickr