RUHR-UNIVERSITÄT BOCHUM

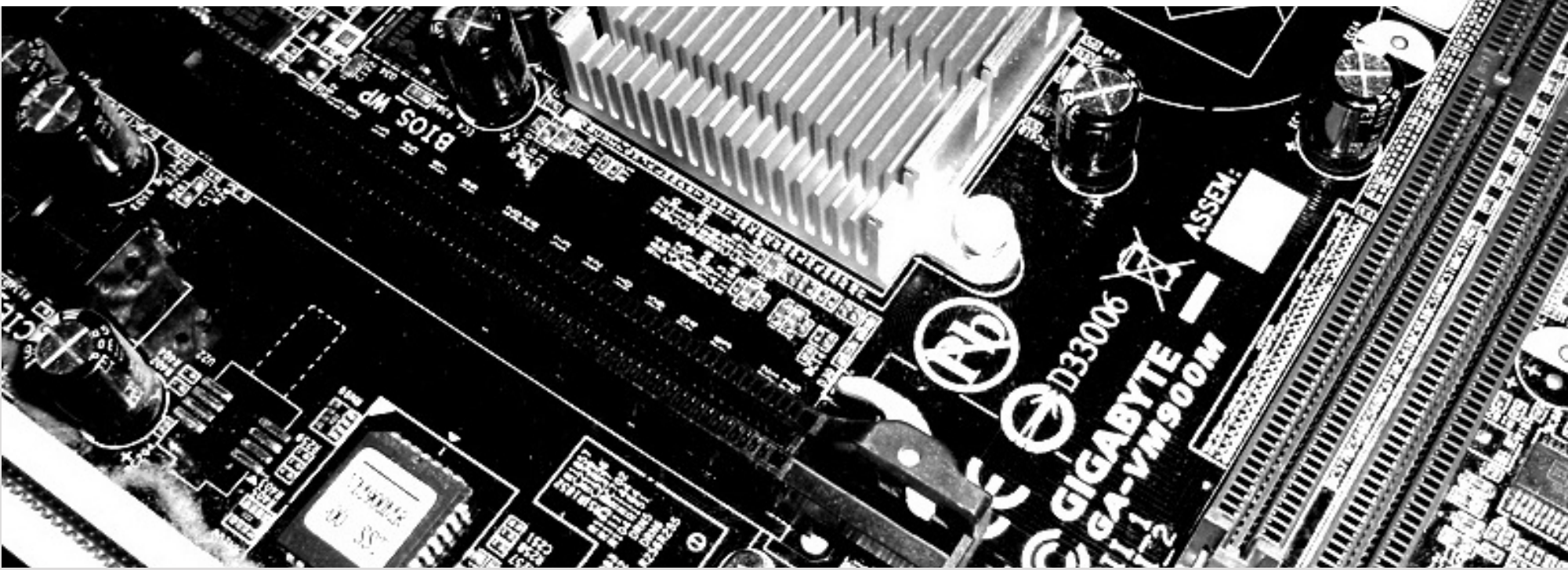
Analysis and Design of Ciphers for the IoT

October 4th, 2016

Workgroup Symmetric Cryptography
UbiCrypt – Horst Görtz Institute
Ruhr University Bochum

Friedrich Wiemer

UbiCrypt
Cryptography in Ubiquitous Computing



Progress

- Started my PhD

Progress

- Started my PhD
- . . .

Questions?

Thank you for your attention!

Mainboard & Questionmark Images: flickr

Progress

- High-Speed Implementation of bcrypt Password Search using Special-Purpose Hardware

  (Wiemer, Zimmermann: ReConfig 2014)

Progress

- High-Speed Implementation of bcrypt Password Search using Special-Purpose Hardware

  (Wiemer, Zimmermann: ReConfig 2014)

- Parallel Implementation of BDD enumeration for LWE

  (Kirshanova, May, Wiemer: ACNS 2016)

Progress

RUB

- High-Speed Implementation of bcrypt Password Search using Special-Purpose Hardware

  (Wiemer, Zimmermann: ReConfig 2014)

- Parallel Implementation of BDD enumeration for LWE

  (Kirshanova, May, Wiemer: ACNS 2016)

- Linear Cryptanalysis: Key Schedules and Tweakable Block Ciphers

  (Kranz, Leander, Wiemer: in submission)

Progress

- High-Speed Implementation of bcrypt Password Search using Special-Purpose Hardware

  (Wiemer, Zimmermann: ReConfig 2014)
- Parallel Implementation of BDD enumeration for LWE

  (Kirshanova, May, Wiemer: ACNS 2016)
- Linear Cryptanalysis: Key Schedules and Tweakable Block Ciphers

  (Kranz, Leander, Wiemer: in submission)

- Future
  - Read more paper and do more research
  - Cross-Disciplinary Project and Research Visit
  - Basically: enjoy my PhD 😎

Linear Cryptanalysis

See Thorsten's slides.

Linear Cryptanalysis

RUB

See Thorsten's slides.

Fourier Coefficient for *Key-Alternating Function*

$$\widehat{F}_k(\alpha,\gamma) := \sum_{\beta\in\mathbb{F}_2^n} (-1)^{\langle\beta,k\rangle}\widehat{F}(\alpha,\gamma) = \sum_{\substack{\beta\in\mathbb{F}_2^n\\ x\in\mathbb{F}_2^n}} (-1)^{\langle\alpha,x\rangle+\langle\beta,k\rangle+\langle\gamma,F(x)\rangle}$$

Linear Cryptanalysis

RUB

See Thorsten's slides.

Fourier Coefficient for *Key-Alternating Function*

$$\widehat{F}_k(\alpha,\gamma) := \sum_{\beta\in\mathbb{F}_2^n} (-1)^{\langle\beta,k\rangle}\widehat{F}(\alpha,\gamma) = \sum_{\substack{\beta\in\mathbb{F}_2^n\\ x\in\mathbb{F}_2^n}} (-1)^{\langle\alpha,x\rangle+\langle\beta,k\rangle+\langle\gamma,F(x)\rangle}$$

But:

- How to (*efficiently?*) compute the Fourier Coefficient?
- How does the key dependency influence our cipher's security?
- How does the key schedule influence the Fourier Coefficient?

Computing the Fourier Coefficient

Experimentally

Correct way:

- Choose α and γ.
- For all possible β *and*
  For all possible keys *and*
  For all possible plaintexts
  - Either increase or decrease the Fourier Coefficient's sum

Computing the Fourier Coefficient

Experimentally

Correct way:

- Choose α and γ.
- For all possible β *and*
  For all possible keys *and*
  For all possible plaintexts
  - Either increase or decrease the Fourier Coefficient's sum

Not feasible for real world ciphers. Thus approximate:

- Choose α and γ.
- For *many* β *and*
  For *many* keys *and*
  For *many* plaintexts
  - Either increase or decrease the Fourier Coefficient's sum

Computing the Fourier Coefficient

Ohkuma's Observation

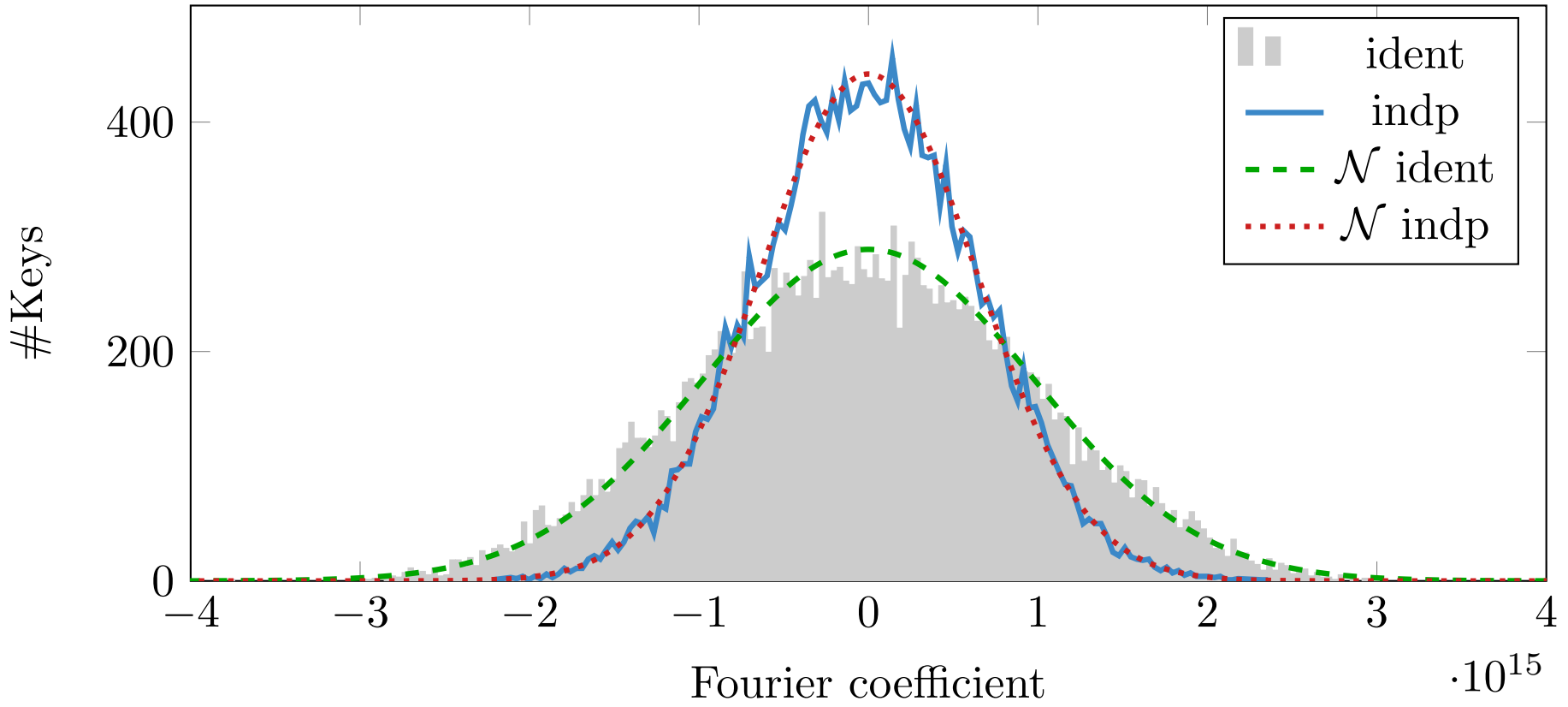
Experiments with PRESENT

Different S-boxes and Constant Round Keys

Experiments with PRESENT

Resulting Fourier Coefficient Distributions

Standard PRESENT

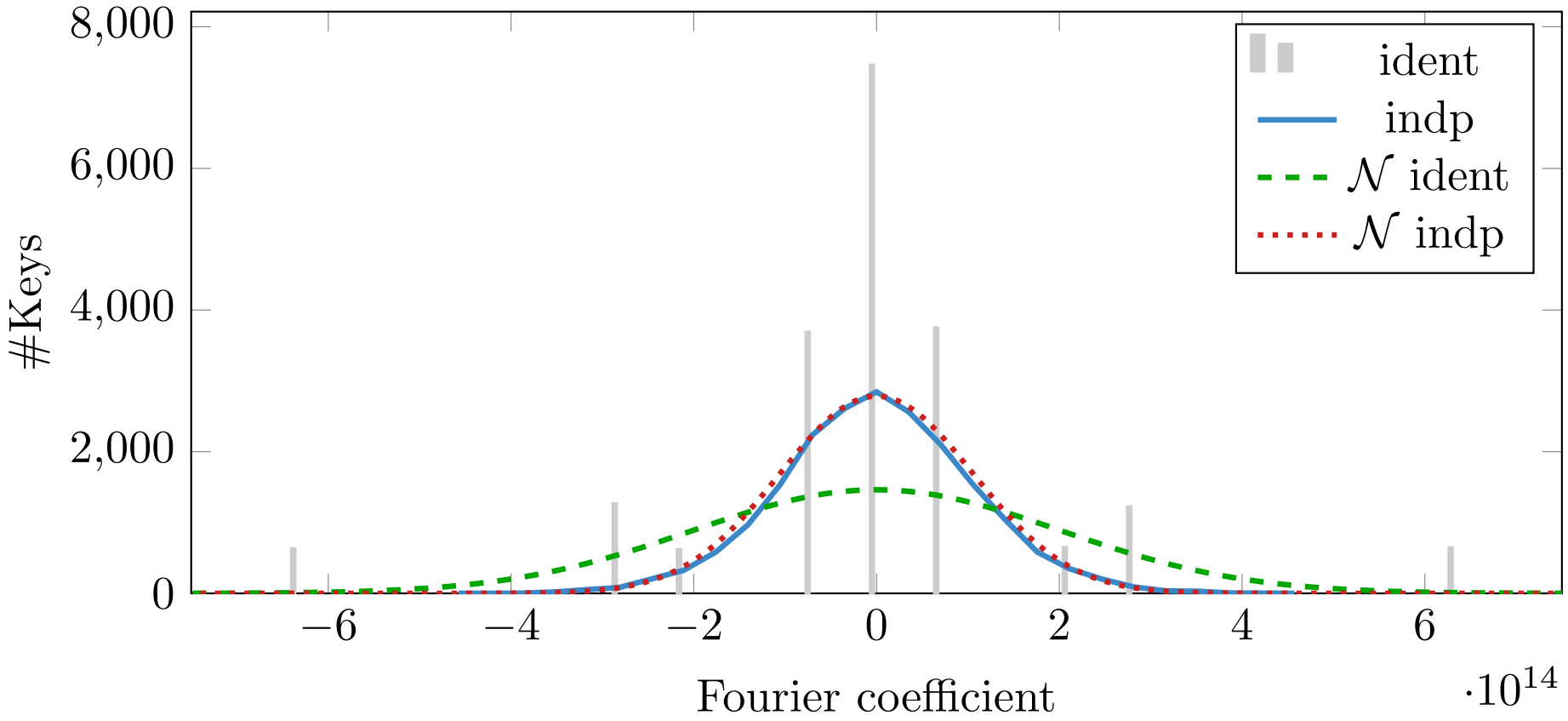


Experiments with PRESENT

Tchebysheff's Bound

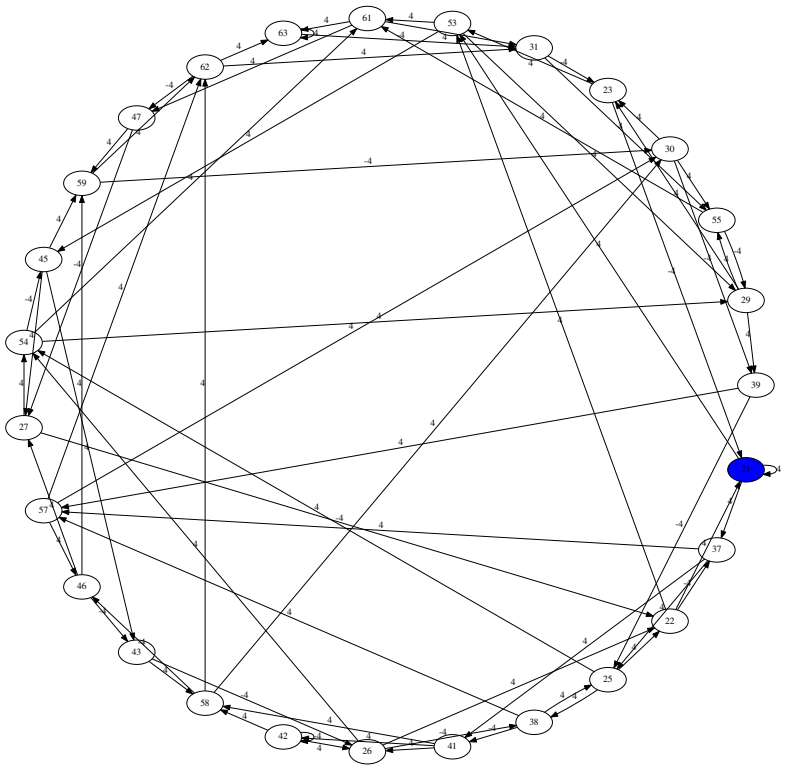
RUB

PRESENT with different S-box

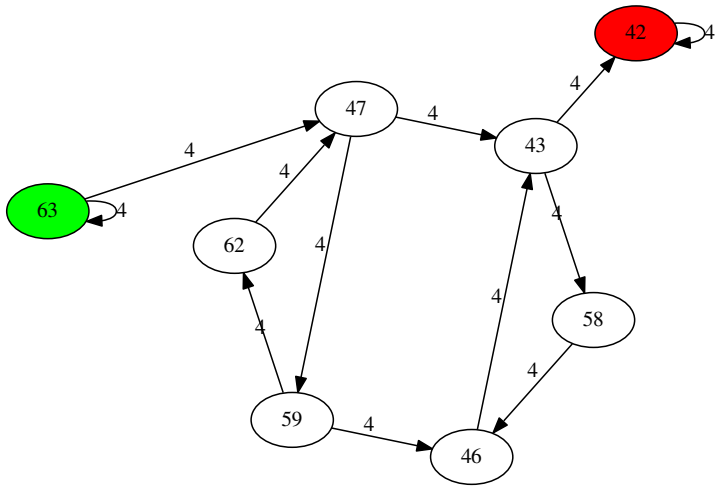


Key Influence

Standard PRESENT



PRESENT with different S-box



Wrap Up

Design Consequences

We cannot hope to prove better results for generic SPN's than Tchebysheff's bound.

Wrap Up

Design Consequences

We cannot hope to prove better results for generic SPN's than Tchebysheff's bound.

Thank you for your attention!
Any quesions?