

# Security Arguments and Tool-based Design of Block Ciphers

April 6th, 2020

Friedrich Wiemer

RUB





# whoami

Friedrich Wiemer



# whoami

Friedrich Wiemer

Private





Private



IT-Security at Ruhr Uni Bochum





# whoami

Friedrich Wiemer

## Private



## Doctoral Studies

Topic:

Design & Analysis of Block Ciphers *for the IoT*

## IT-Security at Ruhr Uni Bochum





# whoami

Friedrich Wiemer

Private



Doctoral Studies

Topic:

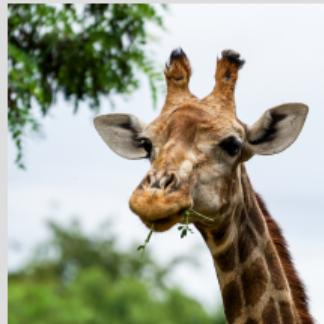
Design & Analysis of Block Ciphers *for the IoT*

IT-Security at Ruhr Uni Bochum



cryptosolutions





[asante.dev/photos](http://asante.dev/photos)

- "High-Speed Implementation of bcrypt Password Search using Special-Purpose Hardware"
- "Parallel Implementation of BDD enumeration for LWE"
- "Out of Oddity – New Cryptanalytic Techniques against Symmetric Primitives Optimized for Integrity Proof Systems"

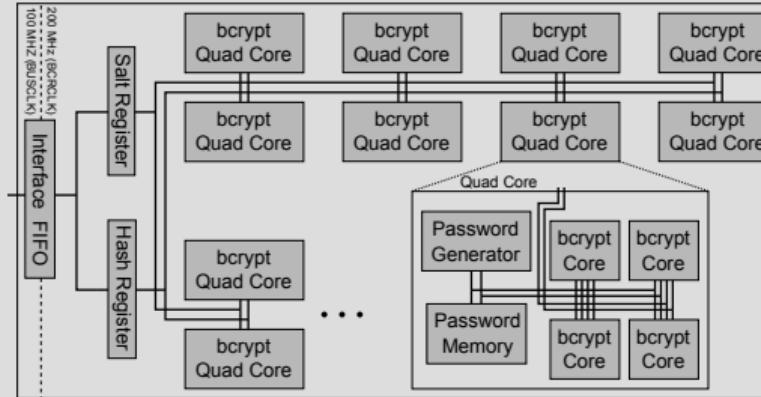
## Topics besides PhD Thesis

A white rectangular box containing various research topics and their connections. The topics include:

- LWE
- CVP
- VHDL
- PARALLEL
- STARK
- FPGA
- BLOCKCHAIN
- PASSWORD CRACKING
- CRYPTANALYSIS OF LATTICE-BASED CRYPTO
- CRYPTANALYSIS OF ALGEBRAIC-OPTIMISED HASHES
- NEAREST PLANES
- BDD ENUMERATION

The topics are arranged in a non-linear, overlapping manner, suggesting interconnected research areas.

# High-Speed Implementation of bcrypt Password Search



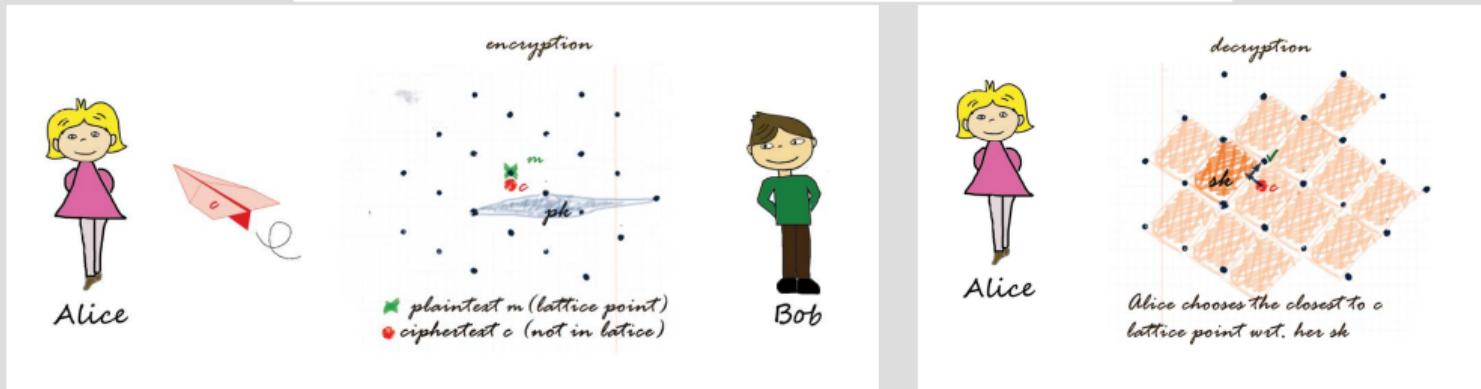
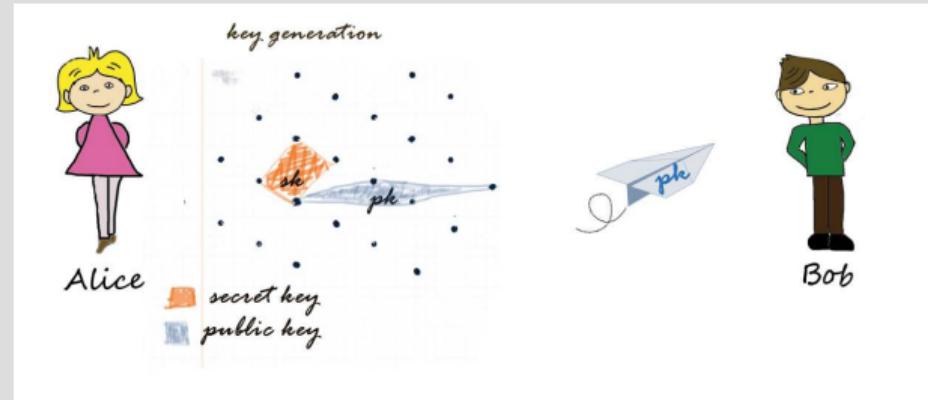
```
root@localhost:~# hexdump -C -v -n 64 /dev/xillybus_mem_8
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000040
root@localhost:~#
```

Salt Hash Password Status Register

The screenshot shows a terminal window displaying the output of the 'hexdump' command. The memory dump is divided into four columns: Salt, Hash, Password, and Status Register. The first three columns each contain 16 bytes of zeros. The fourth column, labeled 'Status Register', contains zeros for the first 15 bytes and a red box around the 16th byte, which is also zero.

- Zedboard implementation: 4x increase to previous work

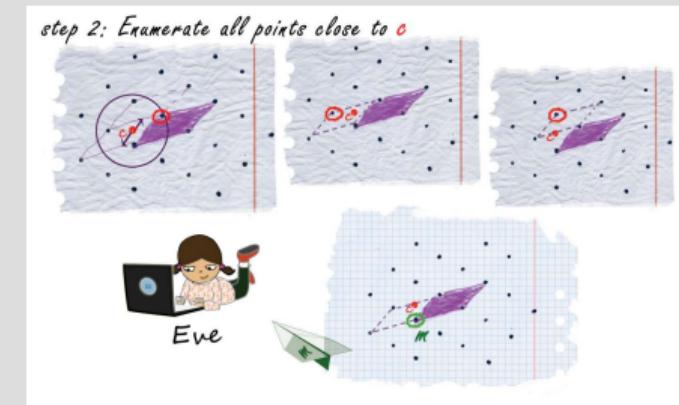
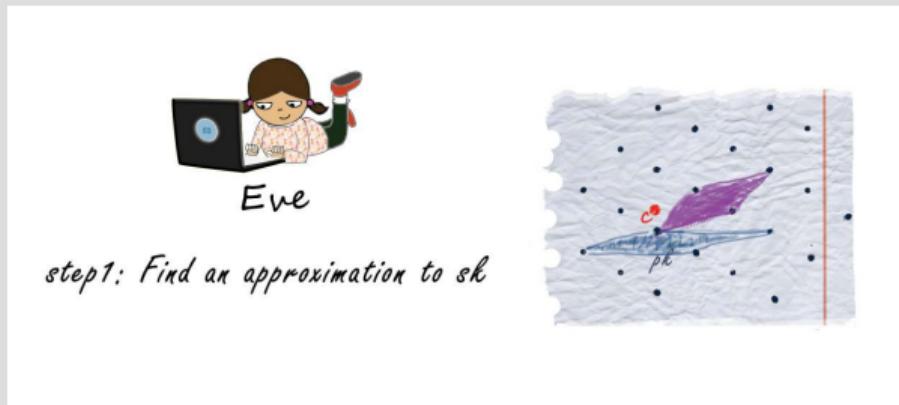
# Parallel Implementation of BDD enumeration for LWE



# Parallel Implementation of BDD enumeration for LWE



# Parallel Implementation of BDD enumeration for LWE



- Result: Enumeration step can be very good parallelized; Best Student Paper award at ACNS.

- “Linear Cryptanalysis: Key Schedules and Tweakable Block Ciphers”
- “Shorter Linear Straight-Line Programs for MDS Matrices”
- “Searching for Subspace Trails and Truncated Differentials”
- “BISON”
- “Observations on the DLCT and Absolute Indicators”
- (“Spook”)

## Topics of PhD Thesis



# Topic Classification within Symmetric Crypto

Security

vs.

Efficiency

SoK: Linear Cryptanalysis

Theory

Subspace Trail Analysis

Theory

Algorithm

Shorter SLPs

Implementation

BISON

Instantiation

DLCT

Theory

Spook

Instantiation

# Activity in the Cryptographic Community



RUHR  
UNIVERSITÄT  
BOCHUM

# RUB

Home Current Archives Submissions FAQ Editorial Board Contact FSE

IACR Transactions on Symmetric Cryptology

News

- FSE 2020 has been postponed to November 8-12 due to the COVID-19 outbreak. The schedule of the FSE 2021 conference might also be modified.
- The submission server for ToSC 2020, Issue 2 is up.
- The timeline and Call for Papers for 2020/2021 are available.
- The Call for Papers for the Special Issue on Designs for the NIST Lightweight Standardisation Process is online.
- The Volume 2019 third issue is available.
- ToSC is now indexed by Scopus.
- ToSC is now indexed by DOAJ.

General Information

The IACR Transactions on Symmetric Cryptology (ToSC) has the ISSN 2519-173X.



RUHR  
UNIVERSITÄT  
BOCHUM

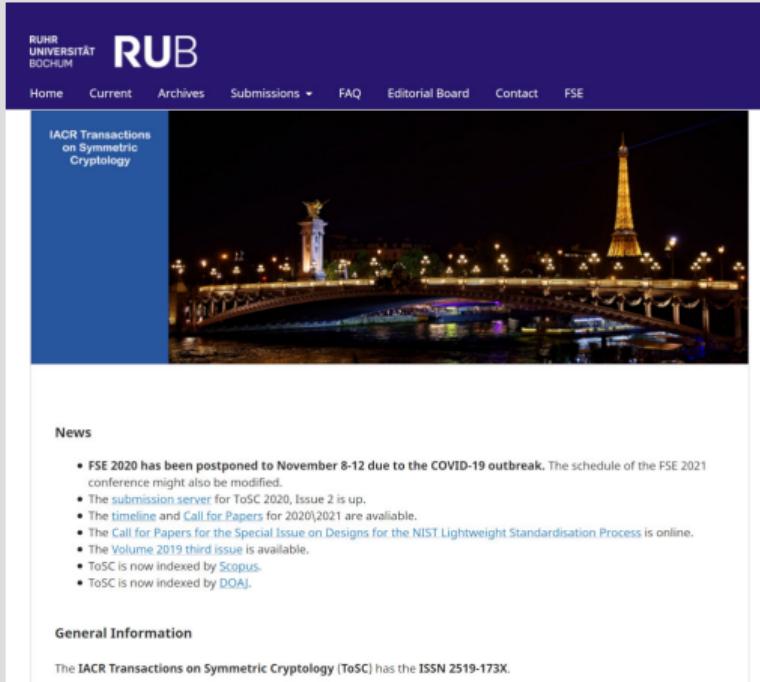
# RUB

Home Current Archives Call for Papers Paper Submission Editorial Board FAQ CHES Contact

IACR Transactions on Cryptographic Hardware and Embedded Systems

- IACR Conferences move to *Gold Open Access* publications
- Published by Ruhr Uni Bochum

# Activity in the Cryptographic Community



The screenshot shows the homepage of the IACR Transactions on Symmetric Cryptology (ToSC) website. At the top, there is a dark blue header bar with the Ruhr University Bochum logo and the RUB logo. Below the header, a large banner image of the Eiffel Tower and the Seine River at night is displayed. The main content area has a white background. On the left side, there is a sidebar with the title "IACR Transactions on Symmetric Cryptology". The main content area contains a "News" section with a bullet-point list about the postponement of the FSE 2020 conference due to COVID-19, and a "General Information" section mentioning the ISSN 2519-173X.

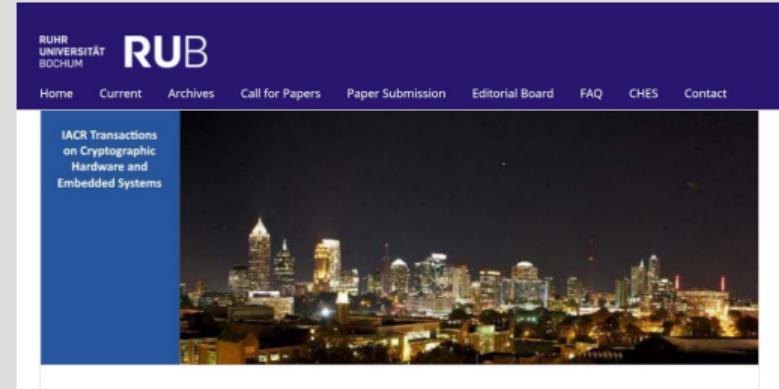
IACR Transactions on Symmetric Cryptology

News

- FSE 2020 has been postponed to November 8-12 due to the COVID-19 outbreak. The schedule of the FSE 2021 conference might also be modified.
- The submission server for ToSC 2020, Issue 2 is up.
- The timeline and Call for Papers for 2020/2021 are available.
- The Call for Papers for the Special Issue on Designs for the NIST Lightweight Standardisation Process is online.
- The Volume 2019 third issue is available.
- ToSC is now indexed by Scopus.
- ToSC is now indexed by DOAJ.

General Information

The IACR Transactions on Symmetric Cryptology (ToSC) has the ISSN 2519-173X.



The screenshot shows the homepage of the IACR Transactions on Cryptographic Hardware and Embedded Systems (ToCRES) website. It features a dark blue header bar with the Ruhr University Bochum logo and the RUB logo. A banner image of a city skyline at night is visible. The main content area includes a sidebar with the title "IACR Transactions on Cryptographic Hardware and Embedded Systems".

IACR Transactions on Cryptographic Hardware and Embedded Systems

- IACR Conferences move to *Gold Open Access* publications
- Published by Ruhr Uni Bochum

- NIST Lightweight Crypto Competition (LWC) round 2 candidate: Spook

- Open Source Computer Algebra System
- Supports Components of Cryptographic Algorithms (S-boxes, Boolean Functions)
- Useful to play with mathematical structures
- Nice open source project to contribute to (my contributions)

```
@cached_method
def difference_distribution_table(self):
    m, n = self.input_size(), self.output_size()
    nrows, ncols = 1<<m, 1<<n
    A = Matrix(ZZ, nrows, ncols)
    for i in range(nrows):
        si = self(i)
        for di in range(nrows):
            A[di, si^self(i^di)] += 1
    A.set_immutable()
    return A
```