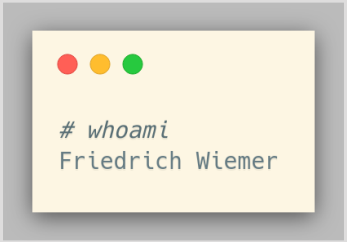
RUHR-UNIVERSITÄT BOCHUM

Security Arguments and Tool-based Design of Block Ciphers

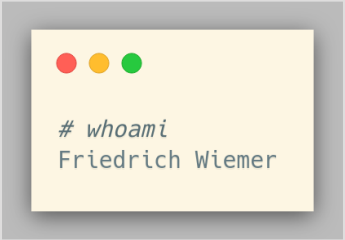
April 6th, 2020

Friedrich Wiemer

Me



Me



Private



Me

```
# whoami
Friedrich Wiemer
```

Private



IT-Security at Ruhr Uni Bochum

Me

RUB

```
# whoami
Friedrich Wiemer
```

IT-Security at Ruhr Uni Bochum

Private



Doctoral Studies

Topic:
Design & Analysis of Block Ciphers *for the IoT*

Me

RUB

```
# whoami
Friedrich Wiemer
```

IT-Security at Ruhr Uni Bochum

Private



Doctoral Studies

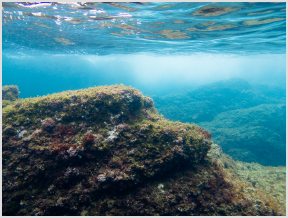
Topic:
Design & Analysis of Block Ciphers *for the IoT*

cryptosolutions

Analogue





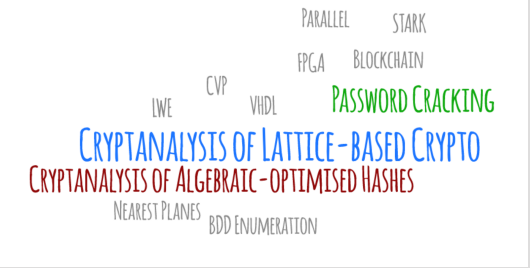



asante.dev/photos

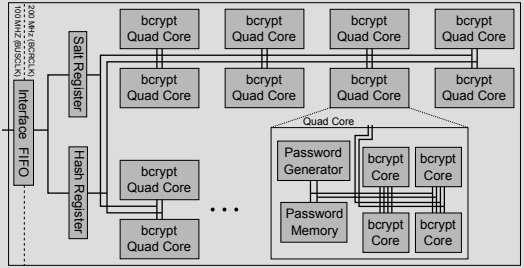
Research

- “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



High-Speed Implementation of bcrypt Password Search

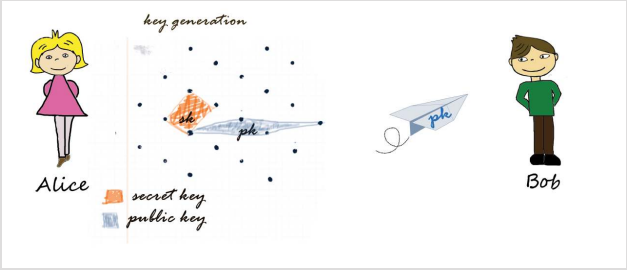


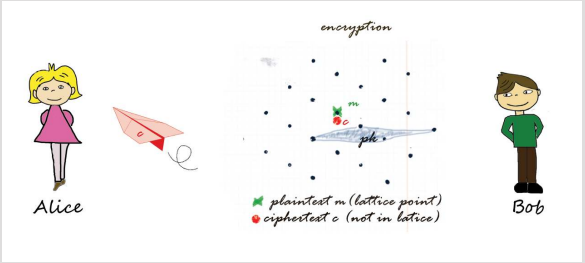

```
root@localhost:~# hexdump -C -v -n 64 /dev/xillybus_mem_8
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030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

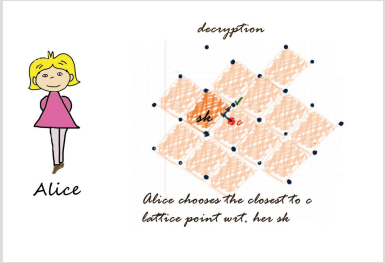
Salt Hash Password Status Register

- Zedboard implementation: 4x increase to previous work

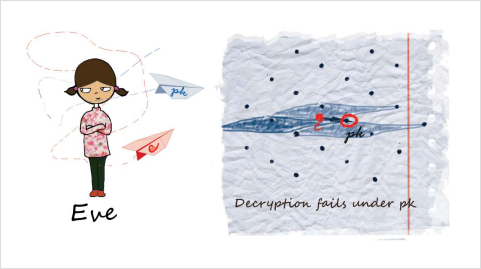
Parallel Implementation of BDD enumeration for LWE



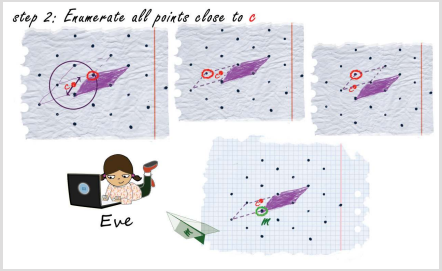




Parallel Implementation of BDD enumeration for LWE



Parallel Implementation of BDD enumeration for LWE



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

Research

- “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

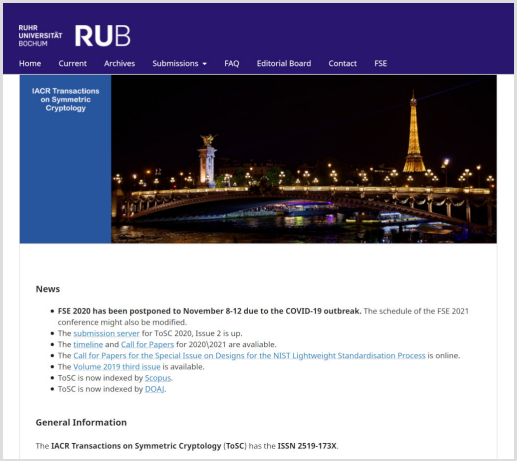
Topic Classification within Symmetric Crypto

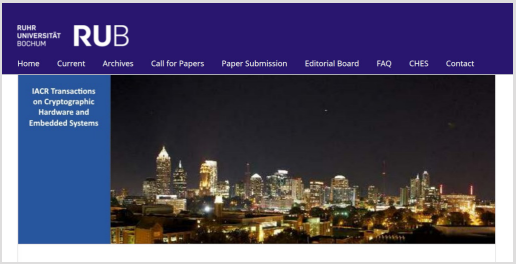
RUB

Security vs. Efficiency

SoK: Linear Cryptanalysis			Theory
Subspace Trail Analysis			Theory
			Algorithm
		Shorter SLPs	Implementation
	BISON		Instantiation
DLCT			Theory
	Spook		Instantiation

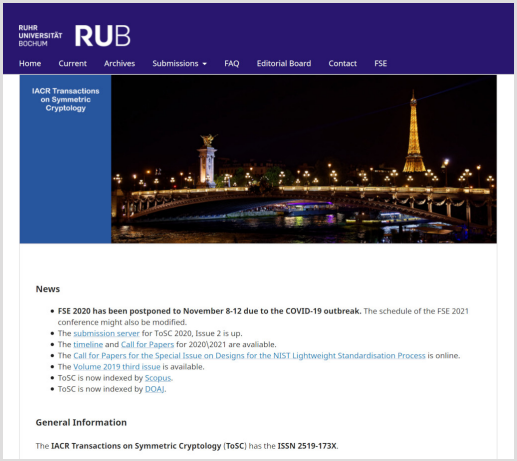
Activity in the Cryptographic Community

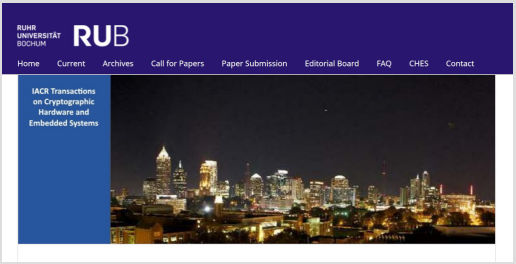




- IACR Conferences move to *Gold Open Access* publications
- Published by Ruhr Uni Bochum

Activity in the Cryptographic Community





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

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

SageMath

- 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
```