Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures

Lejla Batina, Amitabh Das, Barış Ege, *Elif Bilge Kavun*, Nele Mentens, Christof Paar, Ingrid Verbauwhede, Tolga Yalçın

RFIDSec'13 – Graz, Austria – July 11, 2013

Overview

- Lightweight Devices and Lightweight Cryptography
- Contribution and Architectures
- Evaluation Methodology
- Results and Discussion
- Conclusion and Future Directions

Overview

- **Lightweight Devices and Lightweight Cryptography**
- Contribution and Architectures
- Evaluation Methodology
- Results and Discussion
- Conclusion and Future Directions

Lightweight Devices

- RFID-Tags
- Smart Cards
- Wireless Sensors

Lightweight Devices

Applications

- Electronic passports

- Logistics

- Road toll-collection

Lightweight Devices

Applications – The Security Need

- Control on access: Car key systems, etc.
- Enforcing business models: Electronic wallet, etc.
- Counterfeiting: Batteries, etc.
- Privacy protection: Medical sensors, etc.

Lightweight Devices

Important Metrics

- Power and energy consumption
  - Active devices with on-chip batteries
  - Battery-less passive devices that rely on limited EM-transmitted power
- Area and complexity
  - Gate count, I/O pin count, storage

Lightweight Cryptography

- Algorithms with particularly low implementation costs
  - Tailored to fulfill previously mentioned requirements

Lightweight Cryptography

Lightweight Block Ciphers

- Early examples:
  - PRESENT, CLEFIA – *ISO standards*
  - KATAN, mCrypton, etc.
- Recently-developed:
  - KLEIN, LED, PRINCE, etc.

Lightweight Cryptography

Lightweight Block Ciphers

- Early examples:
  - PRESENT, CLEFIA – *ISO standards*
  - KATAN, mCrypton, etc.
- Recently-developed:
  - KLEIN, LED, PRINCE, etc.

And many more…

Lightweight Cryptography

Lightweight Block Ciphers

- Early examples:
  - PRESENT, CLEFIA – *ISO standards*
  - KATAN, mCrypton, etc.
- Recently-developed:
  - KLEIN, LED, PRINCE, etc.

And many more…

Above are the implemented ciphers in this work!

Lightweight Block Ciphers

PRESENT

- 64-bit block size, 80/128-bit key size
- Substitution-permutation network
- 4x4-bit S-box
- 31 rounds
- ISO standard!

Lightweight Block Ciphers

CLEFIA

- 128-bit block size, 128/192/256-bit key size
- Feistel network
- 18/22/26 rounds
- ISO standard!

Horst Görtz Institute for IT-Security

RUB

Lightweight Block Ciphers

KATAN

- 32/48/64-bit block size, 80-bit key size
- LFSR structure
- 254 rounds
- Extremely efficient in hardware

Lightweight Block Ciphers

mCrypton

- 64-bit block size, 64/96/128-bit key size
- Substitution-permutation network
- Four 4x4-bit S-boxes
- 12 rounds

Lightweight Block Ciphers

KLEIN

- 64-bit block size, 64/80/96-bit key size
- Substitution-permutation network
- 4x4-bit S-box
- 12/16/20 rounds

Lightweight Block Ciphers

LED

- 64-bit block size, 64/128-bit key size
- Substitution-permutation network
- 4x4-bit S-box (PRESENT S-box)
- 8*4=32 / 12*4=48 rounds

Lightweight Block Ciphers

PRINCE

- 64-bit block size, 128-bit key size
- Substitution-permutation network
- 4x4-bit S-box
- 12 rounds

Regular Block Ciphers

AES

- 128-bit block size, 128/192/256-bit key size
- Substitution-permutation network
- 8x8-bit S-box
- 10/12/14 rounds
- NIST standard!

Regular Block Ciphers

AES

- 128-bit block size, 128/192/256-bit key size
- Substitution-permutation network
- 8x8-bit S-box
- 10/12/14 rounds
- NIST standard!

Included in analysis for a fair comparison – to a standard cipher!

Regular Block Ciphers

AES

- 128-bit block size, 128/192/256-bit key size
- Substitution-permutation network
- 8x8-bit S-box
- 10/12/14 rounds
- NIST standard!

Included in analysis for a fair comparison –

to a standard cipher!

6 different architectures (w.r.t. S-box) investigated

Overview

- Lightweight Devices and Lightweight Cryptography
- **Contribution and Architectures**
- Evaluation Methodology
- Results and Discussion
- Conclusion and Future Directions

Contribution

- Up to now, dominant comparison metric: Area
  - Measured in Gate Equivalents (GE)!
  - Helpful but does not answer all questions
- Good power and energy consumption prediction important
  - For battery-powered systems
  - For passive systems
- Extending existing studies to an extensive suite of recent lightweight symmetric schemes

Architectures

All implementations re-implemented from scratch based on the references!

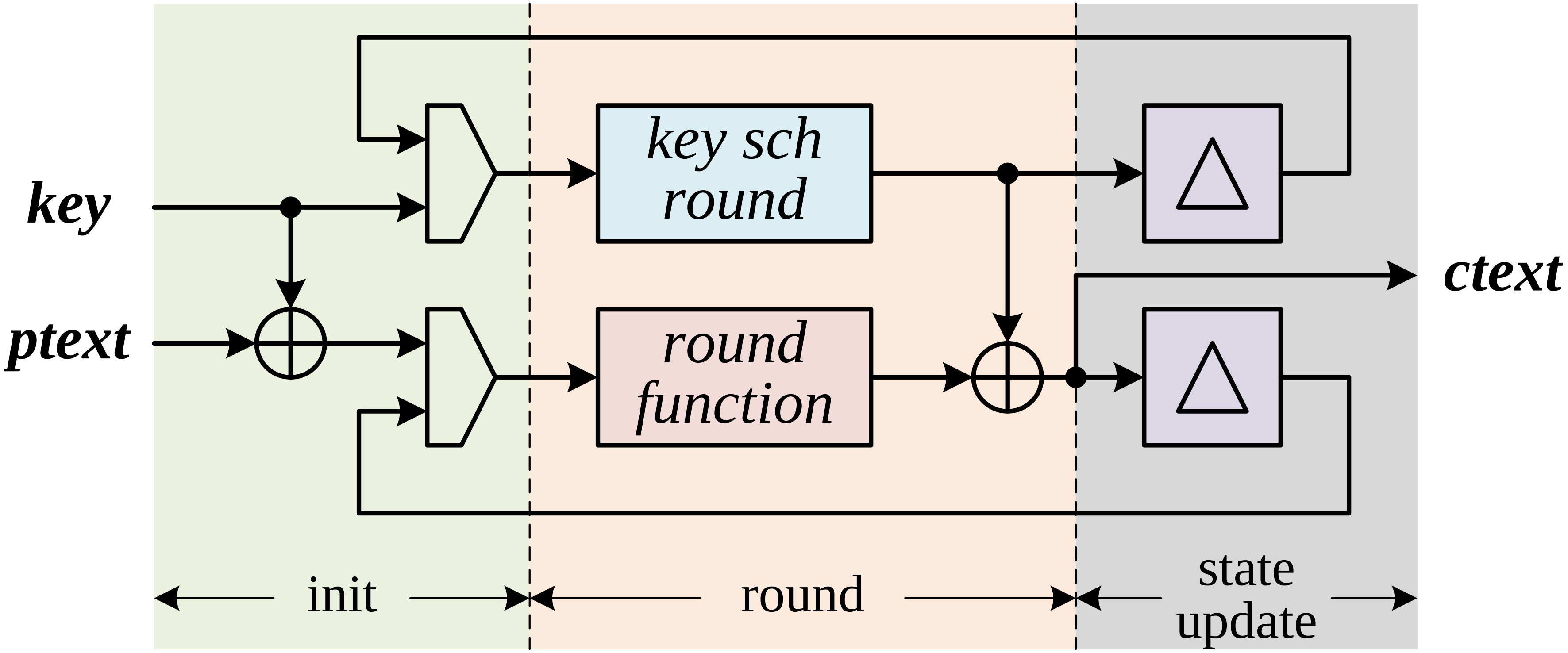
Architectures

Parallel Implementations

- Encryption-only
- 128-bit block size:
  - Clefia-128
- 64-bit block size:
  - PRESENT-80
  - mCrypton-96
  - KLEIN-64
  - LED-128
  - PRINCE-128

Architectures

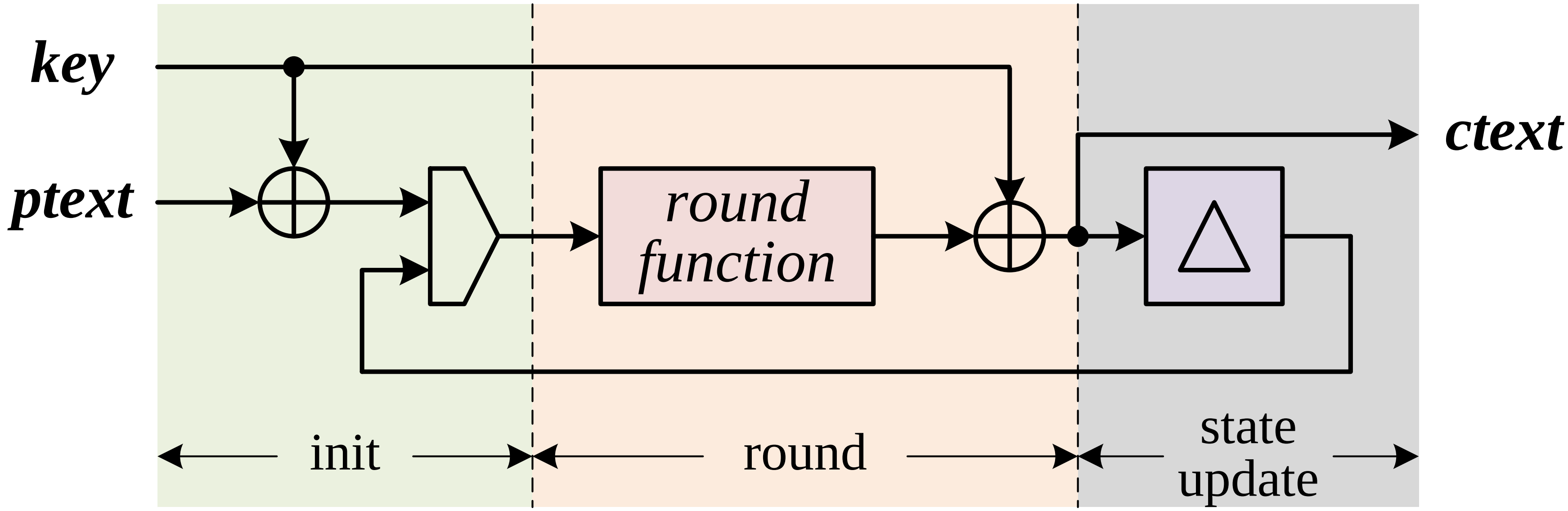
Parallel Implementations



- Repeated as many rounds as the cipher is defined for
- In the case of PRINCE, final whitening key added to output node

Architectures

Parallel Implementations – No Key Update



- In some cases there is fixed key or a simple function of the key (LED and PRINCE)

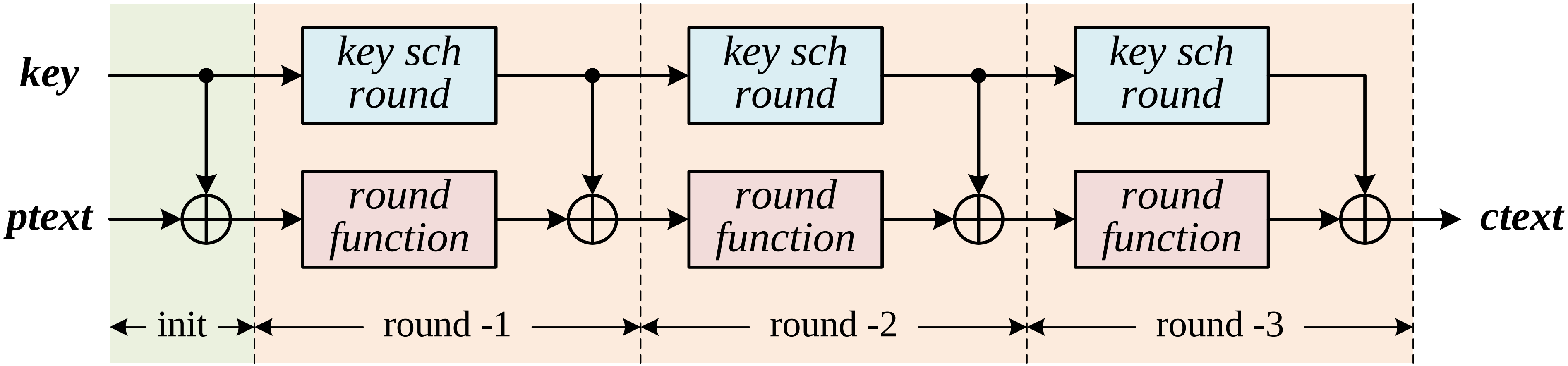
Architectures

Unfolded Implementations

- Encryption-only
- 64-bit block size:
  - PRINCE-128

Architectures

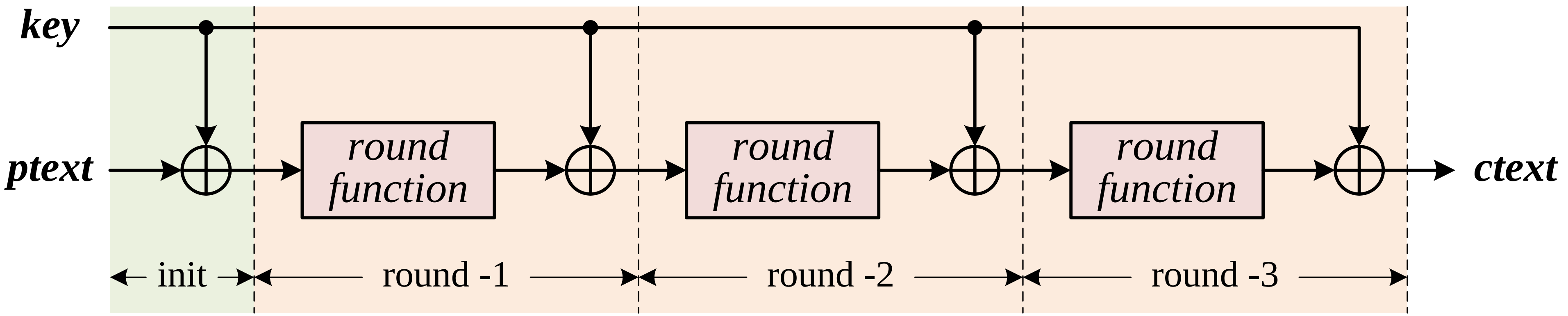
Unfolded Implementations



- Various numbers of round function – as many rounds as the cipher

Architectures

Unfolded Implementations – No Key Update



- We use this one…
- 12 consecutive round functions for PRINCE

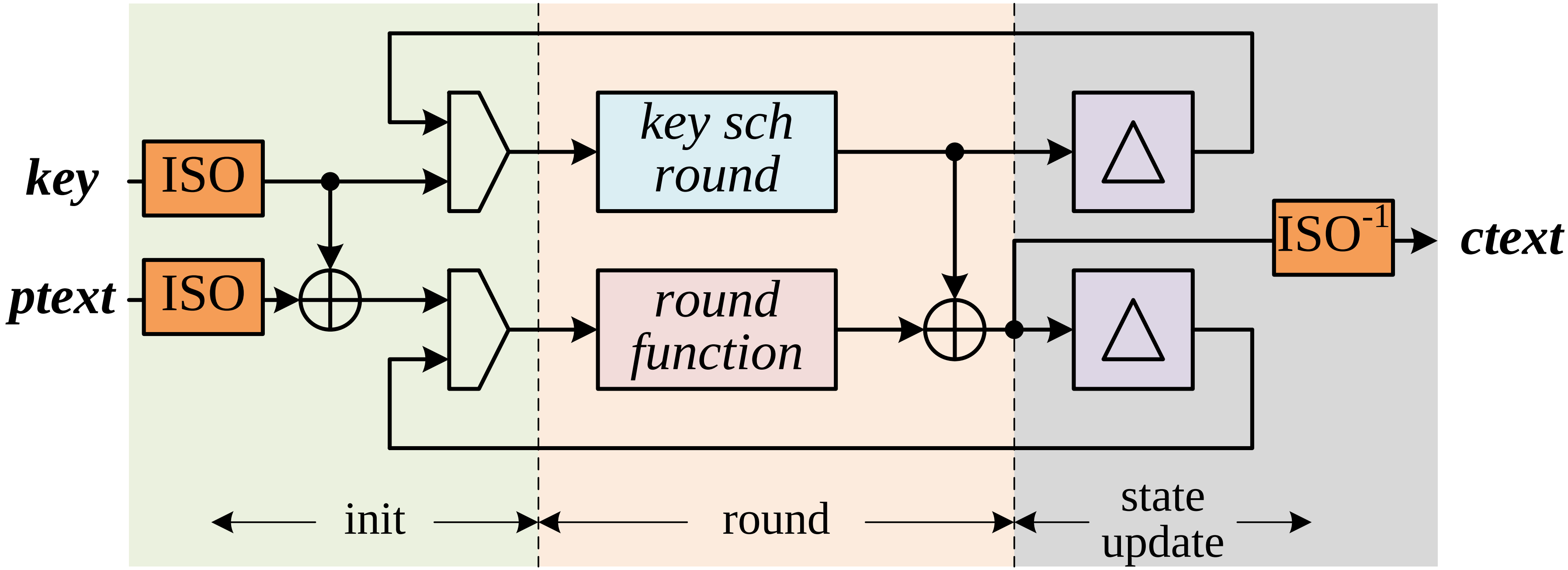
Architectures

AES Implementations

- Serial:
  - Byte-based implementation of Moradi et al.
  - Uses one S-box implemented in composite field $GF(((2^2)^2)^2)$
  - No use of scan flip-flops as suggested: Due to conventional tool flow
- Parallel:
  - S-box implemented in composite field $GF(((2^2)^4)$
  - S-box implemented in composite field $GF(((2^2)^2)^2)$
  - S-box implemented in composite field $GF(((2^2)^4)$ with isomorphic transform
  - S-box implemented in composite field $GF(((2^2)^2)^2)$ with isomorphic transform
  - S-box implemented as lookup table

Architectures

AES Implementations – With Isomorphic Transform



Overview

- Lightweight Devices and Lightweight Cryptography
- Contribution and Architectures
- **Evaluation Methodology**
- Results and Discussion
- Conclusion and Future Directions

Evaluation Methodology

Architectural Decisions

- All I/O of ciphers buffered through a flip-flop
- Encryption-only architectures
  - Most modes of operation do not need encryption

Evaluation Methodology

Evaluation of Design Parameters – Tools

- Implementations synthesized in UMC 130 nm low-leakage Faraday technology library
- Using Cadence Encounter RTL Compiler
- Simulation tool: Modelsim

Evaluation Methodology

Evaluation of Design Parameters – Metrics

- Area (GE): Gate Equivalence
  - Dividing silicon area of cipher with a given std-cell library by area of 2-input NAND gate
- Dynamic power: Power when circuit active
  - Proportional to operation frequency
- Static power: Power during no activity
  - Significant for low frequency operation
- Energy/bit:
  - (Total power × Cycle count) / (Frequency × Block length)

Evaluation Methodology

Evaluation of Design Parameters

- Each module first synthesized for best power
- Generated netlists used to simulate actual module with 100 random keys together with 10 random plaintexts per key to get best statistics
- SAIF files generated in these simulations
- SAIF files sent back to synthesis tool together with netlist to run power analysis

Overview

- Lightweight Devices and Lightweight Cryptography
- Contribution and Architectures
- Evaluation Methodology
- **Results and Discussion**
- Conclusion and Future Directions

Results and Discussion

Cipher Architecture	Block length	Encryption time (# cycles)	Freq. (KHz)	Area (GEs)	Static Power (μW)	Dynamic Power (μW)	Energy per bit (pJ/bit)	Energy (nJ)
AES_small_core_1 [12]	128	211	100	3685	6.25	11.31	186.44	37.05
AES_2_2_2_enc_128	128	10	100	12405	24.46	210.15	164.18	23.46
AES_4_2_enc_128	128	10	100	11453	21.37	135.26	105.67	15.66
AES_iso_2_2_2_enc_128	128	10	100	15442	30.41	52.85	41.29	8.33
AES_iso_4_2_enc_128	128	10	100	13052	25.19	37.06	28.95	6.23
AES_lut_enc_128	128	10	100	19591	30.81	96.11	75.09	12.69

Results and Discussion

Cipher Architecture	Block/Key length	Encryption time (# cycles)	Freq. (KHz)	Area (GEs)	Static Power (μW)	Dynamic Power (μW)	Energy per bit (pJ/bit)	Energy (nJ)
CLEFIA	128/128	18	100	6941	13.24	37.09	52.19	9.06
KLEIN_parallel	64/64	12	100	2760	4.88	2.18	4.09	0.85
KLEIN_serial	64/64	98	100	1432	2.56	1.48	22.66	3.96
LED	64/128	48	100	3194	5.62	2.34	17.55	3.82
mCrypton	64/96	13	100	3197	5.80	2.50	5.08	1.08
PRESENT	64/80	31	100	2195	3.75	1.14	5.52	3.82
PRINCE_folded	64/128	12	100	2953	5.75	2.80	5.25	1.03
PRINCE_unfolded	64/128	1	100	39938	16.13	120.20	1.46	1.36
Katan_32	32/80	254	100	801	1.52	0.43	34.13	4.94
Katan_48	48/80	254	100	925	1.71	0.49	25.93	5.60
Katan_64	64/80	254	100	1048	1.94	0.56	22.23	6.34

Overview

- Lightweight Devices and Lightweight Cryptography
- Contribution and Architectures
- Evaluation Methodology
- Results and Discussion
- **Conclusion and Future Directions**

Conclusion and Future Directions

- Area, power, energy evaluation of
  - 11 lightweight block cipher architectures
  - 6 different AES architectures
- Discussion of power consumption in relation to area
  - LUT-based AES largest in area, best in dynamic power consumption
  - Others depend on complexity of round function
- Dynamic power consumption plays an important role for high frequency operation
  - Try to estimate dynamic power consumption via measuring toggle activity
- Lightweight applications run at low frequency → Static power consumption is also very important

Thanks for Listening!

Any Questions?

elif.kavun@rub.de