

Hold Your Breath, PRIMATEs Are Lightweight

Danilo Šijačić¹, Andreas B. Kidmose², Bohan Yang¹,
Subhadeep Banik³, Begül Bilgin¹, Andrey Bogdanov²,
Ingrid Verbauwhede¹

¹ESAT/COSIC, KU Leuven and iMinds, Belgium

²Technical University of Denmark, Denmark

³Temasek Labs, Nanyang Technological University, Singapore

August 12, 2016

Introduction

CAESAR Competition

- Goal: Portfolio of authenticated encryption ciphers
- Authenticated encryption: $(C, T) = \mathcal{E}_K(N, A, M)$
- Different use cases are considered
 - Lightweight
 - “Defense In-Depth”
 - High Performance

Notion of Lightweight

- Defined by a specific application in practice
- Common criteria used in the literature
 - Maximal area: equivalent to 2000 NAND2 gates (2000 GE)
 - Minimal usable throughput: 12 kbit/s at 100 kHz
 - Minimal security level: 80-bit
 - Power consumption: 1–10 $\mu\text{W}/\text{MHz}$



Application Requirements

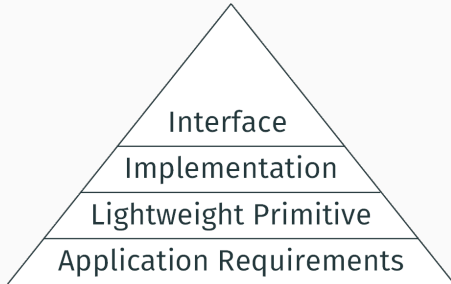
Notion of Lightweight

- Defined by a specific application in practice
- Common criteria used in the literature
 - Maximal area: equivalent to 2000 NAND2 gates (2000 GE)
 - Minimal usable throughput: 12 kbit/s at 100 kHz
 - Minimal security level: 80-bit
 - Power consumption: 1–10 $\mu\text{W}/\text{MHz}$



Notion of Lightweight

- Defined by a specific application in practice
- Common criteria used in the literature
 - Maximal area: equivalent to 2000 NAND2 gates (2000 GE)
 - Minimal usable throughput: 12 kbit/s at 100 kHz
 - Minimal security level: 80-bit
 - Power consumption: 1–10 $\mu\text{W}/\text{MHz}$



PRIMATEs Family of Authenticated Encryption Ciphers

APE: APE-80, APE-120

HANUMAN: HANUMAN-80, HANUMAN-120

GIBBON: GIBBON-80, GIBBON-120

PRIMATEs Family of Authenticated Encryption Ciphers

APE: APE-80, APE-120

HANUMAN: HANUMAN-80, HANUMAN-120

- General lightweight applications
- Based on an ideal permutation

GIBBON: GIBBON-80, GIBBON-120

PRIMATEs Family of Authenticated Encryption Ciphers

APE: APE-80, APE-120

HANUMAN: HANUMAN-80, HANUMAN-120

- General lightweight applications
- Based on an ideal permutation

GIBBON: GIBBON-80, GIBBON-120

- Performance-critical lightweight applications
- Speed-security tradeoff

PRIMATEs Family of Authenticated Encryption Ciphers

APE: APE-80, APE-120

- “Defense in-depth” lightweight applications
- Nonce-misuse resistance, release of unverified plaintext

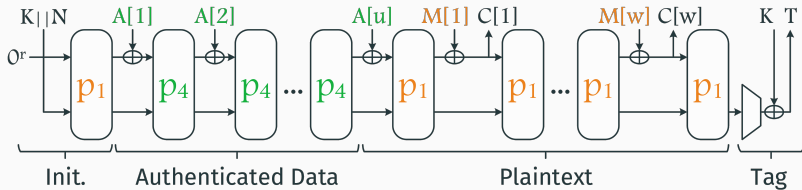
HANUMAN: HANUMAN-80, HANUMAN-120

- General lightweight applications
- Based on an ideal permutation

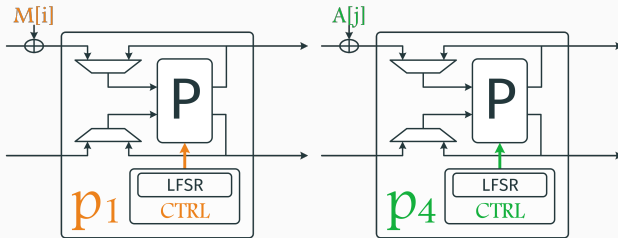
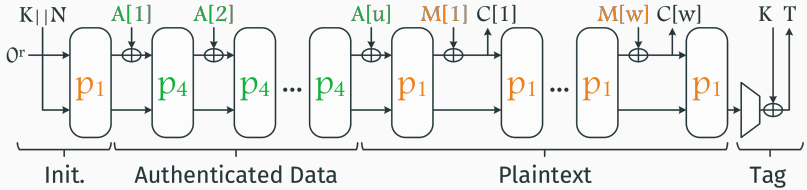
GIBBON: GIBBON-80, GIBBON-120

- Performance-critical lightweight applications
- Speed-security tradeoff

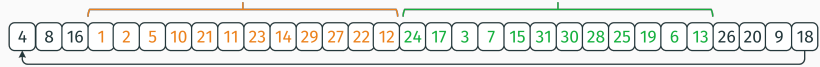
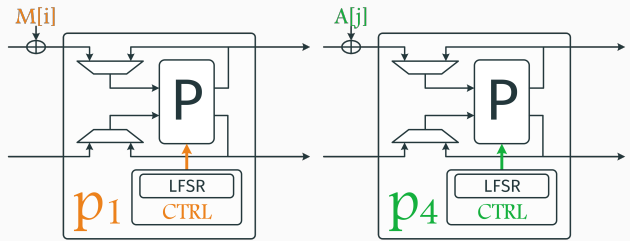
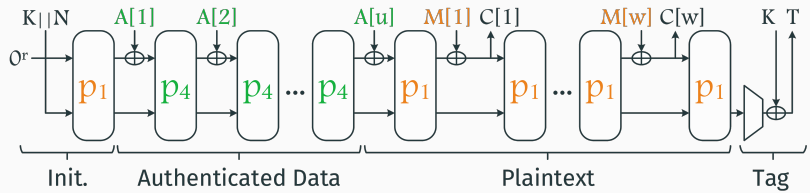
HANUMAN



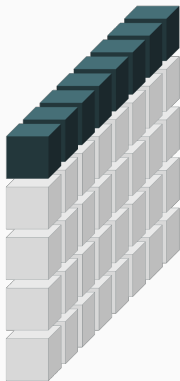
HANUMAN



HANUMAN



Round Permutation P-80

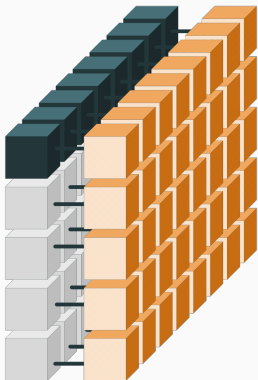



Rate Element
(5-bit storage)





Capacity Element
(5-bit storage)

Round Permutation P-80

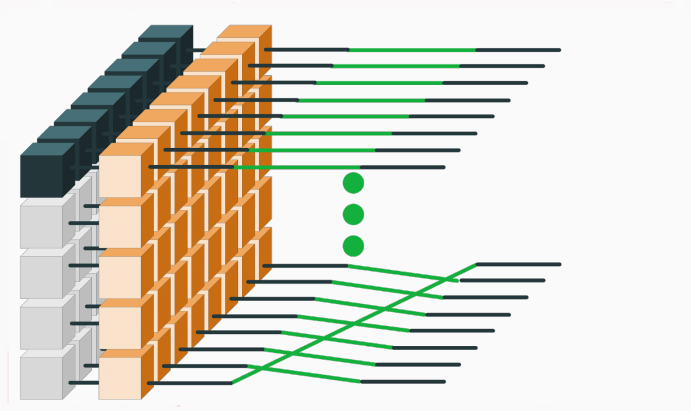



 Rate Element
(5-bit storage)


 PRIMATES S-Box
(5-bit permutation)


 Capacity Element
(5-bit storage)

Round Permutation P-80

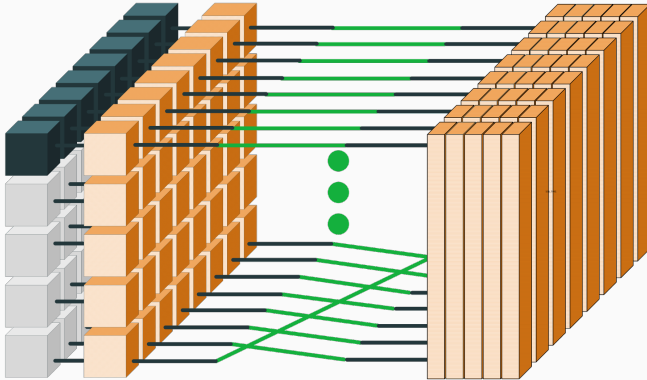



 Rate Element
(5-bit storage)


 PRIMATeS S-Box
(5-bit permutation)


 Capacity Element
(5-bit storage)


Round Permutation P-80



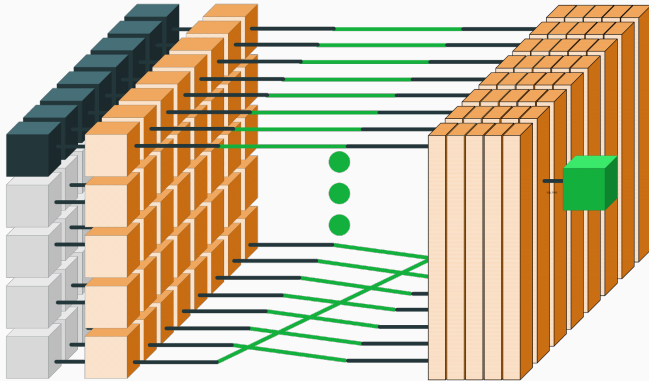
 Rate Element
(5-bit storage)

 PRIMATES S-Box
(5-bit permutation)

 Capacity Element
(5-bit storage)

 Recursive MDS Matrix
Multiplication
(25-bit mapping)

Round Permutation P-80



Rate Element
(5-bit storage)



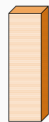
Capacity Element
(5-bit storage)



PRIMATES S-Box
(5-bit permutation)







Constant Addition
(5-bit XOR)










Recursive MDS Matrix
Multiplication
(25-bit mapping)

Compact Implementations

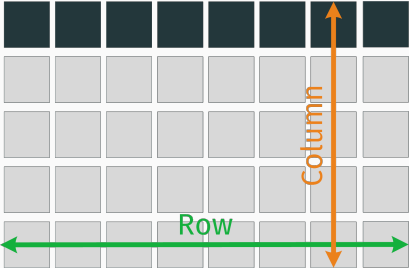
Implementation Cost Overview

| Core Components | Size [GE] | |
|--|-----------|------------|
| | Single | Full State |
|  Elem. DFF | 21.25 | 850.00 |
|  S-Box | 28.22 | 1128.96 |
|  $\sqrt[5]{\text{MDS}}$ | 36.26 | 1450.40 |
|  Elem. XOR | 12.5 | 12.5 |

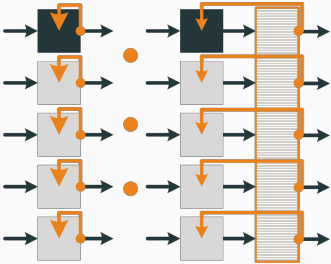
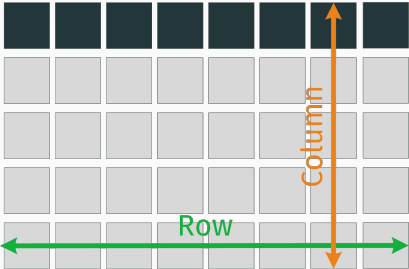
Implementation Cost Overview

| Core Components | Size [GE] | |
|--|-----------|------------|
| | Single | Full State |
|  Elem. DFF | 21.25 | 850.00 |
|  S-Box | 28.22 | 1128.96 |
|  $\sqrt[5]{\text{MDS}}$ | 36.26 | 1450.40 |
|  Elem. XOR | 12.5 | 12.5 |
| Serialization Overhead | Single | Full State |
|  Elem. MUX2 | 11.25 | 450.00 |
|  Elem. MUX3 | 18.75 | 750.00 |
|  Elem. MUX4 | 25.00 | 1000.00 |

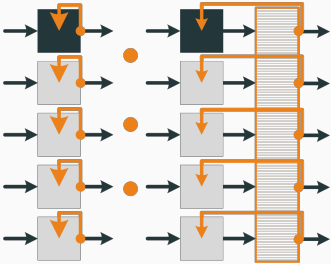
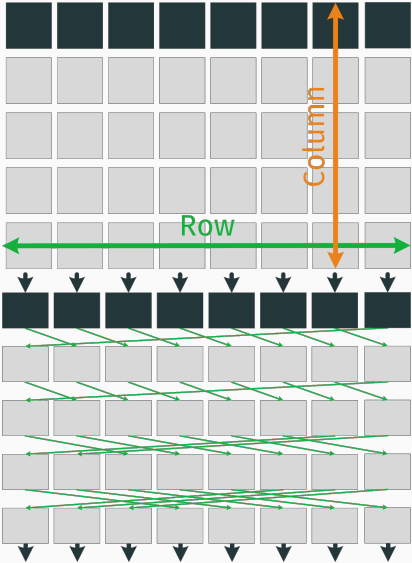
Serial Implementation Strategy



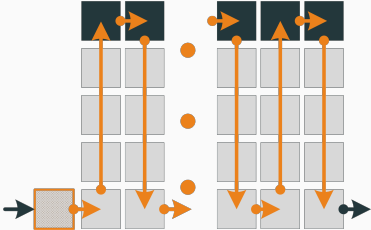
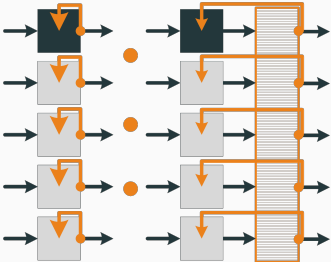
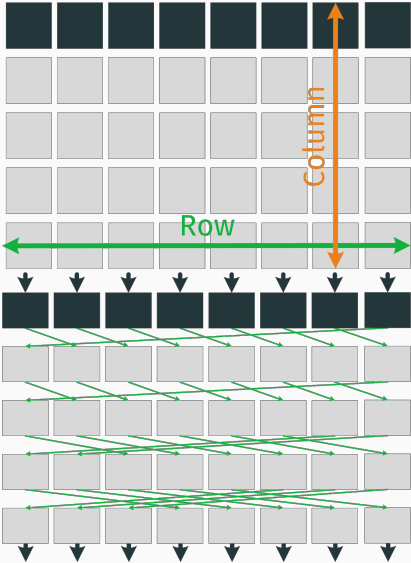
Serial Implementation Strategy



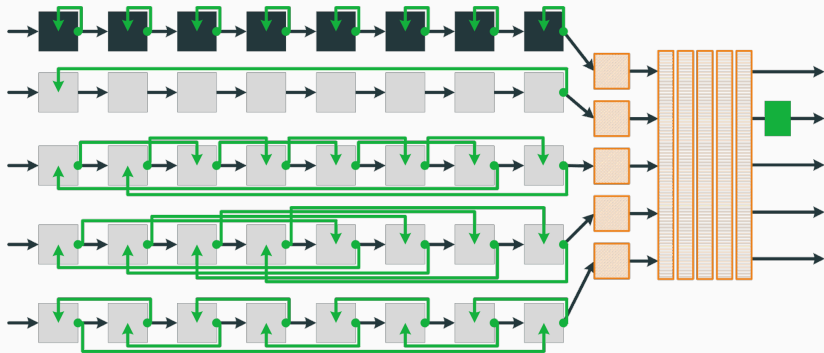
Serial Implementation Strategy



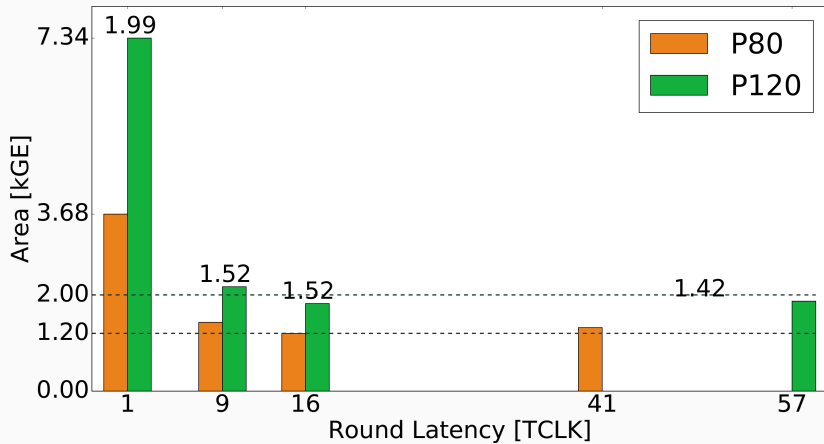
Serial Implementation Strategy



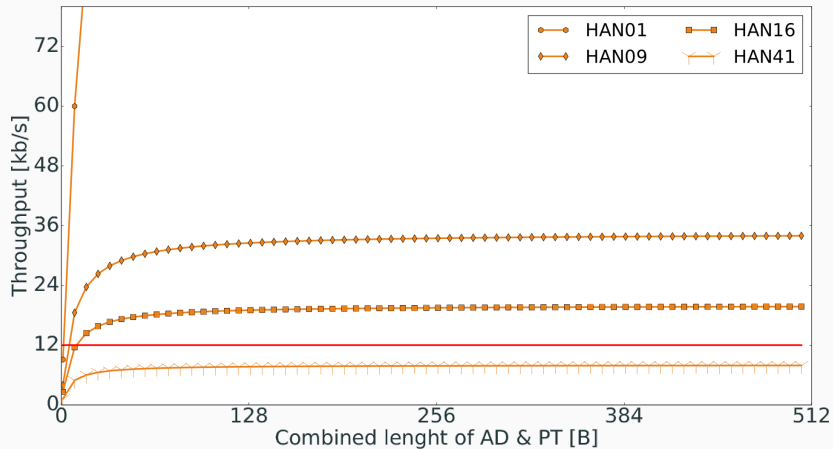
P80-9 Architecture



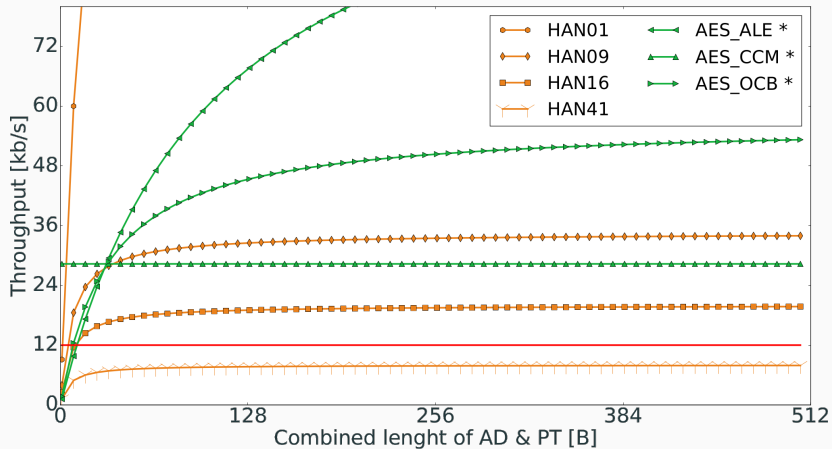
PRIMATE Round Permutation Cost



Throughput Estimate at 100 kHz

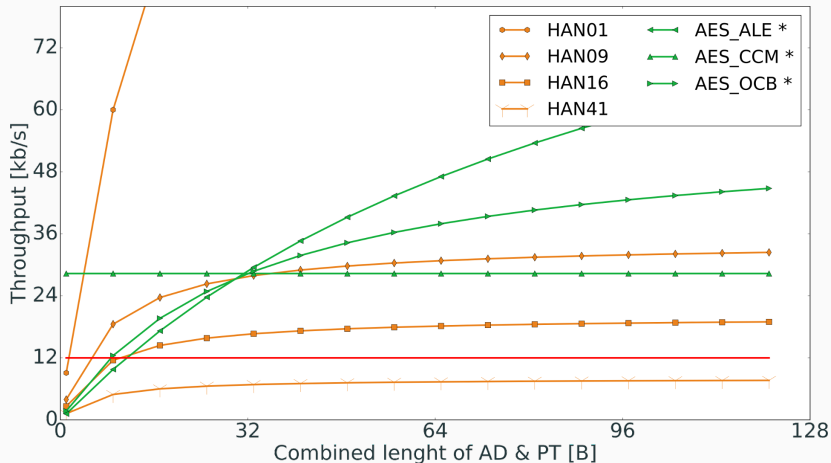


Throughput Estimate at 100 kHz



* Bogdanov et al.

Throughput Estimate at 100 kHz



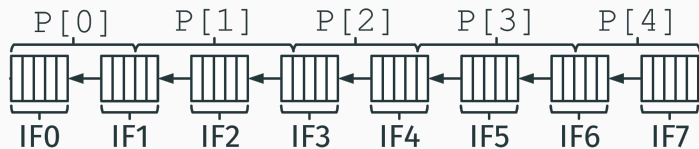
* Bogdanov et al.

Coprocessor

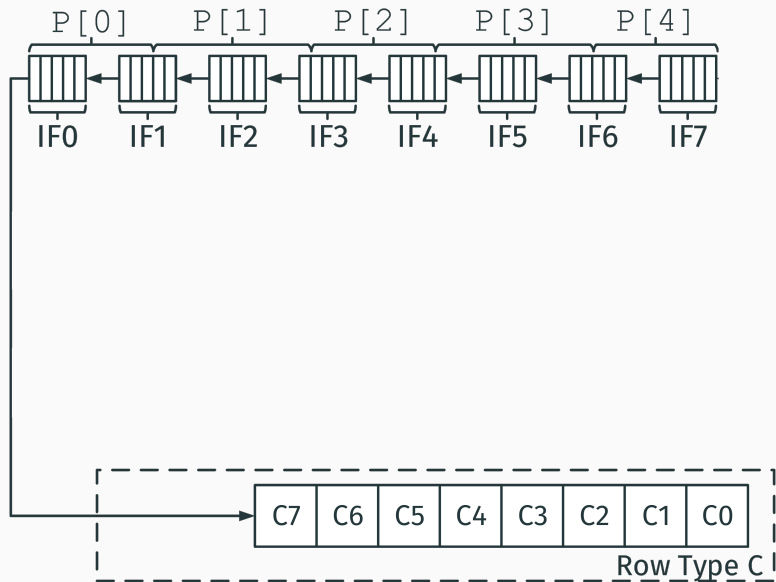
Lightweight Interface Requirements

- Low area overhead
 - Minimize the additional read/write logic of the SRF
- Low latency overhead
 - Minimize additional latency, including μ C latency
- Compatibility with 8-bit microcontrollers
 - Translate PRIMATES' words (25-bit datapath, 40-bit block)

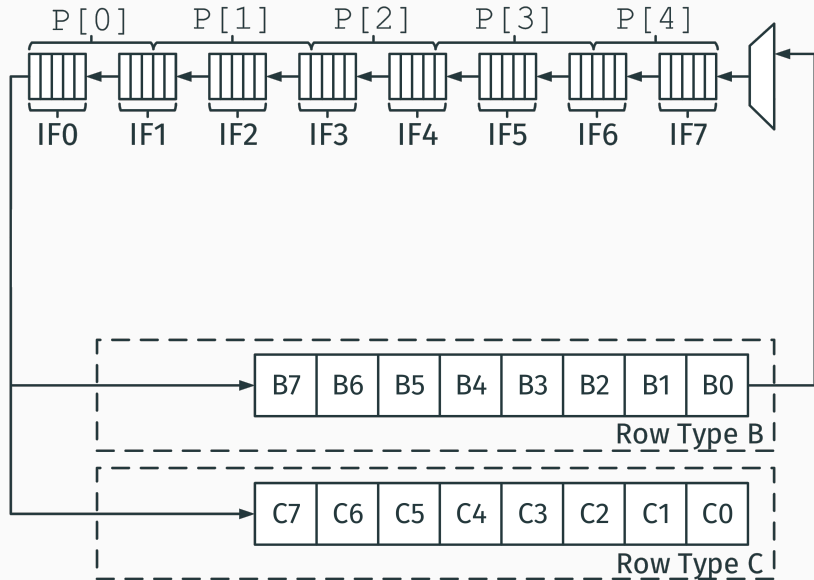
PRIMATEs Row Interface



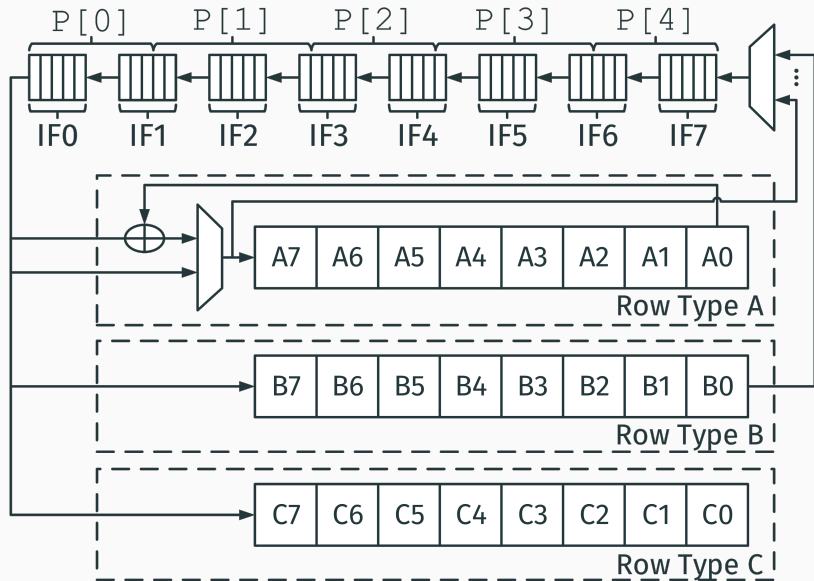
PRIMATEs Row Interface



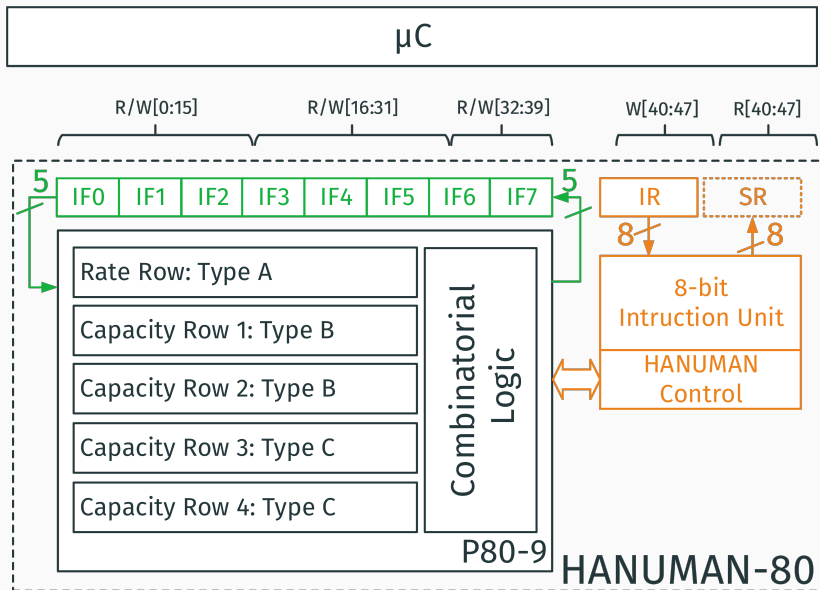
PRIMATEs Row Interface



PRIMATEs Row Interface



HANUMAN-80 Architecture



Performance & Cost

Lightweight Requirements

| | HANUMAN-80 | Required |
|------------------------------|------------|-----------|
| Area [kGE] | 2.00 | max. 2.00 |
| Throughput at 100 kHz [kb/s] | 33 | min. 12 |
| Power [μ W/MHz] | 5.3 | 1–10 |
| Energy [pJ/bit] | 15.64 | n/a |

Performance & Cost

Lightweight Requirements

| HANUMAN-80 | | Required |
|------------------------------|-------|-----------|
| Area [kGE] | 2.00 | max. 2.00 |
| Throughput at 100 kHz [kb/s] | 33 | min. 12 |
| Power [μ W/MHz] | 5.3 | 1–10 |
| Energy [pJ/bit] | 15.64 | n/a |

IF Register: 0.27 kGE

Glue Logic: 0.13 kGE

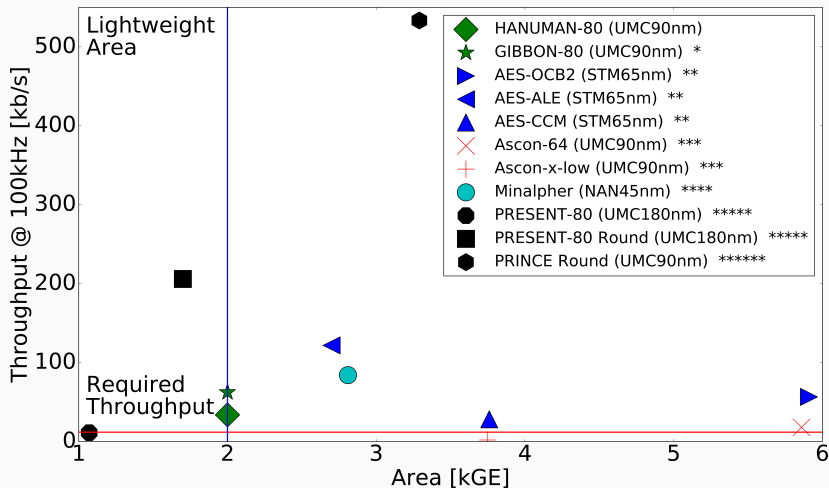
P80-9: 1.43 kGE

Instruction
Unit:
0.12 kGE

HANUMAN
Control:
0.05 kGE

Max. throughput. [Mb/s]: 65.36 (at 192.81 Mhz) Latency: 118 CLK/block

Performance Comparison



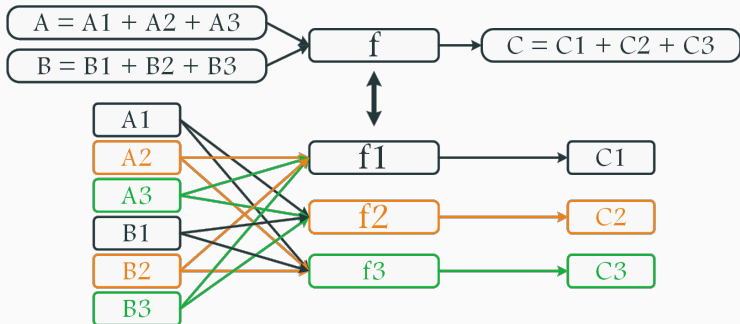
* Estimate
 *** Dobraunik et al.
 ***** Rolfes et al.

** Bogdanov et al.
 **** Sasaki et al.
 ***** Borghoff et al.

Threshold Implementations

Threshold Implementations (TI)

- Provable security against first-order differential power analysis
- Boolean masking scheme based on secret sharing
- Required properties: correctness, uniformity, non-completeness



Shared PRIMATEs S-Box

- Other transformations are linear; have trivial sharing
- S-Box is a 5-bit permutation designed to be naturally resilient
 - Best attainable linear and differential probabilities (2^{-4})
 - Quadratic, requires only 3 shares for TI

| # | Area [GE] | Correct | Uniform | Non-complete | Re-mask |
|---|-----------|---------|---------|--------------|---------|
| 3 | 246 | ✓ | | ✓ | ✓ |
| 4 | 255 | ✓ | ✓ | ✓ | |

Implementation Results

| Design | Area [kGE] | Randomness [bit] | |
|--------------------------------------|---------------|------------------|-----------|
| | | Initial sharing | Per round |
| P80-9 _A -3 _{sh} | 5.18 | 400 | 5 |
| P80-95 _A -3 _{sh} | 4.72 | | |
| P80-9 _A -4 _{sh} | 6.15 | 600 | 0 |
| P80-95 _A -4 _{sh} | 6.19 | | |

Conclusion

Conclusion

- PRIMATEs family can be implemented efficiently in hardware
- PRIMATEs family design allows versatile security and performance tradeoffs with minimal differences in hardware
- PRIMATEs family of authenticated encryption ciphers is most suitable for lightweight applications (e.g., across the Internet of Everything)

Questions?

HANUMAN-80 Instruction Set

| Mnemonic | Code | Description |
|----------|----------|---|
| RESET | 0----- | Perform software reset. |
| WAIT | 1000-000 | Put coprocessor in a idle state. |
| P1 | 1----001 | Perform p_1 permutation. |
| P1S | 1----101 | Perform p_1 permutation with padding spill into capacity. |
| P4 | 1----001 | Perform p_4 permutation. |
| RATEX | 10011111 | XOR in to rate. |
| RATES | 10010111 | Shift in to rate. |
| RDRATE | 10011111 | XOR in 0^{40} to rate; emulated rate read. |
| CAP1S | 10100111 | Shift in to capacity row 1, R/W. |
| CAP2S | 10110111 | Shift in to capacity row 2, R/W. |
| CAP3S | 11000111 | Shift in to capacity row 3, W. |
| CAP4S | 11010111 | Shift in to capacity row 4, W. |

Why Should Anyone Hold Their Breath?

