Towards Green Cryptography: a Comparison of Lightweight Ciphers from the Energy Viewpoint

Stéphanie Kerckhof, François Durvaux, Cédric Hoquet,
David Bol, François-Xavier Standaert

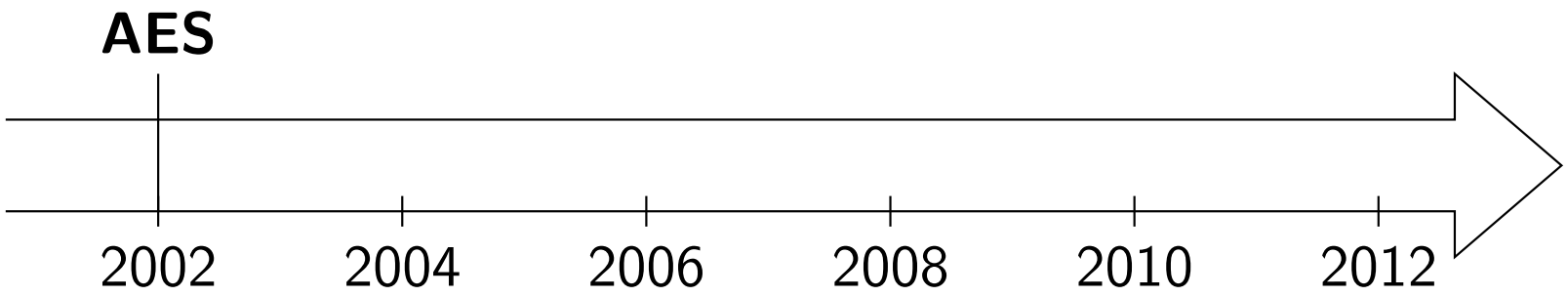
CHES 2012 – September 2012

Context

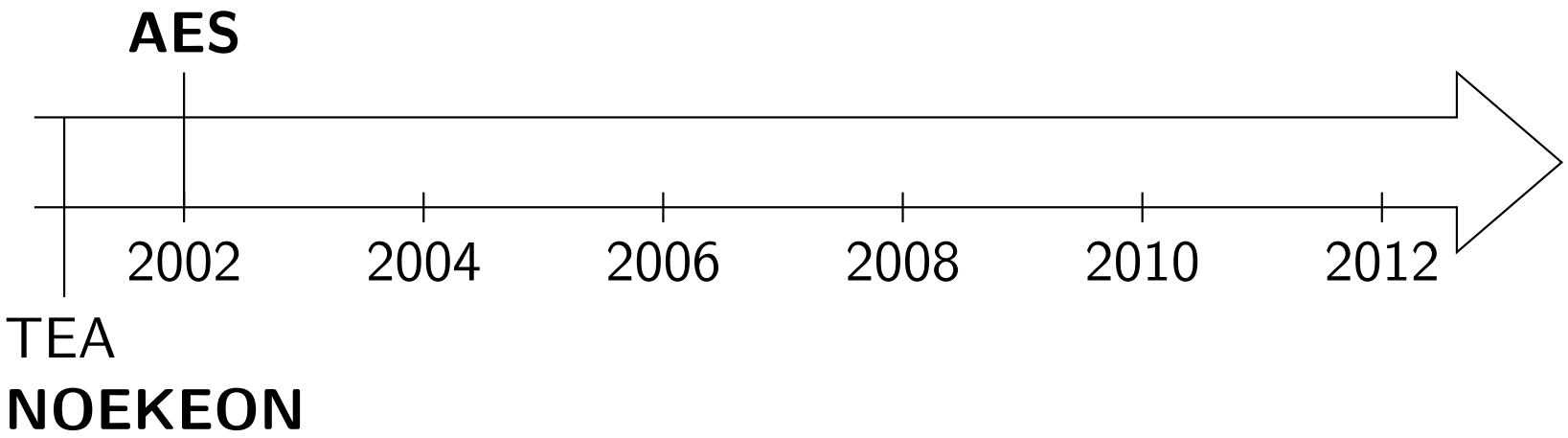
- More lightweight devices in more applications

Outline

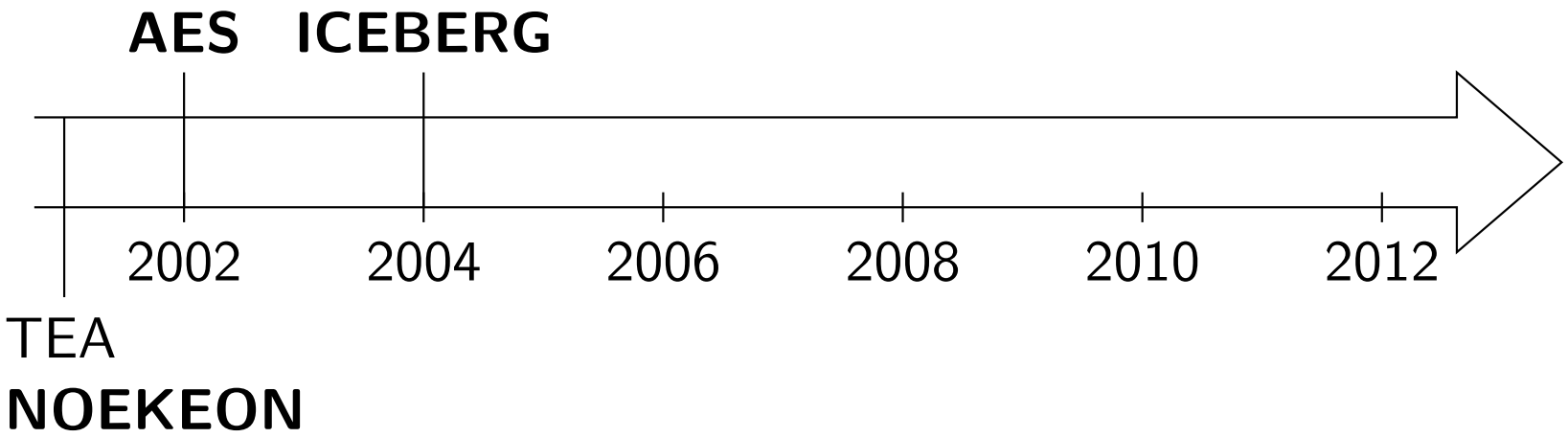
Lightweight Ciphers



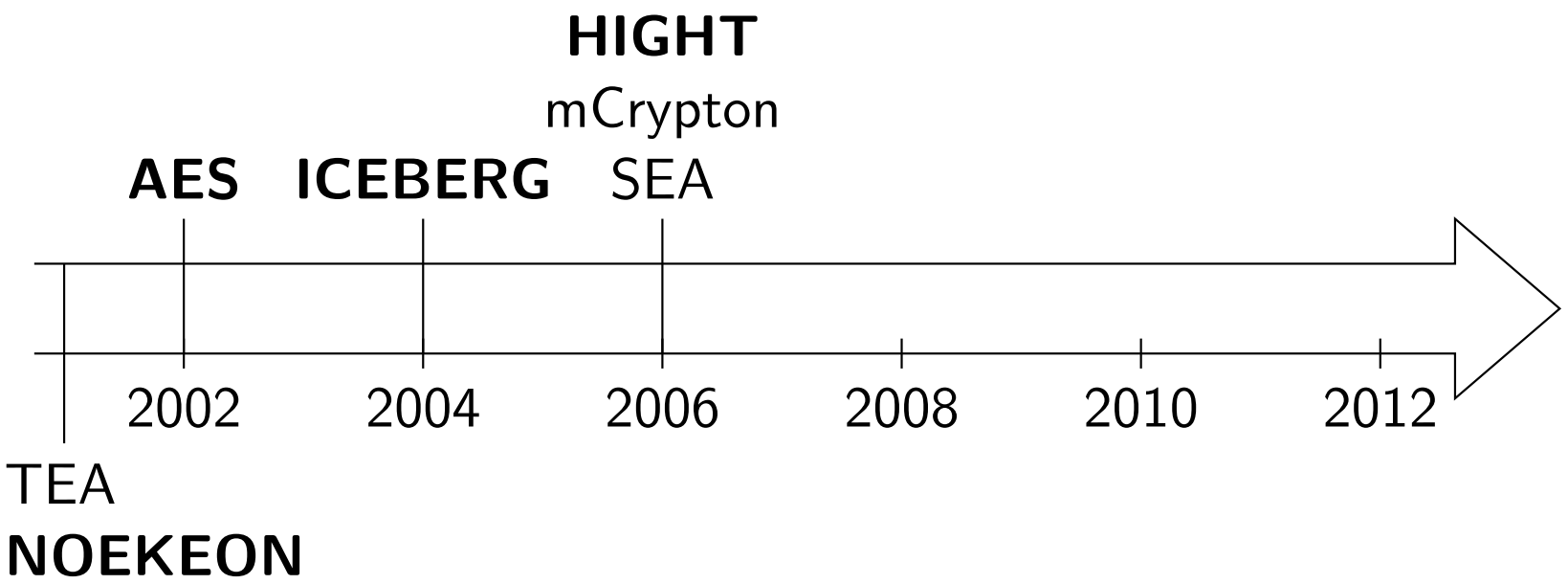
Lightweight Ciphers



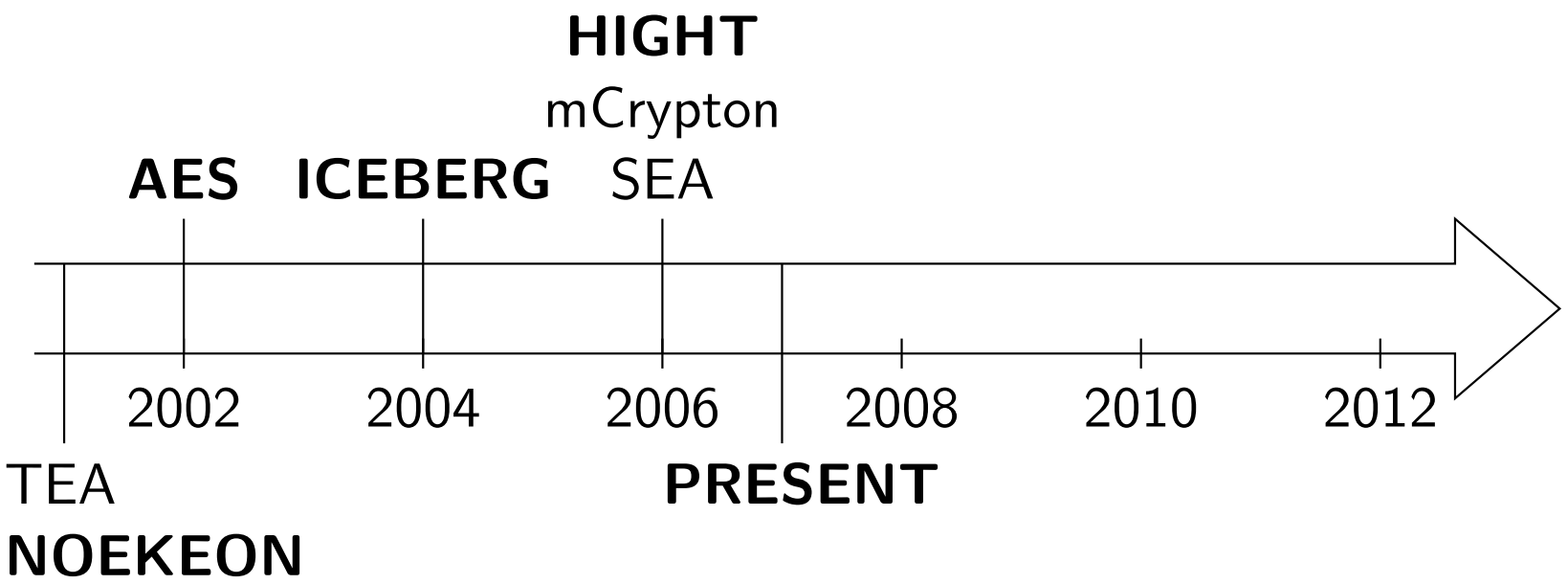
Lightweight Ciphers



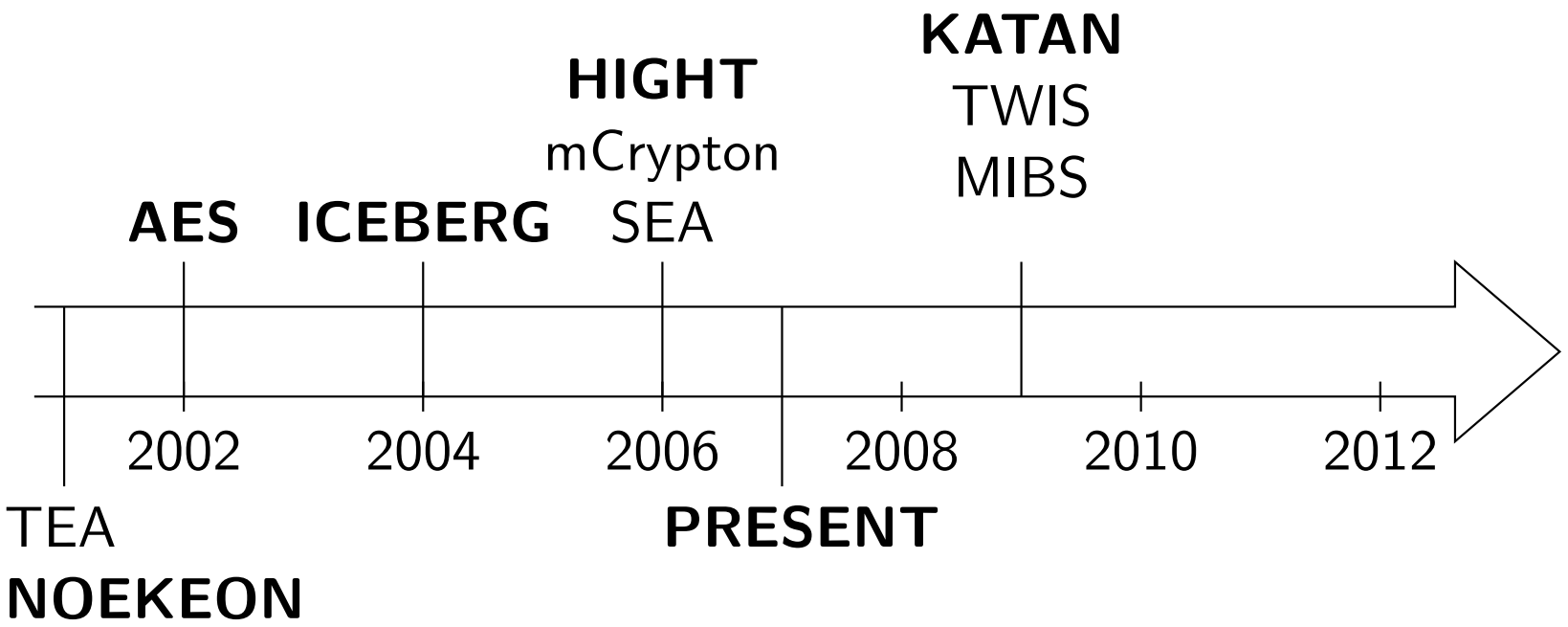
Lightweight Ciphers



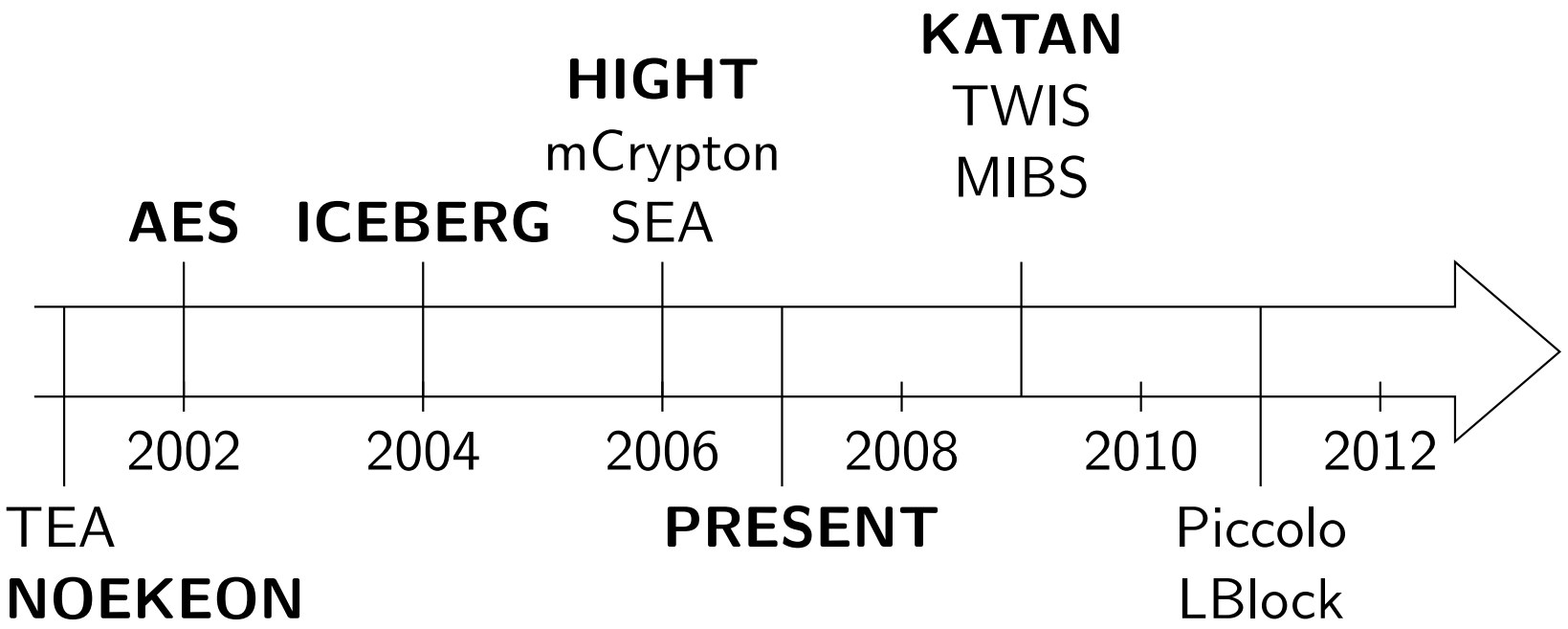
Lightweight Ciphers



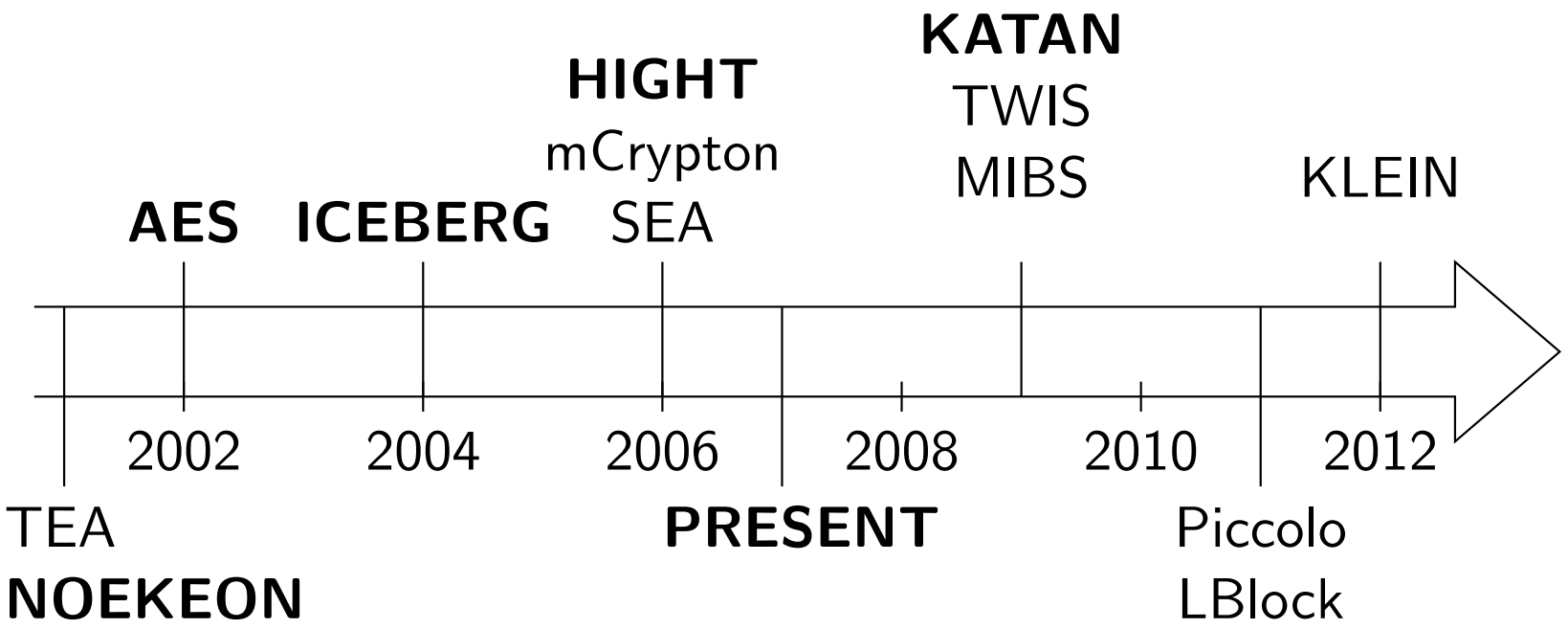
Lightweight Ciphers



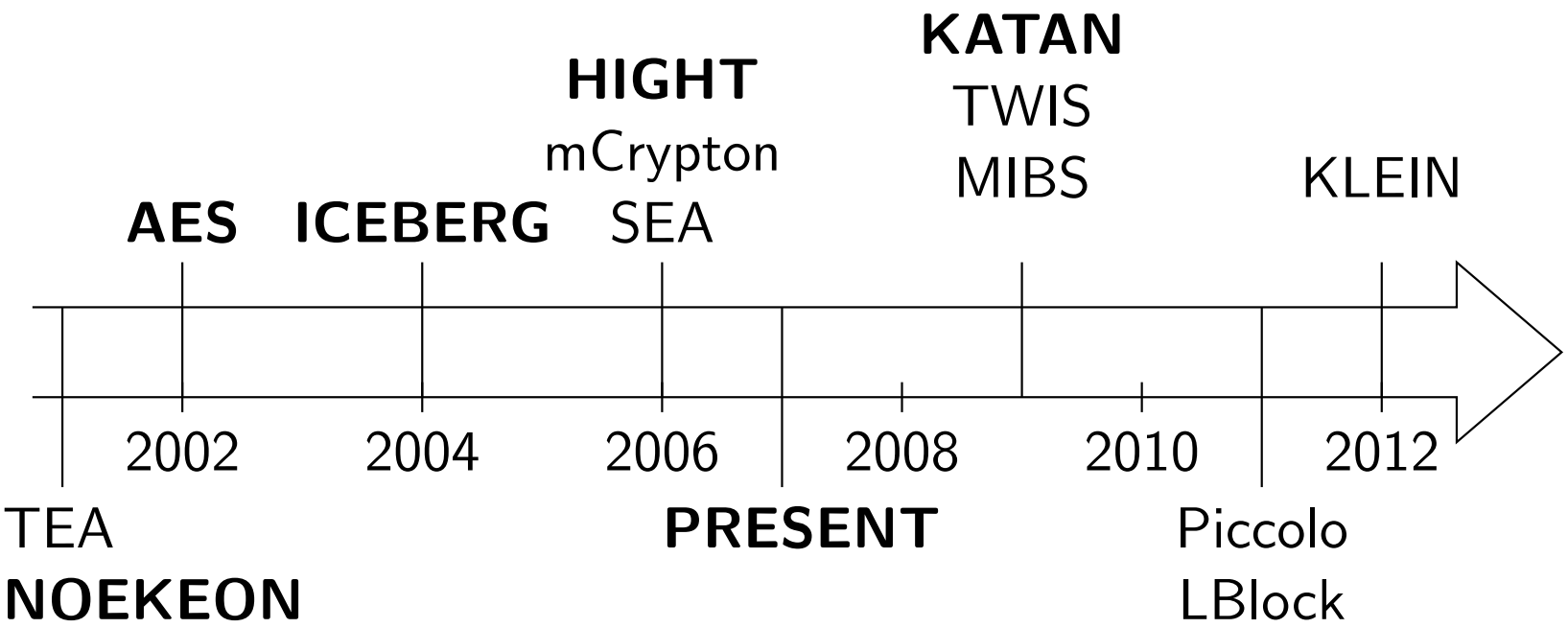
Lightweight Ciphers



Lightweight Ciphers

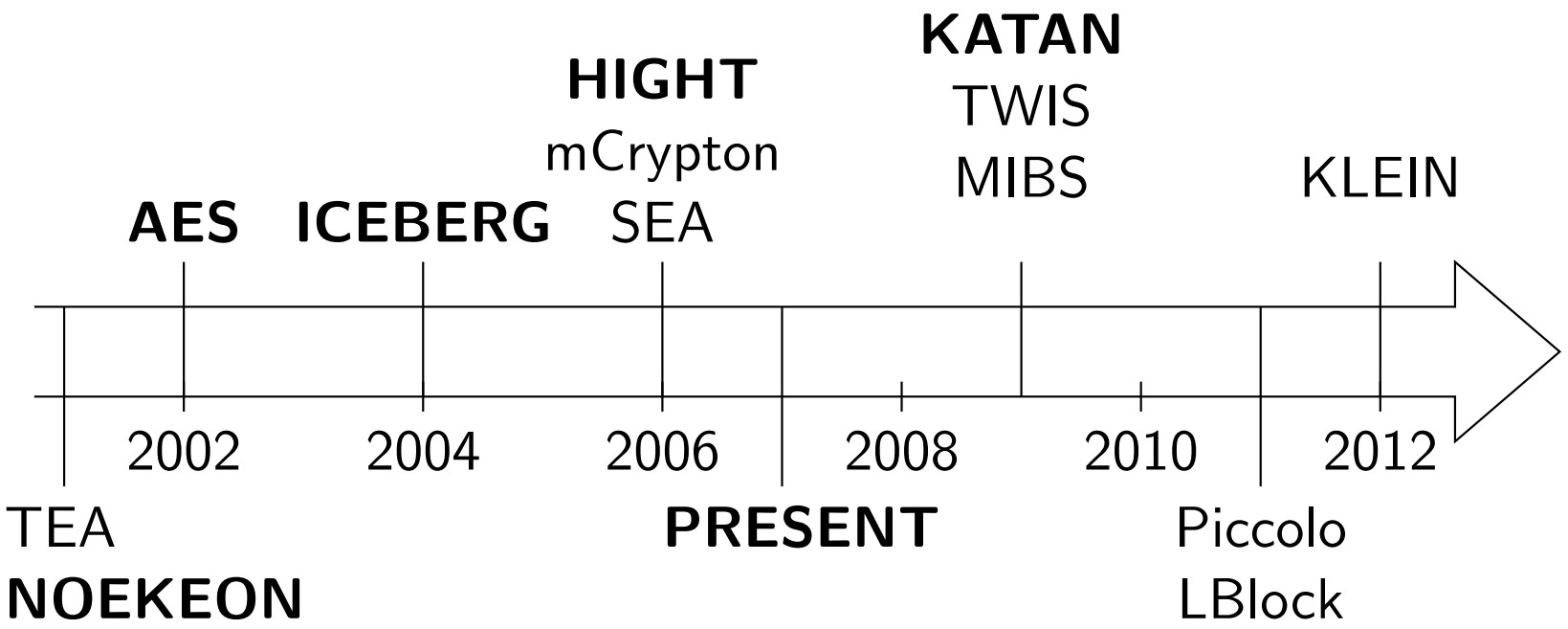


Lightweight Ciphers



- Many lightweight ciphers

Lightweight Ciphers

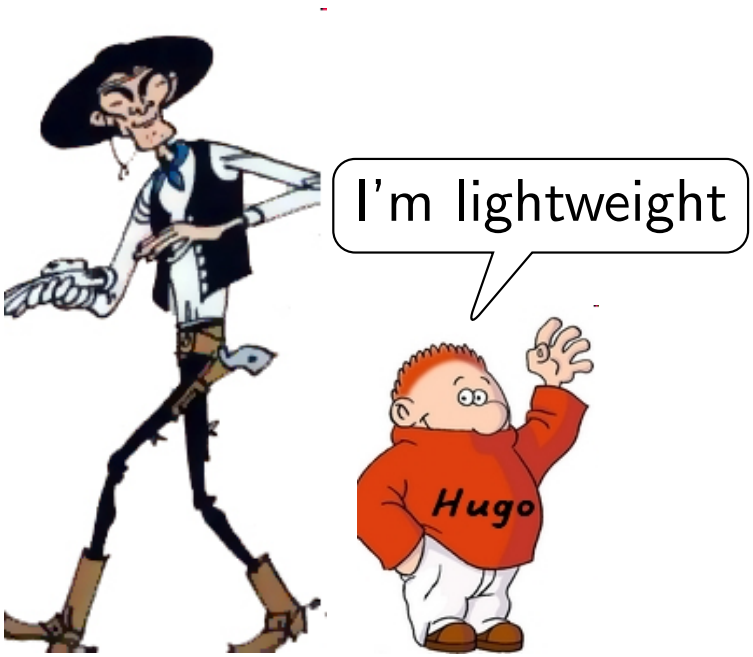


- Many lightweight ciphers
- Few comparative studies → Lack of standardization?
- Existing implementations → Different technologies
  → Focused on gate count

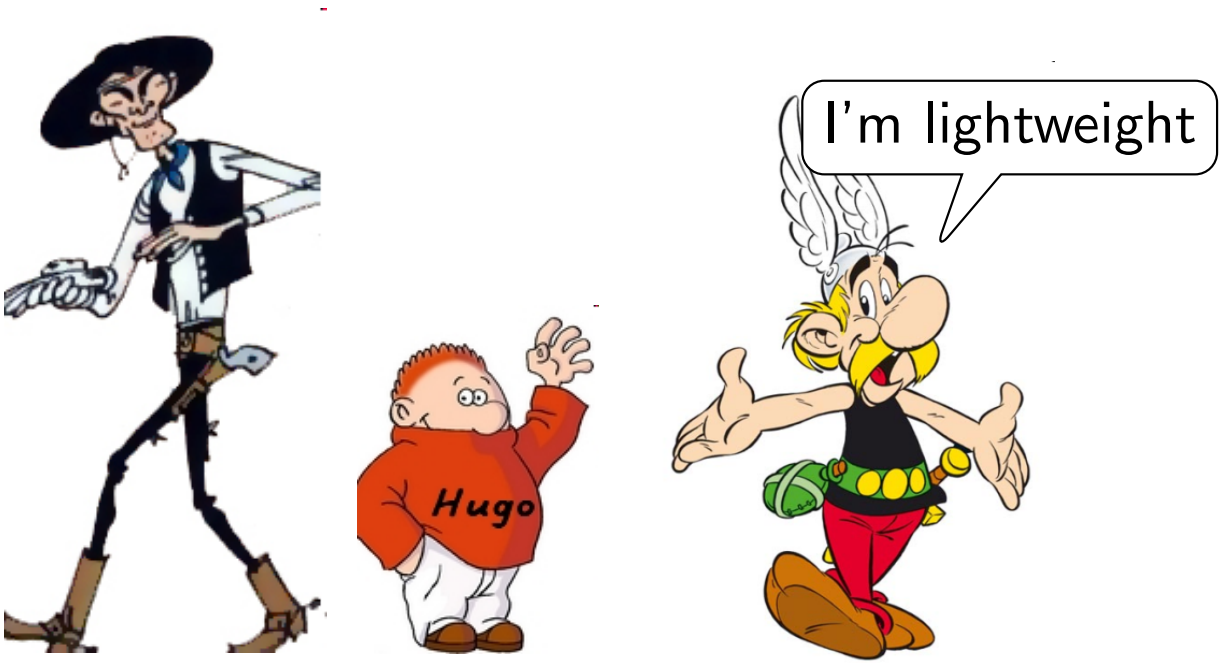
What is Lightweight?

What is Lightweight?

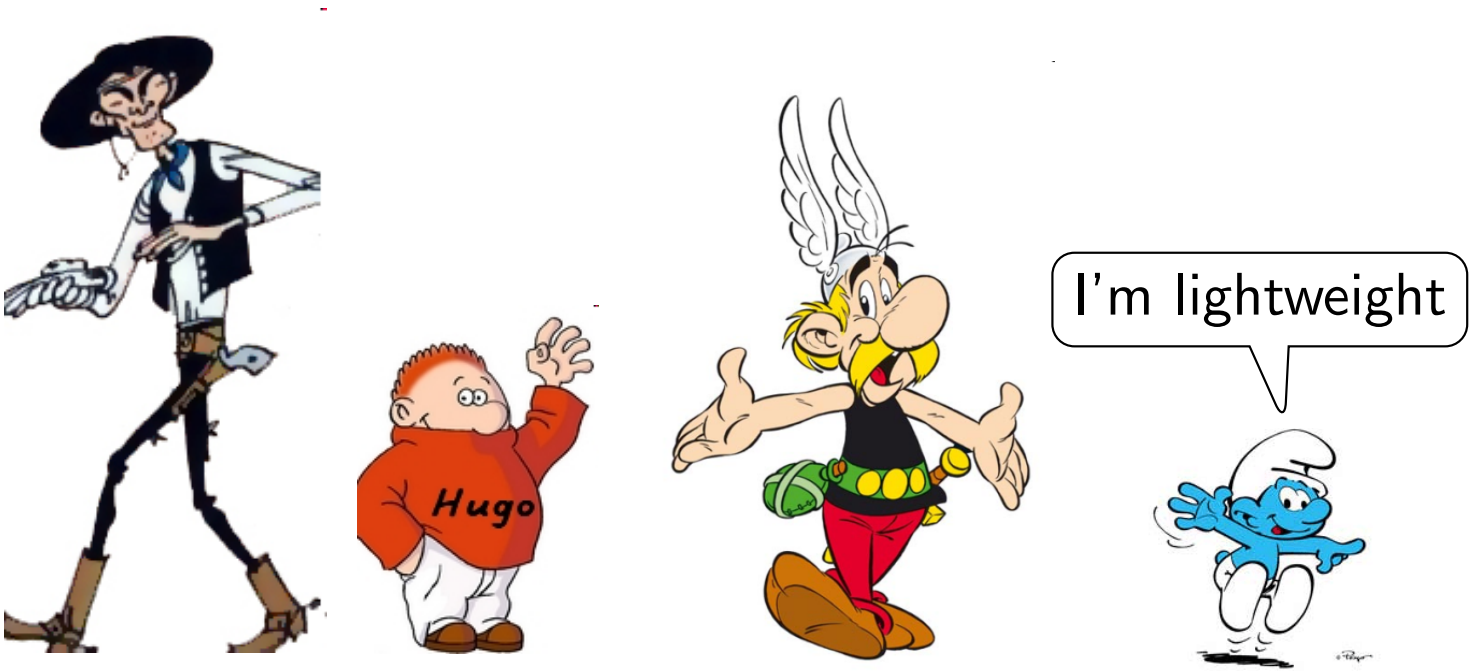
What is Lightweight?



What is Lightweight?



What is Lightweight?



What is Lightweight?

- Which criteria?
  - → Low area?
  - → Low power?
  - → Low energy?
  - → Still fast?
- Limitation: Relativity of metrics
  - → Possibility to optimize one criteria at the expense of another one

How Relevant is Lightweight Cryptography?

- Changing algorithm is expensive
- How much do we gain compared to
  - Hardware design choices (e.g. architecture)
  - Implementation choices (e.g. frequency/voltage scaling)

Outline

This Work

Algorithms choice

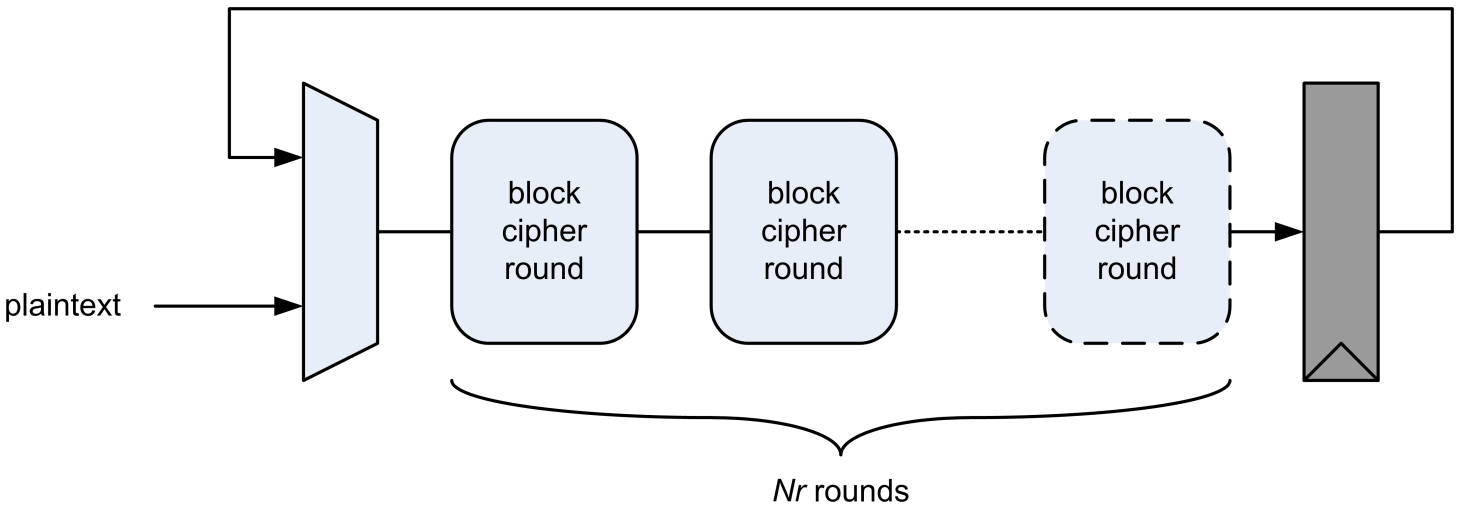
- Block and key sizes
- Different types of key scheduling
- Different combinations of encryption/decryption

Block	Key	Ciphers	
128	128	AES	NOEKEON
64	128	HIGHT	ICEBERG
64	80	KATAN	PRESENT

This Work

Flexible architecture

- 3 core options (Enc, Dec, Enc/Dec)
- Unrolling parameter Nr



This Work

Technology: Low-power 65 nm CMOS

Comparative study

- At fixed frequency f_{100}
- At maximum frequency f_{max} (max. area penalty = 10%)
- For all metrics

Area	Frequency	Power	**Energy**	Throughput

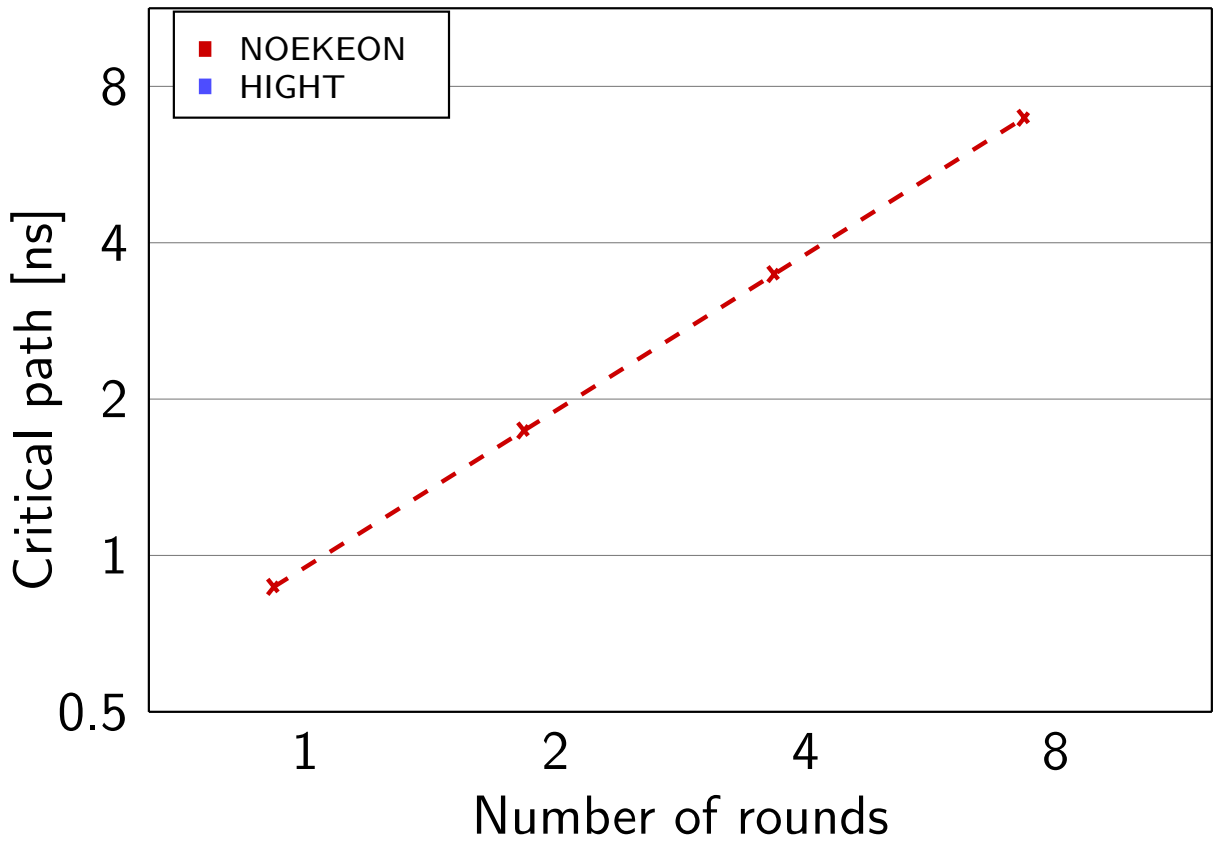
Frequency/Voltage scaling

$$E_{op} = \frac{1}{2} N_{sw} C_L \mathbf{V_{dd}^2} + E_{leak}$$

Outline

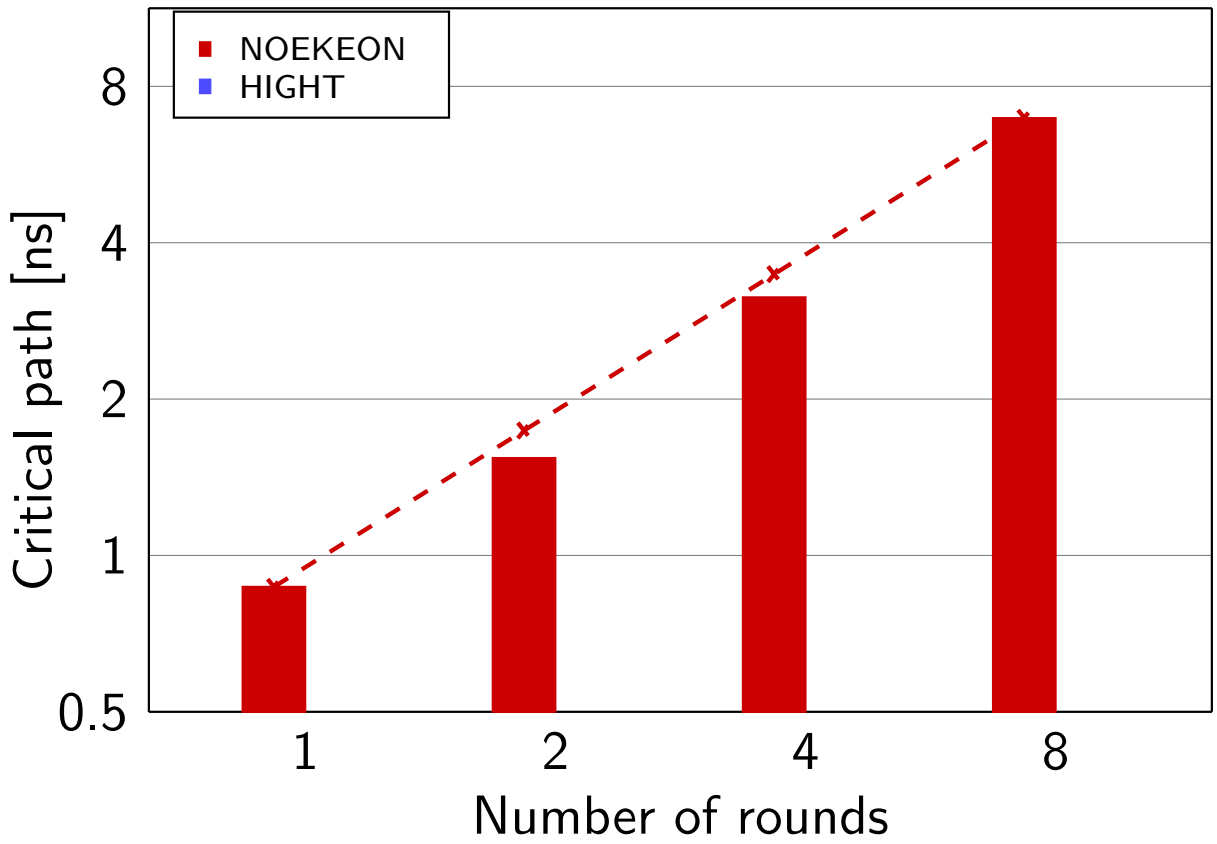
Critical Path

Expectation: Number of rounds x 2 $\Rightarrow$ Critical path x 2



Critical Path

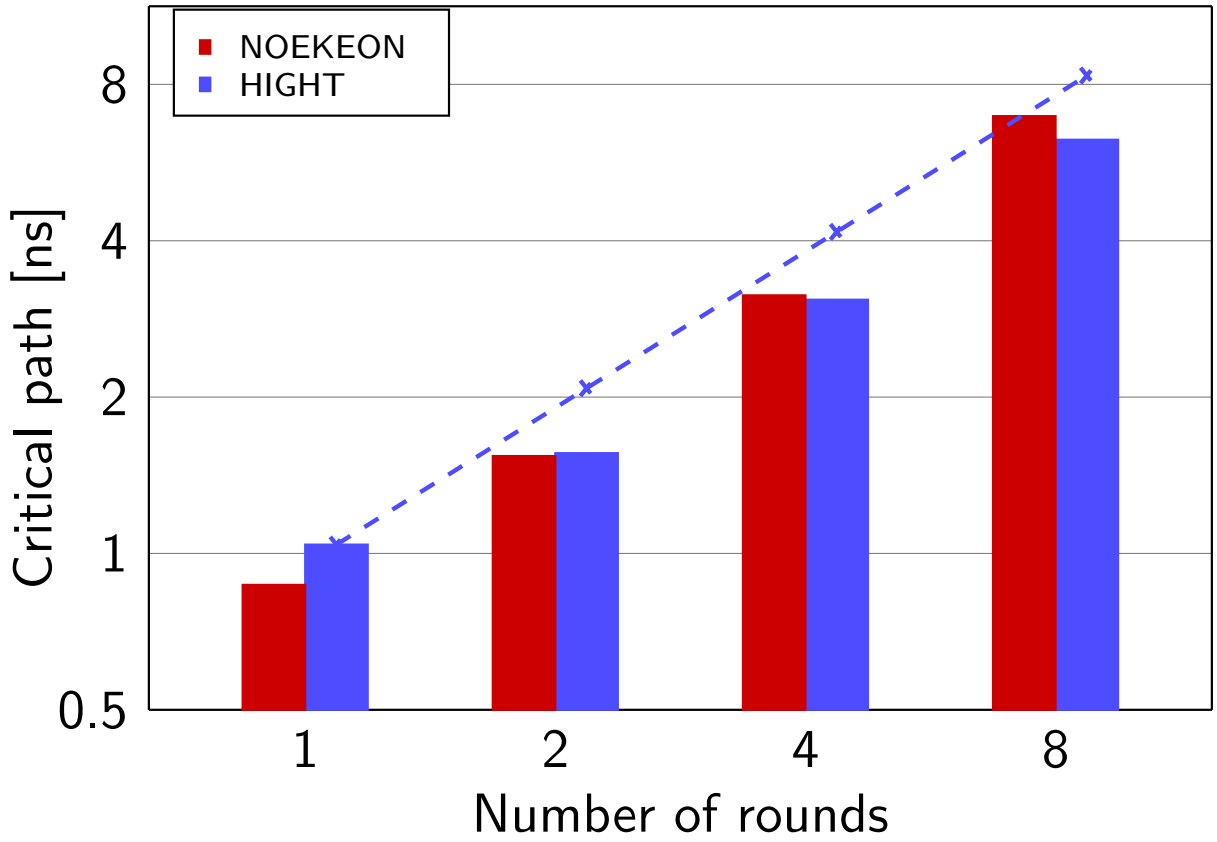
Expectation: Number of rounds x 2 $\Rightarrow$ Critical path x 2



Critical Path

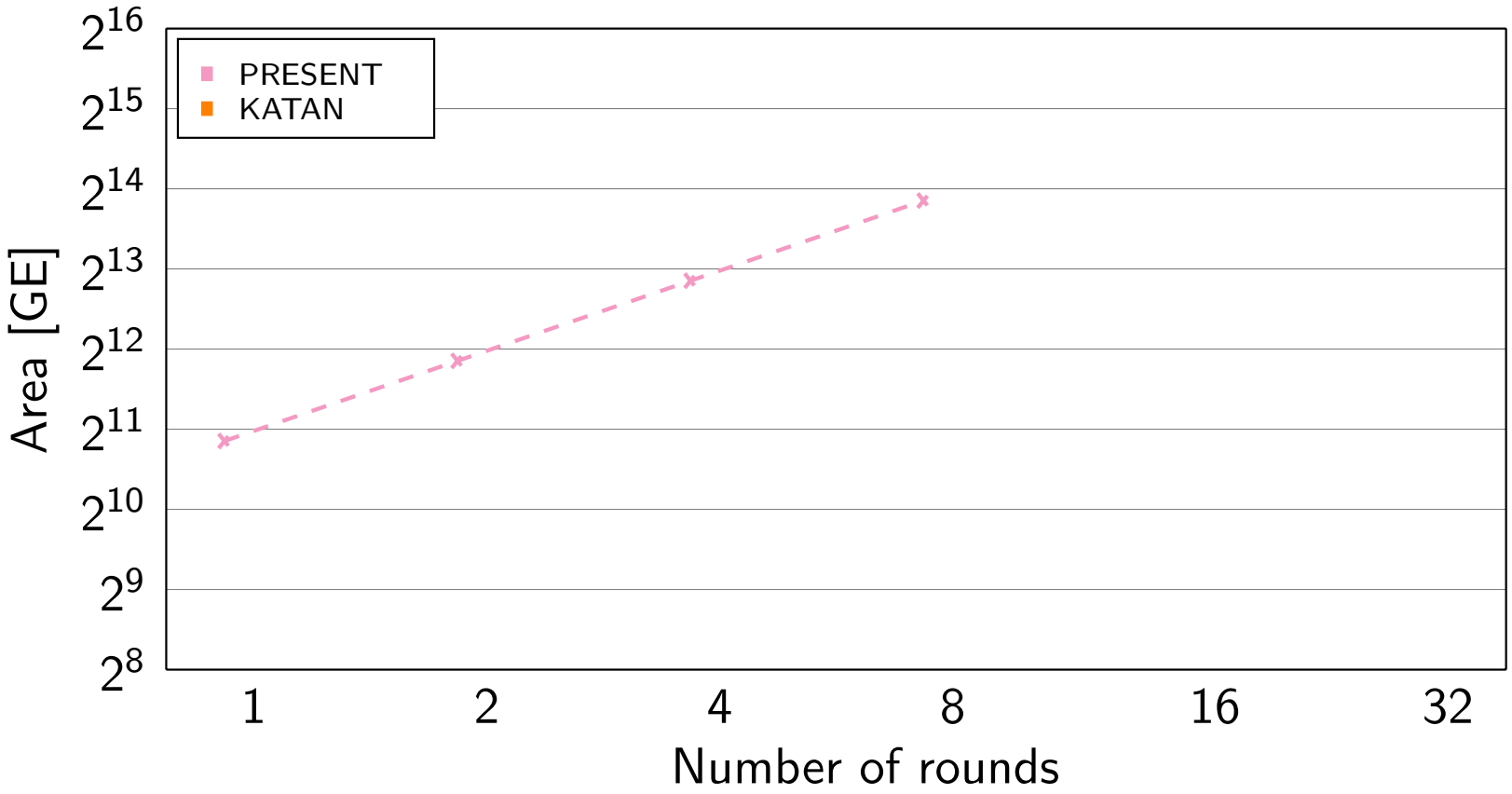
Expectation: Number of rounds x 2 $\Rightarrow$ Critical path x 2

Observation: Critical path not always in the round logic



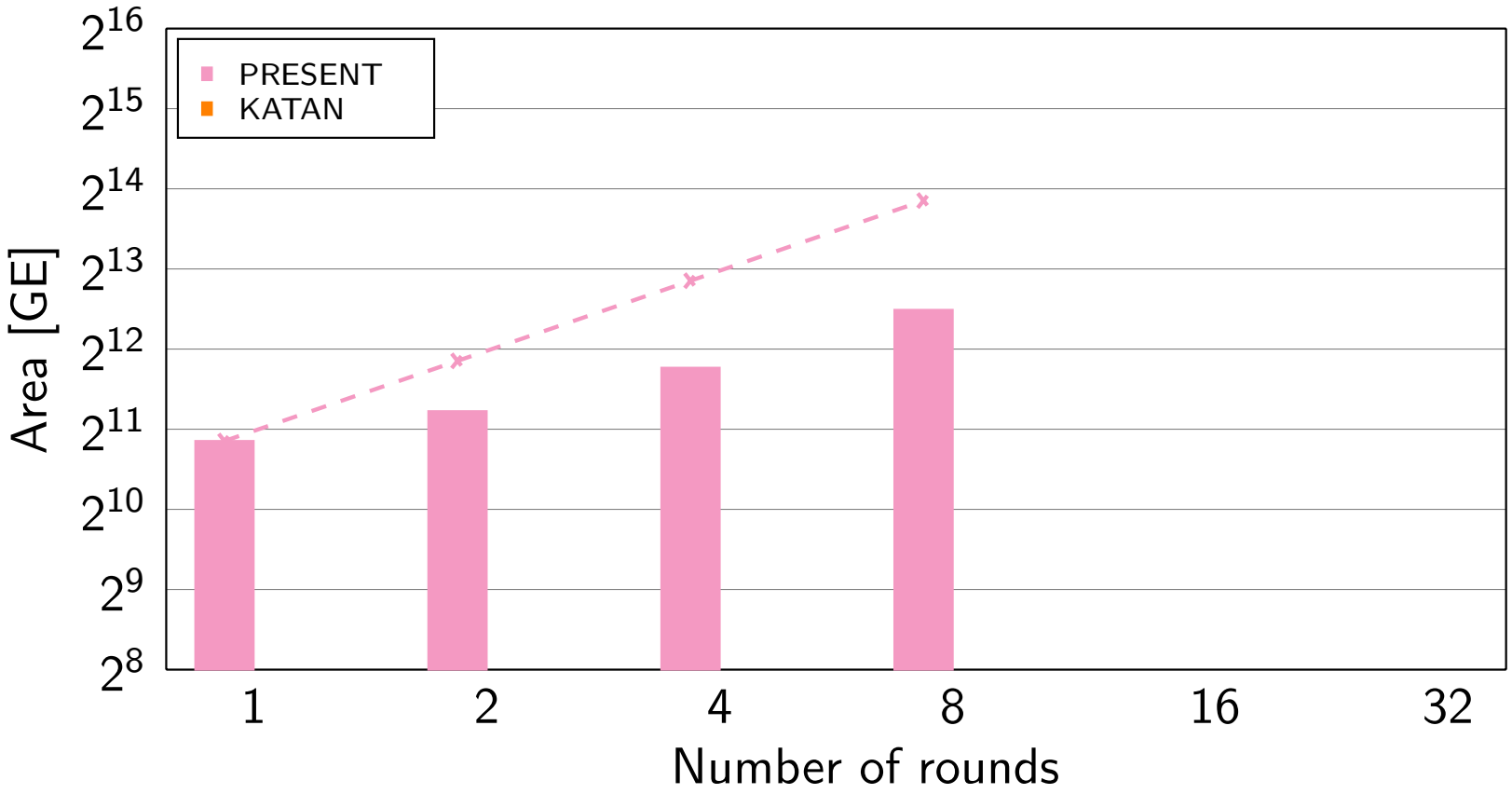
Area

Naive expectation: Number of rounds x 2 $\Rightarrow$ Area x 2



Area

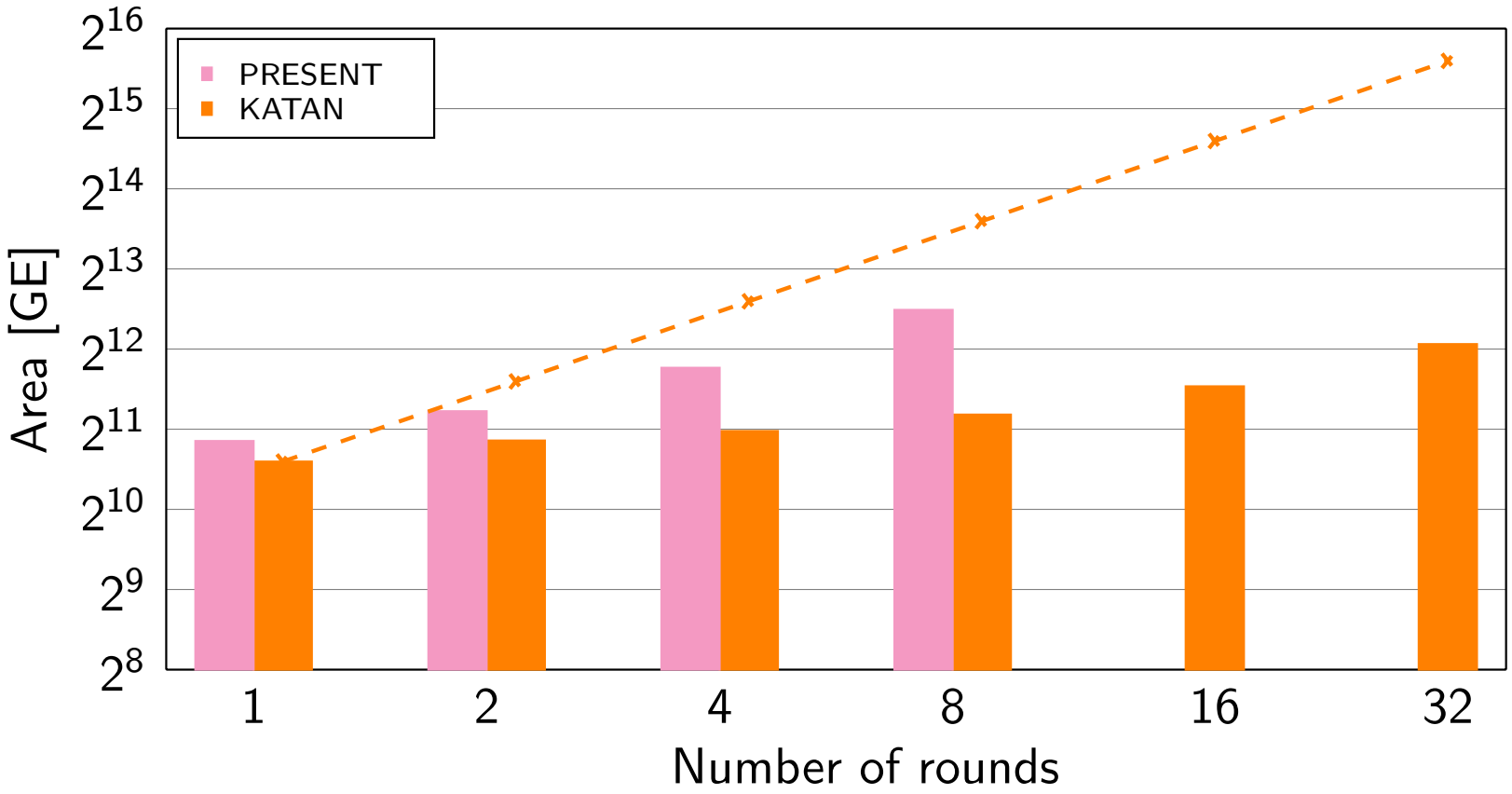
Naive expectation: Number of rounds x 2 $\Rightarrow$ Area x 2



Area

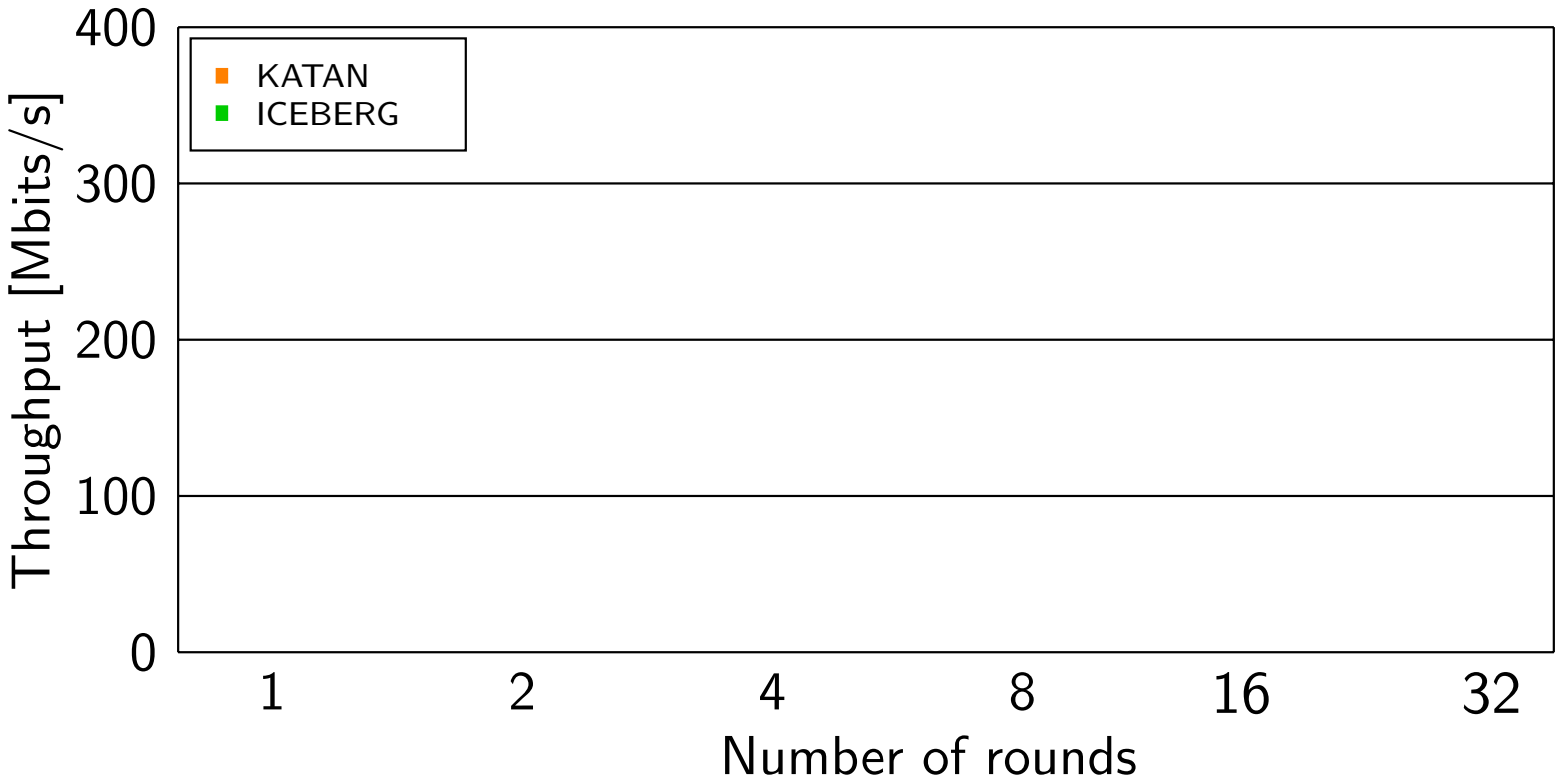
Naive expectation: Number of rounds x 2 ⇒ Area x 2

Observation: Main component of area = state register



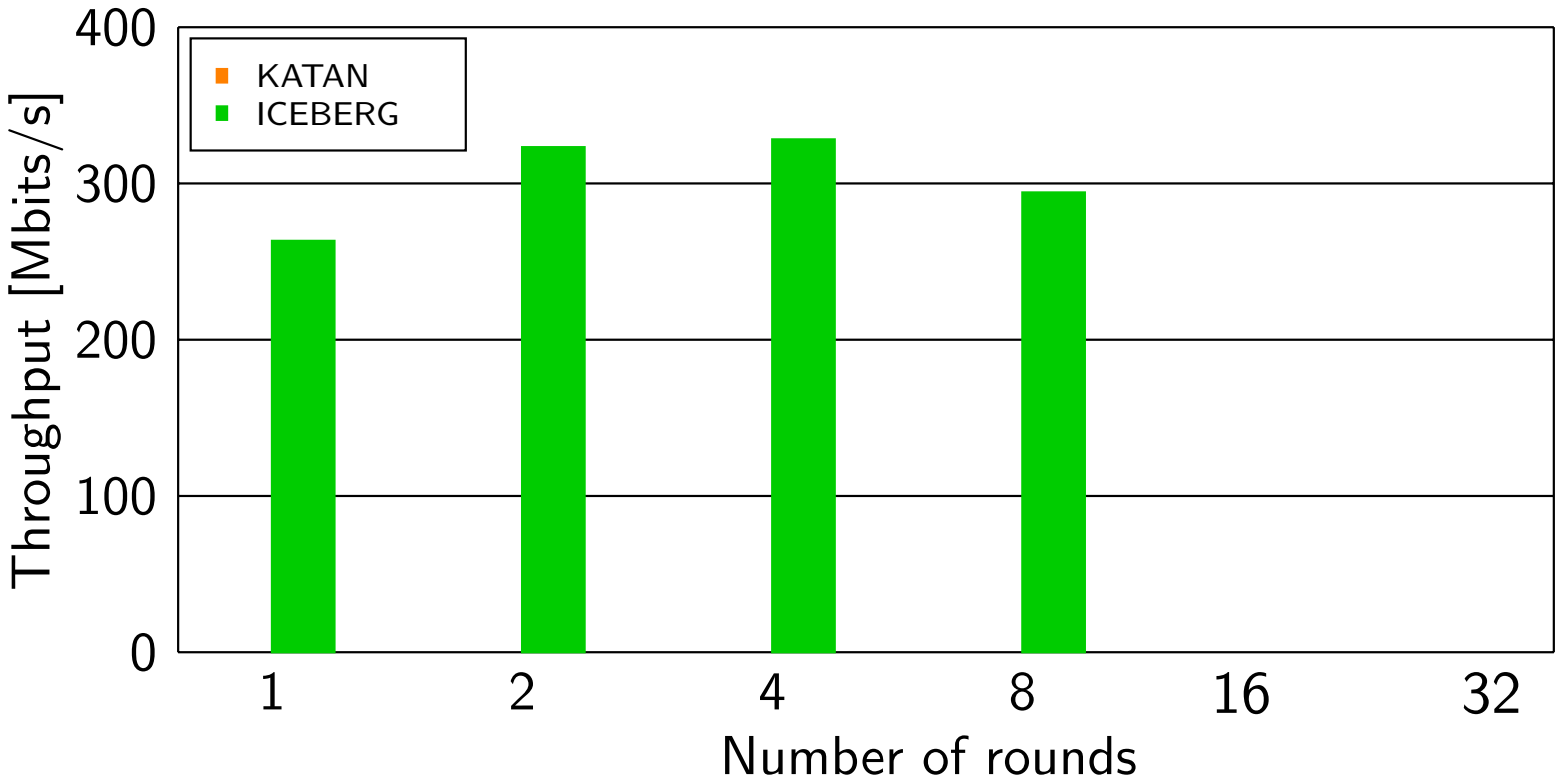
Throughput

Expectation: Round unrolling should not make sense at f_{max}



Throughput

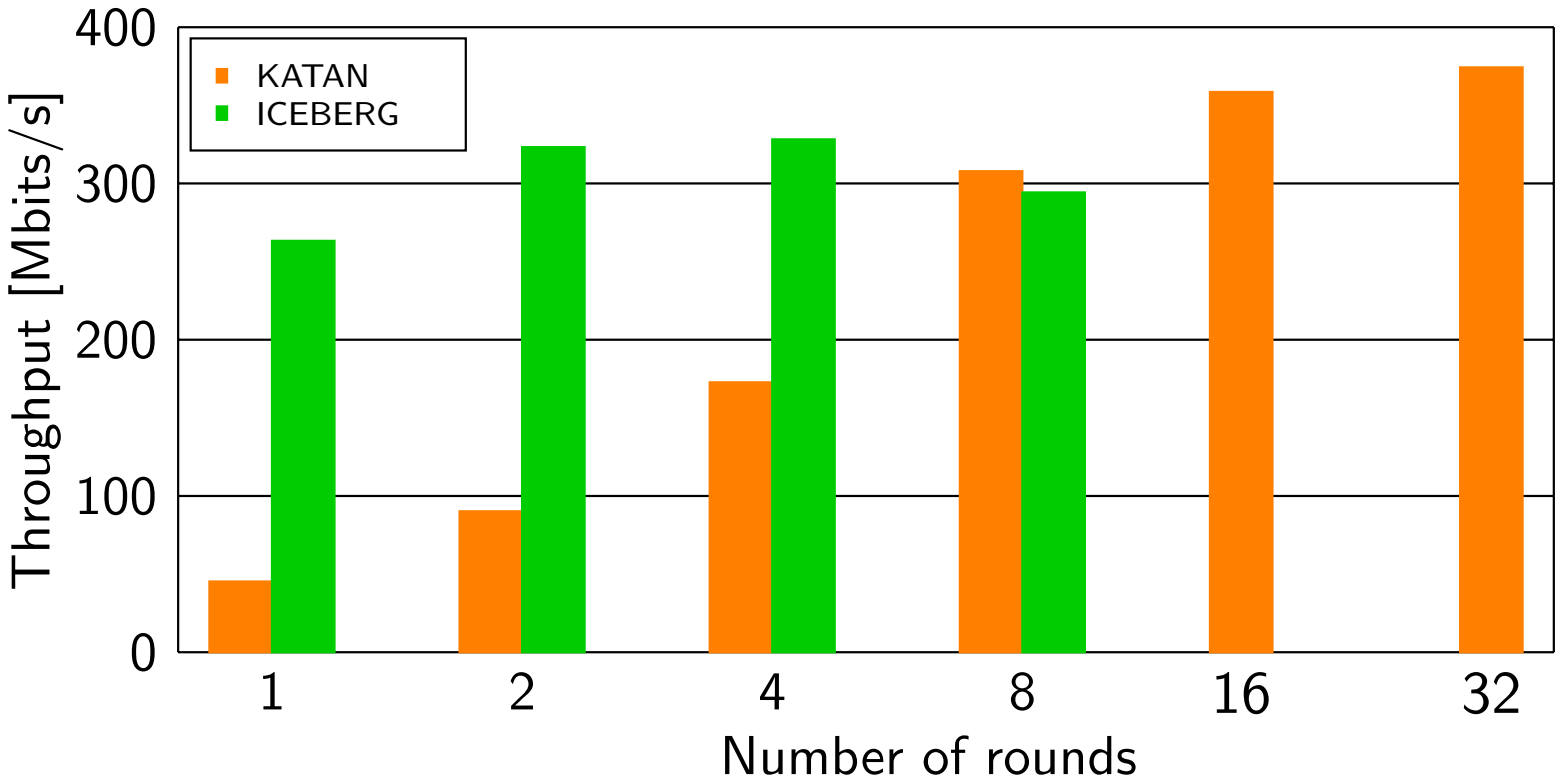
Expectation: Round unrolling should not make sense at f_{max}



Throughput

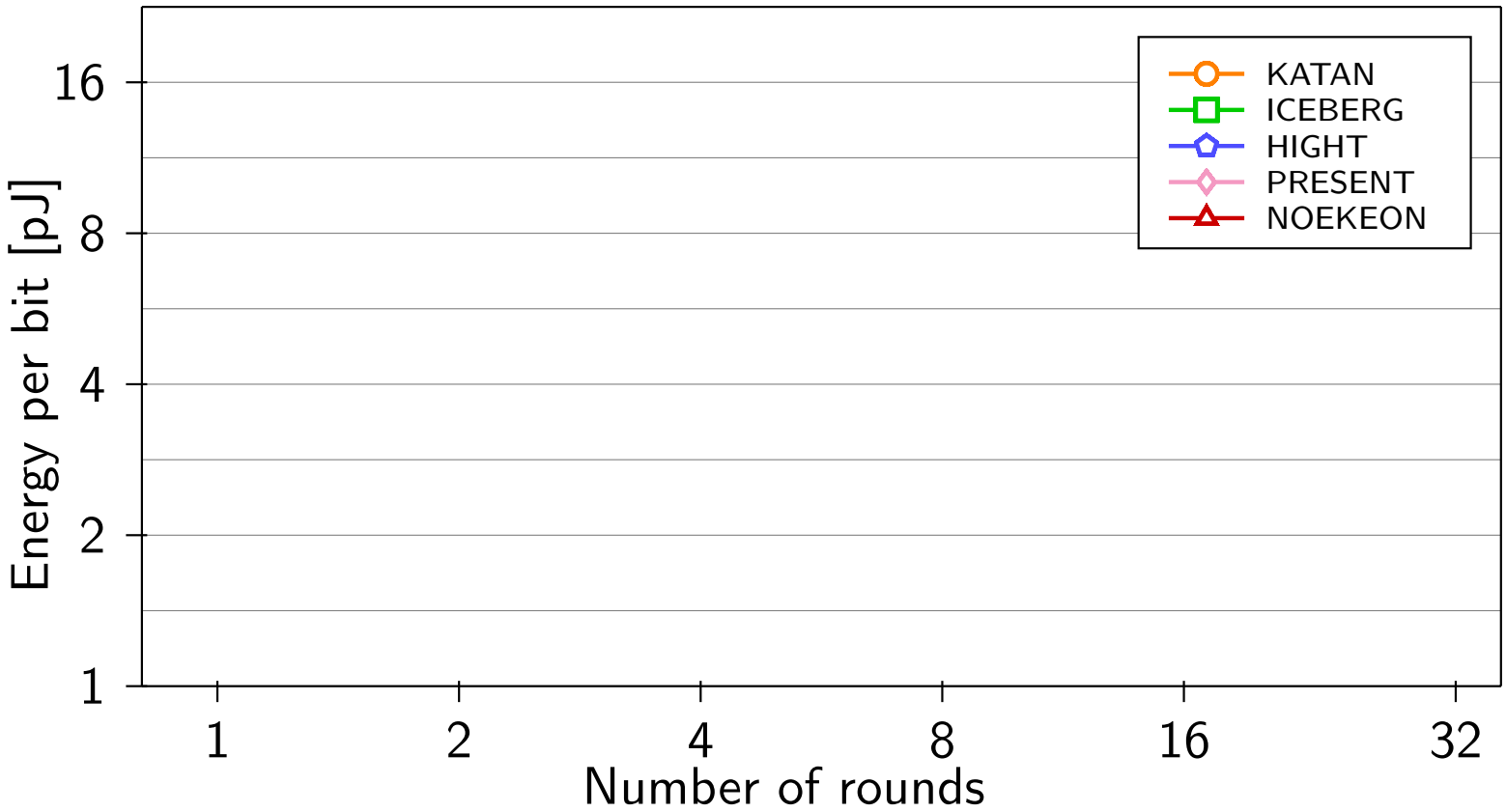
Expectation: Round unrolling should not make sense at f_{max}

Observation: And for extremely simple rounds



Energy

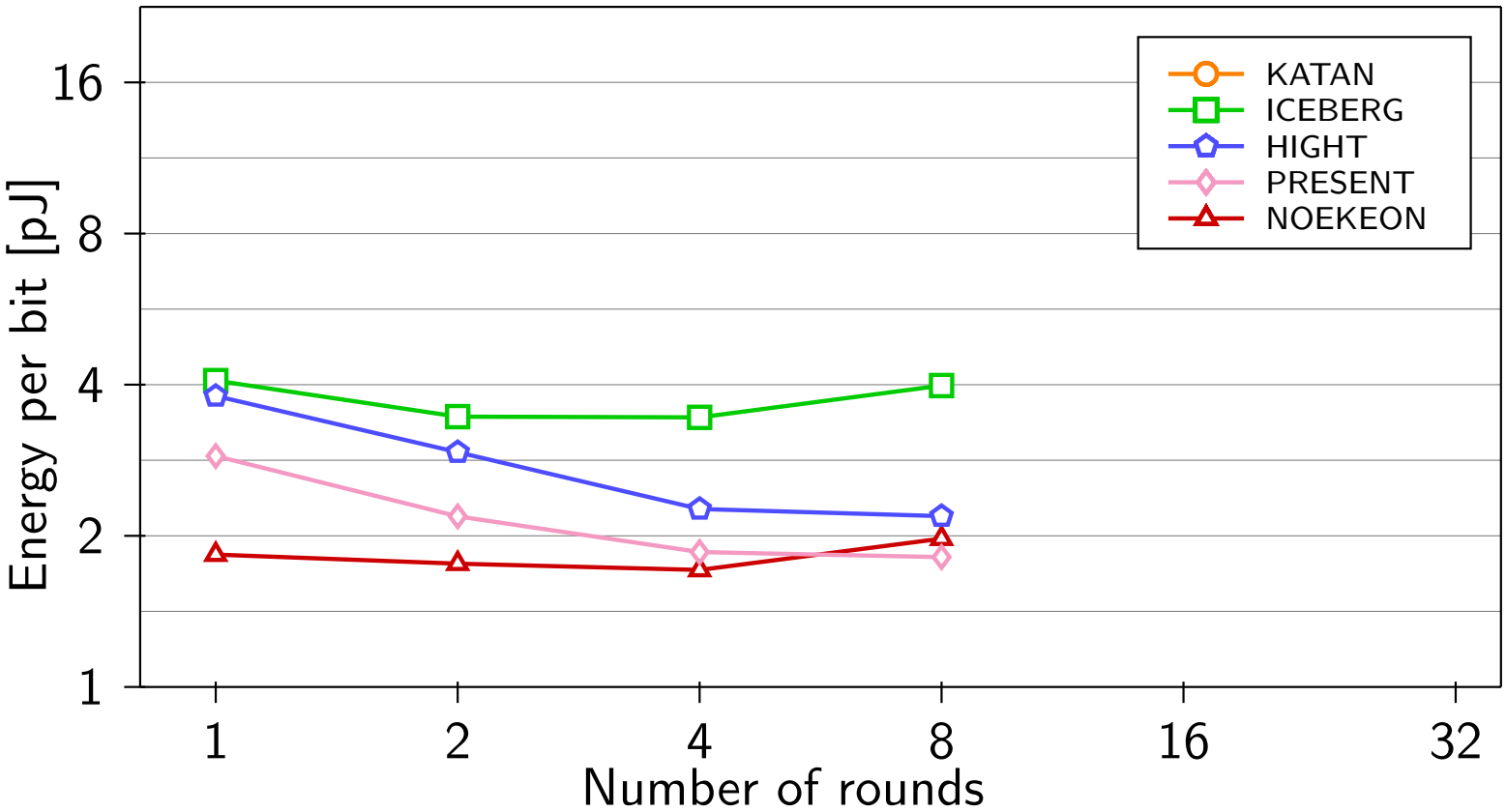
Expectation: Energy stable with number of rounds



Energy

Expectation: Energy stable with number of rounds

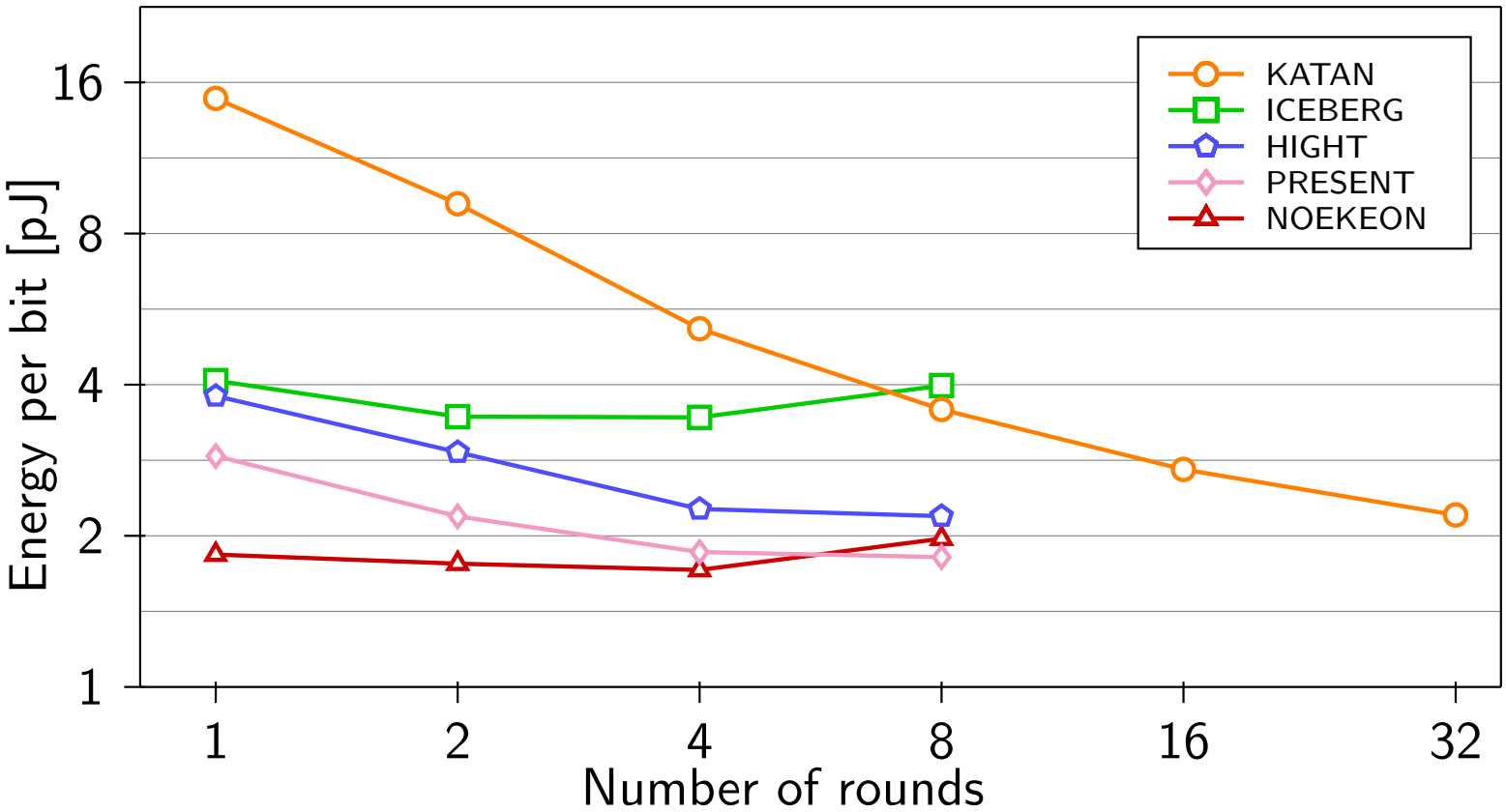
Observation: Energy more or less stable



Energy

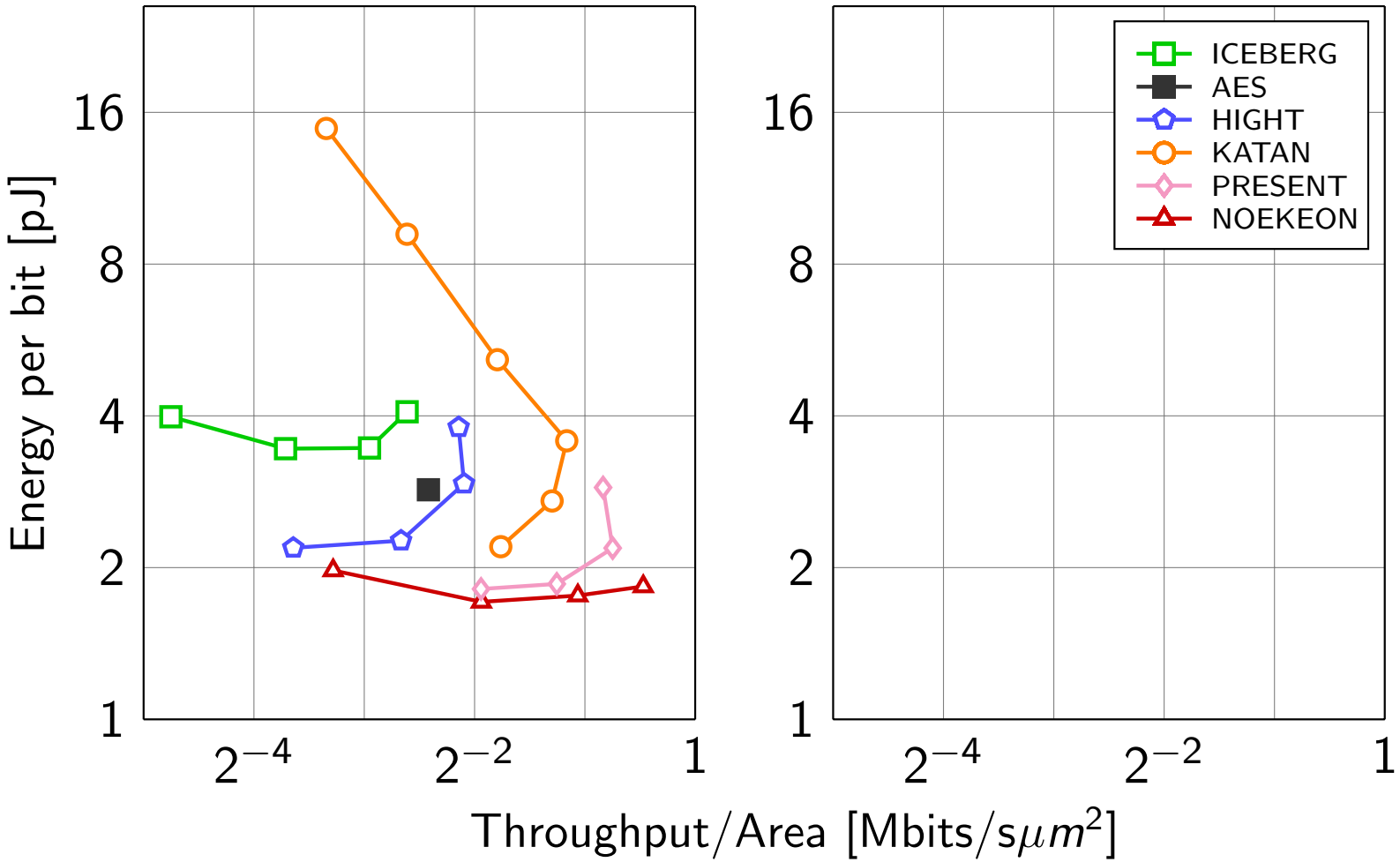
Expectation: Energy stable with number of rounds

Observation: Trend observed later for KATAN

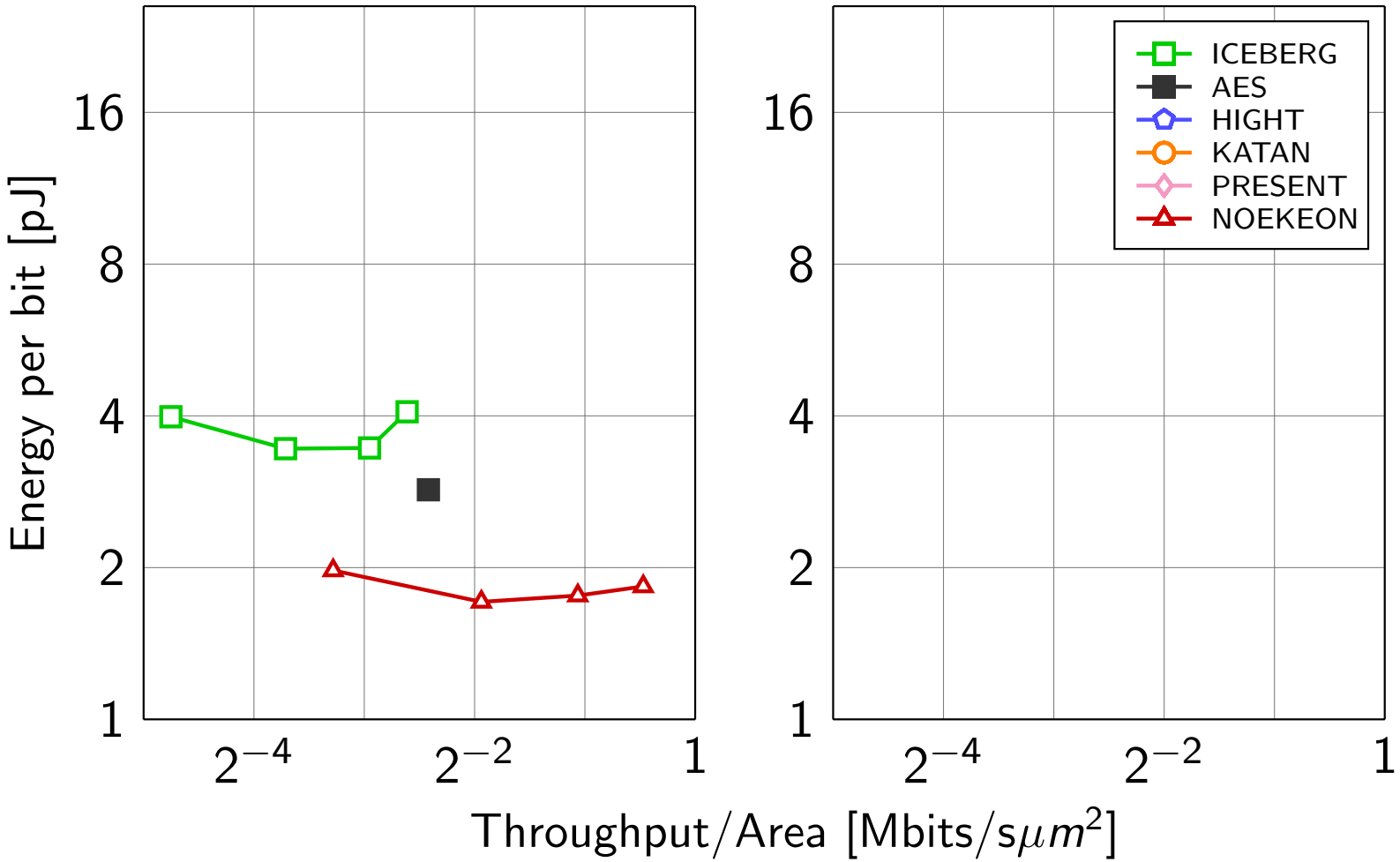


Outline

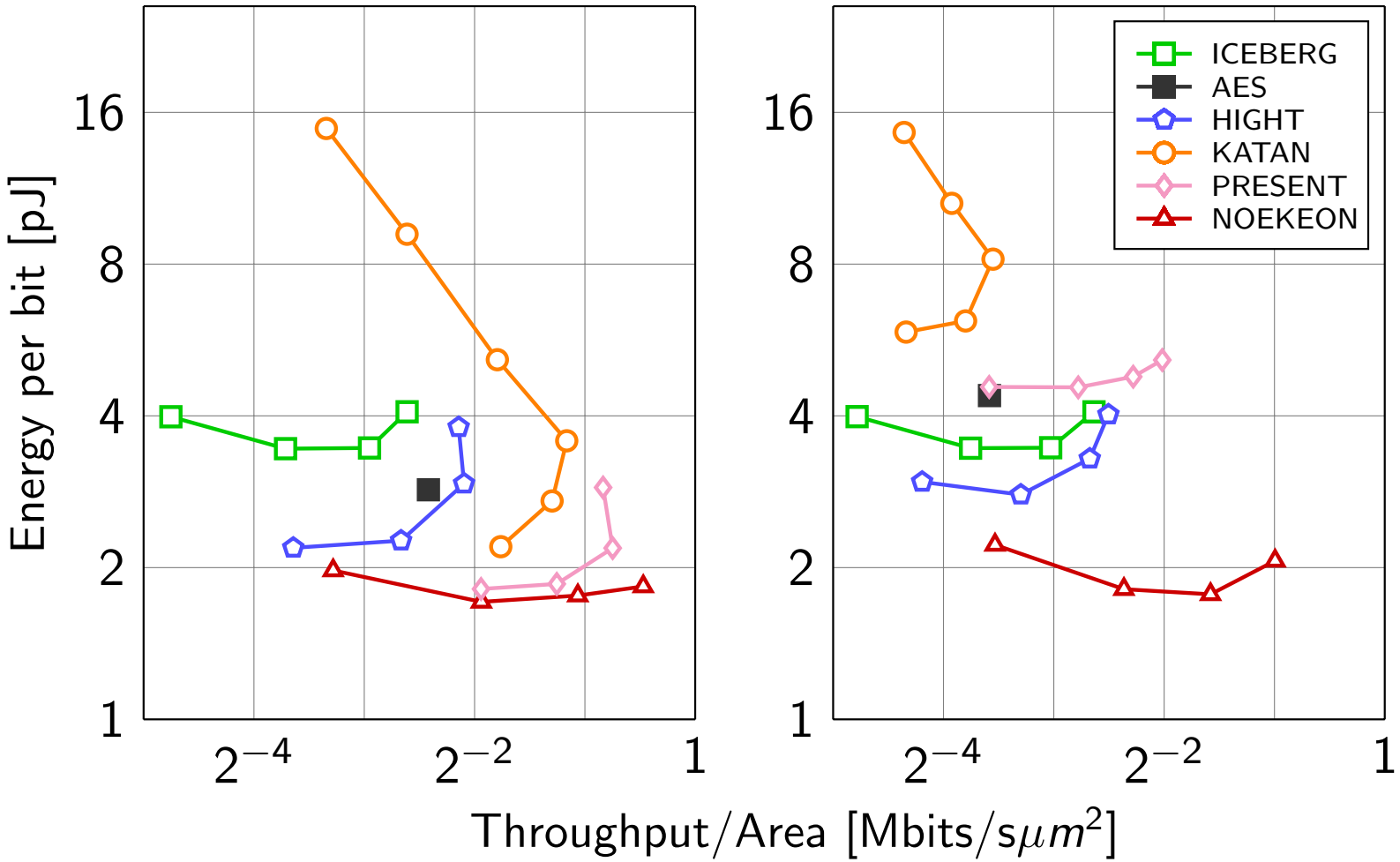
Encryption Only



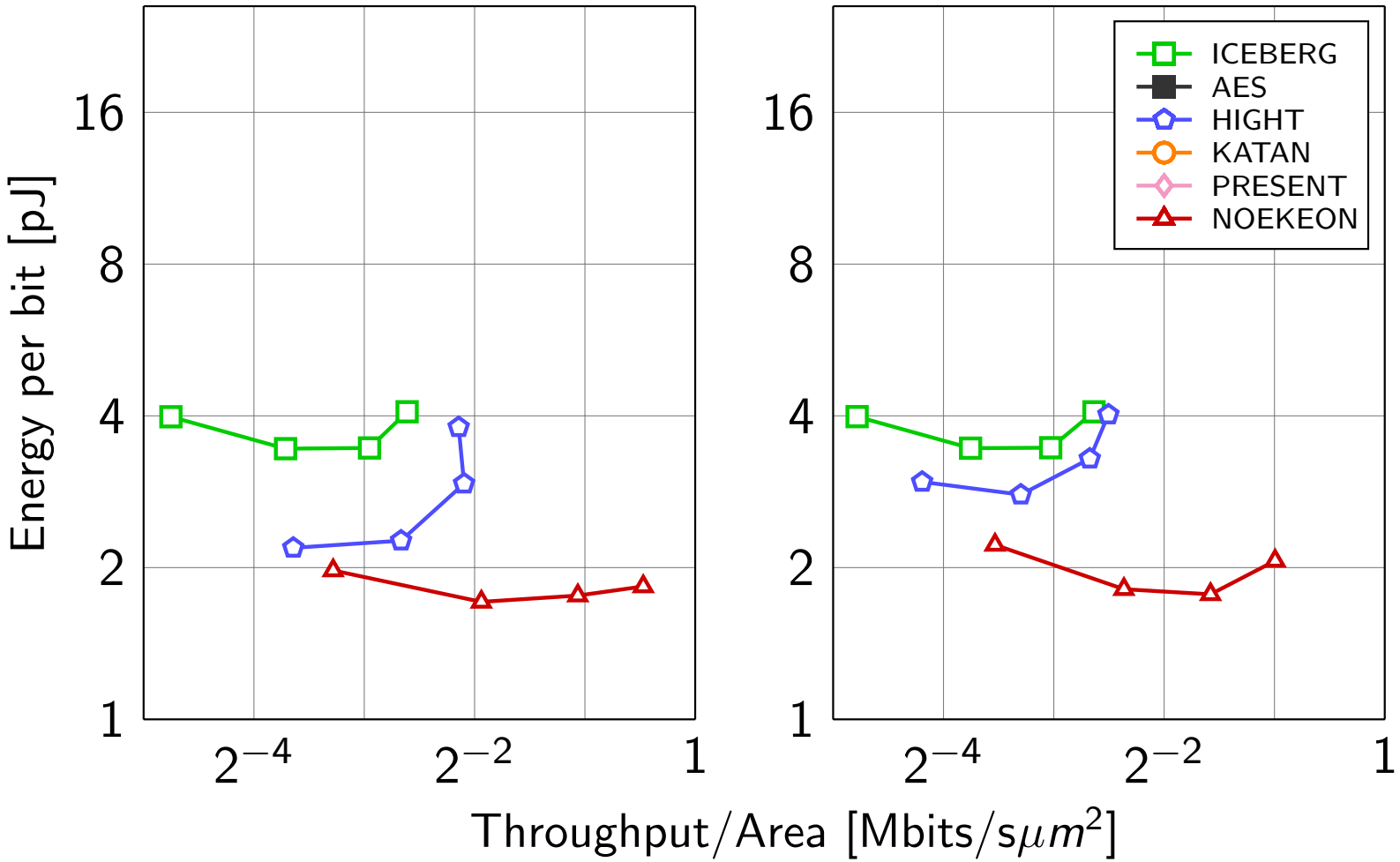
Impact of Key Scheduling



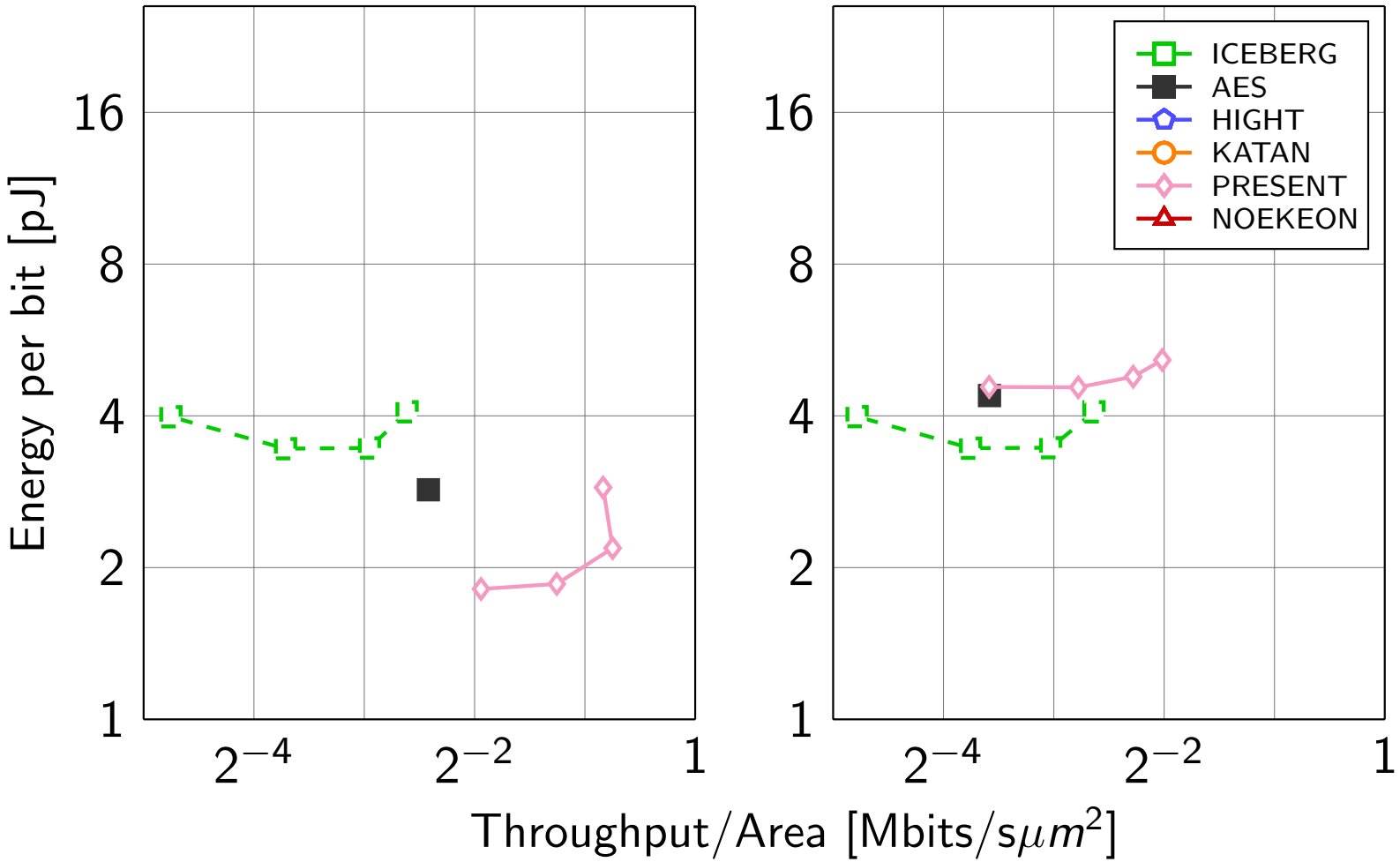
Encryption/Decryption



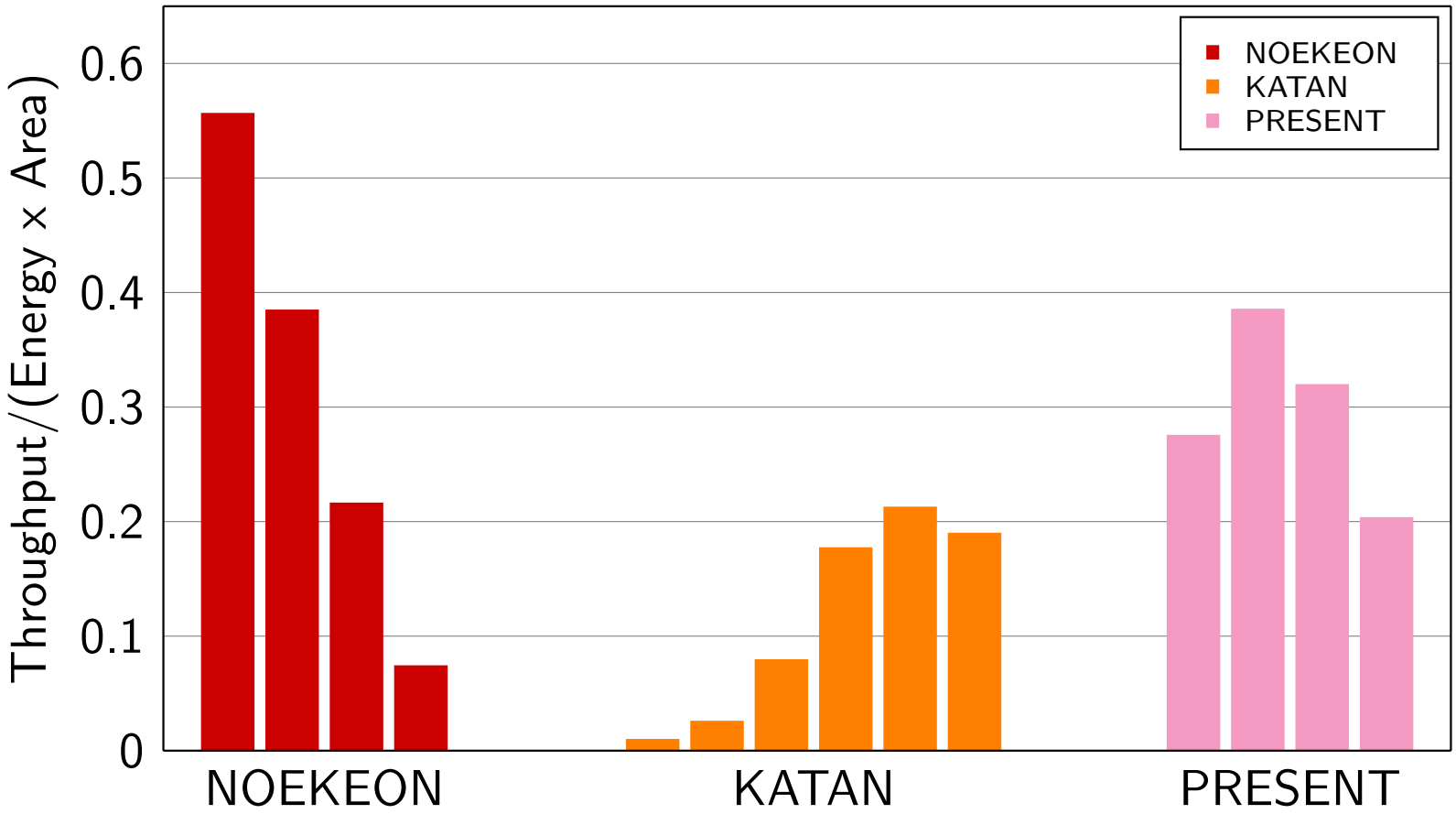
"On the Fly" Key Scheduling



vs. not "On the Fly" Key Scheduling

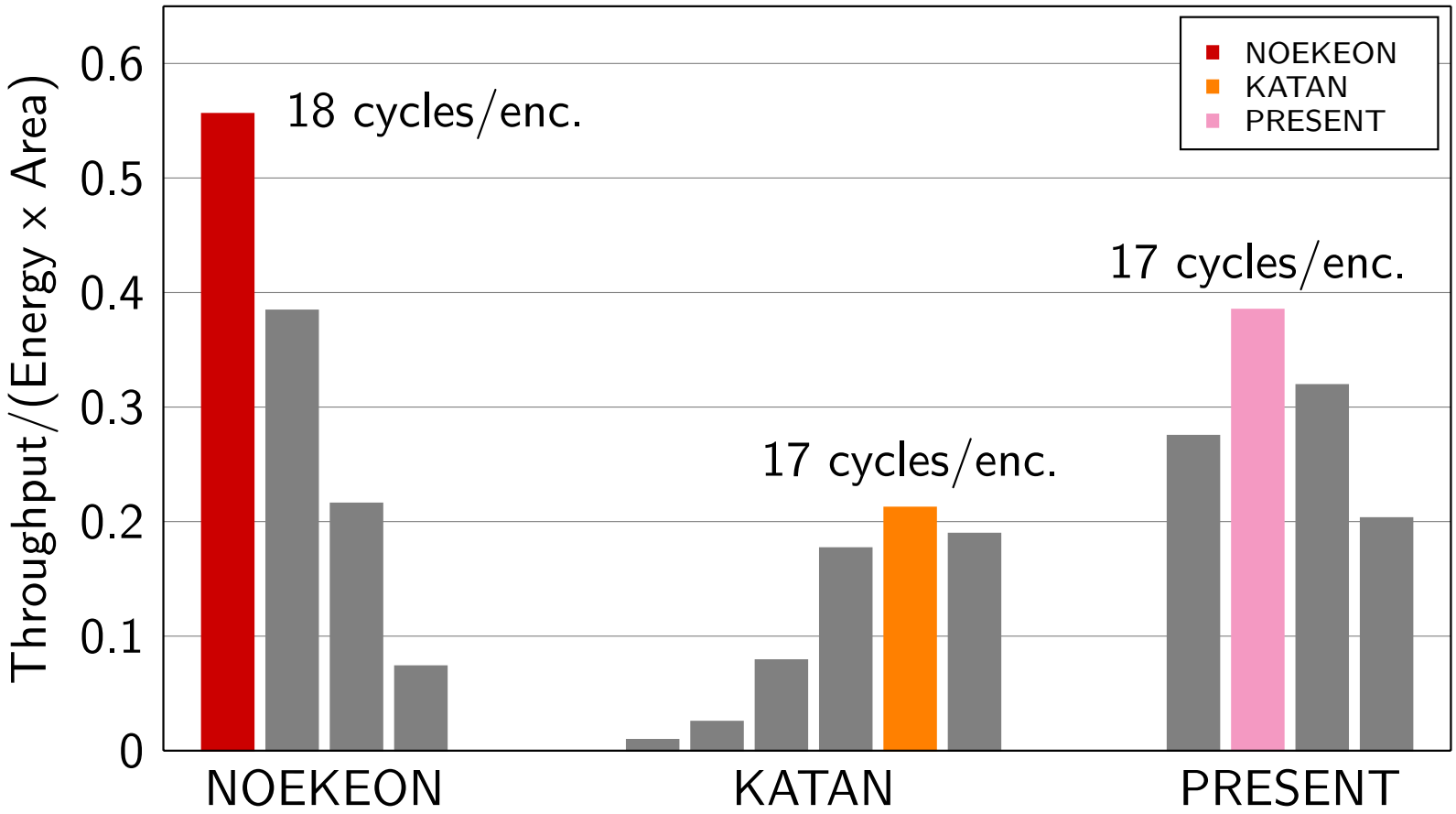


Efficiency


Throughput/(Energy x Area)
0.6
0.5
0.4
0.3
0.2
0.1
0
NOEKEON
KATAN
PRESENT
NOEKEON
KATAN
PRESENT

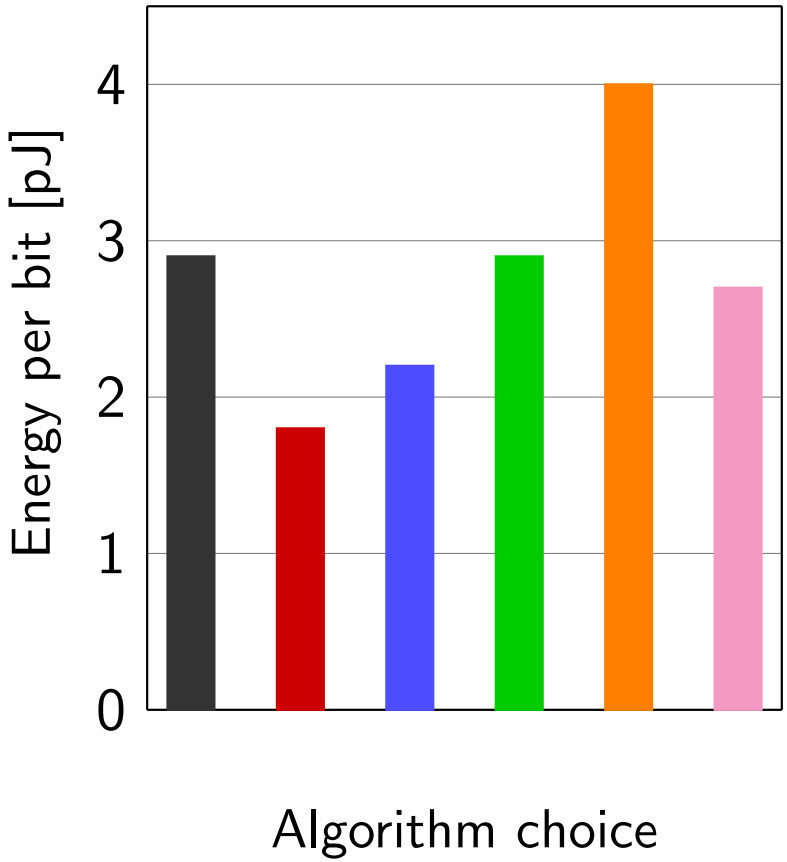
Efficiency

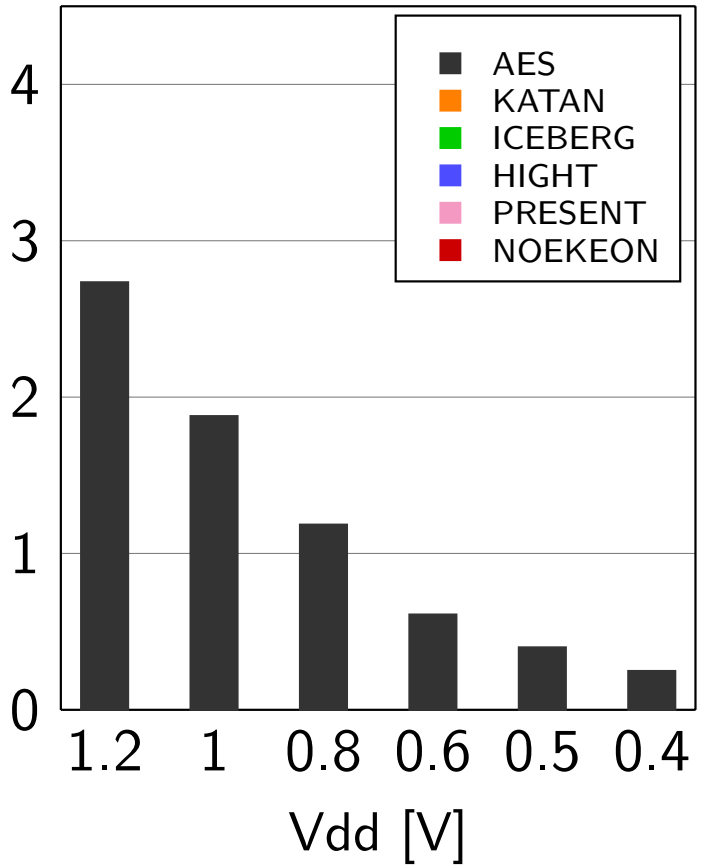
Observation: Definition of round is arbitrary



Frequency/Voltage Scaling

Observation: Better energy gain with frequency/voltage scaling





Outline

Conclusion

Comparative studies are usefull

Energy: Interesting efficiency metric

Algorithm design

- Definition of round is arbitrary
- Impact of key scheduling
- Efficient combination of encryption and decryption

AES is a low energy cipher

Voltage scaling: If allowed, has strong impact on energy

Thank you!