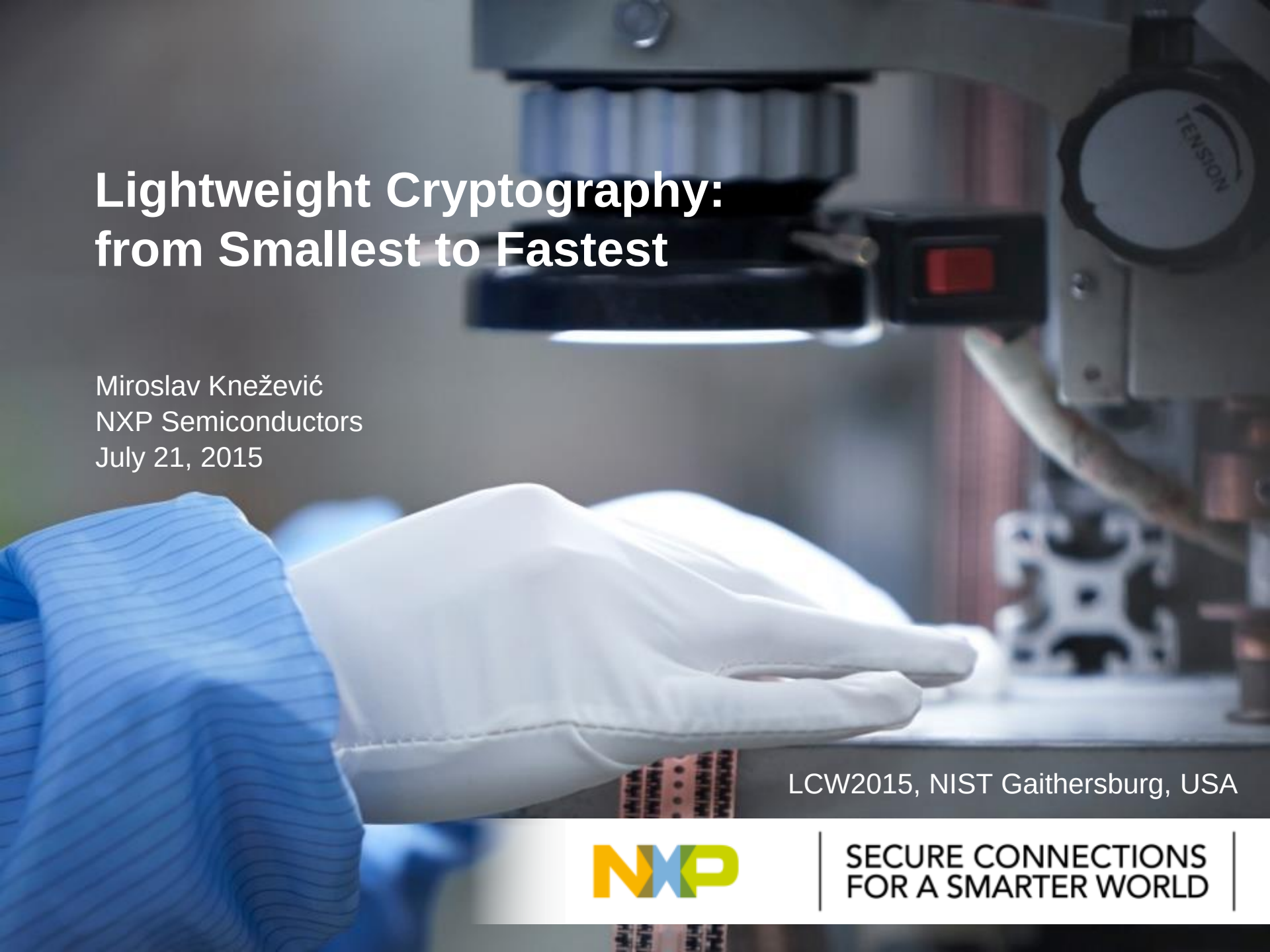
Lightweight Cryptography: from Smallest to Fastest

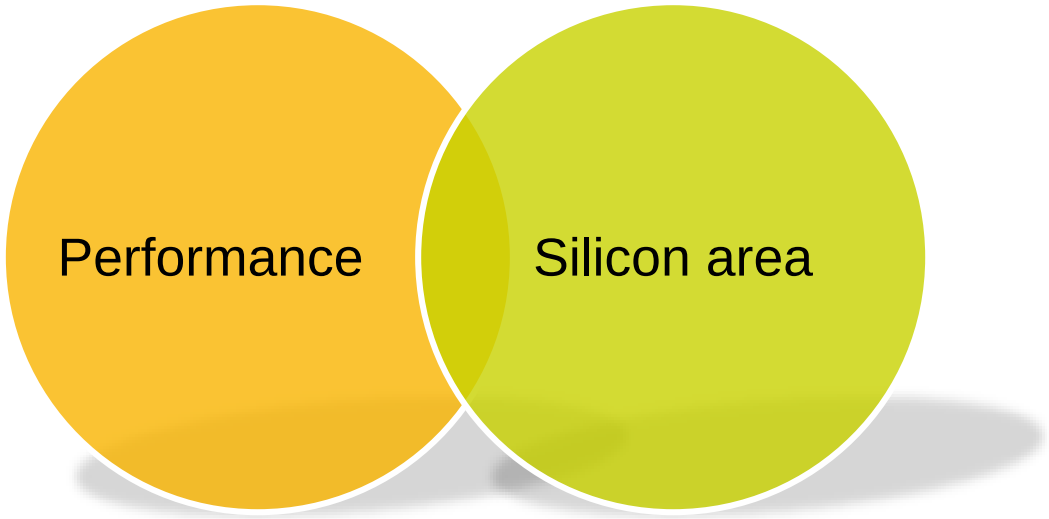
Miroslav Knežević
NXP Semiconductors
July 21, 2015

LCW2015, NIST Gaithersburg, USA

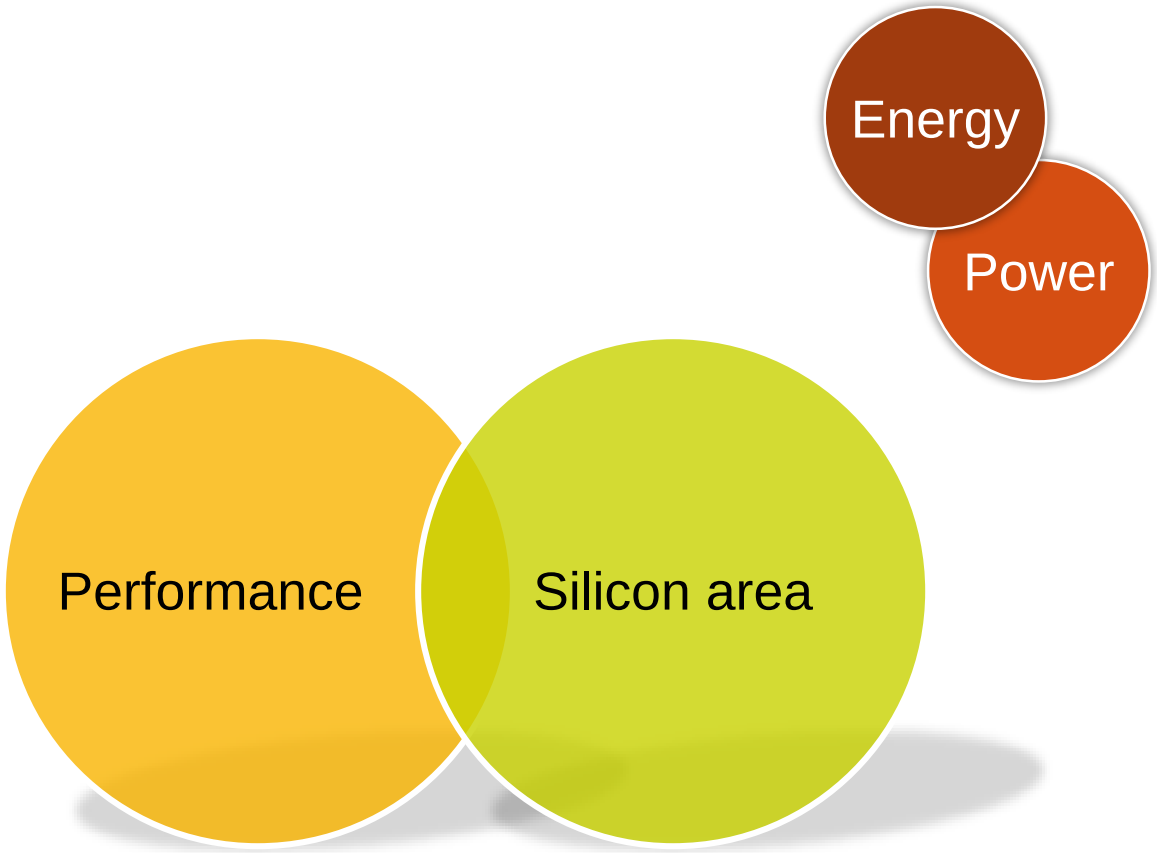


NXP SECURE CONNECTIONS FOR A SMARTER WORLD

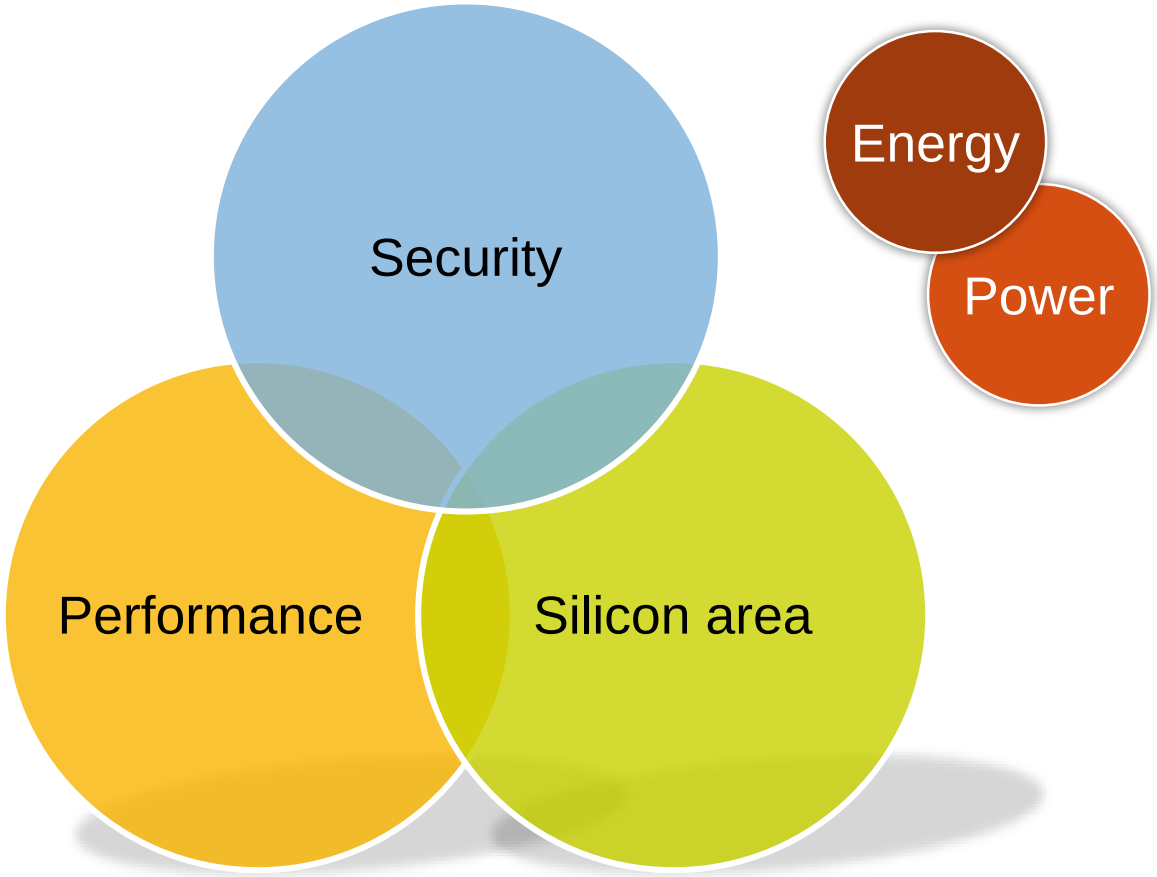
Trade-offs in HW



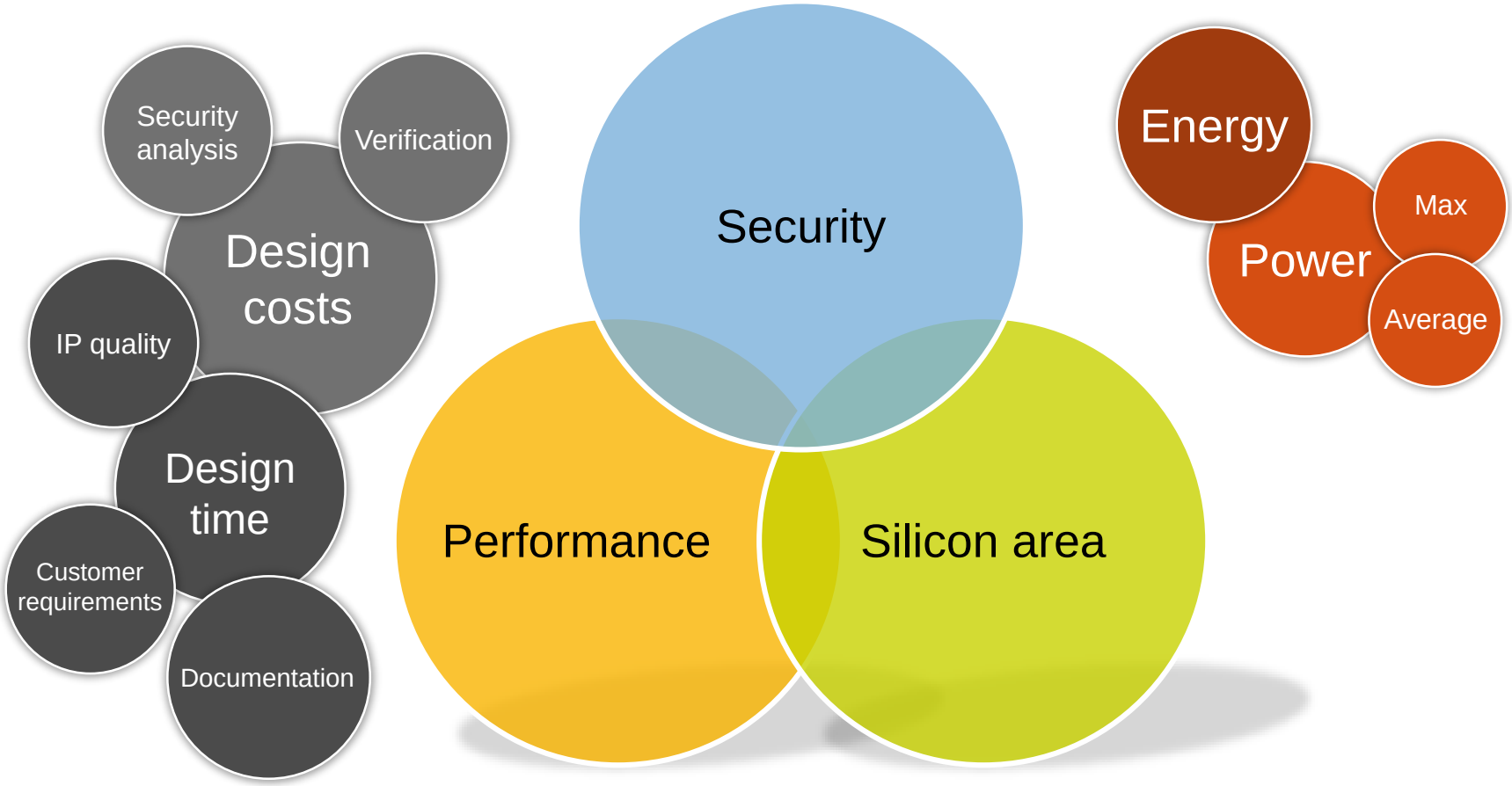
Trade-offs in HW



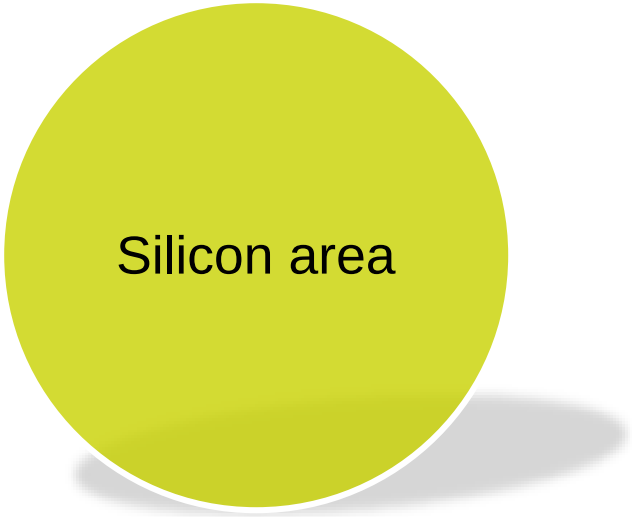
Trade-offs in Crypto HW



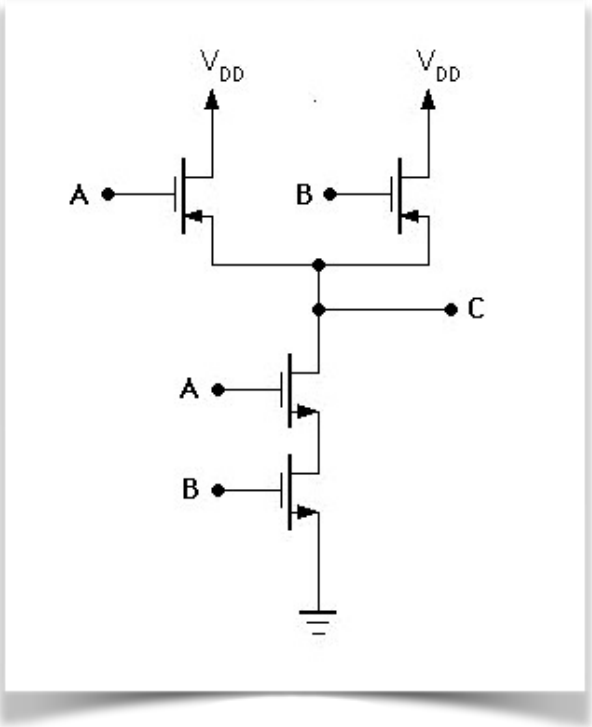
Trade-offs in Crypto HW



Designing the Smallest Block Cipher



NAND gate



- Smallest logic gate with two inputs.
- GE (gate equivalence) = physical area of a single NAND gate.
- (Ab)used for comparing HW designs across different CMOS technologies.
- When comparing lightweight crypto algorithms NEVER trust GE!

XOR gate

2-3 GE

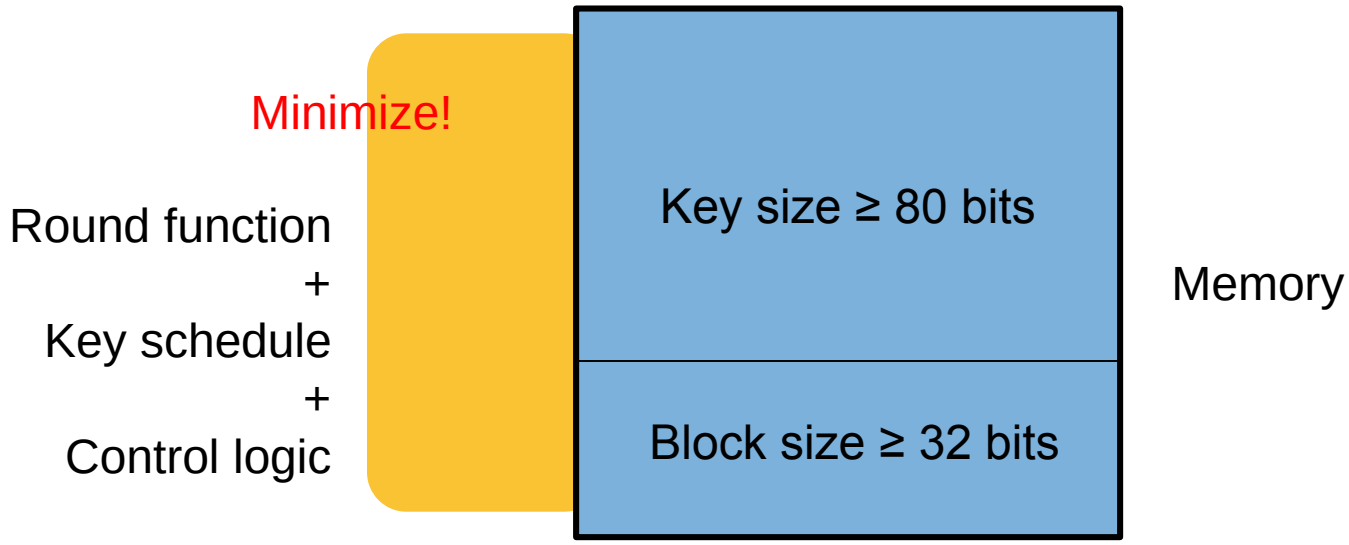
Modern Lightweight Ciphers

< 1000 GE

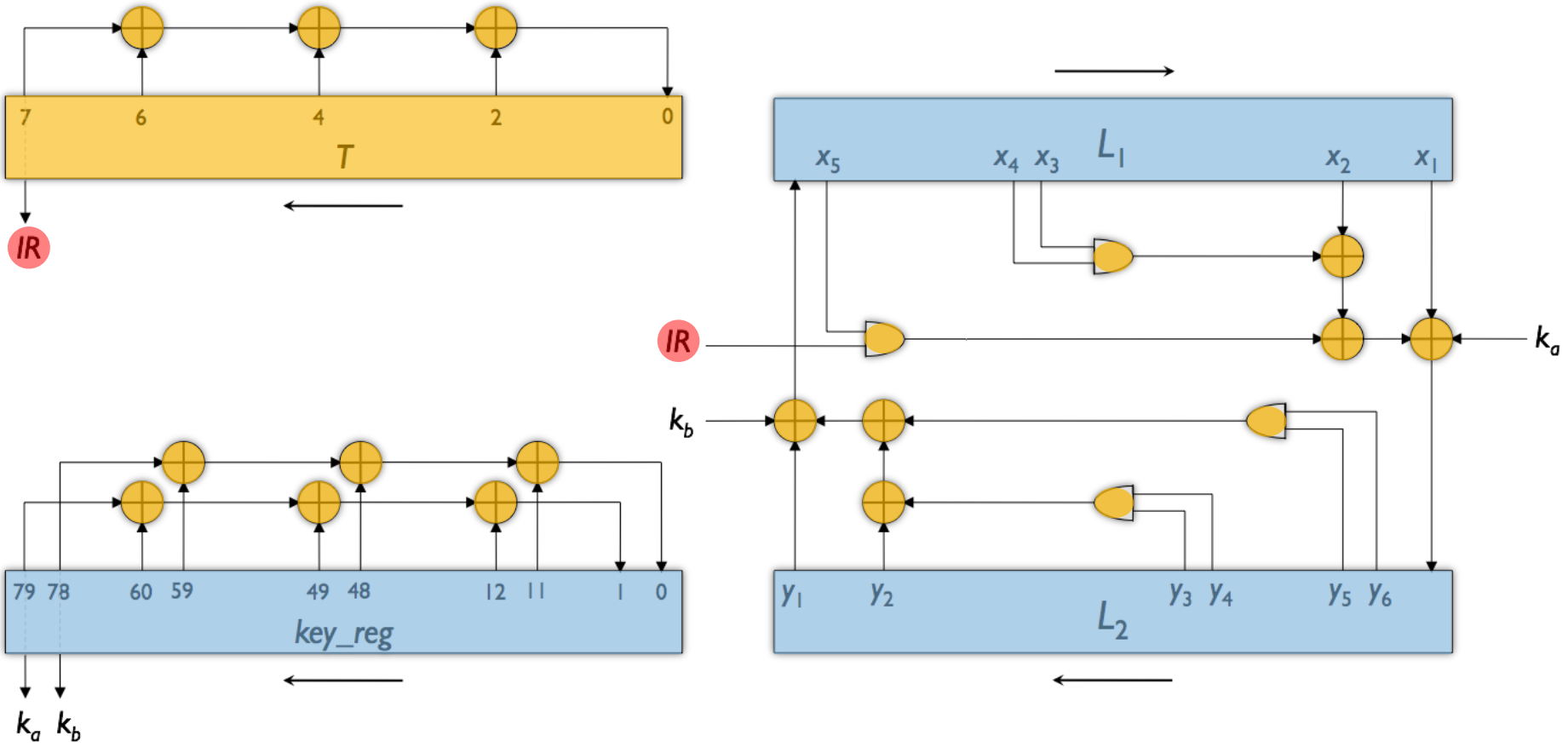
AES (128-bit key, ENC only)

2500 GE

Block Cipher – HW Perspective

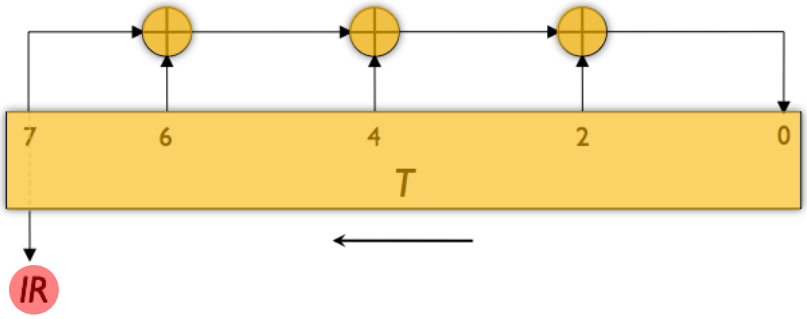


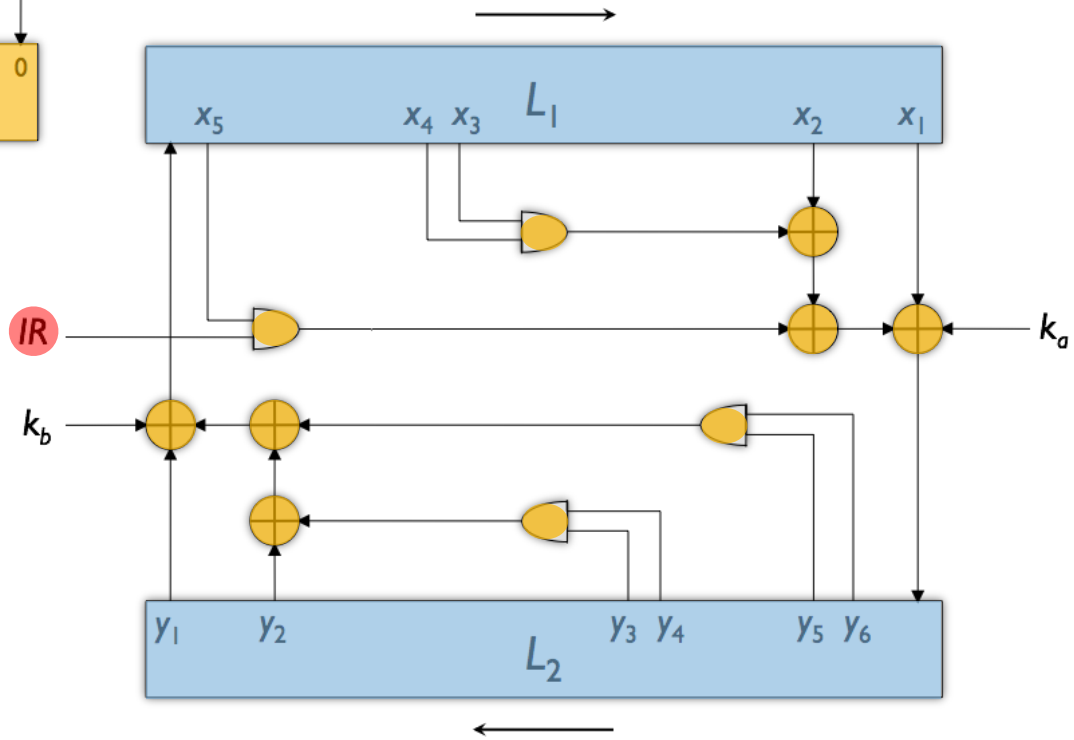
KATAN – The Smallest Block Cipher



KATAN32 = 462 GE

KATAN – The Smallest Block Cipher





Only 508 bits of expanded key!

KATAN32 = 315 GE + 508 bits of ROM

How does KATAN compare to the competition?

It's (one of) the smallest known cipher(s): < 500 GE

But it's not very fast: 254 clock cycles

Still scalable: 3 times faster for negligible area overhead

Fine, but let's really compare it to others!

PRESENT
UMC180
IHP250
AMIS350
Synopsys
~1kGE

KATAN
UMC130
Synopsys
≥ 460 GE

LED
180nm
Synopsys
≥ 700 GE

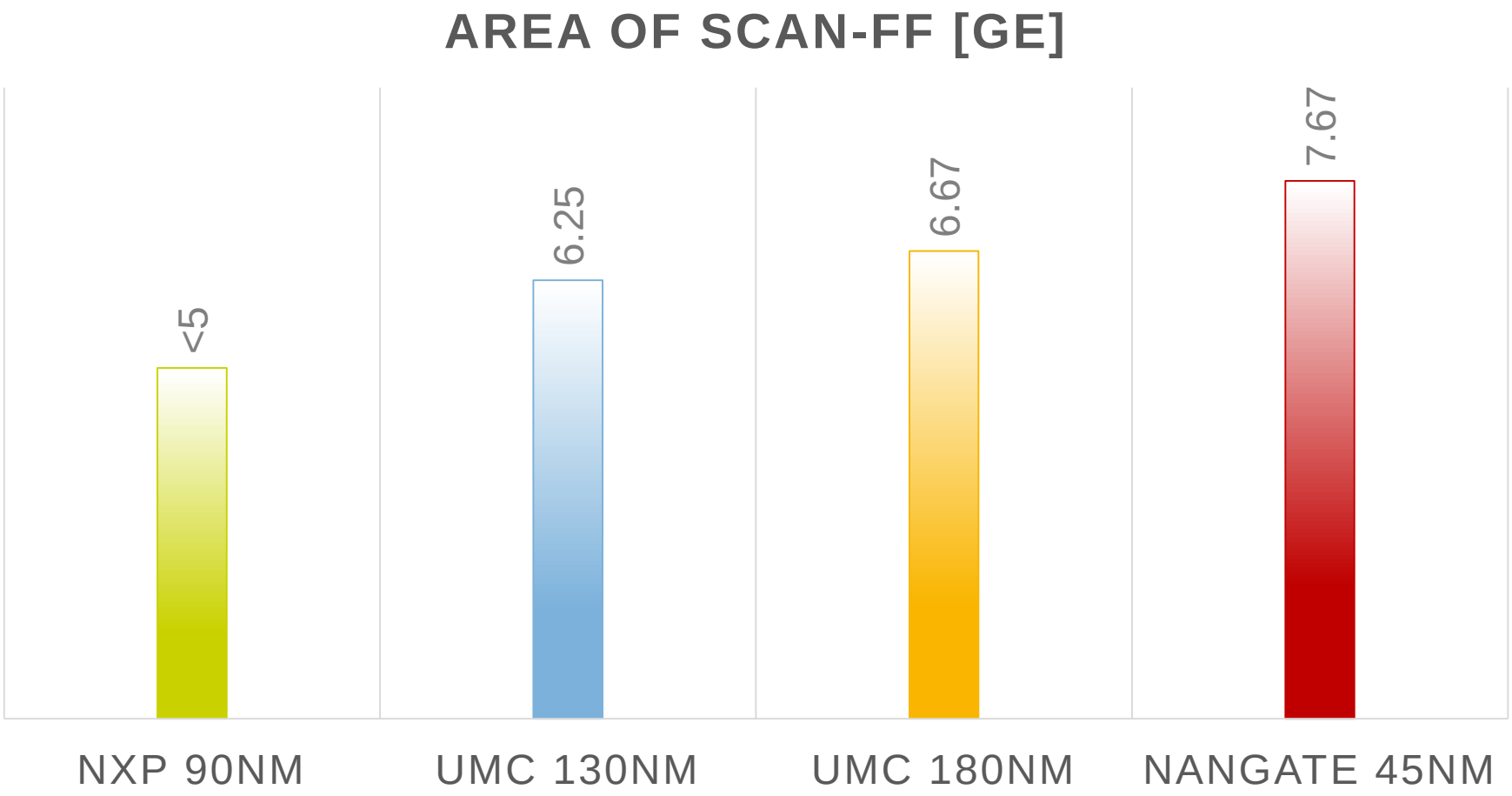
Piccolo
130nm
Synopsys
≥ 700 GE

SIMON
IBM130
Synopsys
≥ 520 GE

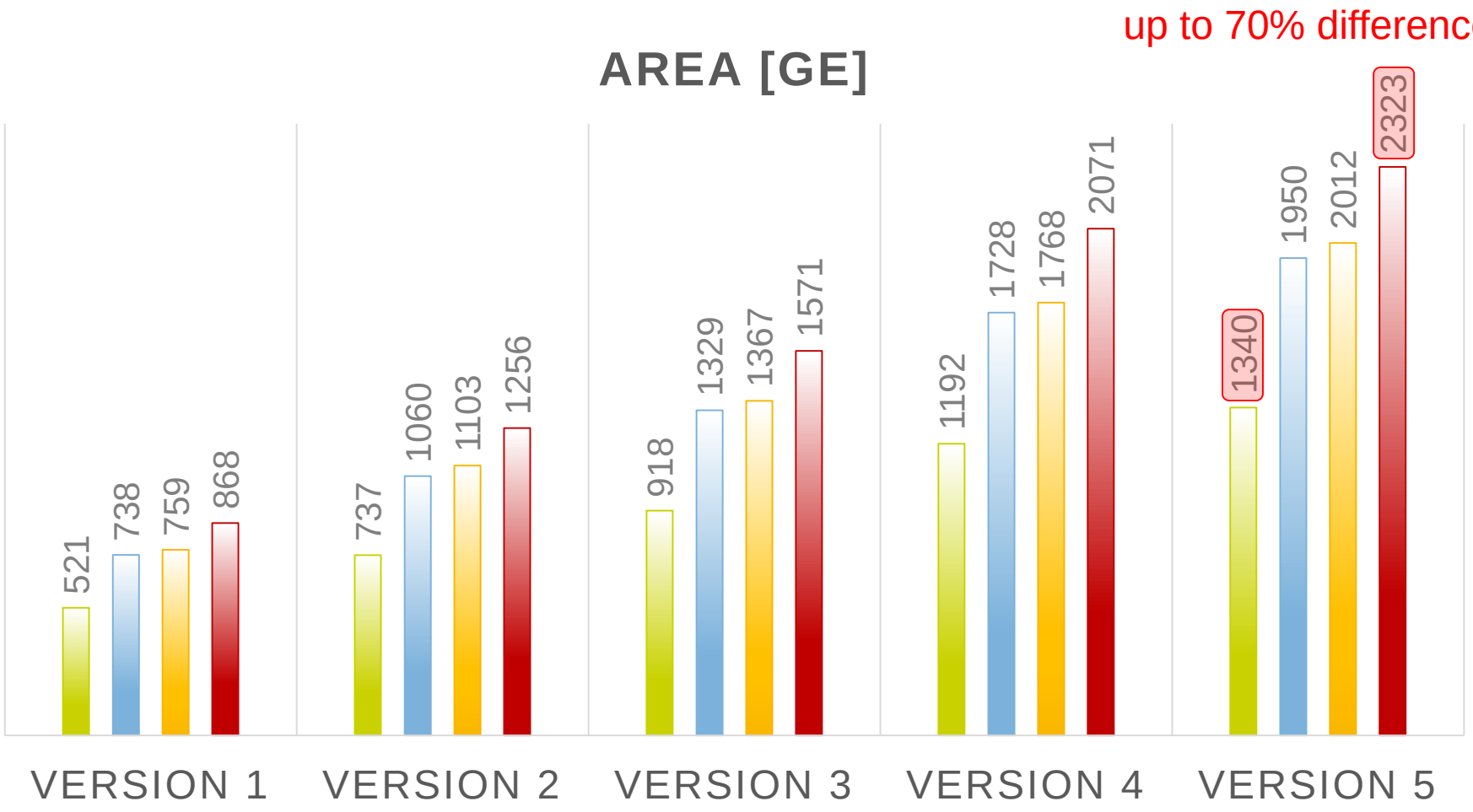
SPECK
IBM130
Synopsys
≥ 580 GE

KLEIN
TSMC180
Synopsys
≥ 1.3 kGE

Memory Elements in different CMOS Technologies



SPONGENT in different CMOS Technologies

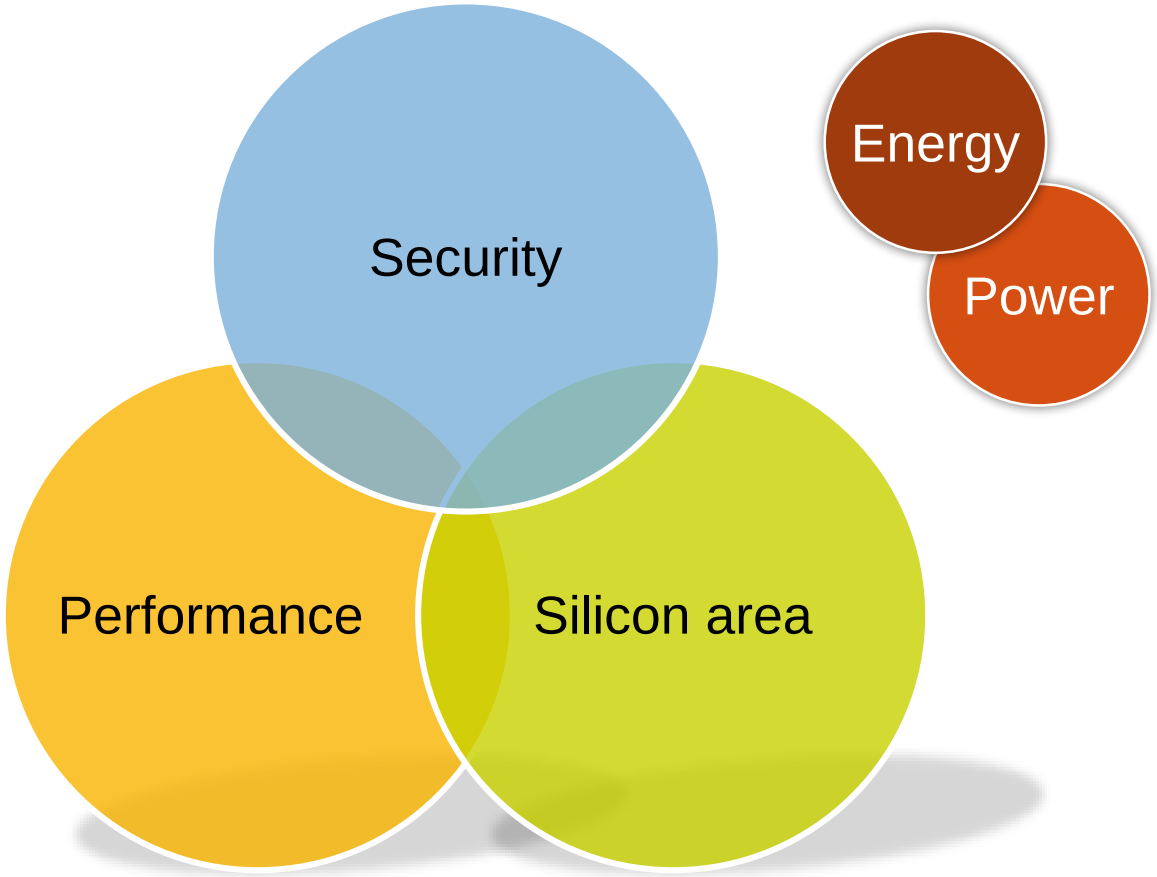


How can we do a fair comparison?

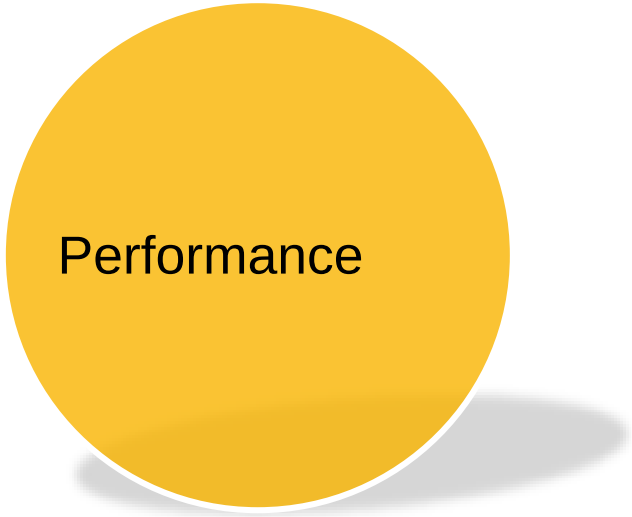
Difficult in practice.
But why not using an open-core library at least?

http://www.nangate.com/

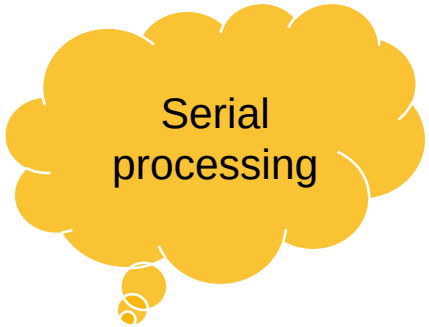
Trade-offs in Crypto HW

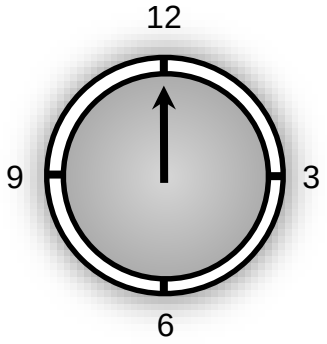


Designing the Fastest Block Cipher



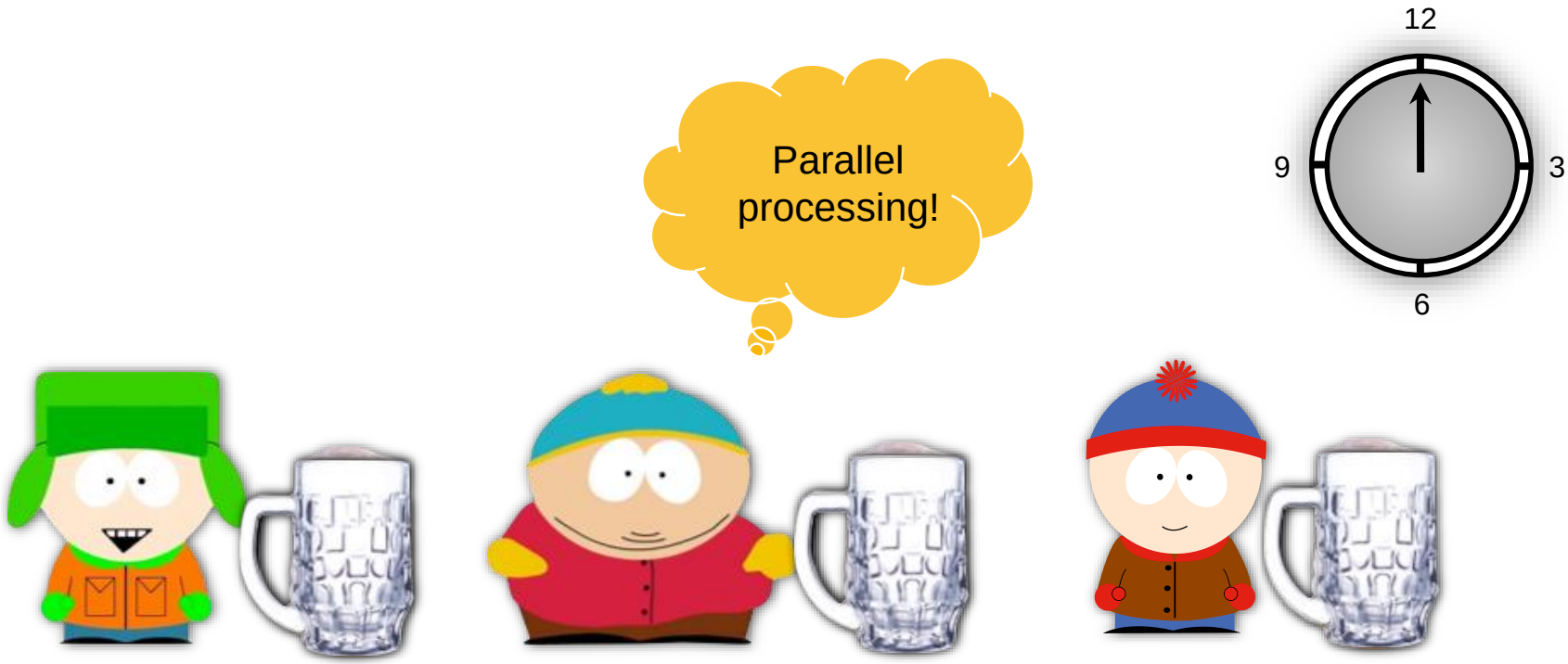
Latency vs Throughput





Latency = 15 s
Throughput = 0.067 beer/s

Latency vs Throughput



Latency = 15 s

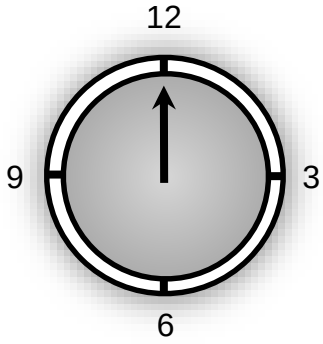
Throughput = 0.2 beer/s

Latency vs Throughput

Latency = 15 s

Throughput = 0.2 beer/s

Latency vs Throughput



bottom-up!

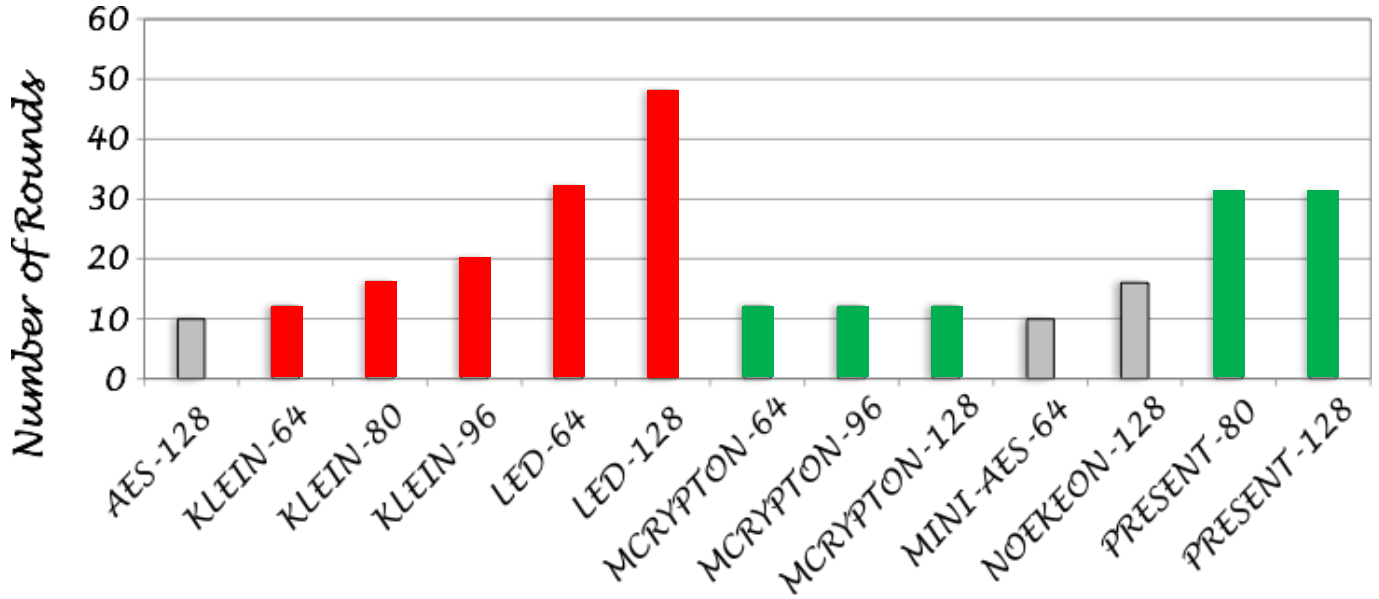
Latency = 5 s

Throughput = 0.2 beer/s

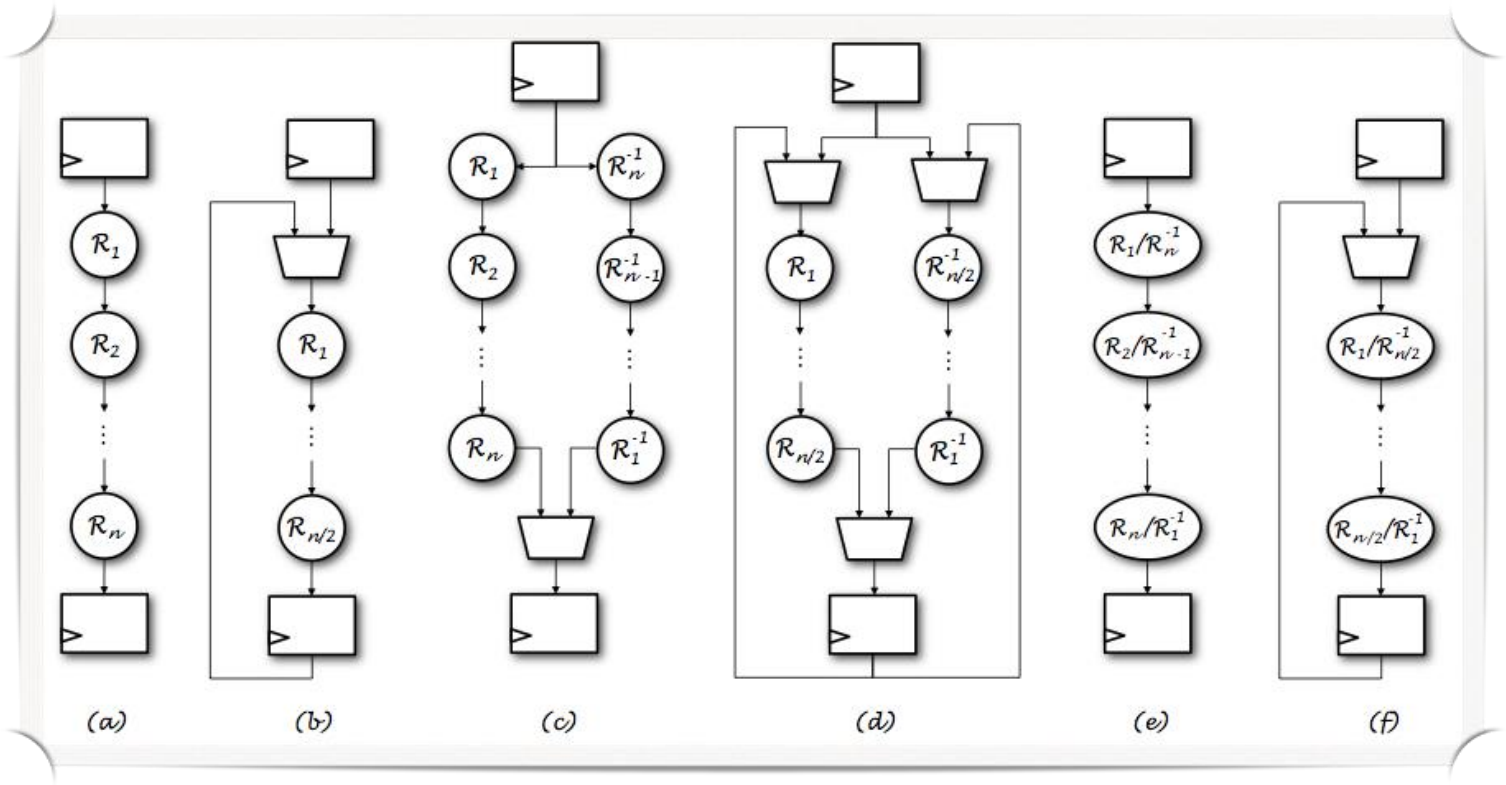
Latency of Existing Ciphers – **Is Lightweight = “Light + Wait”?**

	BLOCK-SIZE	KEY-SIZE	S-BOX	P-LAYER	K-SCHEDULE
AES	128	128	8	MDS	LIGHT
NOEKOEN	128	128	4	BINARY	NO
MINI-AES	64	64	4	MDS	LIGHT
MCRYPTON	64	64, 96, 128	4	BINARY	LIGHT
PRESENT	64	80, 128	4	BIT PERMUTATION	LIGHT
KLEIN	64	64, 80, 96	4	MDS	LIGHT
LED	64	64, 128	4	MDS	NO

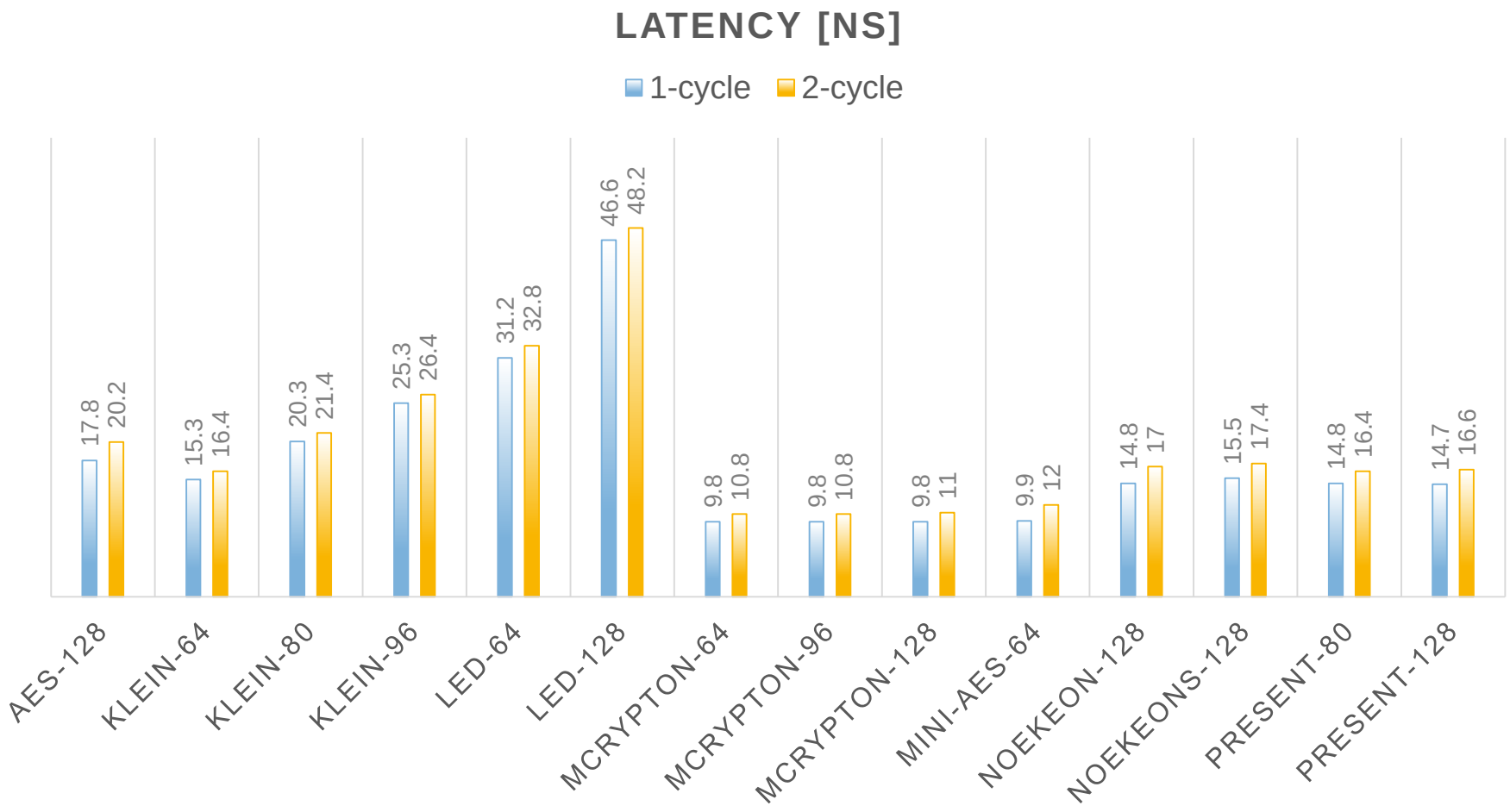
Number of Rounds vs Key Size



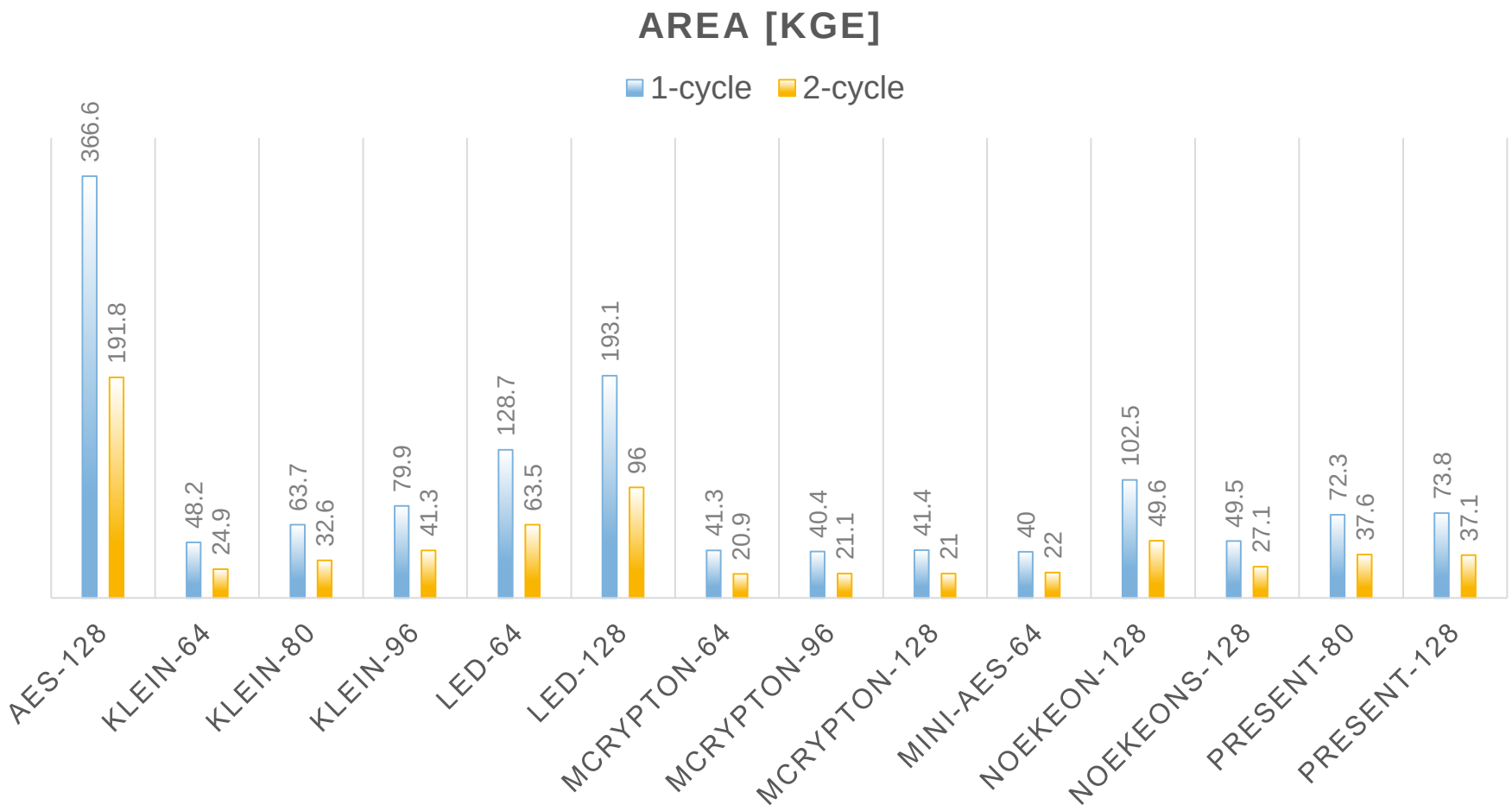
Unrolled HW Architectures



Results – Latency

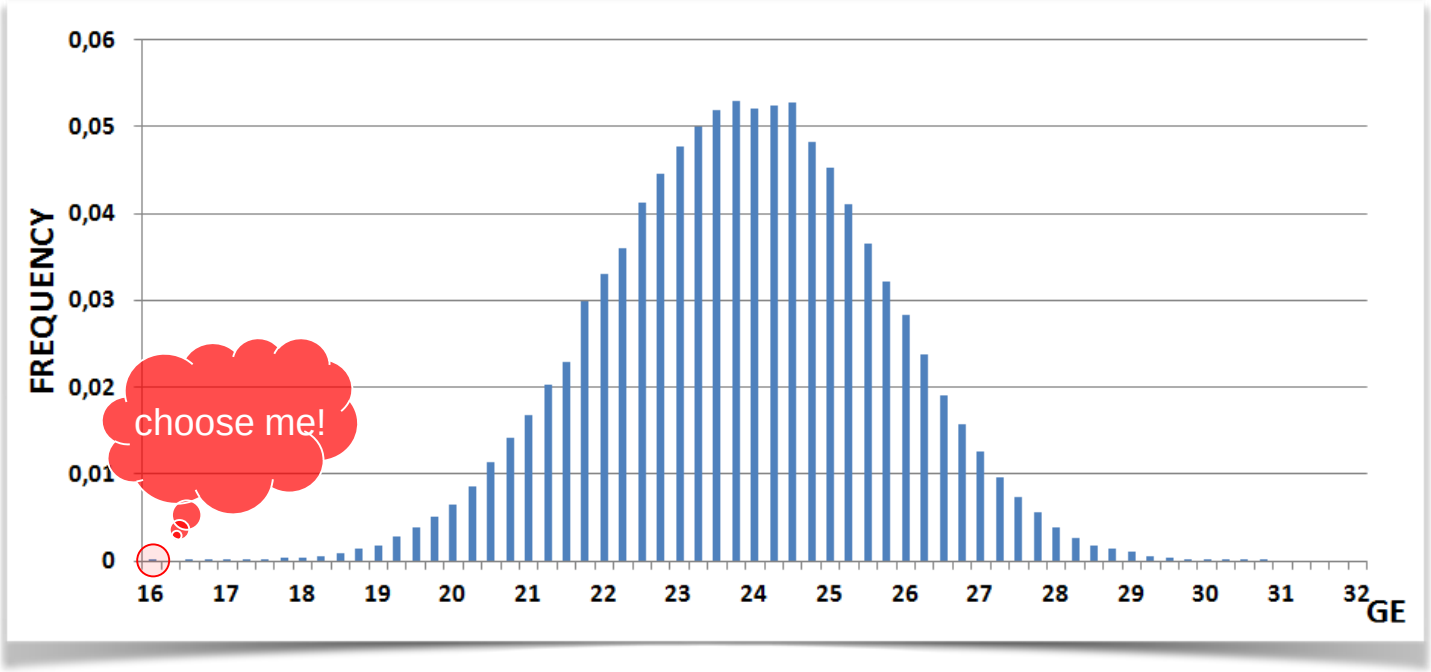


Results – Area



Low Latency Encryption
S-box

- Use small S-boxes (e.g. 5-bit, 4-bit, 3-bit)
- Almost everything follows the normal distribution. So does the S-box!



slide credit:
Gregor Leander

Low Latency Encryption
Number of Rounds

Minimize!

Low Latency Encryption
Round Complexity

- Not too low complexity.

- Reduce the number of rounds at the cost of (slightly) heavier round.

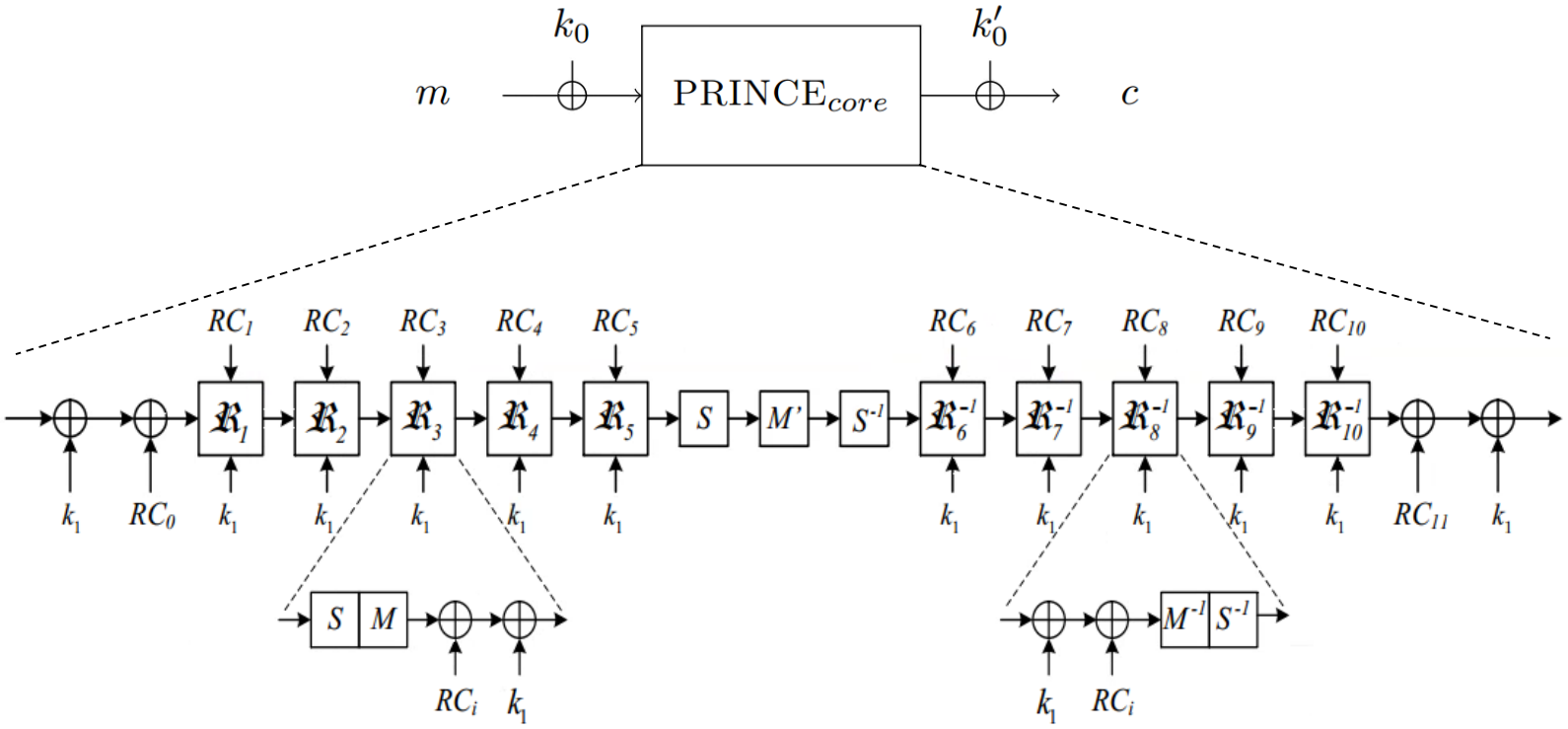
Low Latency Encryption
Key Schedule

- Number of rounds should be independent of the key schedule.
- Use constant addition instead of a key schedule (if possible).

Low Latency Encryption
Encryption vs Decryption

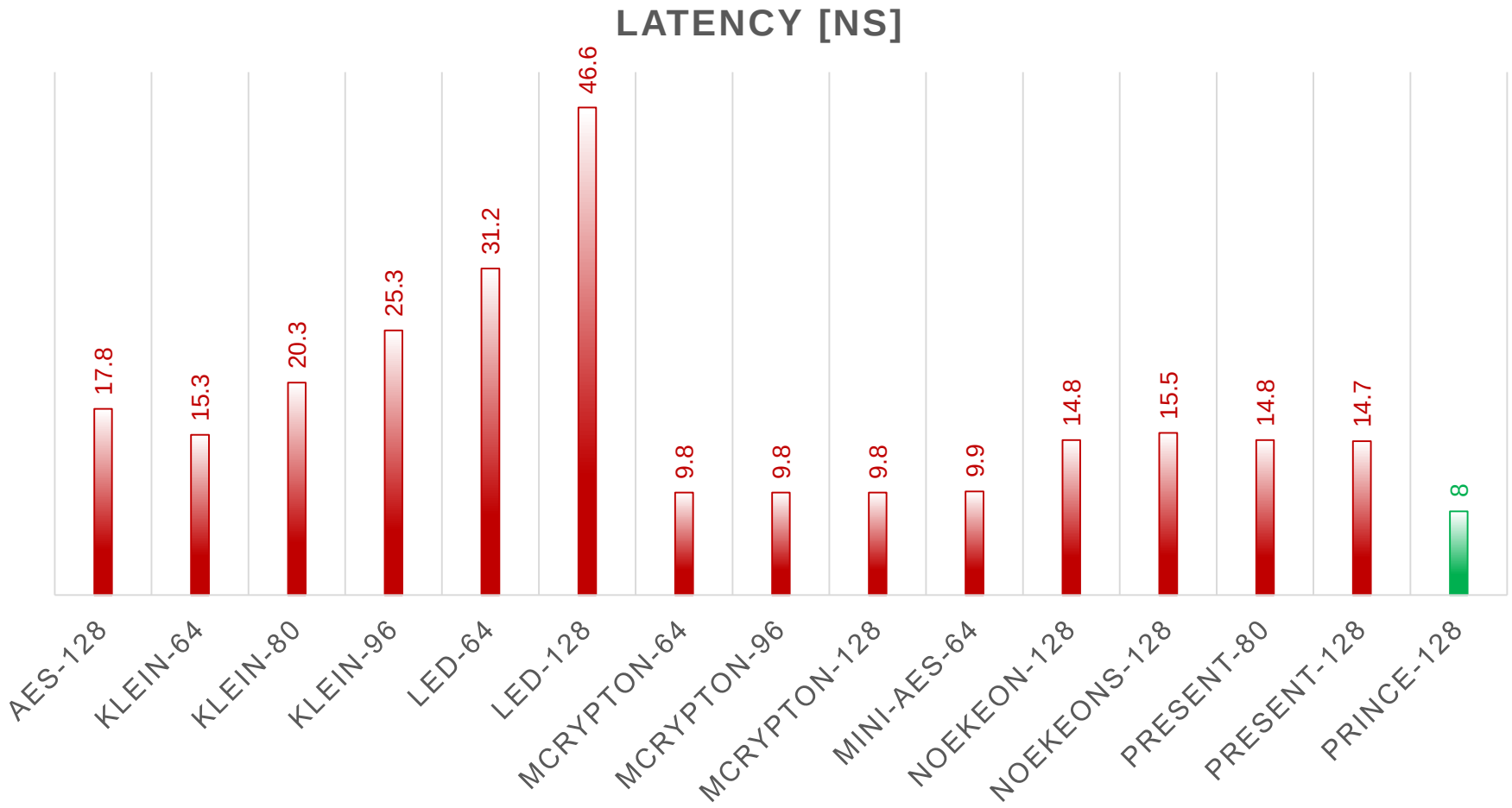
- Use involution where possible: $f\big(f(x)\big) = x$.
- Make Encryption and Decryption procedures similar.
- BUT: think application oriented – sometimes it is beneficial to have asymmetric constructions.

Low Latency Encryption
Meet PRINCE

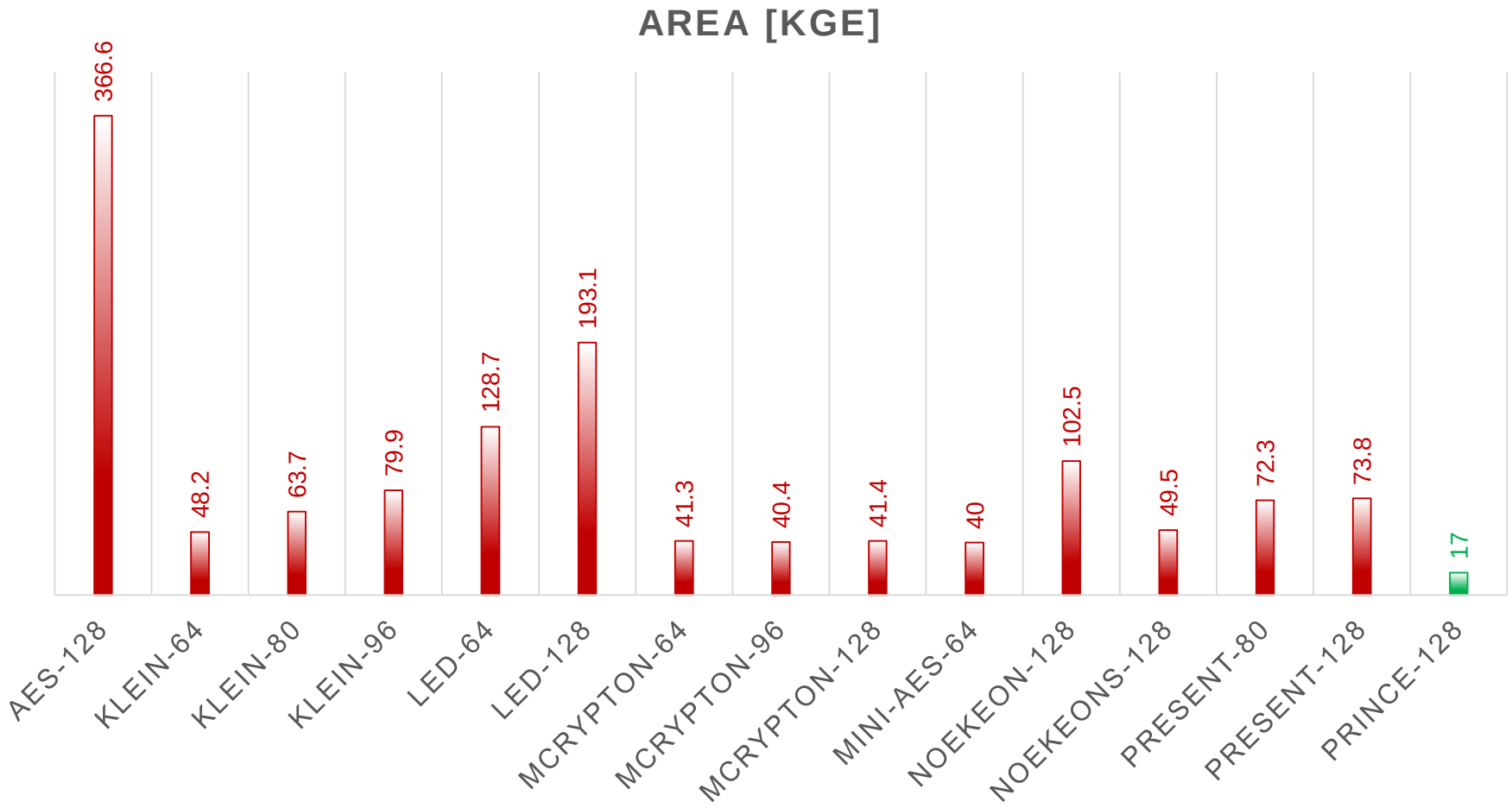


α-reflection property: $D_{(k_0||k_0'||k_1)}(\cdot) = E_{(k_0'||k_0||k_1 \oplus \alpha)}(\cdot)$

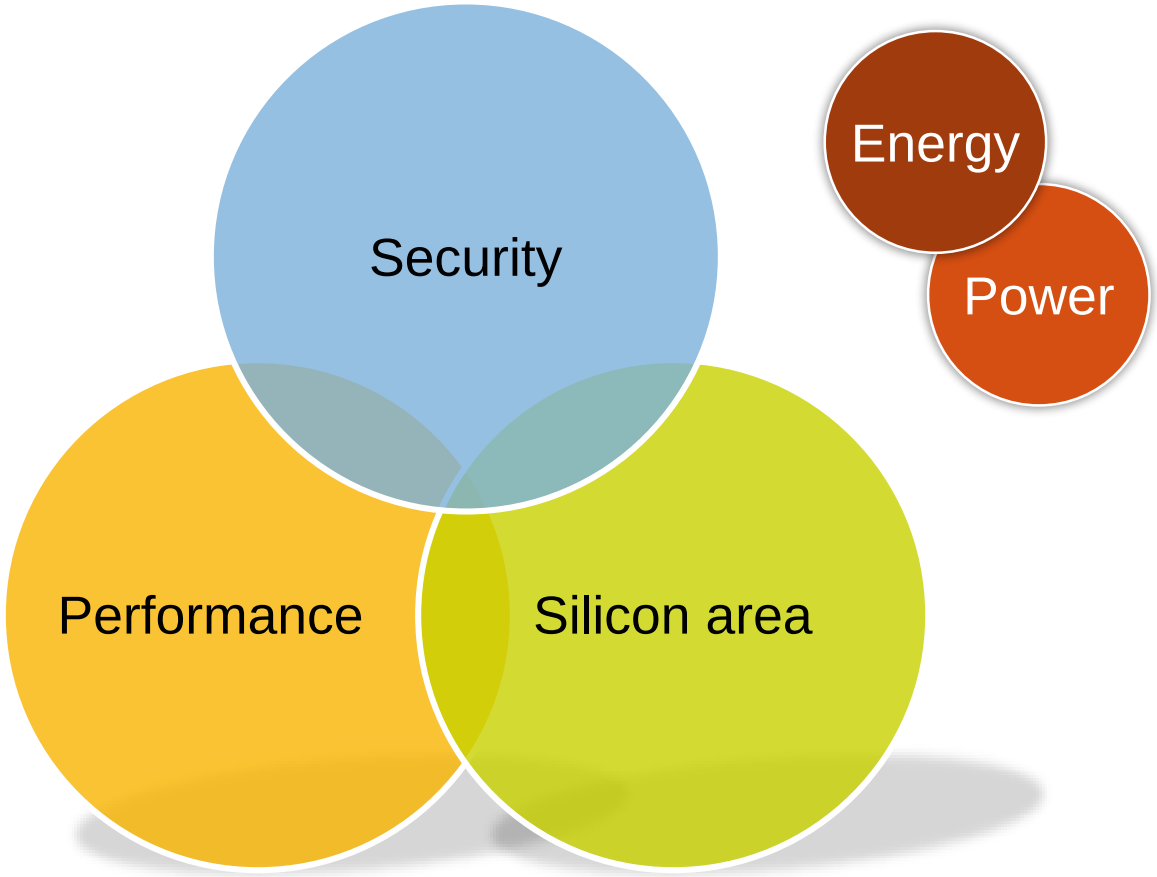
Low Latency Encryption
Meet PRINCE



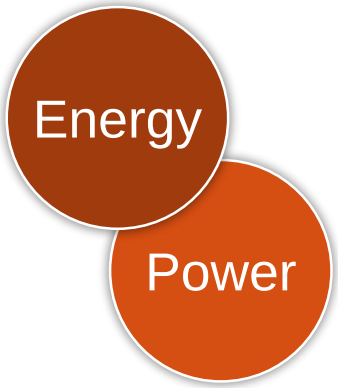
Low Latency Encryption
Meet PRINCE



Trade-offs in Crypto HW



Power vs Energy



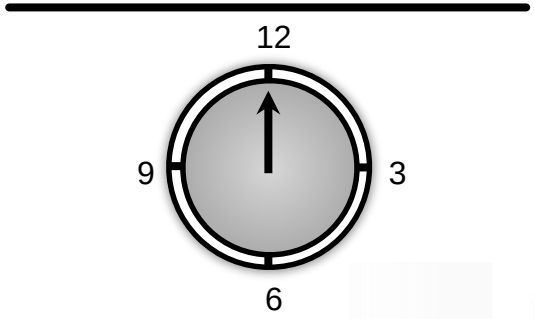
Power vs Energy

Energy

=

Power

=



Every mW matters!

Total number of mobile devices in 2015 = 8.6 billion*

Average (regular) power consumption of a smartphone = 160 mW**

Total energy spent = €2.5 billion* a year!**

* Mobile Statistics Report 2014-2018, The Radicati Group Inc.

** An Analysis of Power Consumption in a Smartphone, A Carroll, G Heiser, USENIX 2010.

*** average electricity price in 2014 in EU was €0.208 per kWh.

Reducing Power Consumption

$$P_{tot} = P_{switching} + P_{leakage}$$

$$P_{switching} \approx C_{eff} \cdot V_{DD}^2 \cdot f_{clk} \cdot sw$$

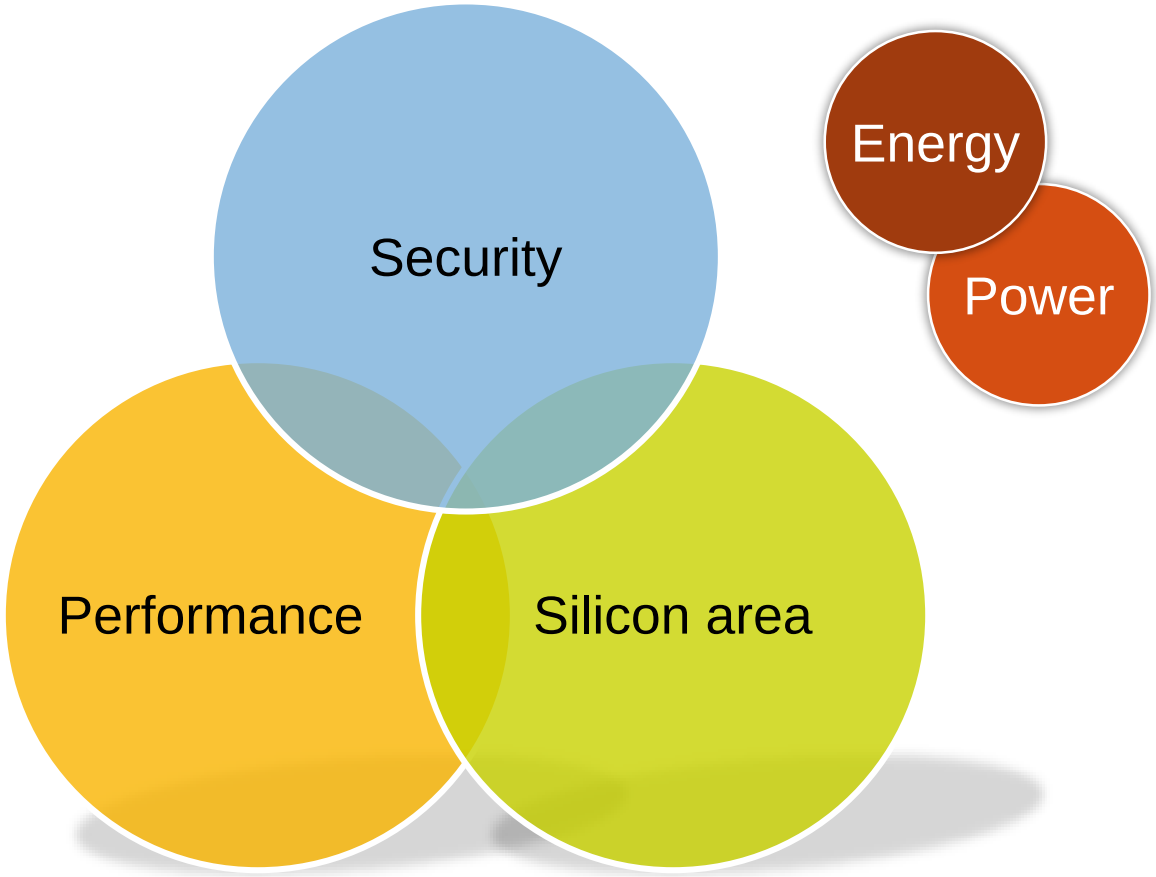
- Reduce circuit area (e.g. serializing): $C_{eff} \downarrow$
- Reduce switching activity (e.g. clock gating): $sw \downarrow$
- Move to smaller CMOS technologies: $C_{eff} \downarrow, V_{DD} \downarrow$, but $P_{leakage} \uparrow$
- Reduce the operating clock frequency: $f_{clk} \downarrow$

Known Throughput Optimization Techniques and their Impact* on Power and Energy

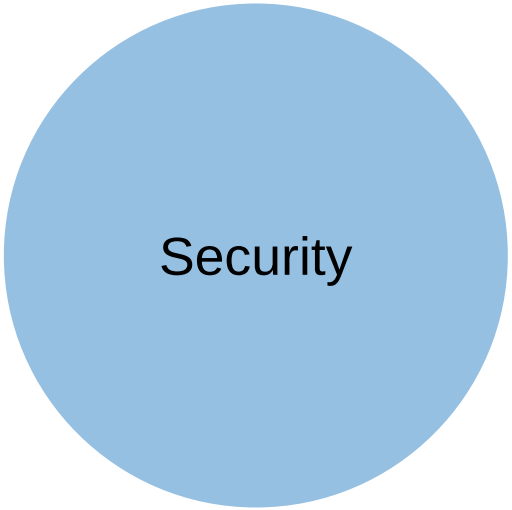
	serialization	parallelism	unrolling	pipelining
Power	+	−	− +	− +
Energy	−	+	+ −	+ −

* in the context of symmetric block cipher design

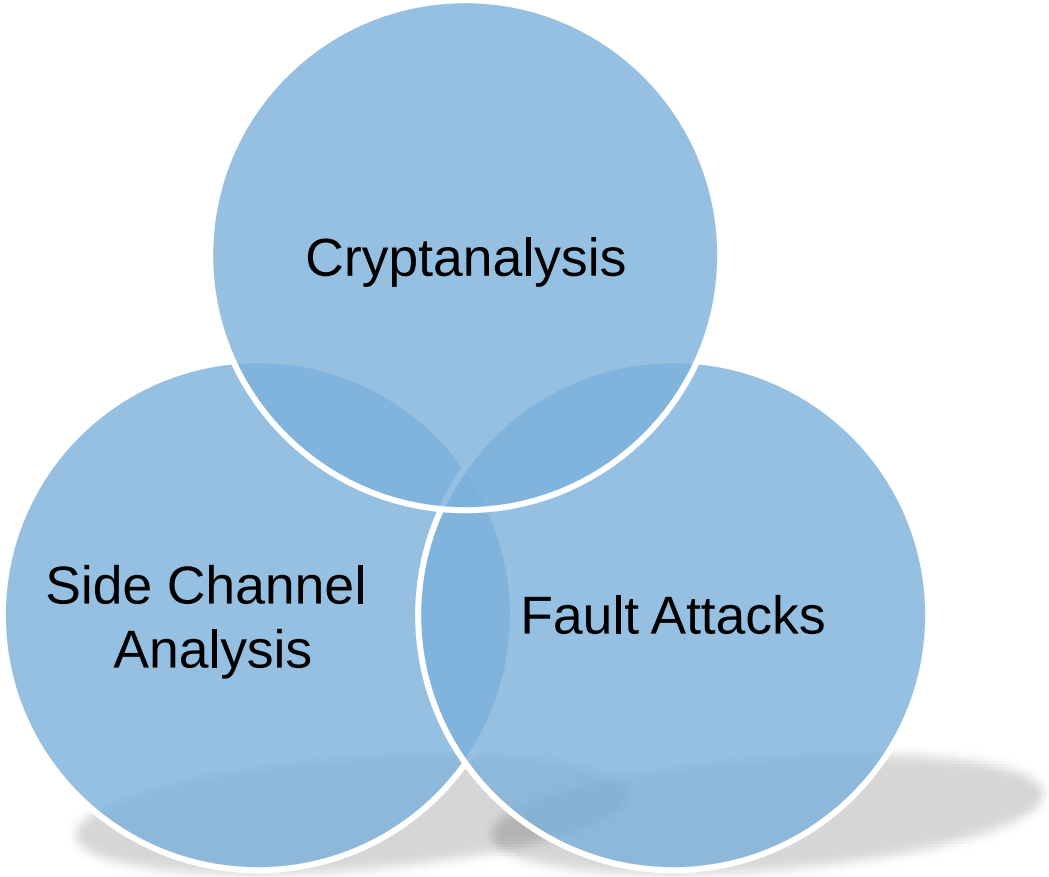
Trade-offs in Crypto HW



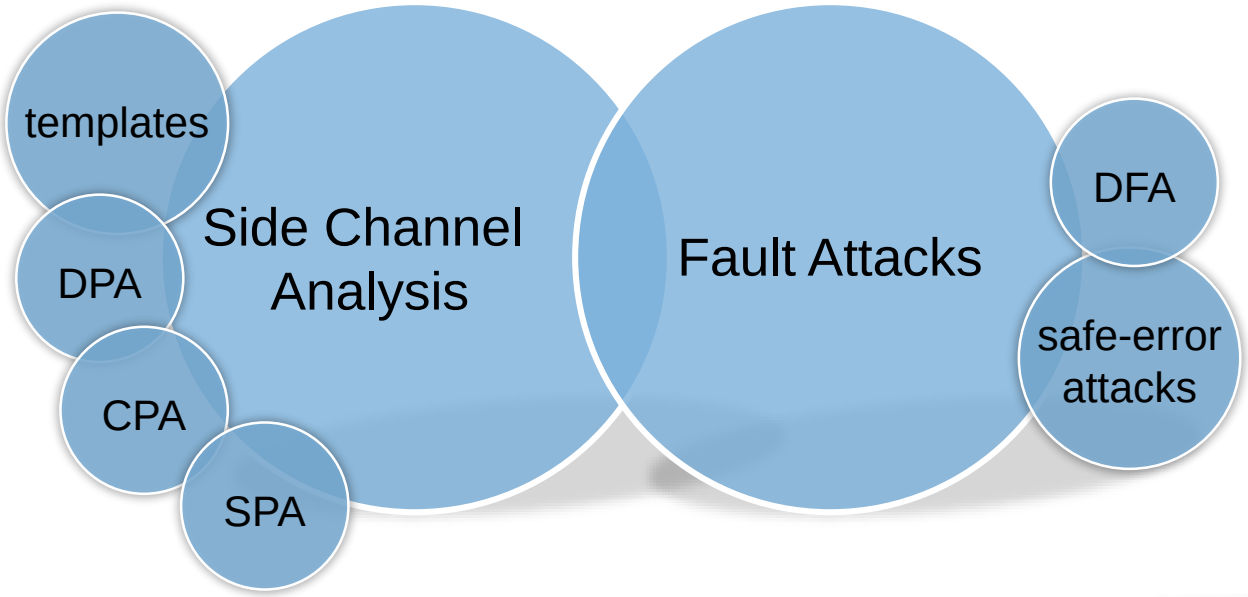
Designing the Most Secure Block Cipher



Designing the Most Secure Block Cipher

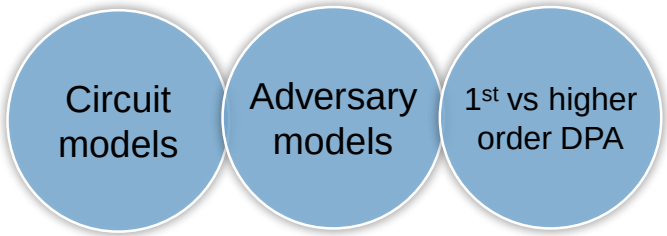


Designing the Most Secure Block Cipher



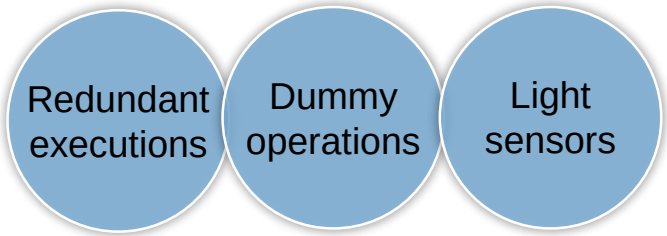
Challenges with SCA Countermeasures

INCOMPLETE MODELS



Challenges with FA Countermeasures

LACK OF CREATIVITY



THANK YOU!

Thanks to the teams of
KATAN, SPONGENT, PRINCE, FIDES

SECURE CONNECTIONS
FOR A SMARTER WORLD