Low-Latency Encryption

- Is "Lightweight = Light + Wait?" -

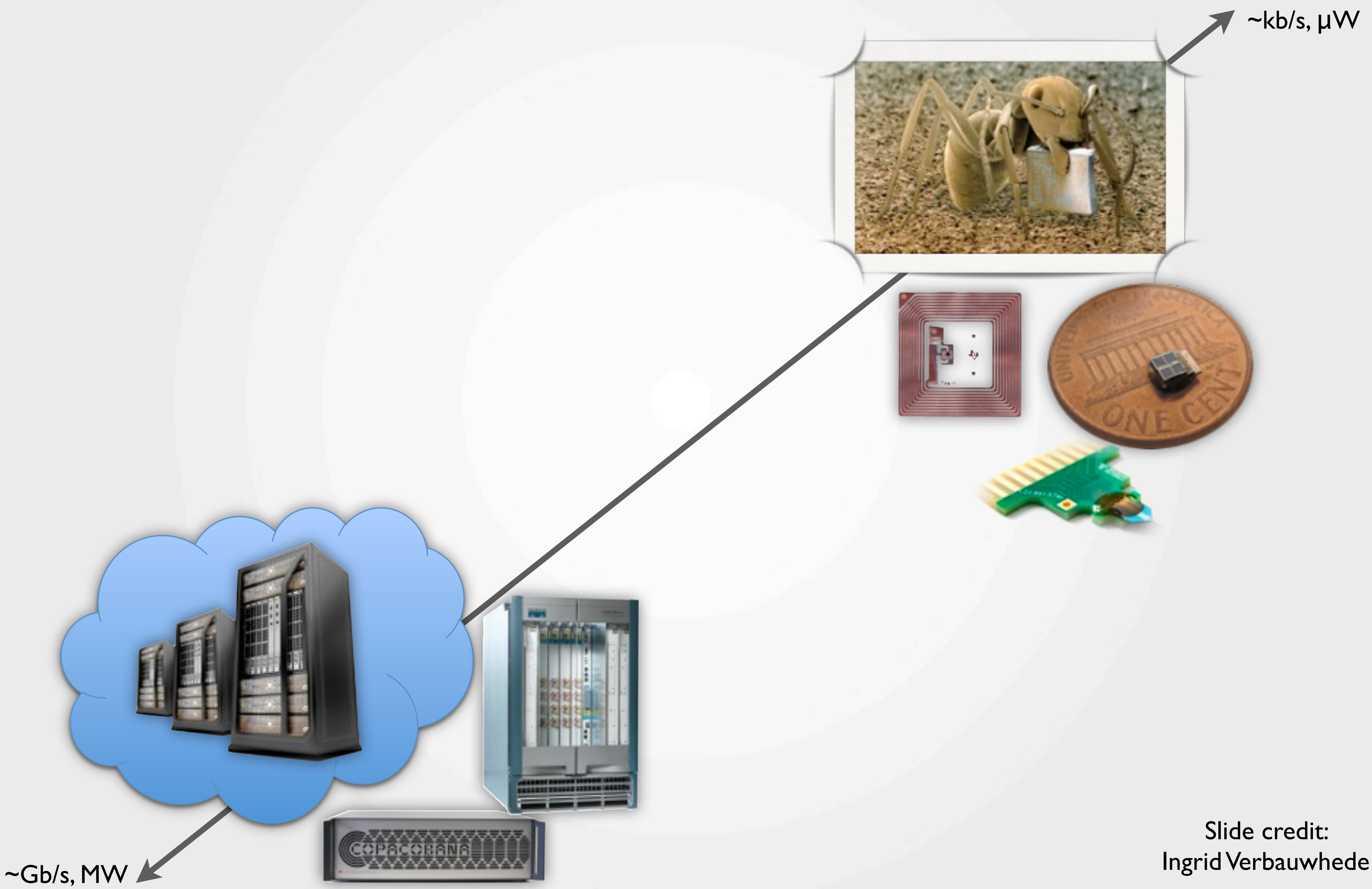
Miroslav Knežević, Ventzislav Nikov, Peter Rombouts

CHES 2012, Leuven, Belgium, September 10-12, 2012

Digital Continuum

Slide credit:
Ingrid Verbauwhede

Digital Continuum



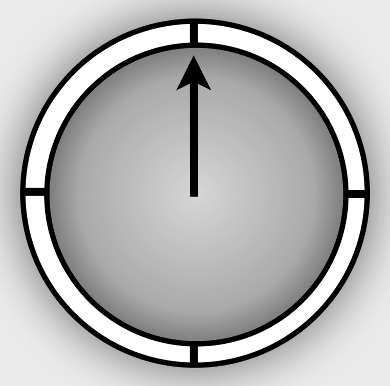
Slide credit:
Ingrid Verbauwhede

Digital Continuum

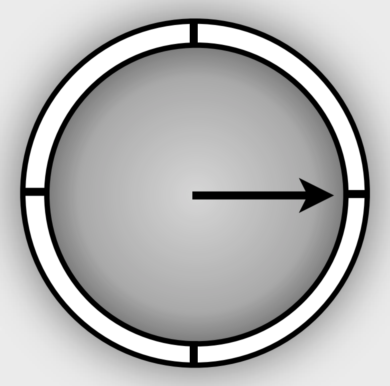
Slide credit:
Ingrid Verbauwhede

Latency vs Throughput

Latency vs Throughput

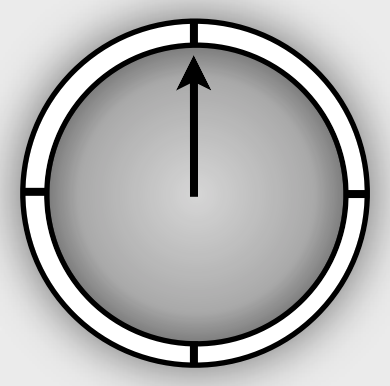


Latency vs Throughput



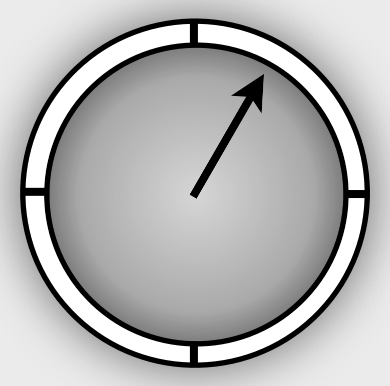
Latency = 15 s
Throughput = 0.067 beer/s

Latency vs Throughput



Ad Fundum

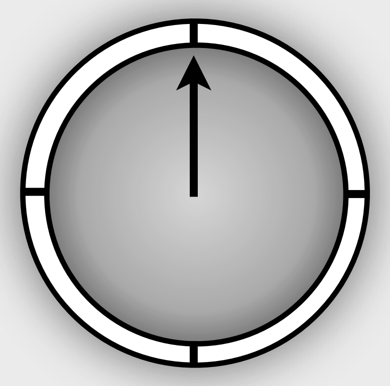
Latency vs Throughput



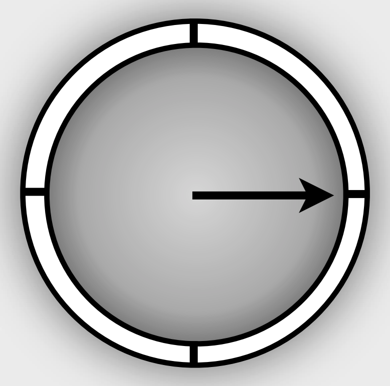
Ad Fundum

Latency = 5 s
Throughput = 0.2 beer/s

Latency vs Throughput



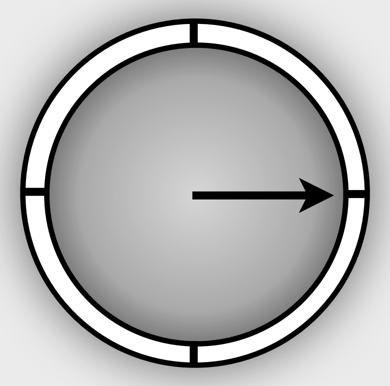
Latency vs Throughput



Latency = 15 s

Throughput = 0.2 beer/s

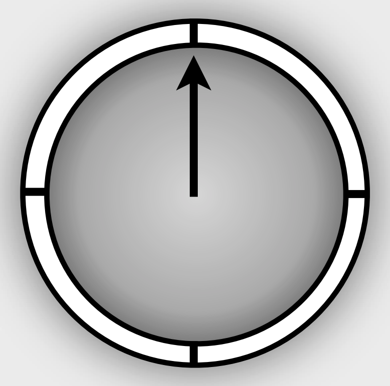
Latency vs Throughput



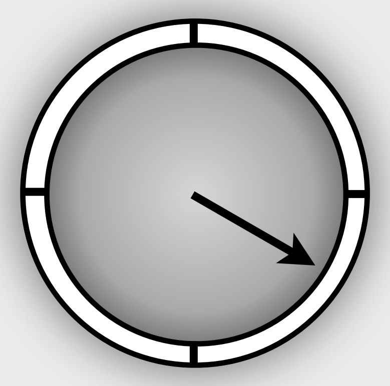
Latency = 15 s
Throughput = 0.2 beer/s

Parallel Processing

Latency vs Throughput



Latency vs Throughput

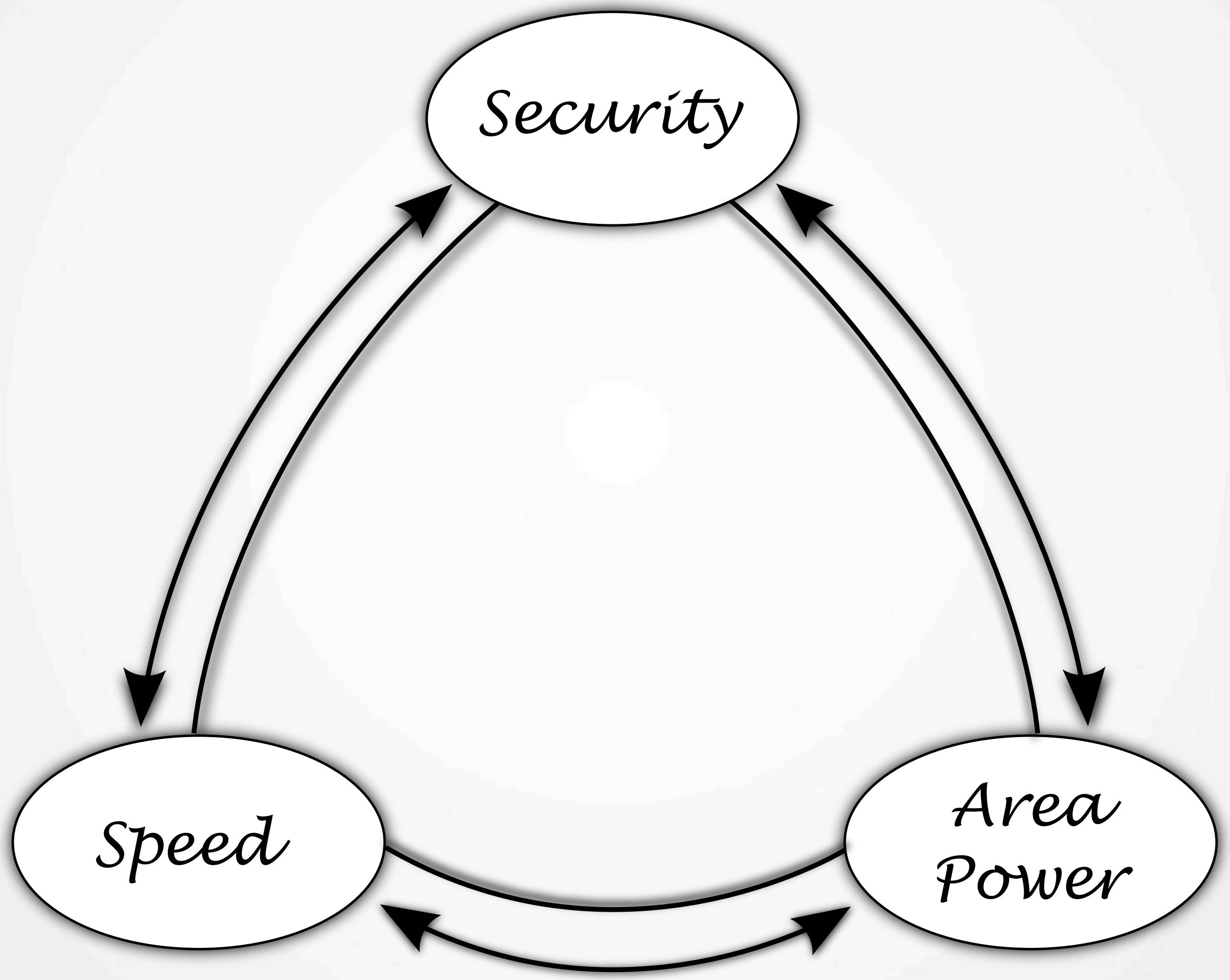


Latency = 15 s

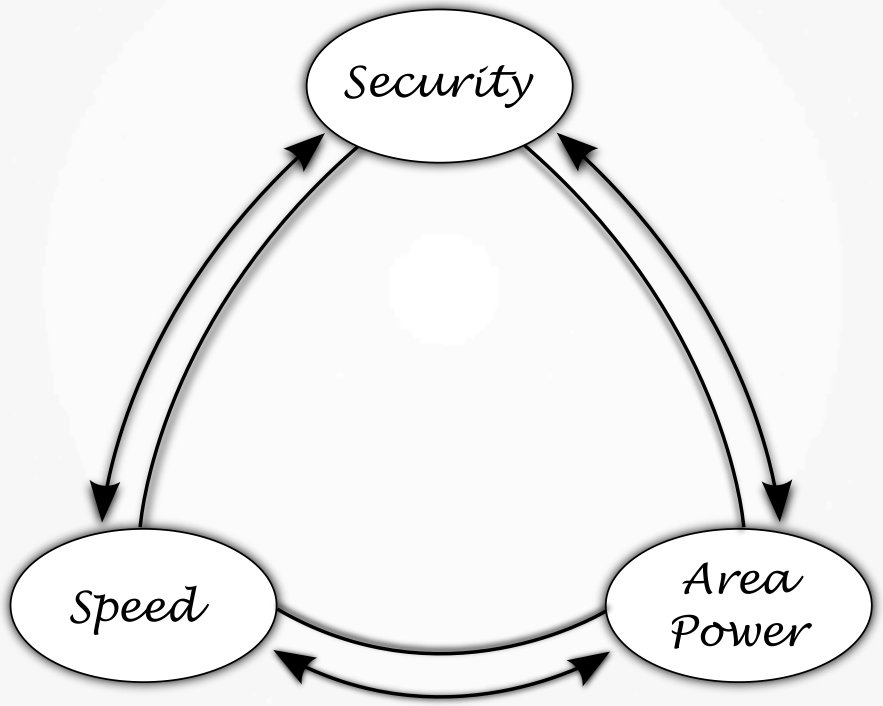
Throughput = 0.2 beer/s

Pipelining

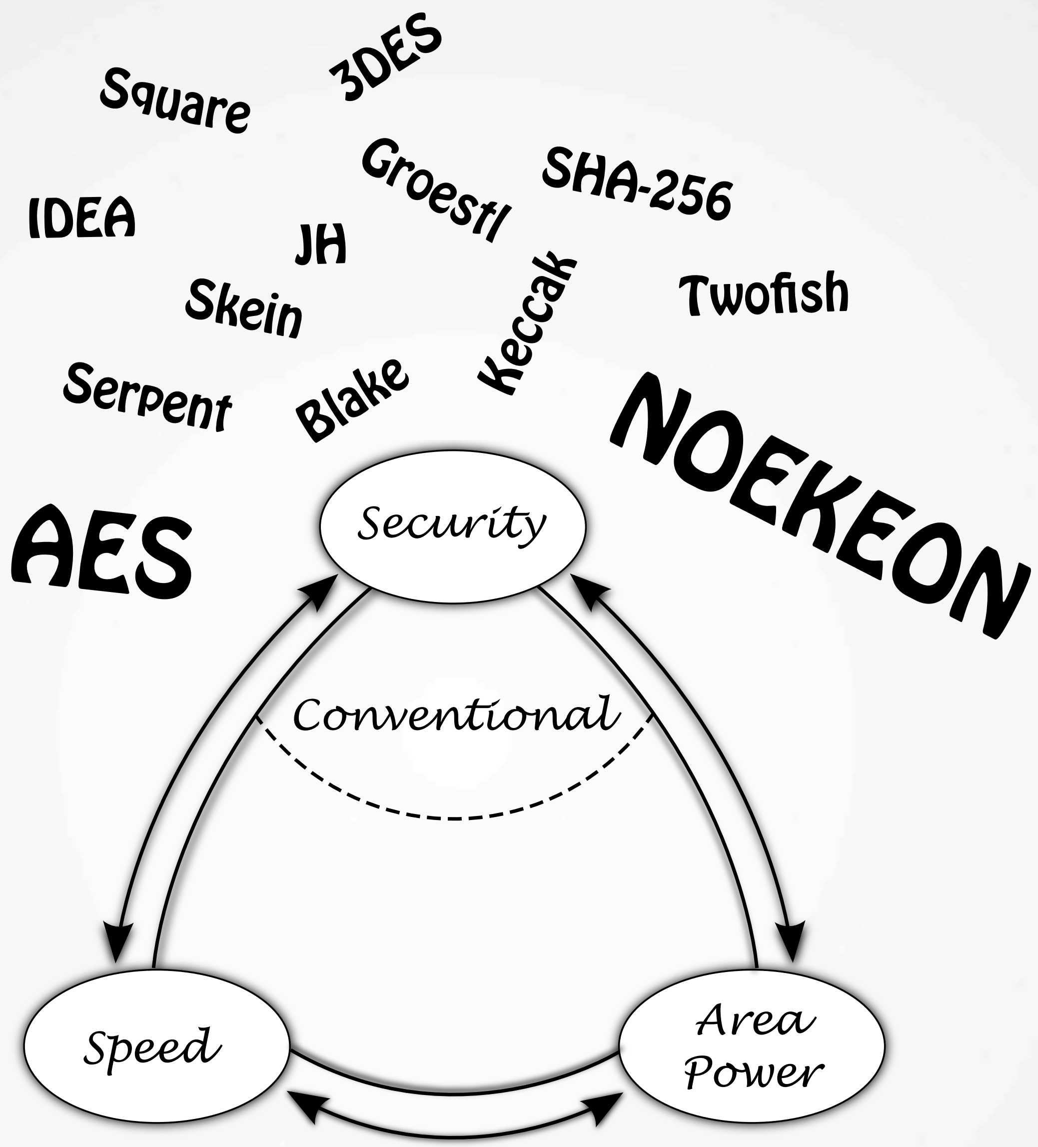
Typical Trade-offs in Crypto



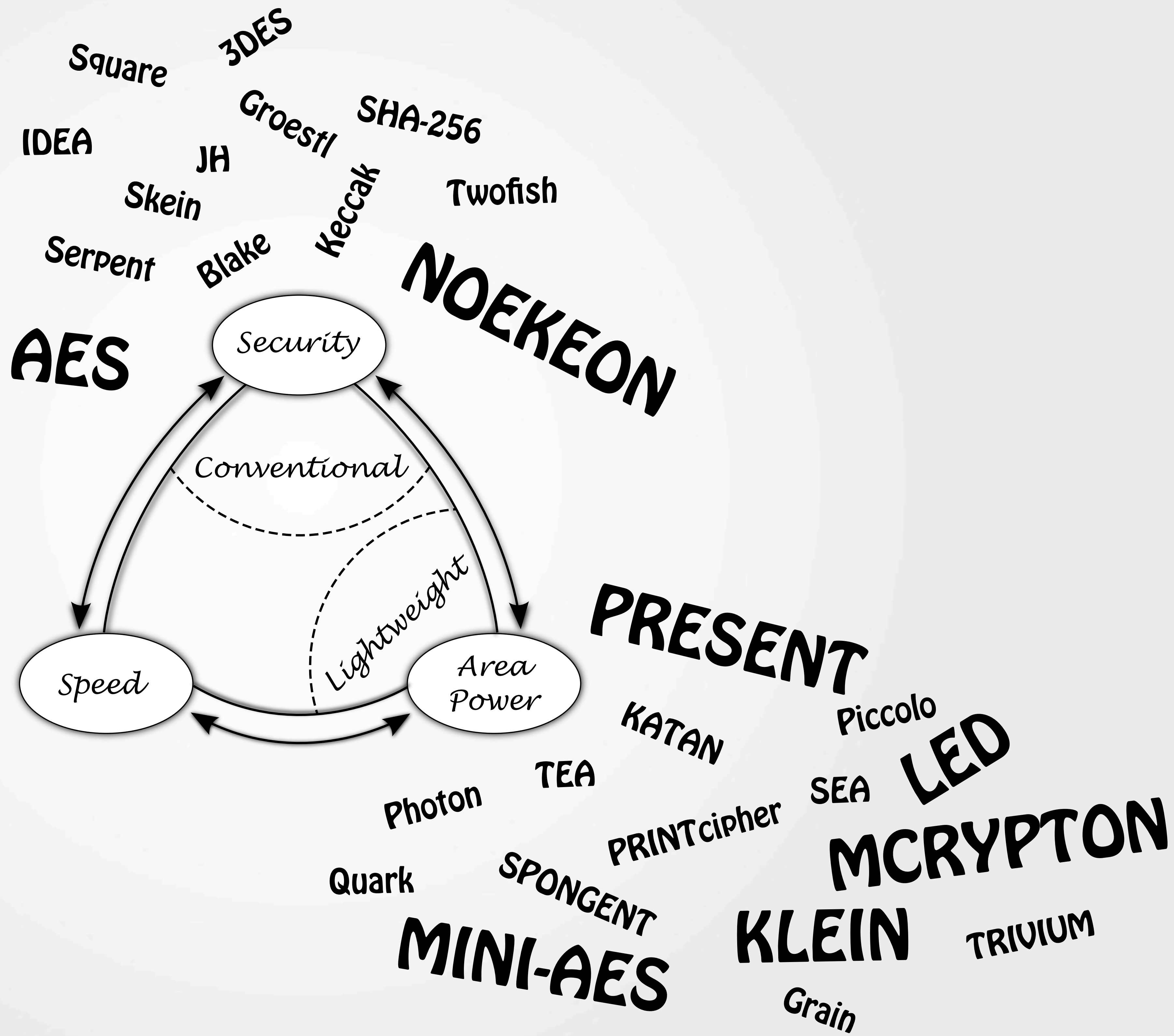
Typical Trade-offs in Crypto



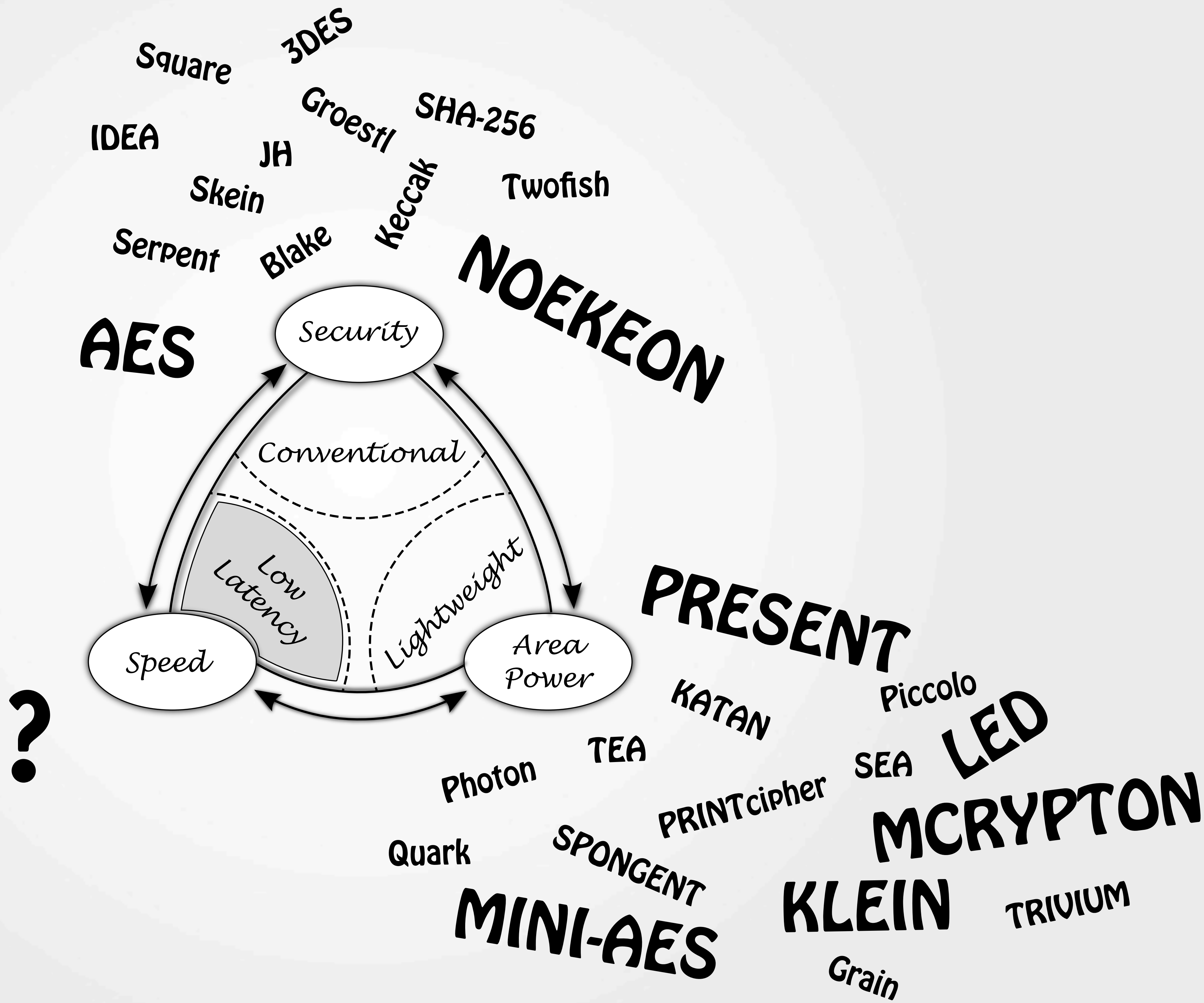
Typical Trade-offs in Crypto



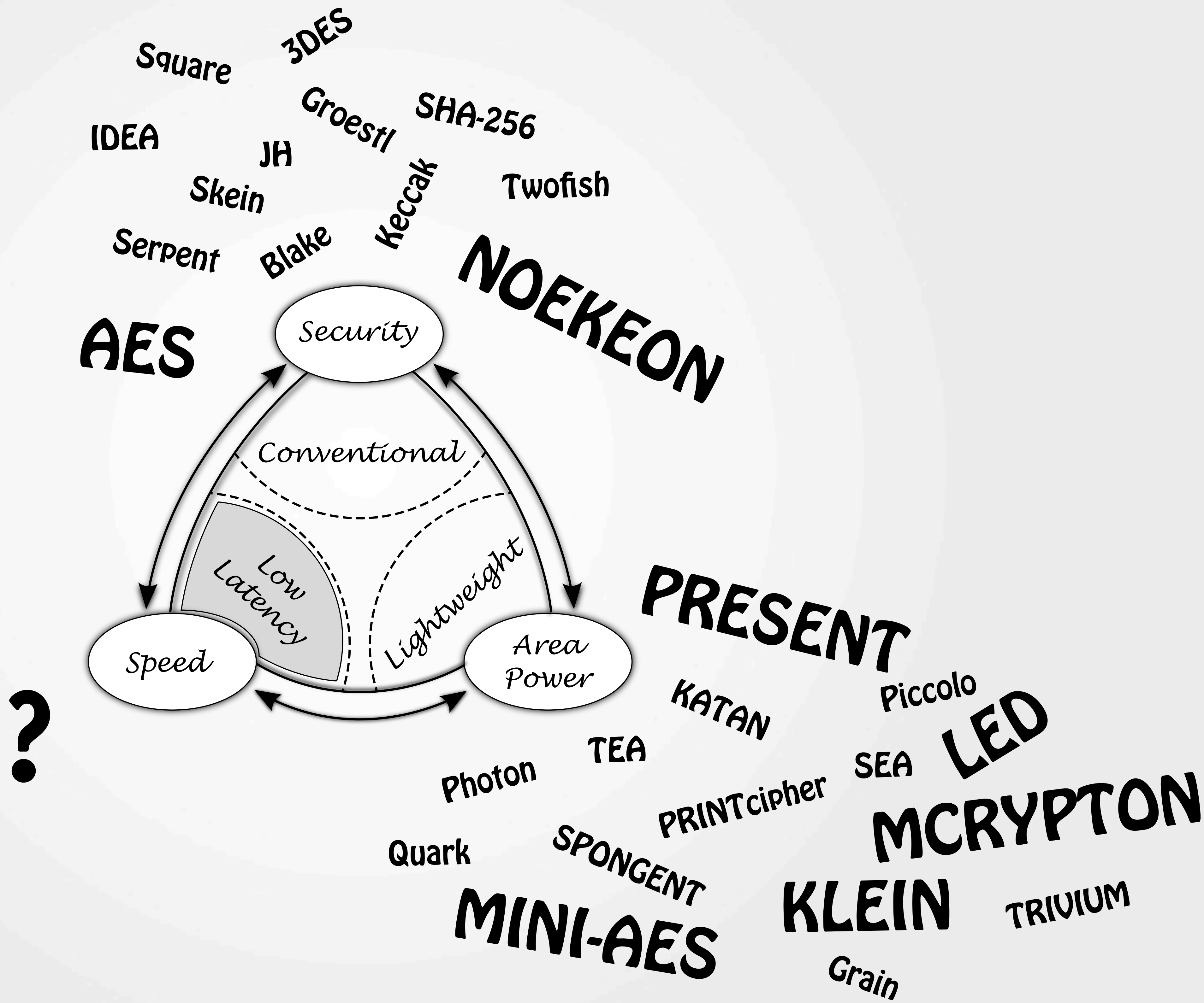
Typical Trade-offs in Crypto



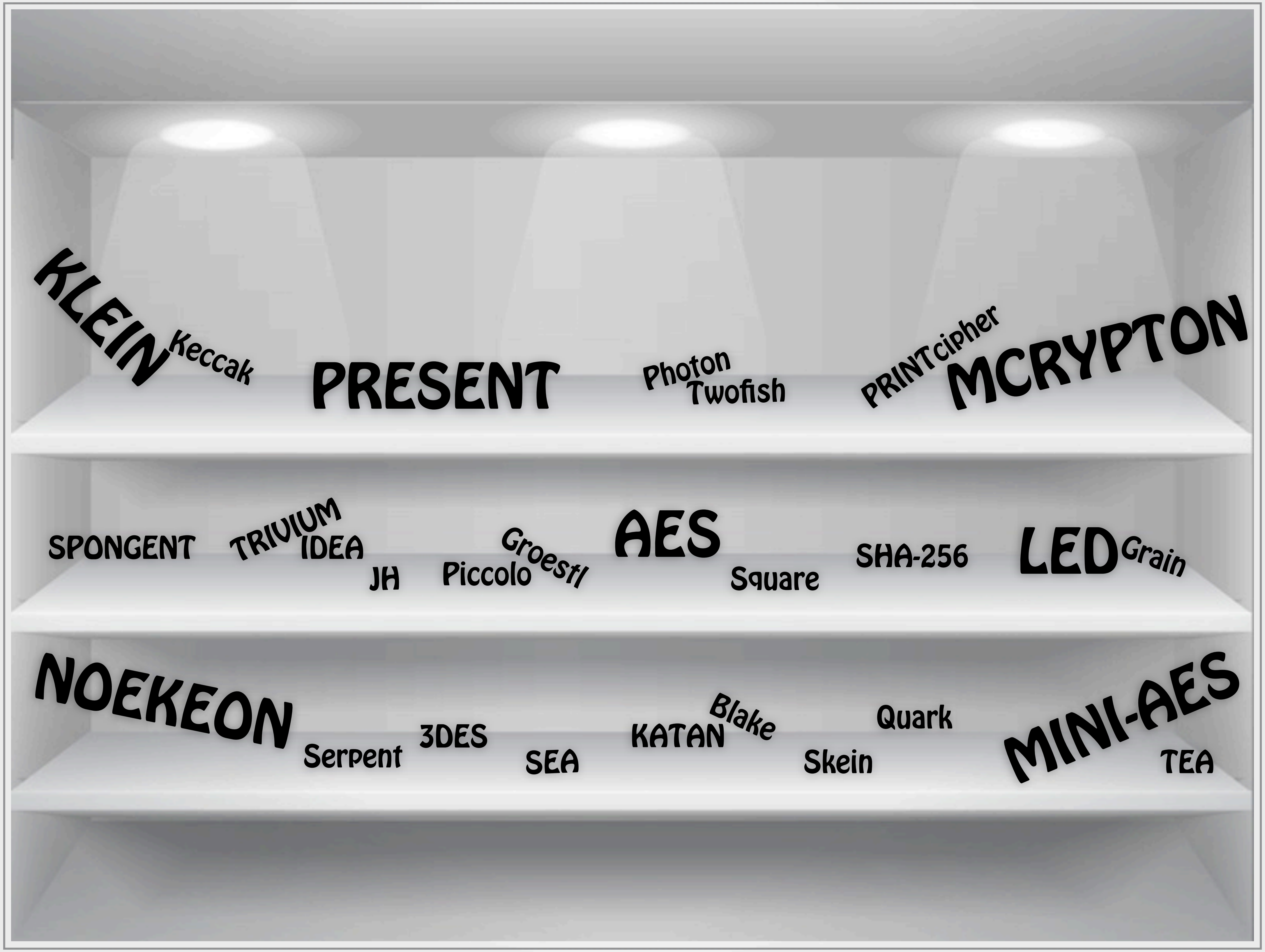
Typical Trade-offs in Crypto



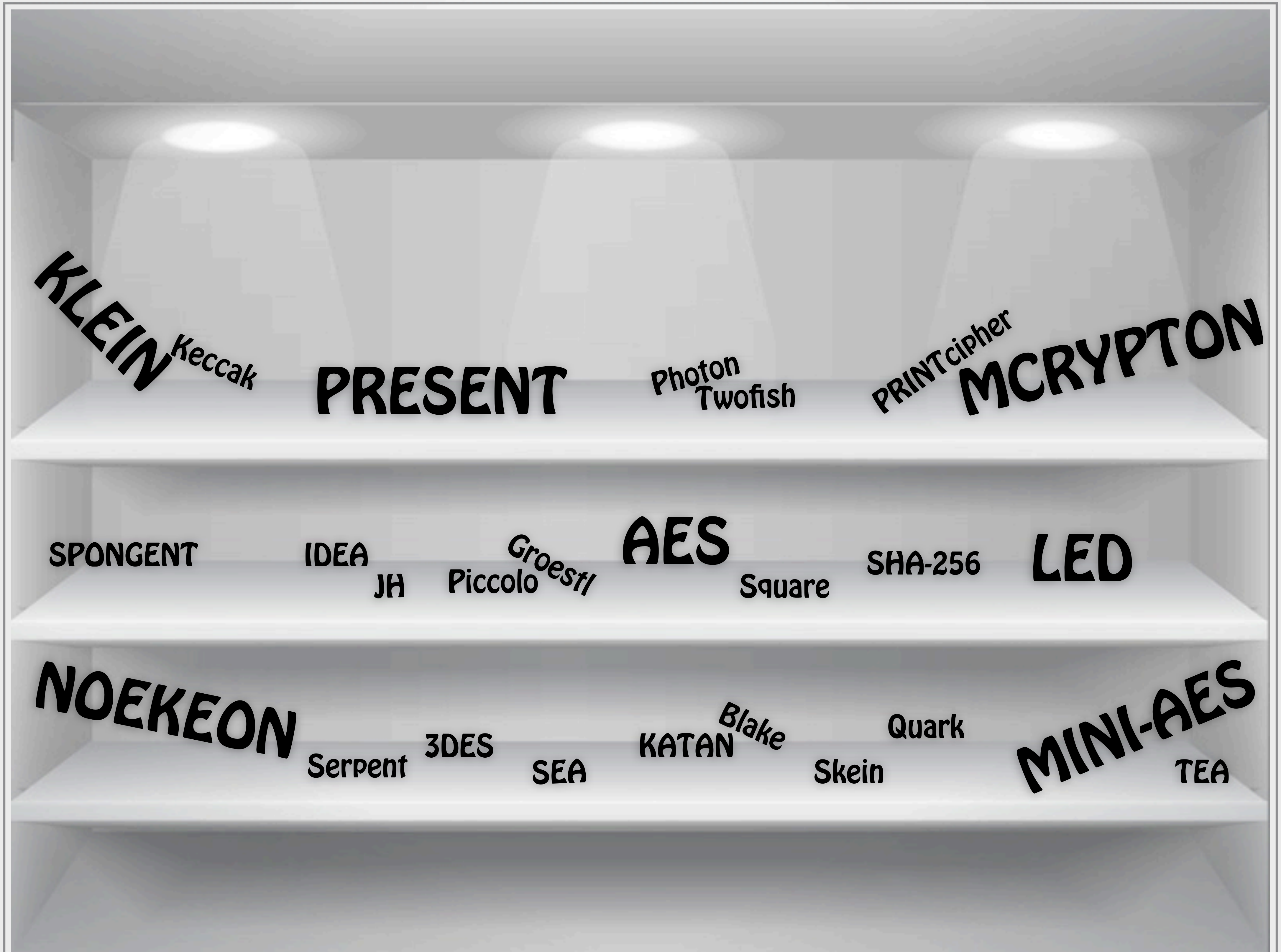
Typical Trade-offs in Crypto



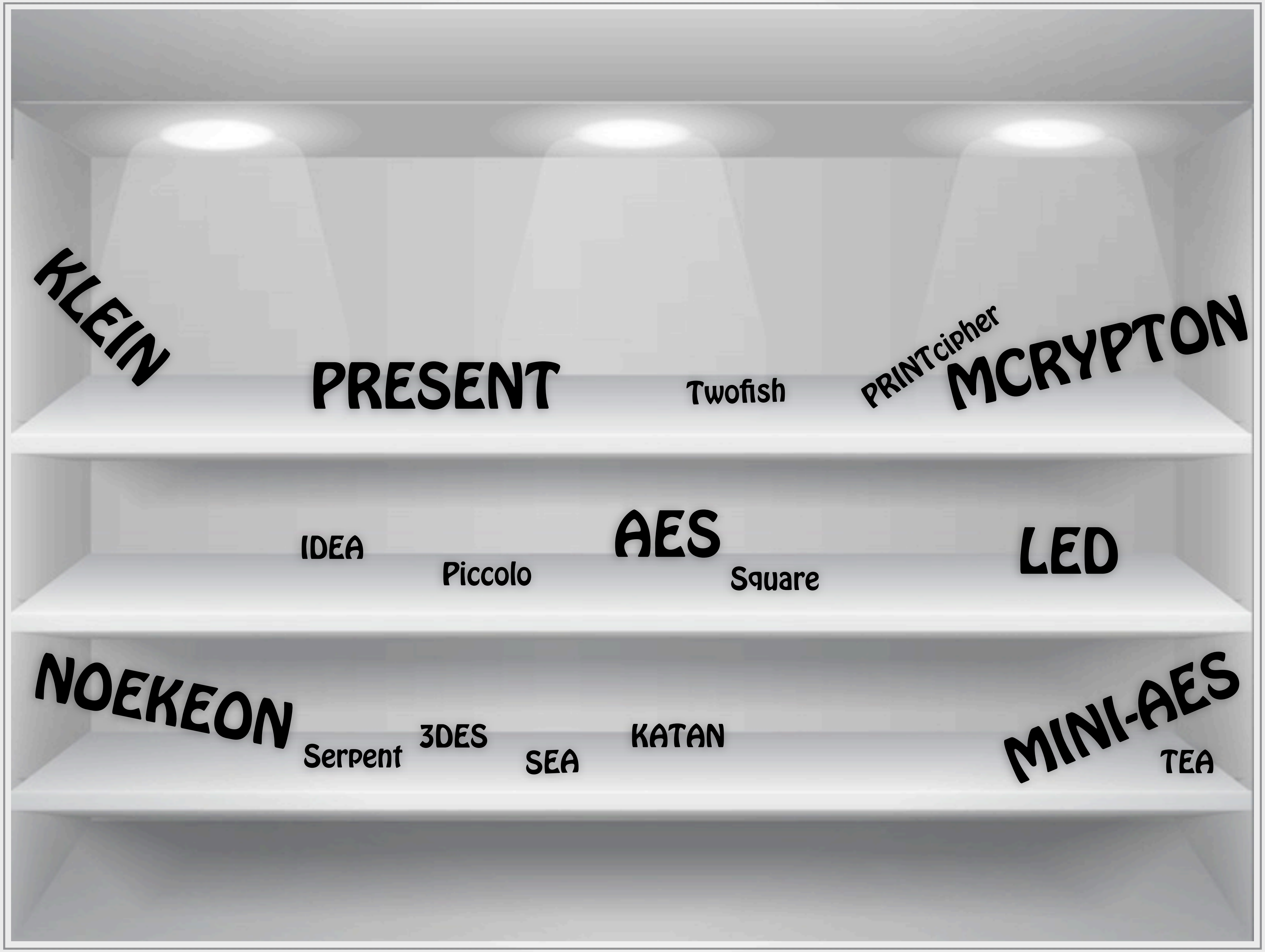
A kid in a Toy store



A kid in a Toy store

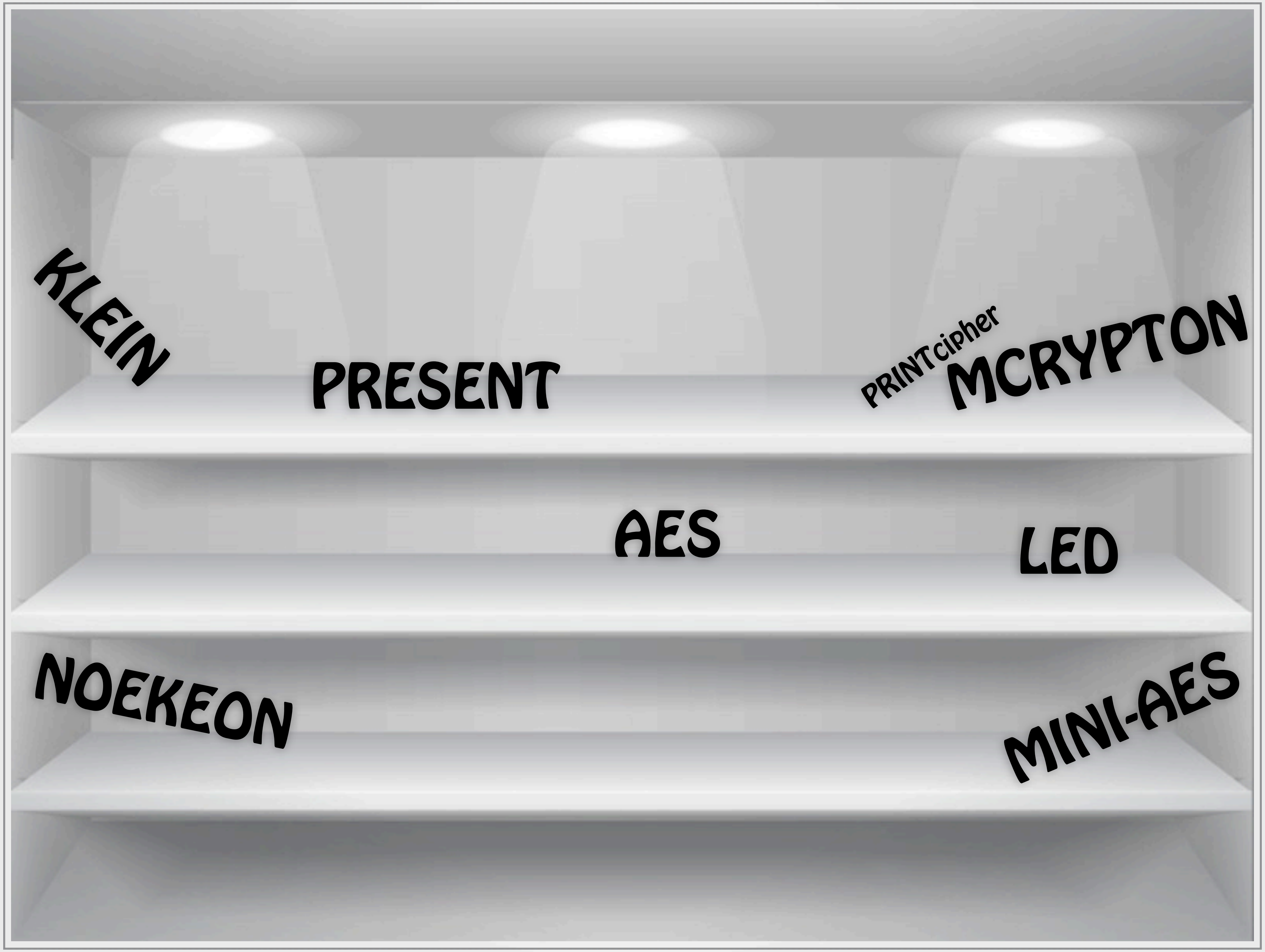


A kid in a Toy store

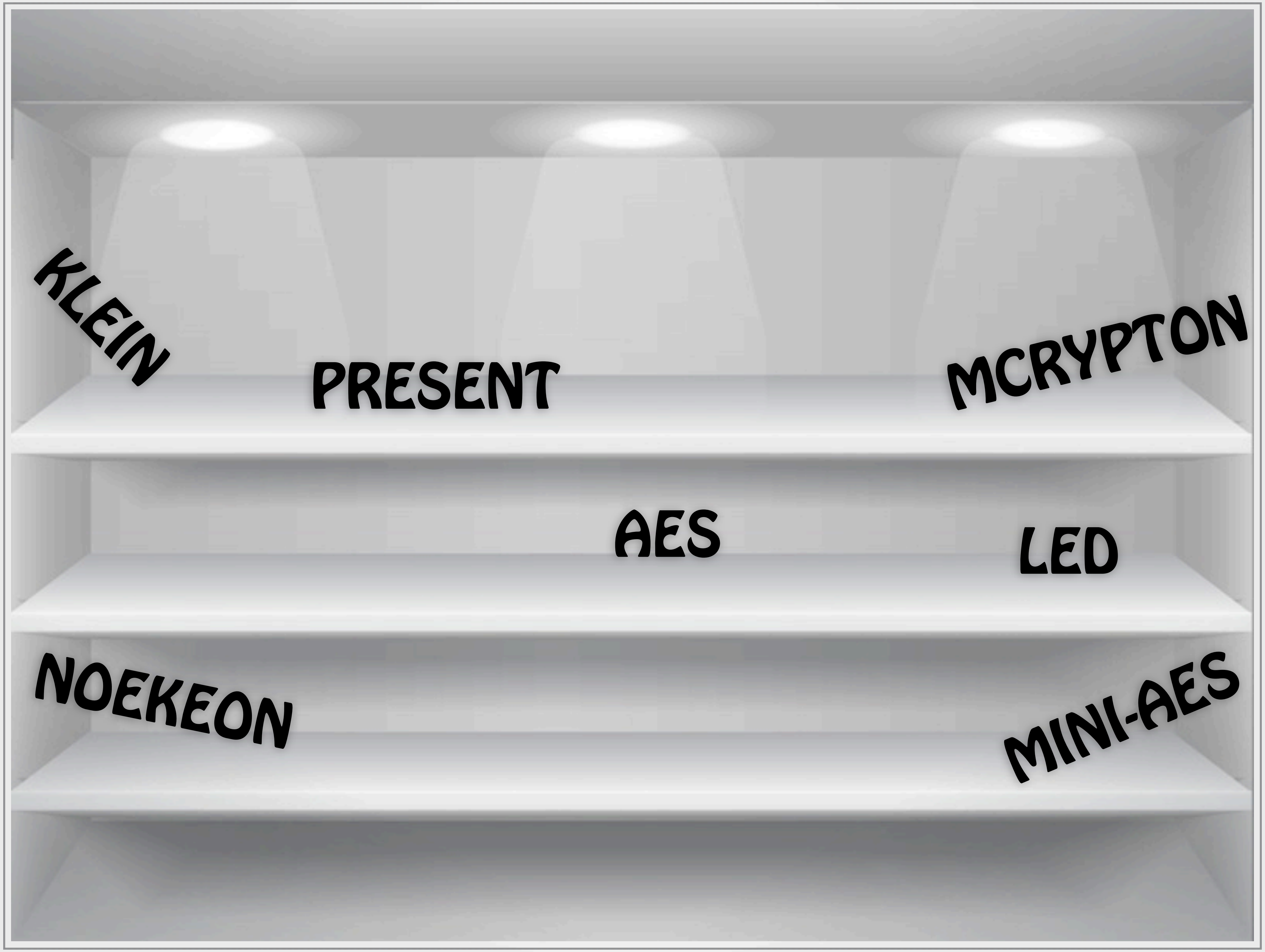


A kid in a Toy store

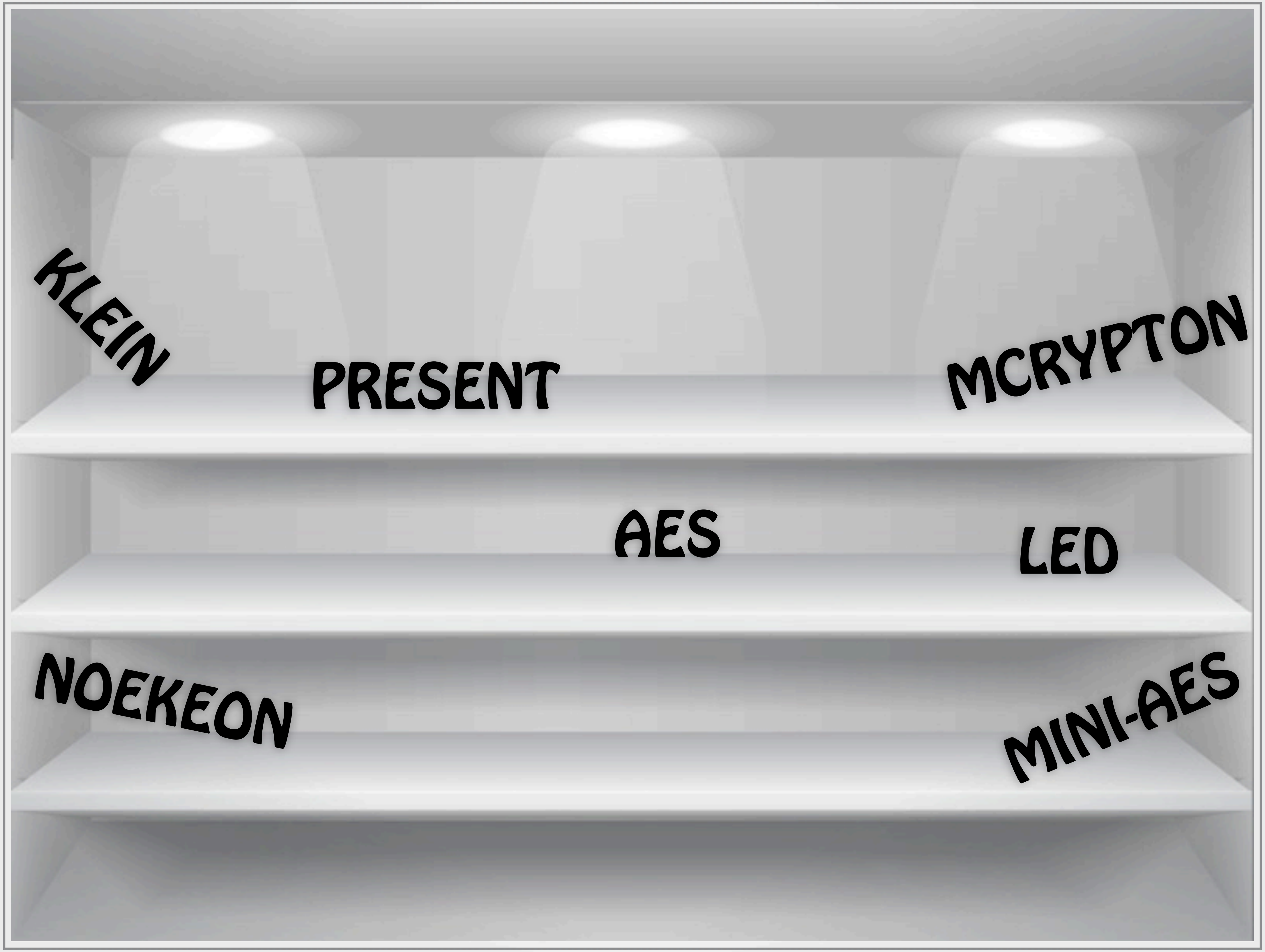
A kid in a Toy store



A kid in a Toy store



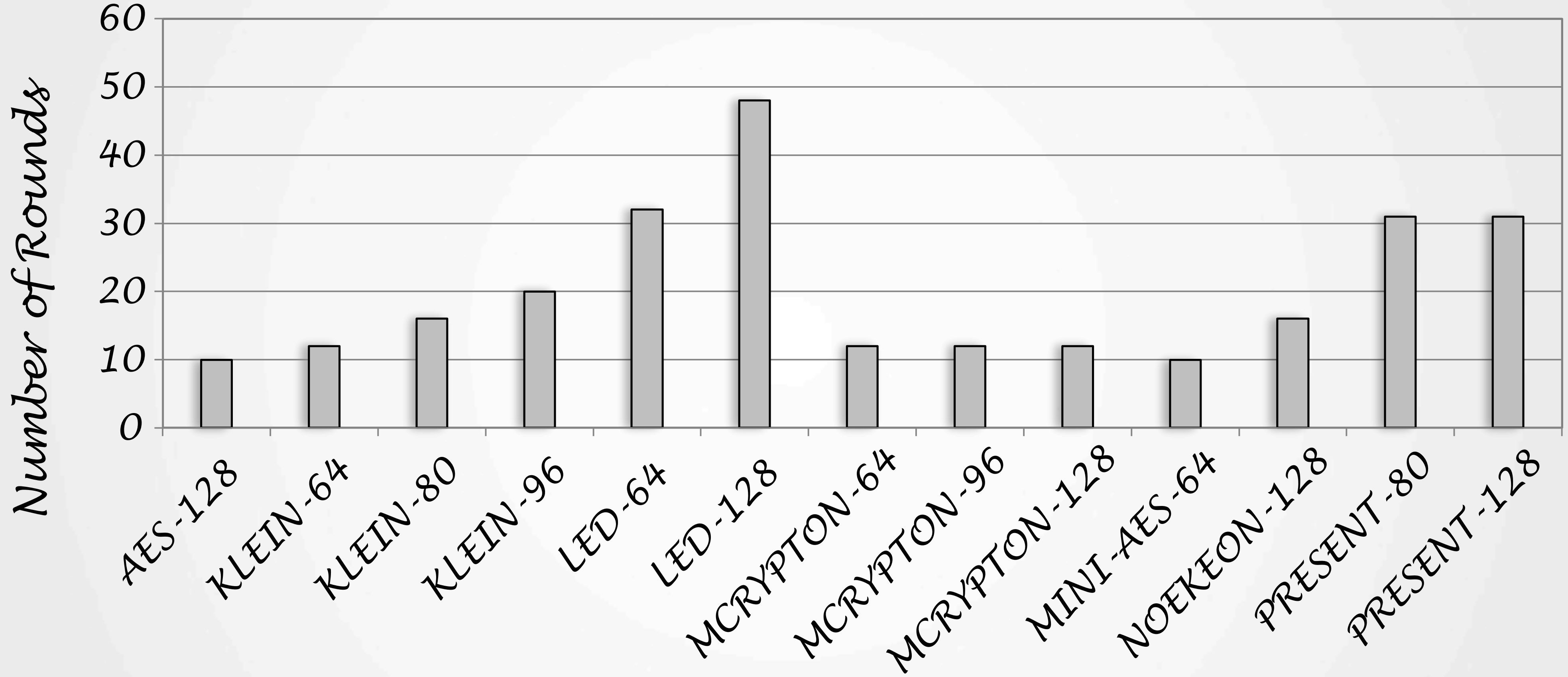
A kid in a Toy store



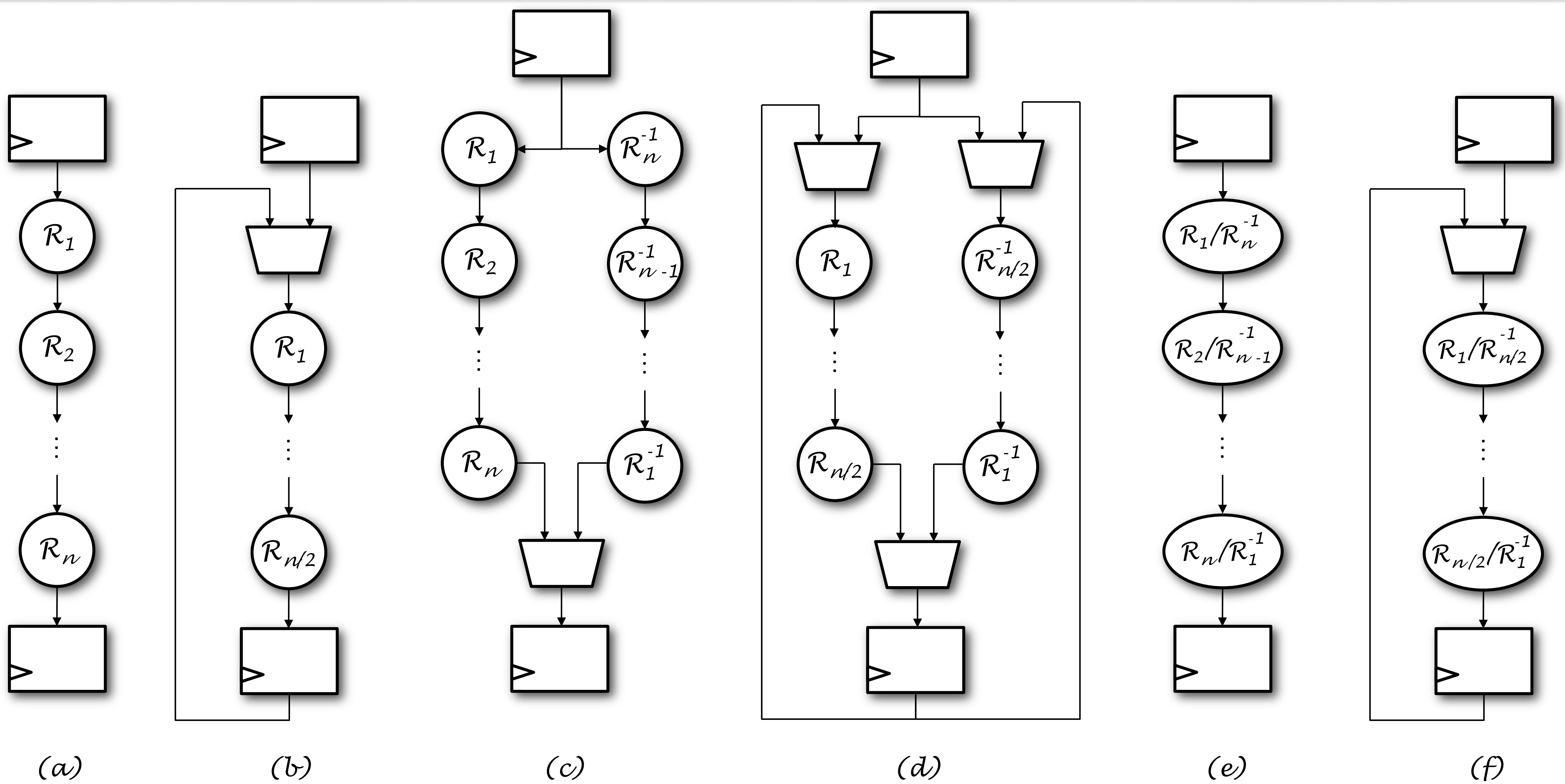
Variety of Choices

	BLOCK-SIZE	KEY-SIZE	S-BOX	P-LAYER	KEY SCHEDULE
AES	128	128	8	MDS	LIGHT
NOEKEON	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

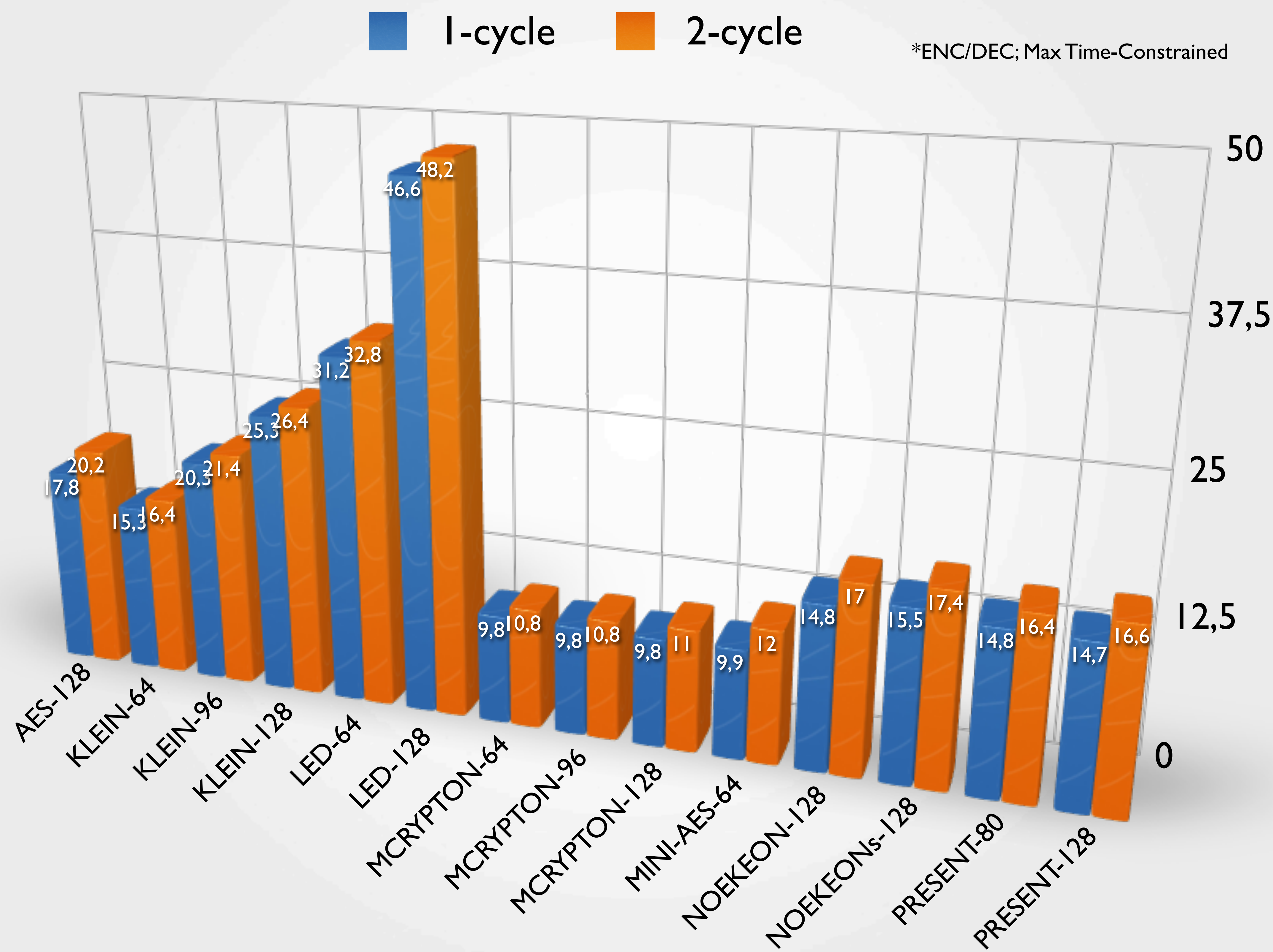


Six Architectures



Results - Latency

Results - Latency

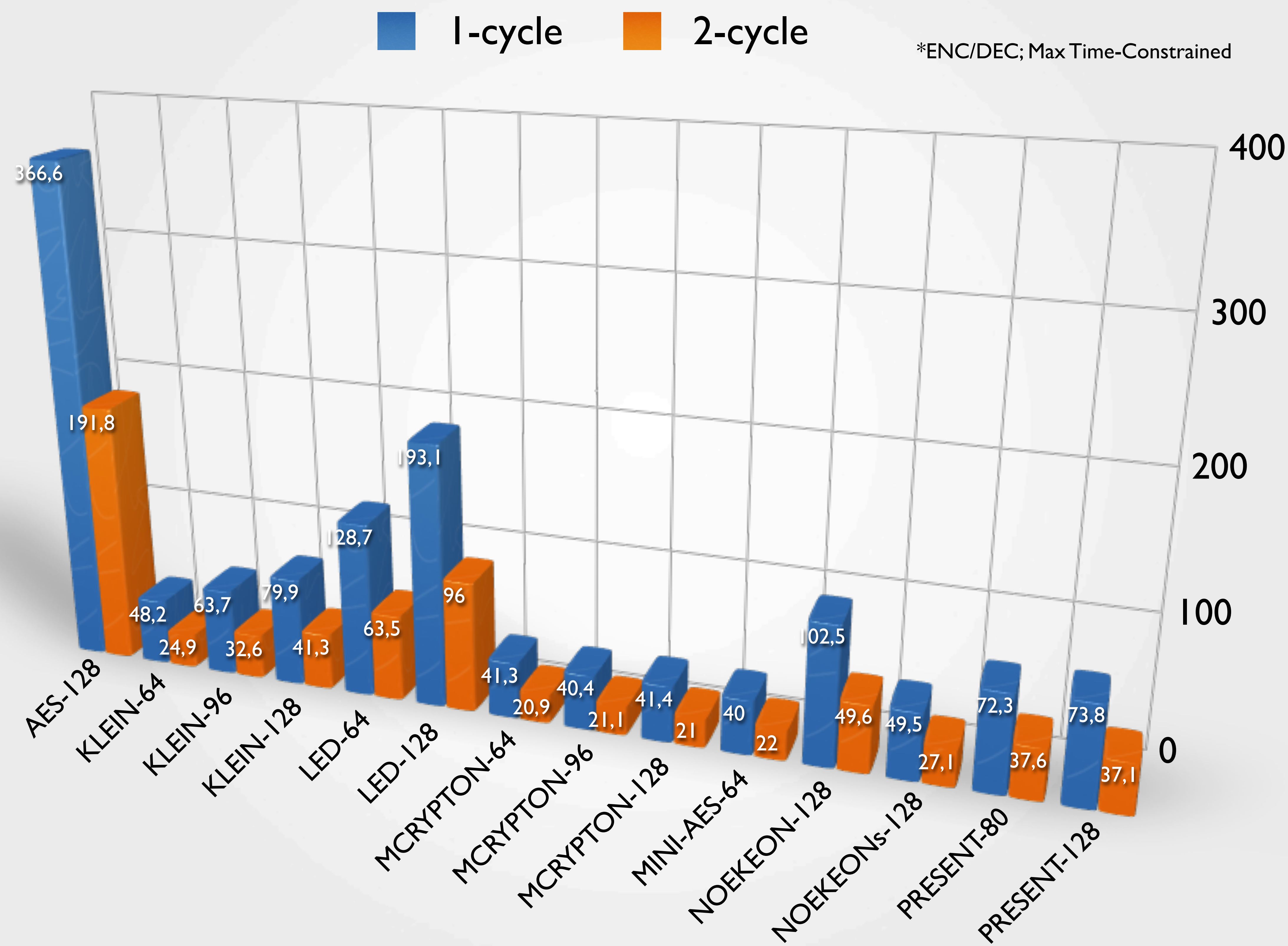


Results - Area

1-cycle 2-cycle

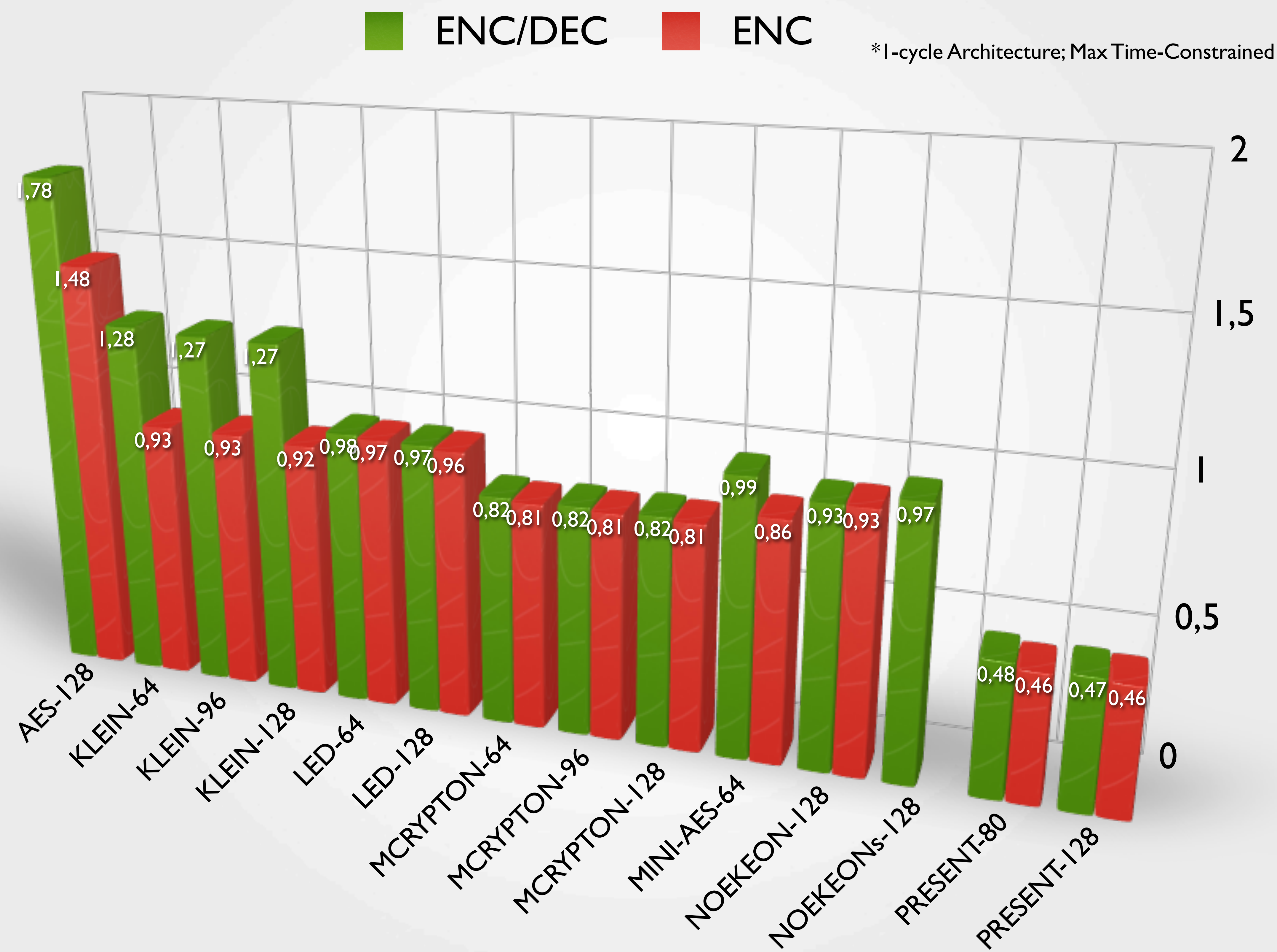
*ENC/DEC; Max Time-Constrained

Results - Area



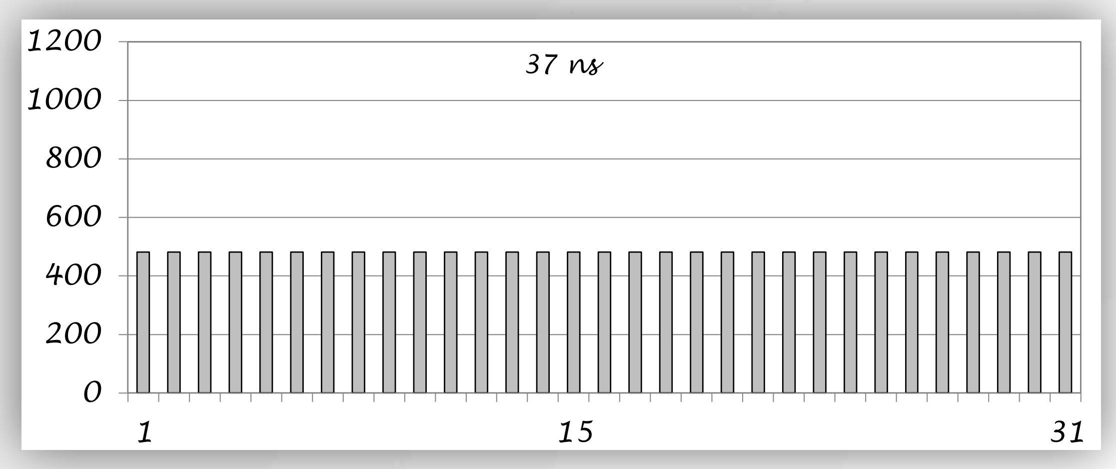
Results - Average Latency per Round

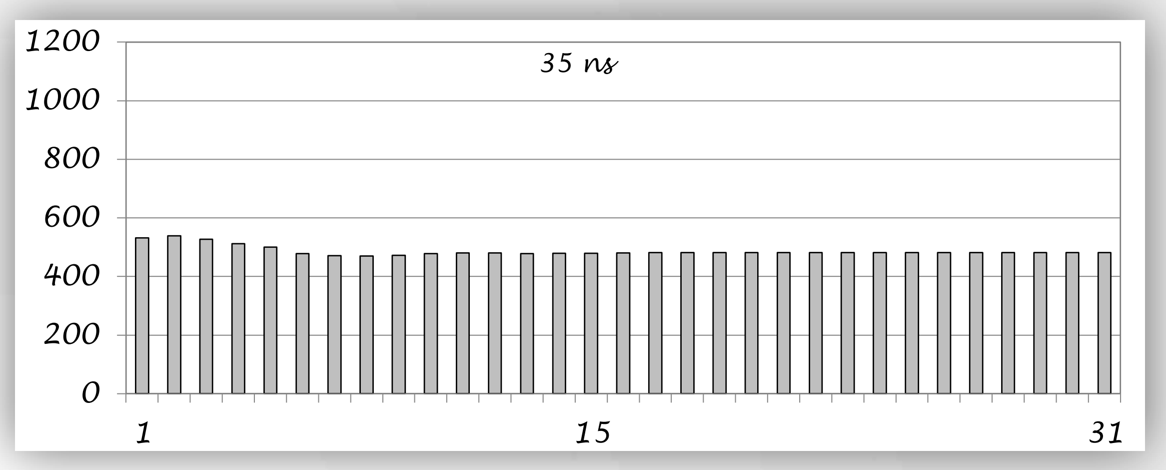
Results - Average Latency per Round

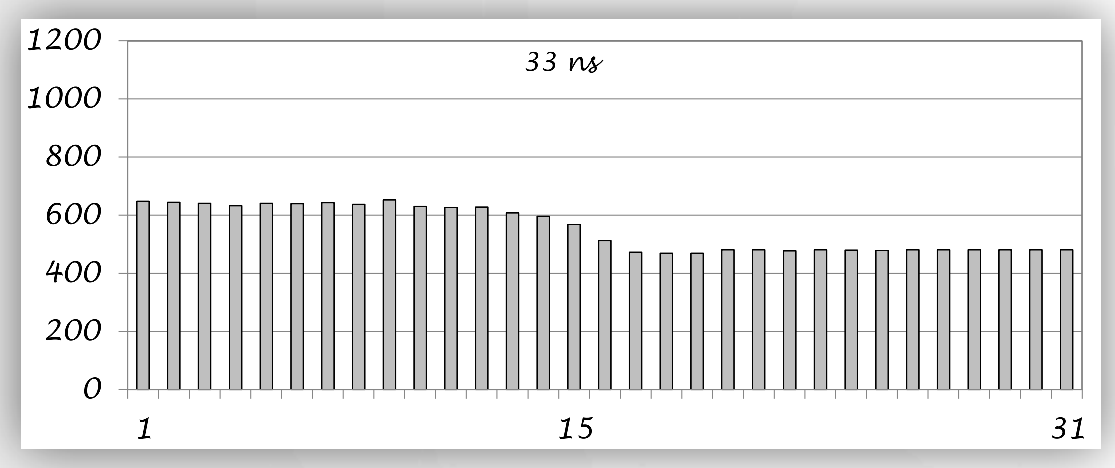


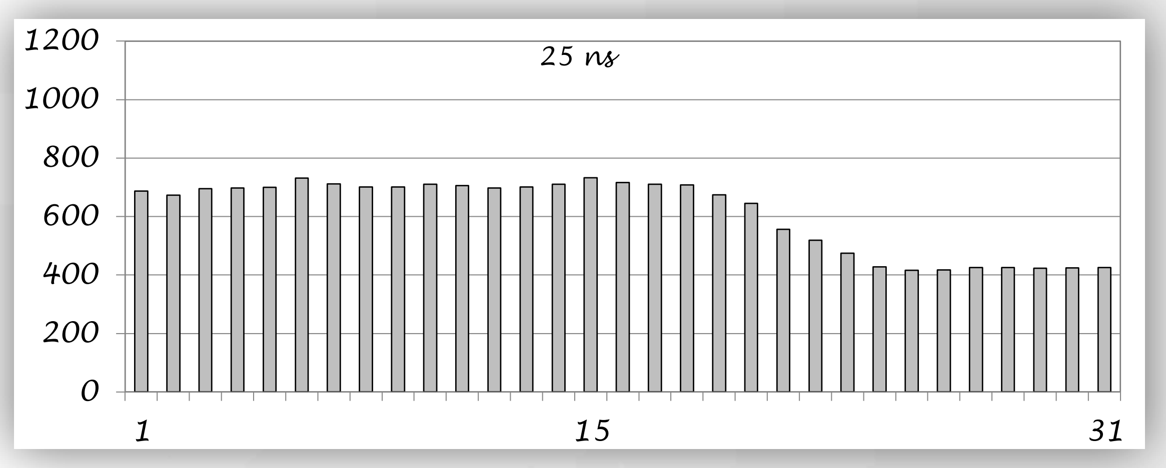
Results - Area per Round Distribution

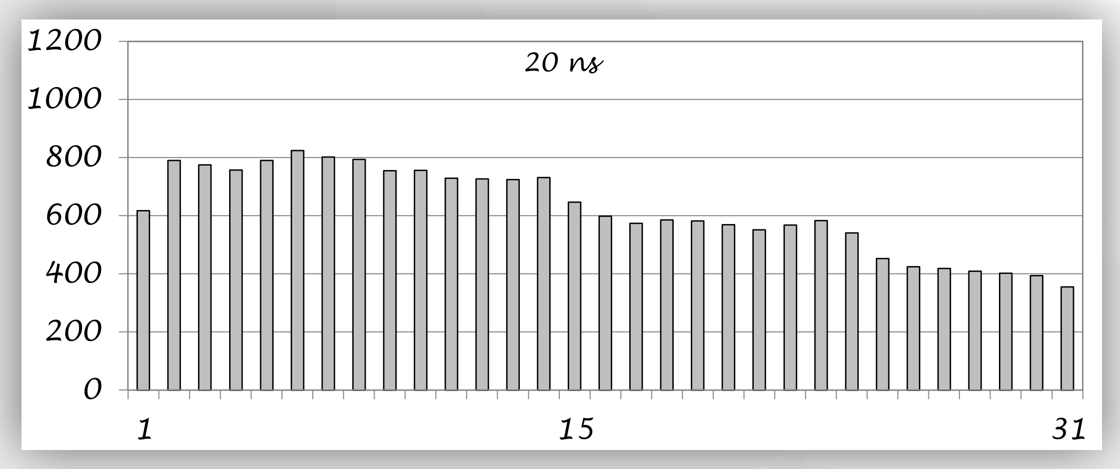
PRESENT-80, ENC only

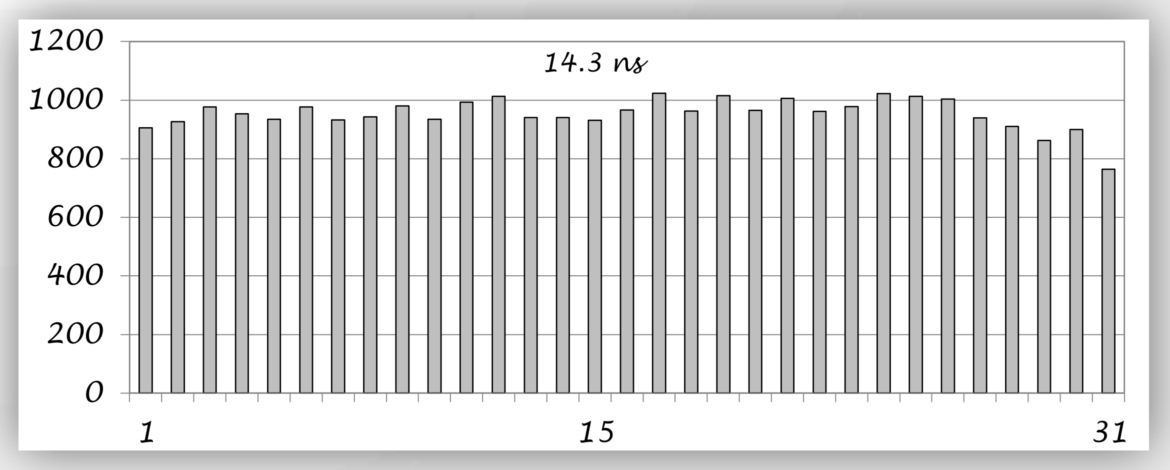












Hardware Recommendations

- We provide hardware recommendations for designing low-latency primitives.
- Evaluated ciphers are designed with low-area and low-power in mind and not to satisfy new low-latency requirements.
- Still, we can learn quite a lot from their constructions.

Hardware Recommendations
-Sbox-

- Use small Sboxes (4-bit or even 3-bit ones).
- Even among them there are significant differences in latency and area [24].
- These differences are library dependent.

[24] G. Leander and A. Poschmann, On the Classification of 4-bit Sboxes, in Arithmetic of Finite Fields, First International Workshop - WAIFI 2007, volume 4547 of Lecture Notes in Computer Science, pages 159-176, 2007.

Hardware Recommendations

-Number of Rounds-

Minimize!

Hardware Recommendations
-Round Complexity-

- Not too low complexity.
- Reduce the number of rounds at the cost of (slightly) heavier round.

Hardware Recommendations
-Key Schedule-

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

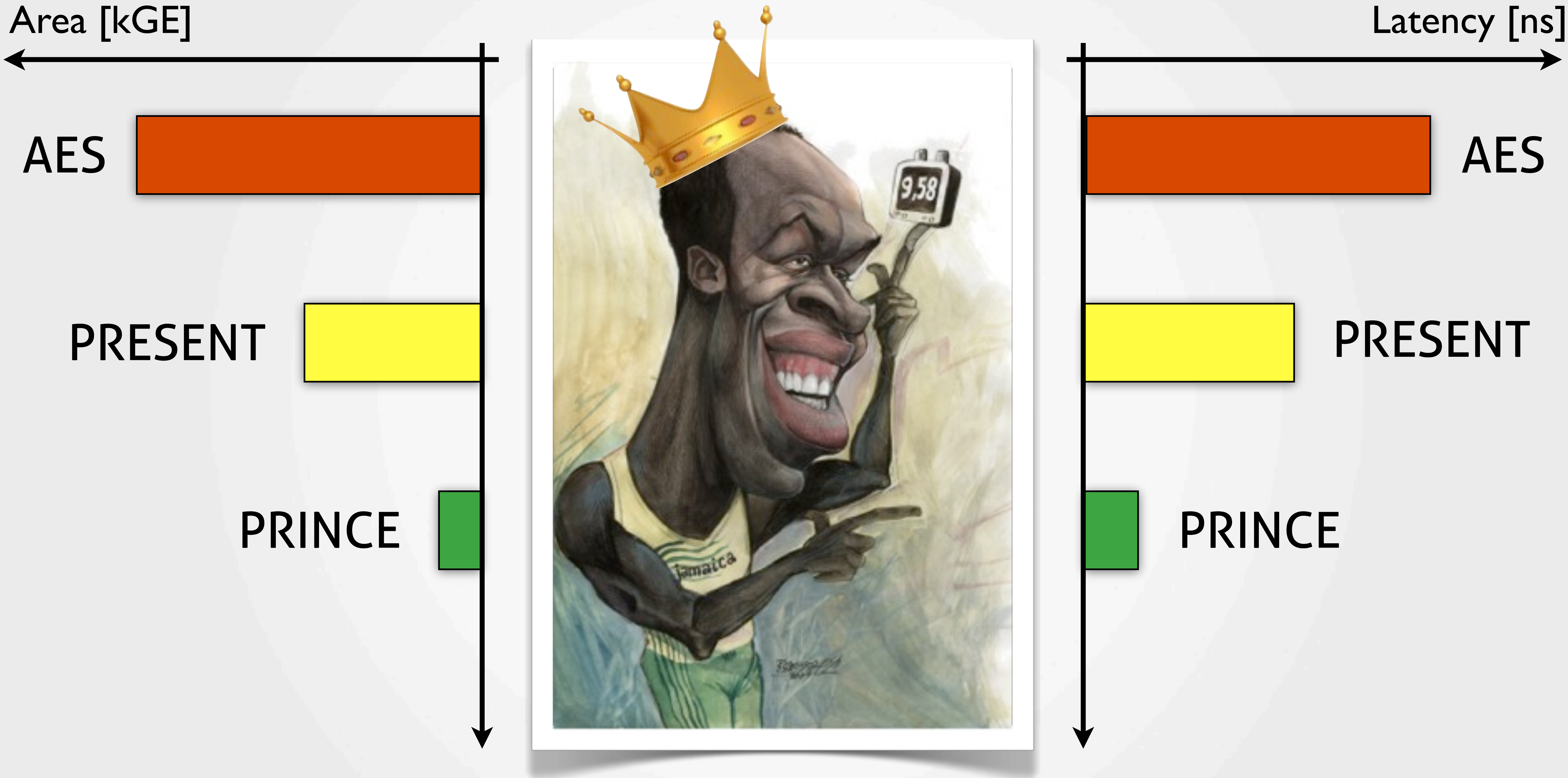
Hardware Recommendations
-Heterogeneous Constructions-

- Last few rounds of the cipher are smaller than the middle ones.
- Make those few rounds more computationally complex.
- Not very good for compact implementations.

Hardware Recommendations
-Encryption vs Decryption-

- Use involution: $f(f(x)) = x$.
- Make Encryption and Decryption procedures similar.
- BUT: Think "application oriented" - sometimes is beneficial to have "asymmetric" constructions.

Conclusions
meet PRINCE



J. Borghoff, A. Canteaut, T. Guneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. Thomsen, T. Yalcin, **PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications**, to appear in ASIACRYPT 2012.

Thank you!