SPONGENT:
A Lightweight Hash Function

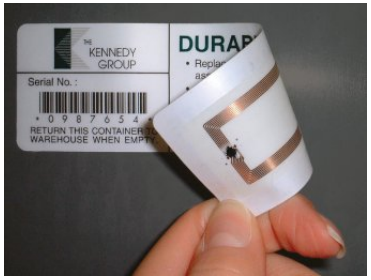
Andrey Bogdanov, Miroslav Knežević, Gregor Leander,
Deniz Toz, Kerem Varıcı, Ingrid Verbauwhede
K.U.Leuven, NXP, DTU

October 1, 2011
CHES'11, Nara, Japan

Ubiquitous Computing

Implants

Sensor networks



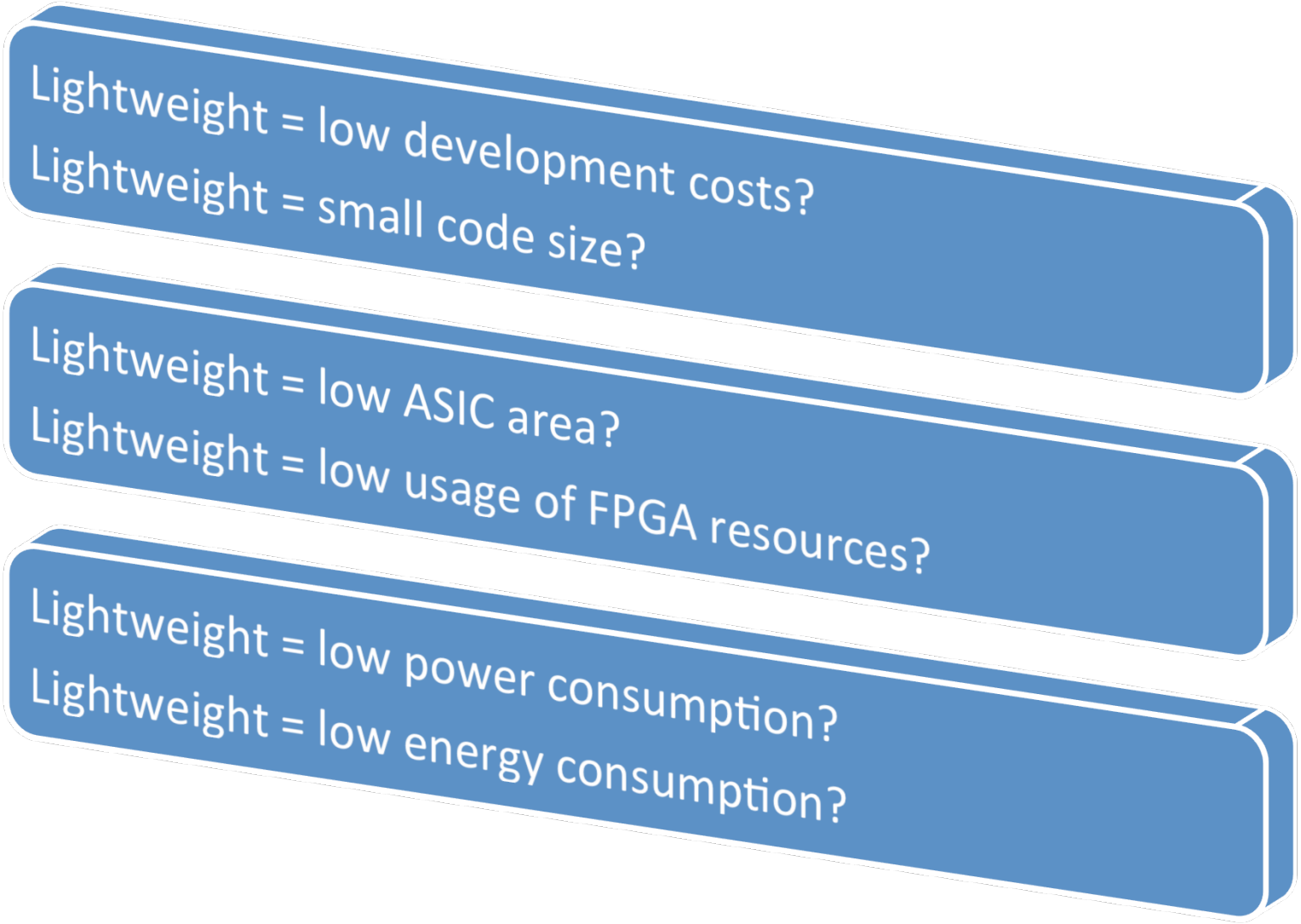
Logistics

Transportation

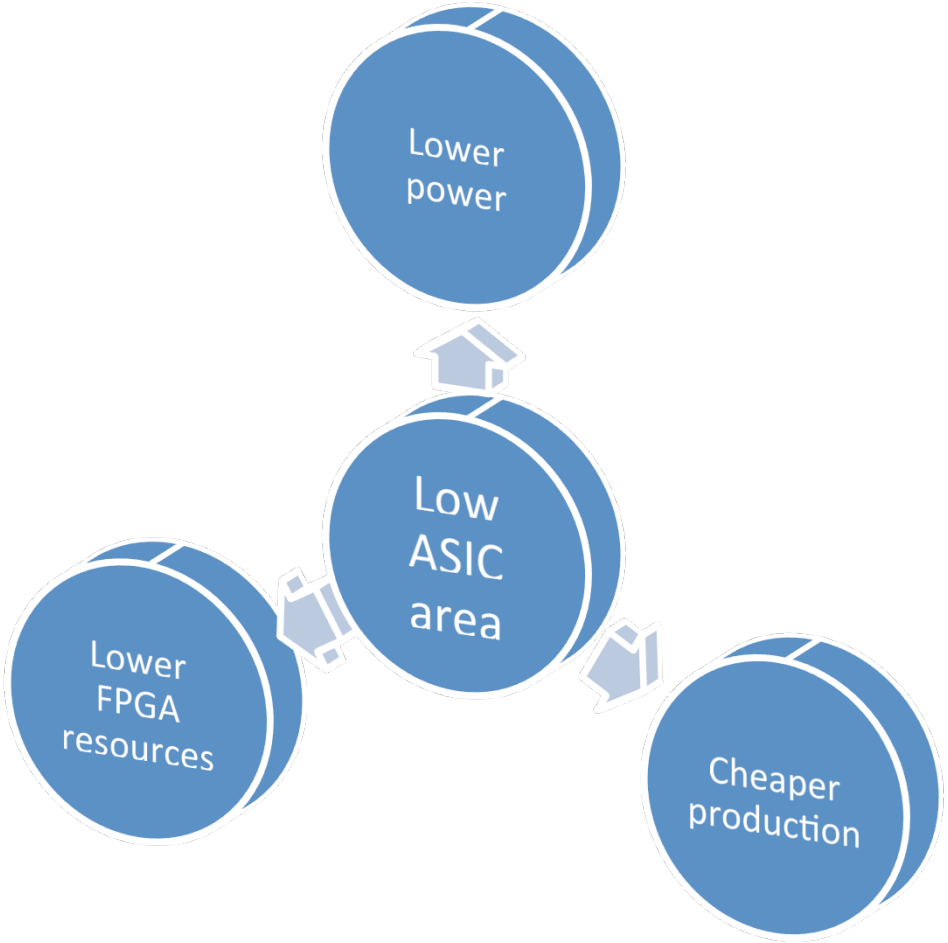
Access control

IDs

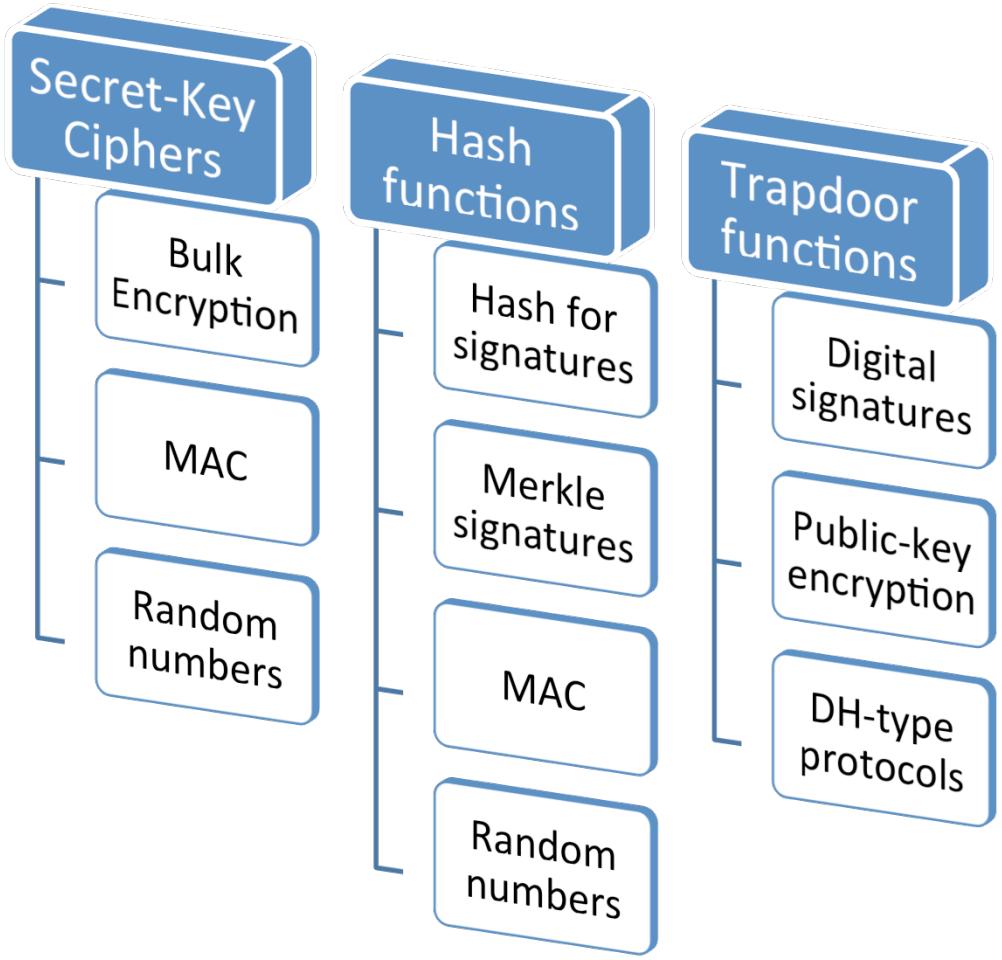
Lightweight = Low Cost



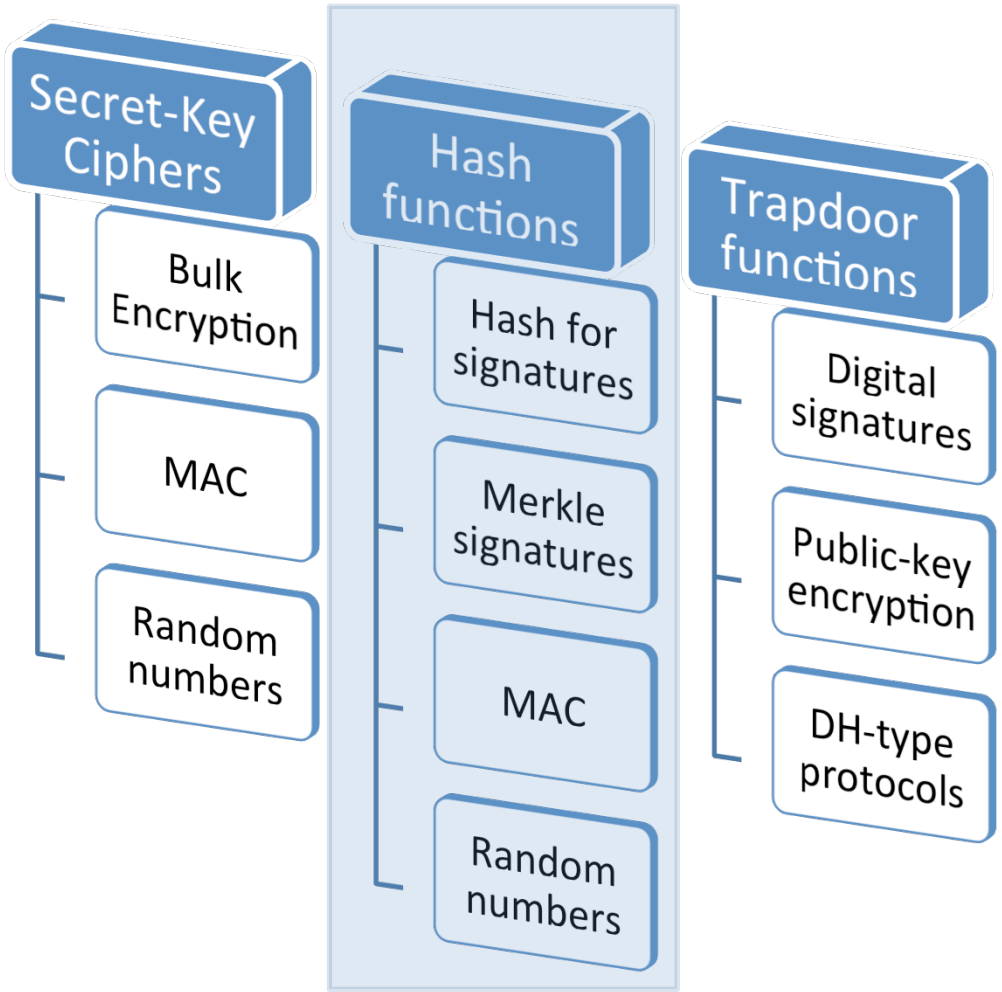
Lightweight =Low ASIC Area



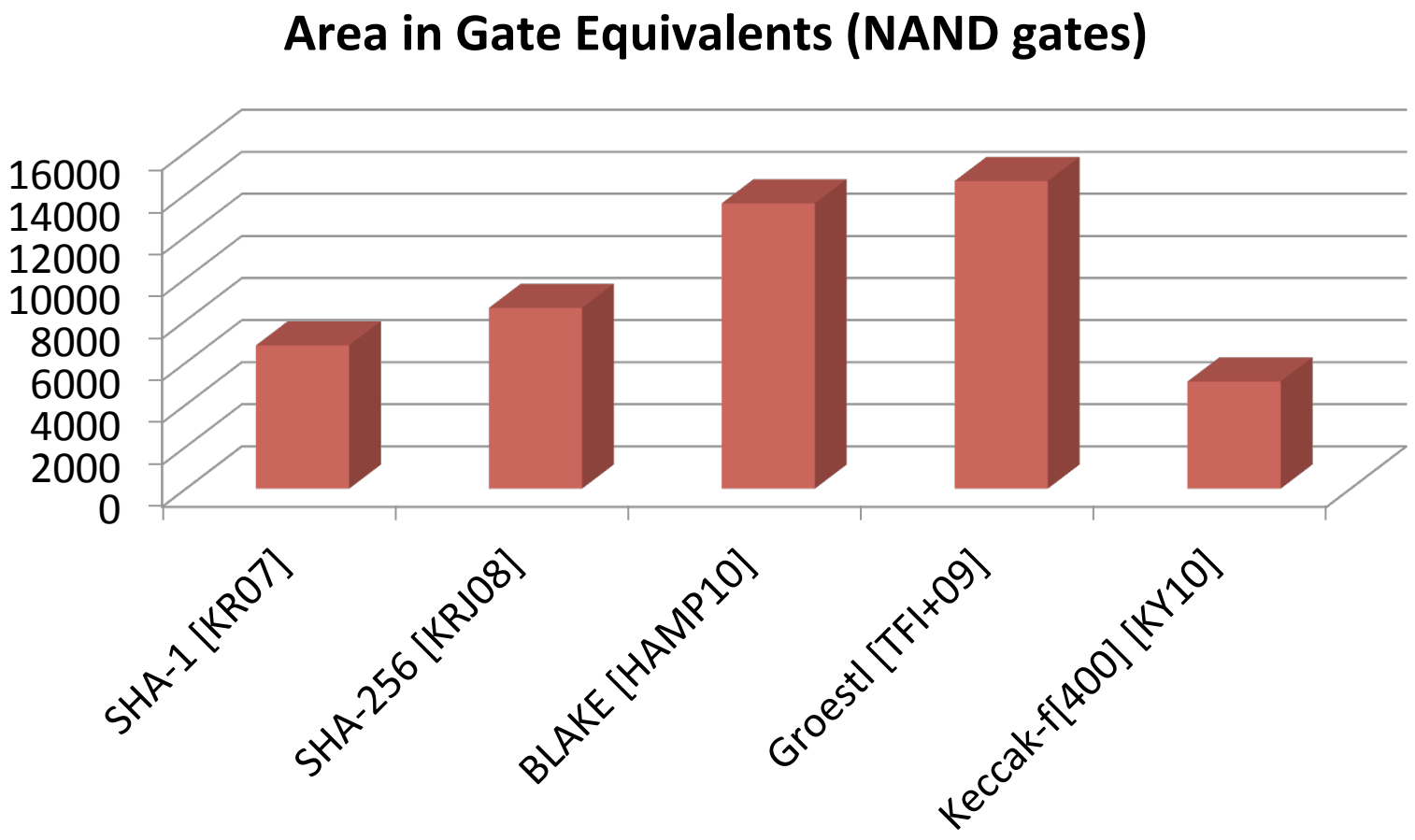
Crypto Algorithms to Meet Basic Security Needs



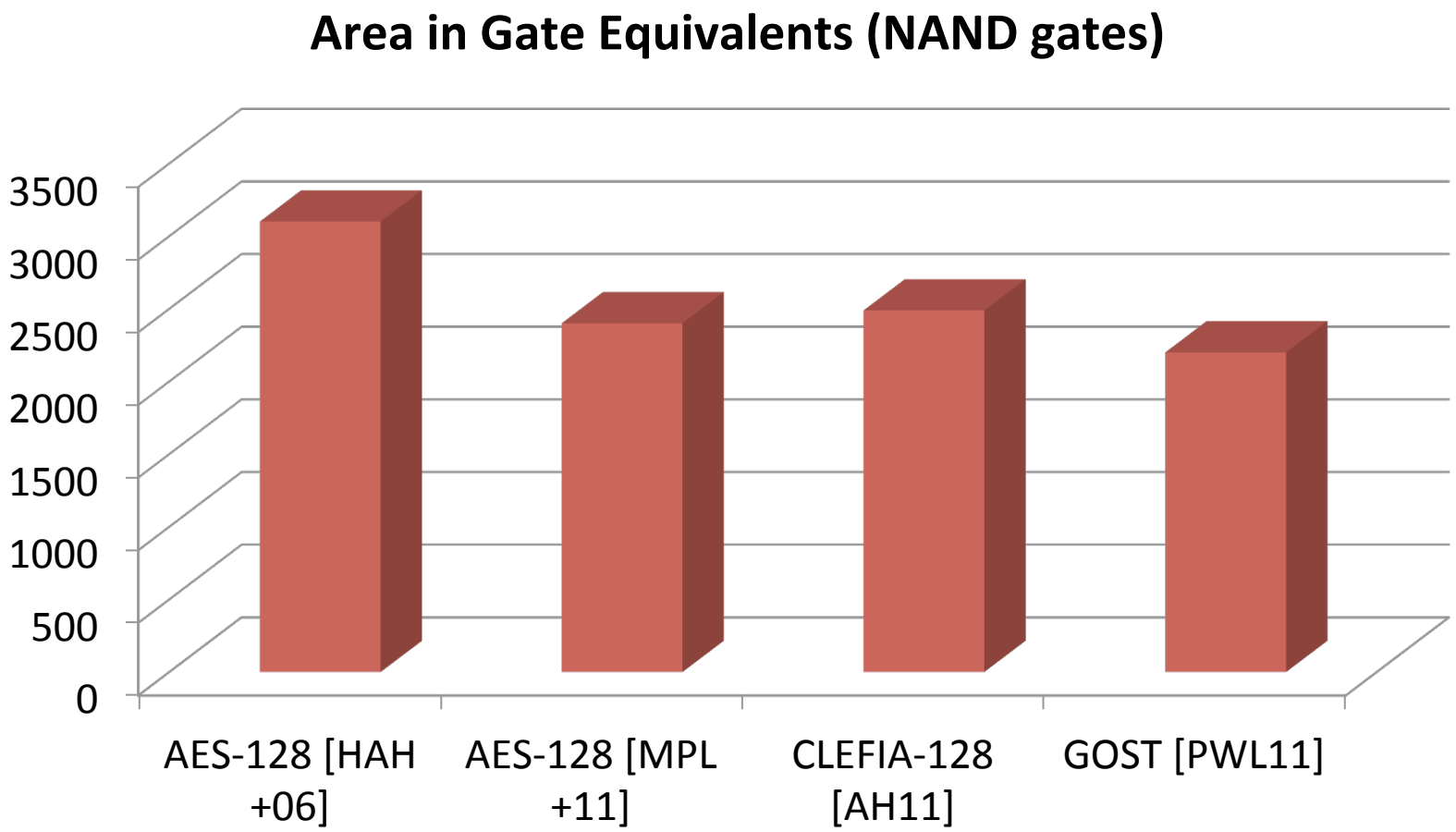
Crypto Algorithms to Meet Basic Security Needs



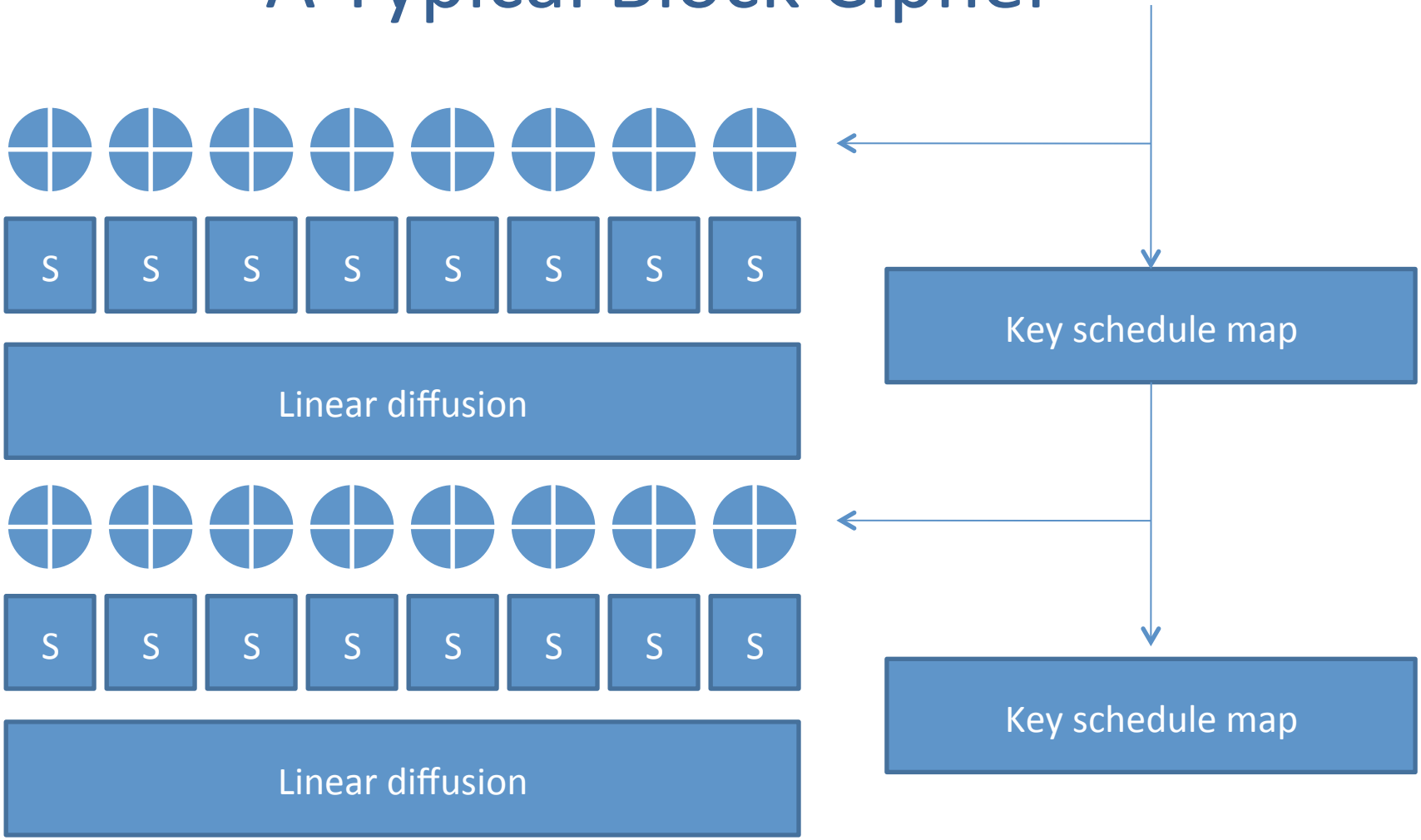
General-Purpose Hash Functions



Some Block Ciphers

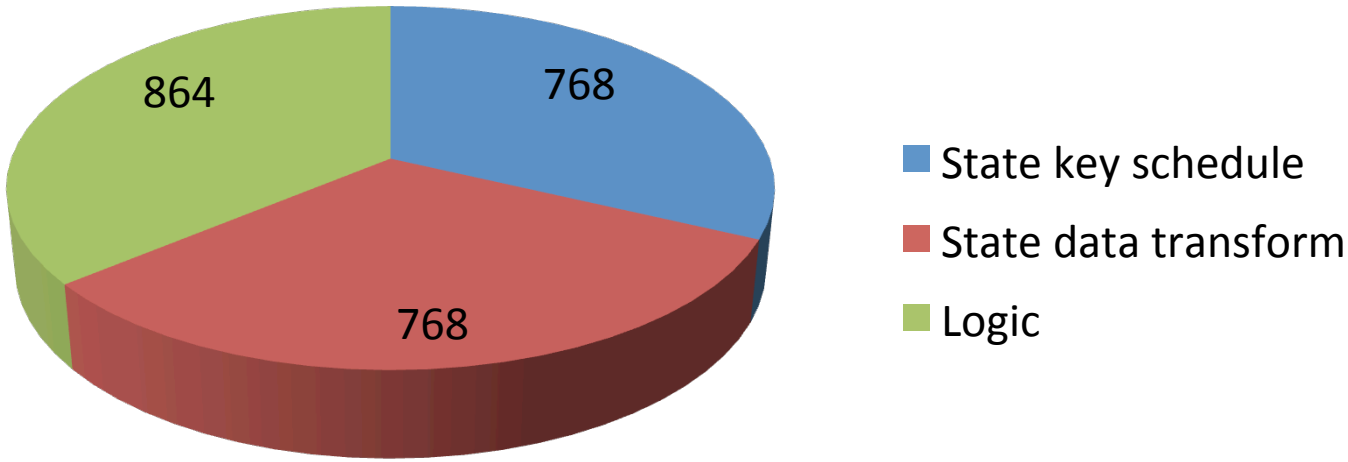


Substitution-Permutation: A Typical Block Cipher



Contribution of Building Blocks

Approximate area of AES-128 [MPL+11] in GE



How to optimize the design of a cipher for low area?

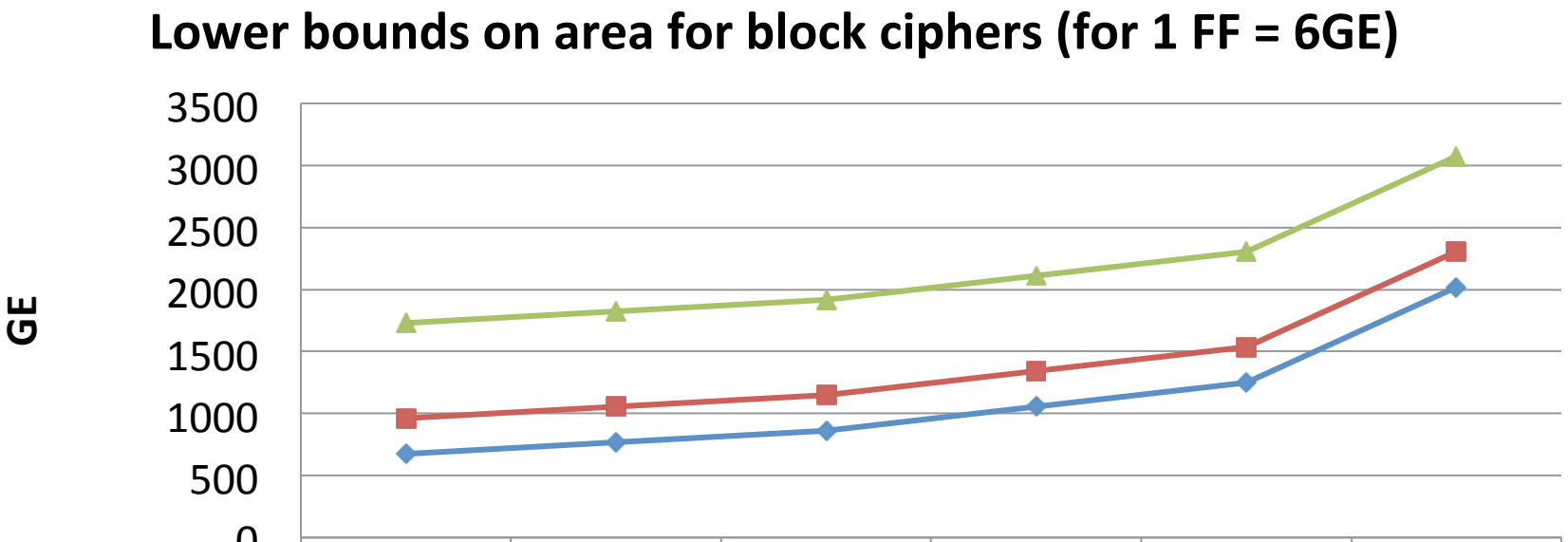
For given block and key sizes, minimize logic!

Area of Elementary Blocks

Logical operation	Cost in ASIC hardware
NAND(x,y)	**1.00 GE**
AND(x,y)	1.25 GE
OR(x,y)	1.25 GE
XOR(x,y)	2.25 GE
MUX(x,y;c)	2.50 GE
AND(x,y,z)	1.50 GE
MAJ(x,y,z)	2.25 GE
XOR(x,y,z)	**4.00 GE**

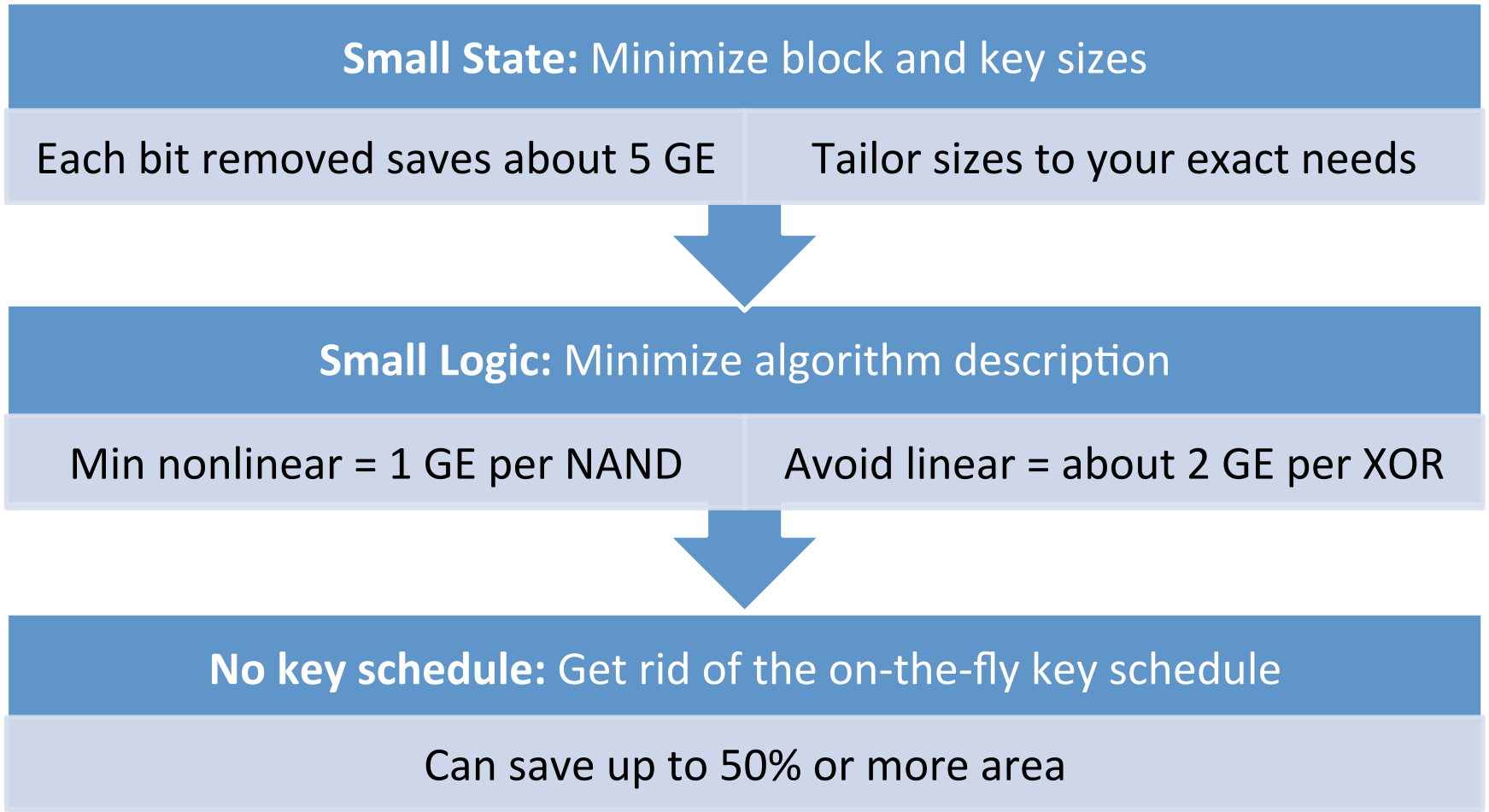
State (flip-flop)	Cost in ASIC hardware
1 bit	5.50 -7.50 GE

Minimum Area for Security Parameters

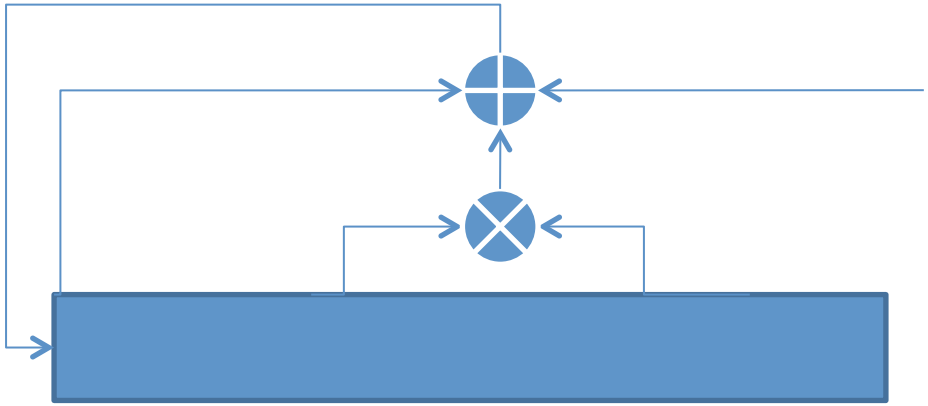


	block size 32	block size 48	block size 64	block size 96	block size 128	block size 256
key size 80	672	768	864	1056	1248	2016
key size 128	960	1056	1152	1344	1536	2304
key size 256	1728	1824	1920	2112	2304	3072

Design Ideas



The Extreme Lightweight Cipher

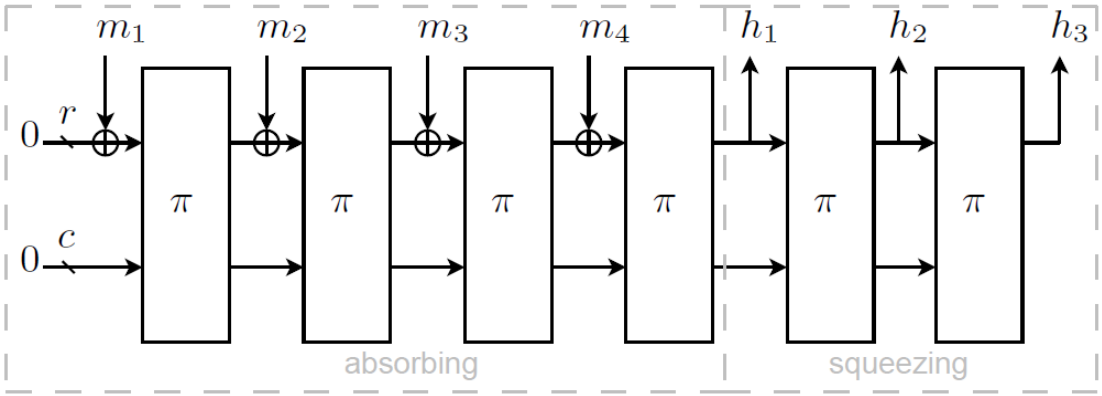


At least several thousand rounds required to attain security!

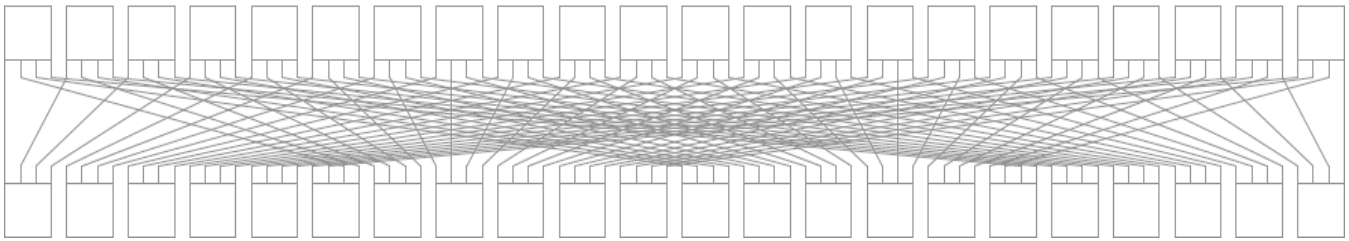
block size n	area: 5+6n GE
32	192
48	293
64	384
96	581
128	773

SPONGENT Hash: The Overview

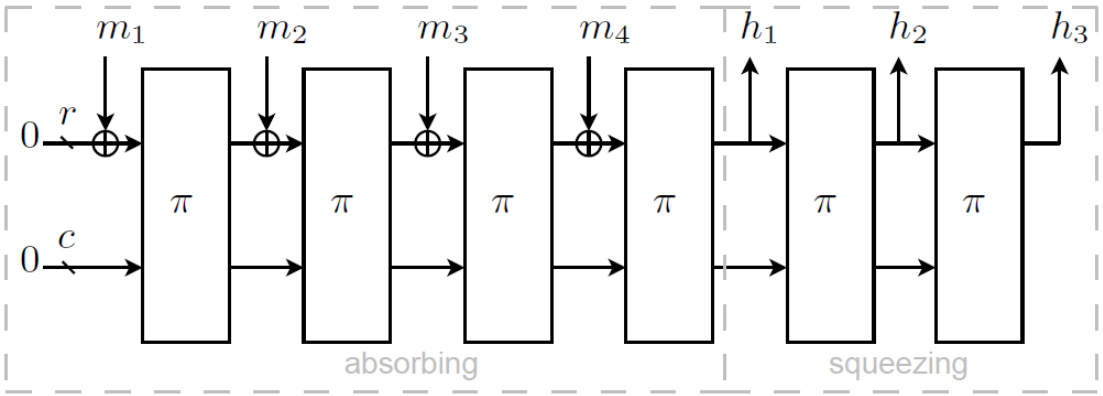
SPONGE construction



Unkeyed **PRESENT**-type permutation π: 4-bit S-box and bit diffusion

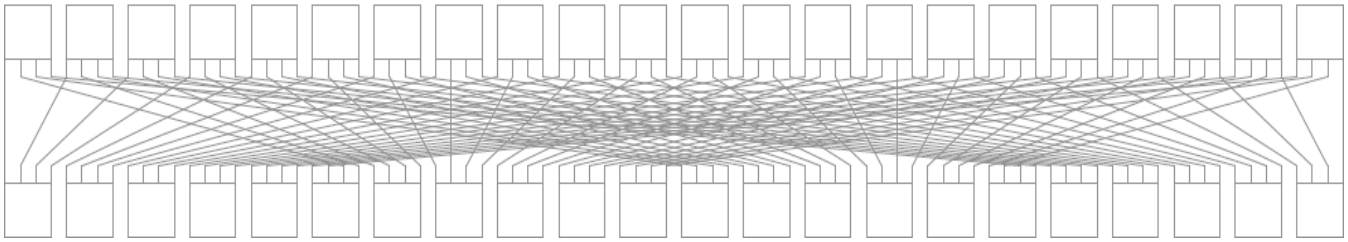


SPONGENT: The Parameters



	n (bit)	b (bit)	c (bit)	r (bit)	R number of rounds	security(bit) preimage	2nd preimage	collision
SPONGENT-88	88	88	80	8	45	80	40	40
SPONGENT-128	128	136	128	8	70	120	64	64
SPONGENT-160	160	176	160	16	90	144	80	80
SPONGENT-224	224	240	224	16	120	208	112	112
SPONGENT-256	256	272	256	16	140	240	128	128

SPONGENT: Building Blocks



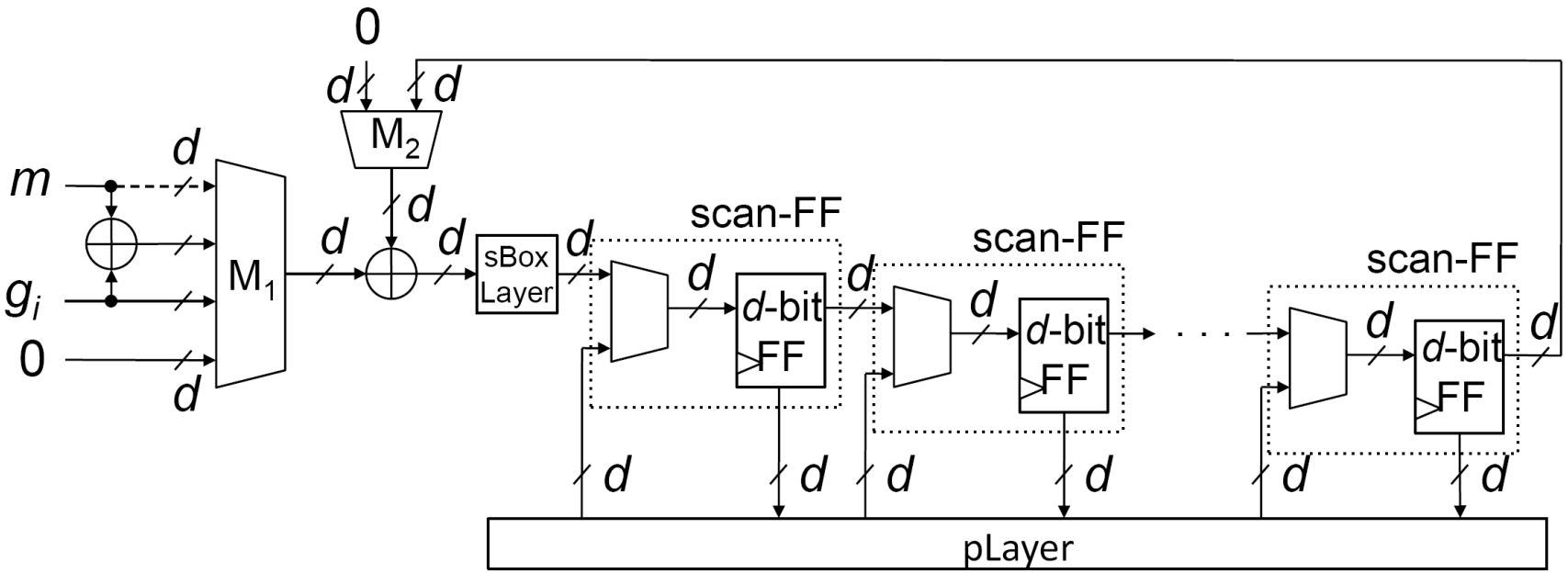
New 4-bit S-box fulfilling the PRESENT S-box criteria:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	E	D	B	0	2	1	4	F	7	A	8	5	9	C	3	6

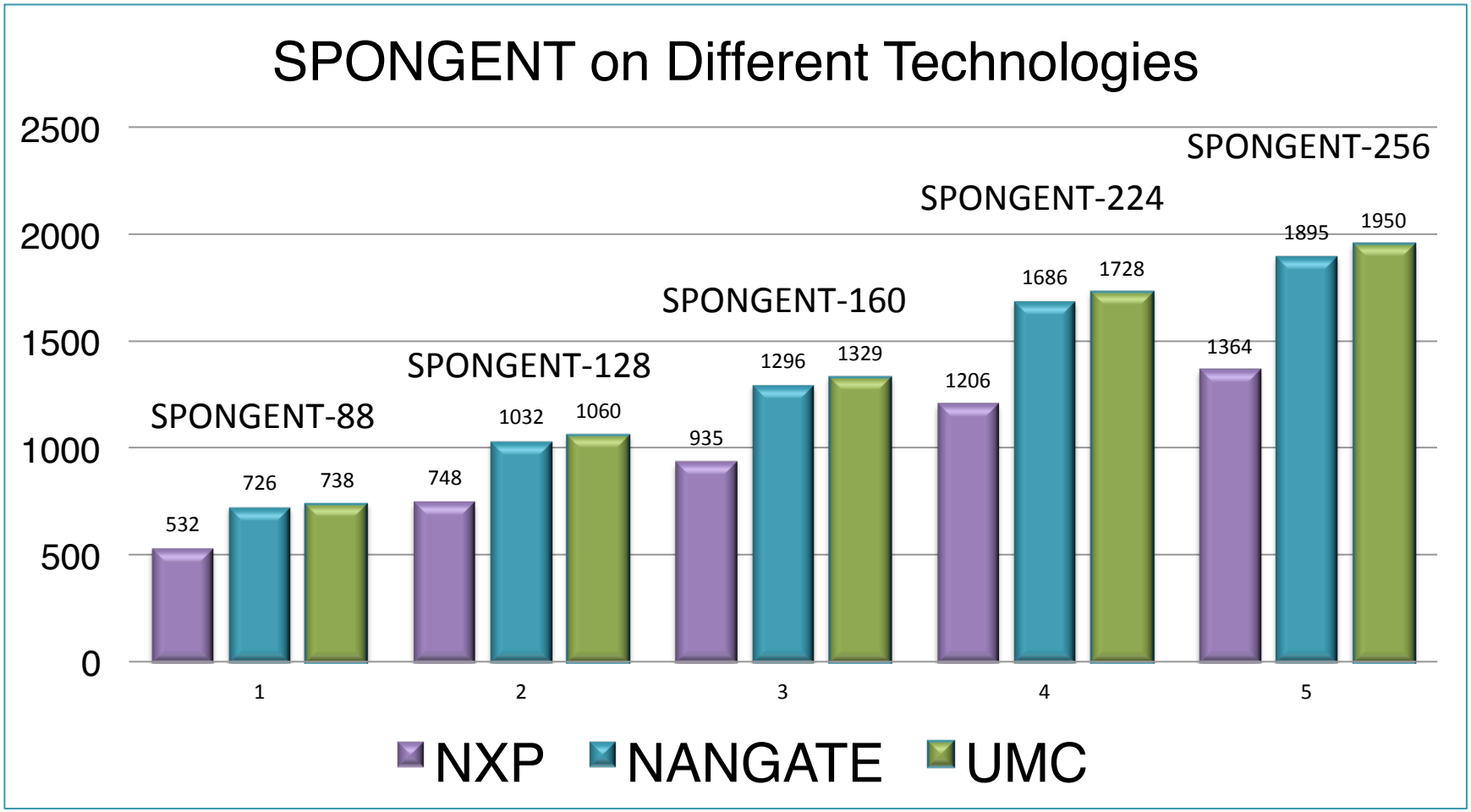
PRESENT-type bit permutation:

$$P_b(j) = \begin{cases} j \cdot b/4 \mod b-1, & \text{if } j \in \{0,\ldots,b-2\} \\ b-1, & \text{if } j = b-1. \end{cases}$$

SPONGENT: Serial ASIC Implementation



SPONGENT: The Impact of Technology



SPONGENT: The Area, UMC 130nm

Hash Function	Cycles	Datapath [bit]	Area [GE]	Throughput [kb/s]
SPONGENT-88	900	4	**738**	0.81
	45	88	**1127**	17.78
SPONGENT-128	2380	4	**1060**	0.34
	70	136	**1687**	11.43
SPONGENT-160	3960	4	**1329**	0.40
	90	176	**2190**	17.78
SPONGENT-224	7200	4	**1728**	0.22
	120	240	**2903**	13.33
SPONGENT-256	9520	4	**1950**	0.17
	140	272	**3281**	11.43

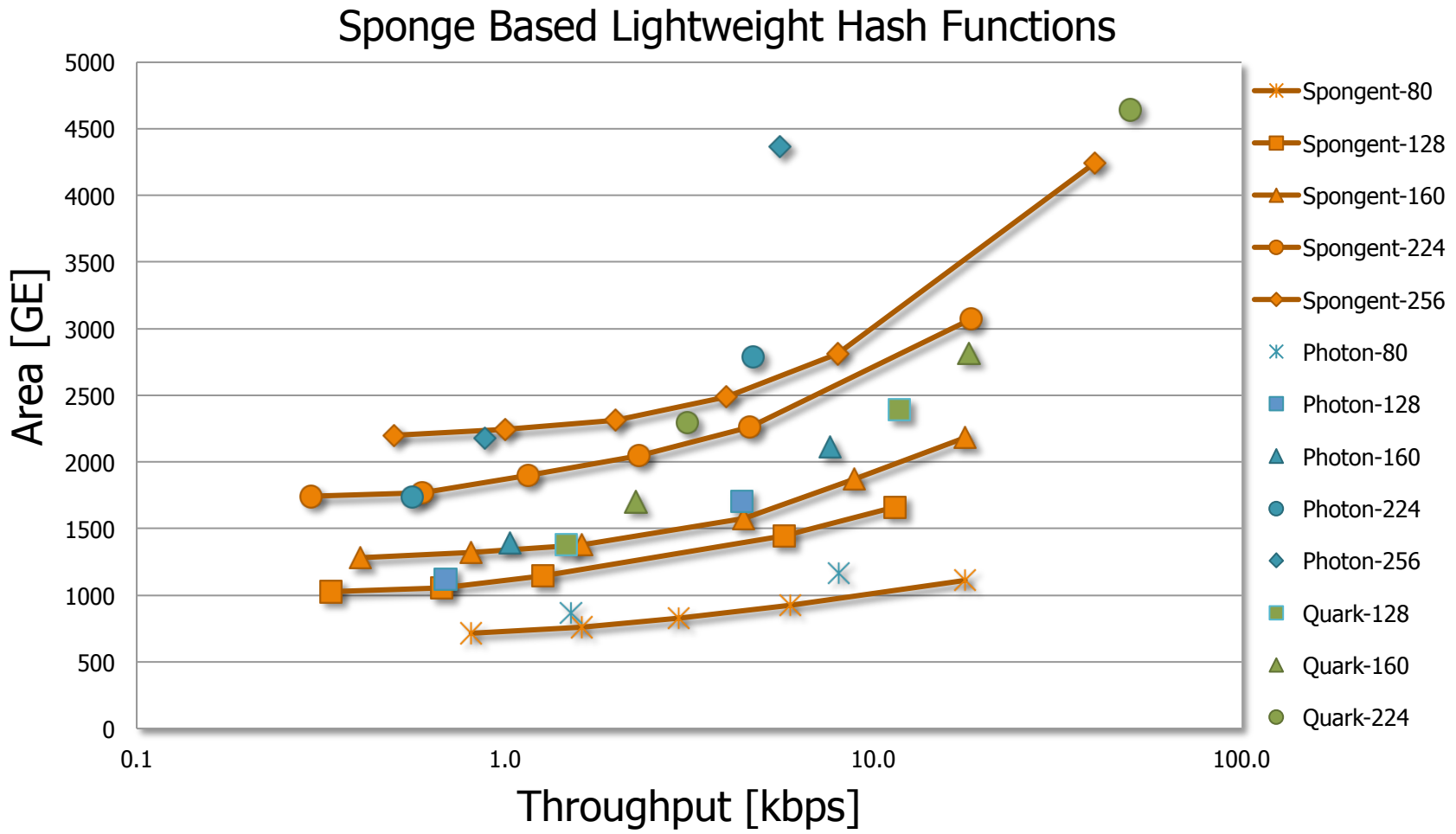
SPONGENT: The Area, NANGATE 45 nm

Hash Function	Cycles	Datapath [bit]	Area [GE]	Throughput [kb/s]	Area compared to UMC
SPONGENT-88	900	4	**726**	0.81	-2%
	45	88	**1164**	17.78	+3%
SPONGENT-128	2380	4	**1032**	0.34	-3%
	70	136	**1706**	11.43	+1%
SPONGENT-160	3960	4	**1296**	0.40	-2%
	90	176	**2272**	17.78	+4%
SPONGENT-224	7200	4	**1686**	0.22	-2%
	120	240	**3053**	13.33	+5%
SPONGENT-256	9520	4	**1895**	0.17	-3%
	140	272	**3425**	11.43	+4%

SPONGENT: The Area, NXP 90 nm

Hash Function	Cycles	Datapath [bit]	Area [GE]	Throughput [kb/s]	Area compared to UMC
SPONGENT-88	900	4	**532**	0.81	**-28%**
	45	88	**892**	17.78	**-21%**
SPONGENT-128	2380	4	**748**	0.34	**-29%**
	70	136	**1301**	11.43	**-23%**
SPONGENT-160	3960	4	**935**	0.40	**-30%**
	90	176	**1752**	17.78	**-20%**
SPONGENT-224	7200	4	**1206**	0.22	**-30%**
	120	240	**2334**	13.33	**-20%**
SPONGENT-256	9520	4	**1364**	0.17	**-30%**
	140	272	**2612**	11.43	**-20%**

SPONGENT vs Quark and Photon



SPONGENT: Some Security Properties

Theorem 1. *Any 5-round differential characteristic of the underlying permutation in* SPONGENT-$\{88, 128, 160, 224, 256\}$ *has a minimum of* 10 *active S-boxes.*

# of rounds	SPONGENT-88		SPONGENT-128		SPONGENT-160		SPONGENT-224		SPONGENT-256	
	ASN	Prob	ASN	Prob	ASN	Prob	ASN	Prob	ASN	Prob
5	10	2^{-21}	10	2^{-22}	10	2^{-21}	10	2^{-21}	10	2^{-20}
10	20	2^{-47}	29	2^{-68}	20	2^{-50}	20	2^{-43}	–	–
15	30	2^{-74}	-	-	30	2^{-79}	30	2^{-66}	–	–

Moreover, to thwart linear multidimensional/saturation attacks, the new 4x4-bit S-box is chosen such that the linear hull contains at most one trail with a single active S-box in every round

Conclusions

- Sponge construction with reduced security claims so far most suitable for low-area hashing
  - almost no overhead in the footprint with respect to the absolute minimum
- The underlying permutation is based on the PRESENT design ideas
  - similar differential and better linear properties
- Multidimensional linear properties (discovered for round-reduced PRESENT) eliminated by the new S-box

Outlooks I

- SPONGENT is a hermetic design (the permutation is not allowed to have structural weaknesses) → higher numbers of rounds needed
- But this does not seem to be necessary for the concrete (second) preimage and collision security

→**Open problem:** In sponge-type constructions, argue provable security in a more relaxed model (maybe no more indifferentiability) and go for simpler permutations to increase performance in designs

Outlooks II

- In some applications, only full collision security is necessary
- In permutation-based sponge, one can put

  Rate = ½ Capacity

  to sacrifice preimage security for speed

→**Faster SPONGENT variants:** Stay tuned!

- For applications with full 2^{nd} preimage security requirements, the state has to be almost doubled

→**SPONGENT variants with full 2^{nd} preimage security:** Coming soon!