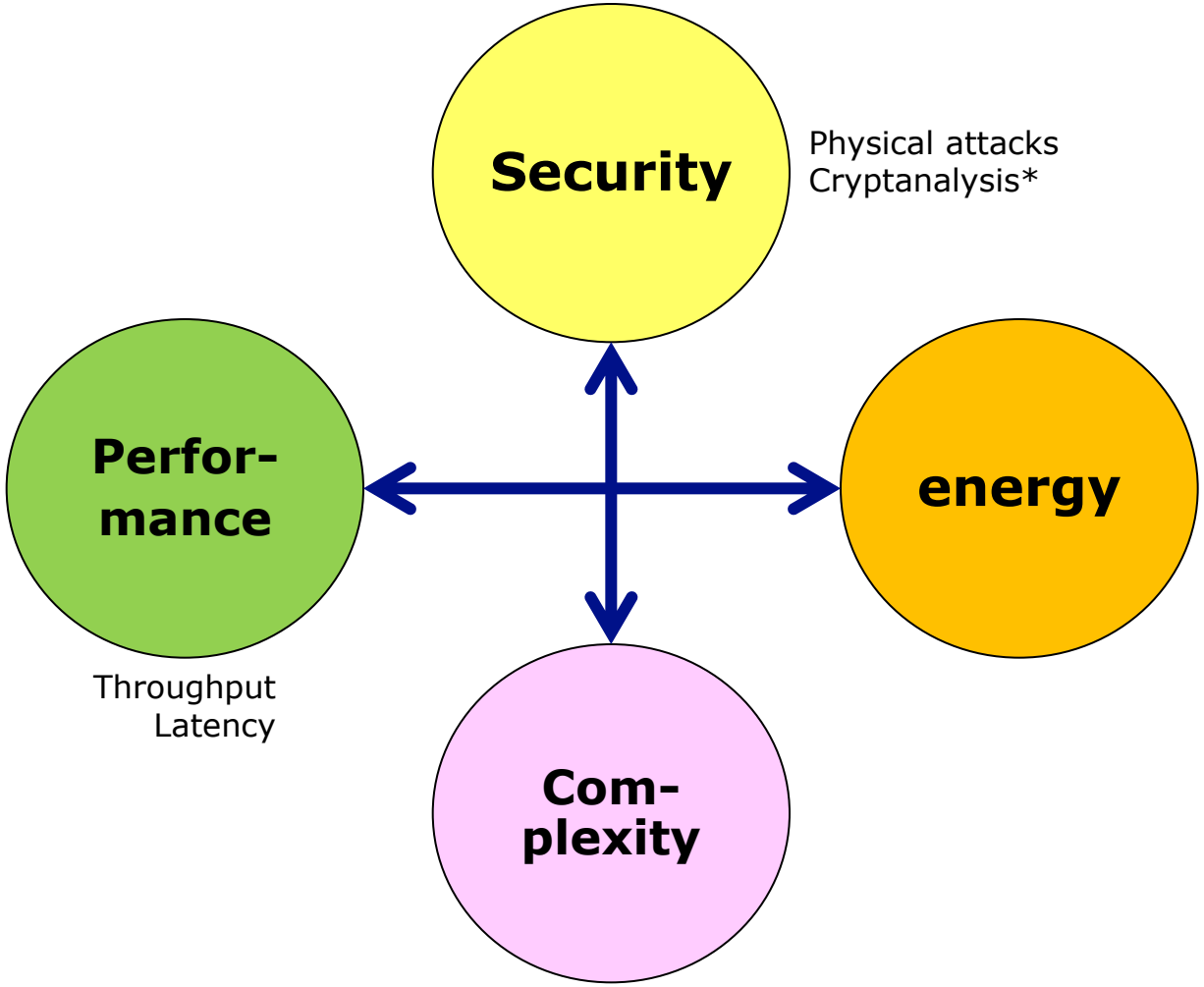
Implementation Trade-offs for Symmetric Cryptography

Jean-Luc Danger
Télécom Paris

Implementation Trade-offs

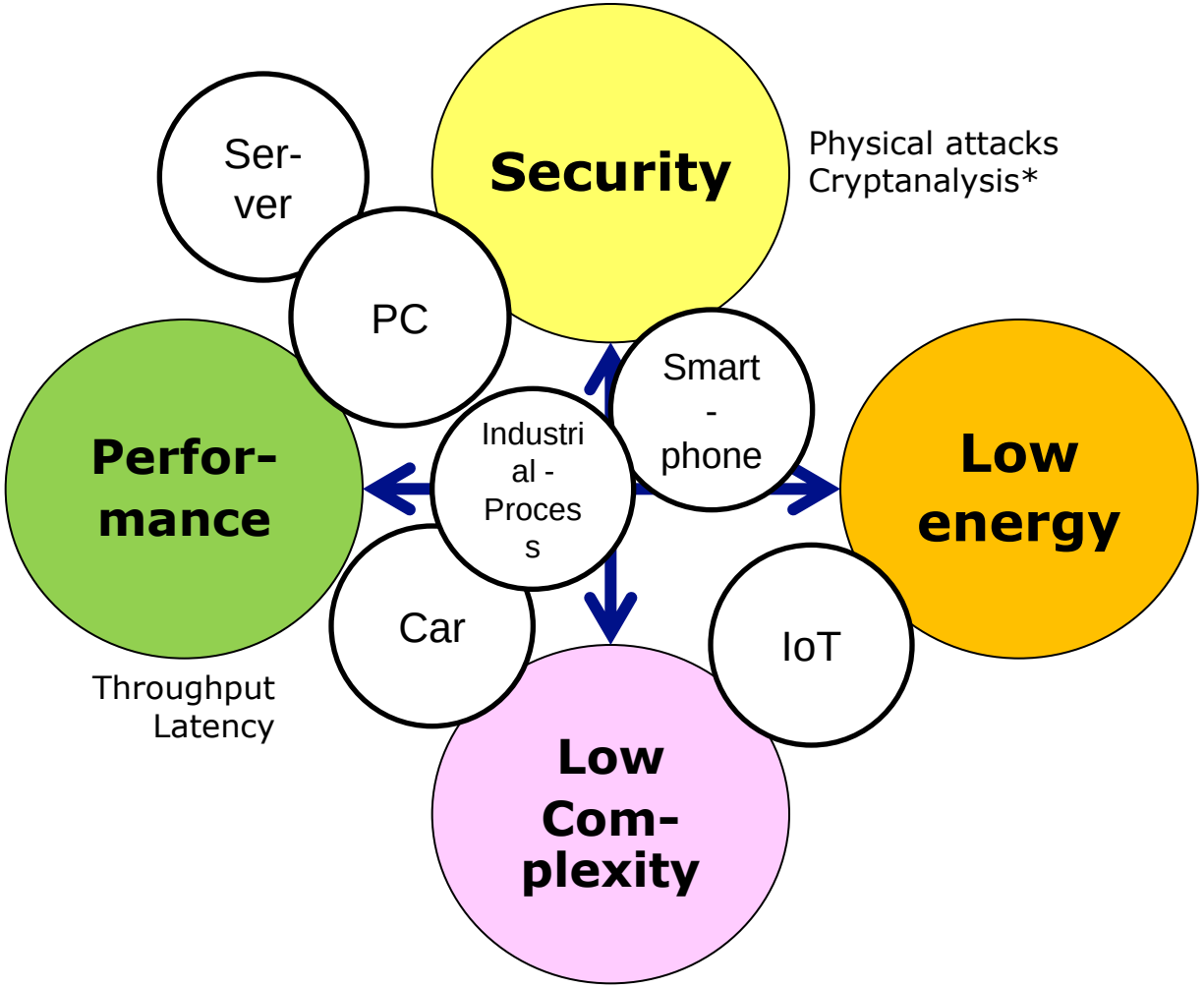


* Depends on algorithm, not implementation

Cryptography type vs applications

- **Classical Cryptography**
  - Servers, PCs, Smartphones
  - Main constraints = security, performance
- **Lightweight cryptography for IoT**
  - Always connected to a network
    - Sensor networks, cars, industrial process...
  - Main constraints = security, complexity
- **Ultra-lightweight cryptography**
  - Temporary connected
    - RFIDs, sensors
  - Main constraints = complexity, energy

Implementation Trade-offs



* Depends on algorithm, not implementation

Software metrics

- **Complexity**
  - Code size
  - Memory
- **Performance**
  - Throughput
  - Latency
- **Energy**
  - nJoule/bit
- **Security**
  - Physical attack resistance : SCA and Fault
    - No metrics, just assesment by succes rate, guessing entropy, fault models…
- **Testbench for lightweight crypto in software : FELICS**

Dinu, D., Biryukov, A., Großschädl, J., Khovratovich, D., Corre, Y. L., & Perrin, L. (2015, July). FELICS–Fair Evaluation of Lightweight Cryptographic Systems. In *NIST Workshop on Lightweight Cryptography*.

Hardware metrics

- **Security**
  - Physical attack resistance : SCA and Fault
    - No metrics, just assesment by succes rate, guessing entropy, fault models
- **Complexity**
  - Gate Equivalent (NAND 4 transistors)
    - e.g. AES 128-bit key => ~2500GE
  - Memory
    - RAM, LUTs
    - Registers
- **Performance**
  - Throughput
    - Block ciphers = clock frequency*nb_bits / nb_rounds
    - Stream ciphers = clock frequency
  - Latency
- **Energy**
  - pJoule/bit

Hardware vs Software

- **Hardware is always better**
  - Parallelism => more throughput and less latency
  - Energy : at least 20 times lower in HW
  - Security : more side-channel attacks in SW
    - Many leakage points for DPA
    - Great SNR
    - Cache attacks

	SW-XTEA			HW-AES		
Payload [B]	Time [ms]	Throughput [kB/s]	Energy [mJ]	Time [ms]	Throughput [kB/s]	Energy [mJ]
1	2,48	0,39	0,23	0,24	4,03	0,01
15	2,51	5,83	0,23	0,28	53,26	0,01
16	4,99	3,13	0,46	0,52	30,21	0,03
31	5,03	6,02	0,47	0,55	54,82	0,03
32	7,51	4,16	0,69	0,79	39,33	0,04
47	7,55	6,08	0,70	0,83	55,35	0,04
48	10,03	4,68	0,93	1,07	43,75	0,06
63	10,06	6,11	0,94	1,11	55,59	0,06
64	12,54	4,98	1,17	1,35	46,34	0,07
79	12,58	6,13	1,17	1,38	55,74	0,07
80	15,05	5,19	1,40	1,63	48,04	0,08
95	15,09	6,15	1,40	1,66	55,86	0,09
96	17,57	5,34	1,63	1,90	49,26	0,10
104	17,59	5,77	1,64	1,92	52,85	0,10

Botta, M., Simek, M., & Mitton, N. (2013, July). Comparison of hardware and software based encryption for secure communication in wireless sensor networks. In *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on* (pp. 6-10). IEEE.

Lightweight Crypto type SPN

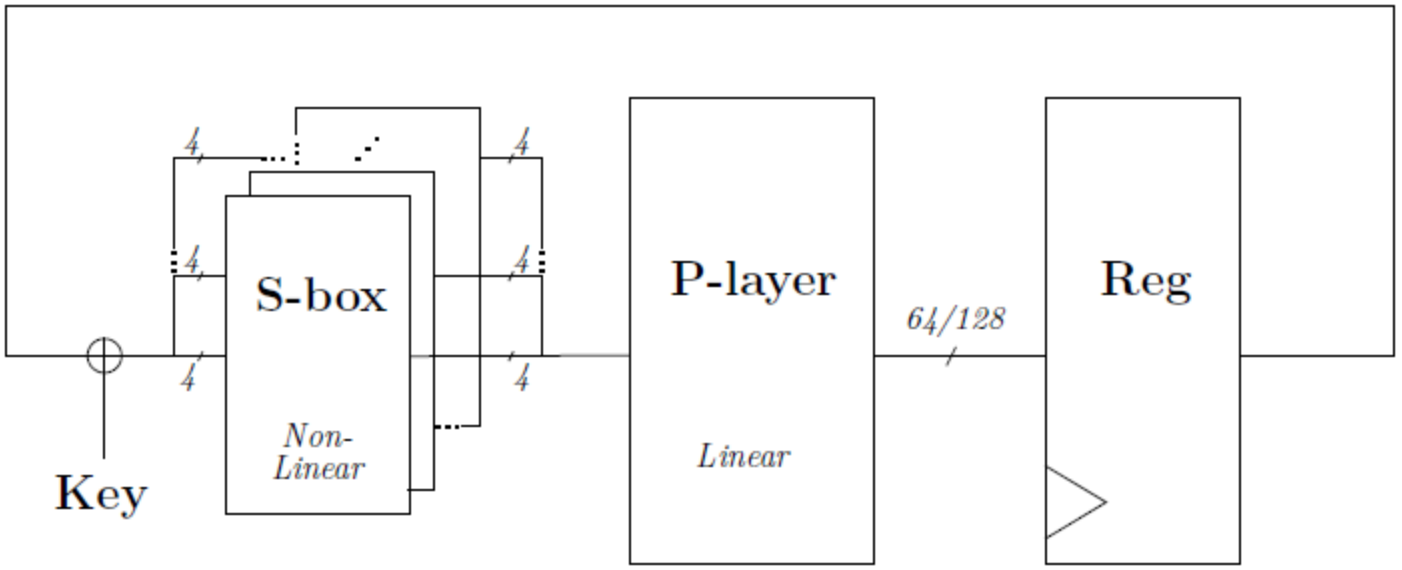


Figure 1: Generic iterated round function (SPN structure)

SPN with α reflexion

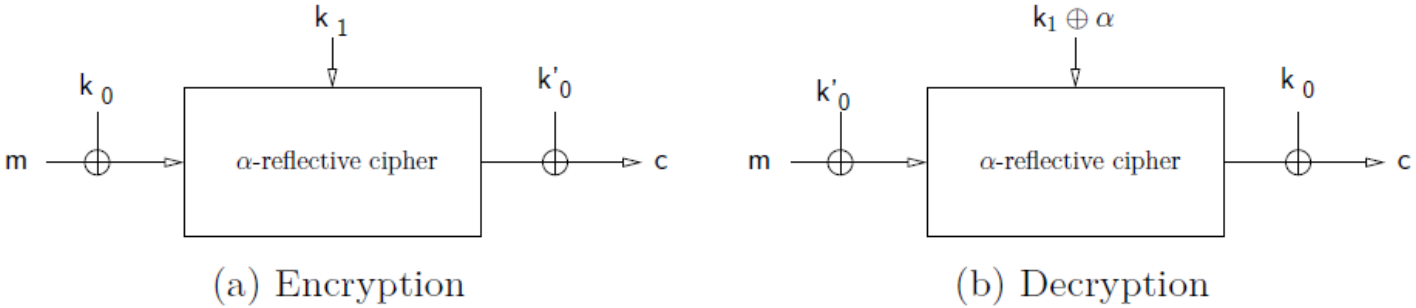


Figure 2: α-reflective ciphers for encryption and decryption

Lightweight Crypto type Feistel

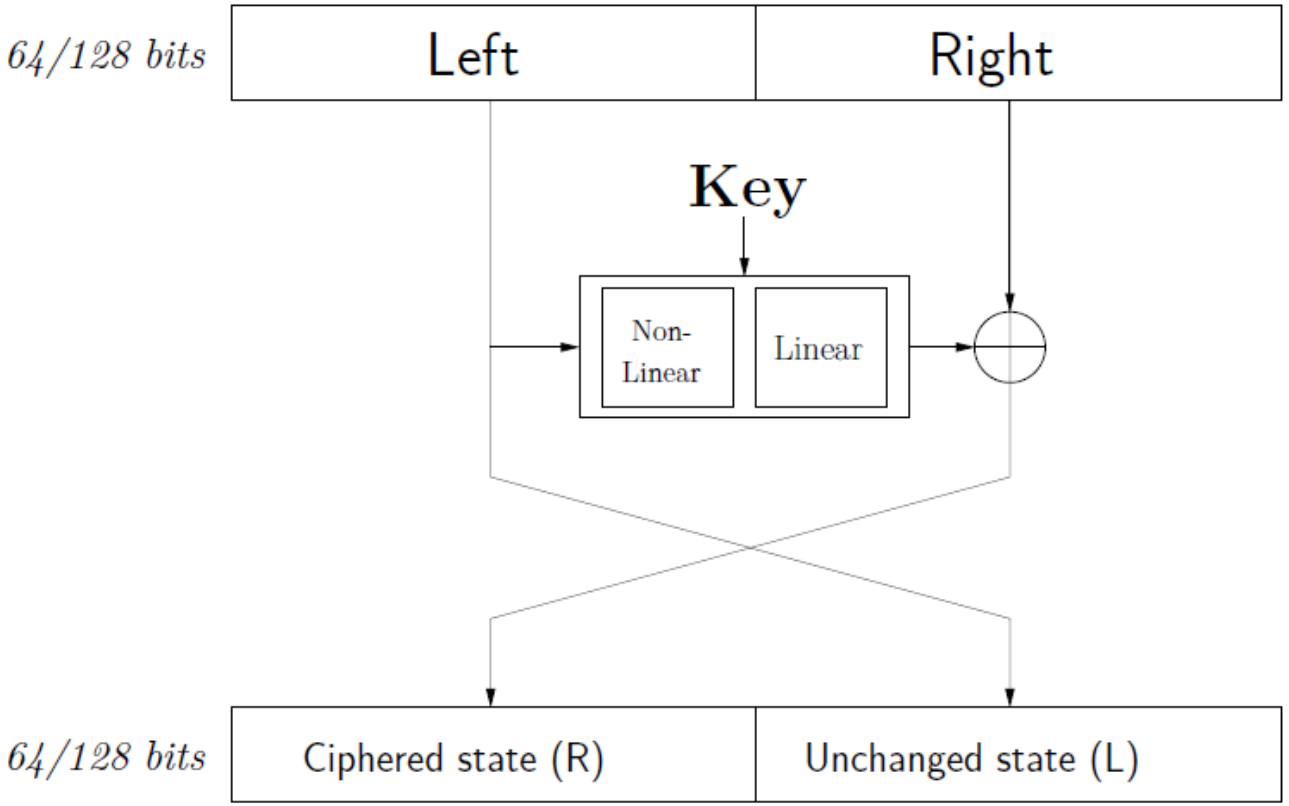


Figure 3: Generic Feistel Round

Summary of common Lightweight Crypto

Cipher	Block size	Type	Rounds	E/ED	Key Process	Focus
PRINCE	64	SPNα	12	SHW	KExp	Latency
NOEKEON	128	SPN	16	SHW	KS	Area
Piccolo	64	GFN	33	SHW	KS	Energy
Midori	64	SPN	16	MDO	None	Energy
	128	SPN	20	MDO	None	Energy
SIMON	64	Feistel	44	SHW	KS	Area
	128	Feistel	68	SHW	KS	Area
Speck	64	Feistel	27	SHW	KS	Area
	128	Feistel	32	SHW	KS	Area
SKINNY	64	SPN	32	MDO	Tweak	Area
	128	SPN	40	MDO	Tweak	Area
LED	64	SPN	48	-	None	Area
Mantis	64	SPNα	14	SHW	Tweak	Latency
PRESENT	64	SPN	32	MOp	KS	Area
GIFT	64	SPN	28	MOp	KS	Area
	128	SPN	40	MOp	KS	Area

Table 1: Summary of properties of Lightweight block ciphers

Stage TPT Etienne Tehrani

Complexity comparison 1

Table 1. Hardware implementation results of selected symmetric encryption algorithms.

Algorithm		key size	block size	cycles/ block	Tech. [μm]	Area [GE]
Stream Ciphers						
Trivium	[13]	80	1	1	0.13	2,599
Grain	[13]	80	1	1	0.13	1,294
Block Ciphers						
PRESENT	[36]	80	64	547	0.18	1,075
SEA	[23]	96	96	93	0.13	3,758
mCrypton	[6]	96	64	13	0.13	2,681
ICEBERG	[23]	128	64	16	0.13	7,732
HIGHT	[16]	128	64	34	0.25	3,048
AES	[10]	128	128	1,032	0.35	3,400
AES	[14]	128	128	160	0.13	3,100
DESXL	[22]	184	64	144	0.18	2,168

Poschmann, A., Moradi, A., Khoo, K., Lim, C. W., Wang, H., & Ling, S. (2011). Side-channel resistant crypto for less than 2,300 GE. *Journal of Cryptology*, *24*(2), 322-345.

Complexity Example 2 with 64-bit blocks

Cipher	Ref.	Tech (nm)	Architecture (cycle/round)	Area (GE)	Latency (ns)	TPmax (Gbps)	TP@100kHz (kbps)
Block size : 64-bit							
PRINCE	[7]	90	1/32	7996	13.9	4.56	-
PRESENT	[3]	90	32/32	1560	52.16	1.23	-
LED	[8]	180	48/48	1265	-	-	3.4
Midori64	[2]	90	16/16	2450	33.92	1.89	-
Piccolo	[10]	130	33/33	1362	-	-	12.12
	[10]	130	2112/33	818	-	-	193.94
SIMON 64	[4]	130	44/44	1417	-	-	133.3
	[3]	90	44/44	1458	-	80.52	0.79
Speck-64	[4]	130	27/27	1658	-	-	206.5
SKINNY 64	[5]	180	32/32	1696	59.84	0.95	177.78
	[5]	180	1/32	17454	51.59	1.24	6400
	[5]	180	128/32	1399	121.60	0.09	8.12
	[5]	180	2048/32	1172	2170.88	0.02	2.03
	[3]	90	32/32	1477	58.88	0.96	-
Mantis7	[5]	180	1/14	11209	20.5	3.12	-
	[5]	180	1/14	23926	11.0	5.82	-
GIFT-64	[3]	90	28/28	1345	51.24	1.25	-
	[3]	90	112/28	1113	239.68	0.06	-
	[3]	90	2048/32	930	4784.64	0.01	-

Table 2: Comparison of Area and Latency for 64-bit block size unrolled, round and serialized implementations of Lightweight block ciphers

Complexity Example 2 with 128-bit blocks

Cipher	Ref.	Tech (nm)	Architecture (cycle/round)	Area (GE)	Latency (ns)	TPmax Gbps	TP@100kHz kbps
Block size : 128-bit							
Midori128	[2]	90	20/20	3661	48.80	2.62	-
Speck-128	[4]	130	32/32	2727	-	-	376.5
SIMON 128	[4]	130	68/68	2090	-	-	182.9
	[3]	90	68/68	2064	127.16	1.01	-
SKINNY 128	[5]	180	40/40	2391	115.60	1.11	320.00
	[5]	180	1/40	32415	97.93	1.31	12800
	[5]	180	320/40	1840	329.60	0.14	14.68
	[5]	180	5120/40	1481	5376.00	0.02	1.83
	[3]	90	40/40	2104	74.00	1.73	-
GIFT-128	[3]	90	40/40	1997	74.00	1.73	-
	[3]	90	160/40	1455	360.00	0.08	-
	[3]	90	5120/40	1213	12595.20	0.01	-

Table 3: Comparison of Area and Latency for 128-bit block size unrolled, round and serialized implementations of Lightweight block ciphers

Stage TPT Etienne Tehrani

Complexity vs throughput vs latency

- **Complexity ~ a . throughput**
  - Example with AES-128
    - Complexity = 10 rounds (unrolled with pipeline) => rate = F
    - Complexity = 1 round => rate = F/10
    - Complexity =¼ round (with 32 bits) => rate = F/40
- **Complexity $^{-1}$ latency**
  - Example with AES-128
    - Complexity = 10 rounds (unrolled with pipeline) => latency = 10/F
    - Complexity = 1 round => latency = 10/F
    - Complexity =¼ round (with 32 bits) => latency = 40/F

Energy

- Very Important for lightweight cryptography
- Highly depends on complexity and glitches

Table 2: Energy consumption per byte for software implementations.

Software Implementations			
Primitive	**Type**	**Platform**	E_n **(nJ/byte)**
Chaskey fast [13]	MAC	ARM M0/STM32F030R8	21.4
Chaskey compact [13]	MAC	ARM M0/STM32F030R8	19.8
Speck 64 bit block [14]	block cipher	ATtiny45	214
Speck 128 bit block [14]	block cipher	ATtiny45	252
Simon 64 bit block [14]	block cipher	ATtiny45	394
Simon 128 bit block [14]	block cipher	ATtiny45	604
AES-128 fast [15]	block cipher	AT90USB162	1,031
AES-128 compact [15]	block cipher	AT90USB646	1,114
DESXL [16]	block cipher	ATmega128	8,830
PRESENT-80 [16]	block cipher	ATmega128	11,099
Lesamnta-LW [17]	hash	8 bit Renesas H8	14,948
D-QUARK [18]	hash	ATtiny45	39,919
PHOTON-160 [18]	hash	ATtiny45	43,560
SPONGENT-160 [18]	hash	ATtiny45	75,050

P; Conr, P. Schaumont :"the role of energy in the lightweight cryptographic profile", NIST document

Energy in HW implementation

Table 4: Absolute energy consumption per byte for block cipher hardware implementations from [27, 28].

Block Cipher Hardware Implementations	
STM 90 nm, 10 MHz [27]	
Block Cipher	E_n **(pJ/byte)**
Midori-128	11.7
PRINCE	18.1
NOEKEON	21.1
PRESENT	21.5
AES	21.9
SIMON 128/128	41.5
UMC 0.130 µm, 100 KHz [28]	
Block Cipher	E_n **(pJ/byte)**
KLEIN-parallel	105.9
PRINCE	170.4
PRESENT	189.5
LED	477.6
CLEFIA	566.2
KATAN-64	793.7
AES	389.0 - 2315.8

More than 1000 times lower than SW

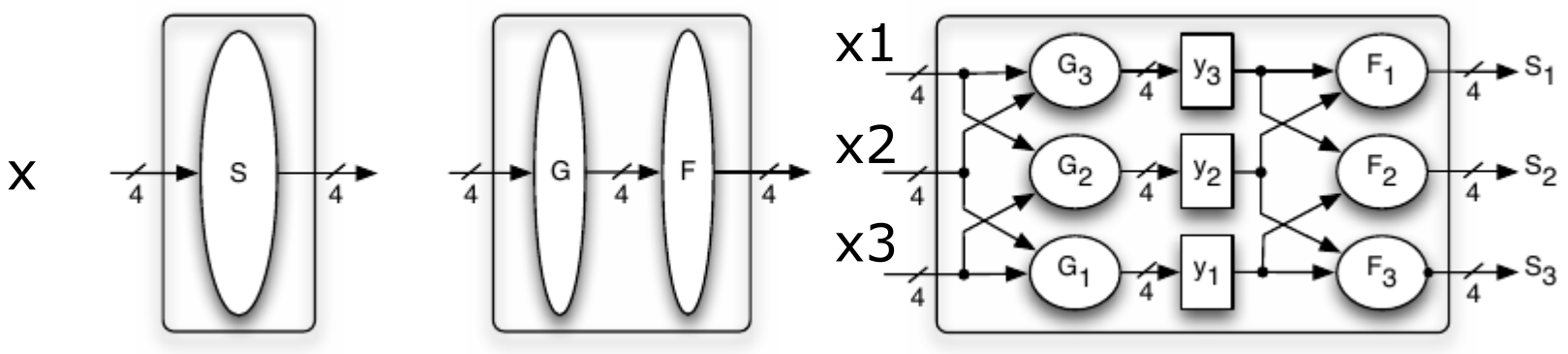
P; Conr, P. Schaumont :"the role of energy in the lightweight cryptographic profile", NIST document

Security

- **Cryptanalysis**
  - Depends only on the algorithm
  - More key bits => more rounds => less throughput
- **Side Channel attack**
  - Protections by hiding or masking => extra complexity, at least x2 in HW, much more in SW
- **Fault Injection attack**
  - Protection by redundancy
    - Spatial => complexity at least x2
    - Temporal => performance at least /2

Example of masking protection: Threshold Implementation*

- **Proven protection against 1st order SCA**
  - Use of 3 shares



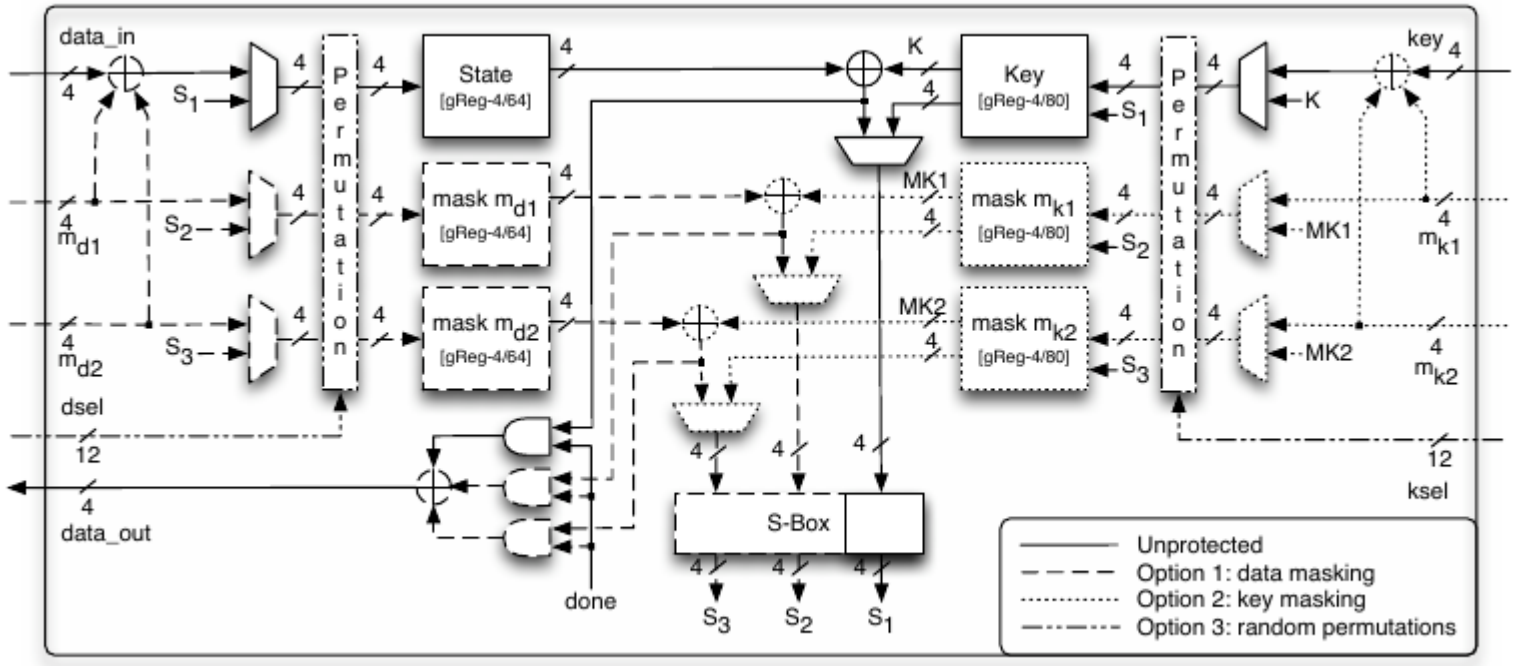
$x = x1 \oplus x2 \oplus x3$ (x2 ⊕ x3: random)

$s = s1 \oplus s2 \oplus s3$

*Nikova, S., Rechberger, C., & Rijmen, V. (2006, December). Threshold implementations against side-channel attacks and glitches. In *International Conference on Information and Communications Security* (pp. 529-545). Springer Berlin Heidelberg.

Example of masking protection: Threshold Implementation*

- **Overall architecture**



TI results

Profile	Sharing Data [Y/N]	Sharing Key [Y/N]	Rand. Perm. [Y/N]	Cycles total [clk]	Cycles rel. [%]	Current total [μA]	Current rel. [%]	Area total [GE]	Area rel. [%]
1	N	N	N	547	100	1.34	100	1,111	100
2	Y	N	N	547	100	2.86	213	2,282	205
3	Y	N	Y	547	100	3.10	231	2,417	218
4	Y	Y	N	578	106	4.23	316	3,322	299
5	Y	Y	Y	578	106	5.02	375	3,582	322

Table 4. Breakdown of the post-synthesis implementation results of different architectures of a serialized PRESENT-80. P stands for Profile.

P	m_{d1} m_{d2} %	m_{d1} m_{d2} GE	m_{k1} m_{k2} %	m_{k1} m_{k2} GE	Rand. Perm. %	Rand. Perm. GE	S-box %	S-box GE	FSM %	FSM GE	State %	State GE	Key %	Key GE	other %	other GE	Sum GE	rel. %
1	0	0	0	0	0	0	3	32	13	145	35	389	45	498	4	47	1,111	100
2	34	778	0	0	0	0	17	387	6	146	17	389	22	498	3	75	2,282	205
3	32	778	0	0	5	121	16	387	6	146	16	389	21	498	4	98	2,417	218
4	23	778	29	970	0	0	11	355	5	156	12	389	15	498	5	176	3,322	299
5	22	778	27	970	7	243	10	355	4	155	11	389	14	498	5	194	3,582	322

Complexity x3

Poschmann, A., Moradi, A., Khoo, K., Lim, C. W., Wang, H., & Ling, S. (2011). Side-channel resistant crypto for less than 2,300 GE. *Journal of Cryptology*, *24*(2), 322-345.

Conclusion

- **The implementation is more important as the algorithm itself, to meet all the properties of:**
  - Security
  - Performance
  - low energy
  - complexity
- **Especially for lightweight cryptography**
- **HW is always better than SW**