Horst-Görtz Institut
für IT Sicherheit

Lightweight Cryptography

From an Engineers Perspective

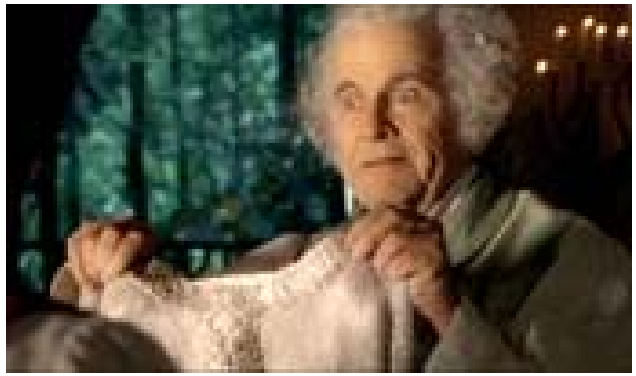
Axel Poschmann

ECC 2007

Acknowledgement

- Christof Paar
- A. Bogdanov, L. Knudsen, G. Leander, M. Robshaw, Y. Seurin, C. Vikkelsoe
- S. Kumar

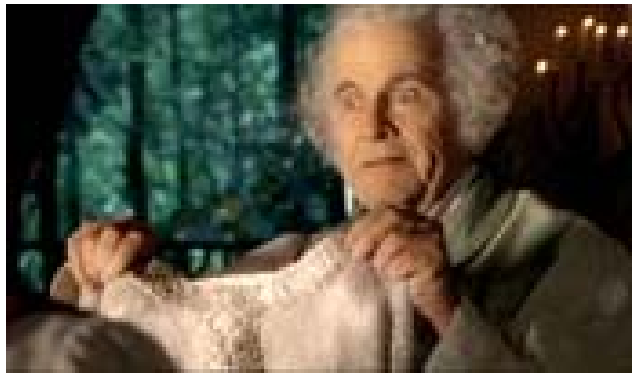
Outline



- Motivation
- Hardware vs. Software
- Symmetric Lightweight Cryptography
- Asymmetric Lightweight Cryptography
- Conclusion

What is Lightweight Cryptography?

"As light as a feather and as hard as dragon scales"



[Gligor05]:

- Cryptography tailored to (extremely) constrained devices
- Not weak crypto
- Not intended for all-powerful adversaries
- Not intended to replace traditional cryptography
  - But LWC should influence new algorithms
- Also dubbed low-cost cryptography (Robshaw)

Why Lightweight?

past | present | future

Mainframe (n : 1) | Personal (1 : 1) | Pervasive (1 : n)

Pervasive = wireless + embedded + cheap = ASIC
= constrained in CPU, memory, battery

Standard vs. Lightweight Cryptography

Horst-Görtz Institut für IT Sicherheit

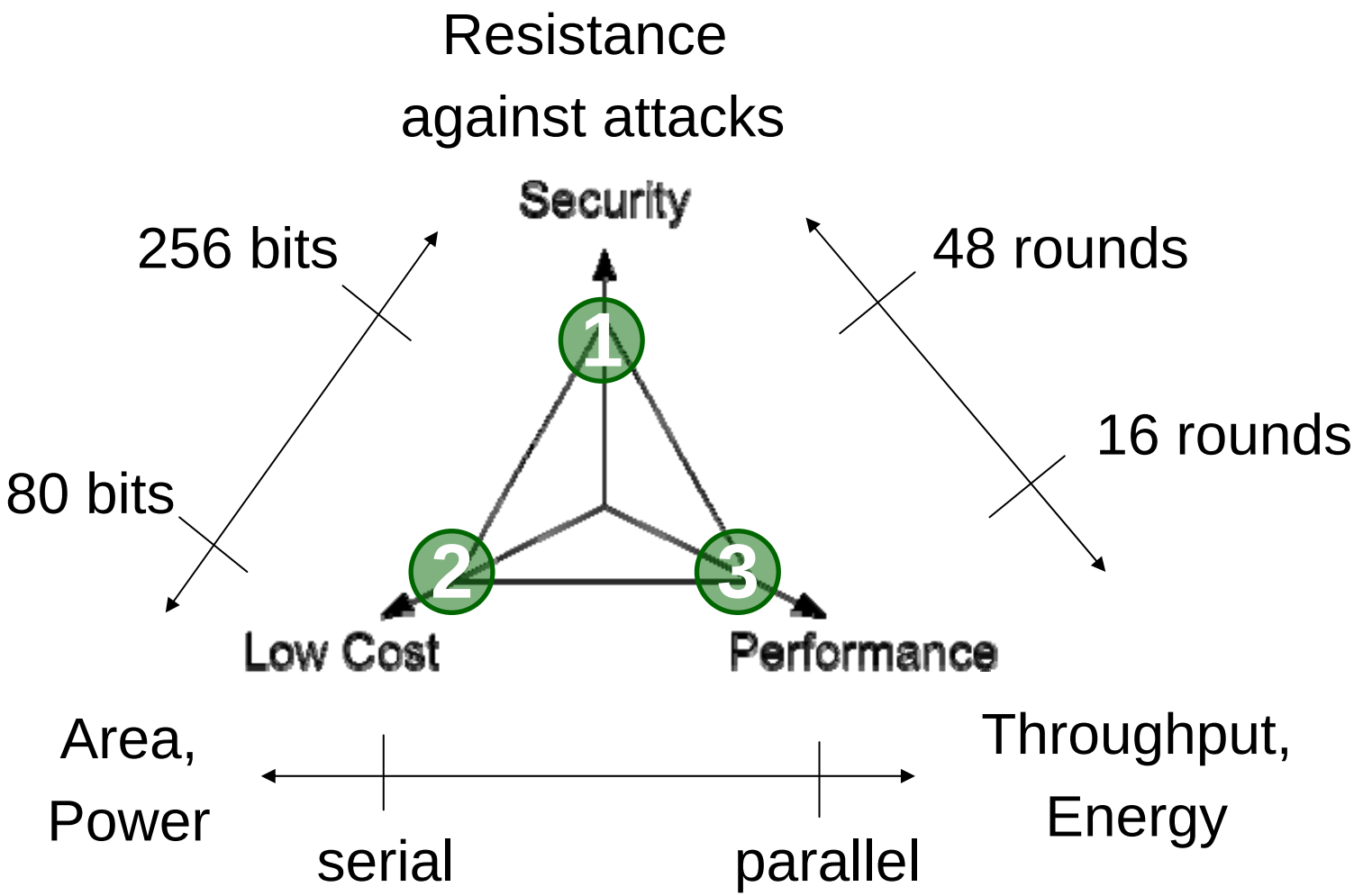
	Standard	vs.	Lightweight
App. scenario:	Server		RFID
Throughput:	High		Low
Max. power:	High		Low (few µW)
Price:	High		Low

crypto

=

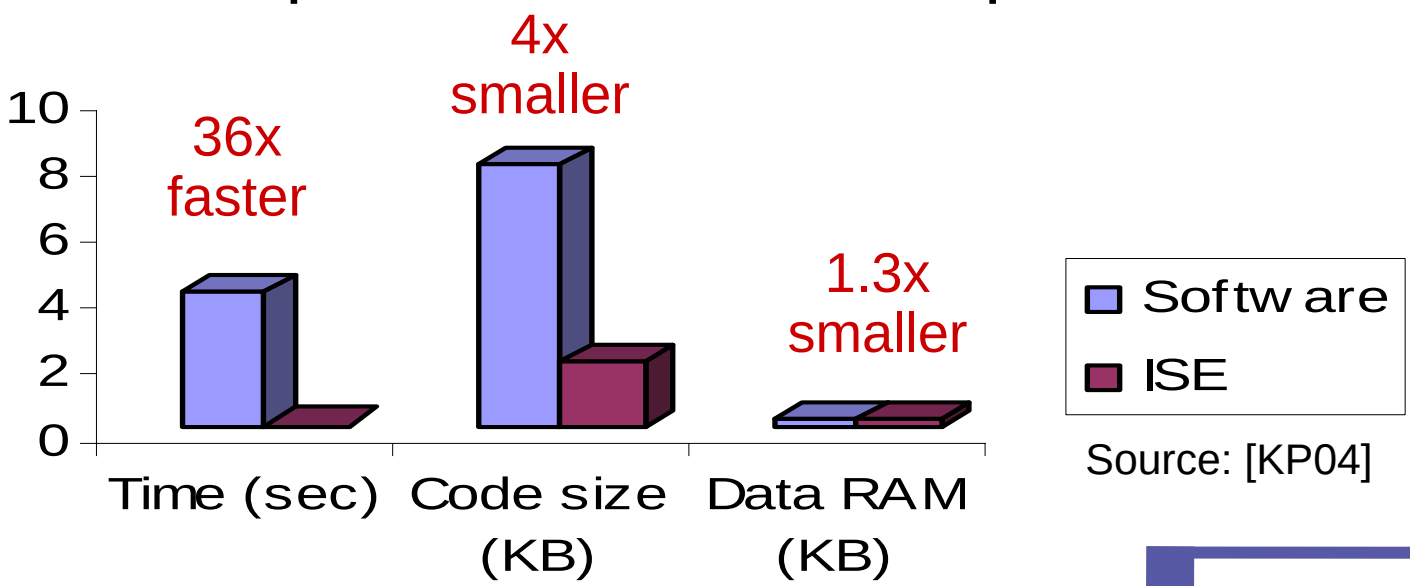
footwear

Metric and Tradeoffs for LWC



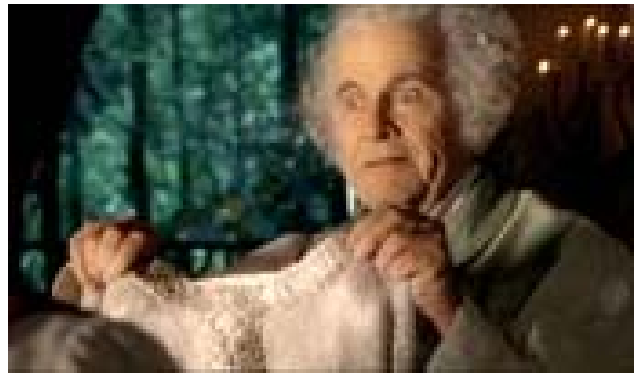
Why Hardware?

- SW is flexible…
- But *pervasive* implies:
  - High volumes => cheap devices
  - Power/Energy constraints
- Example: 160*160 bit multiplication



Source: [KP04]

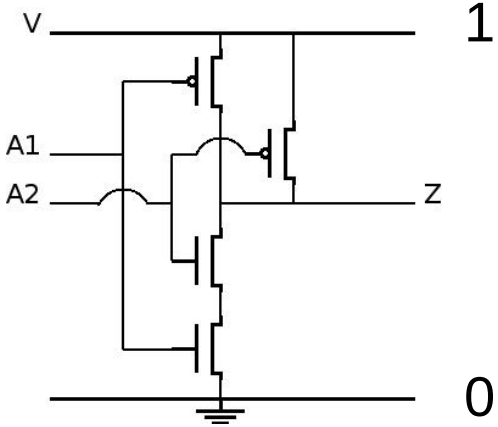
Outline



- Motivation
- Hardware vs. Software
- Symmetric Lightweight Cryptography
- Asymmetric Lightweight Cryptography
- Conclusion

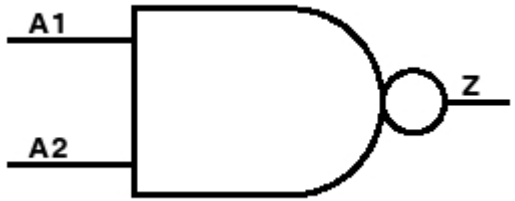
Gate Equivalent

NAND



A1	A2	Z
0	0	1
0	1	1
1	0	1
1	1	0

Standard Cells UMCL18G212T3



HDNAN2D1
9.677 µm²

1 GE

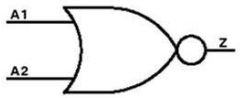
Athlon XP

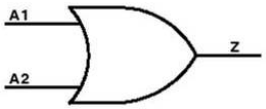
13.24 Mio GE

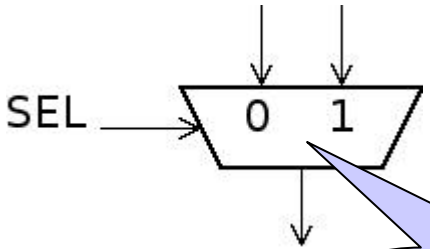
Note for Mathematicians:
NAND + constants = base

Basic Gates

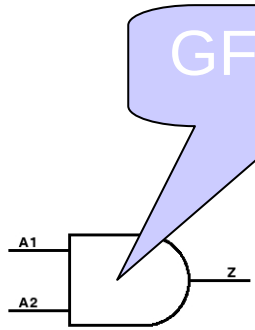
Gate	GE
NOT	0.5
NOR	1
AND	1.33
OR	1.33
XOR	2.67
2-1-MUX	2.67



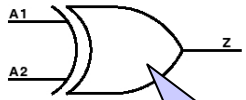




If(sel)

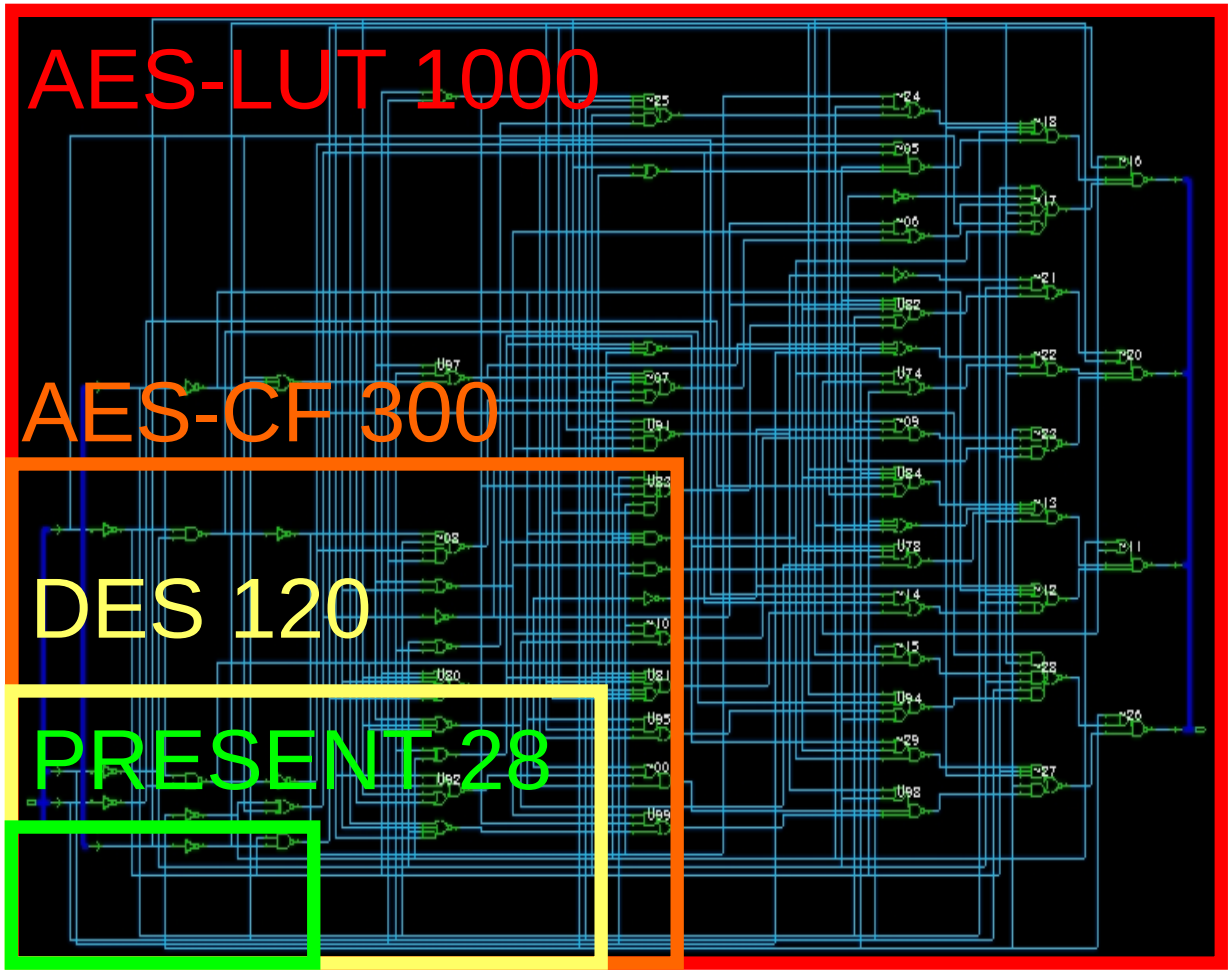


GF(2) MUL



GF(2) ADD

S-Boxes in Hardware



- LUT are realized as boolean functions
- Highly non-linear
- High boolean complexity
- Big area

8 x 8

6 x 4

4 x 4

S-Boxes in Software

Horst-Görtz Institut für IT Sicherheit

		SW	HW
8 x 8	const uint8_t AES_Sbox[256] = { .... }; 256 B ROM		
6 x 4	const uint8_t DES_SBox[64] = { ... }; 64 B ROM		
4 x 4	const uint8_t PRESENT_Sbox[16] = { ... }; 16 B ROM		

PRESENT Permutation

Hardware

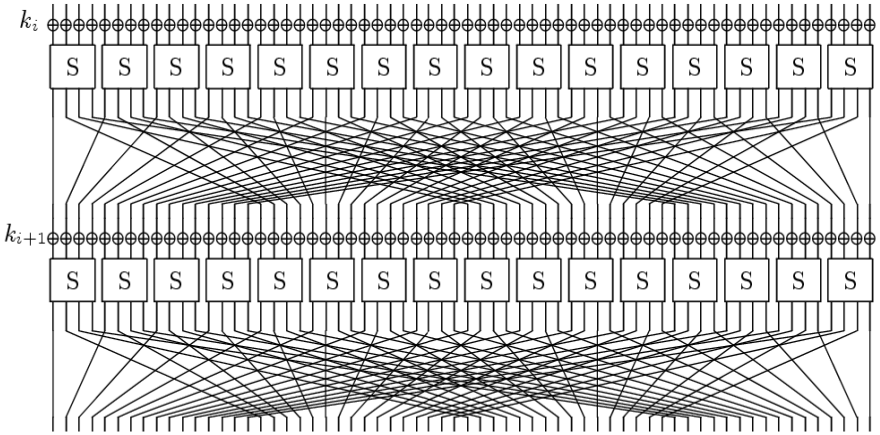


Fig. 1. . The S/P network for PRESENT.

- Just wires
- No delay
- **0 GE** (some wiring)

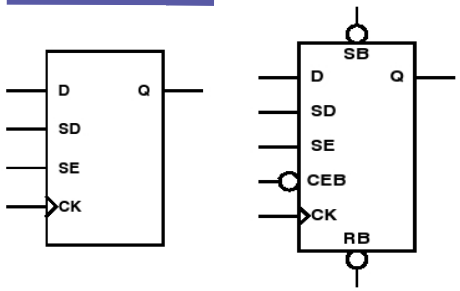
Software

```
for ( PBit = 0, out = 0; PBit<64; PBit++ )
{
        out = rotate1l_64(out);
        out |= ( ( text >> 63-Pbox[PBit] ) & 1 );
}

const uint8_t Pbox[64] =
{
0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60,
 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49,53, 57, 61,
 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46,50, 54, 58, 62,
 3, 7, 11, 15, 19, 23, 27, 31,35, 39, 43, 47, 51, 55, 59, 63
};
```

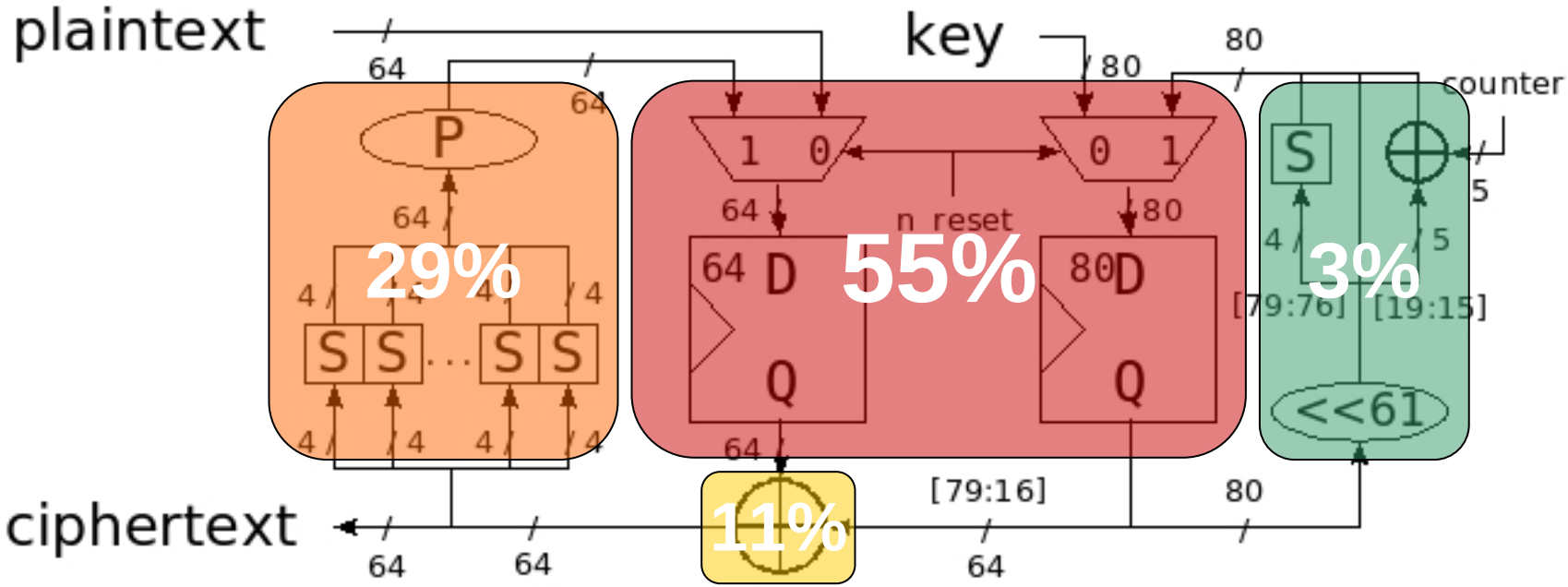
- Cumbersome bit operations
- 64 cycles
- 64 B ROM

Flipflops/Register



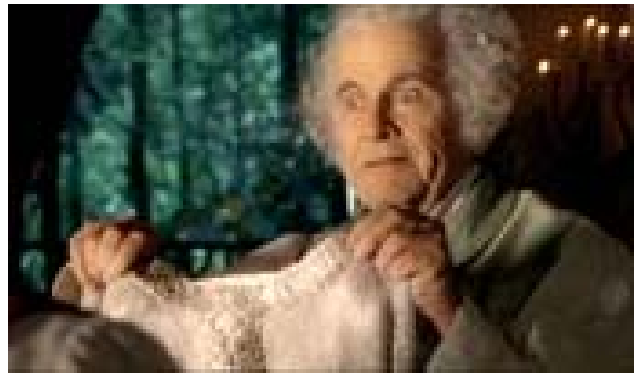
6 - 12 GE per bit

Minimum:
state (64) + key (80) = 144*6 = 864 GE



Storage is very expensive in HW

Outline

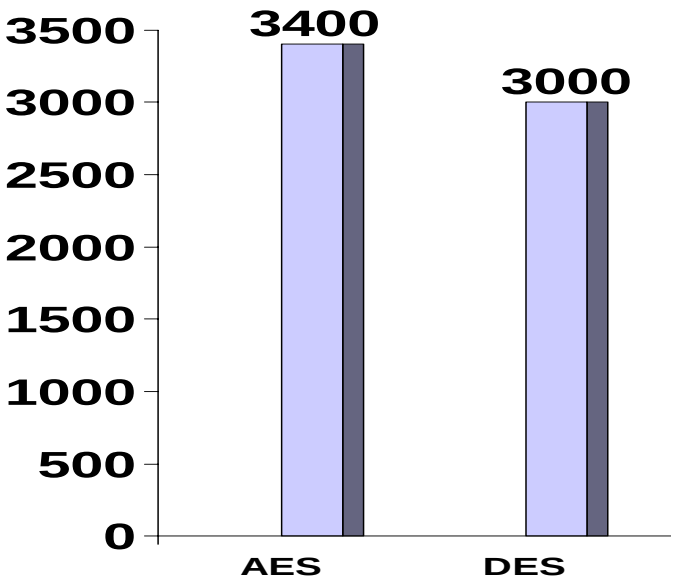


- Motivation
- Hardware vs. Software
- Symmetric Lightweight Cryptography
- Asymmetric Lightweight Cryptography
- Conclusion

Evolution of LW Block Ciphers

Starting Point

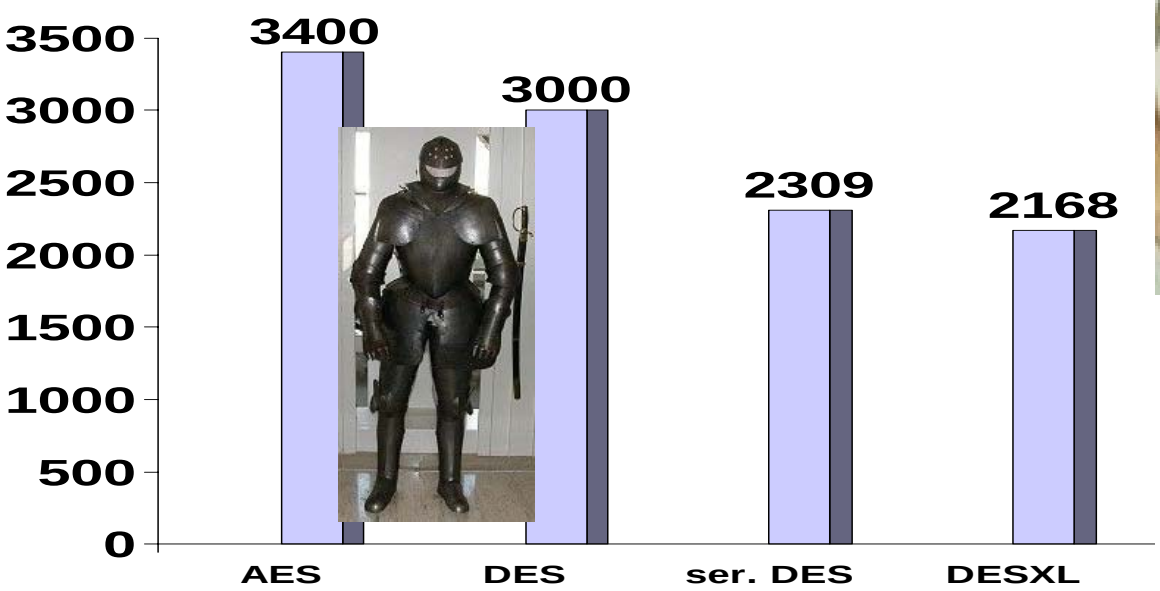
- AES [FWR05]
- DES [VHV+88]



Evolution of LW Block Ciphers

Horst-Görtz Institut für IT Sicherheit

1. Step: Serialization
- Serialized DES [LPP+07]
2. Step: new S-layer
- DESXL [LPP+07]



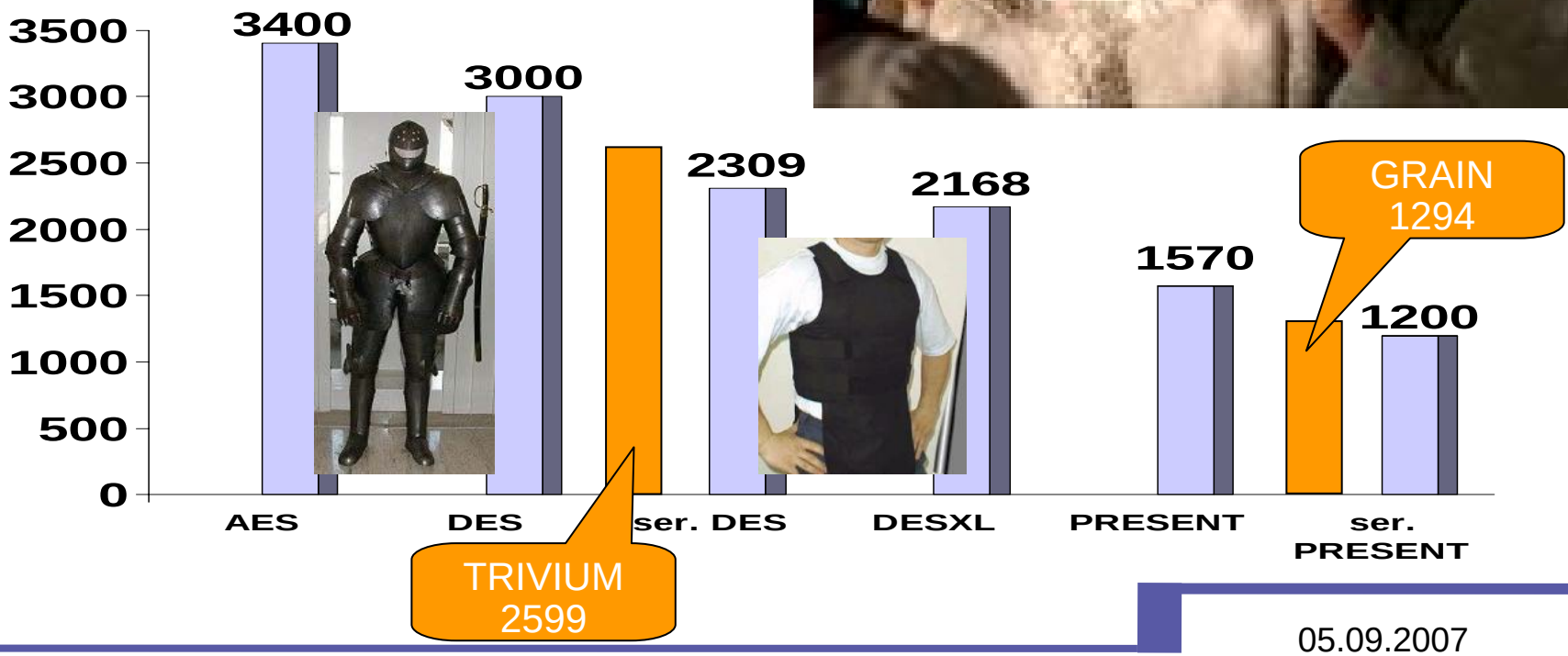
Evolution of LW Block Ciphers

3. step: new cipher

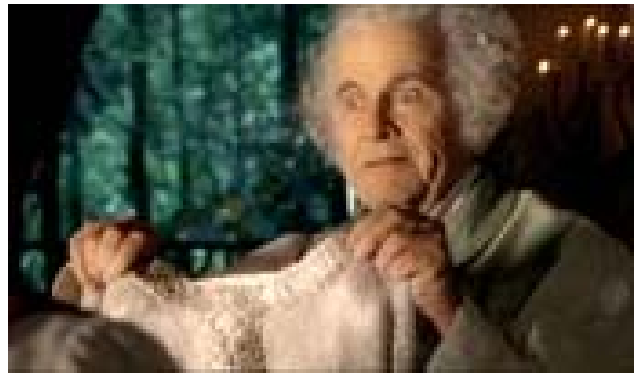
- PRESENT [BKL+07]

Next step.

- Serialized PRESENT

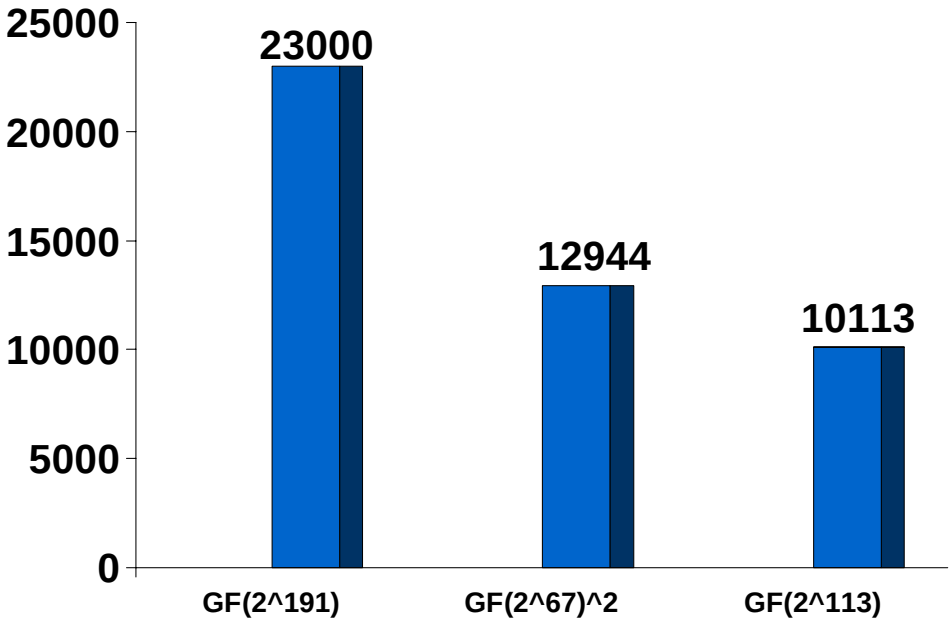


Outline

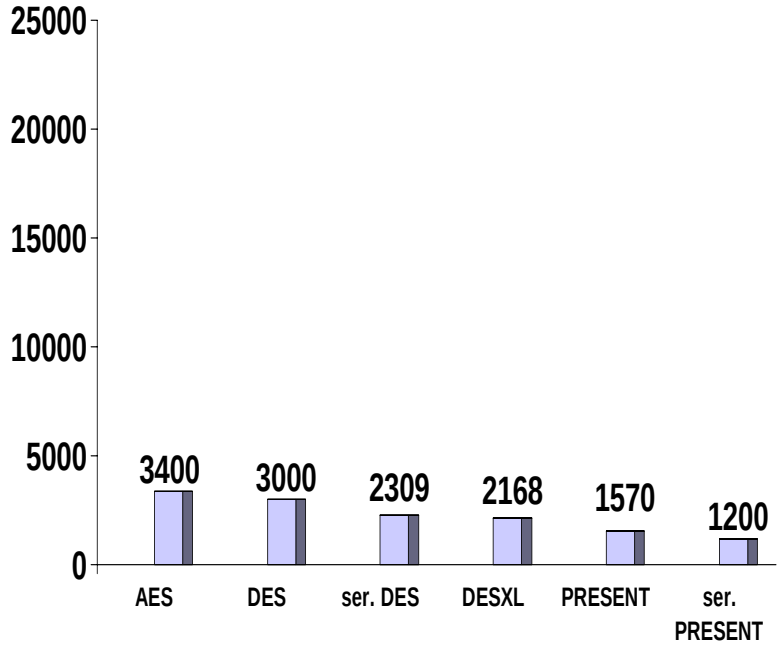


- Motivation
- Hardware vs. Software
- Symmetric Lightweight Cryptography
- Asymmetric Lightweight Cryptography
- Conclusion

ECC Implementations



[W04] [BGK+07] [KP06]



ECC 5-10 x bigger than block ciphers

Alternatives?

- NTRU
  - Very efficient in HW 3000 GE
  - Not yet stable => flexibility required
- MQ Algorithms
  - Yet another MQ algorithm broken (SFLASH 2007)
  - Have huge keys
  - eTTS 1KB
  - Quartz 70KB!!! => high storage effort => expensive

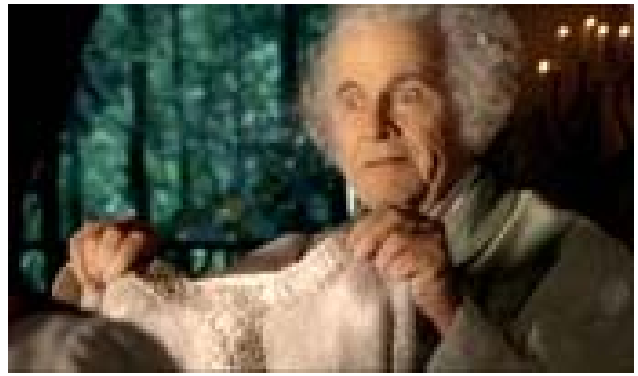
Why ECC?

ECC…

- Has short key length
- Has short processing time on 8-bit µC
- Has short signatures

ECC is best suited for pervasive computing

Outline



- Motivation
- Hardware vs. Software
- Symmetric Lightweight Cryptography
- Asymmetric Lightweight Cryptography
- Conclusion

Conclusion

- Pervasive Computing implies severe constraints:
  - Small area
  - Low power
  - Low energy
  - Short messages
- S-boxes are expensive in HW…
- …but cheap in SW (smaller are better)
- Permutations can be very efficient in HW…
- …and very cumbersome in SW
- Storage is the most expensive part in hardware

Conclusion

- Lightweight algorithms should…
  - Have a short internal state (to lower area)
  - Allow serialization (to lower power)
  - Have a short processing time (to lower energy)
  - Have a short output (to lower communication cost)
  - Should be based on the same primitive
- Lightweight block ciphers have similar footprint as stream ciphers
- NTRU might be an alternative to ECC if it becomes stable
- ECC is best suited for pervasive computing

References

[FWR05] M. Feldhofer, J. Wolkerstorfer, V. Rijmen, AES Implementation on a Grain of Sand, Information Security, IEE Proceedings, Vol. 152, Nr. 1, pp. 13-20, 2005

[BKL+07] Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe "PRESENT: An Ultra-Lightweight Block Cipher". Cryptographic Hardware and Embedded Systems - CHES 2007, 9. International Workshop, Vienna, Austria, Proceedings. LNCS, Springer-Verlag, September 10 - 13, 2007

[LPP+07] Leander, C. Paar, A. Poschmann, K. Schramm "New Lightweight DES Variants". Fast Software Encryption 2007 - FSE 2007, Luxembourg City, Luxembourg, März 26-28, 2007.A.

[VHV+88] I. Verbauwhede, F. Hoornaert, J. Vandewalle, and H. De Man. Security and Performance Optimization of a New DES Data Encryption Chip. IEEE Journal of Solid-State Circuits, 23(3):647?656, 1988.

[KP04] Sandeep Kumar, Christof Paar, "Reconfigurable Instruction Set Extension for enabling ECC on an 8-bit Processor", International Conference on Field-Programmable Logic and Applications (FPL) 2004, Antwerp, Belgium, August 30 - September 1, 2004

[KP06] Sandeep Kumar and Christof Paar, Are Standards Compliant Elliptic Curve Cryptosystems feasibe on RFID?, Workshop on RFID Security 2006, Graz, Austria, Juli 2006

[BGK+07] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, ``Public-Key Cryptography for RFID-Tags", Proceedings of IEEE International Workshop on Pervasive Computing and Communication Security 2007, New York, USA 2007

[W04] Johannes Wolkestorfer, Hardware Aspects of Elliptic Curve Cryptography, Phd Thesis, Graz University of Technology, Graz, Austria, 2004

Horst-Görtz Institut
für IT Sicherheit

Thank you!

Questions?

www.crypto.rub.de
poschmann@crypto.rub.de