ECRYPT
http://www.ecrypt.eu.org

Perspectives on Lightweight Cryptography

Bart Preneel
COSIC, K.U.Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be
http://homes.esat.kuleuven.be/~preneel
Inscript 2010, Shanghai, October 2010

1

Information processing

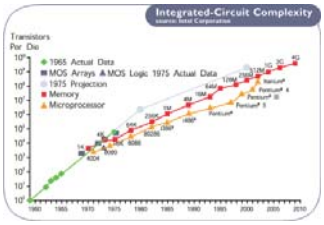
the Internet of things, ubiquitous computing, pervasive computing, ambient intelligence (10^{12})

Internet and mobile (10^9)

PCs and LANs (10^7)

mainframe (10^5)

mechanical (10^4)



2

Information processing

Everything is always connected everywhere

Continuum between software and hardware
ASIC (microcode) – FPGA – fully programmable processor

Research ↔ Practice

DES, RSA, DH, CBC-MAC
Provable security (PKC), ZK, ElGamal, ECC, stream ciphers
Quantum crypto
MD4, MD5
Provable security (SKC)
Key escrow
Quantum cryptanalysis
How to use RSA? Alternatives to RSA
PKI
AES
ID-Based Crypto

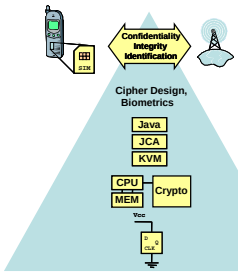
HARDWARE 70
Limited (govt+financial sector)
DES, 3DES 80

SOFTWARE 90
GSM, PGP
C libraries (RSA, DH)
SSL/TLS, IPsec, SSH, S/MIME
Java crypto libraries
WLAN

EVERYWHERE
Trusted computing, DRM, 3GPP, RFID, sensor nodes
…

4

Implementations in embedded systems



Protocol: Wireless authentication protocol design

Algorithm: Embedded fingerprint matching algorithms, crypto algorithms

Architecture: Co-design, HW/SW, SOC

Micro-Architecture: co-processor design

Circuit: Circuit techniques to combat side channel analysis attacks

Technology aware solutions?

Slide credit: Prof. Ingrid Verbauwhede 5

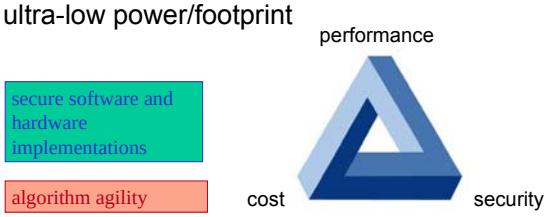
Lightweight crypto design

- Overall protocol crucial
- Security architecture: SK-PK, central-distributed
- Relative cost of computation/communication/storage
- Architectural decisions
  - area
  - clock frequency
  - power consumption and energy
- Flexibility can be sacrificed
- Side channel attacks

6

Challenges for crypto

- security for 50-100 years
- authenticated encryption of Terabit/s networks
- ultra-low power/footprint



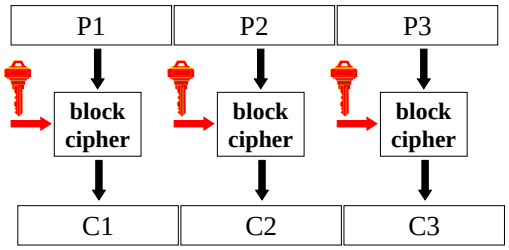
7

Outline

- Context
- Block ciphers
- Stream ciphers
- Hash functions
- (MAC algorithms)
- Public-key cryptography
- Secure implementations

8

Block cipher



- larger data units: 64…128 bits
- memoryless
- repeat simple operation (round) many times

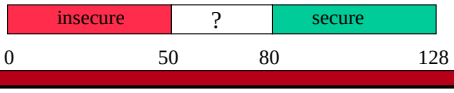
9

Block ciphers

64-bit block	96-bit block	128-bit block
3-DES (112-168)	SEA (96)	AES (128-192-256)
IDEA (128)	PRINTcipher-96 (160)	CAMELLIA
MISTY1 (128)		RC6
KASUMI (128-3G, 64-2G)		CLEFIA
HIGHT (128)		
PRESENT (80-128)		
TEA (128)		
mCRYPTON (96)		
KATAN (80)		

56 bits: 4 seconds with M$ 5
80 bits: 2 year with M$ 5
128 bits: 256 billion years with B$ 5

Symmetric key lengths



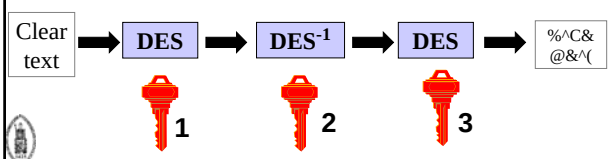
10

3-DES: NIST Spec. Pub. 800-67

(May 2004)

extremely vulnerable to a related key attack

- single DES abandoned (56 bit)
- double DES not good enough (72 bit)
- 2-key triple DES: until 2009 (80 bit)
- 3-key triple DES: until 2030 (100 bit)



11

AES (2001)

- FIPS 197 published on December 2001after 4-year open competition
  - other standards: ISO, IETF, IEEE 802.11,…
- fast adoption in the market
  - except for financial sector
  - NIST validation list: 1492 implementations
    - http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html
- 2003: AES-128 also for classified information and AES-192/-256 for secret and top secret information!
- security:
  - algebraic attacks of [Courtois+02] not effective
  - side channel attacks: cache attacks on unprotected implementations

[Shamir '07] AES may well be the last block cipher

12

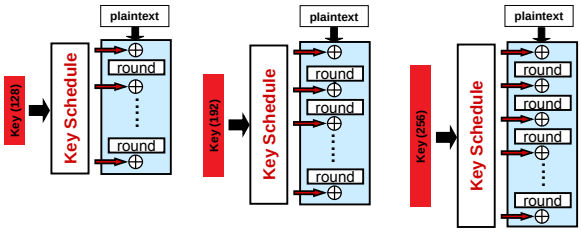
AES implementations: efficient/compact

- HW: 43 Gbit/s in 130 nm CMOS ['05]
- Intel: new AES instruction in Westmere processors 0.75 cycles/byte ['09-'10]
- SW: 7.6 cycles/byte on Core 2 or 110 Mbyte/s bitsliced [Käsper-Schwabe'09]
- HW: most compact: 3600 gates
  - PRESENT: 1029, KATAN: 1054, CLEFIA: 4950

13

AES variants (2001)

- AES-128
  - 10 rounds
  - sensitive
- AES-192
  - 12 rounds
  - classified
- AES-256
  - 14 rounds
  - secret/top secret

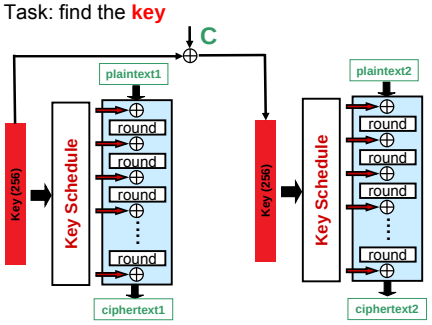


Light weight key schedule, in particular for the 256-bit version

14

What is a related key attack?

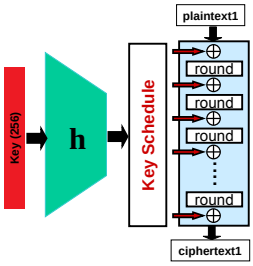
- Attacker chooses **plaintexts** and **key difference** C
- Attacker gets **ciphertexts**
- Task: find the **key**



15

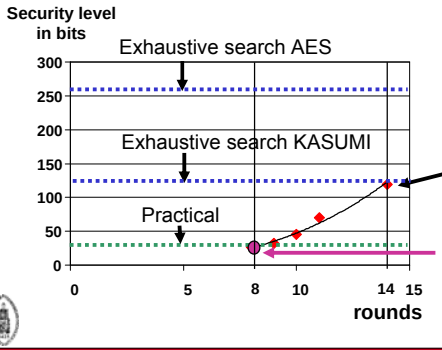
Should I worry about a related key attack?

- Very hard in practice (except some old US banking schemes and IBM control vectors)
- If you are vulnerable to a related key attack, you are making very bad implementation mistakes
- This is a very powerful attack model: if XOR is replaced by AND, any cipher can be broken
- If you are worried, hashing the key is an easy fix



16

Related key attacks on AES-256 and KASUMI



[Biryukov-Khovratovich'09] 4 related keys data & time complexity $2^{119} << 2^{256}$

[Dunkelman-Keller-Shamir'10] Related key attack: 4 keys, 2^{26} data & 2^{32} time $<< 2^{128}$

17

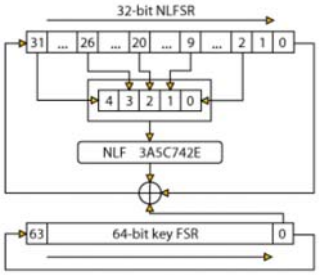
KASUMI (2002)

- Widely used in all 3G phones
- Present in 40% of GSM phones but not yet used
- Good news: related key attacks do not apply in in the GSM or 3G context

18

Keeloq [Smit+/-'85] aka the M$10 cipher

- block length: 32
- key length: 64
- rounds: 528



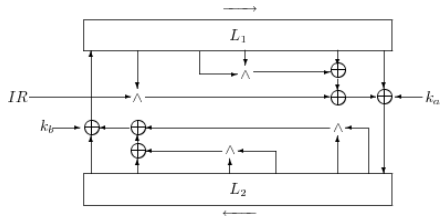
19

KATAN/KTANTAN

[De Cannière-Dunkelman-Knežević'09]
http://www.cs.technion.ac.il/~orrd/KATAN/

- block length: 32, 48, 64
- key length: 80
- rounds: 254

462-1054 gates



20

PRINTcipher

[Knudsen-Leander-Poschmann-Robshaw'10]

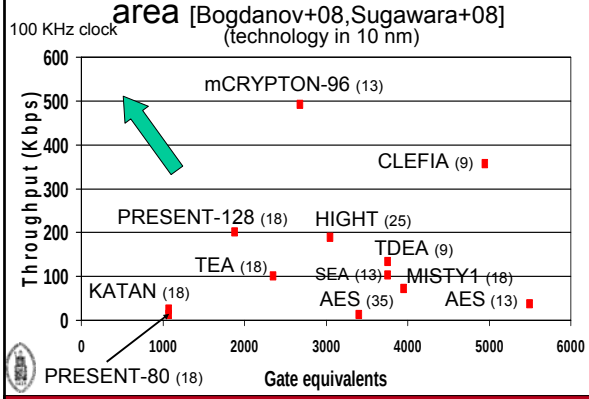
- IC printing technology (different for each print)
- block length: 48, 96
- key length: 80, 160
- rounds: 48, 96
- 3-bit S-boxes
- key-dependent bit-permutations

402-967 gates

21

Low cost hw: throughput versus area [Bogdanov+08,Sugawara+08]

(technology in 10 nm)



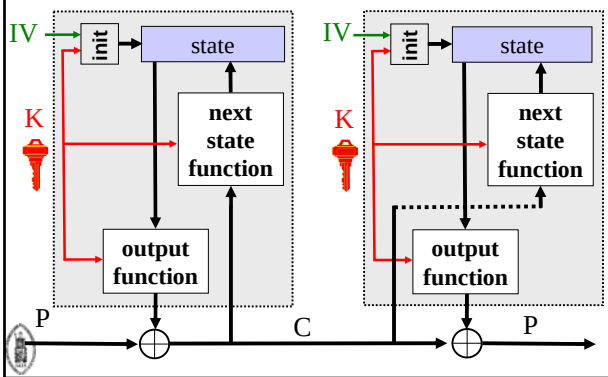
22

Block ciphers: conclusions

- Several mature block ciphers available
- Security well understood
  - in particular against statistical attacks (differential, linear) and structural attacks
- More work:
  - algebraic attacks
  - related key attacks
  - understanding of structural tradeoffs
- What are the limitations for lightweight block ciphers?

23

Self-Synchronising Stream Cipher (SSSC)



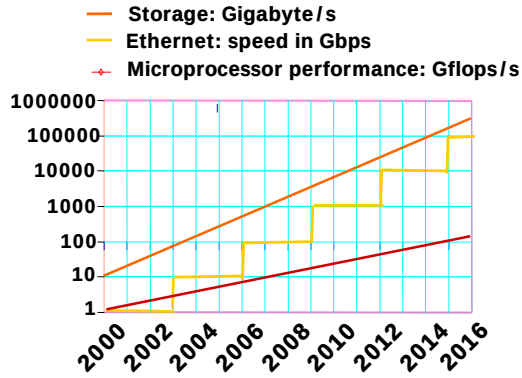
24

Stream ciphers

- historically very important (compact)
  - LFSR-based: A5/1, E0 – practical attacks known
  - software-oriented: RC4 – serious weaknesses
  - block cipher in CTR or OFB (slower)
- today:
  - many broken schemes
  - lack of standards and open solutions
  - standards: SNOW2.0, SNOW3G, MUGI, Rabbit, DECIM, K2,..

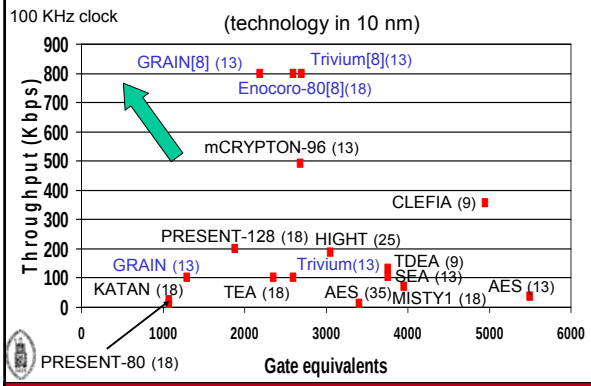
25

Moore's Law: computation/storage 2000-2020



26

Low cost hw: throughput versus area



27

Hash functions

- MDC (manipulation detection code)
- Protect short hash value rather than long text

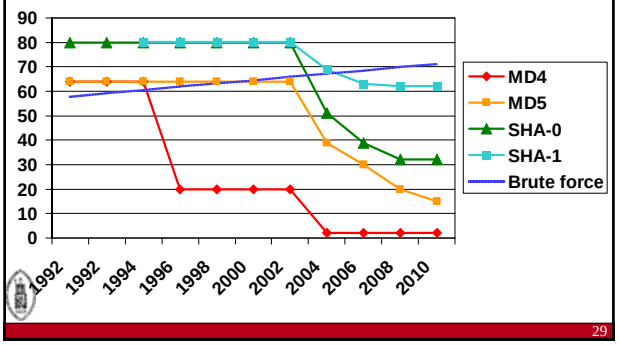
- collision resistance
- preimage resistance
- 2nd preimage resistance

This is an input to a crypto-graphic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs (a collision).

28

The complexity of collision attacks

Brute force: 4 million PCs or US$ 100K hardware (1 year)

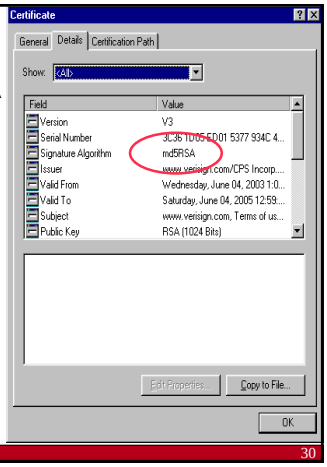


29

MD5

- Advice (RIPE since '92, RSA since '96): stop using MD5
- Largely ignored by industry (click on a cert...)

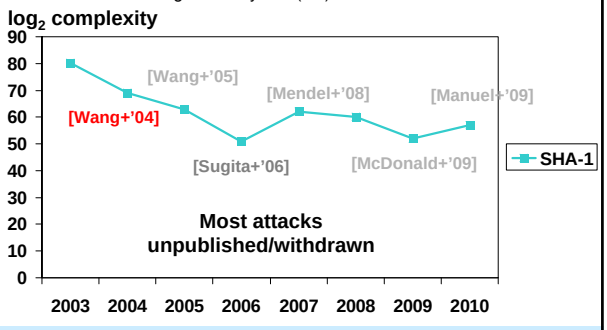
- Collisions for MD5
  - brute force (2^{64}): 1M$ 10 hours in '09
  - [Wang+'04] collision in 15 minutes on a PC
  - [Stevens+'09] collisions in **milliseconds**
- 2nd preimage:
  - [Sasaki-Aoki'09] 2^{123}



30

SHA-1

- SHA designed by NIST (NSA) in '93
- redesign after 2 years ('95) to SHA-1



prediction: collision for SHA-1 in the next 12-18 months

Hash function attacks:

cryptographic ***meltdown*** yet with limited impact

- collisions problematic for future
  - digital signatures for non-repudiation (cf. traffic tickets in Australia?)
- 2nd preimage:
  - MD2: 2^{73} [Knudsen+09]
  - MD4: $2^{97}/2^{70}$ with precomputation [Rechberger+10]
  - MD5: 2^{123} [Sasaki-Aoki'09]
  - SHA-1: 48/80 steps in $2^{159.3}$ [Aoki-Sasaki'09]
- RIPEMD-160 seems more secure than SHA-1 ☺
- use more recent standards (slower and larger)
  - SHA-2 (SHA-256, SHA-224,…SHA-512)
  - SHA-3?

32

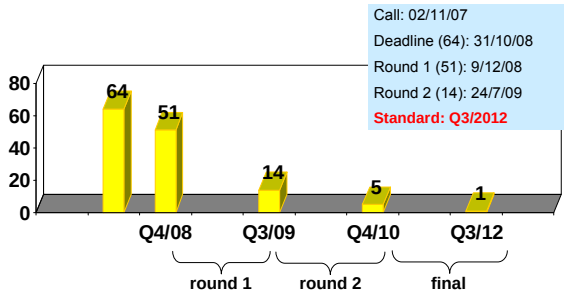
Hash function attacks: impact

- High profile attack on CAs in December 2008
- TLS/SSL has been designed for algorithm negotiation and flexible upgrades
  - …but the negotiation algorithm uses MD5 || SHA-1
  - negotiation cannot be upgraded without changing the standard: TLS 1.1 -> 1.2
  - brings serious cost: no upgrade until there is an economic attack
- HMAC: HMAC-SHA-1 ok

33

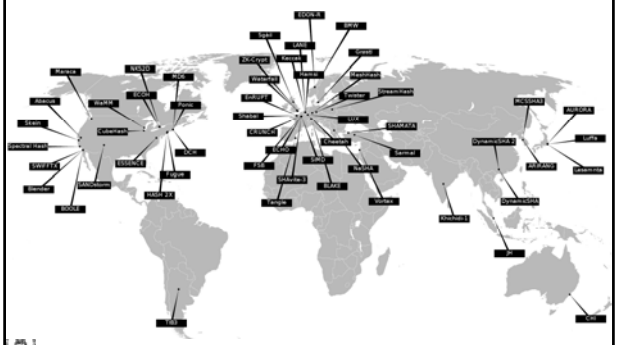
NIST AHS competition (SHA-3)

- SHA-3 must support 224, 256, 384, and 512-bit message digests, and must support a maximum message length of at least 2^{64} bits



34

The Candidates



Slide credit: Christophe De Cannière

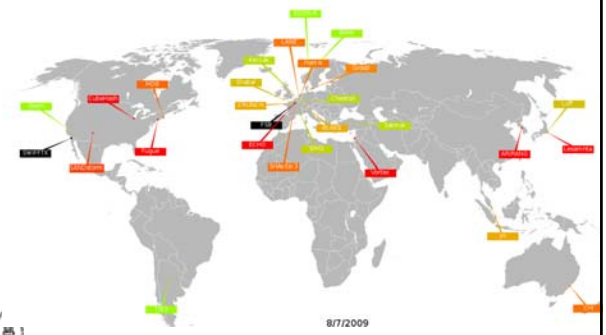
35

Preliminary Cryptanalysis

Slide credit: Christophe De Cannière

36

End of Round 1 Candidates



Slide credit: Christophe De Cannière 37

Round 2 Candidates

Slide credit: Christophe De Cannière 38

Lightweight (?) hash functions

	Area (GE)	Throughput Kbps (@100 KHz)	Throughput/ Area (bps/GE)
SHA-2 (256)	10900	45	4.1
MAME (256)	8100	267	33.0
Cubehash8/1 (512)	7630	2	0.26
PRESENT-based (128)	4256	200	47.0
	2330	11	4.7
Quark (224)	4640	50	10.5
	2296	3.1	1.36

Block cipher-based designs require strong key schedule – otherwise risky

39

Hash functions: conclusions

- Cryptographic meltdown but fortunately implications so far limited
- Designers often too optimistic (usually need 2x more rounds)
- Other weaknesses have been identified in general approach to construction hash functions
- Today, our understanding has improved substantially, so probably it is likely that it will take > 20 years before we have a SHA-4 competition
- No really lightweight hash functions

40

Outline

- Context
- Block ciphers
- Stream ciphers
- Hash functions
- (MAC algorithms)
- Public-key cryptography
- Secure implementations

41

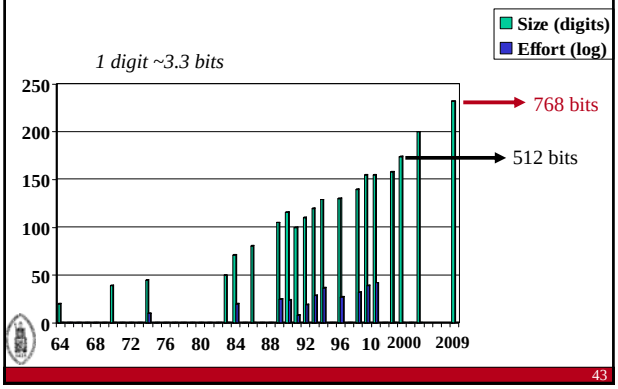
Public key algorithms

- RSA
- ECC/HECC
- NTRU

42

Factorisation records

2009: 768 bits or 232 digits



43

Factorisation

- New record in 2009: 768 bits (or 231 digits) using NFS
- New record in May 2007: 2^{1039}-1 (313 digits) using SNFS
- hardware factoring machine: TWIRL [TS'03] (The Weizmann Institute Relation Locator)
  - initial R&D cost of ~$20M
  - 512-bit RSA keys can be factored with a device costing $5K in about 10 minutes
  - 1024-bit RSA keys can be factored with a device costing $10M in about 6 weeks
- ECRYPT statement on key lengths and parameters
  http://www.ecrypt.eu.org

896-bit factorization in 2012, 1024-bit factorization in 2020?

44

Key lengths for confidentiality

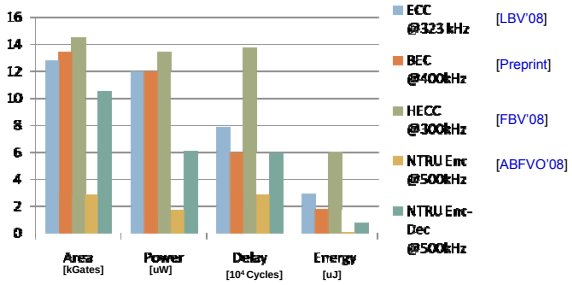
http://www.ecrypt.eu.org

duration	symmetric	RSA	ECC
days/hours	50	512	100
5 years	73	1024	146
10-20 years	103	2048	206
30-50 years	141	4096	282

Assumptions: no quantum computers; no breakthroughs; limited budget

45

Public key performance comparison



* ECC/BEC over GF(2^{163})
* HECC over GF(2^{83})
* NTRU parameters: N=167, q=128, p=3

Slide credit: L. Batina/I.Verbauwhede/J. Fan

46

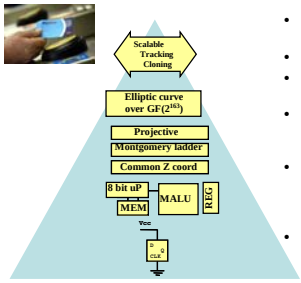
RFID technology

1. Passive tag
2. Battery assisted (BAP)
3. Active tag with onboard power source

Slide credit: L. Batina/I.Verbauwhede/J. Fan

47

Challenge: low power public key



- **Protocol** : asymmetric (most work for the reader)
- **Algorithm**: Elliptic curve (163 bits)
- **Field Operation**: Binary and not Prime fields: easier field operations
- **Projective** coordinate system: (X, Y, Z) instead of (x,y): no field inversions
- **Special coordinate system**: no need to store Y coordinates (Lopez-Dahab) and common Z (only one Z coordinate)
- **Minimize storage**: Only 5 registers (with mult/add/square unit) or 6 registers (with mult/add-only unit)

Address at all abstraction levels!

Slide credit: L. Batina/I.Verbauwhede/J. Fan

48

Performance results

Circuit Area (Gate Eq.)	14,566
Cycles for EC point multiplication	59,790
Frequency	700 KHz
Power	13.8 μW
Energy for EC point multiplication	1.18 μJ

Slide credit: L. Batina/I.Verbauwhede/J. Fan

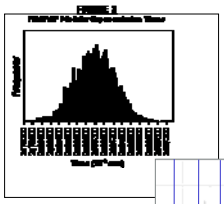
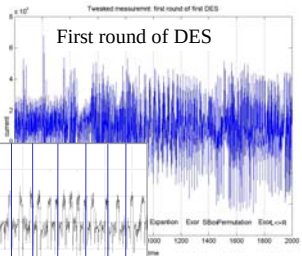
49

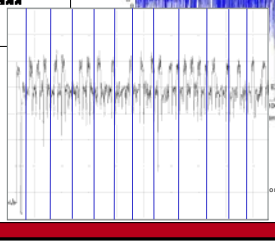
Models and reality



50

Implementations: side channel attacks



RSA

51

Implementation attacks

Sun Tzu, The Art of War:
In war, avoid what is strong and attack what is weak

- measure: time, power, electromagnetic radiation, sound
- introduce faults (even in CPUs – bug attacks)
- combine with statistical analysis and cryptanalysis
- software: API attacks

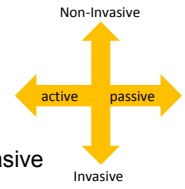
- major impact on implementation cost

L.R. Knudsen: "It is not cryptanalysis, it is vandalism"

52

Classification of Physical Attacks

- Active versus passive
  - Active: Perturbate and conclude
  - Passive: Observe and infer
- Invasive versus non-invasive
  - Invasive: open package and contact chip
  - Semi-invasive: open package, no contact
  - Non-invasive: no modification
- Side channel: passive and non-invasive
  - Very difficult to detect
  - Often cheap to set-up
  - Often: need lots of measurements → automating
- Circuit modification: active and invasive
  - Expensive to detect invasion (chip might be without power)
  - Very expensive equipment and expertise required



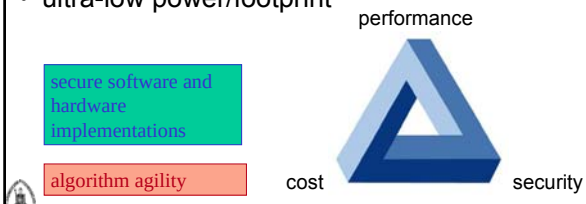
53

Side channel attacks on unprotected implementations?

54

Challenges for crypto

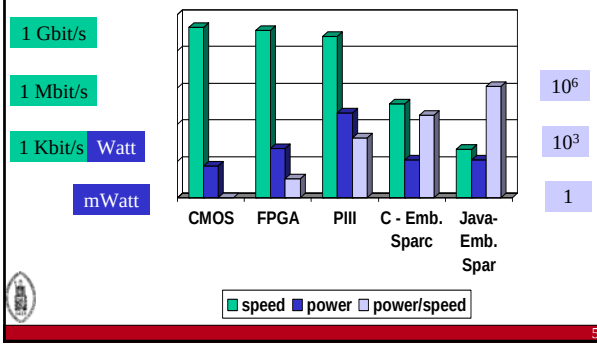
- security for 50-100 years
- authenticated encryption of Terabit/s networks
- ultra-low power/footprint



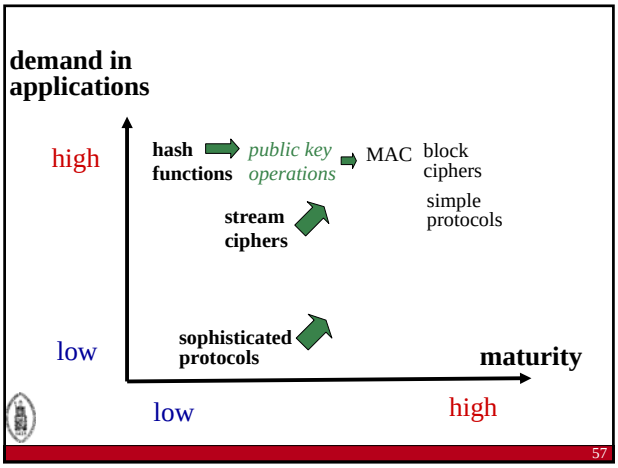
55

The power challenge:

AES-128 speed/power for various platforms (Joule/Gb)

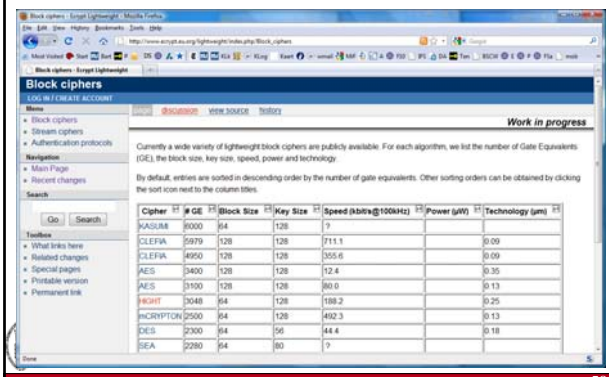


56



57

http://www.ecrypt.eu.org/lightweight/



58

Conclusions

- Major challenges remain in cryptographic algorithm design
- Lightweight crypto has many dimensions
  - no single optimal solution for RFID, sensor nodes, co-processor for 8-bit CPU,…
  - pushing the edge for all aspects
- Symmetric crypto with less than 1000 gates is feasible
  - Cost is then dominated by memory (2 to 8 gates per bit)
  - Energy consumption may be high
  - Software: RAM usage is critical
- Public key crypto with less than 15,000 gates is feasible (if hard-coded and security < 10 years)
- Challenges for implementers: upgrading algorithms and implementation attacks

59