






<http://www.ecrypt.eu.org>

The Cryptographic Year in Review

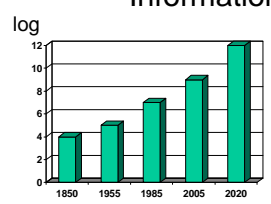
Prof. Bart Preneel
 COSIC
 Katholieke Universiteit Leuven, Belgium
 Bart.Preneel(at)esat.kuleuven.be

October 2009






Information processing



number of computing devices is exploding


low cost crypto everywhere
global connectivity
huge databases
every device/entity is unique

Computer may beat human brain in 2025



Cryptography in 2009

- more than 600 reviewed articles (10,000 pages)
 - before review: <http://eprint.iacr.org>
- 2 conferences/workshops per month on cryptography
- every week a conference with a session on cryptography
- but little in the *The New York Times*




Cryptography \neq security

crypto is only a tiny piece of the security puzzle

- but an important one


most systems break elsewhere

- incorrect requirements or specifications
- implementation errors
- application level
- social engineering (layer 8)



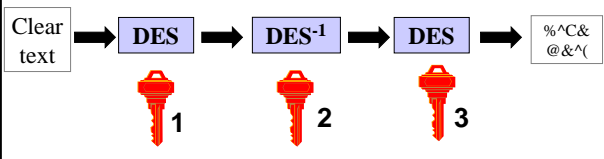
Outline

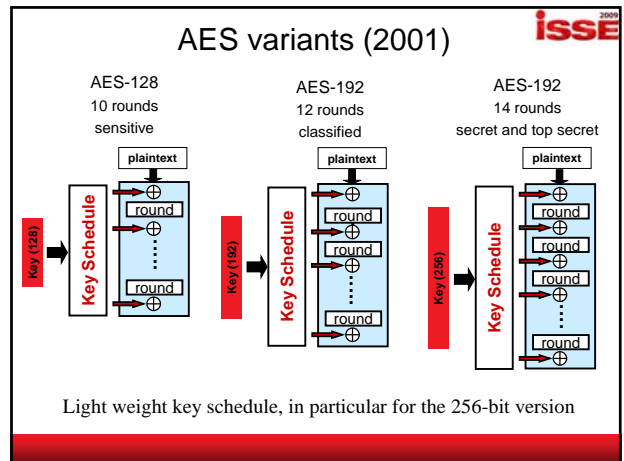
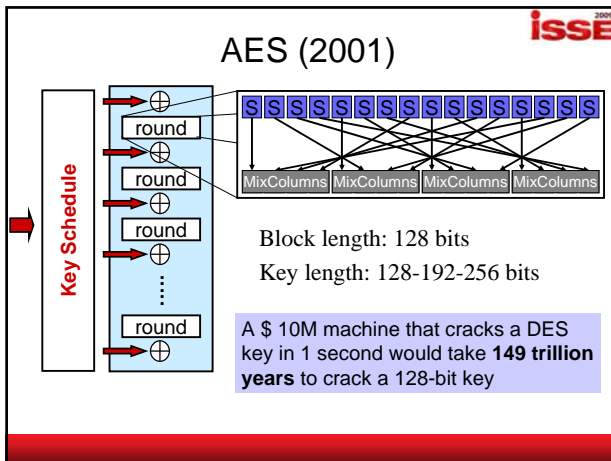
- Context
- Cryptography
 - Block ciphers
 - Hash functions
 - Public-key cryptology
- Protocols and key management
- Research challenges



3-DES: NIST Spec. Pub. 800-67 (May 2004)

Single DES abandoned
 two-key triple DES: until 2009 (80 bit security)
 three-key triple DES: until 2030 (100 bit security)





AES implementations: efficient/compact

NIST validation list: 1187 implementations (2008: 879)
<http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>

- HW: 43 Gbit/s in 130 nm CMOS [‘05]
- Intel: new AES instruction: 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
 - KATAN: 1054, PRESENT: 1570

AES: security

- cryptanalysis: no attack has been found that can exploit this structure (in spite of the algebraic “attack” [Courtois’02])
- implementation level attack
 - cache attack precluded by bitsliced implementations or by special hardware support
 - fault attack requires special countermeasures

AES-256 security

Exhaustive key search on AES-256 takes 2^{256} encryptions

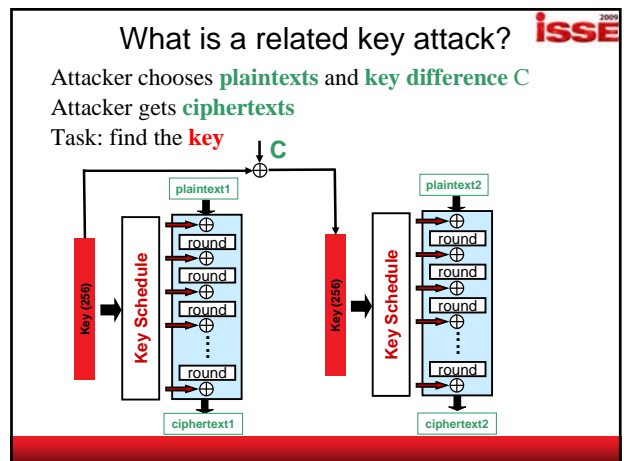
- 2^{64} : 10 minutes with \$ 5M
- 2^{80} : 2 year with \$ 5M
- 2^{120} : 1 billion years with \$ 5B

[Biryukov-Khovratovich’09] **related key attack on AES-256**

- requires 2^{119} encryptions with 4 related keys,
- data & time complexity $2^{119} \ll 2^{256}$

Why does it work? Very lightweight key schedule

- Is AES-256 broken? No, only an academic “weakness” that is easy to fix
- No implications on security of AES-128 for encryption
- Do not use AES-256 in a hash function construction



Should I worry about a related key attack?

Very hard in practice (except some old US banking schemes)

If you are vulnerable to a related key attack, you are making very bad implementation mistakes

This is a very powerful attack model: if an opponent can zeroize 96 key bits of his choice (rather than adding a value), he can find the key in a few seconds

If you are worried, hashing the key is an easy fix

What about reduced-round versions?

[Biryukov-Dunkelman-Keller-Khovratovich-Shamir'09]

[Biryukov-Khovratovich'09]
Related key attack: 4 keys, data & time complexity $2^{119} \ll 2^{256}$

Slide credit: Orr Dunkelman

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 cryptographic 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).

Security requirements (n-bit result)

preimage: 2^n
2nd preimage: 2^n
collision: $2^{n/2}$

> 80% of all designs for collision resistant hash functions are broken

MDx-type hash function history

The complexity of collision attacks

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

MD5

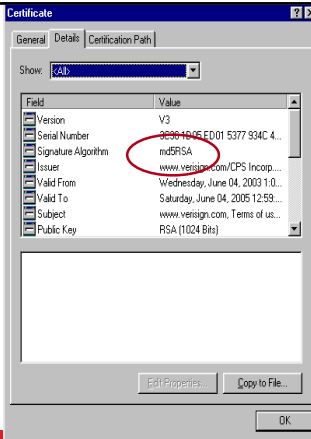
Advice (RIPE since '92, RSA since '96): **stop using MD5**
Largely ignored by industry (click on a cert...)

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:

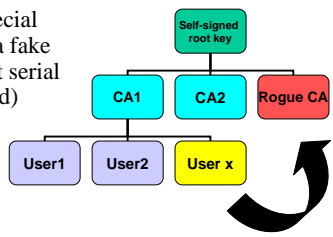
- 2^{123} [Asaki-Aoki'09]



Rogue CA attack

[Sotirov-Stevens-Appelbaum-Lenstra-Molnar-Osvik-de Weger '08]

request user cert; by special collision this results in a fake CA cert (need to predict serial number + validity period)



impact: rogue CA that can issue certs that are trusted by all browsers

6 CAs have issued certificates signed with MD5 in 2008:

- Rapid SSL, Free SSL (free trial certificates offered by RapidSSL), TC TrustCenter AG, RSA Data Security, Verisign.co.jp

Other ways to fool CAs

[Moxie Marlinspike'09] Black Hat

- browsers may accept bogus SSL certs
- CAs may sign malicious certs

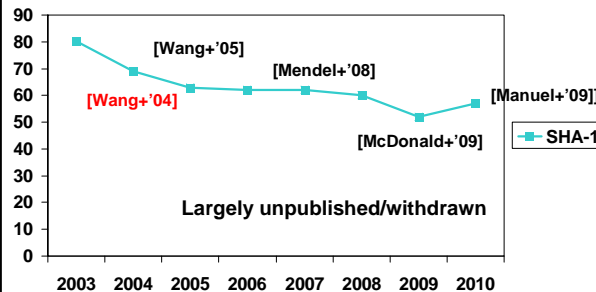
certificate for www.paypal.com \ 0.kuleuven.be will be issued if the request comes from a kuleuven.be admin

response by PayPal: suspend Moxie's account

- http://www.theregister.co.uk/2009/10/06/paypal_banishes_ssl_hacker/

SHA-1

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



Largely unpublished/withdrawn

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^{102} [Leurent'08]
- SHA-1 49/80 steps in 2^{157} [DeCannière-Rechberger'08]

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?

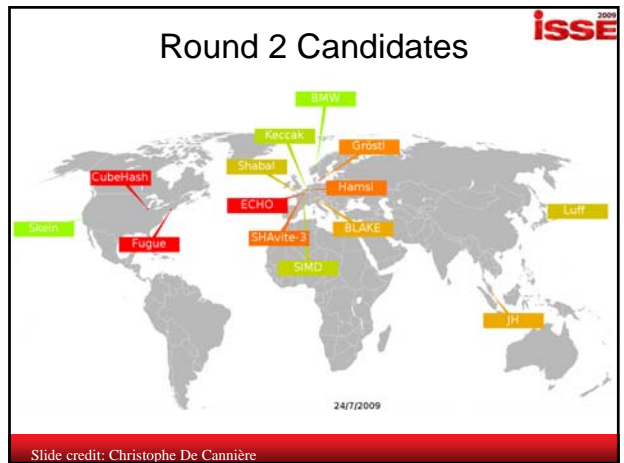
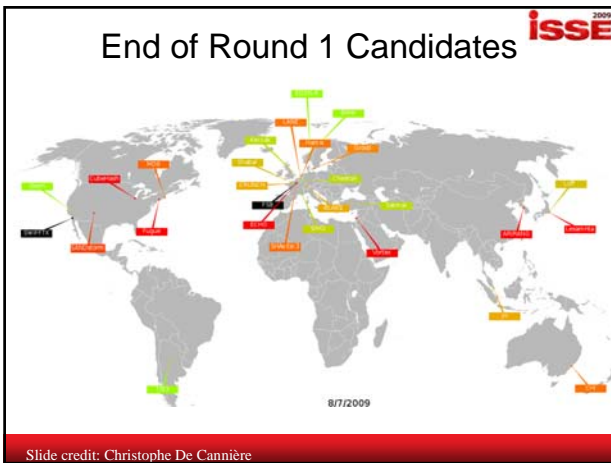
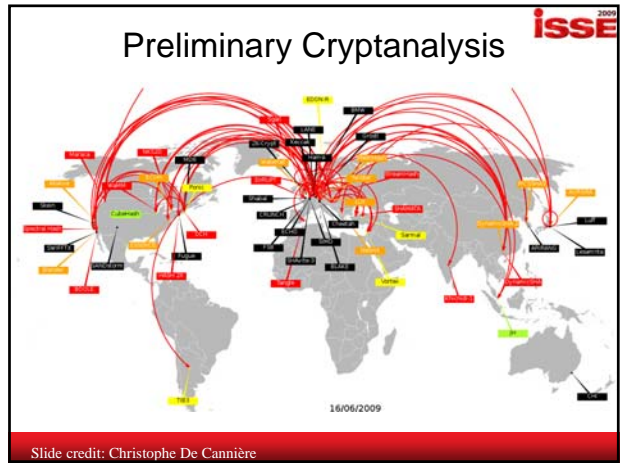
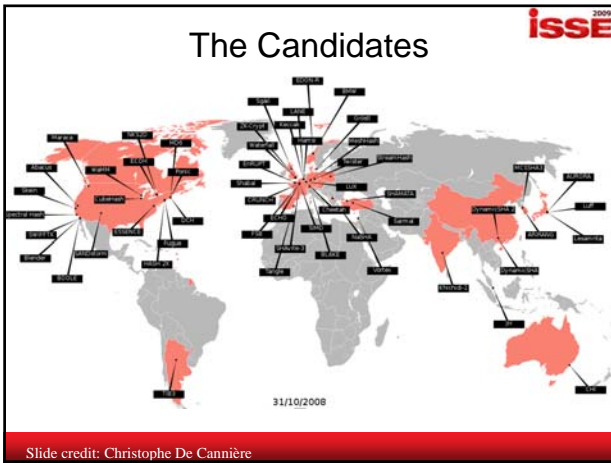
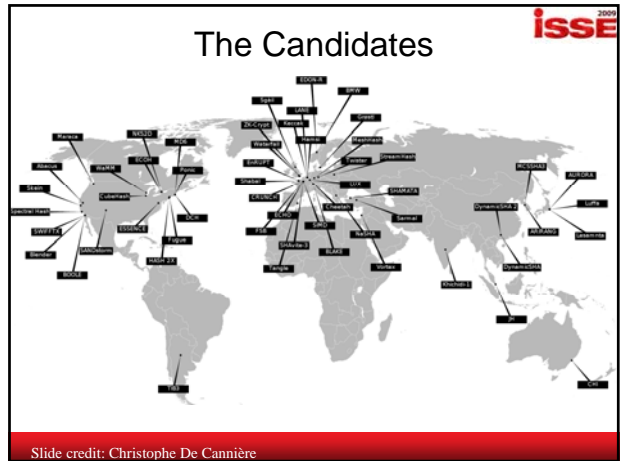
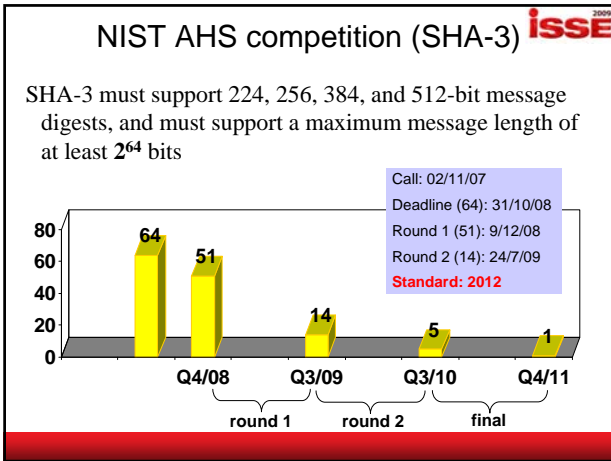
Hash function attacks: impact

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-MD4: 2^{72} chosen plaintexts & 2^{77} time
- HMAC-MD5: 2^{51} chosen plaintexts & 2^{100} time in a related key setting
- HMAC-SHA-1 seems fine for now



Issues arisen during Round 1

isSE 2009

security:

- some limited controversy about some attacks
- proofs have not helped much to survive

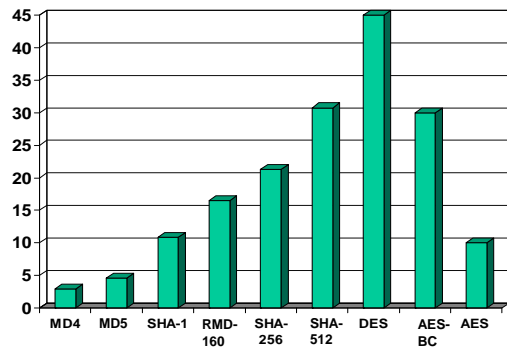
performance: roughly as fast or faster than SHA-2

- tunable security/performance tradeoff: nominal parameters?
- large memory (> 100 bytes) may be a problem for small devices
- can we exploit 64 or 128 cores? Intel AES instruction?

Performance of hash functions - Bernstein

isSE 2009

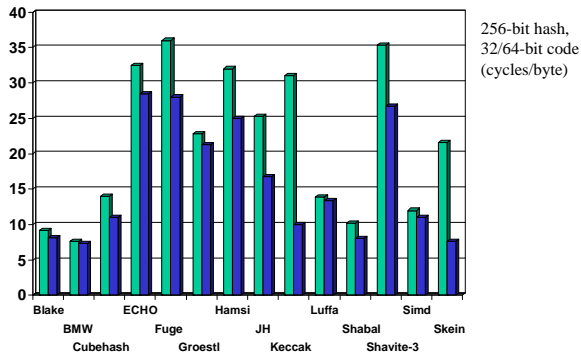
(cycles/byte) AMD Intel Pentium D 2992 MHz (f64)



Performance of hash functions

isSE 2009

[Bernstein09] <http://bench.cr.yp.to/ebash.html>



Hash functions: conclusions

isSE 2009

- Cryptographic meltdown but fortunately implications so far limited
- Designers often too optimistic (usually need 2x more rounds)
- SHA3: some innovation, but 2012 winner will reflect state of the art in 2008
- Today, our understanding has improved substantially, so probably it will take a while before we have a SHA-4 competition

Public-Key Cryptology

isSE 2009

- no new factorization record
- upgrade your RSA-1024 keys by 2010
- increased acceptance of ECC
 - example NSA Suite B in USA
 - Certicom challenge: ECC2K-130: 1 year with 60 KEURO (a large effort is underway)
- progress on pairings leading to more efficient protocols

Attack on ISO 9796-2 [Coron+'09]

isSE 2009

History:

- ISO 9796-1 (1991) was broken and withdrawn in 2001
- ISO 9796-2 was repaired in 2002 after a first attack in 1999

New forgery attack on 9796-2 that works for very long RSA moduli (2048 bits)

- any 160-bit hash function: 800\$ on Amazon cloud
- the specific EMV variant: 45K\$

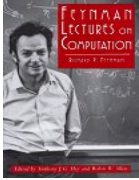
Not a practical threat to 750 million EMV cards since the attack requires a large number of chosen texts (600,000)

isSE 2009

Quantum computers?

exponential parallelism n coupled quantum bits
 \Downarrow
 2^n degrees of freedom !


Shor 1994: perfect for factoring
 But: can a quantum computer be built?



isSE 2009

If a large quantum computer can be built...

All schemes based on factoring (such as RSA) will be insecure
 Same for discrete log (ECC)
 Symmetric key sizes: x2
 Hash sizes: x1.5 (?)

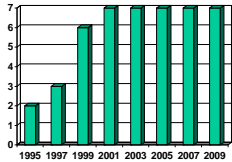


Alternatives: McEliece, NTRU, ...
 So far it seems very hard to match performance of current systems while keeping the security level against conventional attacks


isSE 2009

Quantum computers

Size of quantum computer does not (yet) matter!



Photon machine gun, New scientist, Sept. 09



More important is to keep a few qubits with high reliability for a sufficiently long time (decoherence)

isSE 2009

Outline

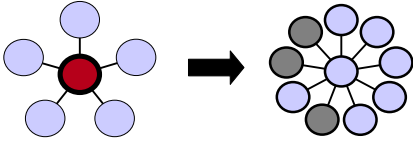
- Context
- Cryptography
 - Block ciphers
 - Hash functions
 - Public-key cryptology
- Protocols and key management
- Research challenges

isSE 2009

Protocols

privacy protecting biometry
 privacy protecting data mining
 social and group crypto
 ...
 multi-party computation

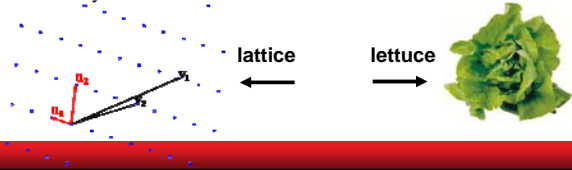
“you can trust it because you don't have to”




isSE 2009

Fully homomorphic encryption

- Once you know $E(x)$ and $E(y)$, you can compute $E(x+y)$, $E(c.x)$ and $E(x.y)$ **without decrypting**
- Many cool applications
- Craig Gentry, IBM [June'09]:
 - first solution using ideal lattices
 - impractical today: performing a Google search with encrypted keywords would increase the computing time by about a trillion




Internet voting



- Spring 2009: rector elections in UC, Belgium
 - 25.000 eligible to vote; turnout 40%
- Helios [Adida'08] www.heliosvoting.org
 - sophisticated cryptographic protocols: open audit
 - open source
- main advantages:
 - remote voting
 - as everything is encrypted, log files can be made public so disputes can be resolved easily
- main disadvantages:
 - coercion risk
 - Trojan or virus can easily undermine these elections (proof of concept [Desmedt'09])

Uniqueness (1)





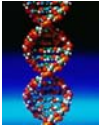
Physics and electronics (accidental)

- Process variation in deep submicron processes
- Radio fingerprinting: unique pattern of each wireless antenna, modulator, filter, oscillator
- Fibers in paper
- Magnetic behavior of certain materials


privacy risk

Human: biometry

- Fingerprint
- Iris
- DNA
- Face
- Gait
- ...

Uniqueness (2): man-made unique features






PUF Physical Unclonable Function

- e.g., start-up of SRAM

applications


- secure key storage
- remote activation to prevent overproduction

EU project: "UNIQUE"

Coating PUFs	Acoustic PUFs	Optical PUFs
Measuring the capacitances of a coating with random dielectric particles	Probing structures with acoustic waves	Disordered structures illuminated by a laser beam
		


Credit:
Philips/
Intrinsic ID


"Hacked"



- MiFare Classic
 - Crypto-1 algorithm reverse engineered [Nohl-Plötz'07] – 48-bit key
 - Dismantling MIFARE Classic [Garcia+'08]
 - Improved attacks in 2009: Wirelessly Pickpocketing a Mifare Classic Card [Garcia+'09]
 - Answer: Mifare+

Layers





applications

protocols

primitives


algorithms

assumptions

Proofs: link security at different levels in a quantitative way

L.R. Knudsen:
 "If it is provably secure, it is probably not"

Challenges for crypto



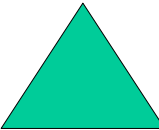
security for 50-100 years

authenticated encryption of Terabit/s networks

ultra-low power/footprint

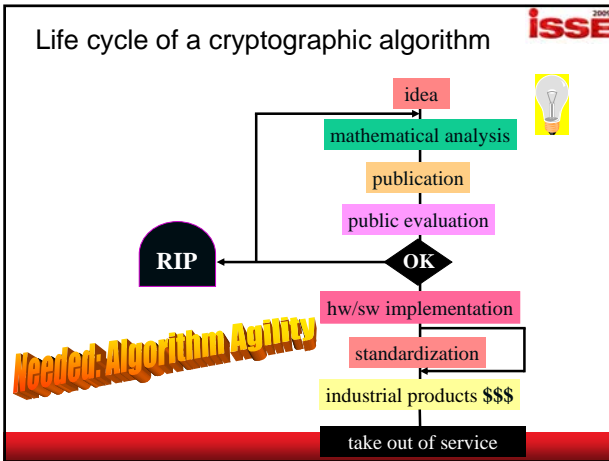
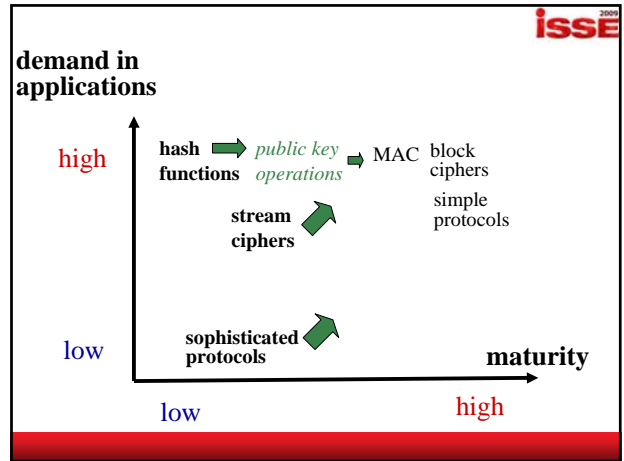
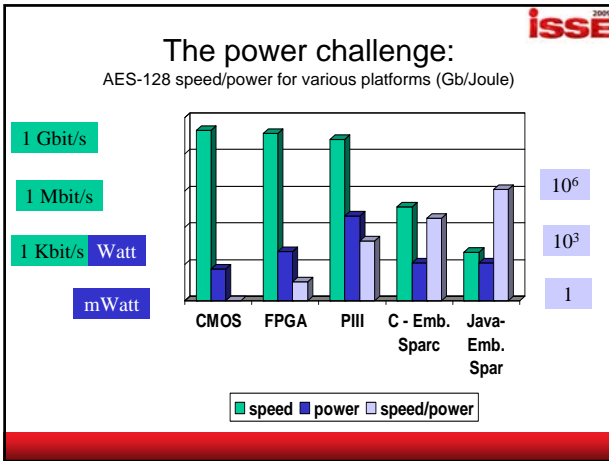
secure software and hardware implementations

Performance



Cost Security

Algorithm agility



Challenges for advanced crypto

- privacy enhancing technologies
- linking crypto with physical world
 - biometrics, physical uncloneable functions
- distributed secure execution
- whitebox cryptography
- cryptography in the encrypted domain
 - searching in encrypted databases – data mining on health care data
- crypto for nanotechnology

Conclusion

- crypto is an essential building block of information security
- interesting and challenging mathematical problems, w.r.t. foundations and engineering aspects
- make sure that you can upgrade your crypto algorithms

Even boring crypto years can be quite interesting

The end

Thank you for your attention