

http://www.ecrypt.eu.org

## Cryptographic Algorithms: Successes, Failures and Challenges

Prof. Bart Preneel  
COSIC, K.U.Leuven, Belgium  
Bart.Preneel(at)esat.kuleuven.be  
http://homes.esat.kuleuven.be/~preneel  
July 2008

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 processing ( $10^4$ )

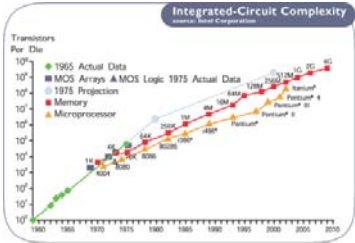
manual processing ( $10^2$ )

2

## Exponential growth

Ray Kurzweil, KurzweilAI.net

- Human brain:  $10^{14}$  ...  $10^{15}$  ops and  $10^{13}$  bits memory
- 2025: 1 computer can perform  $10^{16}$  ops ( $2^{53}$ )
- 2013:  $10^{13}$  RAM bits (1 Terabyte) cost 1000\$



3



4

## Context

DES, RSA, DH, CBC-MAC	<b>HARDWARE</b>	70
Provable security (PKC), ZK, ElGamal, ECC, stream ciphers	Limited (govt+financial sector) DES, 3DES	80
MD4, MD5	<b>SOFTWARE</b>	90
Provable security (SKC)	GSM, PGP	
Key escrow	C libraries (RSA, DH)	
How to use RSA?	SSL/TLS, IPsec, SSH, S/MIME	
Alternatives to RSA	Java crypto libraries	
PKI	WLAN	
AES	<b>EVERYWHERE</b>	
ID-Based Crypto	Trusted computing, DRM, 3GPP, RFID, sensor nodes	
	...	

5

## TLS 1.0 Data Encapsulation Options (01/99)

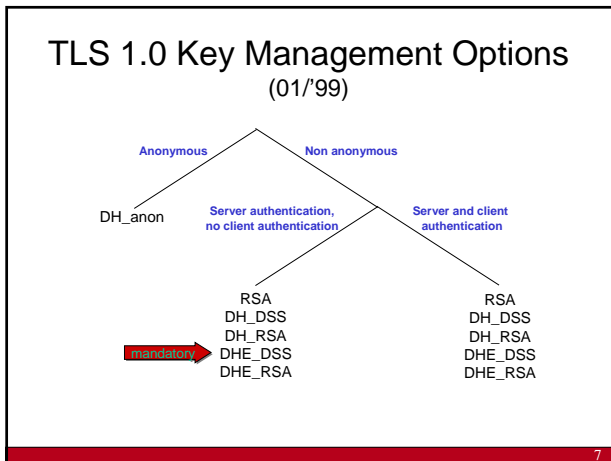
Integrity			
key size	144	160	
algorithm options	HMAC-MD5	HMAC-SHA	

mandatory

Confidentiality				
key size	40	56	128	168
algorithm options	RC4_40 RC4_40 RC2_CBC_40 DES_CBC_40	DES_CBC	RC4 IDEA_CBC	3DES EDE_CBC

mandatory

6



### RFC 3268: AES Ciphersuites for TLS (06/'02)

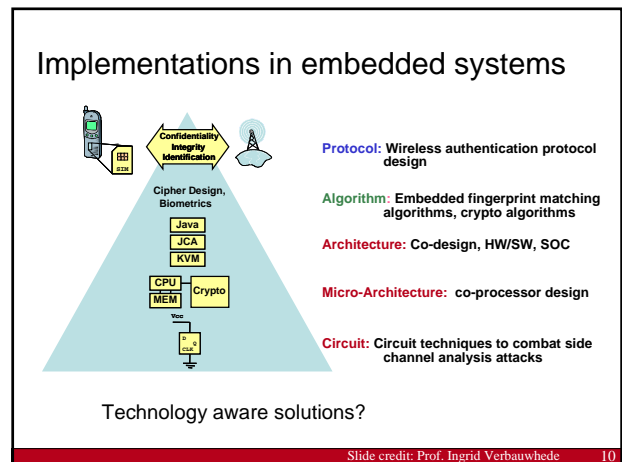
CipherSuite	Key Exchange	Certificate Type
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA
TLS_DH_DSS_WITH_AES_128_CBC_SHA	DH_DSS	DSS
TLS_DH_RSA_WITH_AES_128_CBC_SHA	DH_RSA	RSA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE_DSS	DSS
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA	RSA
TLS_DH_anon_WITH_AES_128_CBC_SHA	DH_anon	
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA
TLS_DH_DSS_WITH_AES_256_CBC_SHA	DH_DSS	DSS
TLS_DH_RSA_WITH_AES_256_CBC_SHA	DH_RSA	RSA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE_DSS	DSS
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA	RSA
TLS_DH_anon_WITH_AES_256_CBC_SHA	DH_anon	

Version 1.2: reduce dependency on MD5/SHA-1, AES mandatory

### IKE Algorithm Selection Mandatory Algorithms

Algorithm Type	IKE v1	IKE v2
Payload Encryption	DES-CBC	3DES_CBC (AES_128_CBC)
Payload Integrity	HMAC-MD5 HMAC-SHA1	HMAC-SHA1
DH Group	768 Bit	1024 (2048) Bit
Transfer Type 1 (Encryption)	ENCR_DES_CBC	ENCR_3DES (ENCR_AES_128_CBC)
Transfer Type 2 (PRF)	PRF_HMAC_SHA1 [RFC2104]	PRF_HMAC_SHA1 [RFC2104]
Transfer Type 3 (Integrity)	AUTH_HMAC_SHA1_96 [RFC2404]	AUTH_HMAC_SHA1_96 [RFC2404]

Source: RFC 3407, December 05



- ### Disclaimer: cryptography ≠ 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
  - for intelligence, traffic analysis (SIGINT) is often much more important than cryptanalysis

[Adi Shamir] We are winning yesterday's information security battles, but we are losing the war. Security gets worse by a factor of 2 every year.

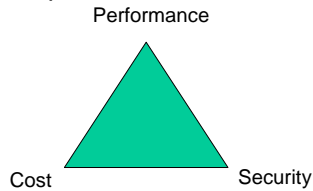
[Andrew Odlyzko] Humans can live with insecure systems. We couldn't live with secure ones.

### Challenges for crypto

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

secure software and hardware implementations

Algorithm agility



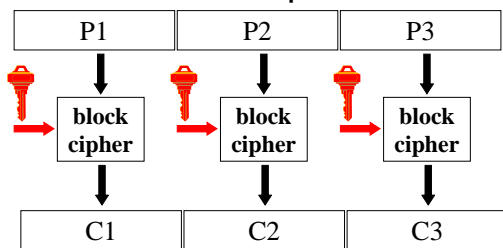
13

### Outline

- Block ciphers
- Hash functions
- Stream ciphers
- Public-key cryptology
- Protocols
- Implementations issues
- Research challenges

14

### Block cipher



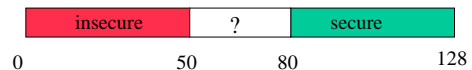
- larger data units: 64...128 bits
- memoryless
- repeat simple operation (round) many times

15

### Block ciphers

- 3-DES (112-168)
- AES (128-192-256)
- KASUMI (128 in 3G, 64 in 2G)
- IDEA (128)

Symmetric key lengths



16

### DES (1977)

- 56-bit key length is too short
- 25/10/99: DES reaffirmed for the 4th time as FIPS 46-3
- 2007: \$1 million search machine: 20 seconds
  - cost per key: less than \$0.50
- 2007: 500 PCs at night: 1 month
  - Cost per key: essentially 0 (+ some patience)



17

### Federal Register, July 24, 2004

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology  
[Docket No. 040602169– 4169– 01]

Announcing Proposed Withdrawal of Federal Information Processing Standard (FIPS) for the Data Encryption Standard (DES) and Request for Comments

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; request for comments.

- **SUMMARY:** The Data Encryption Standard (DES), currently specified in Federal Information Processing Standard (FIPS) 46–3, was evaluated pursuant to its scheduled review. At the conclusion of this review, **NIST determined that the strength of the DES algorithm is no longer sufficient to adequately protect Federal government information.** As a result, NIST proposes to withdraw FIPS 46–3, and the associated FIPS 74 and FIPS 81. Future use of DES by Federal agencies is to be permitted only as a component function of the Triple Data Encryption Algorithm (TDEA).

18

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

- two-key triple DES: until 2009
- three-key triple DES: until 2030

Financial sector will not be ready with upgrade to 3-key 3-DES in 2010

19

### AES (2001)

- open competition: 1997-2000
- FIPS 197 published on December 2001
- mandatory for sensitive US govt. information
- fast adoption in the market
  - > 1000 products
  - July 2008: 835 AES product certifications by NIST
  - standardization: ISO, IETF, IEEE 802.11,...
- slower adoption in financial sector
- mid 2003: AES-128 also for **classified** information and AES-192/-256 for **secret** and **top secret** information!

AES may well be the last block cipher

20

### AES/Rijndael

- Key length: 16/24/32 bytes
- Block length: 16 bytes

A machine that cracks a DES key in 1 second would take 149 trillion years to crack a 128-bit key

21

### AES: rich mathematical structure

- very compact/efficient implementations
  - SW: 14 cycles per byte or 1-2 Gbit/s on high end PCs
  - HW: most compact: 3600 gates
  - HW: fastest up to 43 Gbit/s in 130nm CMOS
  - Intel (+AMD): new AES instruction: 0.75 cycles/ybte
- security
  - is it hard to solve sets of non-linear Boolean equations?
  - no attack has been found that can exploit this structure (in spite of earlier claims)
  - main threat is implementation level attack (cache timing, fault attacks): requires special countermeasures

22

### Modes of Operation for AES

- encryption: ECB/CBC/CFB/OFB;
  - CTR mode allows for pipelining ('01)
- data authentication: CMAC ('05), EMAC
- applications need authenticated encryption:
  - GCM Galois Counter Mode (final draft: July 07)

Issues:

- associated data
- parallelizable
- on-line
- provable security

- IAPM
- XECB
- OCB
- GCM
- EAX
- CCM

patented

23

### Block ciphers: Keeloq

- Microchip Inc algorithm, designed in the 1980s
- Allegedly used in 80% of the cars for car locks, car alarms
- Block cipher with 32-bit blocks, 64-bit keys and 528 simple rounds

24

### Block ciphers: Keeloq (2)

- Leaked on the internet in 2006
- [Bogdanov07] in some cases car key = Master key + Car ID
- [Bogdanov07], [Courtois-Bard-Wagner07] first cryptanalysis
- [Biham-Dunkelman-Indesteeghe-Keller-Preneel07]:
  - 1 hour access to token ( $2^{16}$  known texts)
  - 2 days of calculation on 50 PCs (10.000\$) -  $2^{44.5}$  encryptions
- [Eisenbarth-Kasper-Moradi-Paar-Salmasizadeh-Manzuri-ShalmaniPaar 08]
  - Side channel attack allows to recover master key

in 2010 cryptographers will drive expensive cars

25

### Block ciphers: conclusions

- Several mature block ciphers available
- Security well understood
  - in particular against statistical attacks (differential, linear) and structural attacks
  - algebraic attacks may be further developed

26

### Hash functions

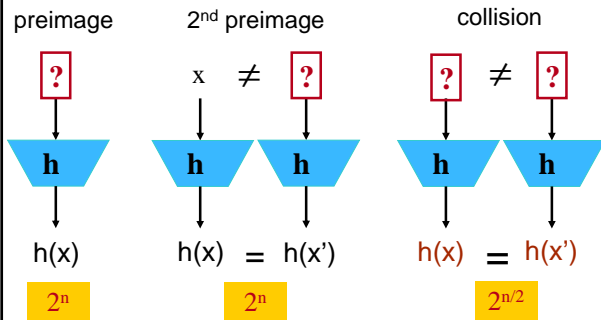
- MDC (manipulation detection code)
- Protect short hash value rather than long text
- collision resistance
- preimage resistance
- $2^{\text{nd}}$  preimage resistance

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).



27

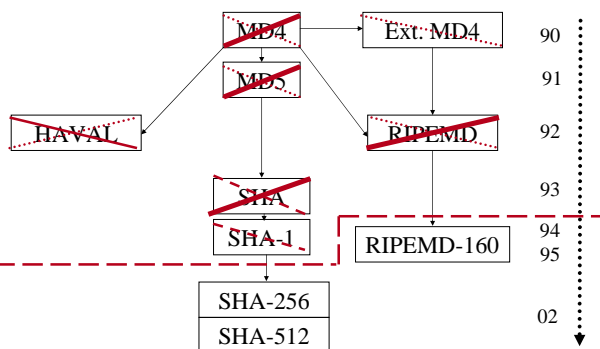
### Security requirements (n-bit result)



> 90% of all designs for collision resistant hash functions are broken

28

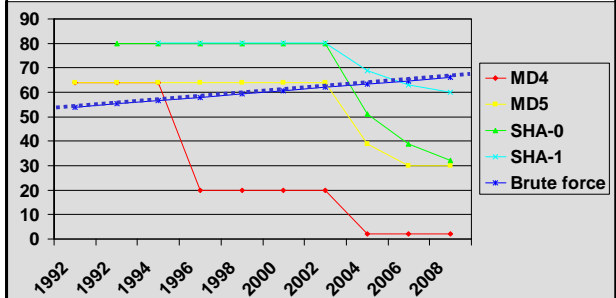
### MDx-type hash function history



29

### Collision attacks

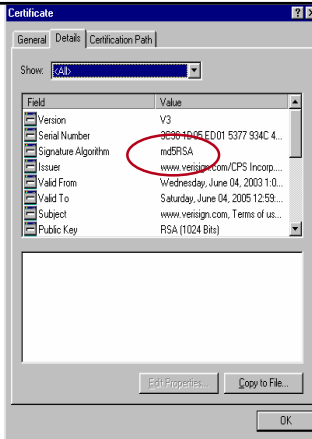
Brute force: 1 million PCs or 100.000\$ hardware



30

### MD5

- Advice (RIPE since '92, RSA since '96): **stop using MD5**
- Largely ignored by industry (click on a cert...)
- Collisions for MD5 are within range of a brute force attack anyway ( $2^{64}$ ): with 100.000\$ a few days
- [Wang+'04] collision in 15 minutes on a PC
- 2007: collisions in seconds




31


### SHA-1

- SHA designed by NIST (NSA) in '93
- redesign after 2 years ('95) to SHA-1
- Collisions found for SHA-0 in  $2^{51}$  [Joux+'04]
- Reduced to  $2^{39}$  [Wang+'05] and  $2^{32}$  [Rechberger+'07]
- Collisions for SHA-1 in  $2^{63}$  [Wang+'05]
- Collisions for SHA-1 found for 70 out of 80 rounds [De Cannière-Mendel-Rechberger+'07] in  $2^{44}$
- Prediction: collision for SHA-1 in 2009; complexity estimate is  $2^{60}$  [Rechberger+'07]

32



33

From: "Cryptography Simplified in Microsoft .NET" Paul D. Sheriff (PDSA.com) [Nov. 2003] 

#### How to Choose an Algorithm

- For example, SHA1 uses a 160-bit encryption key, whereas MD5 uses a 128-bit encryption key; thus, SHA1 is more secure than MD5.
- Another point to consider about hashing algorithms is whether or not there are practical or theoretical possibilities of collisions. Collisions are bad since two different words could produce the same hash. **SHA1, for example, has no practical or theoretical possibilities of collision. MD5 has the possibility of theoretical collisions, but no practical possibilities.**

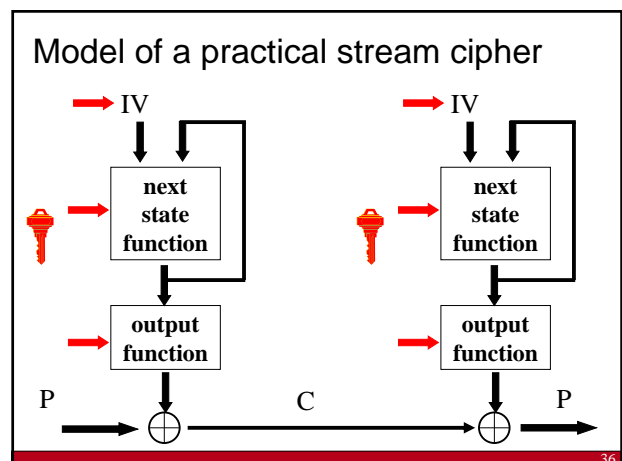
In July 2008 this information was still available on MSDN

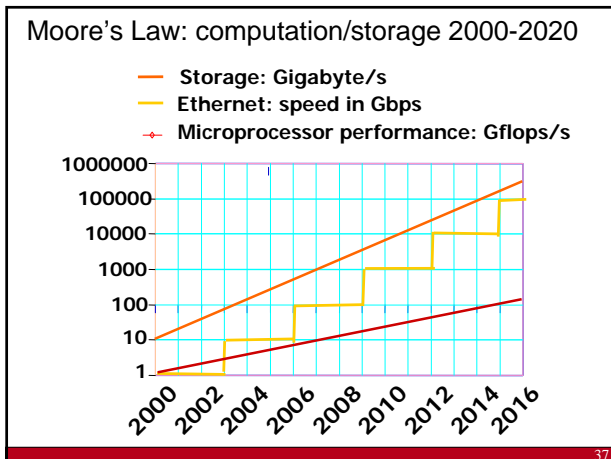
34

### Hash function attacks: impact

- cryptographic meltdown yet with limited impact
- collisions problematic for future
  - digital signatures for non-repudiation (cf. traffic tickets in Australia?)
- 2<sup>nd</sup> preimage only a problem for MD4
- HMAC-MD4 broken, HMAC-MD5 questionable for the long term
- RIPEND-160 seems more secure than SHA-1 ☺
- use more recent standards (slower)
  - SHA-256, SHA-512
  - Whirlpool
- upgrading MD5 and SHA-1 in Internet protocols:
  - it doesn't work: **algorithm flexibility is much harder than expected**
- NIST will run an open competition from 2008 to 2012

35





### 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
  - exception: SNOW2.0, MUGI
  - lack of standards and open solutions

38

### Open competition for stream ciphers

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

- run by ECRYPT
  - high performance in **software** (32/64-bit): 128-bit key
  - low-gate count **hardware** (< 1000 gates): 80-bit key
  - variants: authenticated encryption
- 29 April 2005: 33 submissions
- Many broken in first year
- End of competition: April 2008

39

### Open competition: Feb. 2007 status

SW Phase 3	HW Phase 3
CryptMT	DECIM
DRAGON	<del>Edon-80</del>
HC-128 (-256)	F-FCSR
LEX	Grain
NLS (encrypt only)	MICKEY (-128)
Rabbit	MOUSTIQUE
Salsa20	POMARANCH
SOSEMANUK	Trivium

3-10 cycles per byte      1500..3000 gates

40

### The eSTREAM Portfolio

April 2008

Software	Hardware
HC-128	F-FCSR-H
Rabbit	Grain v1
Salsa20/12	MICKEY v2
Sosemanuk	Trivium

(In alphabetical order)

41

### Lightweight crypto

- SQUASH [Shamir07] – Crypto rump session
  - MAC algorithm for authentication in RFID chips
  - only 500 gates
  - security is related to modular squaring (Rabin cryptosystem)
- PRESENT [Bogdanov07] – CHES 2007
  - 64-bit block cipher for RFID chips
  - only 1750 gates (compare to 3600 for AES)

Stream cipher: because of time-memory trade-offs, for 80-bit security one needs 160 bits memory which costs 1000 gates

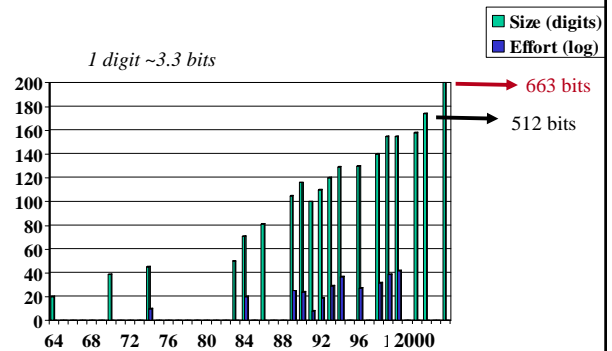
42

### Outline

- Context
- Block ciphers
- Hash functions
- Stream ciphers
- Public-key cryptology
- Protocols
- Implementations issues
- Research challenges

43

### RSA: factorisation records



44

### Factorisation

- New record in May 2005: 663 bits (or 200 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>

768-bit factorization in 2008 and 896-bit factorization in 2010

45

### Key lengths for confidentiality

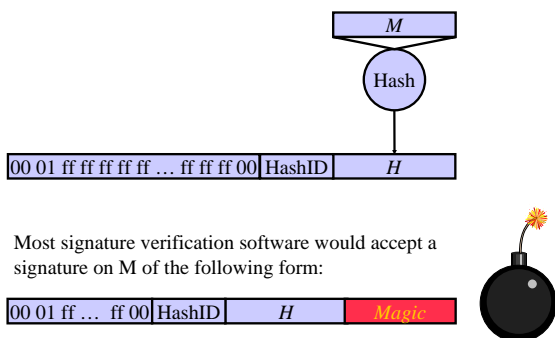
<http://www.ecrypt.eu.org>

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

46

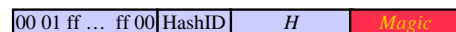
### RSA Signatures: PKCS #1 v1.5 [source: RSA Labs]



47

### Attack on PKCS #1 v1.5 implementations

[Bleichenbacher06]



- Consider RSA with public exponent 3
- For any hash value H, it is easy to compute a string "Magic" such that the above string is a perfect cube of 3072 bits
- Consequence:
  - One can sign any message (H) **without knowing the private key**
  - This signature works **for any public key** that is longer than 3072 bits
- Vulnerable: OpenSSL, Mozilla NSS, GnuTLS
- Fix
  - Write proper verification code (but the signer cannot know which code the verifier will use)
  - Use a public exponent that is at least 32 bits long
  - Upgrade - finally - to RSA-PSS

48

## Protocols (1)

- key transport (email)
- authenticated key agreement (TLS, SSH, GSM, UMTS)
- time-stamping
- notarisation
- credentials (TPM)
- anonymous communication
- e-cash
- voting
- auctions
- threshold cryptography
- robust networking

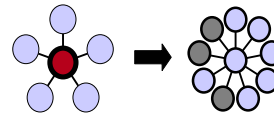
49

## Protocols (2)

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

decryption based on location and context

distance bounding



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

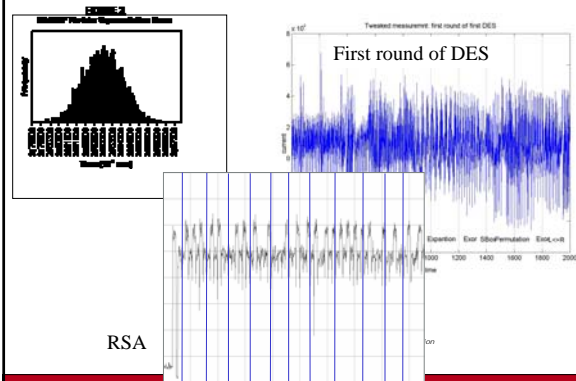


## Models and reality



51

## Implementations: side channel attacks



52

## 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"

53

## Challenges for long term security

- cryptanalysis improves:
  - mathematical attacks A5/1, E0, MD5, SHA-1
  - implementation attacks
- computational power increases:
  - Moore's law
  - exponential progress with quantum computers?
- environment changes – new assumptions
  - packet switched networking
  - open networks
  - dynamic networks
  - untrusted nodes
  - ratio power CPU/memory size
  - outsourcing of data processing

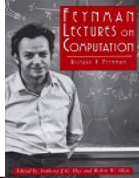
54

## New computational models: quantum computers?

- exponential parallelism  $n$  coupled quantum bits  
 $2^n$  degrees of freedom!



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



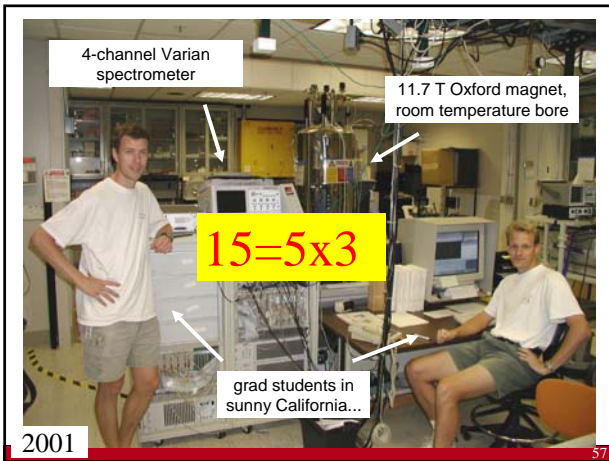
55

## 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:  $\times 2$
- Hash sizes:  $\times 1.5$
- Alternatives: McEliece, HFE, NTRU,...
- So far it seems very hard to match performance of current systems while keeping the security level against conventional attacks



56



2001

57

## News on 13 Sept. 2007

- "Two independent teams (led by Andrew White at the University of Queensland in Brisbane, Australia, and the other by Chao-Yang Lu of the University of Science and Technology of China, in Hefei) have implemented Shor's algorithm using rudimentary laser-based quantum computers"
- Both teams have managed to factor 15, again using special properties of the number

## News on 19 Dec. 2007

- optical quantum computer (team led by Daniel James, University of Toronto)
- factored 15

58

## Layers

applications

protocols

primitives

assumptions algorithms

Proofs: link security at different levels in a quantitative way

L.R. Knudsen:

"If it is provably secure, it is probably not"

59

## Assumptions

research on **hard problems**?

James L. Massey:

A hard problem is one that nobody works on

good lower bounds

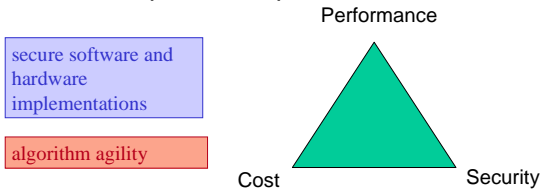
average versus worst case

find new hard problems

60

### Challenges for crypto

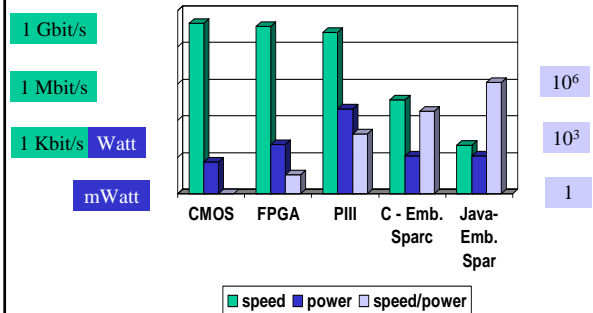
- security for 50-100 years
- authenticated encryption of Terabit/s networks
- ultra-low power/footprint



61

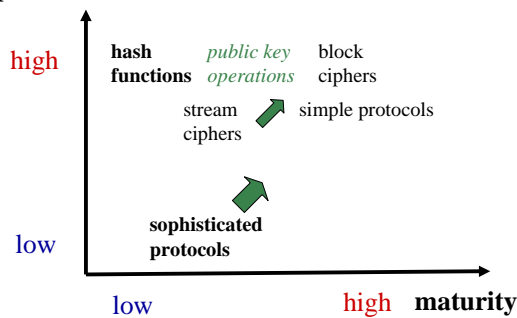
### The power challenge:

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



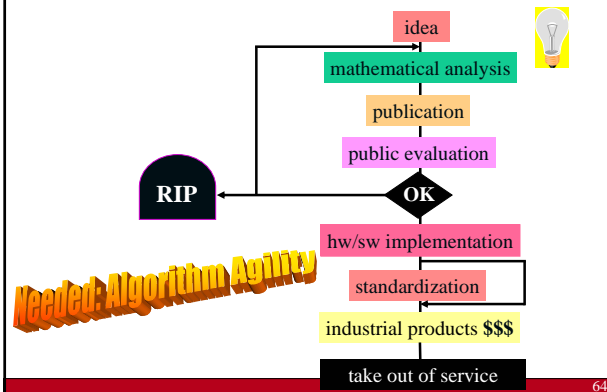
62

### demand in applications



63

### Life cycle of a cryptographic algorithm



64

### Challenges for advanced crypto

- privacy enhancing technologies
- linking crypto with physical world
  - biometrics, physically uncloneable functions
- distributed secure execution
- whitebox cryptography
- cryptography in the encrypted domain
  - searching in encrypted databases - data mining on health care data
  - zero knowledge watermarking - intelligent media sharing
- perceptual hashing
- crypto for nanotechnology

65

### Conclusions

- The “security problem” is not solved
  - Many challenging problems ahead...
  - Make sure that you can upgrade your crypto algorithm and protocol
  - Bring advanced cryptographic protocols to implementations

When will the IACR hold its elections on-line?  
 When will everyone pay with e-cash?  
 Can we reconcile privacy, DRM and data mining?

66