



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

Research Challenges in Applied Cryptography

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

December 2011

Information processing

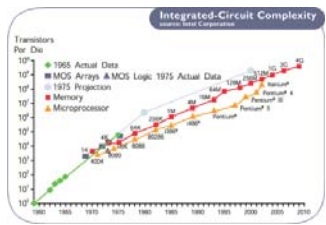
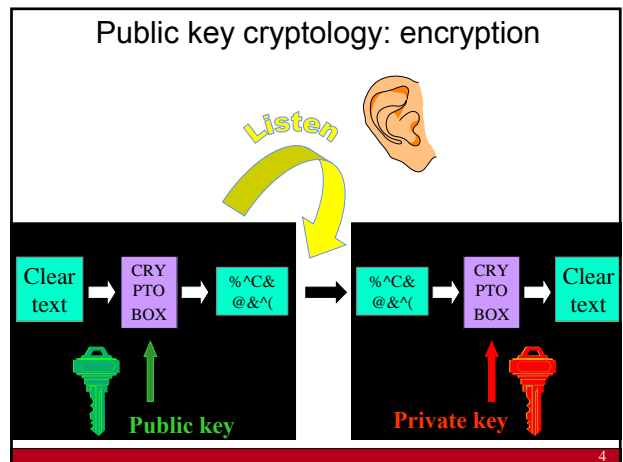
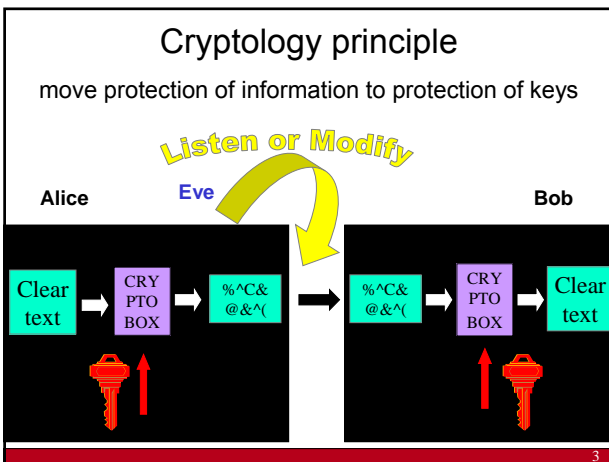
the Internet of things,
ubiquitous computing,
pervasive computing,
ambient intelligence (10^{12})

Internet and mobile (10^9)

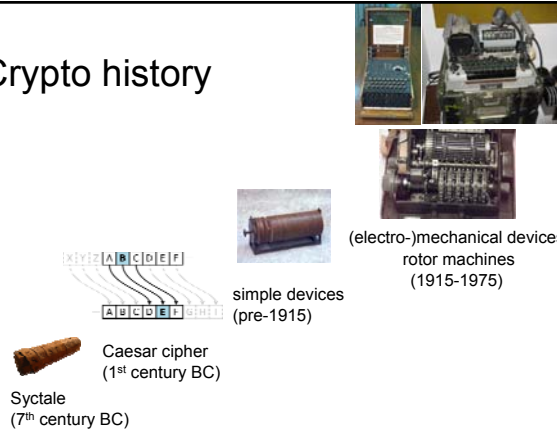
PCs and LANs (10^7)

mainframe (10^5)

mechanical (10^4)

Crypto history



Syciale (7th century BC)

Caesar cipher (1st century BC)

simple devices (pre-1915)

(electro-)mechanical devices rotor machines (1915-1975)

Crypto hardware (1965-...)



Crypto software (1990-...)

7

Crypto “everywhere”

Everything is always connected everywhere

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

10

Use of crypto

COMSEC

9

COMSEC

	Confidentiality	Data authentication	Entity authentication	
1 G (analog)				} Not end to end
2 G (GSM)	weak		unilateral	
3G				
WLAN				
TLS			unilateral	
IPsec		optional ☺		
Skype	not open	not open	not open	

10

Use of crypto: COMPUSEC

- **Data at rest:**
 - Hard disk (Bitlocker)
 - Database
 - Floppy disk/CD/USB
 - Mobile devices
- **Secure execution:**
 - TPM
 - ARM TrustZone
 - Apple DRM

11

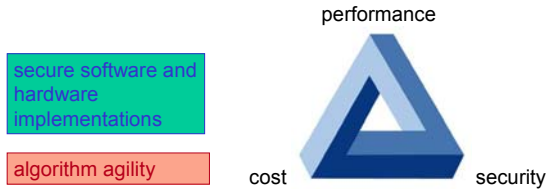
Security for everyone?

warning: this is an oversimplification
– e.g. privacy is a security property

12

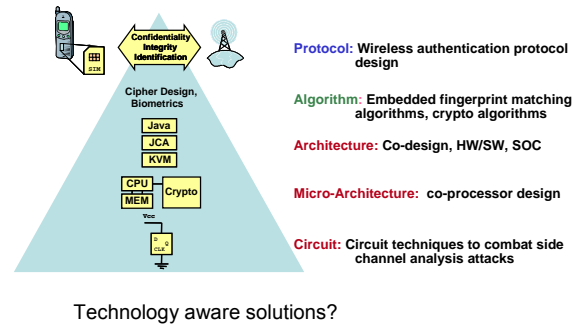
Challenges for crypto

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



13

Implementations in embedded systems



Slide credit: Prof. Ingrid Verbauwhede

14

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

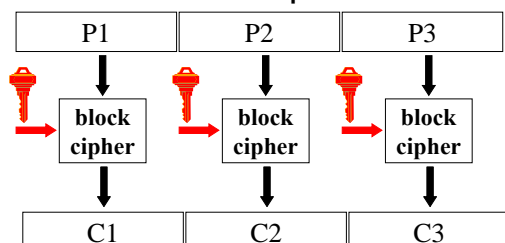
15

Outline

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

16

Block cipher



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

17

DES (1977)



- 56-bit key length is too short
- 25/10/99: DES reaffirmed for the 4th time as FIPS 46-3
- 2011: \$1 million search machine: 3 seconds
 - cost per key: less than \$0.10
- 2011: 80 PCs at night: 1 month
 - cost per key: essentially 0

18

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.

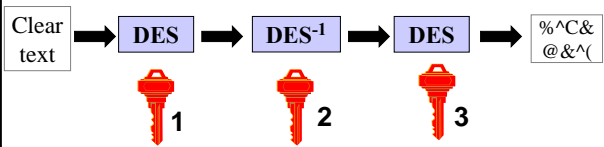
ACTION: Notice; request for comments.

- 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).


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)



AES (2001)



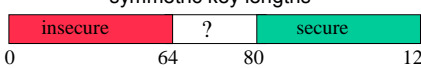
- FIPS 197 published on December 2001
 - other standards: ISO, IETF, IEEE 802.11,...
- fast adoption in the market
 - except for financial sector
 - NIST validation list: 1884 implementations
 - <http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>
- 2003: AES-128 also for **classified** information and AES-192/256 for **secret** and **top secret** information!

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

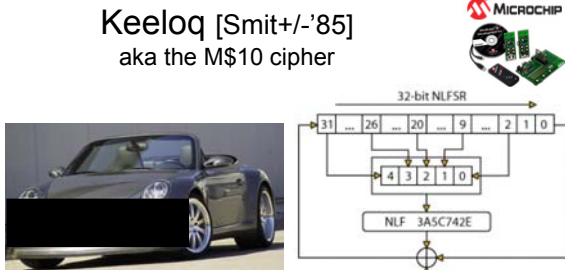
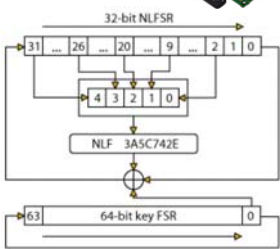
Block ciphers

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
GOST* (256)		CLEFIA
KASUMI** (128-3G, 64-2G)		
HIGHT** (128)		
PRESENT (80-128)		
TEA (128)		
mCrypton (96-128)		
KATAN64 (80)		
KTANTAN64* (80)		
KLEIN* (64-96-128)		
DESXL (144)		
LED (64-128)		
PICCOLO (80-128)		

56 bits: < 1 hour with M\$ 5
80 bits: 2 year with M\$ 5
128 bits: 256 billion years with B\$ 5



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

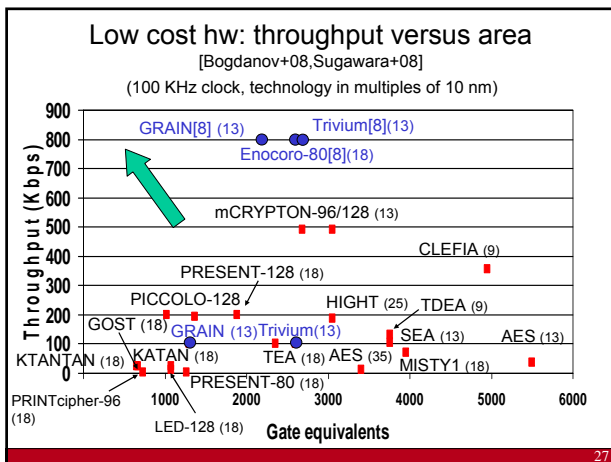
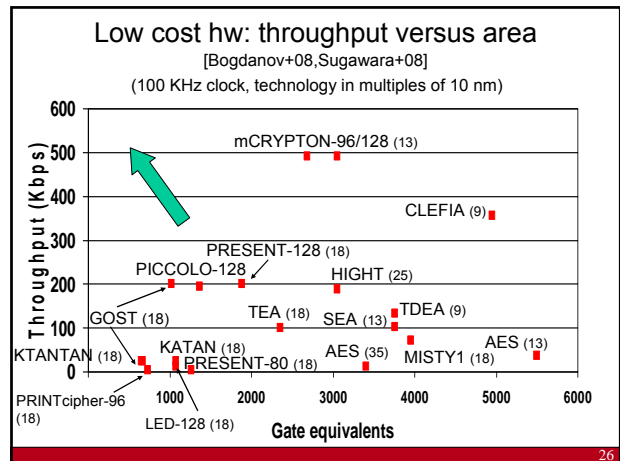
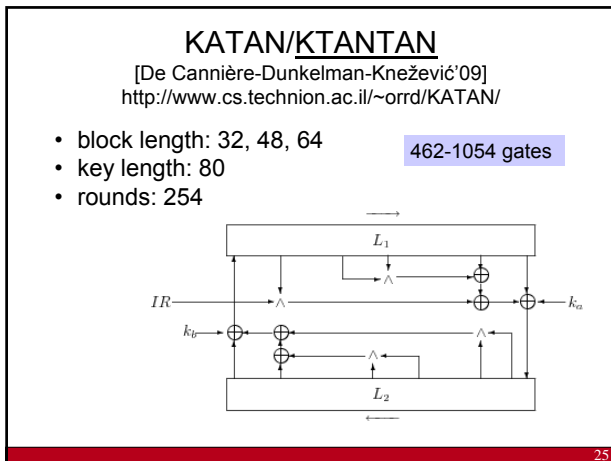



- allegedly used in large % of the cars for car locks, car alarms
- block cipher with 32-bit blocks, 64-bit keys and 528 simple rounds
- leaked on the internet early 2007

Block ciphers: Keeloq (2)

- [Bogdanov07] Car key = Master key + Car ID
- [Biham-Dunkelman-Indesteeghe-Keller-Preneel07]:
 - 1 hour access to token + 2 days of calculation
- [Eisenbarth-Kasper-Moradi-Paar-Salmasizadeh-Manzuri-Shalmani-Paar 08]
 - **Side channel attack allows to recover master key in hopping mode**

in 2012 cryptographers will drive expensive cars



Block ciphers: conclusions

- several mature block ciphers available
- security well understood
 - in particular against statistical attacks (differential, linear) and structural attacks
- more work:
 - key schedule and related key attacks
 - algebraic attacks
 - structural tradeoffs
- what are the limitations for lightweight ciphers?
 - energy ↔ power
 - software ↔ hardware
 - key schedule ↔ hardcoded key

28

Authenticated encryption

- default modes: ECB/CBC/CFB/OFB and CTR
- needed for network security, but only fully understood by crypto community around 2000 (too late)
- new standards:
 - CCM: CTR + CBC-MAC [NIST SP 800-38C]
 - GCM: CTR + GMAC [NIST SP 800-38D]
- both are suboptimal: **new ideas needed**

goals:

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

- IAPM
- XECB
- OCB

- GCM
- CCM
- EAX

patented

29

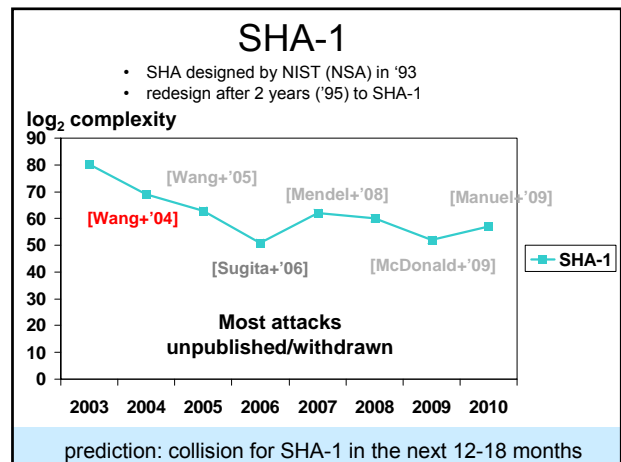
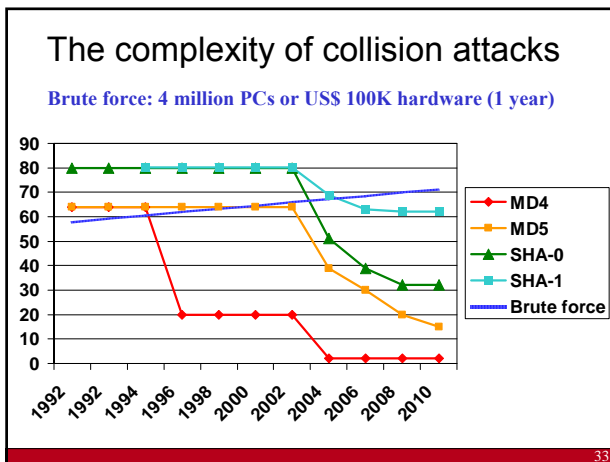
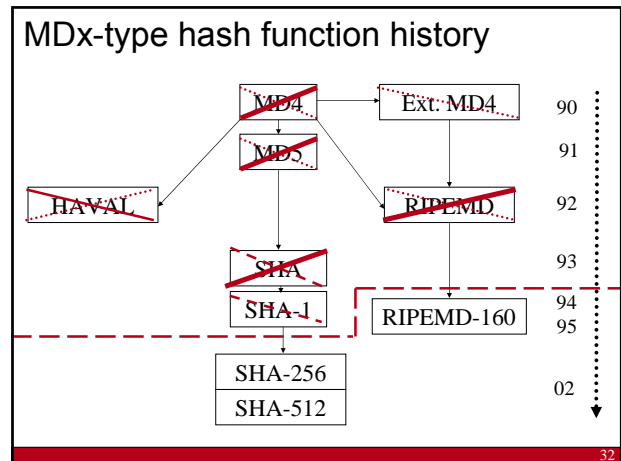
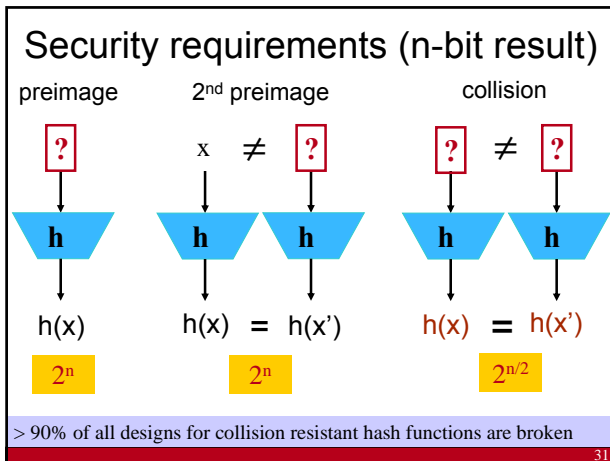
Hash functions

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

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).

1A3FD4128A198FB3CA345932

30



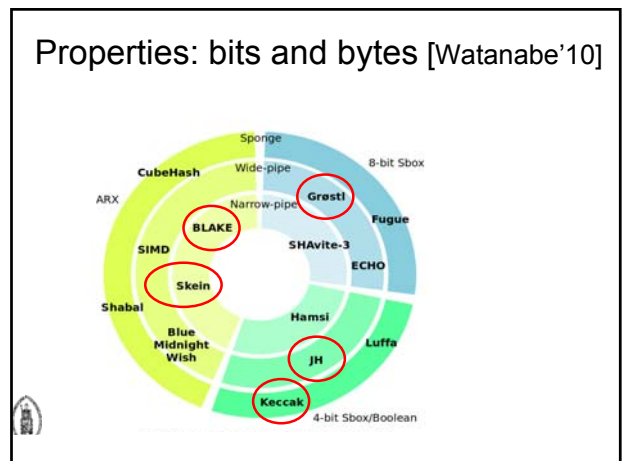
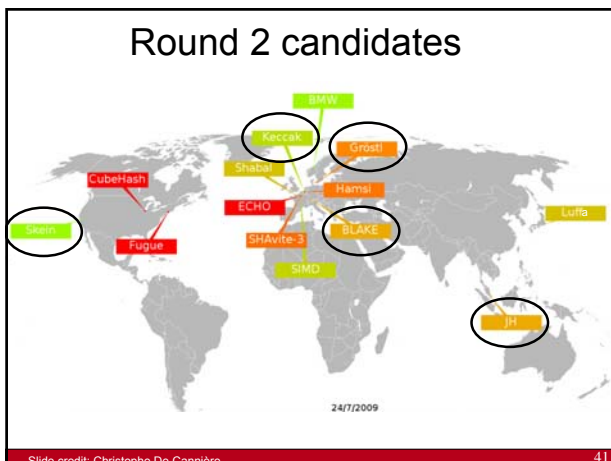
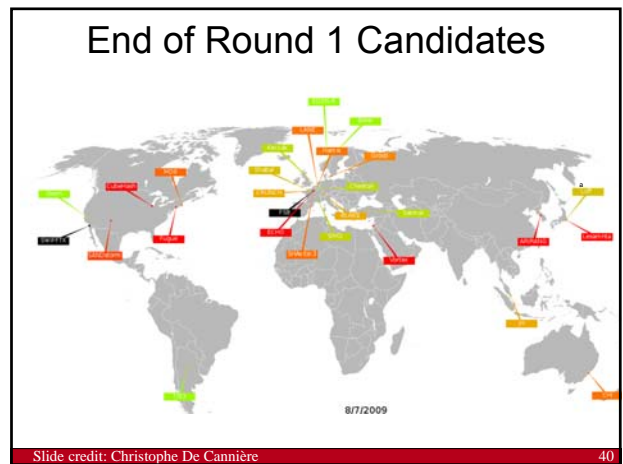
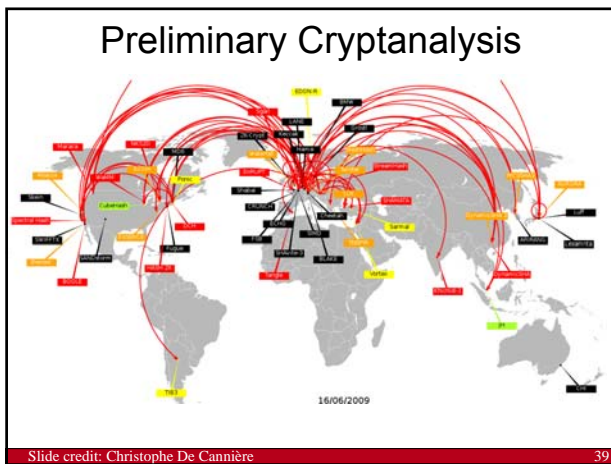
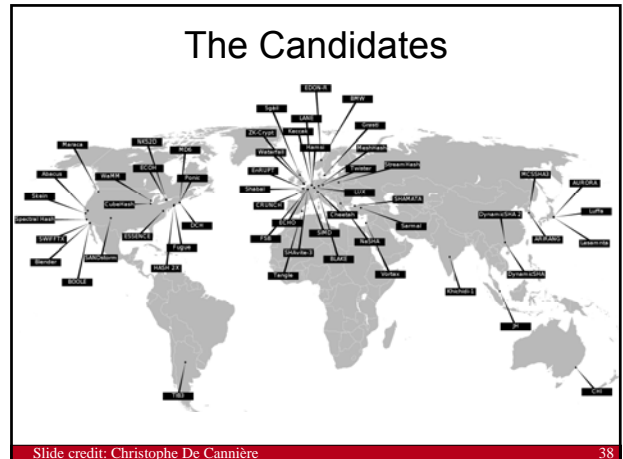
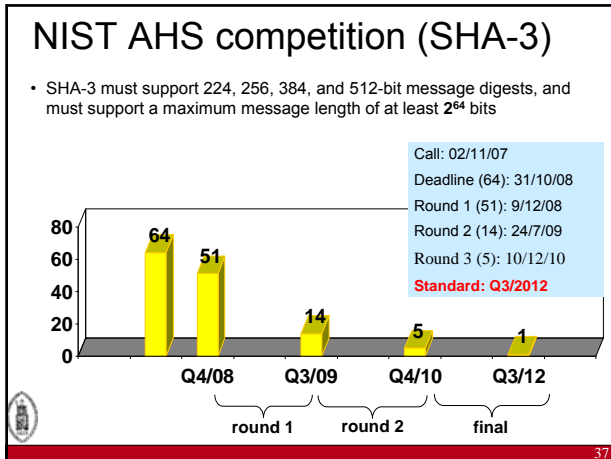
Hash function attacks:

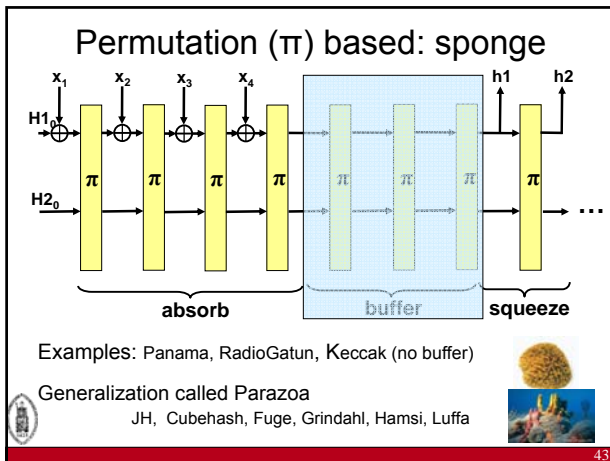
cryptographic **melt**down yet with limited impact

- 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]
- high profile **attack on CAs** in December 2008
- TLS/SSL: MD5 || SHA-1 for algorithm negotiation
 - but this algorithm cannot be negotiated
 - need new version: TLS 1.1 -> 1.2
- HMAC: HMAC-SHA-1 ok

Hash function: quick replacements

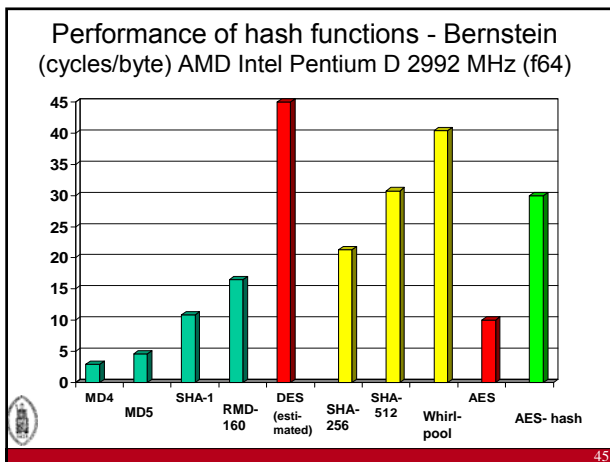
- RIPEMD-160 seems more secure than SHA-1 ☺
- use more recent standards (slower and larger)
 - SHA-2 (SHA-256, SHA-224, ... SHA-512)
 - On some 64-bit machines SHA-512 is faster than SHA-256
 - [Mendel+11] 32/64 steps collisions 1 hour on a cluster
 - 47/64 steps is non-random
 - Whirlpool
 - SHA-3....





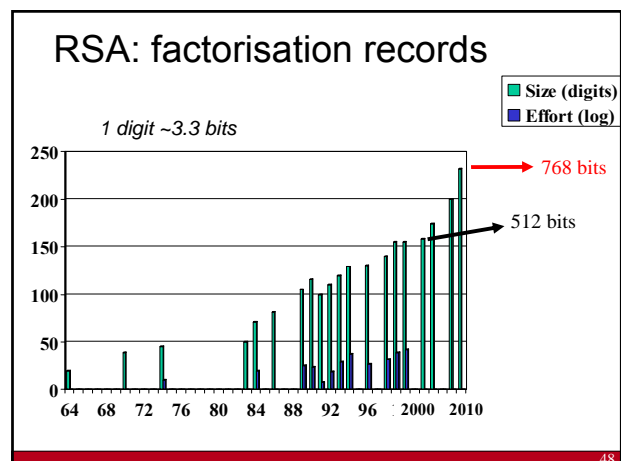
Security reductions [Andreeva-Mennink-P'10]

	compression function			hash function			
	pre	sec	col	pre	sec	col	indiff
BLAKE							
BMW							?
CubeHash							
ECHO					?		?
Fugue							
Grøstl							
Hamsi							?
JH							
Keccak							
Luffa							?
Shabal							
SHAvite-3							
SIMD							?
Skein							
SHA-2							



- ### 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
 - lightweight hash functions under development

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



Factorisation

- record in January 2010: 768-bits (or 232 digits) using NFS
- record in May 2007: $2^{1039}-1$ (313 digits) using SNFS
- “old” 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 2013 and 1024-bit factorization in 2020?

49

Key lengths for confidentiality

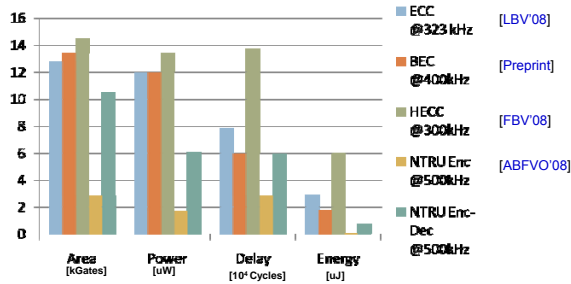
<http://www.ecrypt.eu.org>

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

50

Public key performance comparison



Slide credit: Prof. Ingrid Verbauwhede 51

Public key: attacks on modes

- EIGamal/ECDSA: problems with randomness in digital signatures
 - DSA problem [Bleichenbacher01]
 - GPG problem [Nguyen03]
 - PSP problem [Hackers11]
- ISO 9796-2 attacks [Coron+'09]
- Verification attack on PKCS#1v1.5 [Bleichenbacher06]
- Padding oracle attacks on PKCS#1 v1.5 (chosen ciphertext) [Bleichenbacher01], [Manger01]

52

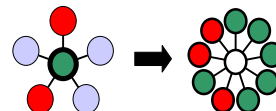
Protocols (1)

- 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

53

Advanced protocols

- 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”

stop building databases with policies – go for privacy by design with true data minimization

54

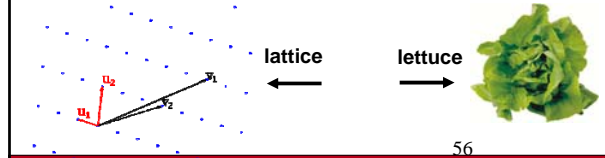
Multi-party computation becomes "truly practical"

- Similar to first public key libraries 20 years ago
 - EU: CACE project (Computer Aided Cryptography Engineering), www.cace-project.eu
 - US: Brown Univ. + UCSD (Usenix 2010)
- Examples
 - efficient zero-knowledge proofs
 - 2-party computation of AES (Bristol)
 - secure auction of beetroots in Denmark (BRICS)
 - oblivious transfer for road pricing (COSIC)

55

Fully homomorphic encryption

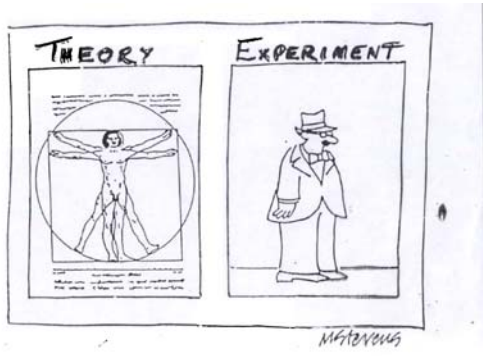
- From $E(x)$ and $E(y)$, you can compute $E(x+y)$, $E(c \cdot x)$ and $E(x \cdot y)$ **without decrypting**
- Many cool applications including cloud computing
- [Gentry'09] ideal lattices = breakthrough
- First implementations require only seconds [Vercauteren-Smart'10], [Gentry-Halevi'10], ...
 - but to ciphertext for 1 bit is 3 million bits and public key is several Mbyte



56

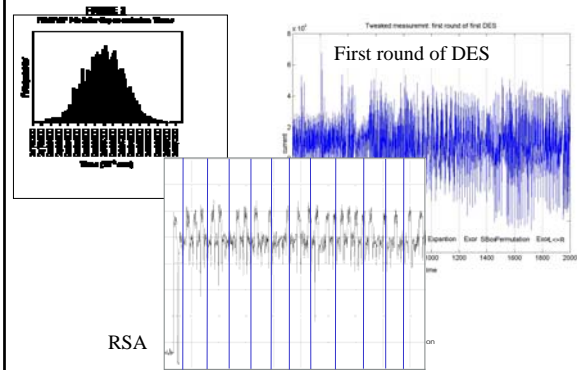
56

Theory versus Experiment



57

Implementations: side channel attacks



58

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)
- combine with statistical analysis and cryptanalysis
- software: API attacks
- major impact on implementation cost

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

59

Outline

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

60

Challenges for long term security

- cryptanalysis improves:
 - mathematical attacks
 - 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

61

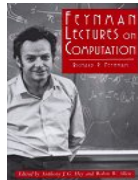
Many proprietary or secret ciphers have been leaked and broken

- Content Scrambling System (CCS) in DVD
- A5/1 and A5/2 in GSM
- E0 in Bluetooth
- DST (TI) in ignition keys
- Keeloq in remotes
- Hitag 2
- Crypto-1 in Mifare Classic
- SecureMemory, CryptoMemory, CryptoRF
- [...]

62

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?



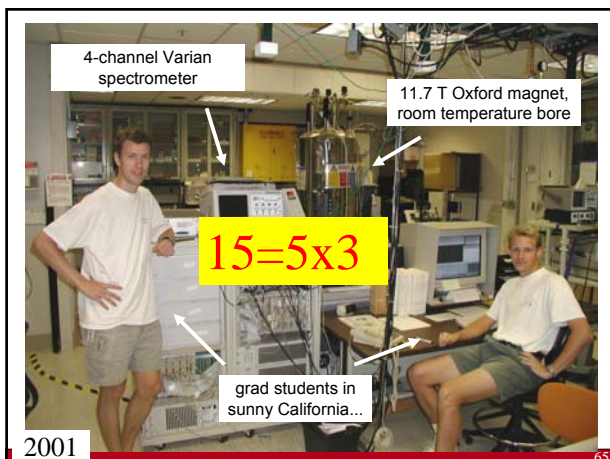
63

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: x2 for preimage resistance
- alternatives: McEliece, HFE, NTRU, ...
- so far it seems very hard to match performance of current systems while keeping the security level against conventional attacks



64



65

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
- What counts is stability, not the size of the computer

66

Layers

assumptions algorithms

Proofs: link security at different levels in a quantitative way

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

67

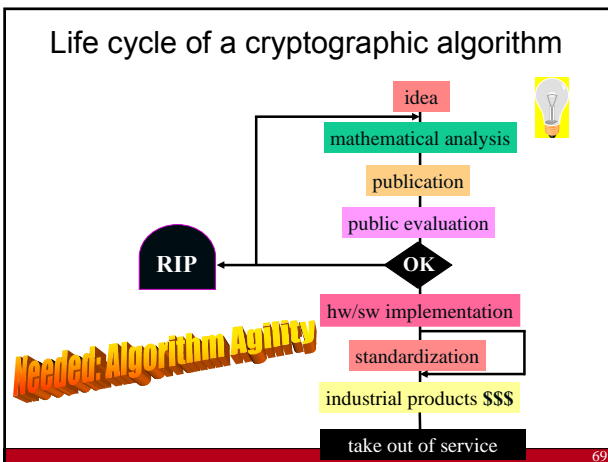
Assumptions

research on **hard problems**?

James L. Massey:
A hard problem is one that nobody works on

good lower bounds
average vs worst case
find new hard problems

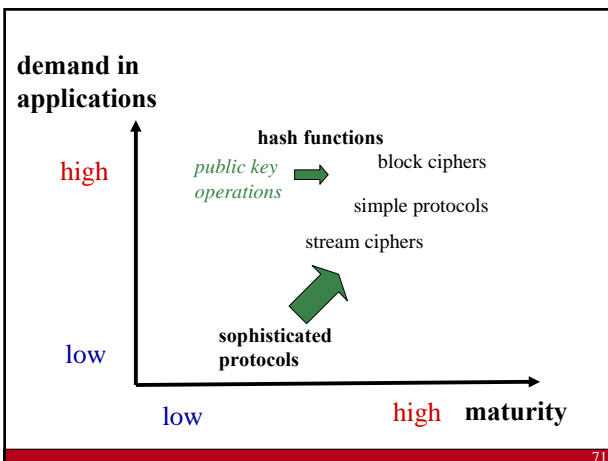
68



Challenges for crypto

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

70



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

72

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 everyone pay with e-cash?

Can we reconcile privacy, DRM, cloud computing and data mining?

73

The end



Thank you for
your attention

74