

**ECRYPT II**  
IF810A-1  
http://www.ecrypt.eu.org

**ISSE** 2010

## The Cryptographic Year in Review

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

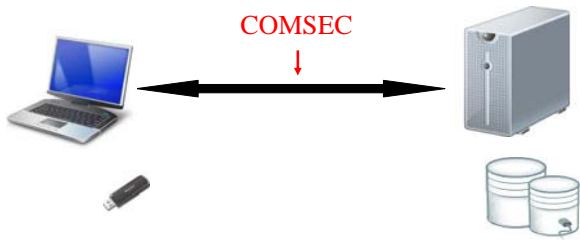
October 2010




**ISSE** 2010

### Use of crypto

**COMSEC**



**COMSEC** **ISSE** 2010

	Confidentiality	Data authentication	Entity authentication
1 G (analog)			
2 G (GSM)	weak		unilateral
3G			
WLAN			
TLS			unilateral
IPsec		optional ☹	
Skype	not open	not open	not open

Not end to end

**ISSE** 2010

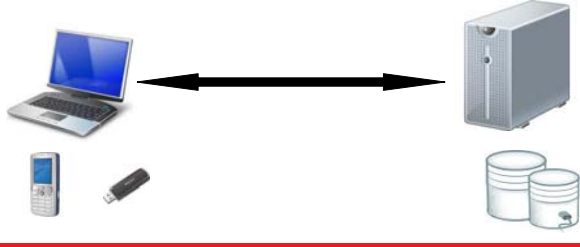
### Use of crypto: COMPUSEC

**Data at rest:**

- Hard disk (Bitlocker)
- Database
- Floppy disk/CD/USB
- Mobile devices

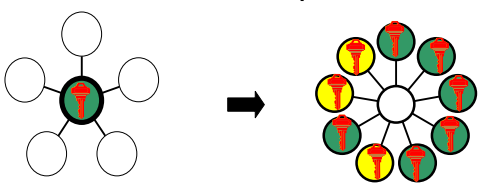
**Secure execution:**

- TPM
- ARM TrustZone
- Apple DRM



**ISSE** 2010

### Secure Computation

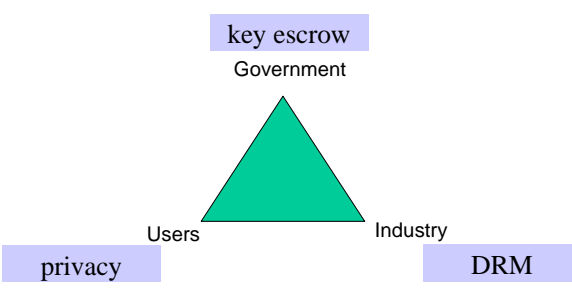


- PKI
- Banking
- Credit card
- Google
- ...

- Multi-party computation

**ISSE** 2010

### Security for everyone



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

### 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
  - Stream ciphers
  - Hash functions
  - Public-key cryptology
- Protocols
- Hacks

### Block ciphers

• larger data units: 64...128 bits

• memoryless

• repeat simple operation (round) many times

### AES

NIST validation list: 1468 implementations

- <http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>

### AES variants (2001)

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

### AES: security

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

### What is a related key attack?

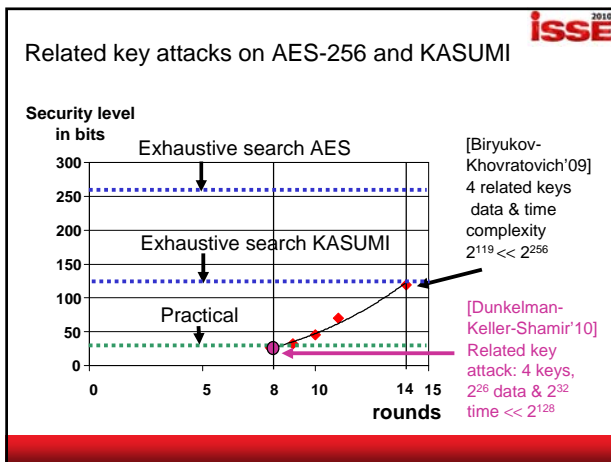
Attacker chooses **plaintexts** and **key difference C**  
Attacker gets **ciphertexts**  
Task: find the **key**

### 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

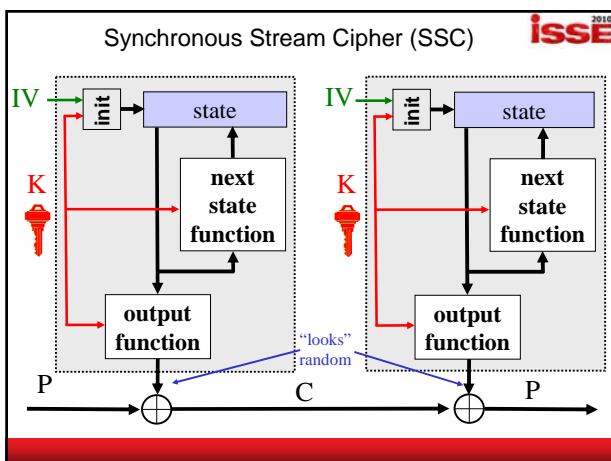
This is a very powerful attack model: if **XOR** is replaced by **AND**, any cipher can be broken

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



### 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 the GSM or 3G context



### GSM

- A5/1 weak
  - [Barkan+03] requires seconds (software not available so requires math)
  - [Nohl10]: Kraken = 2 Terabyte of Rainbow tables <http://reflector.com/trac/a51>
- A5/2 trivially weak (milliseconds)
- A5/3 (=Kasumi) seems ok but not yet used (even if in 1.2 billion out of 3 billion handsets)
- Even simpler attacks
  - eavesdrop after base station (always cleartext)
  - switch off encryption (can be detected)

### GSM

- growing number of open source tools to intercept: GnuRadio, Airprobe, OpenBTS
- but needs more work (1-2 years?)

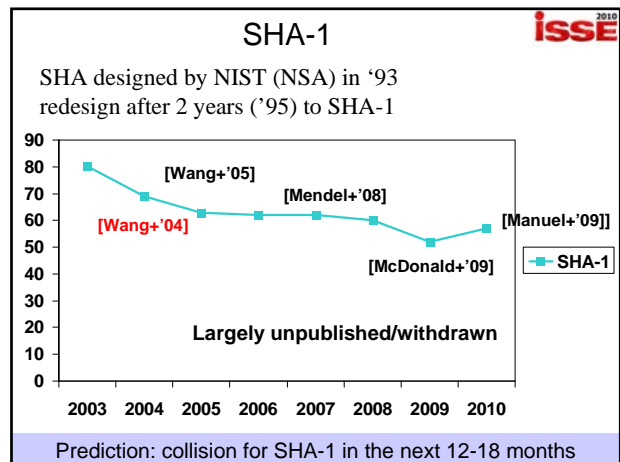
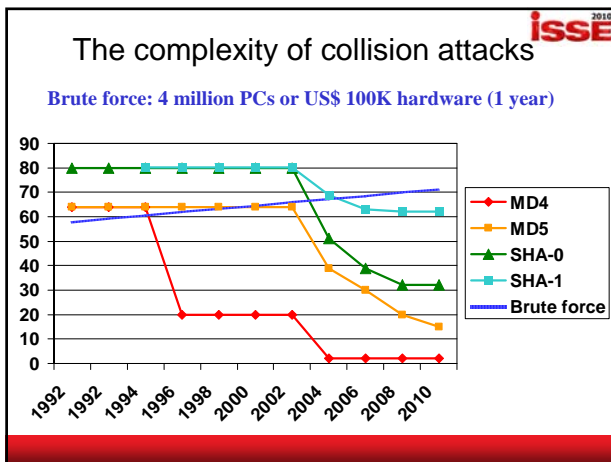
- be careful when rolling out 2-factor authentication via SMS
- intercepting mobile phone traffic is illegal

### Hash functions

Protect short hash value rather than long text

collision resistance  
preimage resistance  
2<sup>nd</sup> 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).*



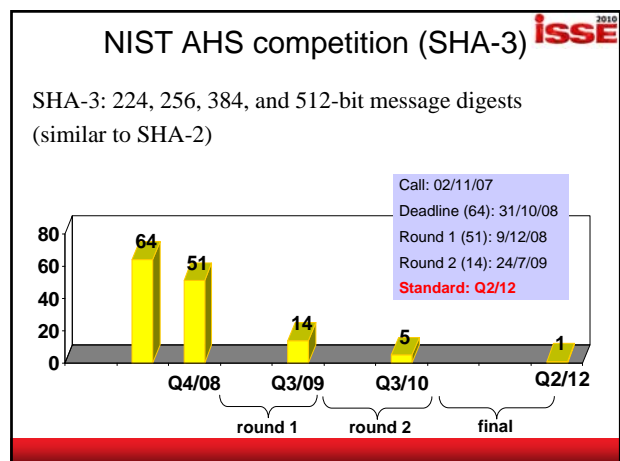
### Alternatives in ISO 10118-3

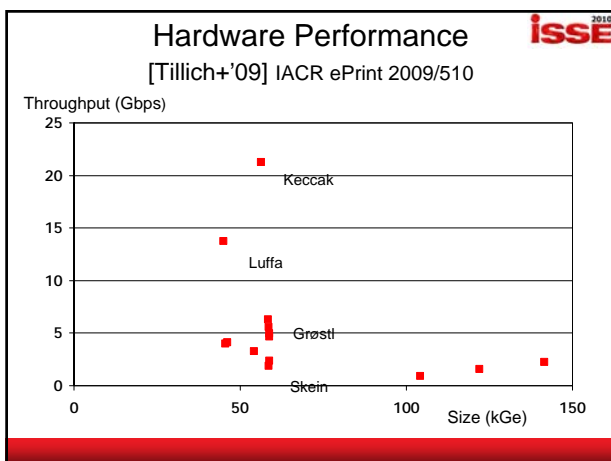
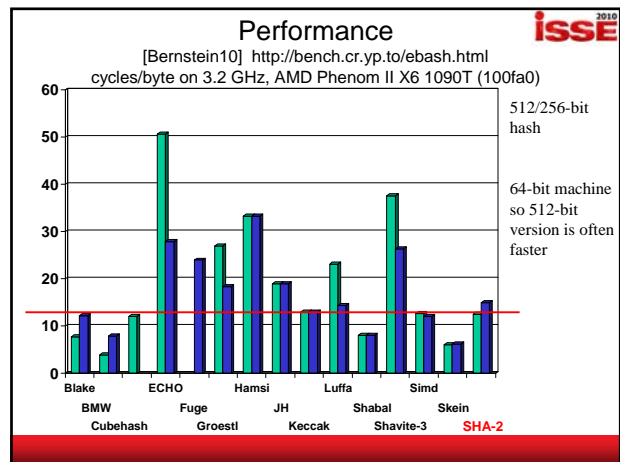
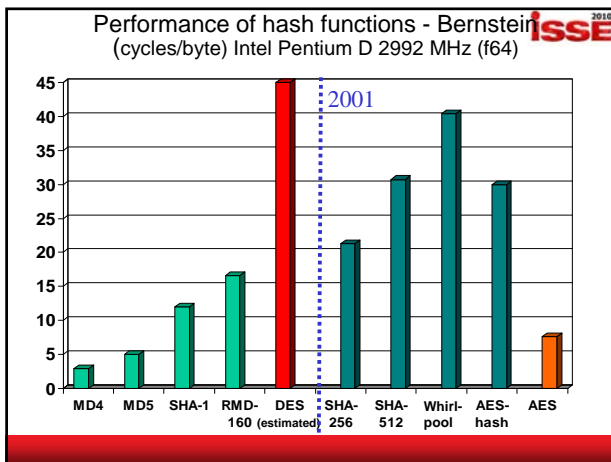
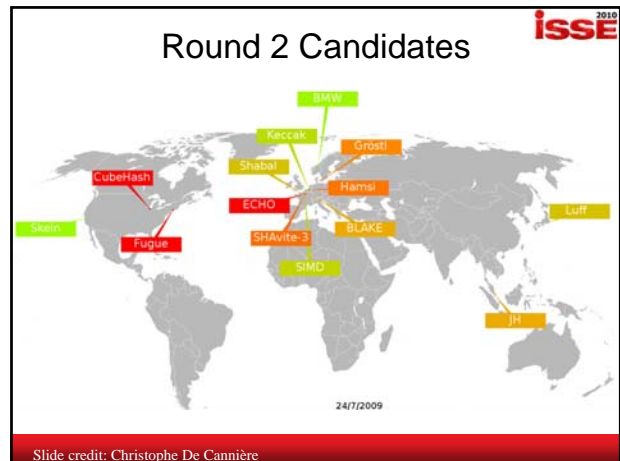
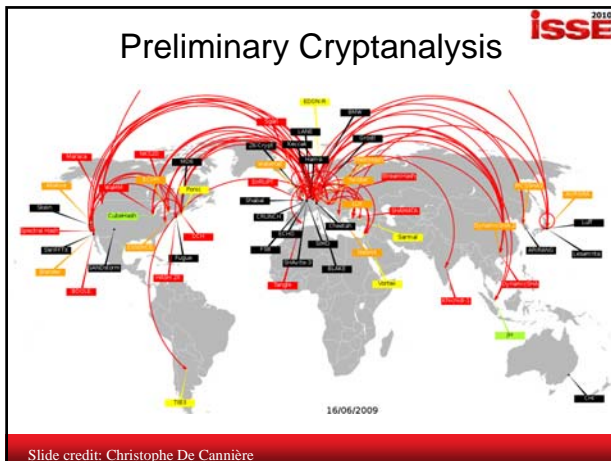
SHA-2 current standard for NIST

- So far no real progress in cryptanalysis

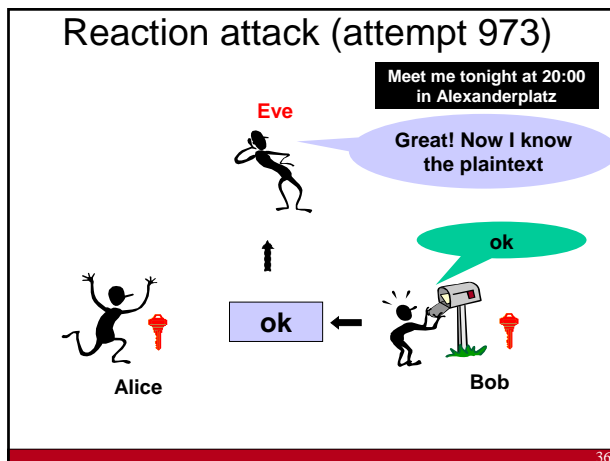
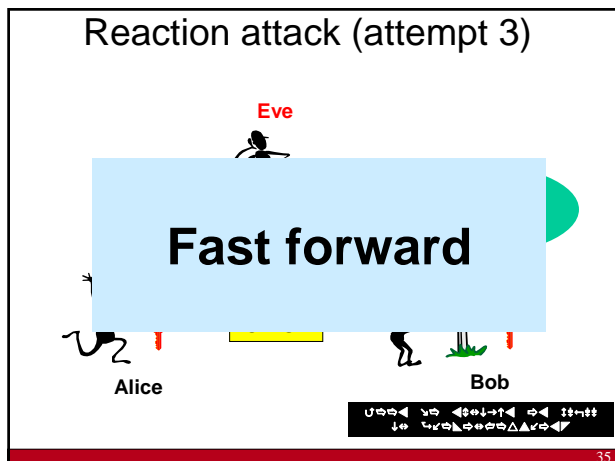
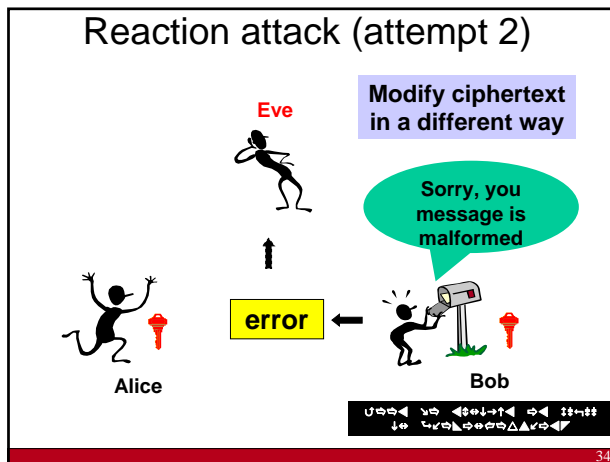
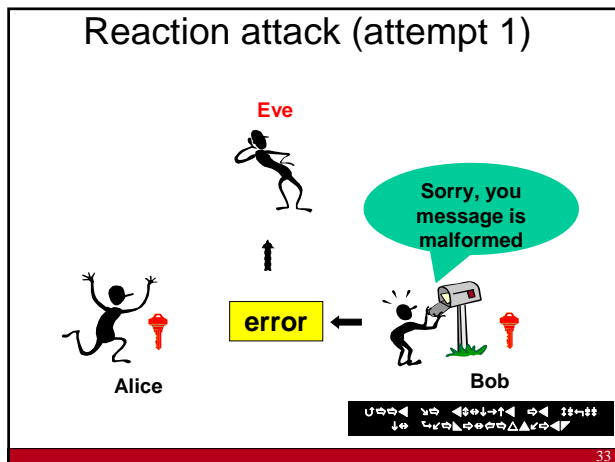
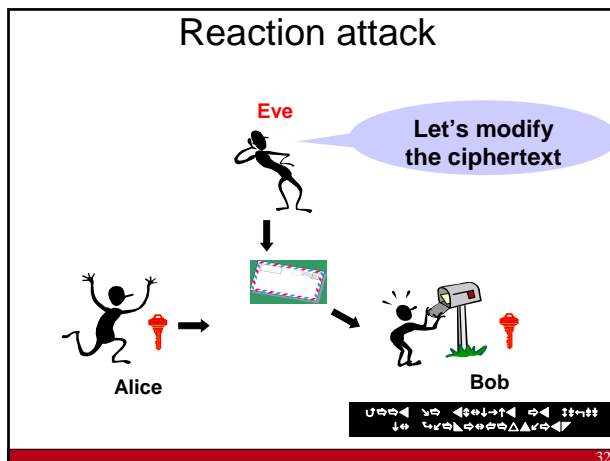
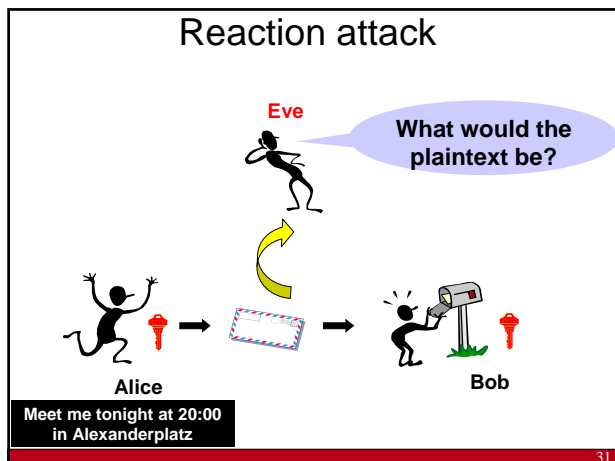
Whirlpool: not too fast

RIPEND-160: 80-bit security against collisions





- ### Issues arisen during Round 2
- security:
    - few real attacks but some weaknesses
    - new design ideas harder to validate
    - very few provable properties
  - performance: roughly as fast or faster than SHA-2
    - SHA-2 gets faster every day
    - widely different results for hardware and software
      - software: large difference between high end and embedded
      - hardware: FPGA and ASIC
  - diversity = third criterion for the final
  - NIST expects that SHA-2 and SHA-3 will co-exist



### Reaction attacks: well known

- [Bleichenbacher98] PKCS #1v1.5 – 1 million chosen ciphertexts; improved by [Klima-Pokorny-Rosa03]
- [Manger01] OAEP PKCS #1v2 – a few 1000 chosen ciphertexts
- [Bellare-Kohno-Namprempre 02]: SSH
- [Vaudenay'02] SSL, IPsec, WTLS...
- [Canvel-Hiltgen-Vaudenay-Vuagnoux03]: SSL/TLS

#### Solution:

- don't send error messages (bad engineering practice)
- authenticated encryption: MAC the ciphertexts and do not decrypt if MAC is incorrect

37

### Authenticated encryption

- needed for network security, but only fully understood by crypto community around 2000 (too late)
- dump CBC mode
- standards:
  - CCM: CTR + CBC-MAC [NIST SP 800-38C]
  - GCM: CTR + GMAC [NIST SP 800-38D]
- both are suboptimal but patent free
- properties
  - associated data
  - parallelizable
  - on-line
  - provable security



38

### Reaction attack strikes again

- 17 Sept. 2010: major attack on ASP.NET that used CBC-AES without authenticating the ciphertext
- affects millions of web apps
- 28 Sept. 2010: patch available

39

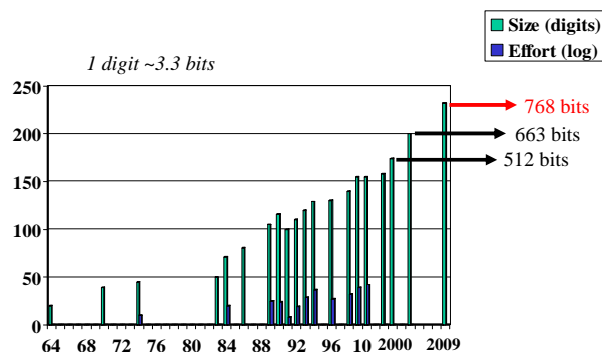
### Outline



- Context
- Cryptography
  - Block ciphers
  - Stream ciphers
  - Hash functions
  - Public-key cryptology
- Protocols
- Hacks

### Factorisation records

Dec 2009: 768 bits or 232 digits



### Factorisation



record in May'07:  $2^{1039}-1$  (313 digits) using SNFS

new record in Dec'09: 768 bits (or 231 digits) using NFS

$2^{67}$  instructions or 2000 "2.2GHz AMD Opteron" years

1024 bits:

- 1000 times harder than 768 bits
- feasible in academic community in period 2015-2017

## Factorisation

**ISSE** 2010

Governments/organized crime want to factor multiple integers – will use dedicated hardware

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 2015?

## Cryptographic protocols

- SK entity authentication
  - be suspicious of “optimized” RFID protocol with a “security proof”
- secret key establishment based on public keys: essential for Internet protocols
- quantum cryptography
- advanced protocols: multi-party computation

## 2 main options for key establishment in TLS

**RSA with long term keys**

choose  $k$   $\xrightarrow{RSA_{PK_B}(k || tA)}$  decrypt with  $SK_B$  to get  $k$

**Signed Diffie-Hellman (STS)**

choose  $x$   $\xrightarrow{\alpha^x}$  choose  $y$

$k=(\alpha^y)^x$   $\xleftarrow{\alpha^y}$   $k=(\alpha^x)^y$

$\sqrt{SigB}$   $\xleftarrow{SigA(\alpha^x, \alpha^y)}$   $\sqrt{SigA}$

## Diffie-Hellman/STS offers one major advantage

- **forward secrecy**: compromise of long term private keys does not expose past session keys
  - Motivation: Google/China incident
- but more expensive
  - 3 moves rather than 1
  - more public operations
  - incompatible with TLS optimizations such as session caching, session tickets, false start

## How to solve this

- [Käsper10] optimize OpenSSL
- ECC (NIST P-224 curve) + RSA-1024

**Intel Core 2 - Handshakes/second**

Configuration	Handshakes/second
RSA-1024	~900
224-ECC	~300
224 ECC (opt)	~700

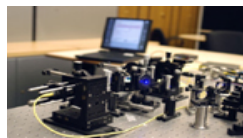
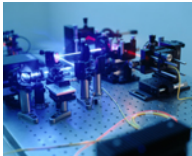
## SSL/TLS

- SSL/TLS well studied
- OpenSSL widely used
- Yet
  - reconnection flaw
  - MiTM by governments
  - 100+ names per certificate



## Quantum cryptography

- Security based
  - on the assumption that the laws of quantum physics are correct
  - rather than on the assumption that certain mathematical problems are hard



49

## Quantum cryptography

- no solution for entity authentication problem (bootstrapping needed with secret keys)
- no solution (yet) for multicast
- dependent on physical properties of communication channel
- cost
- implementation weaknesses (side channels)

50

## Quantum hacking

<http://www.iet.ntnu.no/groups/optics/qcr/>

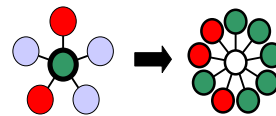


51

## 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

## 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](http://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)

53

## Anonymous credentials

- Chaum in the 1980s: science fiction
  - Proof knowledge of a signature
  - Rather than possession of a private signing key
  - Can also prove predicates on attributes
  - Verifier gains no additional information
    - Except in case of abuse – judge can intervene
  - Secure even if Issuer and Verifier collude (single/multiple show)
- Concrete protocols
  - Chaum-Pedersen and Brands: Credentica – U-Prove (Microsoft)
  - Camenish-Lysyanskaya - Idemix (IBM)
  - DAA in TPM

Recent announcement: patents will be freed

54

### Internet voting

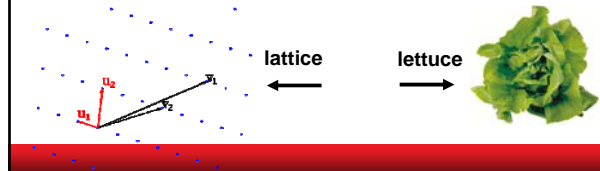
- Helios [Adida'08] [www.heliosvoting.org](http://www.heliosvoting.org)
    - sophisticated cryptographic protocols: open audit
    - open source
  - Spring 2009: rector elections in UC, Belgium
  - August 2010: adopted by IACR
  - +
    - remote voting
    - as everything is encrypted, log files can be made public so disputes can be resolved easily
  - --
    - coercion risk
    - Trojan or virus can easily undermine these elections (proof of concept [Desmedt'09])
- not suitable for public sector elections

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



### Protocols: conclusions

- more modularity and less complexity would be desirable, but large body of legacy standards and code that is hard to change
- public key operations are still a bottleneck at the server side
- advanced protocols can bring added value from the simple (password-based AKE) to more complex multi-party interactions

57

### “Hacked”



- May 2010: Car systems
  - Experimental Security Analysis of a Modern Automobile
- May 2010: EMV
  - Chip and PIN broken
- July 2010: ATM machines
  - Jackpotting Automated Teller Machines Redux
- July 2010: stuxnet worm SCADA systems
- Sept 2010: HDCP

### Privacy violations



### Bad news: the CA mess



[Eckersley10] “An observatory for the SSLiverse”

- 10.8M servers start SSL handshake
- 4.3M use valid certificate chains
- 1482 CA certs trustable by Windows or Firefox
- 1.4M unique valid leaf certs
  - 300K signed by one GoDaddy cert
- 80 distinct keys used in multiple CA certs
- several CAs sign the IP address 192.168.1.2 (reserved by RFC 1918)
- 2 leaf certs have 508-bit keys
- Debian OpenSSL bug (2006-2008)
  - resulted in 28K vulnerable certs
  - fortunately only 530 validate
  - only 73 revoked

How can we fix this mess?

## Good news: DNSSec



- long and winding road (started in 1997)
- several attacks (e.g. cache poisoning [Kaminsky08])
- several TLDs signed 2005-2009
- live in July 2010 for root
- Versign will sign .com early 2011

- <http://www.root-dnssec.org/>
- <http://ispcolumn.isoc.org/2006-08/dnssec.html>

## 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



## Challenges for advanced crypto



- privacy enhancing technologies
- linking crypto with physical world
  - biometrics, physical uncloneable functions
- distributed secure execution
- whitebox cryptography
- crypto for nanotechnology

## Conclusion



- interesting and challenging mathematical problems, w.r.t. foundations and engineering aspects
- make sure that you can upgrade your crypto algorithms and protocols
- lattice based crypto is not a silver bullet for the cloud
- multiparty computation becomes practical

**2010 was an exciting crypto year**

... and IACR uses remote e-voting

# The end



Thank you for  
your attention