

Cryptology Update 2009

Christian Cachin

IBM Research - Zurich & EPFL, LPD

2 December 2009

History of cryptology

- Caesar (~50 BC)
 - First documented use of cryptology
 - Military purpose
 - Mary I of Scotland (1586)
 - Conspiracy against her exploited cryptanalysis
 - Diplomatic purpose
 - Zimmermann telegram (1917)
 - Note from Berlin to German Ambassador in US
 - Deciphered by the British, caused US to enter WW I
 - Cryptanalysis of German Enigma (1939-45)
 - Allies benefited in WW II
-
-

The birth of modern cryptology

- Inter-bank and intra-bank networks
 - **Commercial use**
 - **DES: block cipher standard by US NIST (1975)**
 - With alleged input by NSA (US signal intelligence agency)
 - Public-key cryptography (1976)
 - **Scientific interest**
 - Cryptology as a science (today)
 - **Independent domain**
 - **Links to mathematics, theoretical computer science, algorithms, and electrical engineering**
-
-

Cryptology today

Cryptography is almost never to blame for security problems with IT systems.

... why look at cryptography then?



Cryptology update 2009

1. Key lengths

- Goodbye 1024-bit RSA
- Elliptic-curve cryptography

2. Hash functions

- Collisions in MD5, SHA-1 ...
- Development of new hash function

3. Protocol failures

- SSH, SSL ...

4. Key management

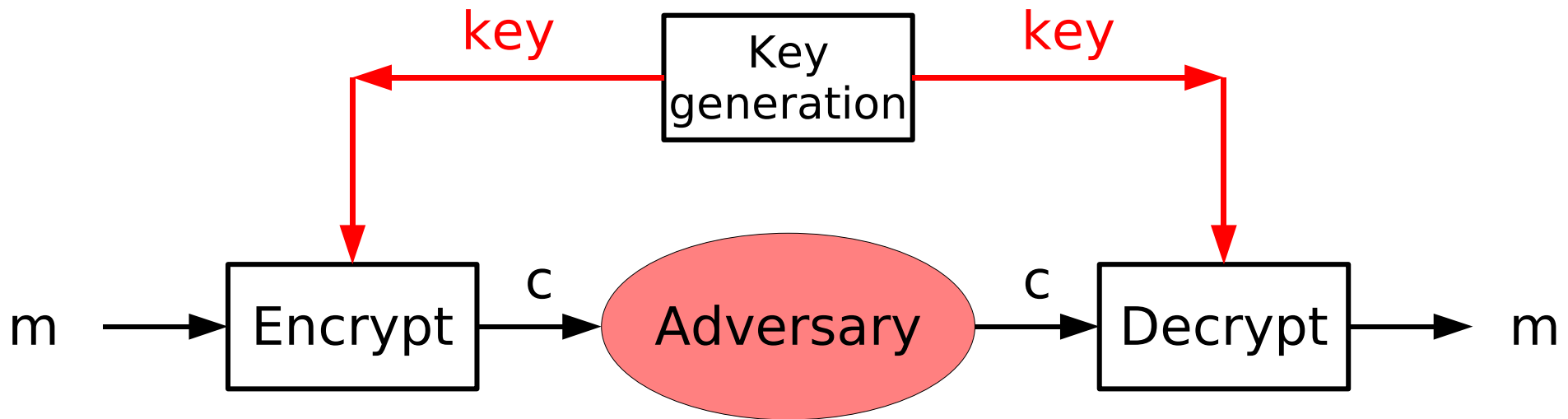
- The Achilles' Heel of cryptography



Part 1: Key lengths

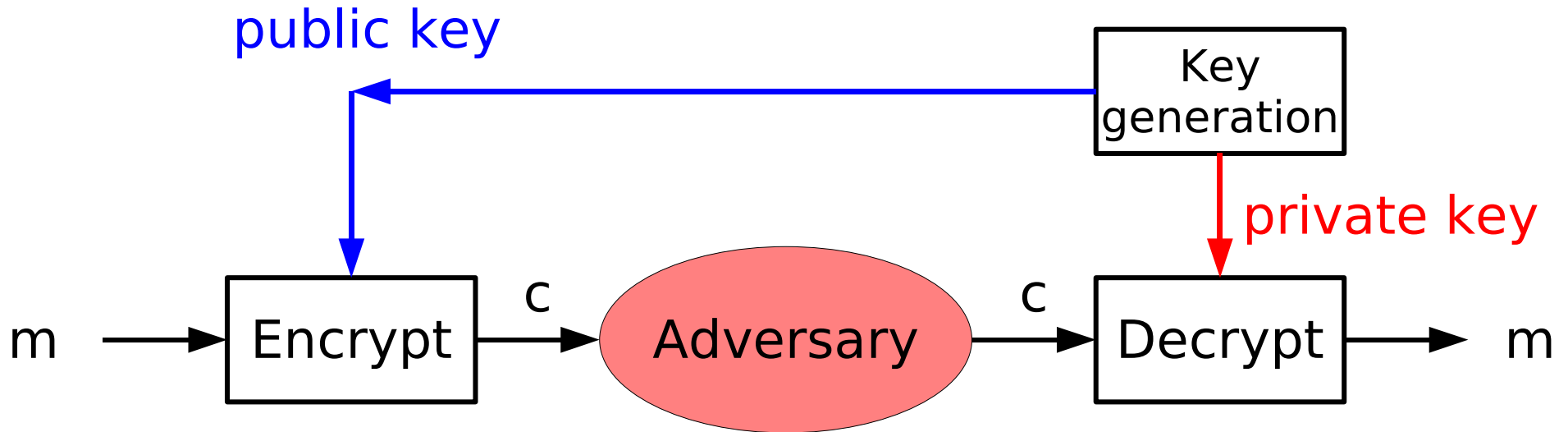


Secret-key encryption ***(Symmetric cryptosystem)***



- **Same key for encryption and decryption**
 - One key per communication
 - **Key distribution confidential and authenticated**
-
-

Public-key encryption (Asymmetric cryptosystem)



- Two keys:
 - Public key for encryption
 - Private key for decryption
 - One key per entity
 - Key distribution authenticated (certificate, PKI)
-
-

Public-key cryptosystems

- RSA - Rivest, Shamir & Adleman (1978)
 - Encryption & signatures
 - Most widely used algorithm, PKCS#1 ...
 - DH - Diffie & Hellman (1976)
 - Integers modulo prime (group Z/p)
 - DSA signatures
 - ElGamal encryption
 - Key agreement (MQV)
 - Elliptic Curve Cryptography (Miller, Koblitz ...)
 - Elliptic curve group instead of Z/p
 - Implements all DH schemes
 - EC-DSA, EC-ElGamal, EC-MQV ...
-
-

Public-key crypto maths

RSA: $N = P \cdot Q$ product of two primes
 $m \in \mathbf{Z}_N$, $\text{Encrypt}(m) = m^e \bmod N$
Security: $|N|$, length of N

DH in \mathbf{Z}/p : $y = g^x \in \mathbf{Z}_p$
 $p = a \cdot q + 1$ for primes p, q
Security: $|p|$ and $|q|$

EC-DH: y point on elliptic curve over \mathbf{F}_p
represented by $(y_0, y_1) \in \mathbf{F}_p \times \mathbf{F}_p$
Security: $|p| / 2$

Why does key length evolve?

- Moore's law (predictable)
 - Transistor count doubles every two years
- Mathematical advances (unpredictable)
 - New factoring algorithms break RSA faster
 - Differentials in hash functions (MD5, SHA-1)



Attacks at work



- 200 PlayStations 3 at LACAL/EPFL (Arjen Lenstra & team)
- Broke 112-bit EC DL problem in 2009 (after 6 months)

Cryptographic difficulty

- Difficulty grows exponentially with key length
- Example
 - $7 \cdot 10^9$ computers (one per person on earth)
 - Running at 4 GHz ($4 \cdot 10^9$ crypto ops per second)
 - Time to find key of length ...

64 bit	1 second
80 bit	12 hours
112 bit	5.9 Mio. years
128 bit	385 Bio. ($385 \cdot 10^9$) years

Security levels

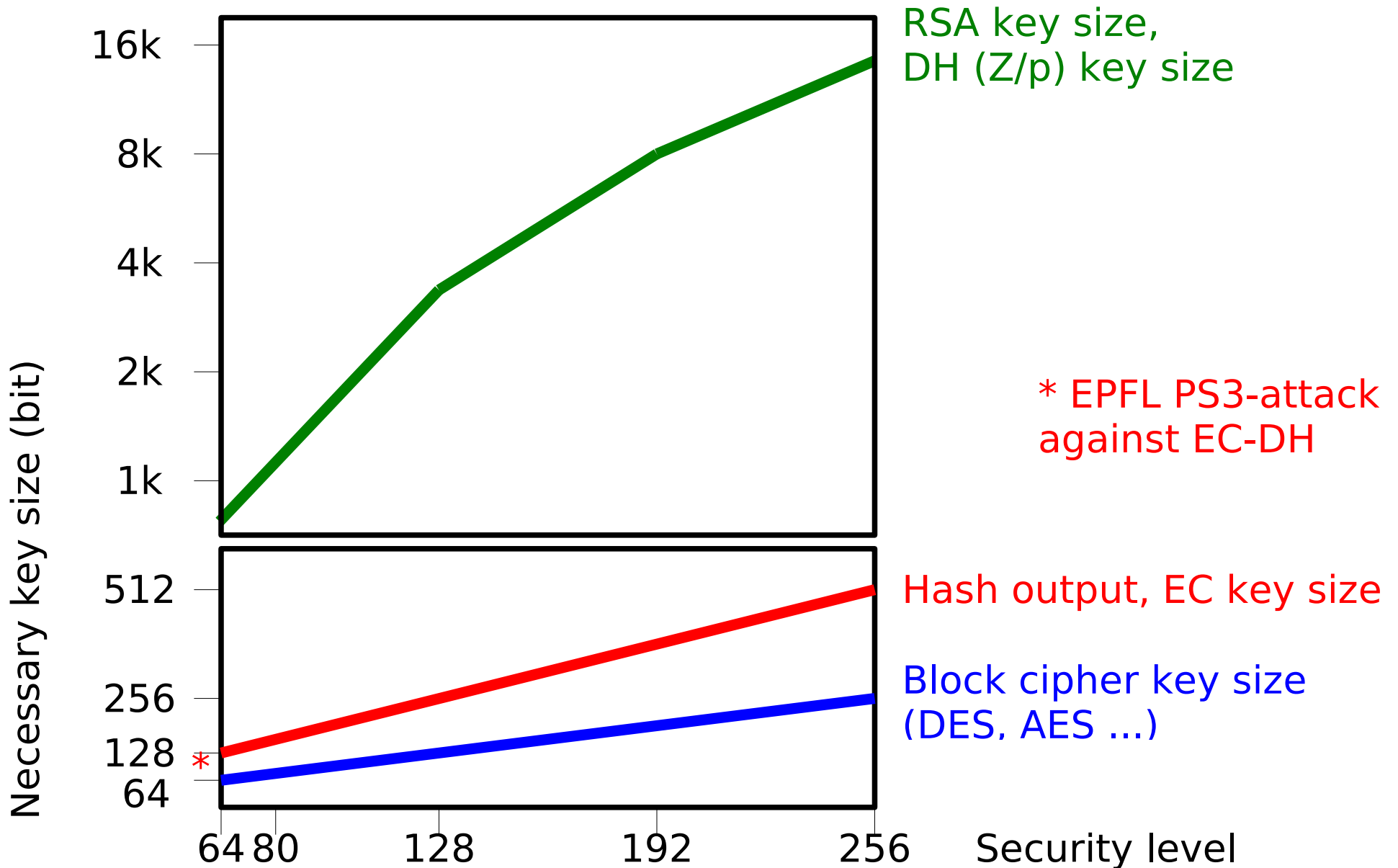
- Security level k = attacker needs 2^k "basic" operations to break cryptosystem
 - Minimal required key length for block cipher
- Depends on attacker

Attacker	Budget	Min. security level
Amateur	0	60
Small org.	10K\$	64
Medium org.	300K\$	68
Large org.	10M\$	78
Major gov.	300M\$	84

[ECRYPT 2006]

Equivalent key lengths

[ECRYPT 2006]



Elliptic-curve cryptography

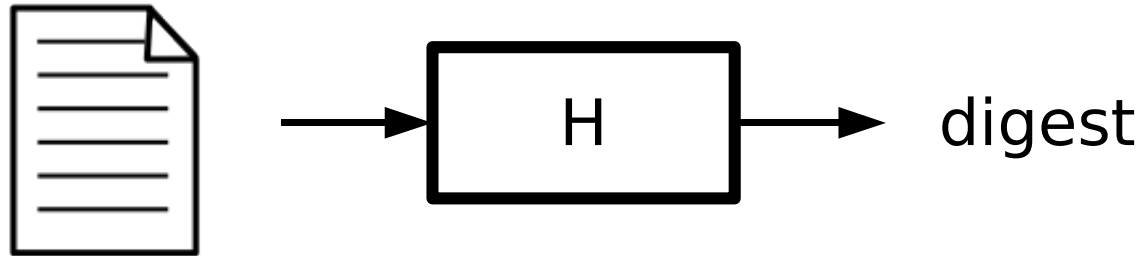
- Alternative representation for discrete-log based cryptosystems
- Better manageable key lengths for future
- First used in smart cards and mobile applications
 - NIST FIPS 201
 - ICAO (E-passport standards)



Part 2: Hash functions



Hash functions



- Computes short digest from (long) input
 - Cryptographic primitive without a key!
 - Properties
 - Infeasible to invert an output
 - Infeasible to find two inputs that map to same digest
 - Output looks random
-
-

Collisions in hash functions

- Hash function maps (long) input to (short) and **unique** digest
 - **Must be collision-free**: no two inputs map to same digest
 - Starting 2004, collisions found in MD5 ...
 - **MD5 has 128-bit output (security level 64)**
 - **Widely used**: digital signatures, software binaries
 - Alternatives?
 - **SHA-1: 160-bit output (security level 80)**
 - Collisions are near (2^{63} attack)
 - **SHA-256 and beyond (security level 128)**
 - Look slightly vulnerable (but no attacks known today)
-
-

Practical consequences?

- Collisions are sparse and look arbitrary, e.g.,

```
SHA1( 132b5ab6 a115775f 5bfddd6b 4dc470eb 0637938a 6cceb733 0c86a386 68080139
      534047a4 a42fc29a 06085121 a3131f73 ad5da5cf 13375402 40bdc7c2 d5a839e2 ) =
SHA1( 332b5ab6 c115776d 3bfddd28 6dc470ab e63793c8 0cceb731 8c86a387 68080119
      534047a7 e42fc2c8 46085161 43131f21 0d5da5cf 93375442 60bdc7c3 f5a83982 ) =
      9768e739 b662af82 a0137d3e 918747cf c8ceb7d4
```

- **But they can be exploited sometimes!**
 - If such data can be embedded "smartly", then signature on one document is also valid on another

→ You: Replace MD5 & SHA1 by SHA-256!

→ Cryptographers: Develop a new hash function!

Development of new hash func.

- **Open, public selection process**
 - Organized by NIST, similar to AES (1996-2001)
 - Sharp contrast to DES (1975)
 - Initial candidates submitted by 10/2008
 - 51 cand. of round 1 selected by NIST in 12/2008
 - First conference in 2/2009
 - Public feedback period
 - About 30 have been broken
 - 14 cand. of round 2 selected by NIST in 7/2009
 - Second conference planned for 2010
-
-

Development of new hash func.

- 14 candidates retained in round 2
 - BLAKE, Blue Midnight Wish, CubeHash, ECHO, Fugue, Grøstl, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD, Skein
 - 8 European
 - 3 US
 - 2 Asia, 1 Israel
- Selection criteria
 - Security
 - No collisions, secure in other common ways of use
 - Cost
 - Computation speed & memory requirements



Development of new hash func.

- Public feedback period continues
 - Very active, competition
 - ECRYPT EU project: "SHA-3 Zoo"
- Round-3 candidates to be selected in 2010
 - Receiving further public comments in 2011
- Determine new hash standard in 2012
 - Third conference to present and discuss feedback
 - Selection of winner by NIST



Part 3: Protocol failures

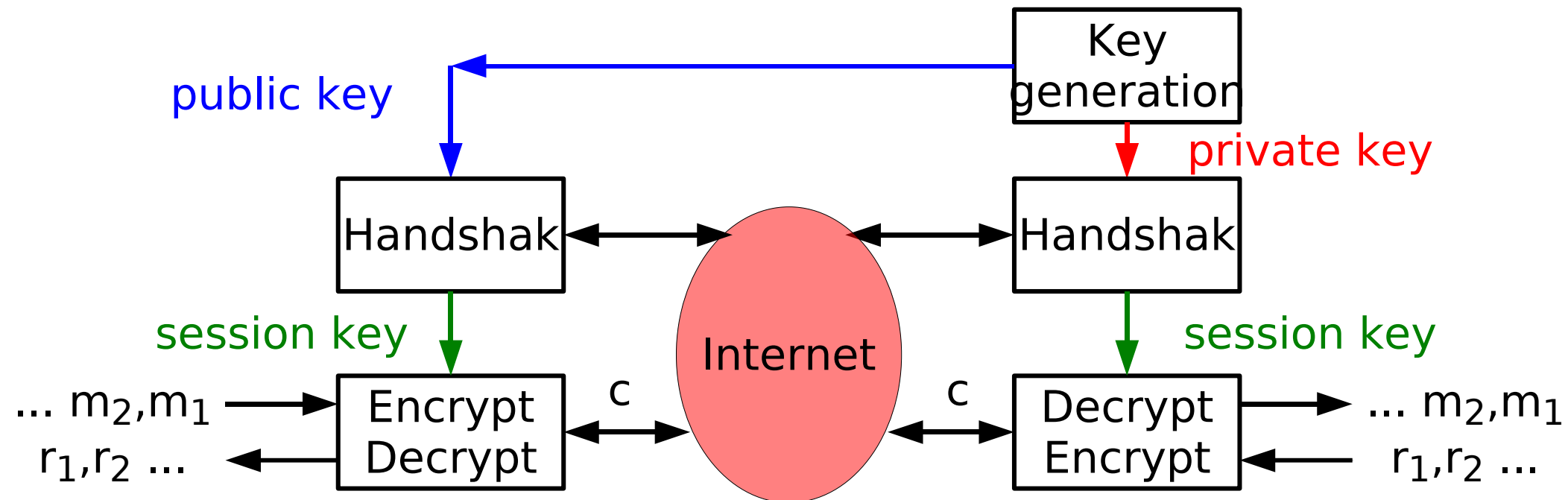


Secure protocols

- Packet-wise encryption
 - IPsec secures IP traffic (usually in VPN)
- Session-wise encryption
 - SSL/TLS and SSH create secure tunnels
- SSL/TLS encrypts application-level traffic today
 - https ...
 - Usually client-server
 - Server has public key with certificate
 - Clients have no keys, usually a root certificate

Session-layer encryption

- SSL/TLS (and SSH) involve multiple steps
 - Handshake to produce session key
 - Stream broken into packets (messages and replies)
 - Packets are encrypted, authenticated, and sent
 - Packets are received and processed

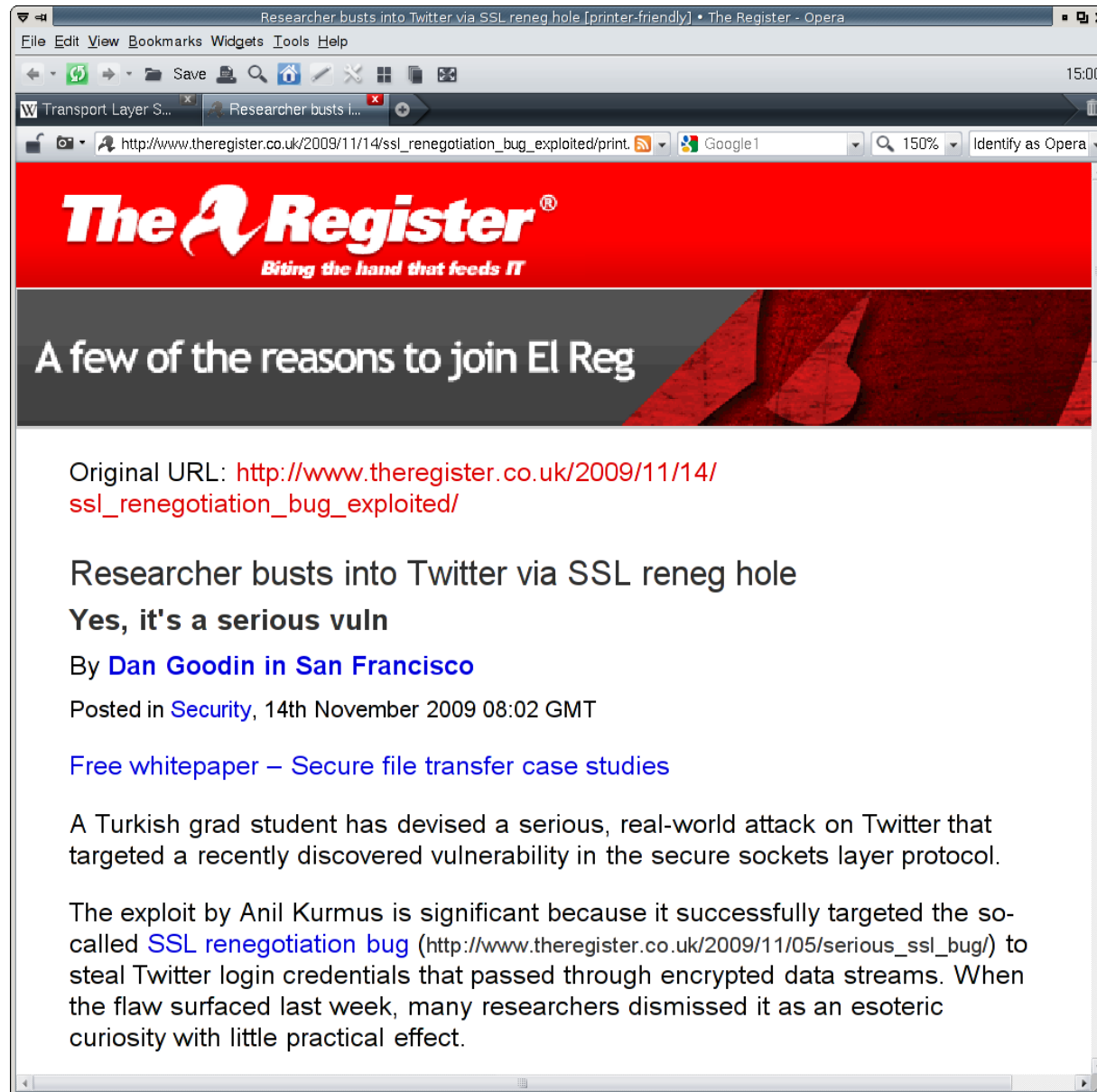


A recent problem in SSL/TLS

- SSL/TLS specification allows attack
 - During re-negotiation of crypto method
 - Attacker can inject its own messages
- History
 - Discovered in Aug. 2009
 - Experts and vendors informed privately
 - Public re-discovery led to disclosure in Nov. 2009
 - Vendors are implementing patches
 - IETF will fix SSL/TLS specification
- Only one example ...



Attack can be exploited



Researcher busts into Twitter via SSL renegot hole [printer-friendly] • The Register - Opera

File Edit View Bookmarks Widgets Tools Help

Save Search Home Stop Print

Transport Layer S... Researcher busts i...

http://www.theregister.co.uk/2009/11/14/ssl_renegotiation_bug_exploited/print Google 150% Identify as Opera

The Register
Bringing the hand that feeds IT

A few of the reasons to join EI Reg

Original URL: http://www.theregister.co.uk/2009/11/14/ssl_renegotiation_bug_exploited/

Researcher busts into Twitter via SSL renegot hole

Yes, it's a serious vuln

By [Dan Goodin in San Francisco](#)

Posted in [Security](#), 14th November 2009 08:02 GMT

[Free whitepaper – Secure file transfer case studies](#)

A Turkish grad student has devised a serious, real-world attack on Twitter that targeted a recently discovered vulnerability in the secure sockets layer protocol.

The exploit by Anil Kurmus is significant because it successfully targeted the so-called [SSL renegotiation bug](#) (http://www.theregister.co.uk/2009/11/05/serious_ssl_bug/) to steal Twitter login credentials that passed through encrypted data streams. When the flaw surfaced last week, many researchers dismissed it as an esoteric curiosity with little practical effect.

Problems with protocols

- Renegotiation is not the only problem in SSL
 - Analysis in recent years
- Deficiencies also shown in SSH protocol
 - Security analysis in 2009 by UK research team
- Why?!?
 - Protocols designed through expert knowledge
 - Best practice: open design and careful review
 - No formal modeling of specification
 - SSL dates to 1995, before appropriate models known
 - Implementation may differ from specification



Developing secure solutions

- Research
 - Develops formal models for cryptographic primitives
 - Models allow composition
- Standardization & engineering
 - Apply best practice and knowledge from research
 - Eventually define only provably secure solutions
- Implementors
 - Must understand interface of standard
 - Must be careful
 - Sending more detailed error message than specified may render protocol insecure!



Developing secure solutions

- Communication protocols
 - Research: Notions of primitives ✓
 - Engineering: IETF standards ✓
 - Products: Up-to-date ✓
 - Privacy-protecting identity management
 - Research: Credential schemes (anon.) ✓
 - Engineering: Work-in-progress -
 - Products: Username/password forever -
 - Storage encryption
 - Research: Notions exist ✓
 - Engineering: Standards emerging ✓
 - Products: Emerging -
-
-

Part 4: Key management

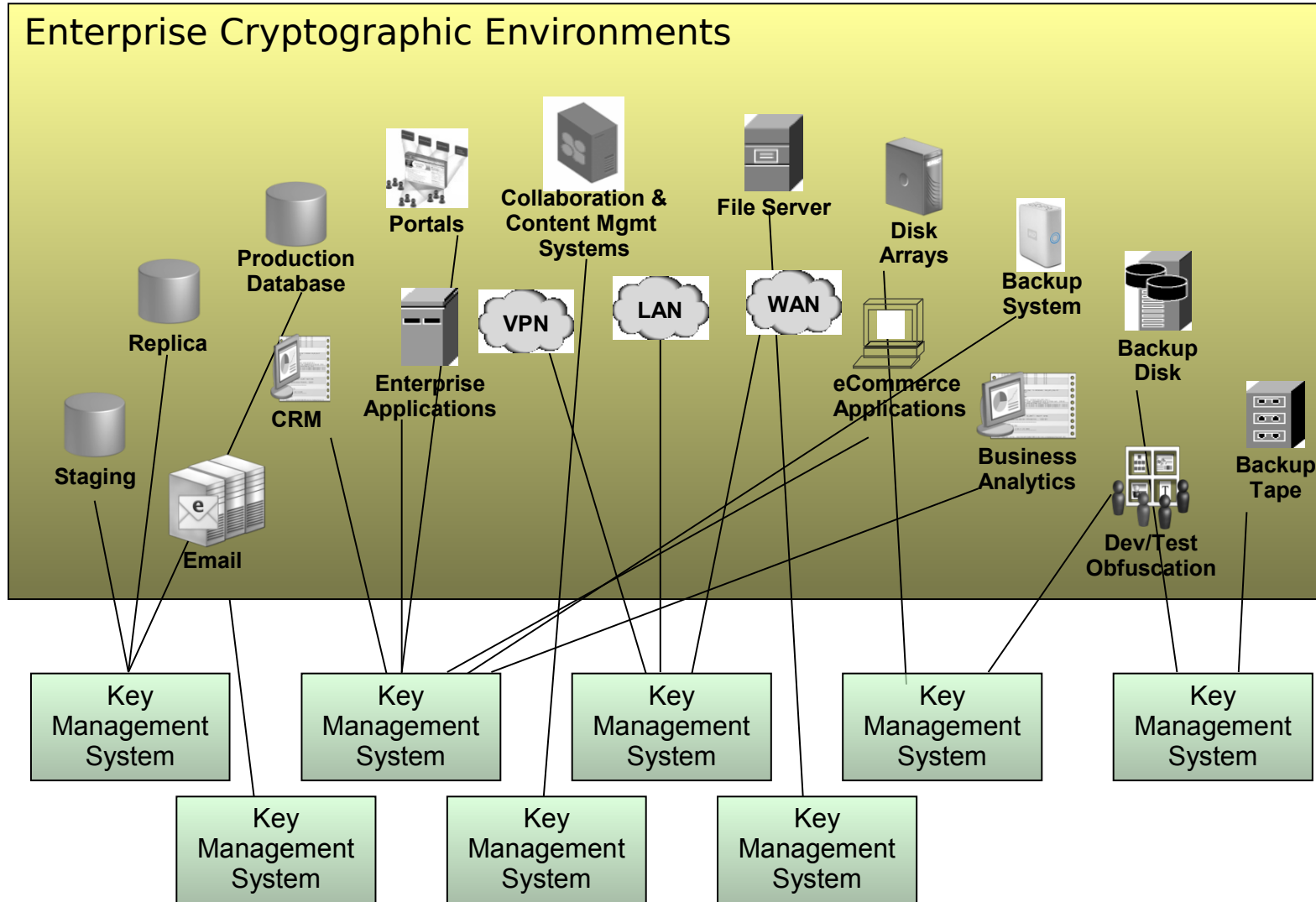
- Current project at IBM Research - Zurich



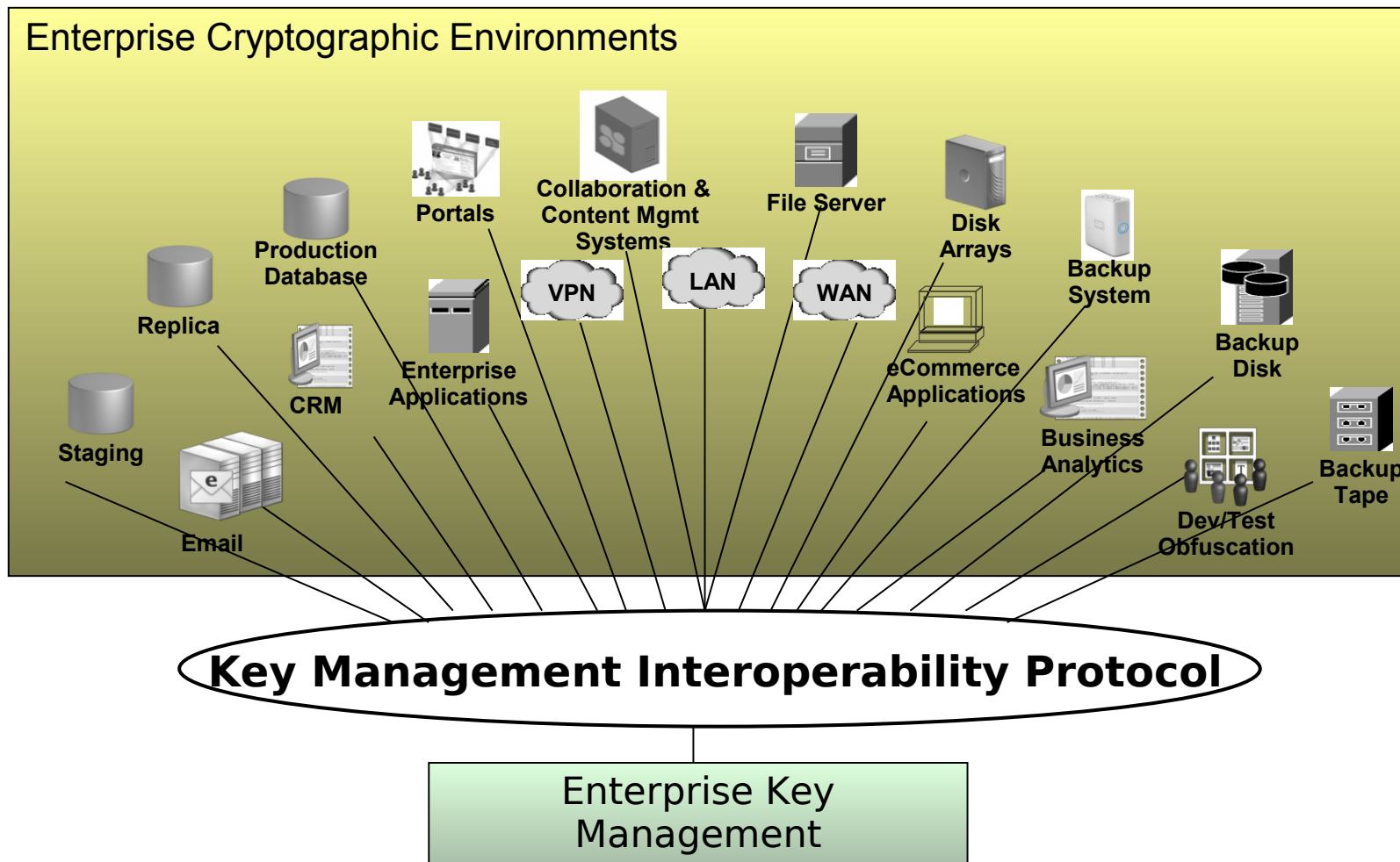
Key management



Today - Proprietary key mgmt.



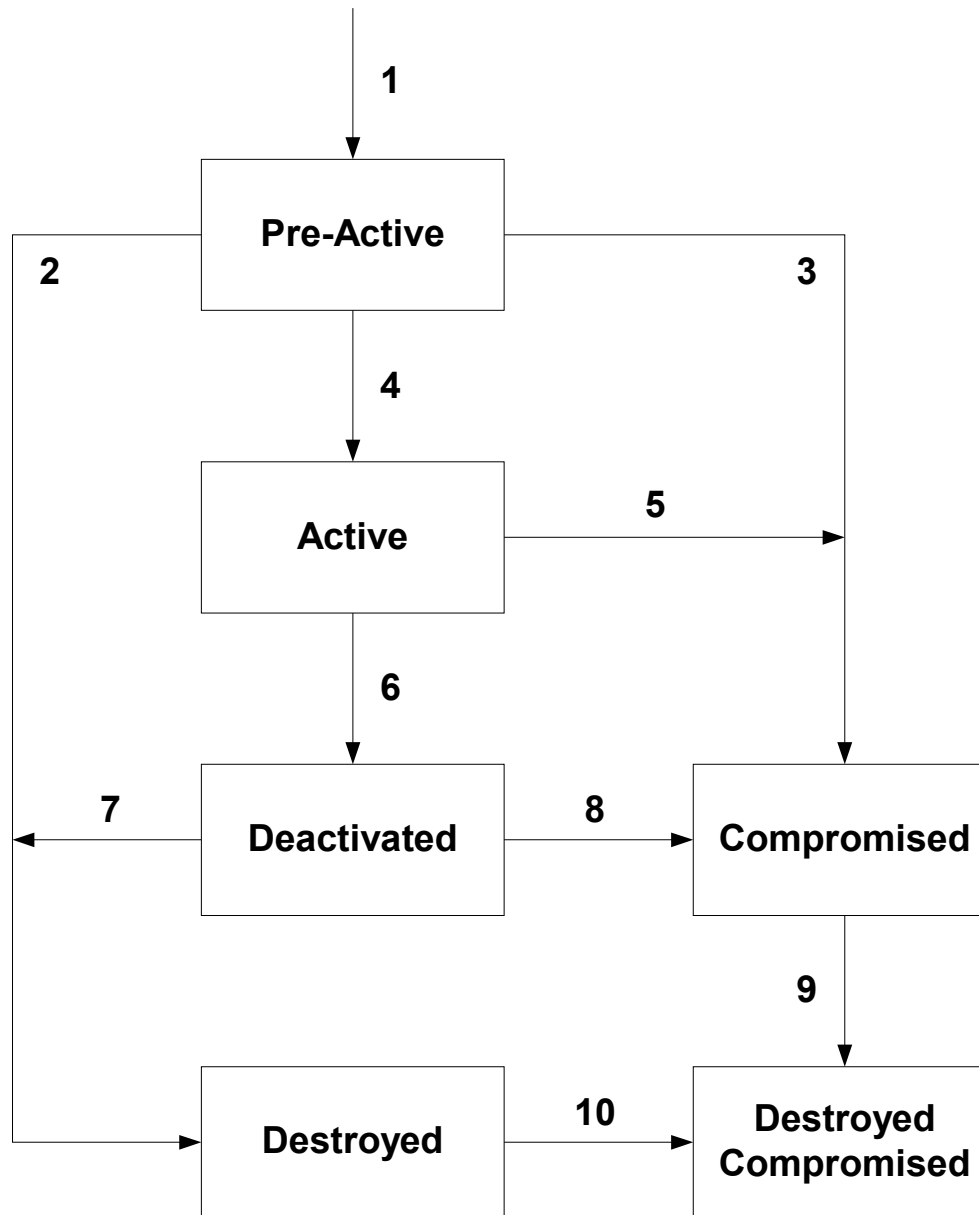
Future - Standardized key management across enterprise



OASIS Key Management Interoperability Protocol (KMIP)

- OASIS: XML
 - Client-server protocol
 - Defines **objects** with **attributes**, plus **operations**
 - **Objects**: symmetric keys, public/private keys, certificates, threshold key-shares ...
 - **Attributes**: identifiers, type, length, lifecycle-state, lifecycle dates, links to other objects ...
 - **Operations**: create, register, attribute handling ...
-
-

Key states in KMIP



OASIS KMIP

- Draft for KMIP V1 prepared by
 - Brocade, HP, IBM, LSI, NetApp, RSA-EMC, Seagate, nCipher/Thales
 - OASIS KMIP TC formed in Apr. 2009
 - <http://www.oasis-open.org/committees/kmip/>
 - IBM Zurich is editor of KMIP standard
 - KMIP V1 currently near finalization
 - To appear soon in storage encryption market
-
-

Conclusion

- Cryptography is mostly secure
- Constant assessment is necessary
 - Key lengths
 - New attacks
- Current developments
 - New hash function standard
 - Provable security
 - Formal methods for engineering



Thank you!

Follow up

<http://www.zurich.ibm.com/csc/security/>

<http://www.zurich.ibm.com/~cca/>

ECRYPT project

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

