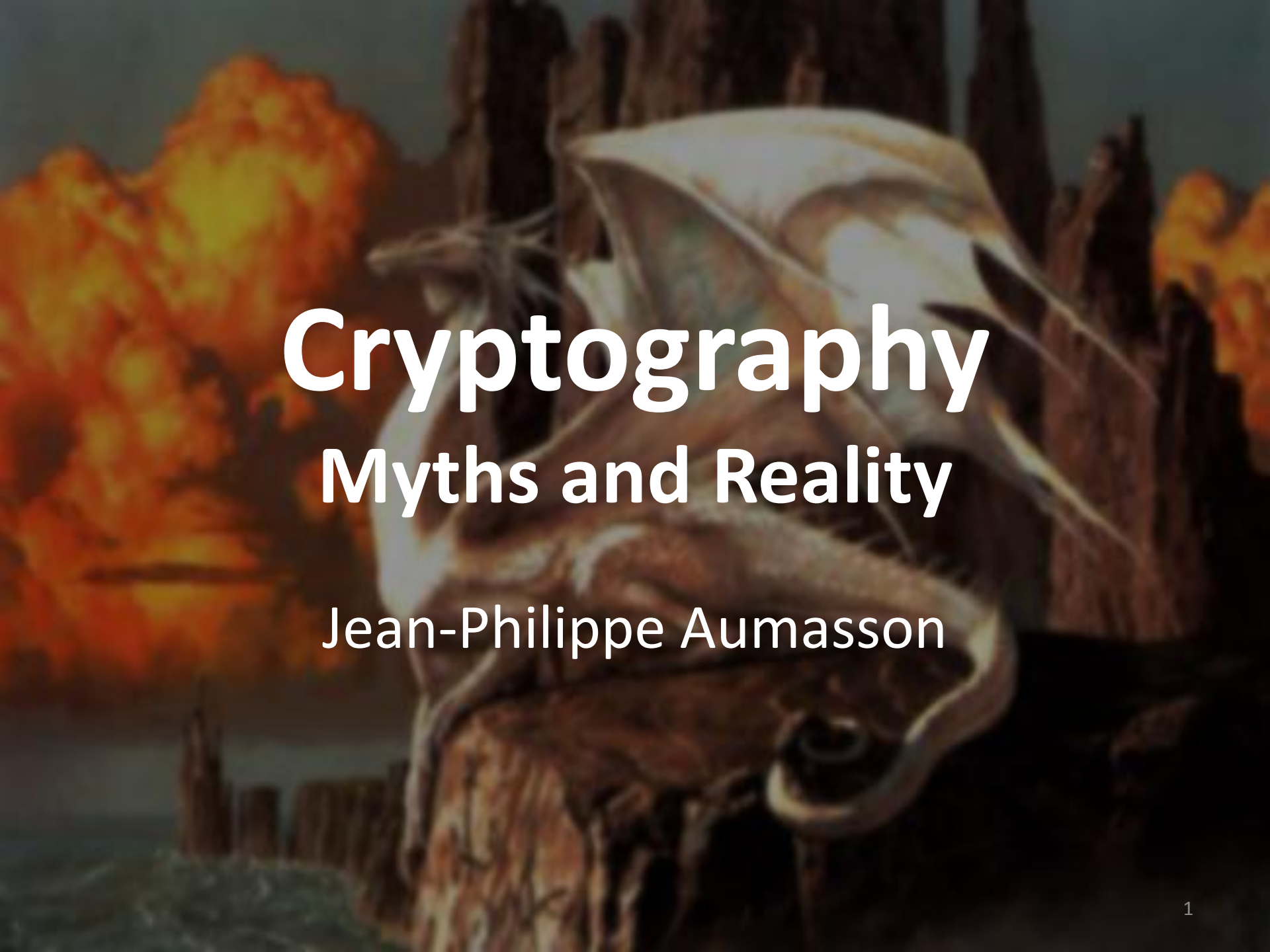
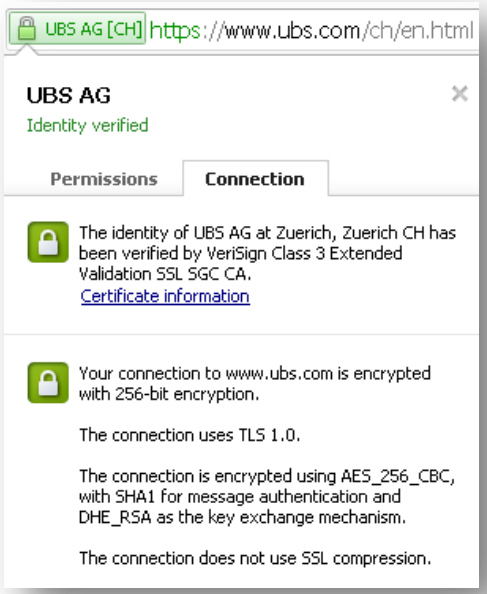


Cryptography
Myths and Reality

Jean-Philippe Aumasson

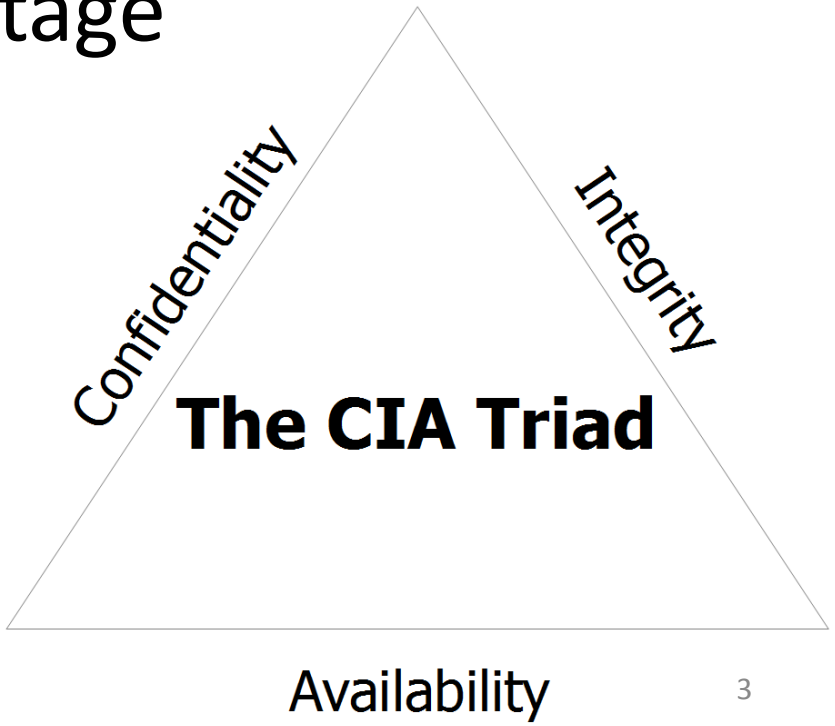
Cryptography is everywhere



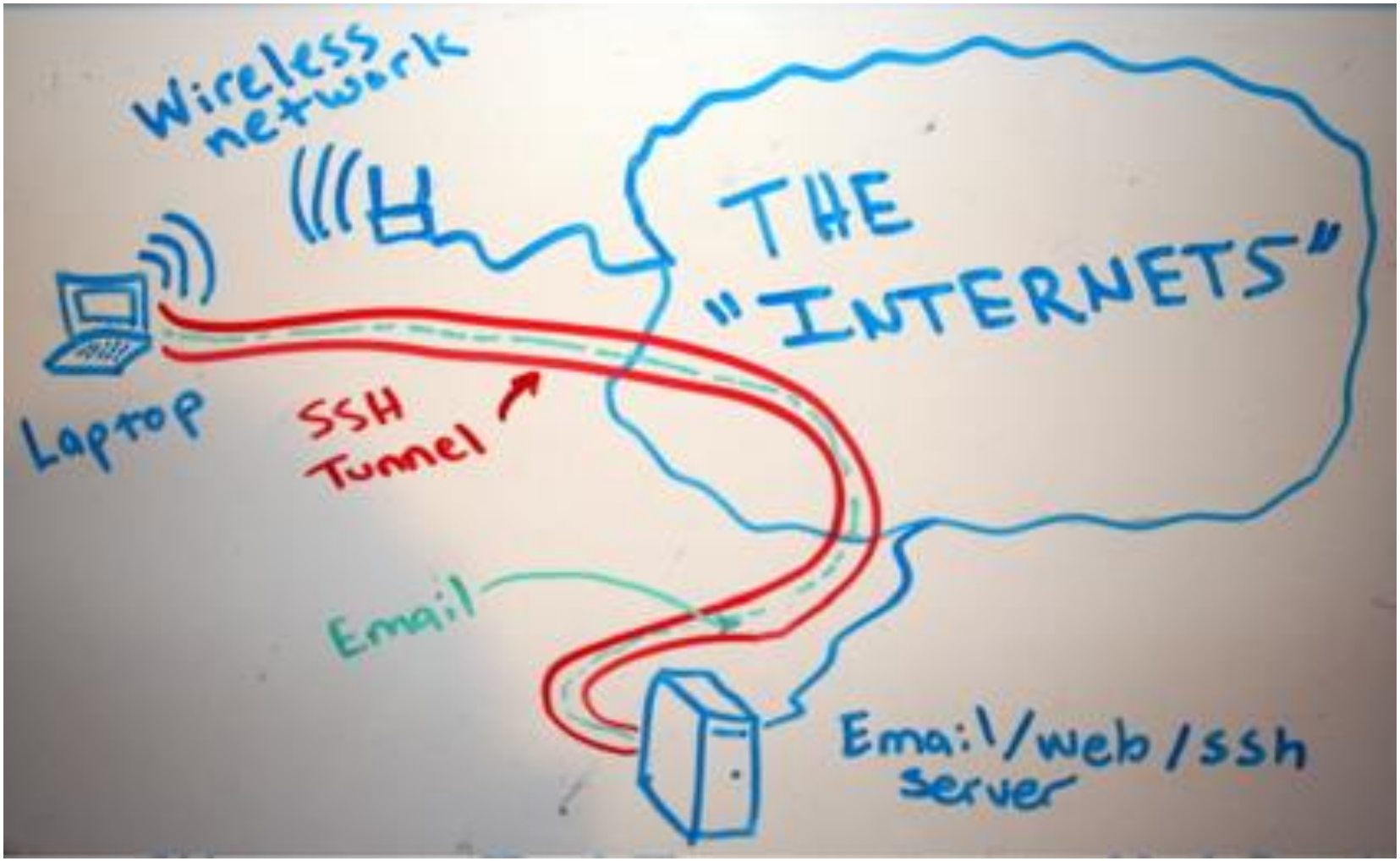
Cryptography promises

Secure communications and data storage:

- **Confidentiality** despite espionage
- **Integrity** despite corruption
- **Availability** despite sabotage



VPNs, SSH tunnels, etc.

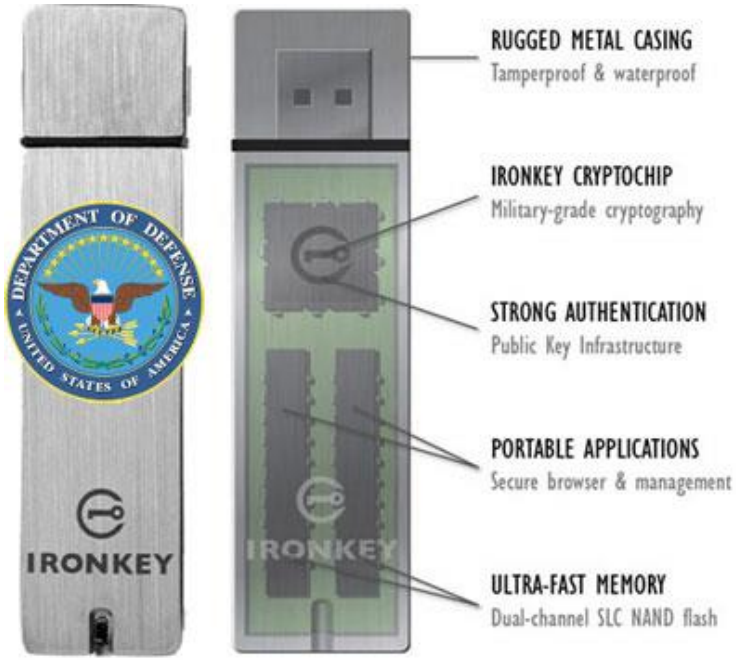


http://code.google.com/p/sshtunnel/

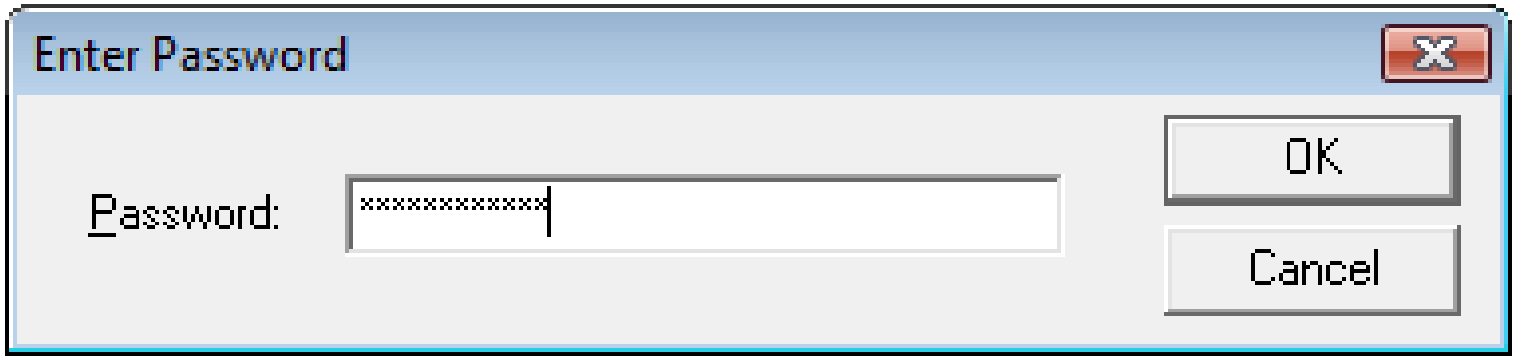
Disk encryption, secure flash USB

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION



Crypto should be taken seriously,



otherwise…

www.engadget.com/2011/06/02/sony-pictures-hacked-by-lulz-security-1-000-000-passwords-claim/

Sony Pictures hacked by Lulz Security, 1,000,000 passwords claimed stolen (update)

By Zachary Lutz *posted Jun 2nd 2011 5:47PM*

BREAKING

www.zdnet.com/blog/btl/6-46-million-linkedin-passwords-leaked-online/79290

6.46 million LinkedIn passwords leaked online

Summary: *More than 6.4 million LinkedIn passwords have leaked to the Web after an apparent hack. Though some login details are encrypted, all users are advised to change their passwords.*

```
df272dfef6127aeaecc5c47c
c886b08ad18cd650b1bc4a76
bd01669b5883f24ebe55930e
ef60e1915933c7c5abde3cb1
991db9efcfa06ae837a4d433
4b757d2f8f7036f8119739e4
13a7bc6d3d74dcc5533d0a75
a4404ac0b635faa6264658fc
546684e9d6d2f217db45229b
54cd6a7aaf905ac2145942f65a03fa7c54cf3ea9:
fb88038b760bc428e4847831aad572339c2e8ecd:
```

UPDATE: IEEE notifies users, confirming the breach.

Data breach at IEEE.org: 100k plaintext passwords.

Using the data to gain insights into the engineering and scientific community

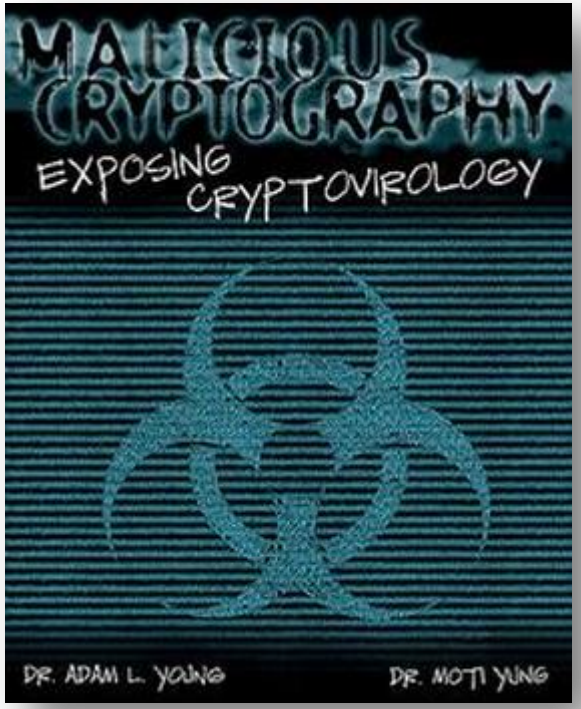
1. Cryptography in use today
2. Future technologies?
   - Homomorphic encryption
   - Leakage-resilient cryptography
   - Quantum cryptography
3. Forecast and conclusions

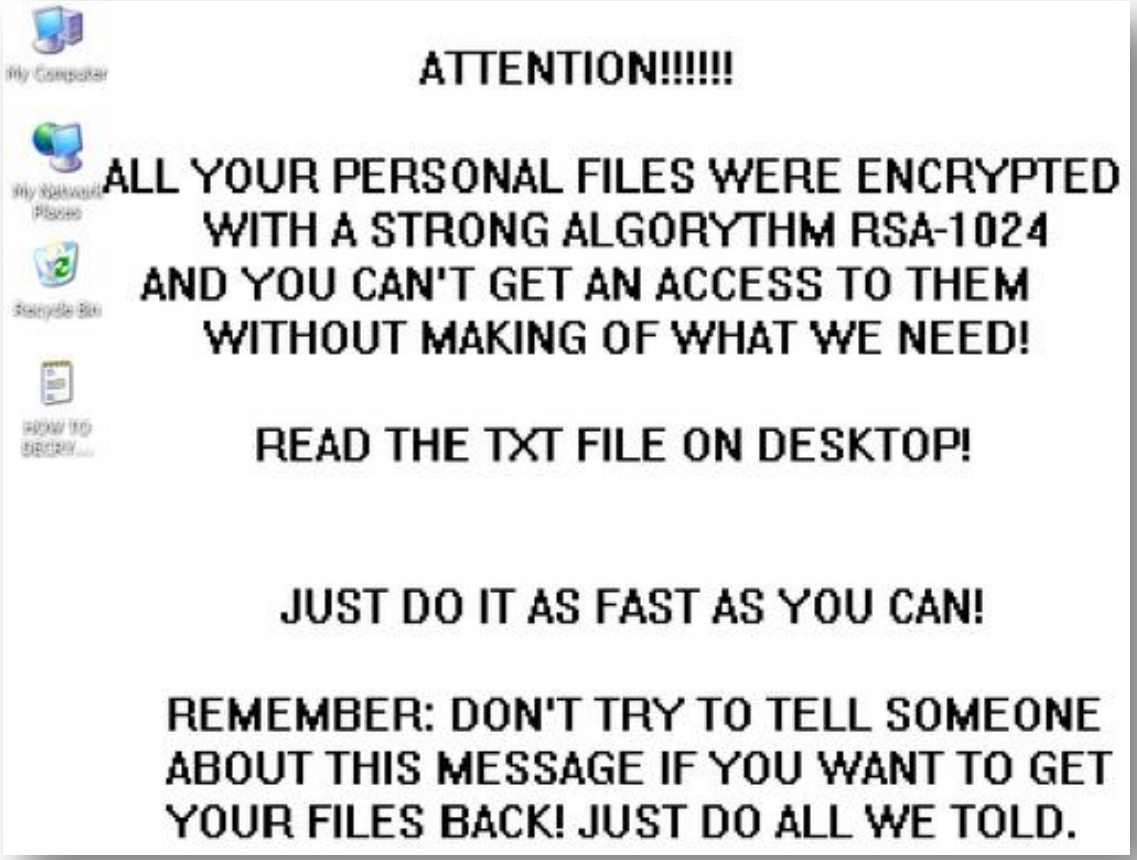
1. **Cryptography in use today**
2. Future technologies?
   - Homomorphic encryption
   - Leakage-resilient cryptography
   - Quantum cryptography
3. Forecast and conclusions

Myth 1

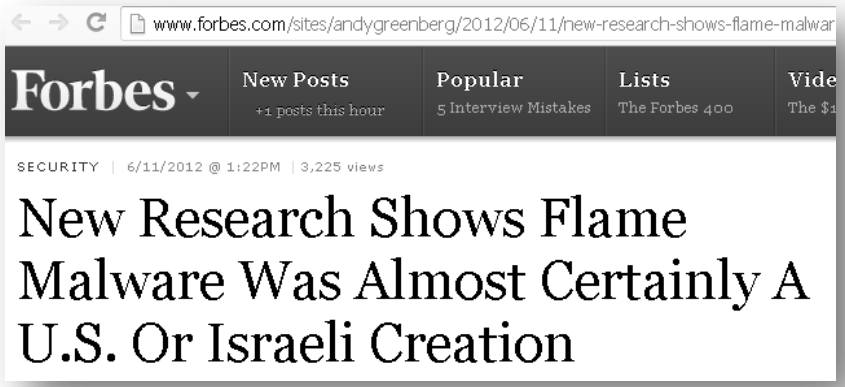
Cryptography is only used for “good”

Inventive applications of cryptography in malware….





MD5 hash collisions exploited in the Flame malware to forge a fake Windows Update



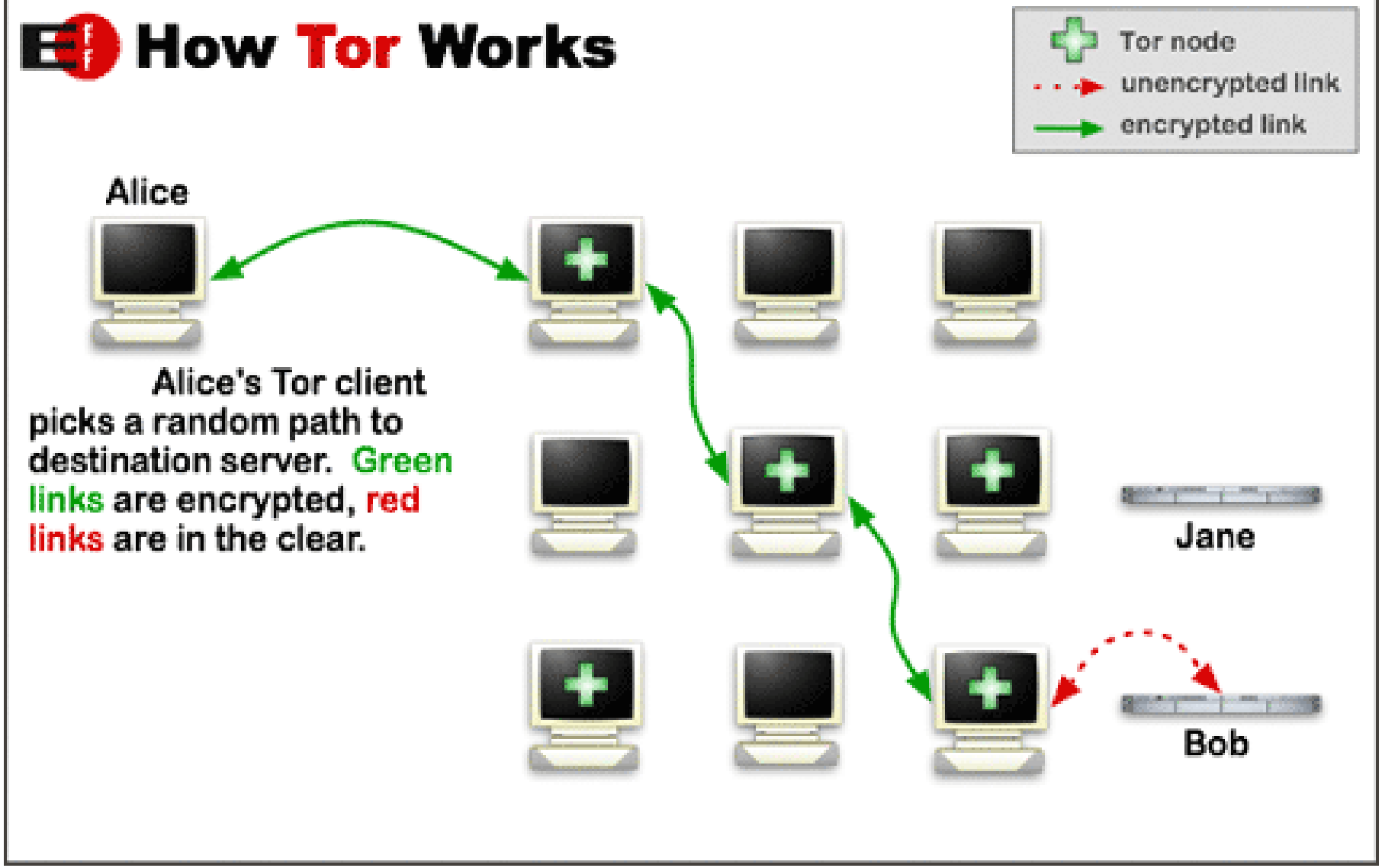
Myth 2

Encrypted VPN ensures strong anonymity

VPNs aim to provide confidentiality, not anonymity

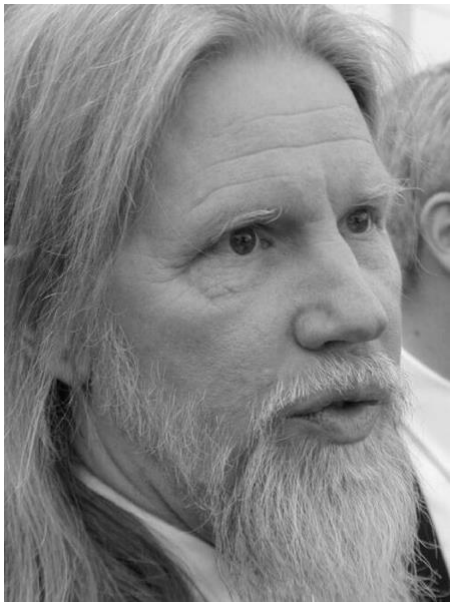
- Single point of trust (logs often kept)
- Anonymity often compromised by user behavior, through profiling, etc.

How Tor Works



Myth 3

Encryption hides all information



“Traffic analysis, not cryptanalysis, is the backbone of communications intelligence”

Susan Landau and Whit Diffie

Spot me if you can:
Uncovering spoken phrases in encrypted VoIP conversations

Charles V. Wright Lucas Ballard Scott E. Coull Fabian Monrose Gerald M. Masson

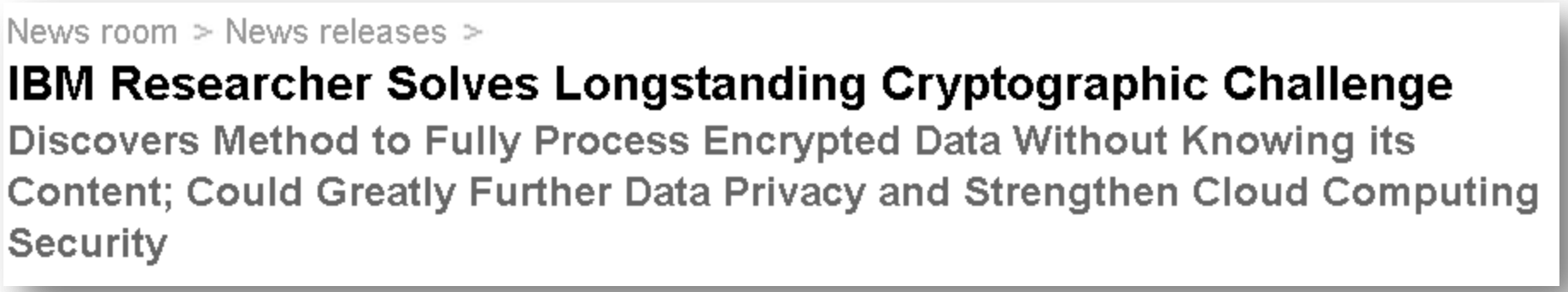
Johns Hopkins University
Department of Computer Science
Baltimore, MD USA 21218
{cvwright,lucas,coulls,fabian,masson}@jhu.edu

1. Cryptography in use today
2. **Future technologies?**
   - Homomorphic encryption
   - Leakage-resilient cryptography
   - Quantum cryptography
3. Forecast and conclusions

Homomorphic encryption

a.k.a. *computing on encrypted data*

2009 breakthrough by Gentry (IBM)


News room > News releases >

IBM Researcher Solves Longstanding Cryptographic Challenge

Discovers Method to Fully Process Encrypted Data Without Knowing its Content; Could Greatly Further Data Privacy and Strengthen Cloud Computing Security

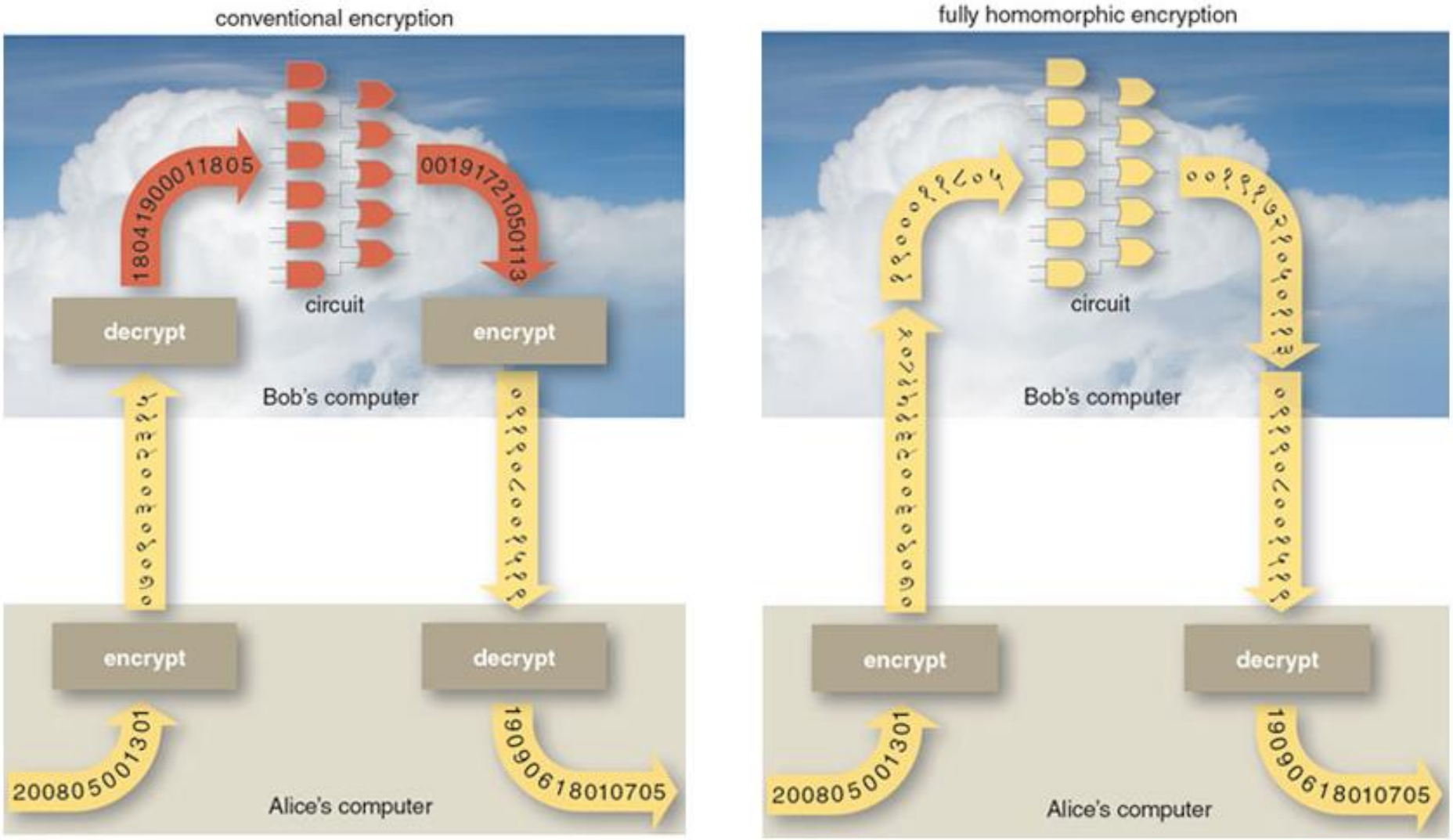
Principle: given encrypted data **Enc(m)**, produce **Enc(f(m))** for any transform **f()**, without decrypting (thus **m** remains secret)

Breakthroughs

IBM's Blindfolded Calculator

Andy Greenberg, 06.24.09, 06:00 PM EDT
Forbes Magazine dated July 13, 2009

A researcher's algorithm could teach computers a new privacy trick.



http://www.americanscientist.org/issues/num2/2012/5/alice-and-bob-in-cipherspace/1

Myth 4

Homomorphic encryption solves the cloud privacy problem

Homomorphic encryption allows to offload computations to the cloud if data is read and written by a **single client**
Ex: cloud storage, tax-preparation

When **multiple clients** are involved, homomorphic encryption is insufficient, (must rely on other mechanisms)
Ex: social networks, shared documents

Myth 5

Homomorphic encryption is practical

"We are not talking about a 10x slowdown here; rather, we are talking about **the whole Amazon EC2 cloud not being able**, in a day, to perform homomorphically a computation which would take **one second on a single iPhone**."

http://security.stackexchange.com/questions/3728/in-what-ways-does-full-or-partial-homomorphic-encryption-benefit-the-cloud

Homomorphic Evaluation of the AES Circuit

Craig Gentry
IBM Research

Shai Halevi
IBM Research

Nigel P. Smart
University of Bristol

June 15, 2012

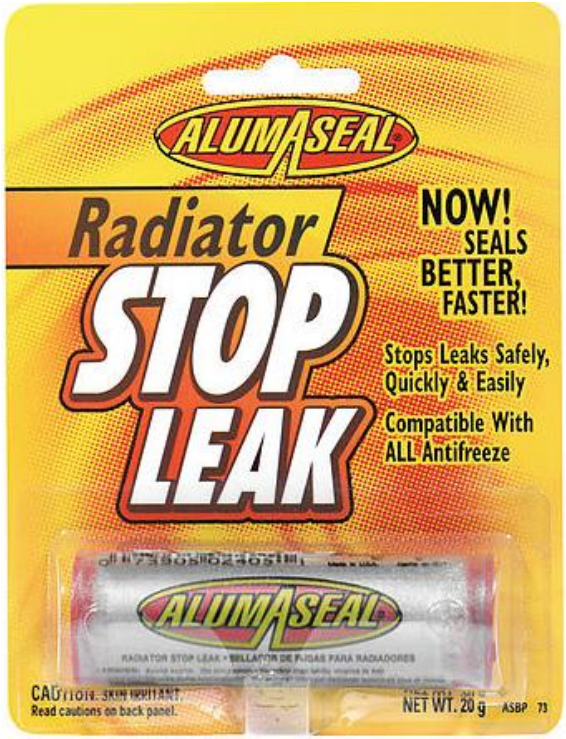
http://eprint.iacr.org/2012/099.pdf

1 AES block encryption in ≈ 36 hours
(on a machine with 256GB RAM)

More improvements are expected, but HE is unlikely to become practical soon

Myth 6

Cryptographers know how to deal with side-channel attacks



Leakage-resilient cryptography

a.k.a. *secure even when secret data leaks*

Active research field since ≈ 2008

Aims to model attacks on the **hardware** exploiting side-channels, data remanence, etc.

Leakage-resilient cryptography

“Grey-box” model: some information leaks from crypto operations (data, operations..)

- Hardware compromised
- Data-dependent execution time
- Etc.

Traditional attacks assume tamper-resistant hardware (“black boxes”)

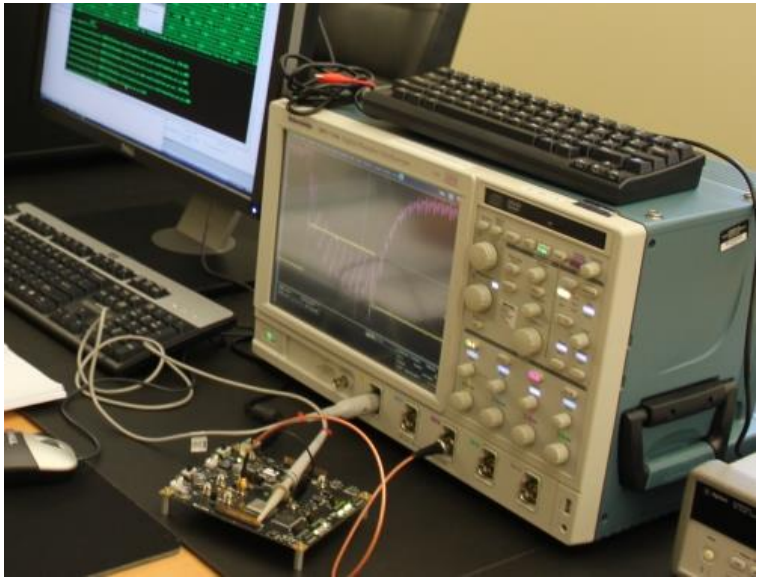
Leakage-resilient cryptography

Exposure-resilience: security preserved even if a large part of the secret key leaks

Motivation: "cold boot" attacks reading RAM content from running computers

Leakage-resilient cryptography

Bounded leakage: computations leak information on the data processed



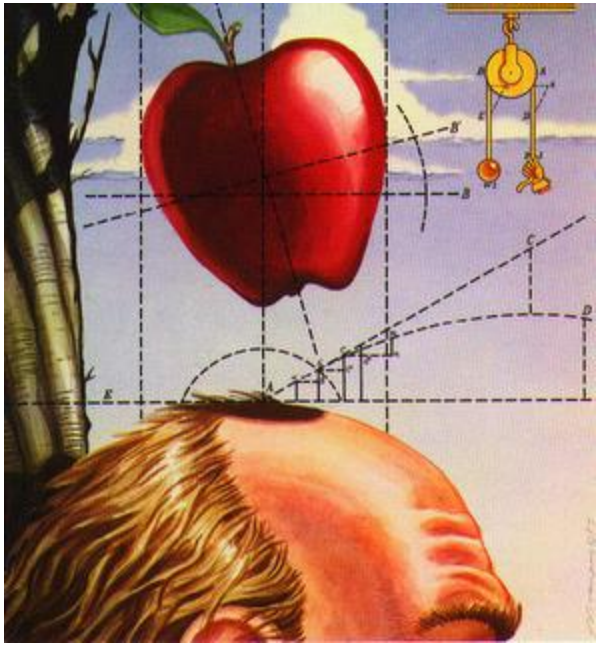
Motivation: attacks based on power or electromagnetic analysis (DPA, TEMPEST, etc.)

- In hardware, countermeasures remain necessary, as for classical schemes
- In software, some attacks will still work, some others won’t
- Models often fail to model real attackers (how to bound leakage in practice?)

Not the “silver bullet”, but promising

Myth 7

Quantum cryptography is as strong as the laws of physics



Quantum cryptography

Use of quantum mechanics (entanglement, non-locality) to perform crypto tasks

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}).$$

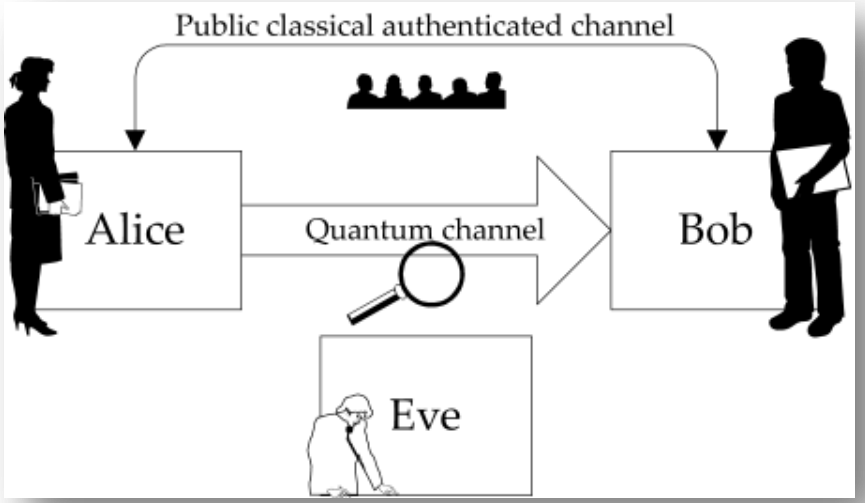
Mainly **quantum key distribution (QKD)**

Security related to physics laws…

Quantum key distribution (QKD)

2-party protocol over a **quantum channel**

Purpose is **not to encrypt**, but establish a shared secret key



Security arguments:

1) By the laws of physics, any eavesdropping would be detected, thus attackers can't succeed

2) The key established is truly random

news.bbc.co.uk/2/hi/science/nature/7661311.stm

BBC | News | Sport | Weather | Travel | TV | Radio

NEWS

Watch ONE-MINUTE WORLD NEWS

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news

Video and Audio

Page last updated at 12:50 GMT, Thursday, 9 October 2008 13:50 UK

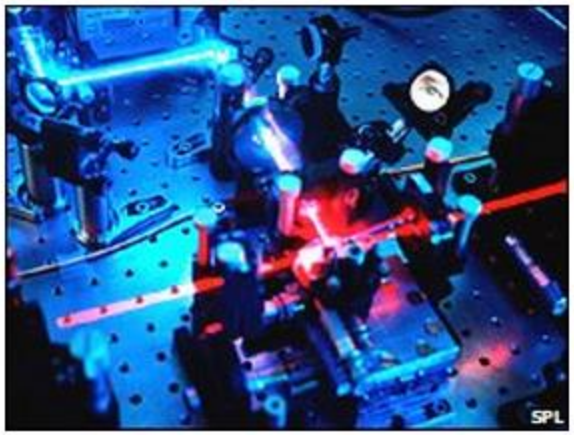
E-mail this to a friend Printable version

'Unbreakable' encryption unveiled

By Roland Pease
BBC Radio Science Unit

Perfect secrecy has come a step closer with the launch of the world's first computer network protected by unbreakable quantum encryption at a scientific conference in Vienna.

The network connects six locations across Vienna and in the nearby town of St Poelten, using 200 km of standard commercial fibre optic cables.



Quantum cryptography is touted as being "unbreakable"

Theory in the 1980's, commercial in late 2000's

A world leader is the **Swiss IdQuantique**

Typical vendor claim (here Quintessence Labs):

"Quantum physics provides a method of achieving an **absolutely secure** information exchange that is guaranteed to be **future proof**."

http://qlabsusa.com/technology/cryptography/quantum-cryptography/

www.nature.com/news/2010/100520/full/news.2010.256.html

nature International weekly journal of science

nature news home | news archive | specials | opinion

nature journal

comments on this story

Published online 20 May 2010 | Nature | doi:10.1038/news.2010.256

News

Quantum crack in cryptographic armour

A commercial quantum encryption system has been fully hacked for the first time.

hackshark.com/?p=325#axzz27egFExJM

Hack Shark

Quantum Cryptography: Perfect Eavesdropper Illustrates Overlooked Loophole in Secure Communications Technology

Jul 11, 2011 // by 0r10n c45p4r // Latest News, Web Threats // No Comments

Leave feedback

Quantum key distribution (QKD) is an advanced tool for secure computer-based interactions, providing confidential communication between two remote parties by enabling them to construct a shared secret key during the course of their conversation.

QKD is perfectly secure in principle, but researchers have long been aware that loopholes may arise when QKD is put into practice. Now, for the first time, a team of researchers at the Centre for Quantum Technologies (CQT) at the National University of Singapore, the Norwegian University of Science and Technology (NTNU) and the University Graduate Center (UNIK) in Norway have created and operated a "perfect eavesdropper" for QKD that exploits just such a loophole in a typical QKD setup. As reported in the most recent

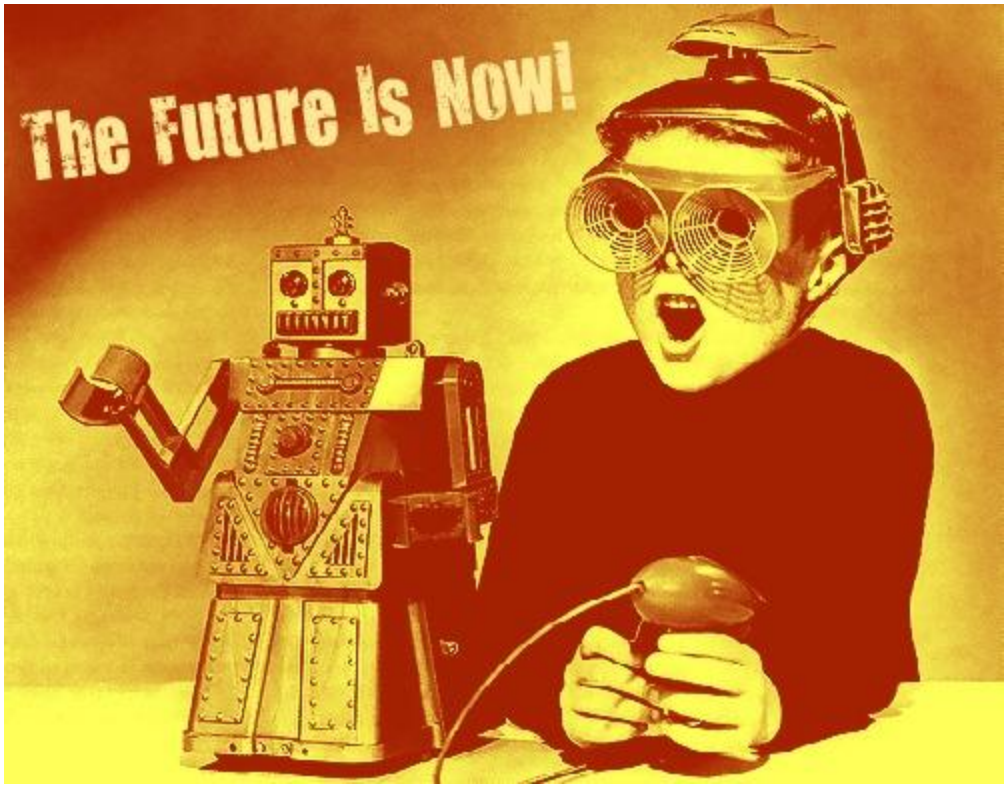
No laws of physics were harmed in these attacks…

“there are **security proofs by the laws of physics**, but of course, those **rely on the model**. On how exactly the photon source, detectors, etc. work. So, **if an adversary can exploit some properties of these devices** that are not captured by the theoretical model, then these schemes **still can be broken**”

http://arstechnica.com/security/2012/09/quantum-cryptography-yesterday-today-and-tomorrow/

Myth 8

Quantum cryptography is “future-proof”



Vendors claim than quantum crypto cannot ever be broken, unlike classical crypto, but…

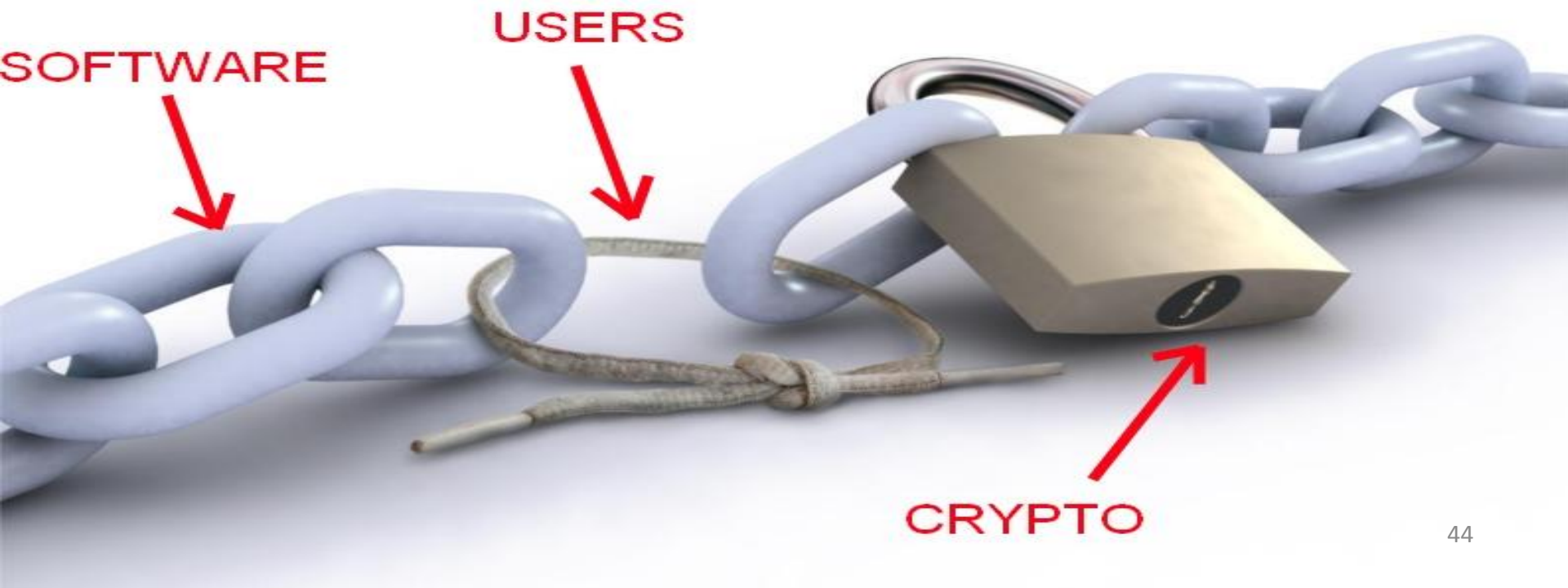
With QKD **data is still encrypted with classical crypto** (which is secure for the foreseeable future)

"It could be broken…" is **not** serious risk analysis

Totally irrelevant and incorrect argument

“The encryption doesn’t even have to be very strong to be useful, it just **must be stronger than the other weak links** in the system. Using any standard commercial risk management model, cryptosystem failure is **orders of magnitude below any other risk**”

Ian Grigg, Peter Gutmann, IEEE Security & Privacy 9(3), 2011



1. Cryptography in use today
2. Future technologies?
   - Homomorphic encryption
   - Leakage-resilient cryptography
   - Quantum cryptography
3. **Forecast and conclusions**

Homomorphic encryption is unlikely to secure cloud applications before 10 years

However…

Existing crypto technologies can guarantee:

- Data stored is not modified by the cloud
- Search with keywords on encrypted data…
- …such that cloud doesn’t see the keywords

Leakage-resilient cryptography may become a useful tool for smartcards security

Quantum crypto will remain in the headlines despite no security added value

www.wired.com/politics/security/commentary/securitymatters/2008/10/securitymatters_1016

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN VIDEO INSI

Security Matters

Commentary by Bruce Schneier

POLITICS : SECURITY

Quantum Cryptography: As Awesome As It Is Pointless

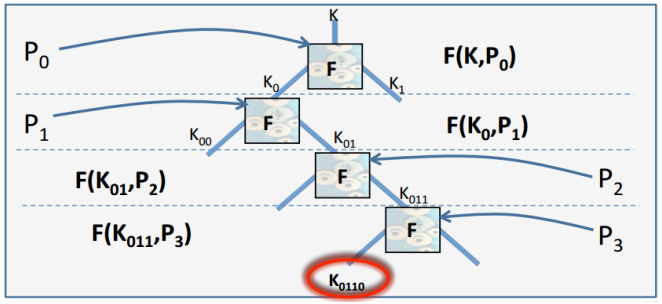
Bruce Schneier 10.16.08

Quantum cryptography is back in the news, and the basic idea is still unbelievably cool, in theory, and nearly useless in real life.

The idea behind quantum crypto is that two people communicating using a quantum channel can be absolutely sure no one is eavesdropping. Heisenberg's uncertainty principle requires anyone measuring a quantum system to disturb it, and that disturbance alerts legitimate users as to the eavesdropper's presence. No disturbance, no eavesdropper — period.

Research-stage technologies examples

Leakage-resistent encryption (CHES 2012)



https://www.cosic.esat.kuleuven.be/ches2012/slides/S1_talk2_Faust.pdf

CS2 searchable cloud storage system

http://research.microsoft.com/en-us/um/people/senyk/slides/CS2.pdf

"Somewhat" homomorphic encryption

http://research.microsoft.com/apps/pubs/default.aspx?id=148825

Fascinating technologies are emerging

<u>But in any case:</u>

Determine the real added value for your business

Run cost-benefit analyses

Seek vendor-neutral evaluations and opinions

Crypto is powerful, but difficult

Rely on trusted experts!

Thank you!

Who am I

Cryptography expert at the Kudelski Group

- Crypto designs & reviews
- CAS security architecture
- Cybersecurity services

Active researcher in applied cryptography

- 40+ research articles in top conferences/journals
- Talks at security conferences (Black Hat, #days, etc.)

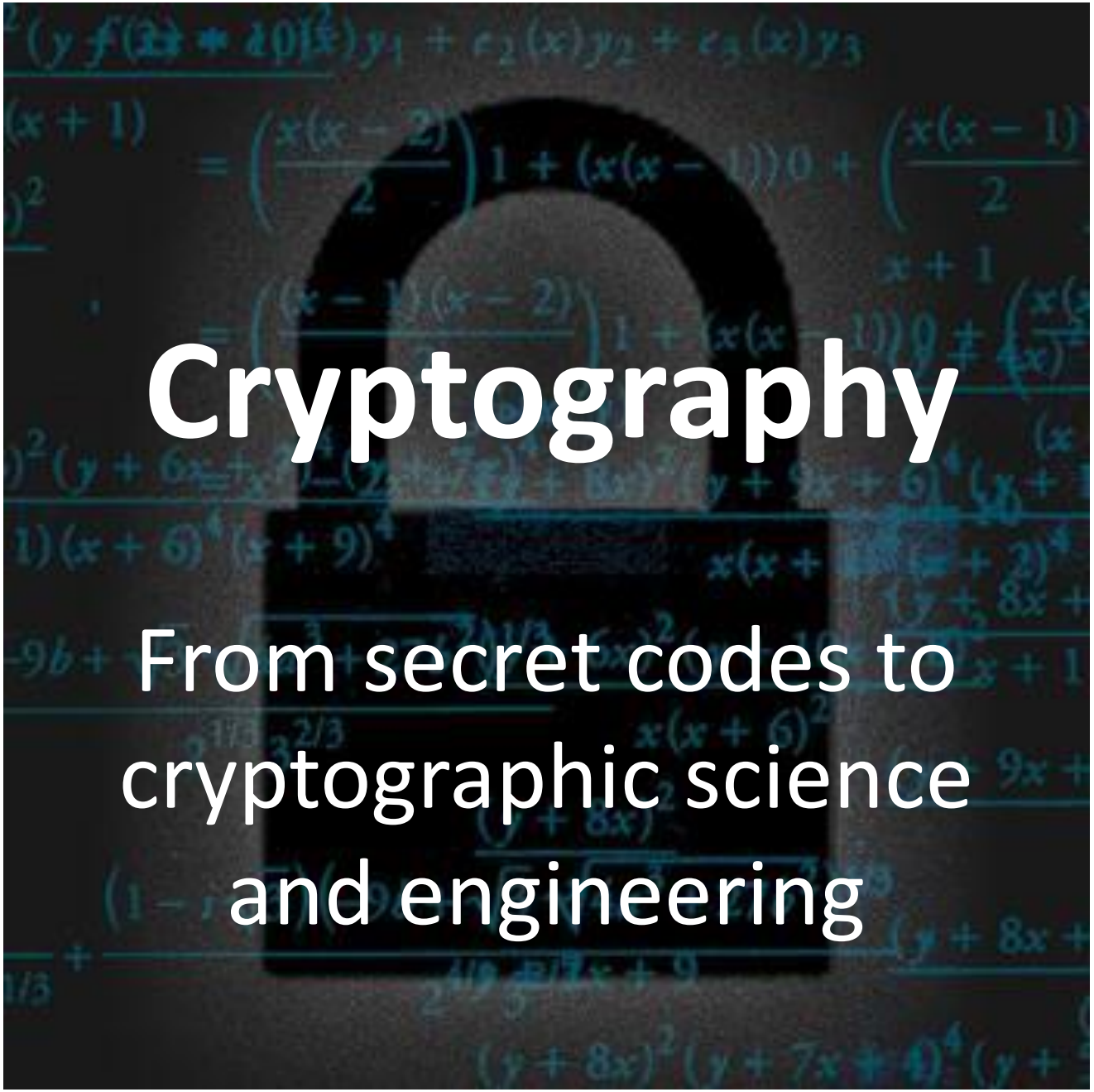
PhD cryptography, FHNW/EPFL, 2009

Who am I

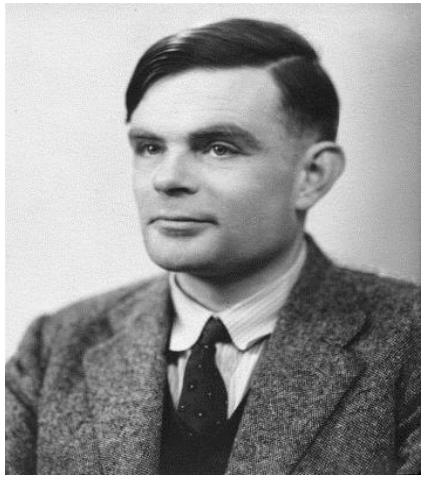
Achievements

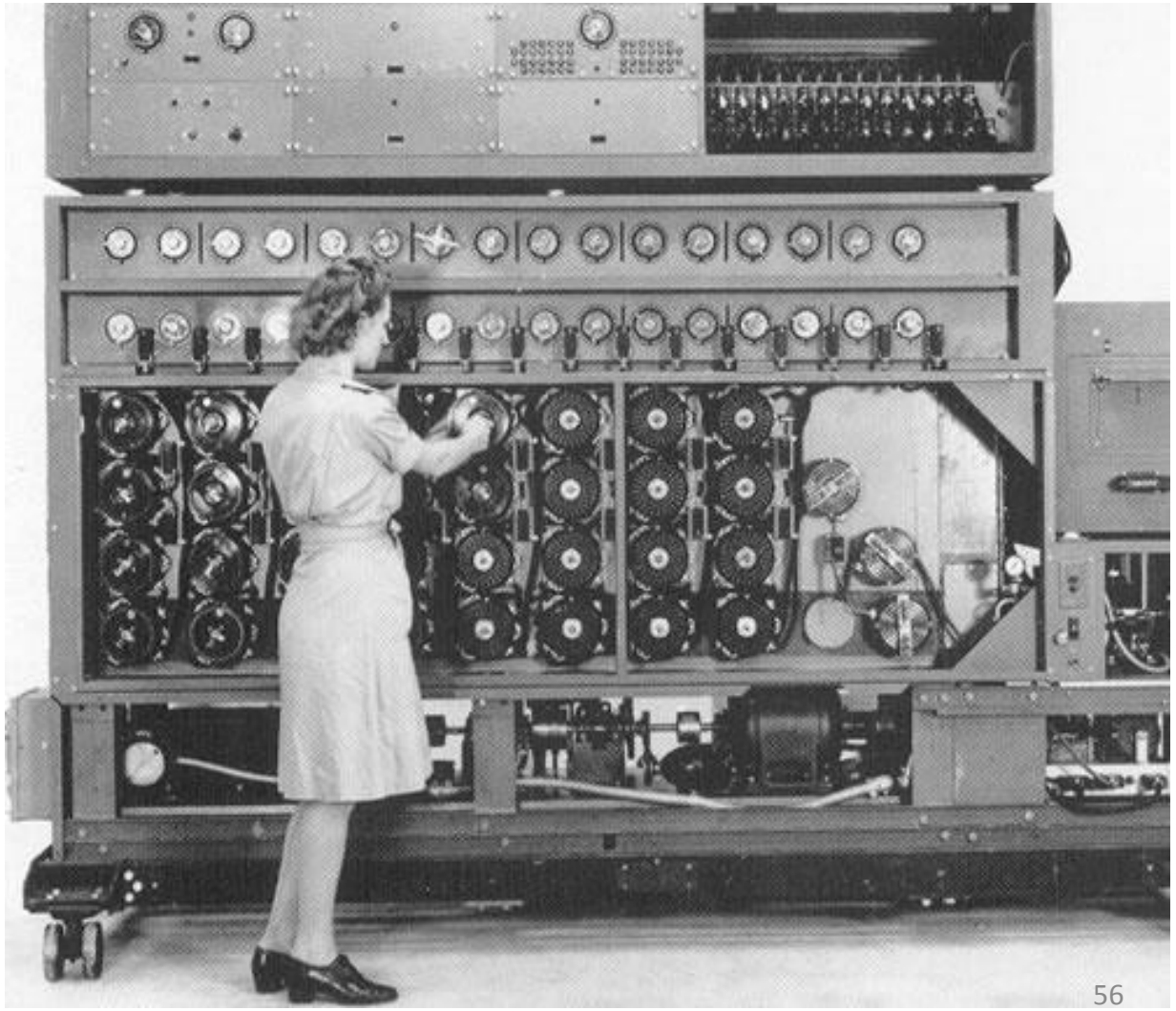
- Main designer of the SHA-3 finalist BLAKE
- Security vulnerabilities reported in Java and Ruby
- “SipHash” against DoS attacks (with D.J. Bernstein)
- Lightweight crypto “Quark” for RFID systems
- “Cube testers” cryptanalysis (with A. Shamir)
- Inventor of “zero-sum attacks” (best attack on SHA-3)
- Several awards and prizes…

jeanphilippe.aumasson@gmail.com
https://131002.net/ https://twitter.com/aumasson


Cryptography
From secret codes to cryptographic science and engineering

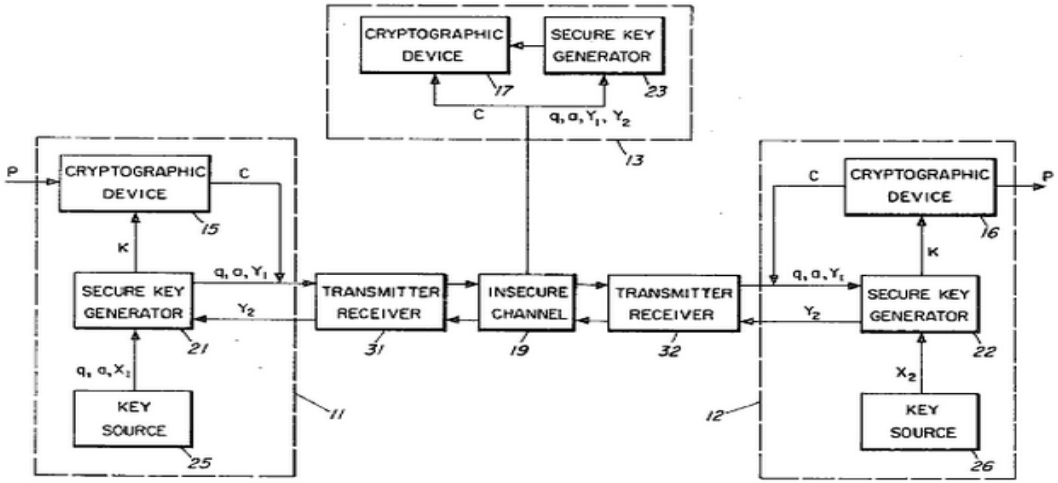
1939: British mathematician Alan Turing breaks Enigma encryption





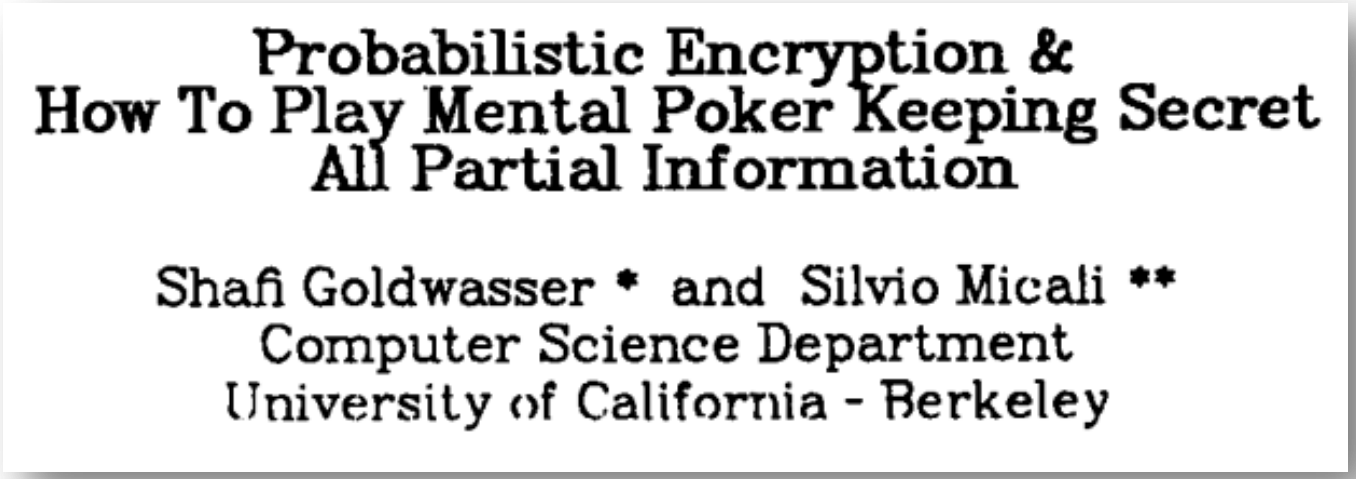
1976-77: invention of public-key crypto (Diffie-Hellman key exchange, RSA)

$$\begin{aligned}\text{RSA-768} = {} & 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489 \cdot \\ & 36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917.\end{aligned}$$

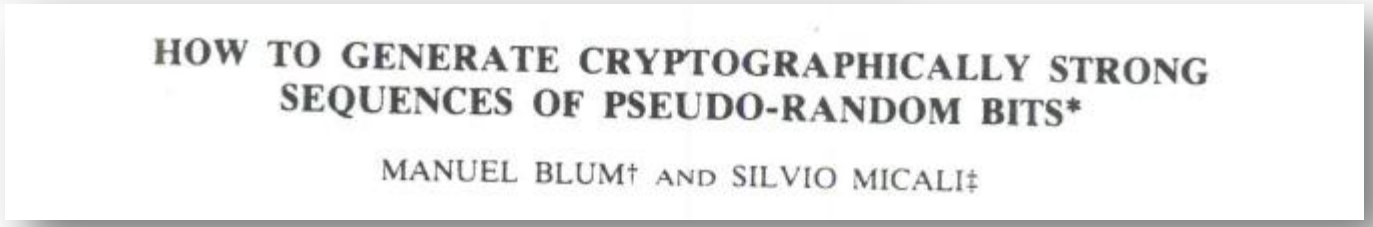


Enabled secure communications over insecure channels (for online commerce, etc.)

1980's: cryptography academic research (complexity theory and math communities)


Probabilistic Encryption &
How To Play Mental Poker Keeping Secret
All Partial Information

Shafi Goldwasser * and Silvio Micali **
Computer Science Department
University of California - Berkeley

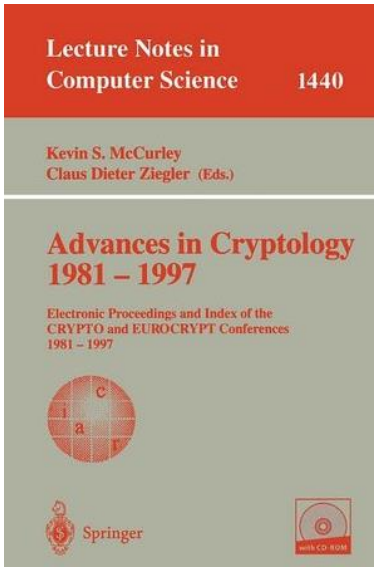

HOW TO GENERATE CRYPTOGRAPHICALLY STRONG SEQUENCES OF PSEUDO-RANDOM BITS*

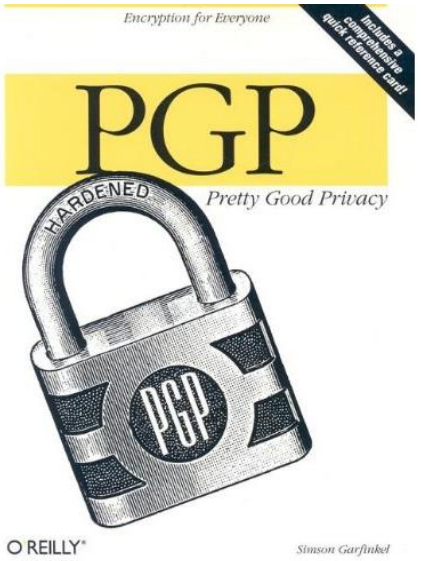
MANUEL BLUM† AND SILVIO MICALI‡


Elliptic Curve Cryptosystems

By Neal Koblitz

1990's: more crypto labs, strong crypto software becomes available to civilians





TOP SECRET

December 23, 1992

Director Sessions

Re: Use of the Clipper Chip in AT&T TSD 3600 During Phase II of Production

This document is classified "SECRET" in its entirety unless otherwise indicated.

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX (paragraph blacked out by NSA) XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX