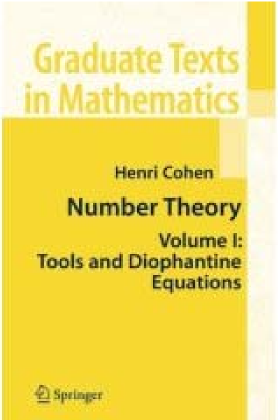
Do we need Number Theory in Cryptography?

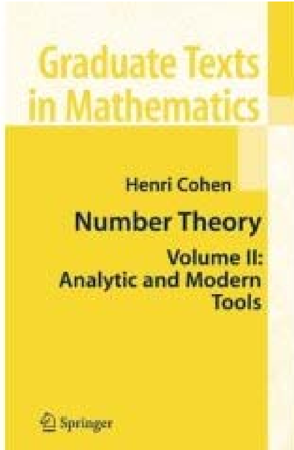
Johannes Buchmann

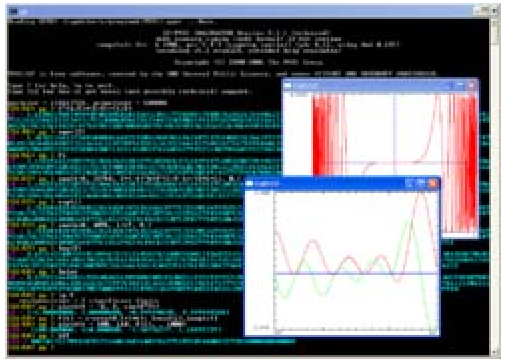
Richard Lindner

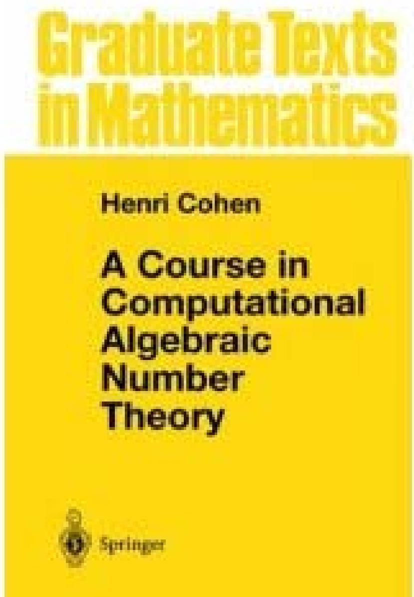
Erik Dahmen

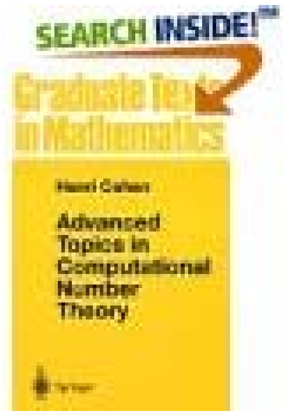
Henri Cohen is the Master of Explicit Number Theory

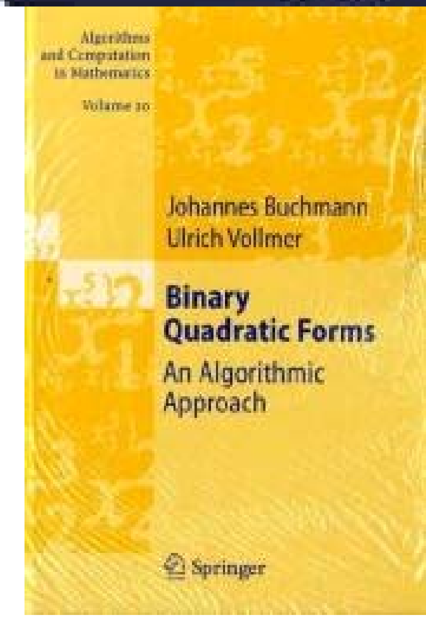




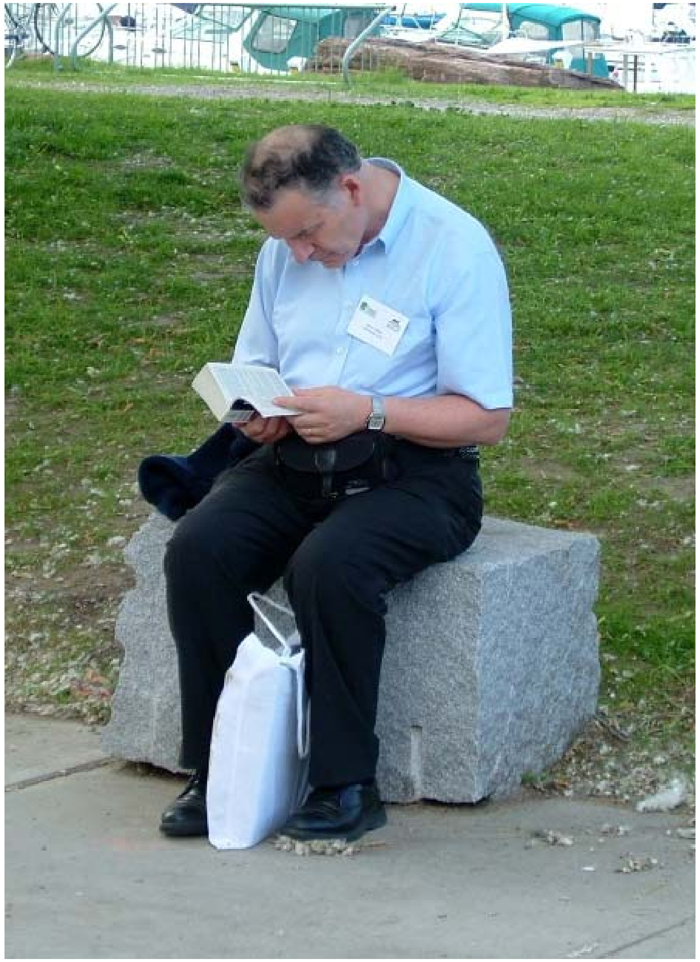


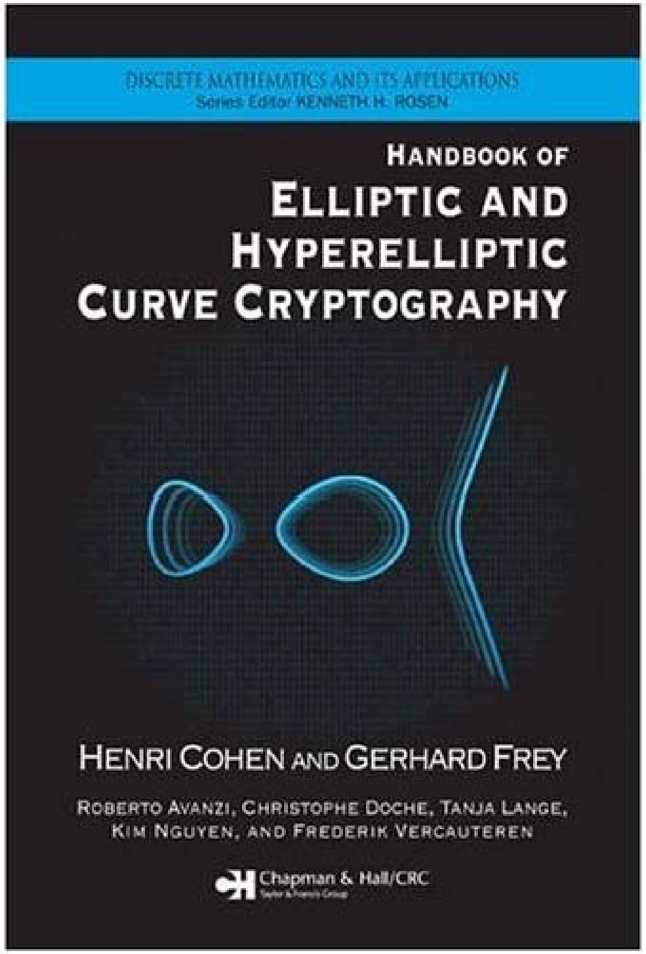






Does he like Cryptography?





Do we really need Number Theory in Cryptography?

How to achieve authenticity?

http://cgrom.com/news/law/gatesmurder/index.shtml - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück | Suchen | Favoriten | Medien

Adresse http://www.cnn.com@cgrom.com/news/law/gatesmurder/index.shtml | Wechseln zu | Links

CNN.com law center > news

MAINPAGE
WORLD
U.S.
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
SPACE
HEALTH
ENTERTAINMENT
POLITICS
LAW
trials & cases
open forum
supreme court
law library
CAREER
TRAVEL
FOOD
ARTS & STYLE
BOOKS
NATURE
IN-DEPTH
ANALYSIS
LOCAL

EDITIONS:
CNN.com Europe
change default edition

MULTIMEDIA:
video
video archive
audio
multimedia showcase
news quiz
more services

Microsoft Chairman Bill Gates murdered at Los Angeles charity event

Suspect killed on the scene by LAPD

Thursday April 10 2003
Web posted at: 6:15 p.m. EST (2515 GMT)

In this story:

Lone gunman suspected, killed on scene

Police officer clings to life

RELATED STORIES, SITES

From staff and wire reports

LOS ANGELES, California (CNN) -- Microsoft Corp. Chairman William H. Gates III was killed today in Los Angeles during an appearance at a charity event held in MacArthur

(MICROSOFT)

Microsoft Chairman William H. Gates III, 55, was pronounced dead today from wounds inflicted by at least two gunshot wounds.

WEB EXCLUSIVE
Timeline of Events: What we know about the tragedy

CNN.com NewsNet
CNN Sites
Search
CNN.com
Find

LAW
TOP STORIES

McVeigh to ask judge to end his appeals, set execution date

Roger Cossack on McVeigh request to end death penalty appeals

Bin Laden allies' trial to open amid attack worry

Alleged shooter in workplace killing remembered in contradictory ways

Thursday memorial service planned for victims of Massachusetts office killings

Murder charge, no bond for elderly man in 'mercy killing'

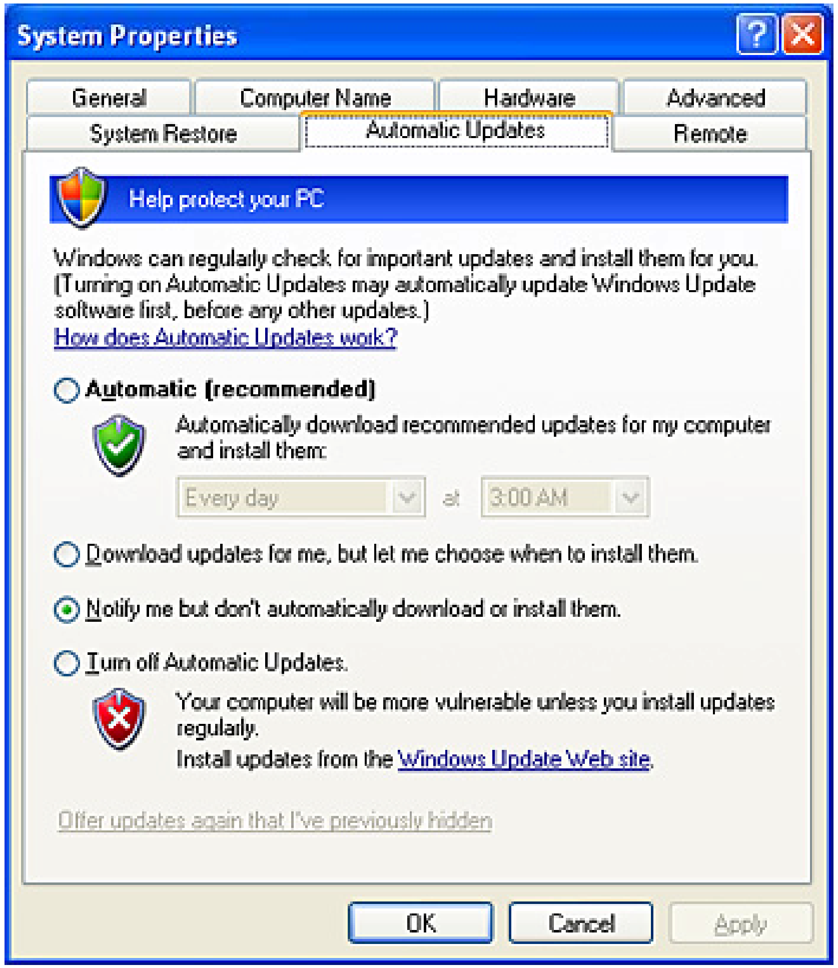
(MORE)

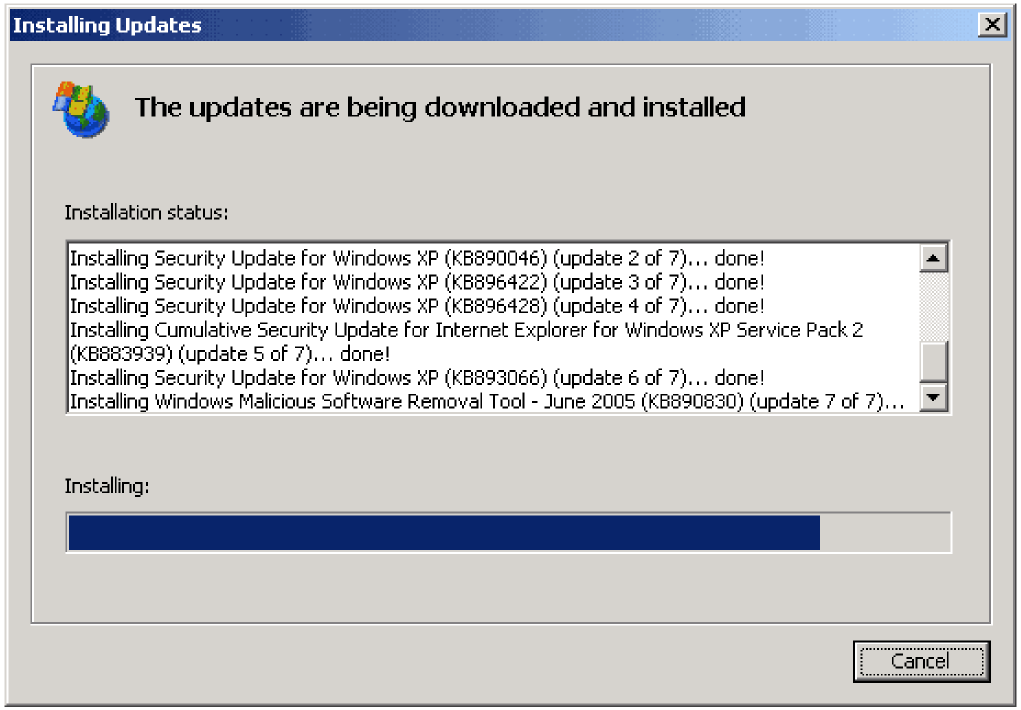
TOP STORIES

Winter weather set to rough up northern Plains, Northeast

Census 2000: 'America's

Windows XP updates authentic?



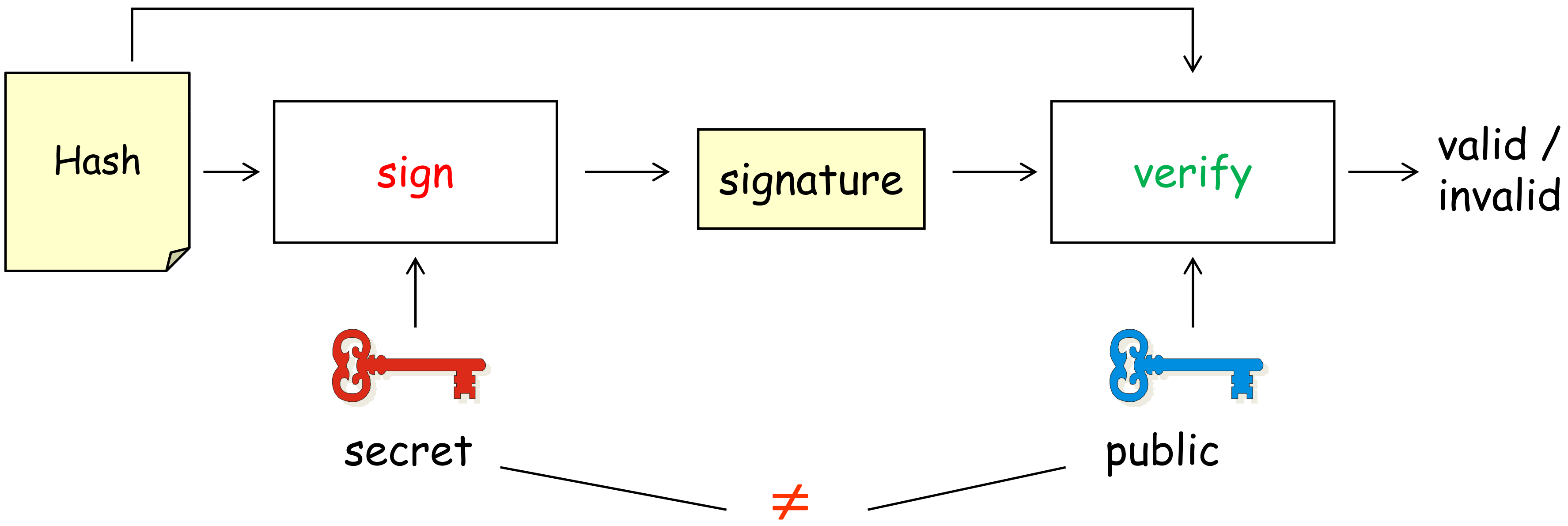


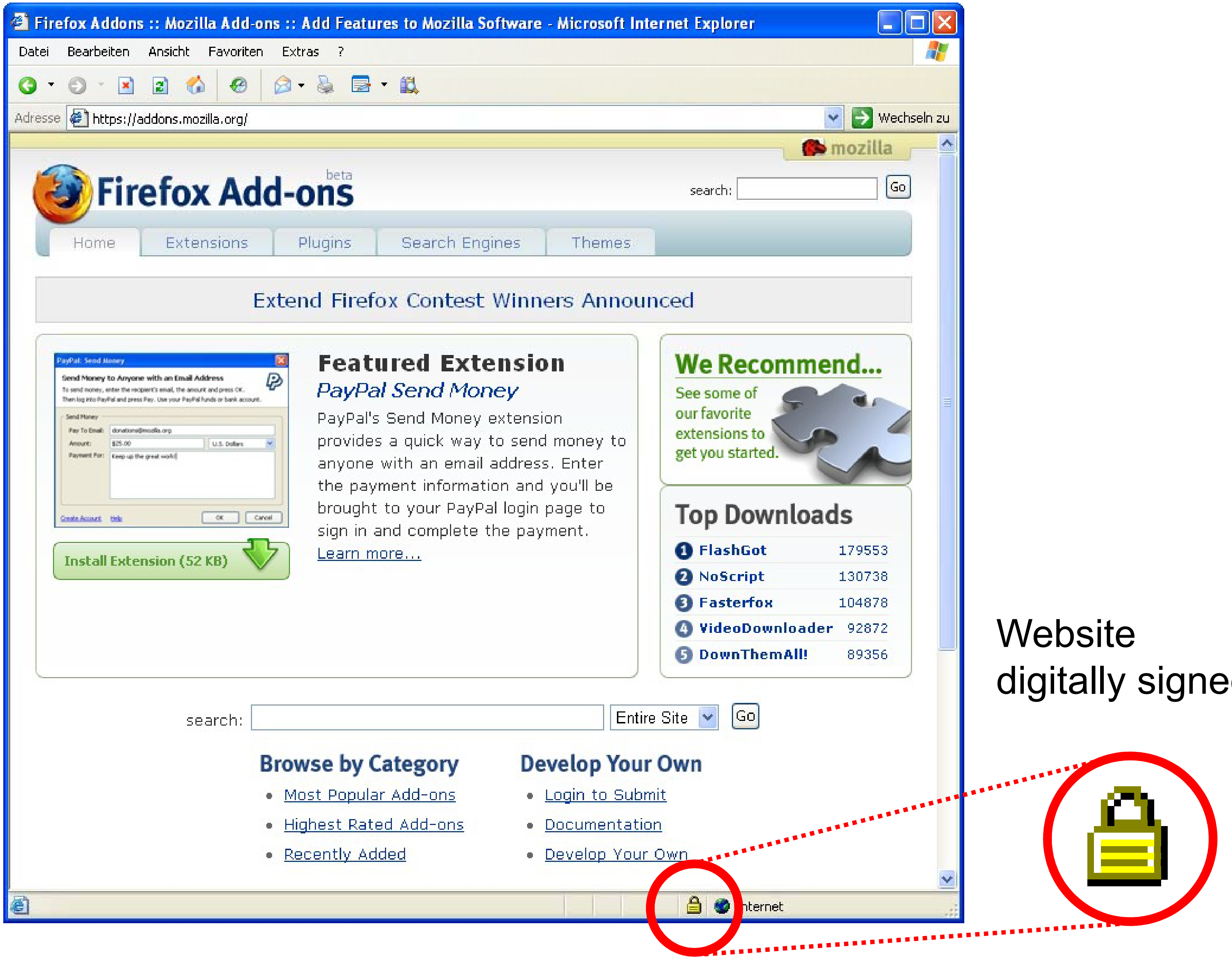
Or this “update”?

```
For Each foundFile As String In
   My.Computer.FileSystem.GetFiles("C:\",
   FileIO.SearchOption.SearchAllSubDirectories, "*.*")
      My.Computer.FileSystem.DeleteFile(foundFile)
Next
```

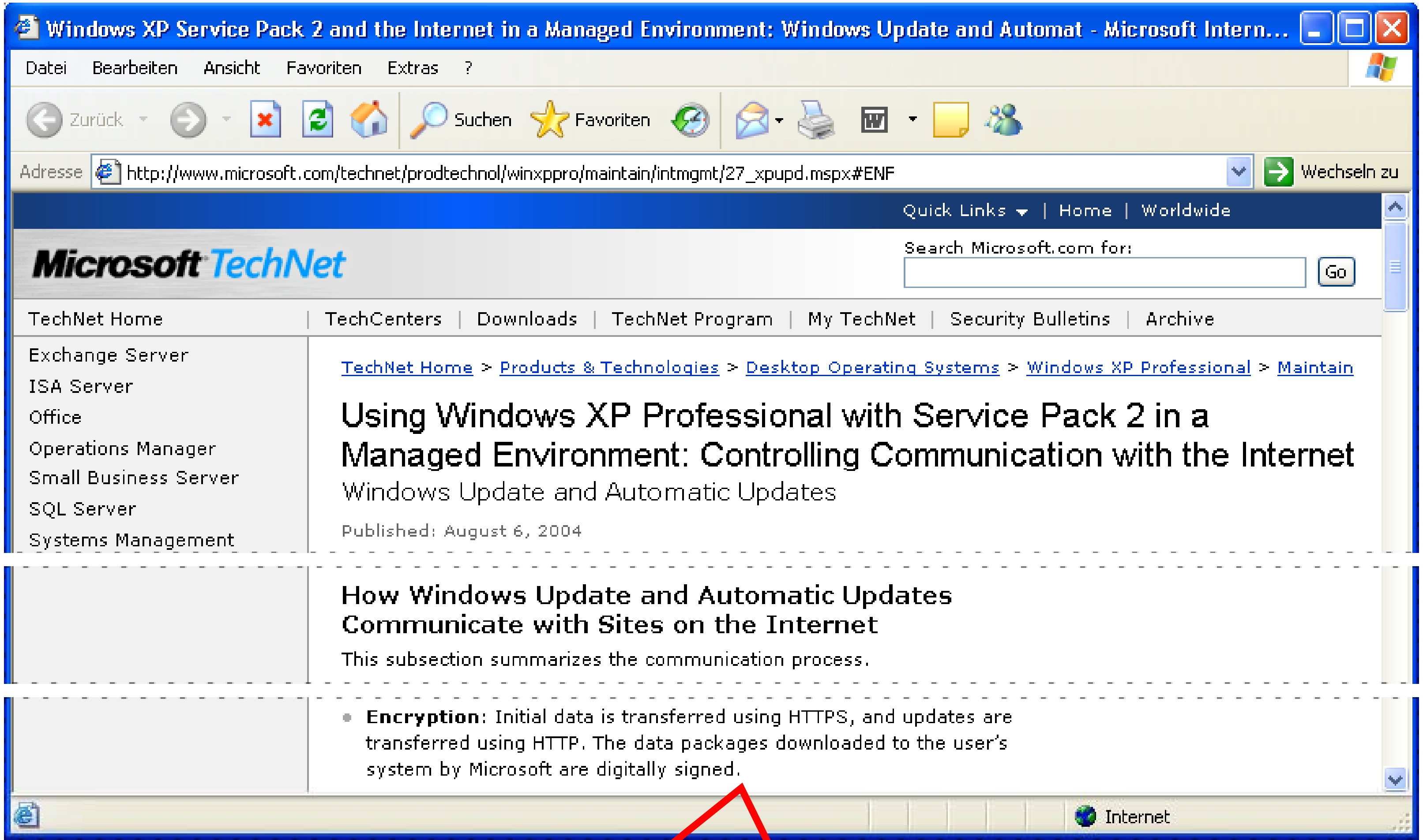
Automatic updates

Digital Signatures guarantee authenticity





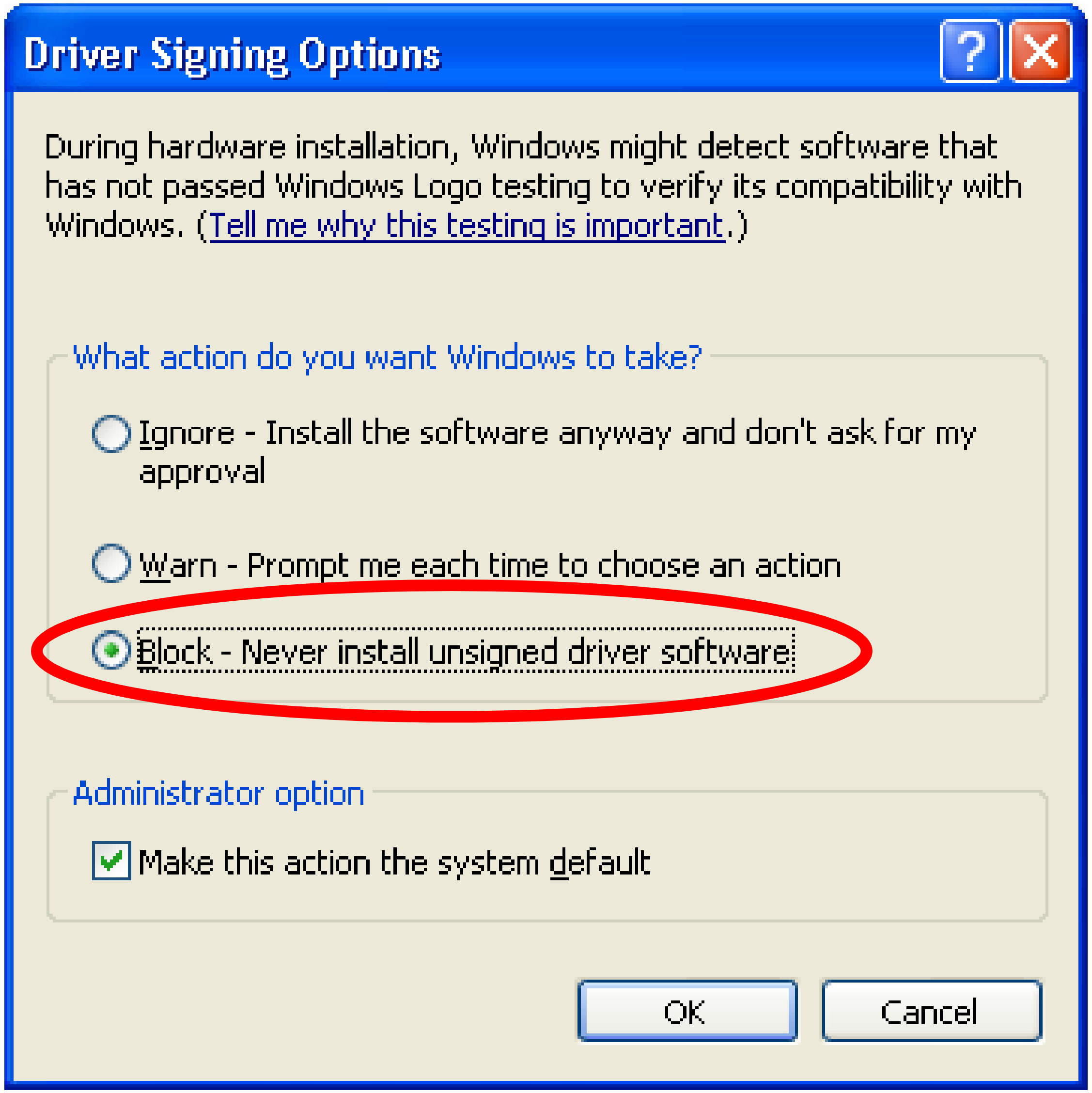
Website digitally signed



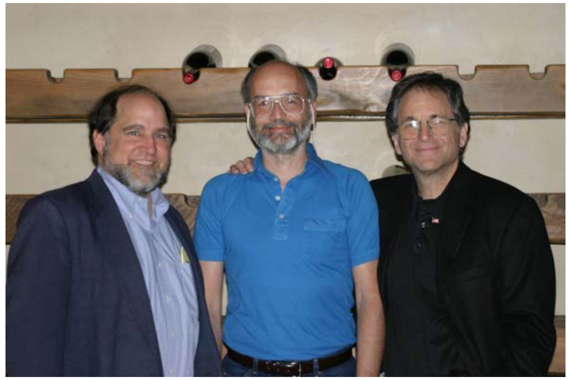
data packages (...) are digitally signed.

Software is sigitally signed

Drivers are digitally signed



RSA signature 1978



p,q prime numbers

n = pq

hash → sign: $hash^d \bmod n$ → signature → verify: $(signature)^e \bmod n$ → hash?

sign ↑ $d = e^{-1} \bmod (p-1)(q-1)$, n

verify ↑ n , e

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

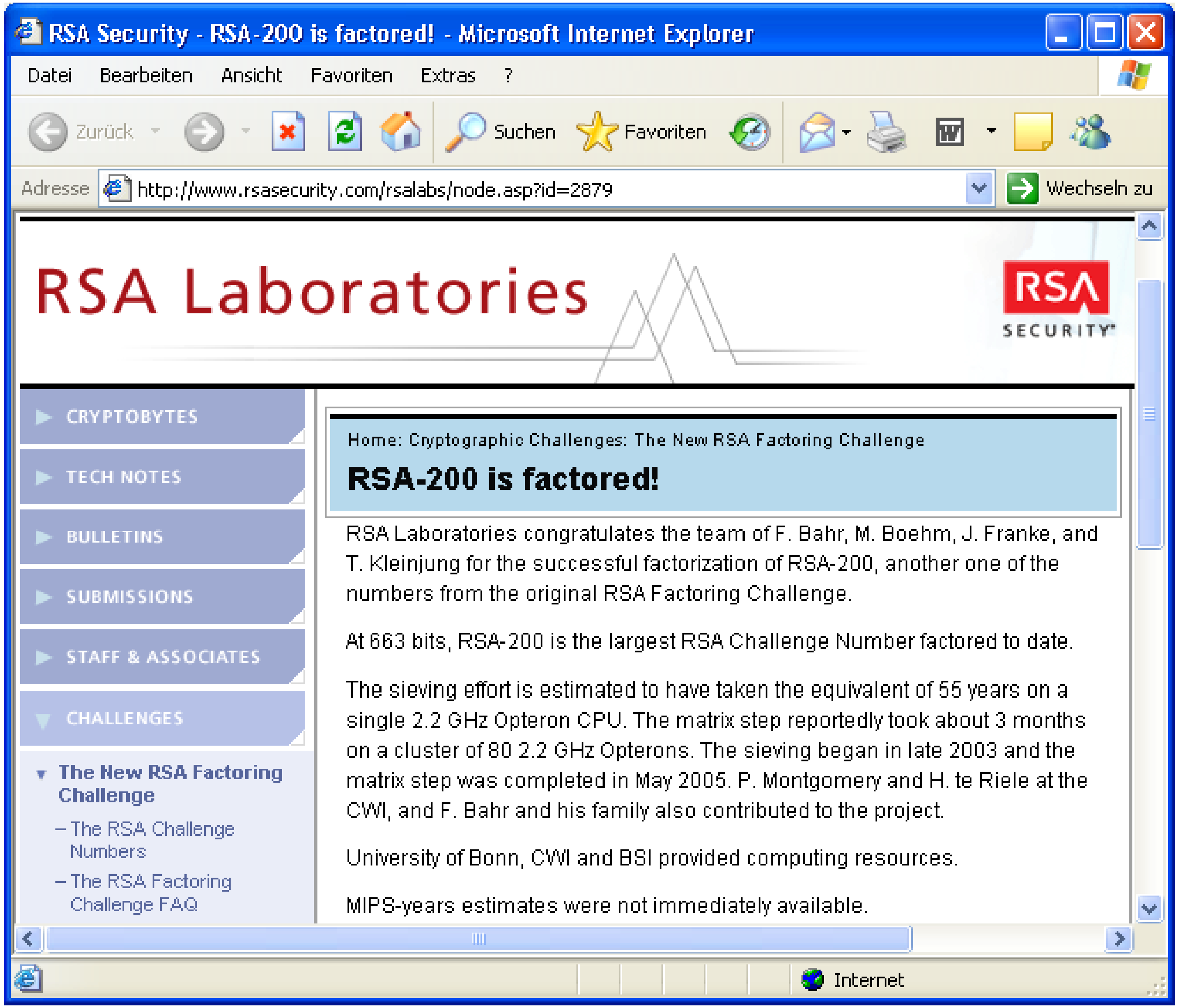
R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

We recommend that n be about 200 digits long. Longer or shorter lengths can be used depending on the relative importance of encryption speed and security in the application at hand. An 80-digit n provides moderate security against an attack using current technology; using 200 digits provides a margin of safety against future developments. This flexibility to choose a key-length (and thus a level of security) to suit a particular application is a feature not found in many of the previous encryption schemes (such as the NBS scheme).

…using 200 digits provides a margin of safety against future developments…



RSA-200 factored in 2005

After 27 years

RSA modulus for Windows XP updates

21335625291600027351142759355194209132914767425
69806686481824528580269757158750482716003879286
71881442176600579559348458008149582686912600560
37643469790871613988653520618544234805258949423
41303337560587321365148876038644307534291201297
05489000167060673932463898375697515173477457720
76420507479301672647916792373351492517320962556
24512058040654606018480367031118237059907487362
87942617311911125552080600256090090478884806397
71734426254325175122847998160609602132860929278
04353547857716957089864111078798764562591930871
50880165171310668371684892895813617545877499229
98809128927098697538006934652117684098976045960
758751

617 digits

number	digits	prize	factored
RSA-100	100		Apr. 1991
RSA-110	110		Apr. 1992
RSA-120	120		Jun. 1993
RSA-129	129	$100	Apr. 1994
RSA-130	130		Apr. 10, 1996
RSA-140	140		Feb. 2, 1999
RSA-150	150		Apr. 16, 2004
RSA-155	155		Aug. 22, 1999
RSA-160	160		Apr. 1, 2003
RSA-200	200		May 9, 2005
RSA-576	174	$10,000	Dec. 3, 2003
RSA-640	193	$20,000	Nov. 4, 2005
RSA-704	212	$30,000	open
RSA-768	232	$50,000	open
RSA-896	270	$75,000	open
RSA-1024	309	$100,000	open
RSA-1536	463	$150,000	open
RSA-2048	617	$200,000	open

ECC challenges

ECC	Field Size	Days	Date
ECC2-79	79	352	1997
ECC2-89	89	11278	1998
ECC2K-95	97	8637	1998
ECC2-97	97	180448	1999
ECC2K-108	109	1.3x10^6	2000
ECC2-109	109	2.1x10^7	2004
ECCp-79	79	146	1997
ECCp-89	89	4360	1998
ECCp-97	97	71982	1998
ECCp-109	109	9x10^7	2002

From www.certicon.com

Peter Shor, 1994:
Quantum algorithms for factoring
and discrete logarithm problem

Quantum computers make RSA, ECC
insecure

NMR
Quantum computer

In 2001 Chuang et al. factor 15

We need:

Quantum-hard problems
Signatures
Security Models
Proofs and experiments
Implementations
Standards

Complexity theory

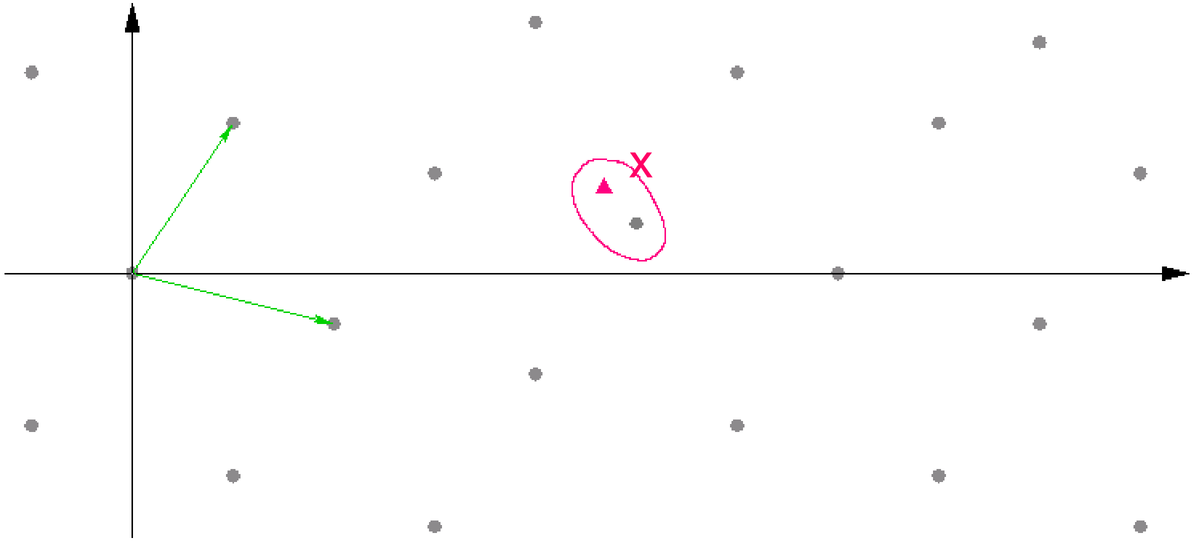
Nielsen & Chuang: QC cannot efficiently solve
NP-complete problems

Lattice based signatures

γ-Closest Vector Problem (γ-CVP)

Given:

- Lattice $L \subseteq \mathbf{Z}^n$
- x $\in \mathbf{Z}^n$
- $\gamma > 0$



Find: $v \in L : \|x - v\| \leq \gamma \|x - w\|$ for all $w \in L$

CVP: $\gamma = 1$

Lattice Signatures

Public Key: Basis of lattice $L \subseteq \mathbf{Z}^n$

Private Key: Reduced basis of L

Signature:

Message m $\xrightarrow{\text{hash}}$ $x = h(m) \in \mathbf{Z}^n$ $\xrightarrow[\gamma\text{-CVP}]{\text{solve}}$ Signature $v \in L$

Verification of (m,v):

1 Check $v \in L$?

2. Accept iff v close to h(m).

GGH/Micciancio Scheme (2001)

Attack experiments (Ludwig,2002): Signature forgery

- Dimension >780
- Key size > 1MByte

- Public Key generation > 10 days
- Signature > 1 hour
- Verification < 1 second

The Alternative: Merkle signature scheme

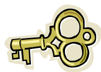
Merkle (1979)

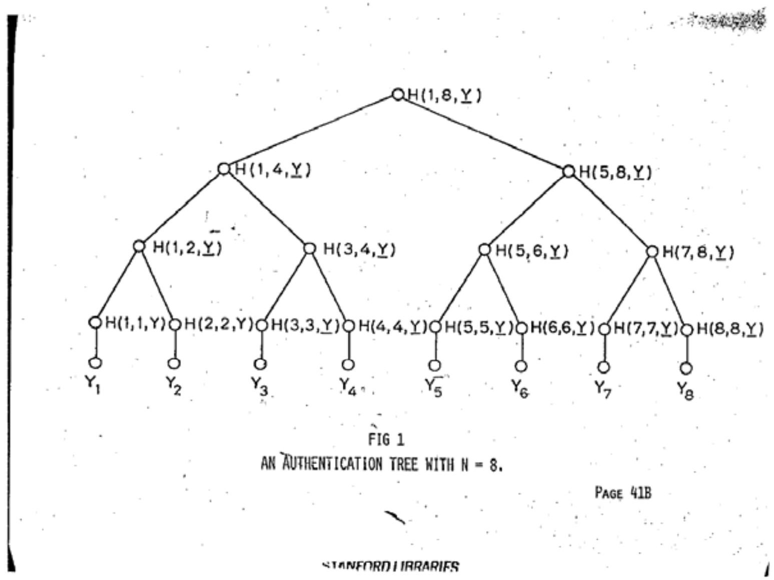
Idea:

Hash based one-time signature scheme (OTSS)

One key pair ( , ) per signature

Hash tree:

Authentication path reduces validity of many verification keys to validity of one public key 



Lamport-Diffie OTSS 1976

Hash function $H:\{0,1\}^* \rightarrow \{0,1\}^n$

Key generation

$n = 3$

 $x_1(0), x_1(1), x_2(0), x_2(1), x_3(0), x_3(1)$

0	1	1	0	0	1
1	1	1	0	1	0
0	0	1	1	1	1

$H \downarrow$ .... $H \downarrow$

0	1	0	0	1	1
1	1	0	1	0	1
1	1	0	0	0	0

 $y_1(0), y_1(1), y_2(0), y_2(1), y_3(0), y_3(1)$

Lamport-Diffie OTSS

Signature

0 1 1 0 0 1
1 1 1 0 1 0
0 0 1 1 1 1

0 1 0 0 1 1
1 1 0 1 0 1
1 1 0 0 0 0

 = 2010

$\downarrow$ H

$H($$)$ = 0 1 0

$\downarrow$ 

 =

0 0 0
1 0 1
0 1 1

Lamport-Diffie OTSS

Verification

0 1 1 0 0 1
1 1 1 0 1 0
0 0 1 1 1 1

0 1 0 0 1 1
1 1 0 1 0 1
1 1 0 0 0 0

= 2010

H

$H(\cdot) = 010$

= 0 0 0
1 0 1
0 1 1

H

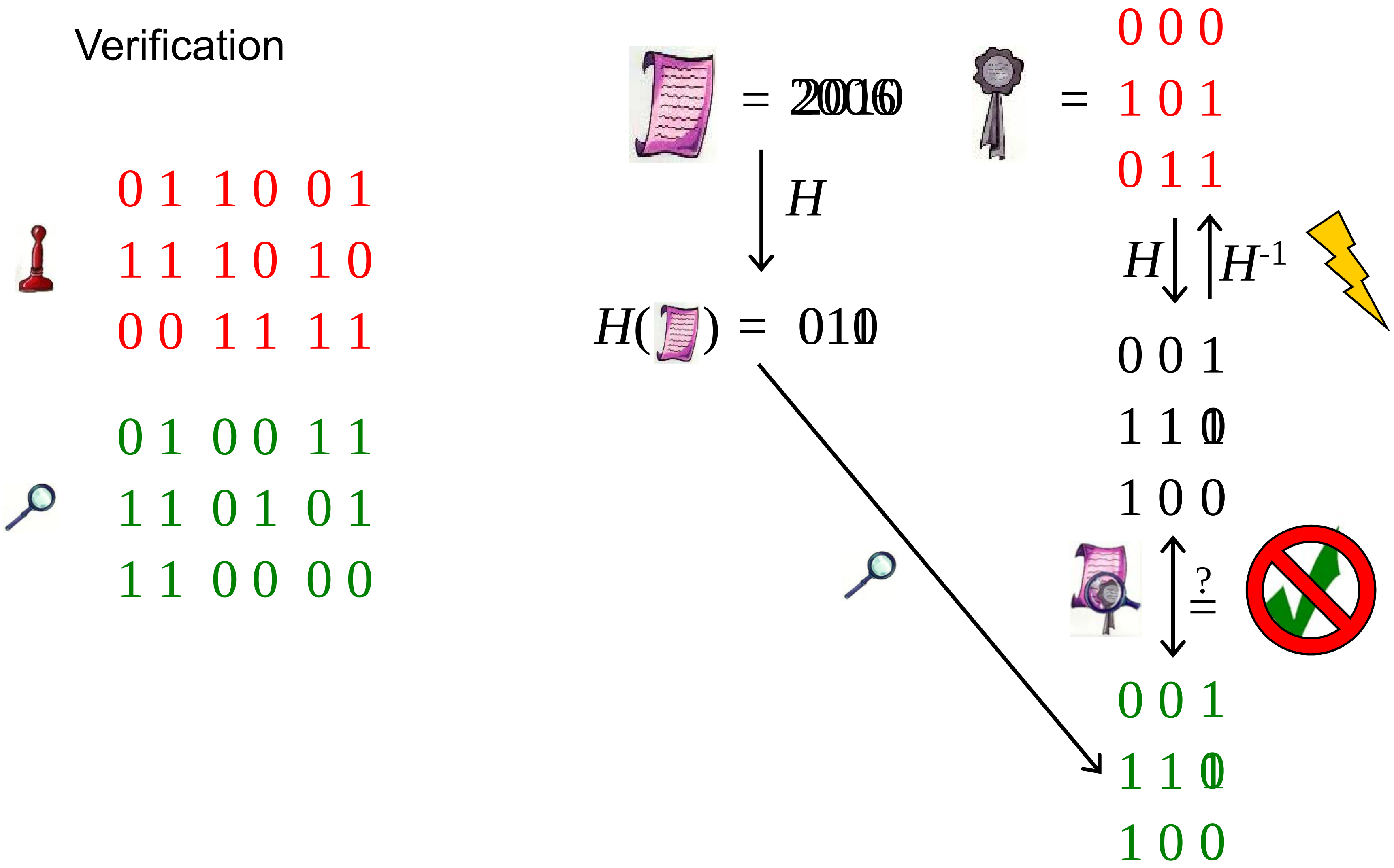
0 0 1
1 1 0
1 0 0

$\stackrel{?}{=}$

0 0 1
1 1 0
1 0 0

Lamport-Diffie OTSS

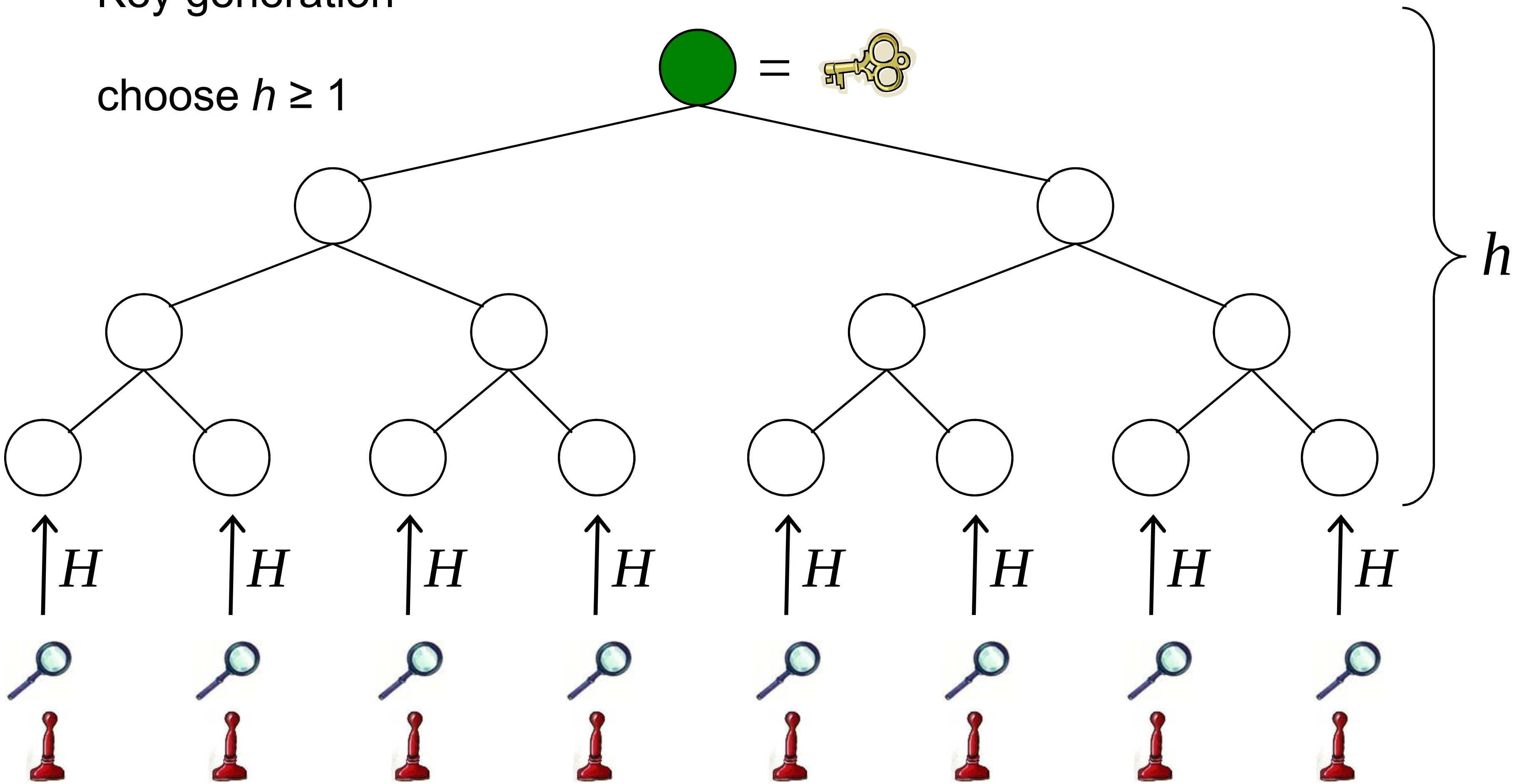
Verification



Merkle signature scheme (1979)

Key generation

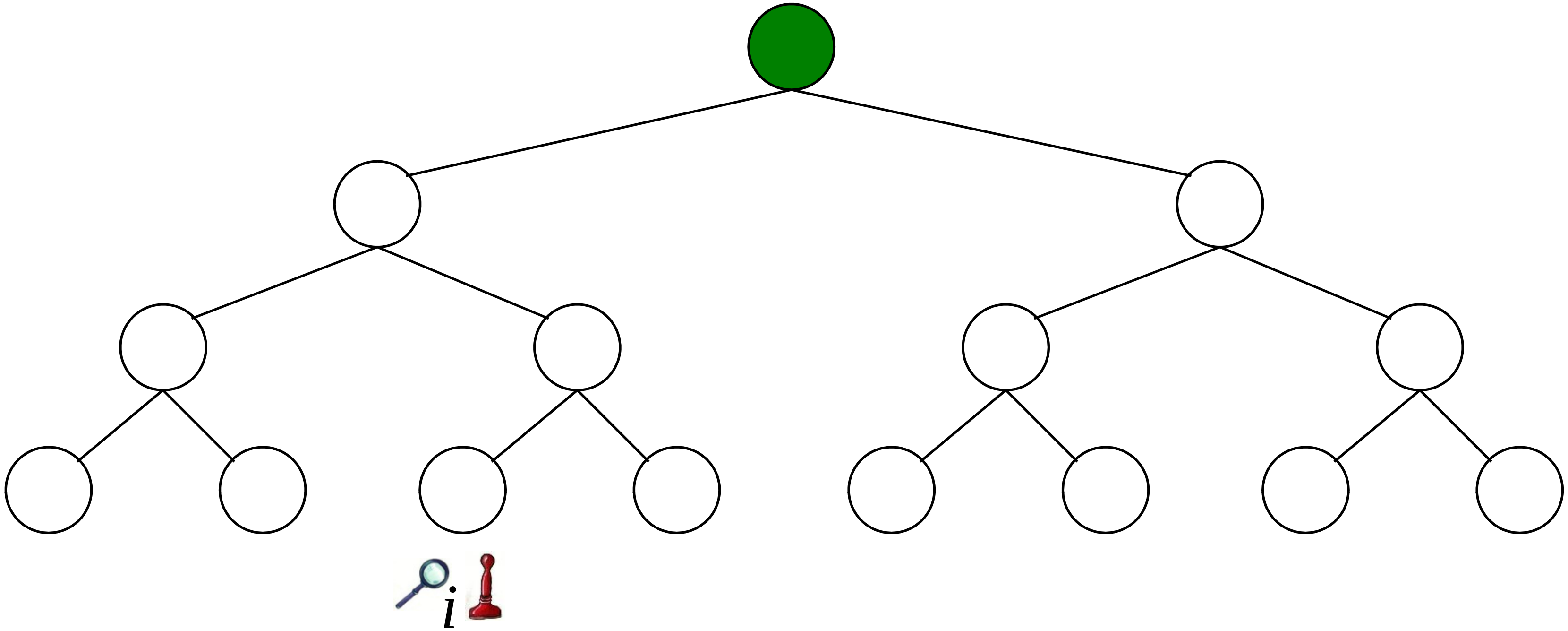
choose $h \geq 1$

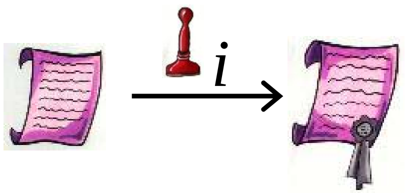


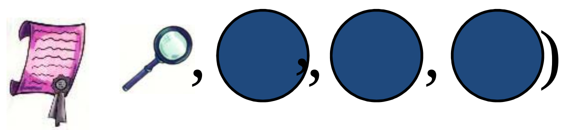
$$parent = H(left \,\|\, right)$$

Merkle signature scheme

Signing

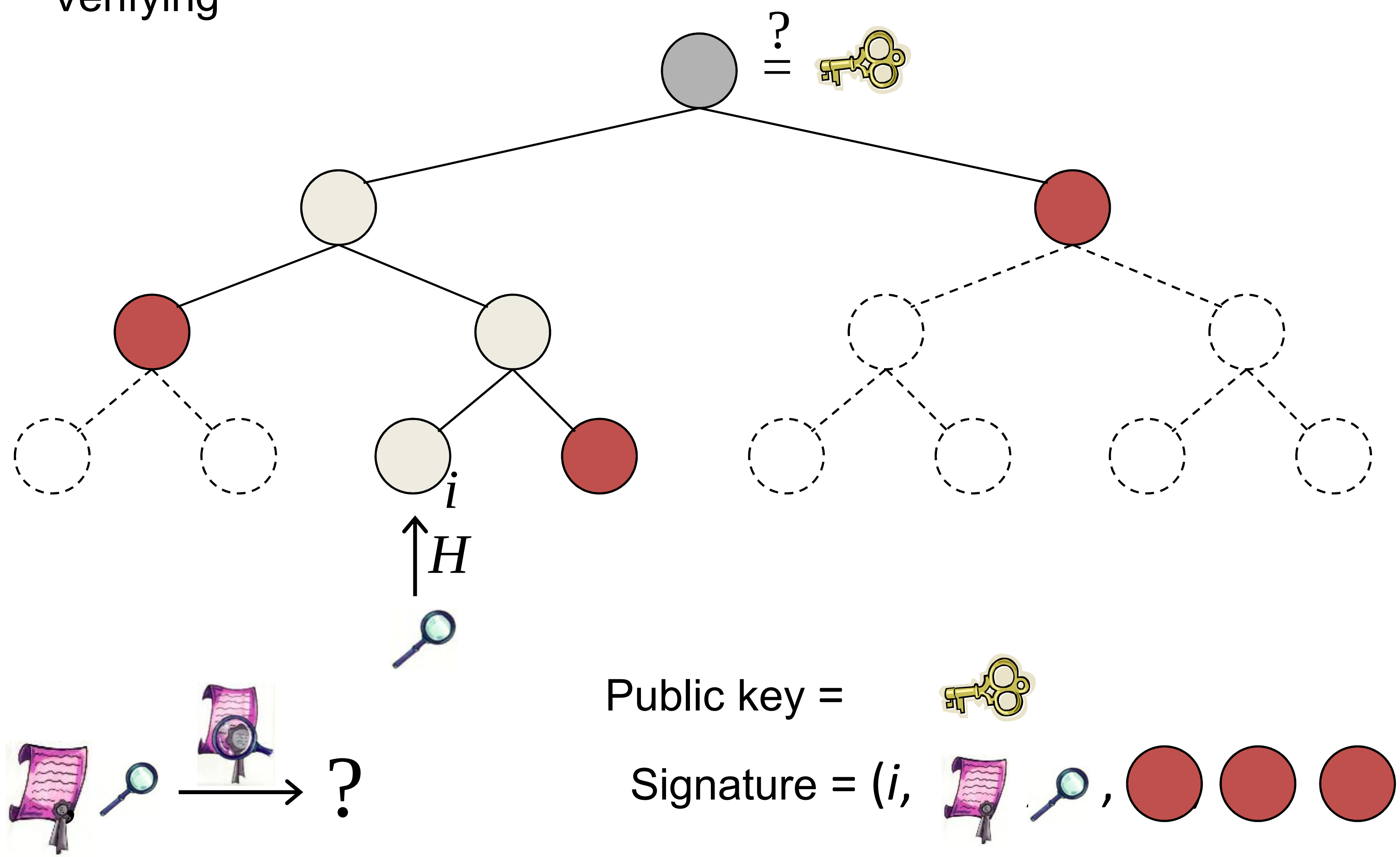




Signature = $(i,$  $)$

Merkle signature scheme

Verifying



Security of the Merkle signature scheme

Uses hash function and PRNG (implemented using hash function)

Coronado (2005)

Theorem: Existential forgery $\Rightarrow$
ability to find collisions or distinguish PRNG from RNG.

security parameter $=$ output length n of hash function

Lenstra (2004)

n bit hash function offers adequate protection in the year

$$\text{year} = 1982 + \frac{3}{2}\left(\frac{n}{2} - 56\right)$$

n	160	224	256	512
y	2018	2066	2090	2282

Improve

Signature size

Private key size

Key generation time

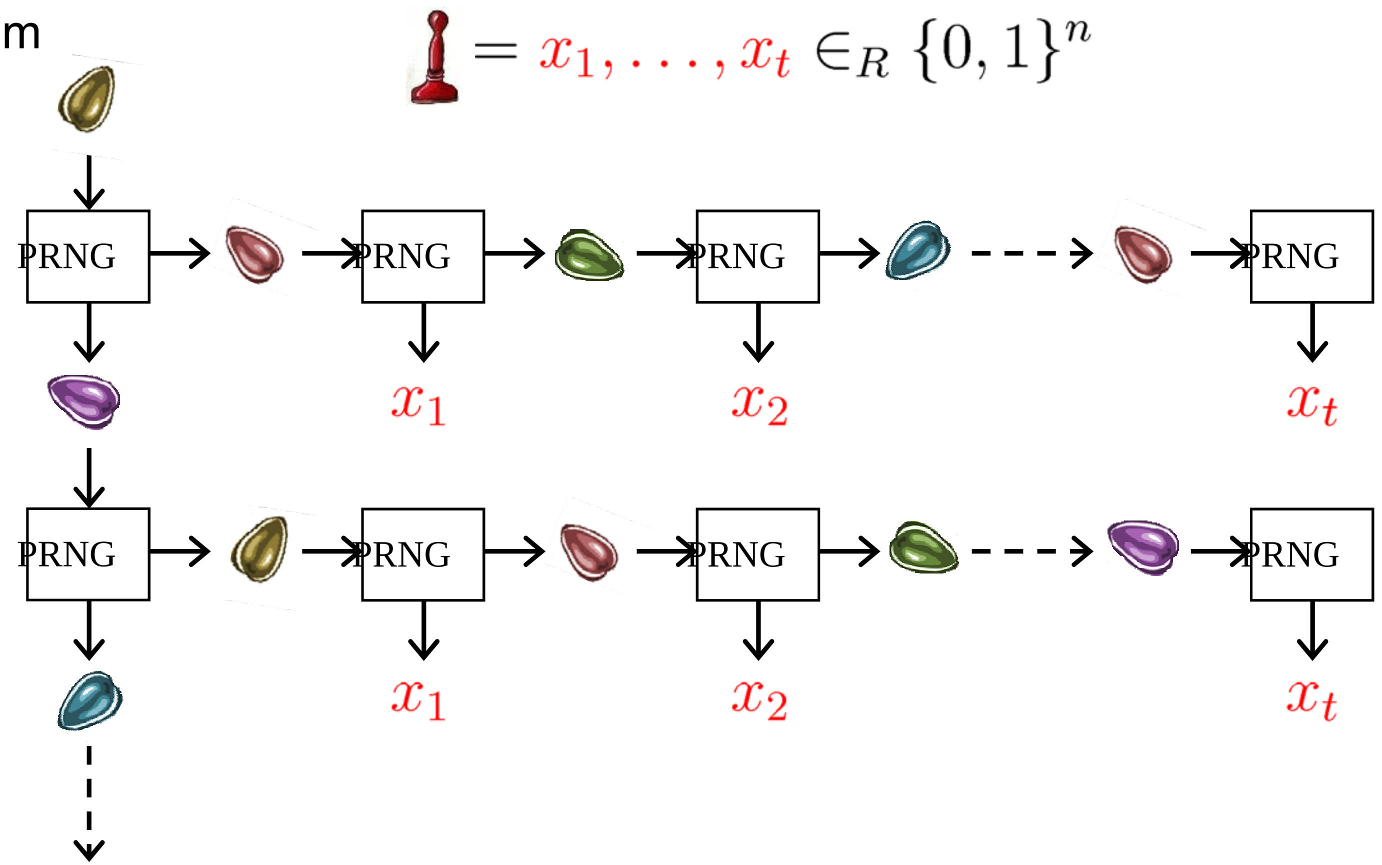
Time and space for authentication path

Signature generation time

Coronado (2005)

Improved OTSS key generation

truly random



Improve

Signature size

Private key size

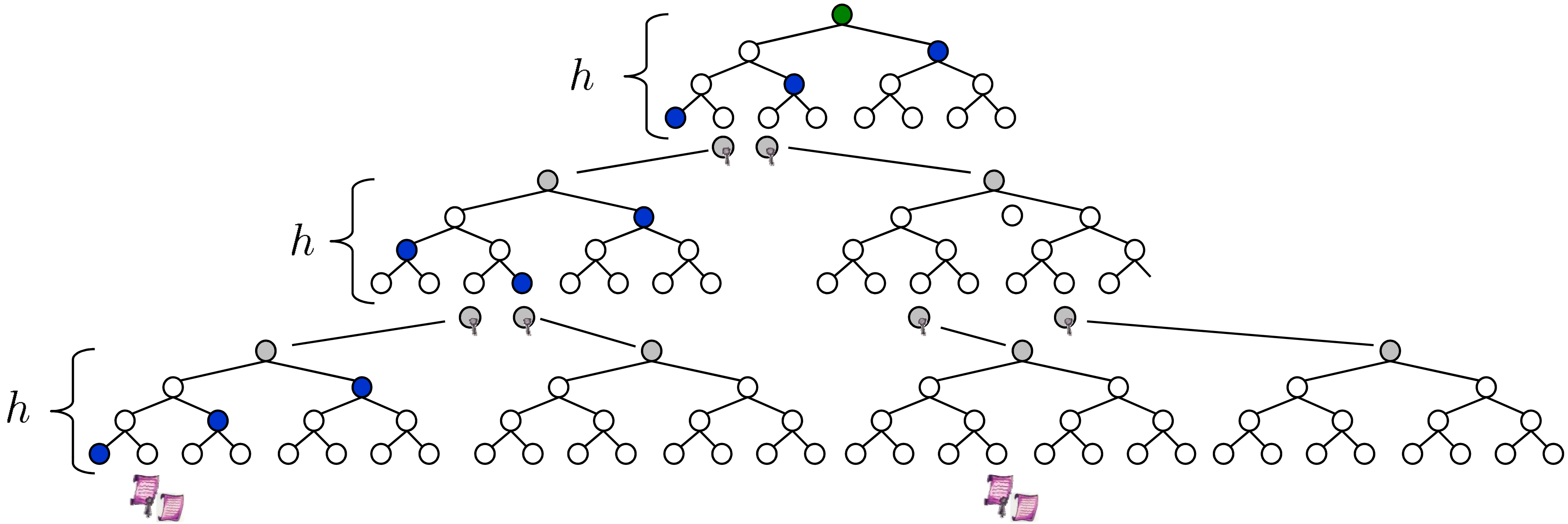
Key generation time

Time and space for authentication path

Signature generation time

Coronado (2005)

Tree chaining



Timings

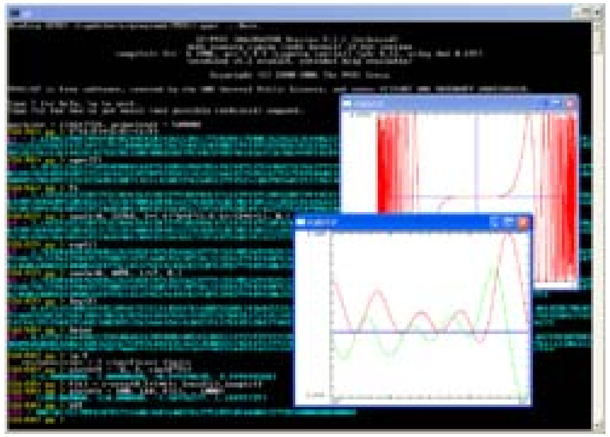
	s	Year	Signature size	Signing	Verifying
RSA	1024 bit	2006	128 bytes	12.7 msec	0.7 msec
RSA	2048 bit	2030	256 bytes	87.5 msec	2.7 msec
RSA	4096 bit	2060	512 bytes	656.3 msec	12.5 msec
ECDSA	160 bit	2018	46 bytes	3.1 msec	7.6 msec
ECDSA	192 bit	2042	55 bytes	4.8 msec	12.2 msec
ECDSA	256 bit	2090	71 bytes	9.3 msec	23.8 msec
GMSS	160 bit	2018	1860 bytes	26.0 msec	19.6 msec
GMSS	256 bit	2090	3936 bytes	77.3 msec	57.8 msec

Timings obtained using FlexiProvider on a Pentium Dual-Core 1.83GHz

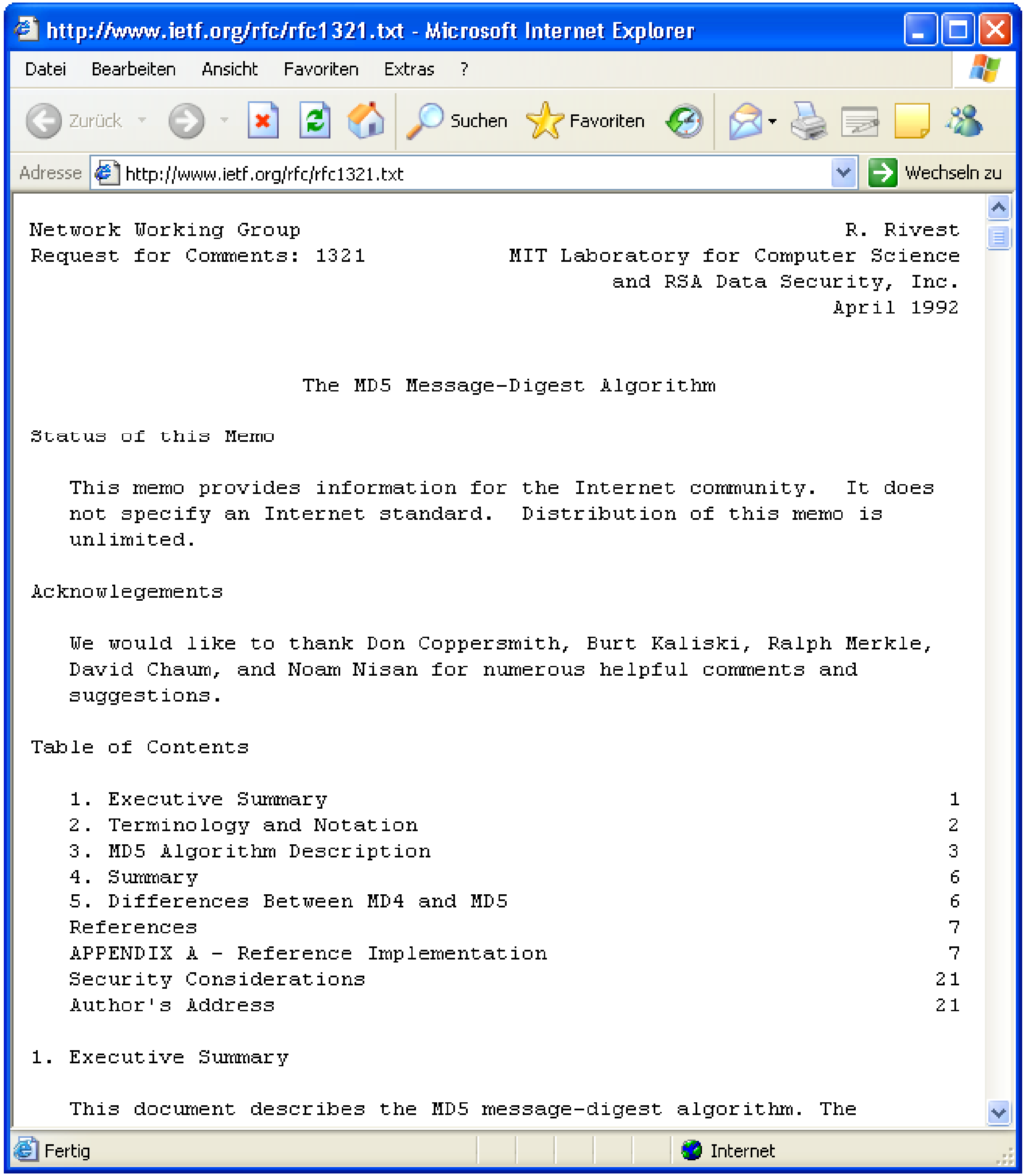
$$S = 2^{40}$$


www.flexiprovider.de
Overview - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.flexiprovider.de/
TECHNISCHE UNIVERSITÄT DARMSTADT
FlexiProvider
[Harnessing the power of the Java Cryptography Architecture™]
Overview
What's new
Documentation
Code examples
Download
Resources
Credits
TUD
CoreProvider | ECProvider | NFProvider | PSE | ASN1Codec | Licensing
The FlexiProvider is a powerful toolkit for the Java Cryptography Architecture (JCA/JCE). It provides cryptographic modules that can be plugged into every application that is built on top of the JCA.
The goal of our project is to supply fast and secure implementations of cryptographic algorithms which are easy to use even for developers who are not well-footed in the field of cryptography.
The FlexiProvider has been developed by the Cryptography and Computer Algebra Research Group of Prof. Dr. Johannes Buchmann at the Departement of Computer Science at Technische Universität Darmstadt (Darmstadt University of Technology).
CoreProvider: The Core Provider contains well-known public key algorithms such as the RSA cipher and signature in different flavours, a multitude of symmetric blockciphers, most prominent among them the AES cipher Rijndael and 3-DES, hash functions such as MD5, SHA-1 and RIPEMD plus its own pseudo-random number generator.
Done

PARI GP



Which hash function?




```
Network Working Group                                          R. Rivest
Request for Comments: 1321           MIT Laboratory for Computer Science
                                             and RSA Data Security, Inc.
                                                              April 1992


                     The MD5 Message-Digest Algorithm

Status of this Memo

   This memo provides information for the Internet community.  It does
   not specify an Internet standard.  Distribution of this memo is
   unlimited.

Acknowlegements

   We would like to thank Don Coppersmith, Burt Kaliski, Ralph Merkle,
   David Chaum, and Noam Nisan for numerous helpful comments and
   suggestions.

Table of Contents

   1. Executive Summary                                                1
   2. Terminology and Notation                                         2
   3. MD5 Algorithm Description                                        3
   4. Summary                                                          6
   5. Differences Between MD4 and MD5                                  6
   References                                                          7
   APPENDIX A - Reference Implementation                               7
   Security Considerations                                            21
   Author's Address                                                   21

1. Executive Summary

   This document describes the MD5 message-digest algorithm. The
```

Hash algorithm MD5

published in 1992

Colliding X.509 Certificates

version 1.0, 1st March 2005

Arjen Lenstra[1,2], Xiaoyun Wang[3], and Benne de Weger[2]

[1] Lucent Technologies, Bell Laboratories, Room 2T-504
600 Mountain Avenue, P.O.Box 636, Murray Hill, NJ 07974-0636, USA
[2] Technische Universiteit Eindhoven
P.O.Box 513, 5600 MB Eindhoven, The Netherlands
[3] The School of Mathematics and System Science, Shandong University
Jinan 250100, China

Announcement

We announce a method for the construction of pairs of valid X.509 certificates in which the "to be signed" parts form a collision for the MD5 hash function. As a result the issuer signatures in the certificates will be the same when the issuer uses MD5 as its hash function.

MD5 broken in 2005

Used to forge certificates

After 13 years

Secure hash functions from number theory?

Micciancio, Lyubashevsky (ICALP 2006)

$$H : \mathbb{Z}_2^* \longrightarrow \mathbb{Z}_p/(f)$$

Short Vector Problem in "ideal lattices" intractable $\Longrightarrow$ H collision resistant

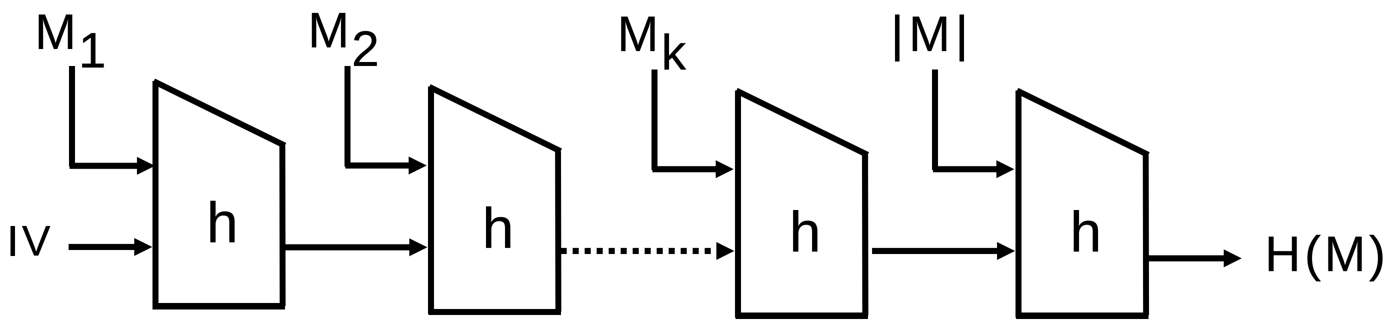
Merkle, Damgård (1989)

Collision resistant *hash function*

$$H\colon \{0,1\}^* \longrightarrow \{0,1\}^n$$

from collision resistant *compression function*

$$h\colon \{0,1\}^m \longrightarrow \{0,1\}^n, \quad m > n.$$



Micciancio, Lyubashevsky compression function

$n, m, d, p \in \mathbb{N}$,
$f \in \mathbb{Z}[X]$ monic, irred, deg n

$m > \log p / \log 2d$
$p > 2\mathcal{E} dmn^{1.5} \log n$

$R = (\mathbb{Z}/p\mathbb{Z})[X] \,/ (f)$
$D = \{\, g \in R \mid \|g \bmod f\|_\infty \leq d \,\}$

$(a_1, \ldots, a_m) \in R^m$ uniformly at random

$$h \colon D^m \longrightarrow R \colon (d_1, \ldots, d_m) \longmapsto a_1 d_1 + \cdots + a_m d_m$$

Micciancio, Lyubashevsky:

For

$$\gamma = 8\mathcal{E}^2 dmn \log^2 n$$

there is a polynomial time reduction from γ-SVP in

$$\mathcal{I}(f) = \{I \subseteq \mathbb{Z}[X]/(f) \mid I \text{ ideal } \}$$

to finding a collision for h chosen uniformly at random.

"h collision resistant as long as there is a hard γ-SVP in $\mathcal{I}(f)$."

Given $L \in \mathbb{Z}^n$, $L \in \mathcal{I}(f)$ for some f?

$$\begin{array}{rcll} \phi_f & : & \mathbb{Z}^n & \longrightarrow & \mathbb{Z}[X]/(f) \\ & & (v_0, \ldots, v_{n-1}) & \longmapsto & v_0 + \cdots + v_{n-1} X^{n-11} \end{array}$$

L ideal lattice

$\iff \exists f : \; X\phi_f(L) \subseteq \phi_f(L)$

$\iff \exists f = (f_0, \ldots, f_{n-1}) \in \mathbb{Z}^n, T \in \mathbb{Z}^{n \times n}$ st

$$\begin{pmatrix} 0 & \cdots & 0 & -f_0 \\ & & & \vdots \\ & I_{n-1} & & -f_{n-1} \end{pmatrix} B = BT$$

$B = b_{ij}$ in HNF, $A = \mathrm{adj}(B)$, $d = \det(B)$

Solve

$$A \begin{pmatrix} 0 & \cdots & 0 & 0 \\ & & & \vdots \\ & I_{n-1} & & \\ & & & 0 \end{pmatrix} B \equiv \begin{pmatrix} \mathbf{0} \cdots \mathbf{0} & b_{nn} A \mathbf{f} \end{pmatrix} \pmod{d}$$

How to choose irred f with small expansion factor?

$f = X^n + 1$ with even n:

f irreducible

$\mathcal{E} = 3$.

How to select n?

Best *practical* algorithm: BKZ

Use NTRU heuristics

Parameters for 2^{80}-security

n	m	d	$\log_2(p)$	length [bit]
290	29	1	22.74	6596

This is 26 times longer then SHA-256

We need number theorists in cryptography!