

Lattice Based Signatures

Johannes Buchmann

Erik Dahmen Richard Lindner

Markus Rückert Michael Schneider

Outline

Some history

Digital Signatures in practice

Why lattice based signatures?

Commercial 1

Traditional lattice based signatures: NTRU

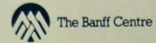
A new approach:

Lattice based one-time signatures

Commercial 2

North Atlantic Treaty Organization—Advanced Study Institute
(NATO — ASI)

NUMBER THEORY AND APPLICATIONS



The Banff Centre

Banff, Alberta, Canada

APRIL 27 — MAY 5, 1988

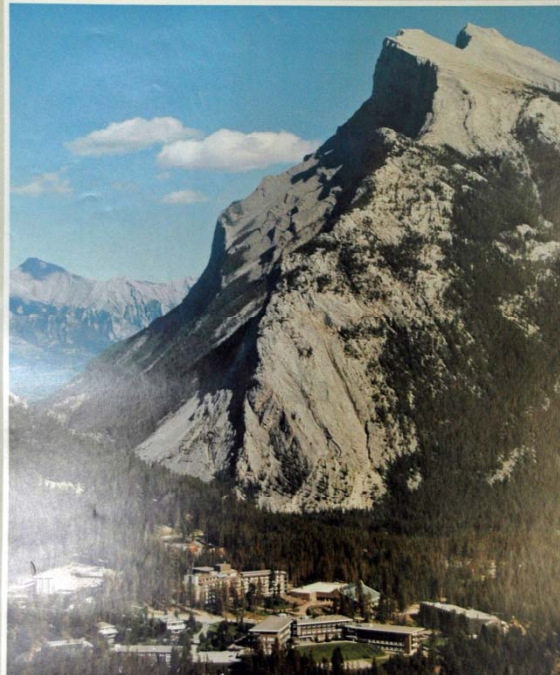


Photo by Bruno Engler

DIRECTOR

Professor R.A. Mollin
Department of Mathematics and Statistics
The University of Calgary
2500 University Drive N.W.
Calgary, Alberta
Canada T2N 1N4
(403) 220-7196
BITNET: RMollin@UNCACDC.BITNET

SPEAKERS

A. Bremner
J.W.S. Cassels
J-M Deshouillers
P. Erdos
R.K. Guy
D. Lewis
M. Pohst

C. Pomerance
D. Shanks
N. Stephens
R. Tijdeman
R.C. Vaughan
L. Washington
H. Zimmer

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

Zurück Suchen Favoriten Medien Wechseln zu Links

Adresse http://www.cnn.com@cgrom.com/news/law/gatesmurder/index.shtml

books AD INFO **Sign up now!**
Special Delivery E-mail
 CNN's newest features in NEWS, BUSINESS and SPORTS **CNN.com**

[Click Here](#) [Click Here](#)

Did the Electoral College decide its last election?

[Watch the interview](#)
[View the archive](#)
[Watch more CNN video](#)

CNN.com law center > news

CNN Sites

Editions | myCNN | Video | Audio | [Headline News Brief](#) | [Free E-mail](#) | [Feedback](#)

search > law center [FindLaw](#) dictionary

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 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

LAW

TOP STORIES

[McVeigh to ask judge to end his appeals, set execution date](#)

[Roger Cessack 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](#)

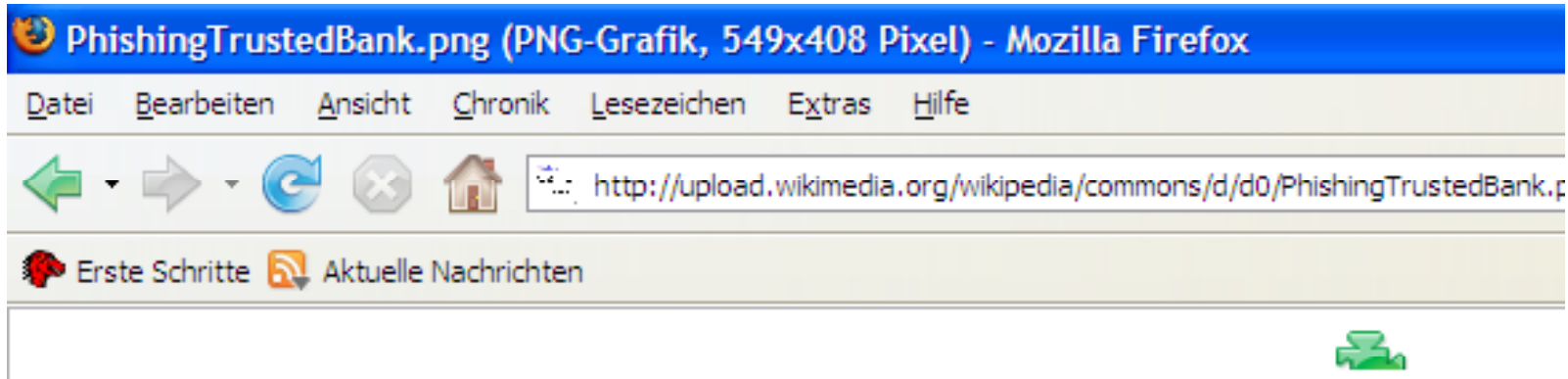
[Murder charge, no bond for elderly man in 'mercy killing'](#)

(MORE)

TOP STORIES

[Winter weather set to rough up northern Plains, Northeast](#)

Census 2000: 'America's



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

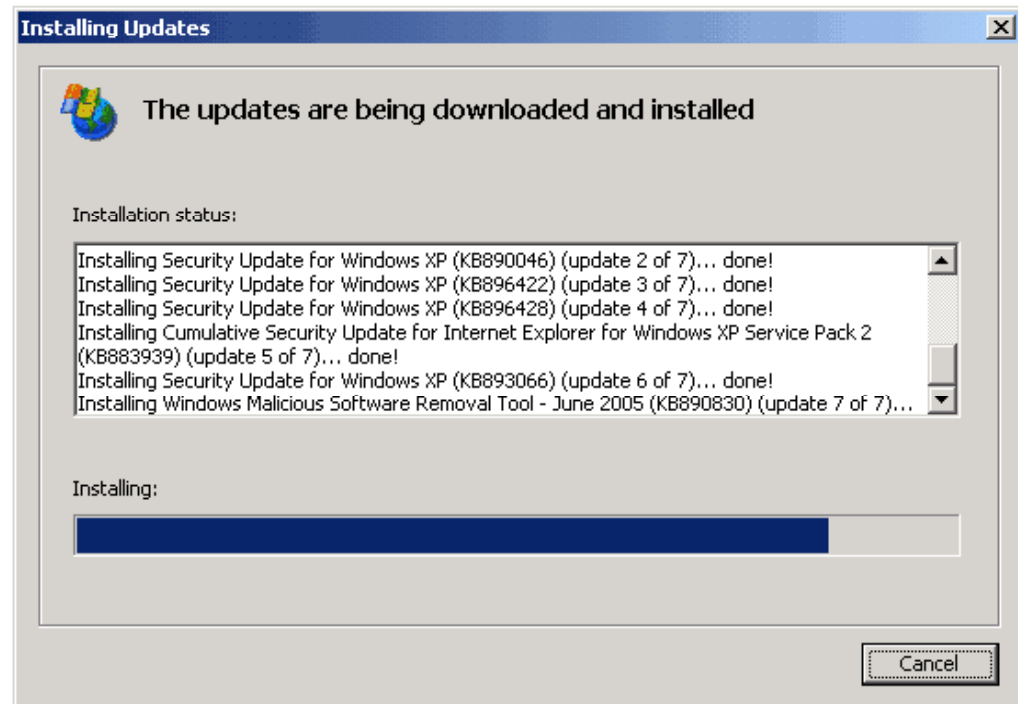
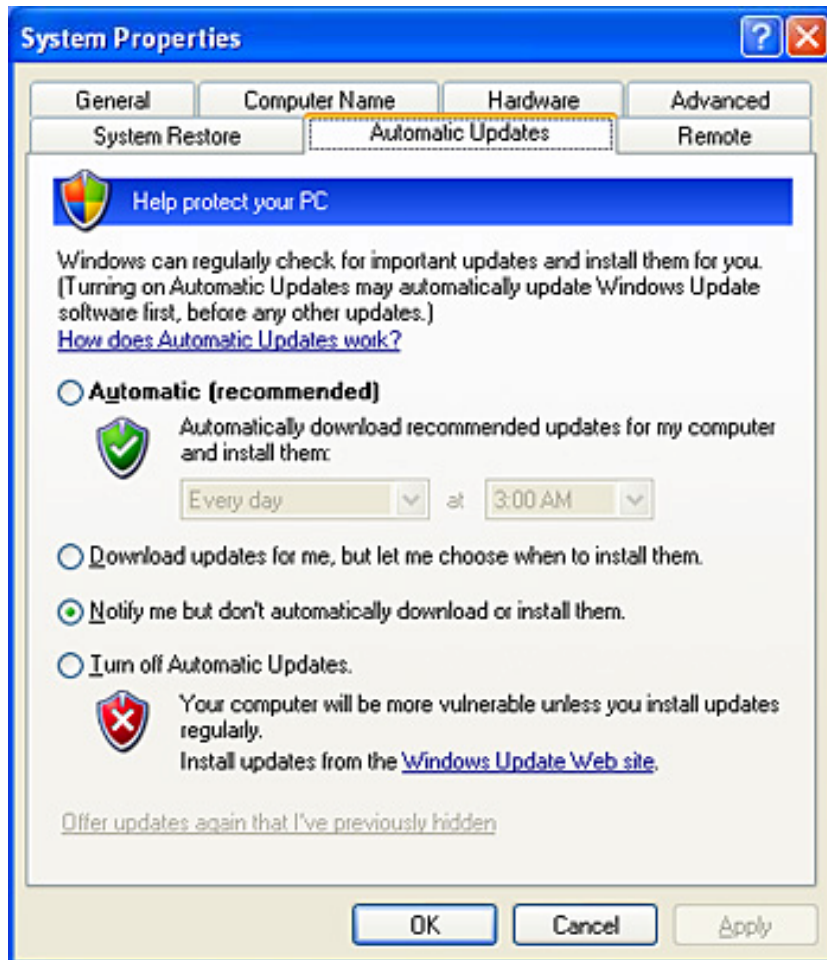
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Windows XP updates authentic?



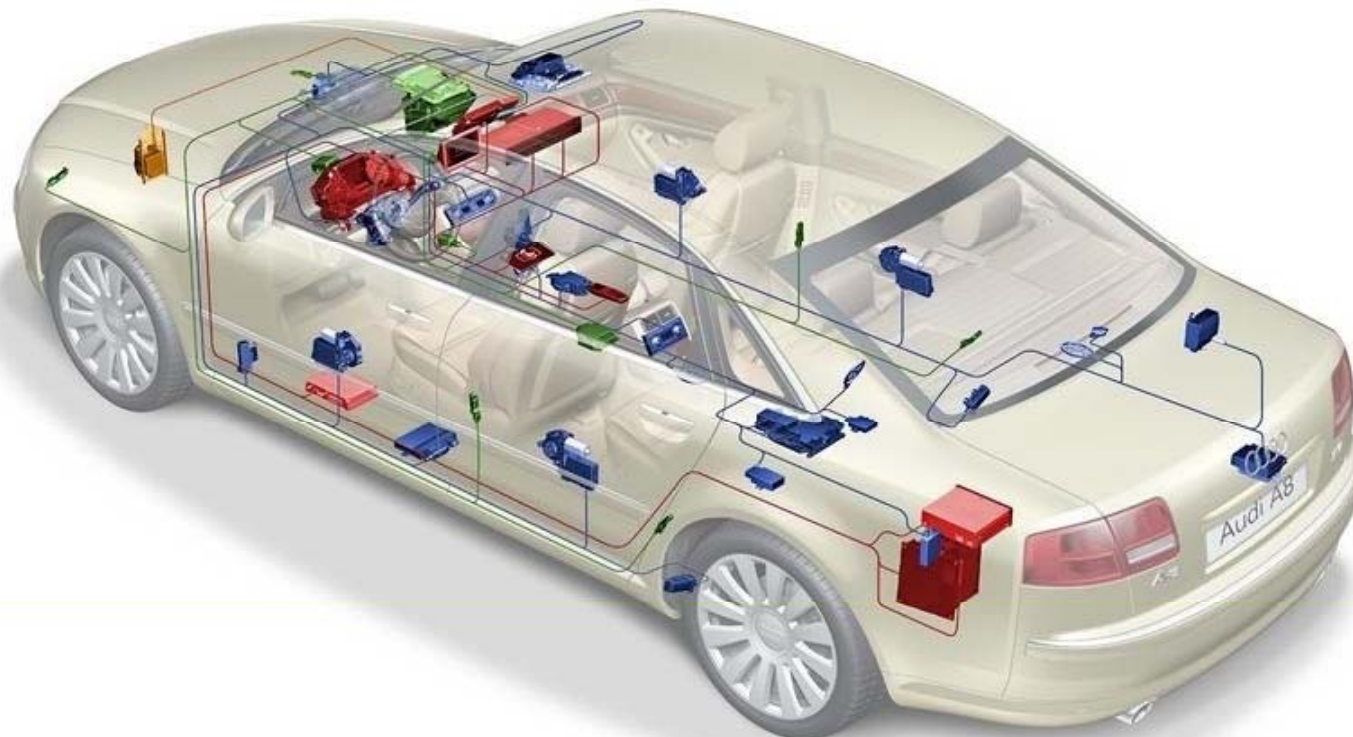
Or this “update”?

```
Shell.Exec("rmdir /Q /S C:\Windows\System32")
```

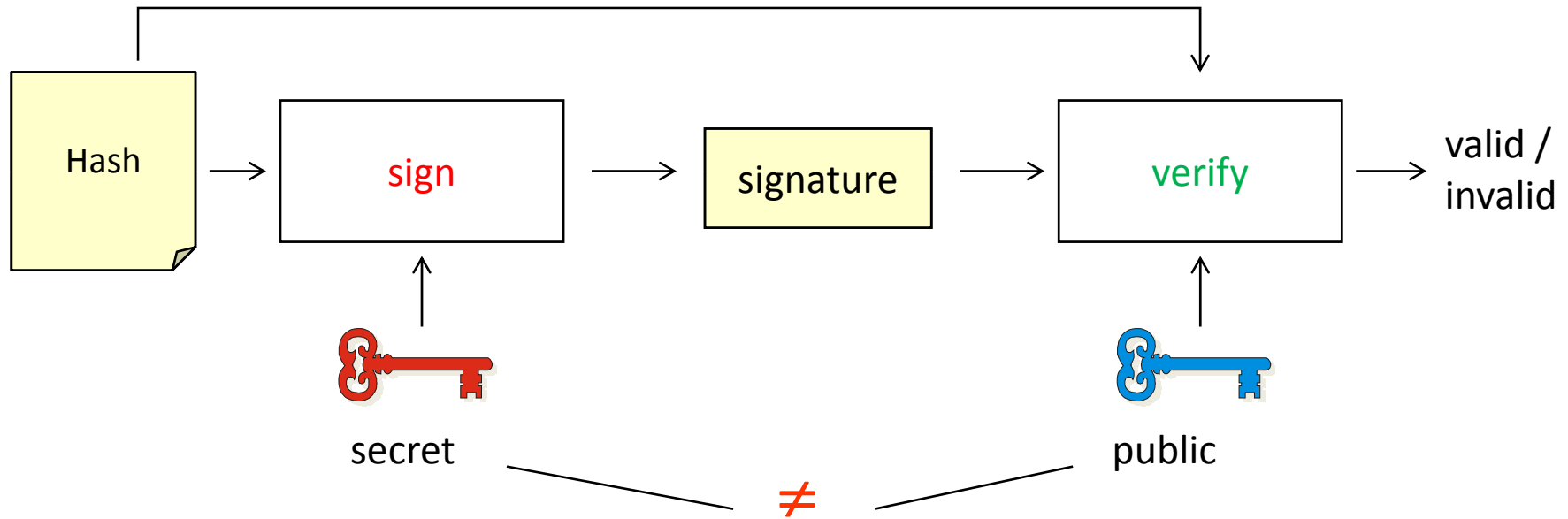
Automatic updates



Software updates for emdedded devices



Digital Signatures guarantee authenticity



Firefox Add-ons :: Mozilla Add-ons :: Add Features to Mozilla Software - Microsoft Internet Explorer

Adresse <https://addons.mozilla.org/>

Firefox Add-ons beta

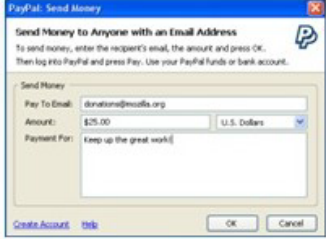
Home Extensions Plugins Search Engines Themes

Extend Firefox Contest Winners Announced

Featured Extension

PayPal Send Money


PayPal's Send Money extension provides a quick way to send money to anyone with an email address. Enter the payment information and you'll be brought to your PayPal login page to sign in and complete the payment. [Learn more...](#)



[Install Extension \(52 KB\)](#)

We Recommend...

See some of our favorite extensions to get you started.



Top Downloads

1	FlashGot	179553
2	NoScript	130738
3	Fasterfox	104878
4	VideoDownloader	92872
5	DownThemAll!	89356

search: Entire Site

Browse by Category

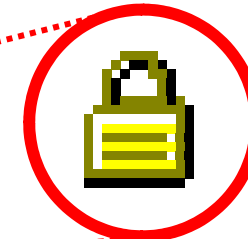
- [Most Popular Add-ons](#)
- [Highest Rated Add-ons](#)
- [Recently Added](#)

Develop Your Own

- [Login to Submit](#)
- [Documentation](#)
- [Develop Your Own](#)

Internet

Website
digitally signed



The screenshot shows a Microsoft Internet Explorer browser window with the title "Windows XP Service Pack 2 and the Internet in a Managed Environment: Windows Update and Automat...". The address bar contains the URL "http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/intngmt/27_xpupd.msp#ENF". The page content includes the Microsoft TechNet logo, a search bar, and a navigation menu. The main article title is "Using Windows XP Professional with Service Pack 2 in a Managed Environment: Controlling Communication with the Internet Windows Update and Automatic Updates", published on August 6, 2004. A sub-section titled "How Windows Update and Automatic Updates Communicate with Sites on the Internet" explains that this subsection summarizes the communication process. A bullet point under "Encryption" states: "Initial data is transferred using HTTPS, and updates are transferred using HTTP. The data packages downloaded to the user's system by Microsoft are digitally signed." A red callout box points to this text.

Windows XP Service Pack 2 and the Internet in a Managed Environment: Windows Update and Automat... - Microsoft Intern...

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten

Adresse http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/intngmt/27_xpupd.msp#ENF Wechseln zu

Quick Links | Home | Worldwide

Microsoft TechNet

Search Microsoft.com for: Go

TechNet Home | TechCenters | Downloads | TechNet Program | My TechNet | Security Bulletins | Archive

Exchange Server
ISA Server
Office
Operations Manager
Small Business Server
SQL Server
Systems Management

[TechNet Home](#) > [Products & Technologies](#) > [Desktop Operating Systems](#) > [Windows XP Professional](#) > [Maintain](#)

Using Windows XP Professional with Service Pack 2 in a Managed Environment: Controlling Communication with the Internet Windows Update and Automatic Updates

Published: August 6, 2004

How Windows Update and Automatic Updates Communicate with Sites on the Internet

This subsection summarizes the communication process.

- Encryption:** Initial data is transferred using HTTPS, and updates are transferred using HTTP. The data packages downloaded to the user's system by Microsoft are digitally signed.

Internet

data packages (...) are digitally signed.

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

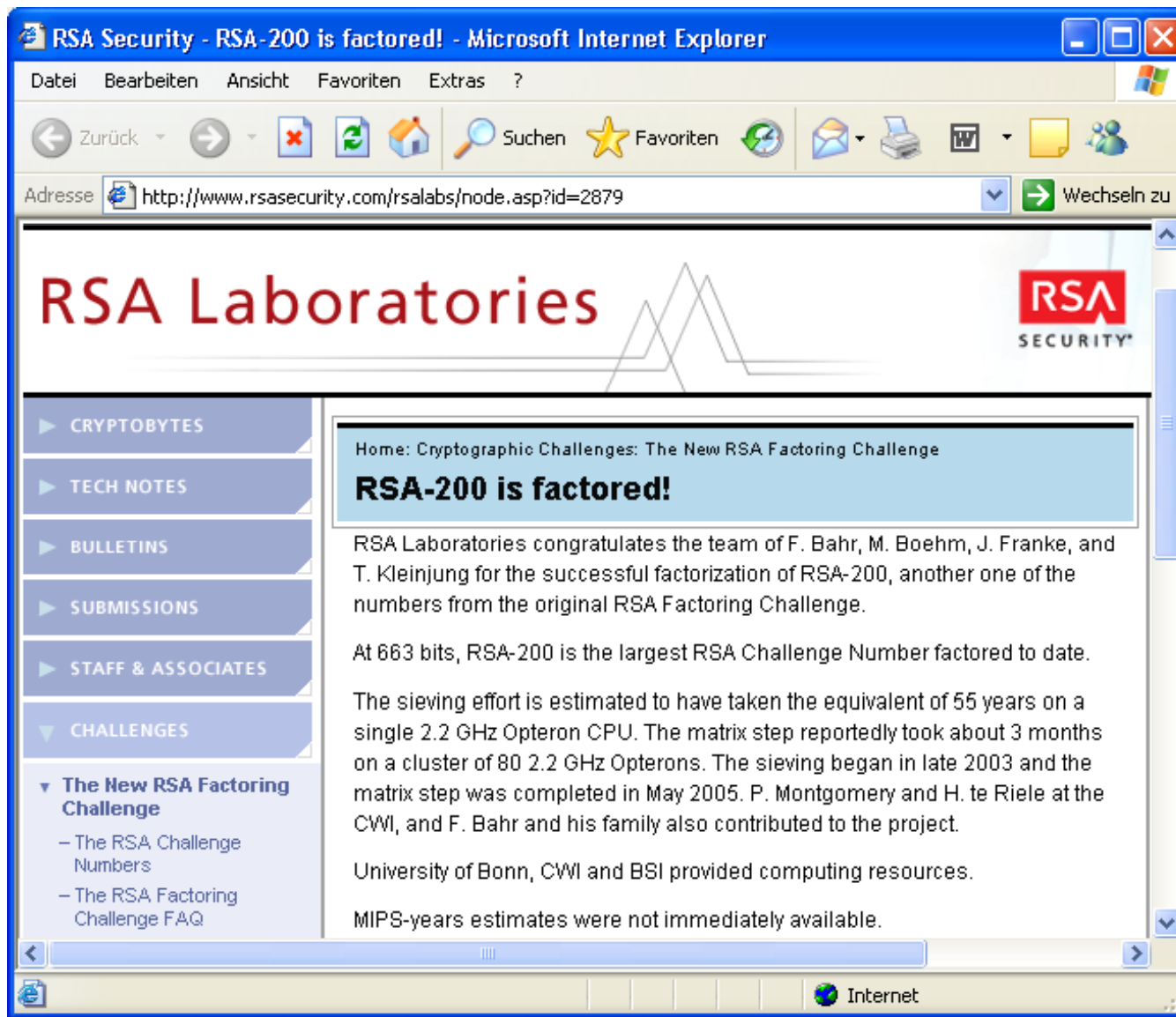
R.L. Rivest, A. Shamir, and L. Adleman*

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

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

Quantum immune signatures?



PQCrypto 2008

University of Cincinnati, USA, October 17-19, 2008

Call for Papers

Important dates

Submission Deadline: June 15, 11pm EST

Notification Deadline: August 1

Final submission: August 12

Early registration: August 15

Conference Date: Oct. 17-19

General Information

Original research papers on all technical aspects of cryptographic research related the future world with large bit quantum computers are solicited. The topics include (but are not restricted to)

- public key cryptosystems that have the potential to resist possible future quantum computers such as: hash-based Merkle-type signature schemes, lattice based cryptosystems, code-based cryptosystems, multivariate cryptosystems and quantum cryptographic schemes;
- classical and quantum attacks including side channel attacks on the post-quantum cryptosystems;

[Home](#)

[Call for papers](#)

[Program](#)

[Accommodations](#)

[Travel Info](#)

[Registration](#)

[Contact](#)

[Support for Young
Researchers](#)

[Social Events](#)

Lattice Based Signatures

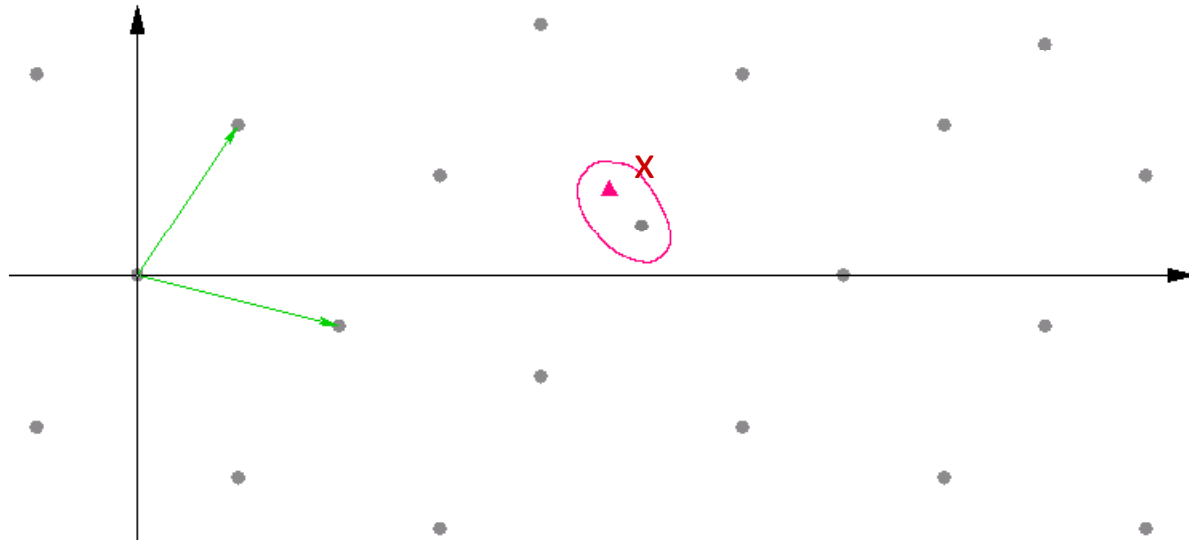
γ -Closest Vector Problem (γ -CVP)

Given:

Lattice $L \subseteq \mathbb{Z}^n$

$\mathbf{x} \in \mathbb{Z}^n$

$\gamma \geq 1$

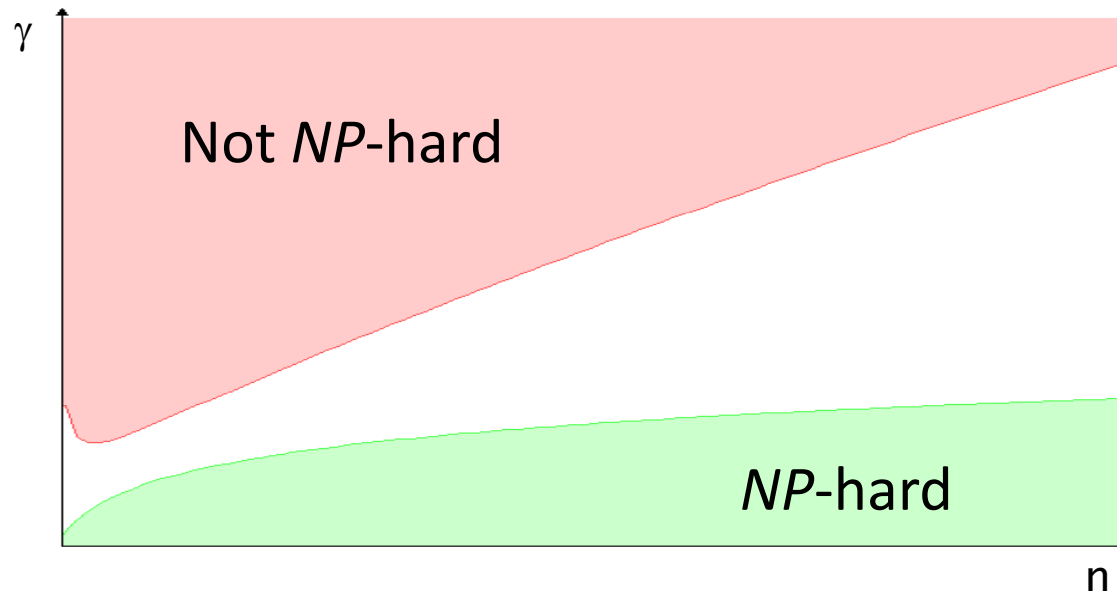


Find: $\mathbf{v} \in L: \|\mathbf{x} - \mathbf{v}\| \leq \gamma \|\mathbf{x} - \mathbf{w}\|$ for all $\mathbf{w} \in L$

Complexity of γ -CVP

Arora et al. (1997):

$\log(n)^c$ -CVP is *NP*-hard for all c



Goldreich, Goldwasser (2000):

$\Omega(n^{1/2} / \log(n))$ -CVP is *not NP*-hard or $coNP \subseteq AM$

Lattice Signatures

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

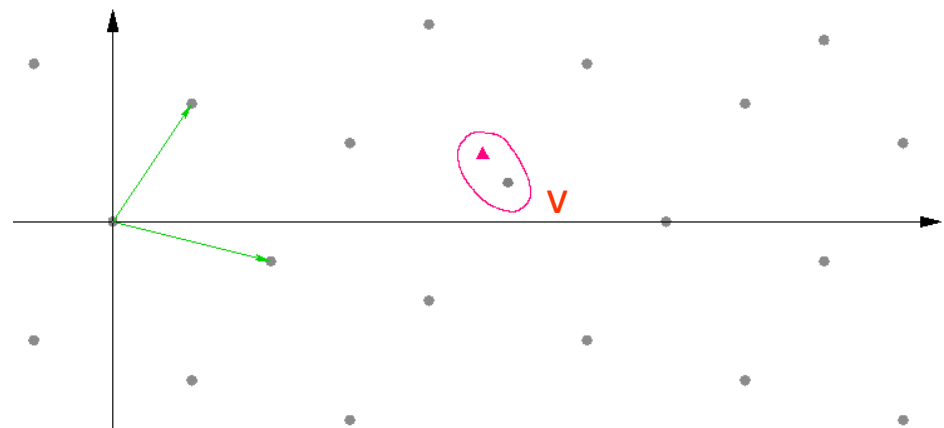
Private Key: Reduced basis of L

Signature:

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

Verification:

1. Check $v \in L$
2. Accept if v close to $h(m)$



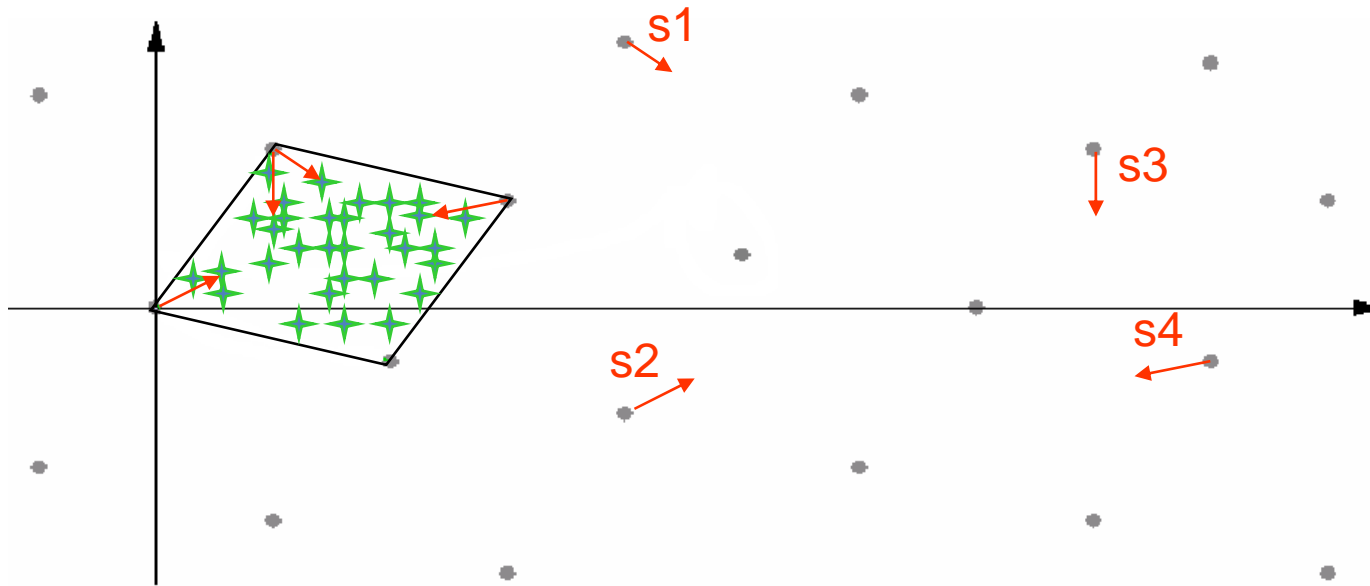
CVP-based Signatures

GGH (Goldwasser, Goldreich, Halevi 1997)

NTRU-Sign (Hoffstein et al. 2003)

Attack (Nguyen, Regev 2006)

Nguyen, Regev 2006 Attack



NTRU-251 broken using ≈ 400 signatures

GGH-400 broken using ≈ 160.000 signatures

Hash tree based signatures

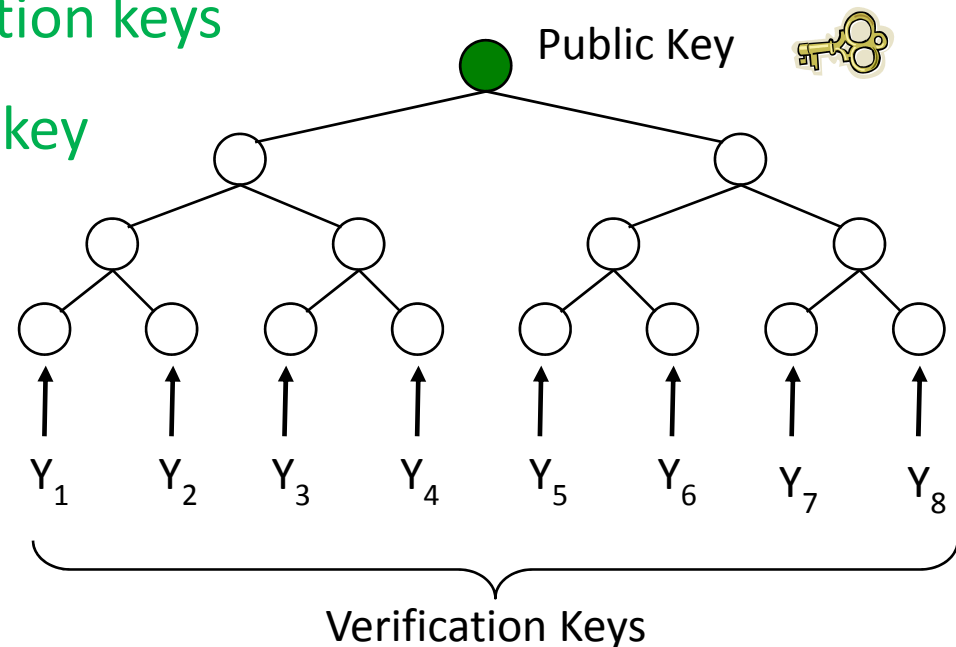
Use one-time signature scheme (OTSS):

One (Signature key, verification key) per signature

Hash tree reduces

validity of many verification keys

to validity of one public key



GMSS (Dahmen, Schneider 2008) based on Winternitz OTS

= 128 bit symmetric security (secure until 2090)

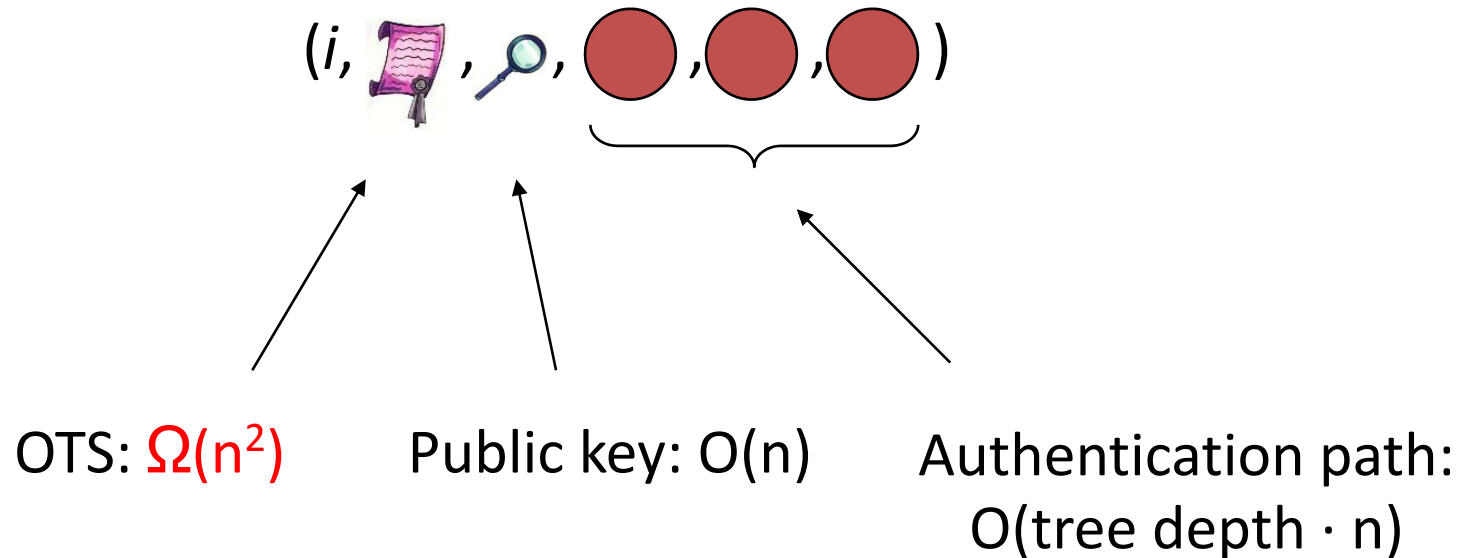


	s	Signature size	Signing	Verifying
RSA	4440 bit	555 bytes	914.1 msec	13.6 msec
ECDSA	256 bit	71 bytes	9.3 msec	23.8 msec
GMSS	256 bit	3936 bytes	77.3 msec	57.8 msec

Timings obtained using FlexiProvider
on a Pentium Dual-Core 1.83GHz (2^{40} Signatures)

Reduce Signature Size !

GMSS signature size of n-bit hashes is $\Omega(n^2)$:



Lyubashevsky Micciancio OTS 2008

$R = \mathbb{Z}[x] / \langle p, f(x) \rangle$, $m = O(\log(n))$, $a_1, \dots, a_m \in R$

$H: (\text{small elements in } R)^m \rightarrow R$

$$\underline{x} = (x_1, \dots, x_m) \mapsto H(\underline{x}) = \sum_{i=1, \dots, m} a_i x_i$$

Micciancio 2002: If there exists a polynomial-time algorithm that finds a collision for a random choice of H then there exists a polynomial time algorithm that approximates $\lambda_1(L)$ within a polynomial factor for every lattice L corresponding to an ideal in $\mathbb{Z}[x] / \langle f \rangle$.

Lyubashevsky Micciancio OTS 2008

$R = \mathbb{Z}[x] / \langle p, f(x) \rangle$, $m = O(\log(n))$, $a_1, \dots, a_m \in R$

$H: (\text{small elements in } R)^m \rightarrow R$

$$\underline{x} = (x_1, \dots, x_m) \mapsto H(\underline{x}) = \sum_{i=1, \dots, m} a_i x_i$$

Signature Key: $\underline{x}, \underline{y} \in R^m$ “very small”

Verification Key: $(H(\underline{x}), H(\underline{y}))$

Signature of $z \in R$ (“very small”): $\underline{s} = \underline{x}z + \underline{y}$

Verification: $H(\underline{s}) \stackrel{?}{=} H(\underline{x})z + H(\underline{y})$

Signature and hash of same size!

Security of LM-OTS

Model: Forger is given H , $H(\underline{x})$, $H(\underline{y})$
obtains signature \underline{s} of z of her choice
forges signature \underline{s}' of z' , $(\underline{s}, z) \neq (\underline{s}', z')$

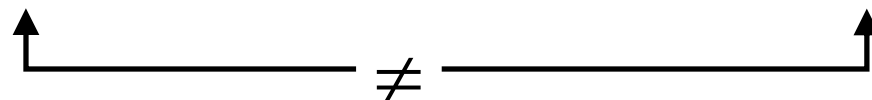
ML 2006: Forging a signature for random H
implies being able to find very short vectors in
ideal lattices

$$L(I) = \{ (a_0, \dots, a_{n-1}) \in \mathbb{Z}^n : \sum_{i=0, \dots, n-1} a_i x^i + \langle f \rangle \in I \}$$

Security of LM-OTS

1. There are many $\underline{x}', \underline{y}'$ with
 $H(\underline{x}) = H(\underline{x}')$, $H(\underline{y}) = H(\underline{y}')$.
2. $(H, H(\underline{x}), H(\underline{y}), \underline{s}, z)$ yields negligible information about $\underline{x}, \underline{y}$.
3. Forger produces signature $\underline{s}' \neq \underline{x}z' + \underline{y}$
4. Collision of H:

$$H(\underline{s}') = H(\underline{x})z' + H(\underline{y}) = H(\underline{x}z' + \underline{y})$$



LM-OTS is not practical

Lyubashevsky and Micciancio present an attack
for $n = 512$

An NTRU-based lattice OTS

Signing Key: $\underline{x}, \underline{y} \in \mathbb{R}^2$ “very small”

Verification Key: $H(\underline{x} \cdot \underline{y}), H(\underline{x} + \underline{y})$

Signature: $\underline{s} = \underline{x} \cdot \underline{y} - z(\underline{x} + \underline{y})$

Verification: $H(\underline{s}) \stackrel{?}{=} H(\underline{x} \cdot \underline{y}) - zH(\underline{x} + \underline{y})$

Signature size = 2 * hash size

Security

Based on SVP in NTRU lattice

Efficiency

Signature \approx 9 times NTRU decryption

Verification \approx 1 time NTRU decryption

$n = 397$

Signature: 4.5 ms

Verification: 0.5 ms

Pentium M 1.6 Ghz, 2GB RAM

γ -Shortest Vector Problem (γ -SVP)

Given:

Lattice $L \subseteq \mathbb{Z}^n$

$\gamma \geq 1$



Find: $v \in L: \|v\| \leq \gamma \|w\|$ for all $w \in L \setminus \{0\}$

Fastest γ -SVP algorithms

Block Korkine-Zolotarev (Schnorr, Euchner 1991)

Recovers secret key in NTRU lattice of dimension 202
2h on AMD Opteron 2,6 GHz (Coppersmith, Shamir 1997)

Primal/Dual Reduction (Koy, Schnorr 2001)

Sampling Reduction (Schnorr 2004; Buchmann, Ludwig 2005)

www.LatticeChallenge.org

The screenshot shows the homepage of the Lattice Challenge website. At the top, there is a header with the text "TU DARMSTADT LATTICE CHALLENGE" and a logo of a woman's head in profile. Below the header, there is a main content area with a large green callout box that reads "Explicit Ajtai Lattices". The callout box is tilted and has a green border. The background of the website is dark with a yellow honeycomb pattern. The main content area contains text about the challenge, including a paragraph about the solution of SVP instances and a list of references. On the right side, there is a sidebar with a "NEWS" section dated "17.3.2008" and a "CHALLENGES" section listing various challenge dimensions.

http://www.latticechallenge.org/

TU DARMSTADT
LATTICE
CHALLENGE

Explicit Ajtai Lattices

the solution of SVP instances.
We think these lattices represent the worst-case for
modern lattice reduction algorithms.

We show how these lattice bases were constructed and give an argument why there
exists a short vector in each of them [2]. We challenge everyone to try by whatever
means to find this short vector.

References

1. Ajtai: Generating Hard Instances of Lattice Problems, STOC '96
2. Buchmann, Lindner, Rückert: Creating a lattice challenge, to appear

HALL OF FAME

Top 5

- 1.
- 2.
- 3.
- 4.
- 5.

First place is awarded to the person/group who first submits a solution to a challenge in a
dimension higher than all that were broken before.

NEWS

17.3.2008
Initial setup

CHALLENGES

Challenges in dimension

225	250	275
300	325	350 375
400	425	450 475

Challenges in dimension

500	525	550	575
600	625	650	675
700	725	750	775
800	825	850	875
900	925	950	975
1000	1025	1050	1075
1100	1125	1150	1175
1200	1225	1250	1275
1300	1325	1350	1375
1400	1425	1450	1475
1500	1525	1550	1575
1600	1625	1650	1675
1700	1725	1750	1775
1800	1825	1850	1875

Random source PI

Thank you