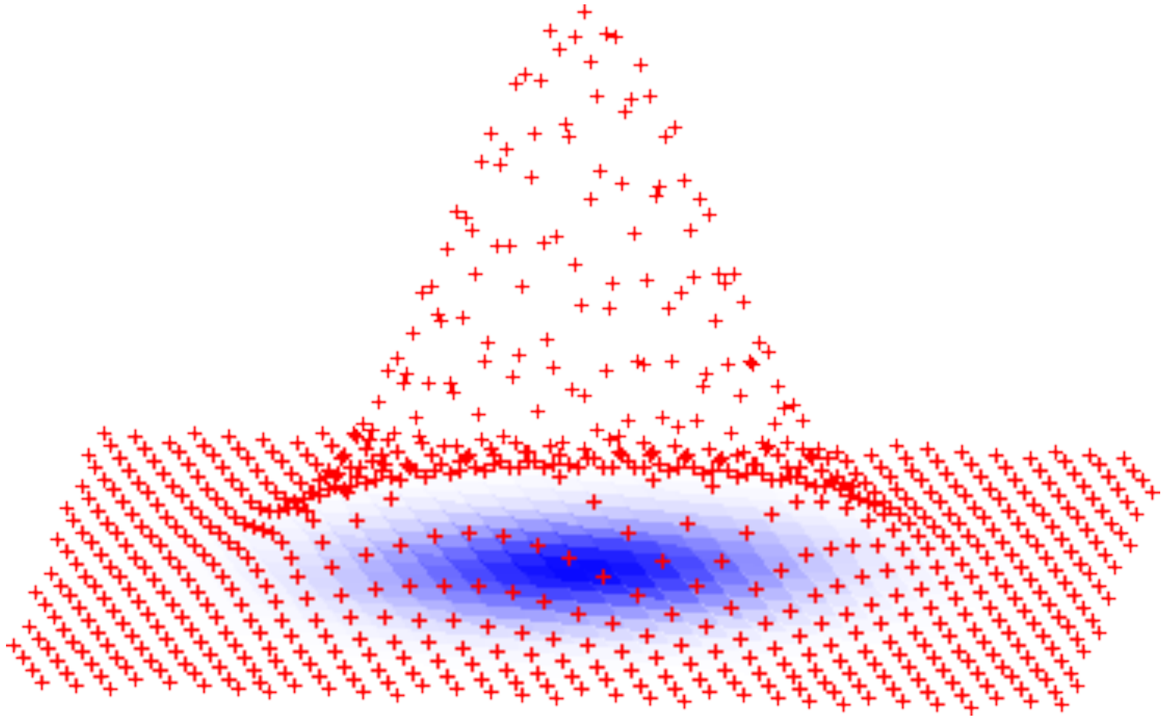
Three Decades of Lattice Cryptography

Chris Peikert
University of Michigan

NSF SaTC PI Meeting
August 2026



The Eras Tour

The Eras Tour

Three decades of **lattice-based cryptography**, each its own era:

The Eras Tour

Three decades of **lattice-based cryptography**, each its own era:

- **Foundations** (’96 – ~’06): a new paradigm, useful substrates

The Eras Tour

Three decades of **lattice-based cryptography**, each its own era:

- **Foundations** (’96 – ~’06): a new paradigm, useful substrates
- **Architecture** (~’06 – ~’16): modular blueprints, rapid expansion

The Eras Tour

Three decades of **lattice-based cryptography**, each its own era:

- **Foundations** (’96 – ~’06): a new paradigm, useful substrates
- **Architecture** (~’06 – ~’16): modular blueprints, rapid expansion
- **Engineering** (~’16 – today): working artifacts, standards, deployments

The Eras Tour

Three decades of **lattice-based cryptography**, each its own era:

- **Foundations** (’96 – ~’06): a new paradigm, useful substrates
- **Architecture** (~’06 – ~’16): modular blueprints, rapid expansion
- **Engineering** (~’16 – today): working artifacts, standards, deployments

This talk: musings on the *scientific/technical*, *epistemic*, and *social* factors underlying its successes.

Prehistory: Public-Key Cryptography

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

A Public-Key Cryptosystem Based On Algebraic Coding Theory

R. J. McEliece
Communications Systems Research Section

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

A Public-Key Cryptosystem Based On Algebraic Coding Theory

R. J. McEliece
Communications Systems Research Section

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-24, NO. 5, SEPTEMBER 1978 525

Hiding Information and Signatures in Trapdoor Knapsacks

RALPH C. MERKLE, STUDENT MEMBER, IEEE AND MARTIN E. HELLMAN, SENIOR MEMBER, IEEE

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

A Public-Key Cryp… Algebraic

Huge keys

(¼—1MB)

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-24, NO. 5, SEPTEMBER 1978

Hiding Information and Signatures in Trapdoor Knapsacks

RALPH C. MERKLE, STUDENT MEMBER, IEEE AND MARTIN E. HELLMAN, SENIOR MEMBER, IEEE

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

A Public-Key Cryp… Algebraic

Huge keys

(¼—1MB)

IEEE TRANSACTIONS ON INFORMATION TH…

Hiding …res in

RALPH C. MERK… …OR MEMBER, IEEE

A POLYNOMIAL TIME ALGORITHM FOR BREAKING THE BASIC MERKLE-HELLMAN CRYPTOSYSTEM

by Adi Shamir

Applied Mathematics
The Weizmann Institute
Rehovot, Israel

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

A Public-Key Cryp… Algebraic

Huge keys

(¼—1MB)

IEEE TRANSACTIONS ON INFO…

Hid… …res in

RALPH C. MERK… …EMBER, IEEE

525

…E ALGORITHM FOR BREAKING …MAN CRYPTOSYSTEM

Solving Low-Density Subset Sum Problems

J. C. LAGARIAS AND A. M. ODLYZKO

AT&T Bell Laboratories, Murray Hill, New Jersey

Appli…

The Weizmann…

Rehovot, Is…

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

A Public-Key Cryp… Algebraic

Huge keys

(¼—1MB)

IEEE TRANSACTIONS ON INFO…

Hid… …s in

RALPH C. M… …EMBER, IEEE

525

…ALGORITHM FOR BREAKING …MAN CRYPTOSYSTEM

Solving Low-Den…

The Rise and Fall of Knapsack Cryptosystems

A. M. Odlyzko

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

The Weizmann… …sey
Rehovot, Is…

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

Prehistory: Public-Key Cryptography

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

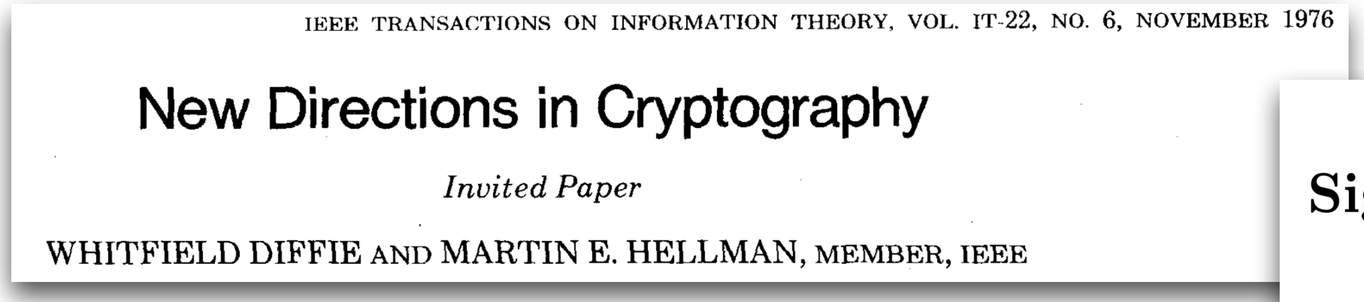
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

Discrete logarithm:

Given $g, g^a \in G$, find a.

Prehistory: Public-Key Cryptography

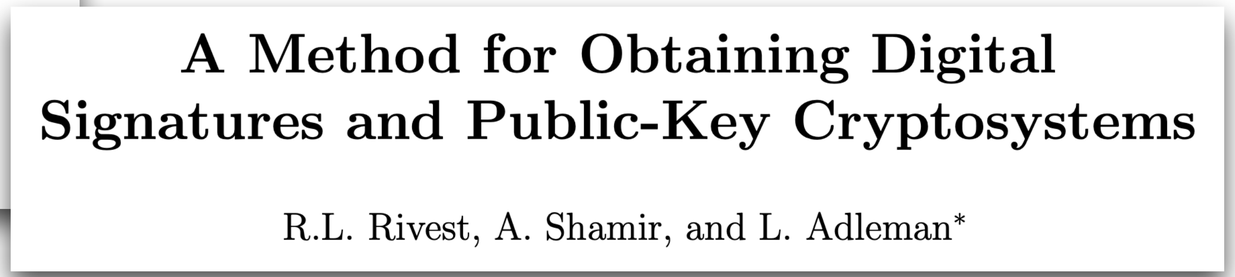


IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE



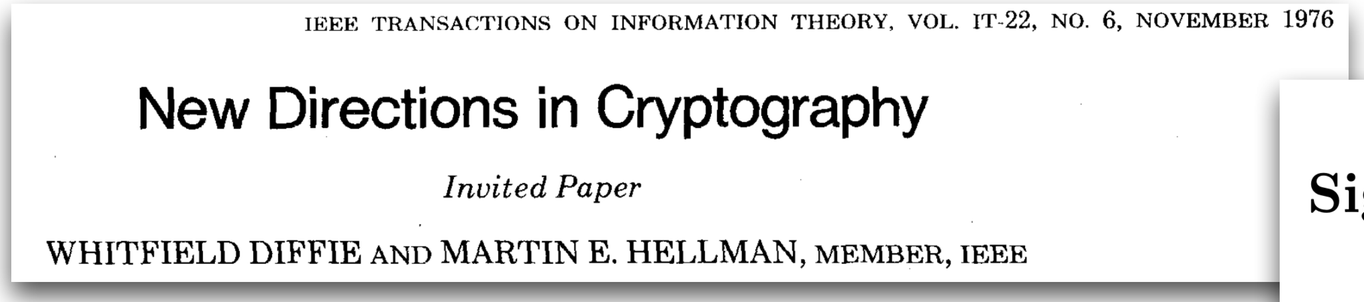
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

Discrete logarithm:
Given $g, g^a \in G$, find a.

Factoring integers:
Given $N = pq$, find p.

Prehistory: Public-Key Cryptography

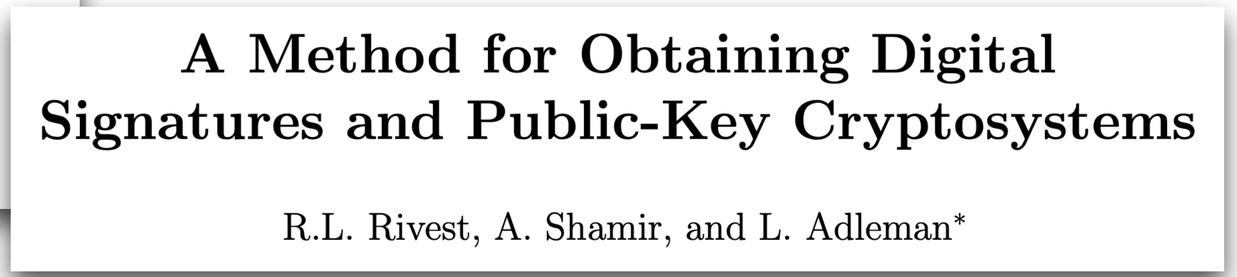


IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE



A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

Discrete logarithm:
Given $g, g^a \in G$, find a.

Factoring integers:
Given $N = pq$, find p.

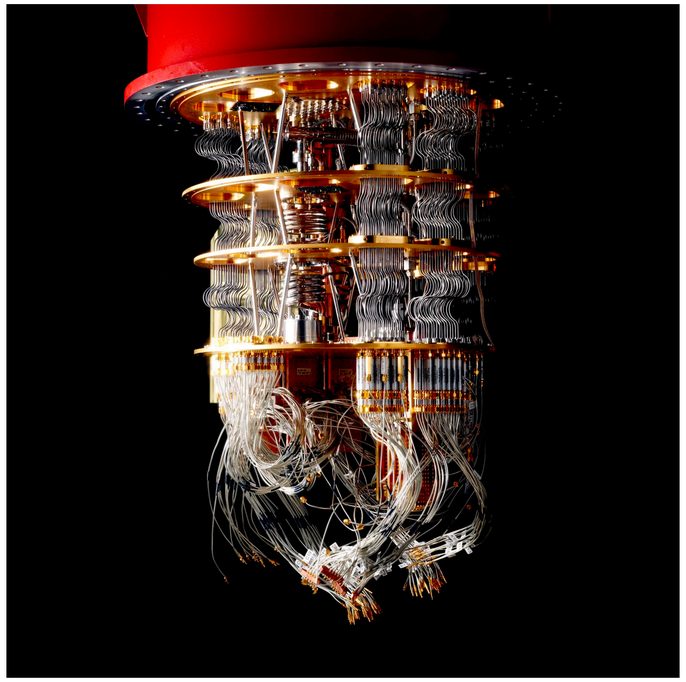
Assumption: for huge enough numbers, these problems are *infeasible* to solve.

Enter |Quantum>

Enter |Quantum>

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†



Enter |Quantum>

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Enter |Quantum>

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

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

Enter |Quantum>

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

IEEE TRANSACTIONS ON INFORMA

New Directions in Cryp

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELL



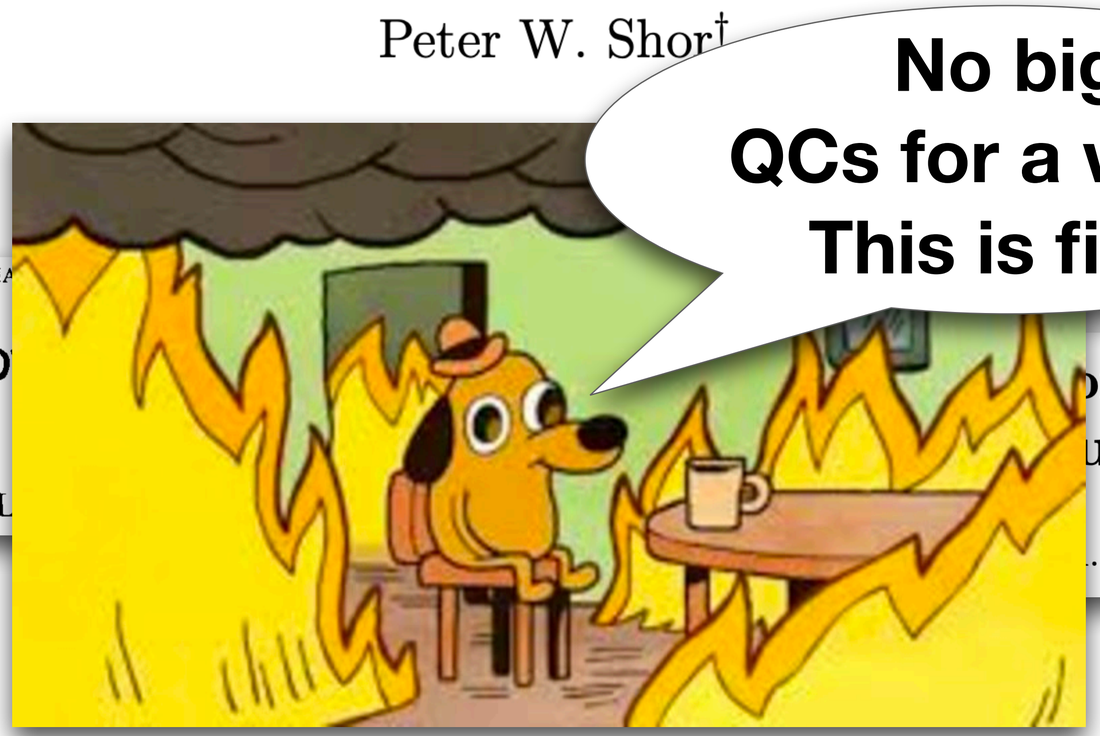
or Obtaining Digital
ublic-Key Cryptosystems

. Shamir, and L. Adleman*

Enter |Quantum>

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†



IEEE TRANSACTIONS ON INFORMA

New Directions in Cryp

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELL

or Obtaining Digital
ublic-Key Cryptosystems

. Shamir, and L. Adleman*

Enter |Quantum>

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

...ter W. Shor†

Store now, break later?!



IEEE TRANSACTIONS ON INFORMATION

New Directions in Cryptog...

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN

...l for Obtaining Digital Public-Key Cryptosystems

...st, A. Shamir, and L. Adleman*

‘Post-Quantum’ Cryptography

‘Post-Quantum’ Cryptography

- **Cryptography that runs on *today’s* (classical) computers, but is believed to be secure against *future* quantum computers.**

‘Post-Quantum’ Cryptography

- **Cryptography that runs on *today’s* (classical) computers, but is believed to be secure against *future* quantum computers.**

- **Late ‘90s/early ‘00s: a somewhat niche research area. (This is when I started on it…)**

‘Post-Quantum’ Cryptography

- **Cryptography that runs on *today’s* (classical) computers, but is believed to be secure against *future* quantum computers.**
- **Late ‘90s/early ‘00s: a somewhat niche research area. (This is when I started on it…)**
- **Today: standardized, deployed, protecting large fractions of Internet traffic**

‘Post-Quantum’ Cryptography

- **Cryptography that runs on *today’s* (classical) computers, but is believed to be secure against *future* quantum computers.**
- **Late ‘90s/early ‘00s: a somewhat niche research area. (This is when I started on it…)**
- **Today: standardized, deployed, protecting large fractions of Internet traffic**
- **But how do we get PQC? *Different math…***

(Point) Lattices

~1770s, 1850s, 1900s

(Point) Lattices

~1770s, 1850s, 1900s







(Point) Lattices

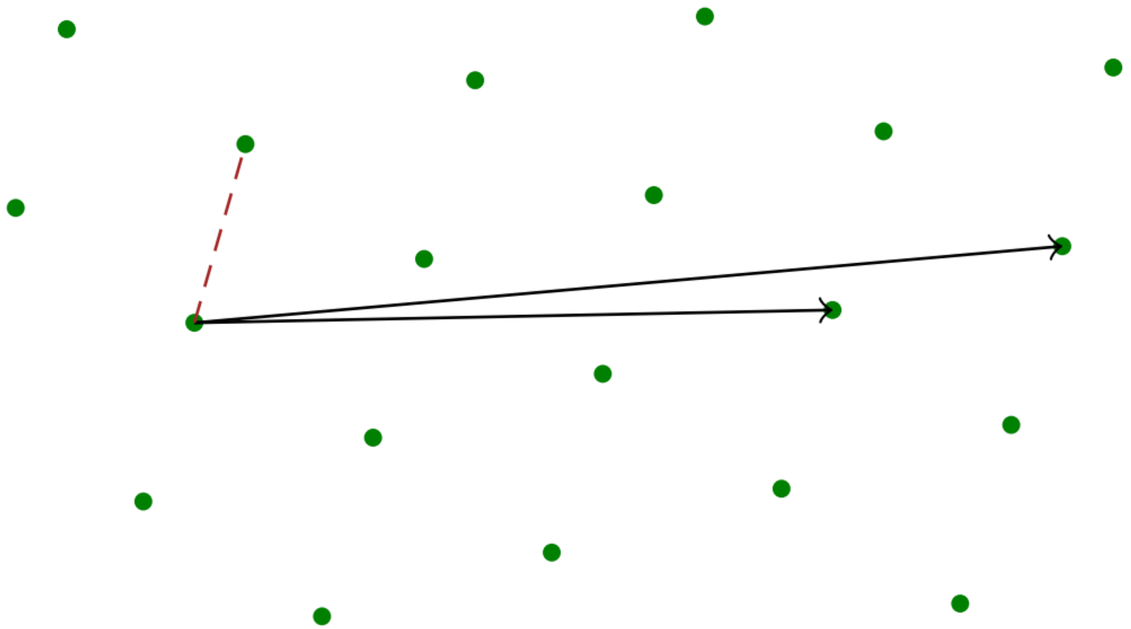
~1770s, 1850s, 1900s







- Lattice: ‘periodic grid’ in $\mathbb{R}^n$.
  Has (non-unique) *basis* of vectors.



(Point) Lattices

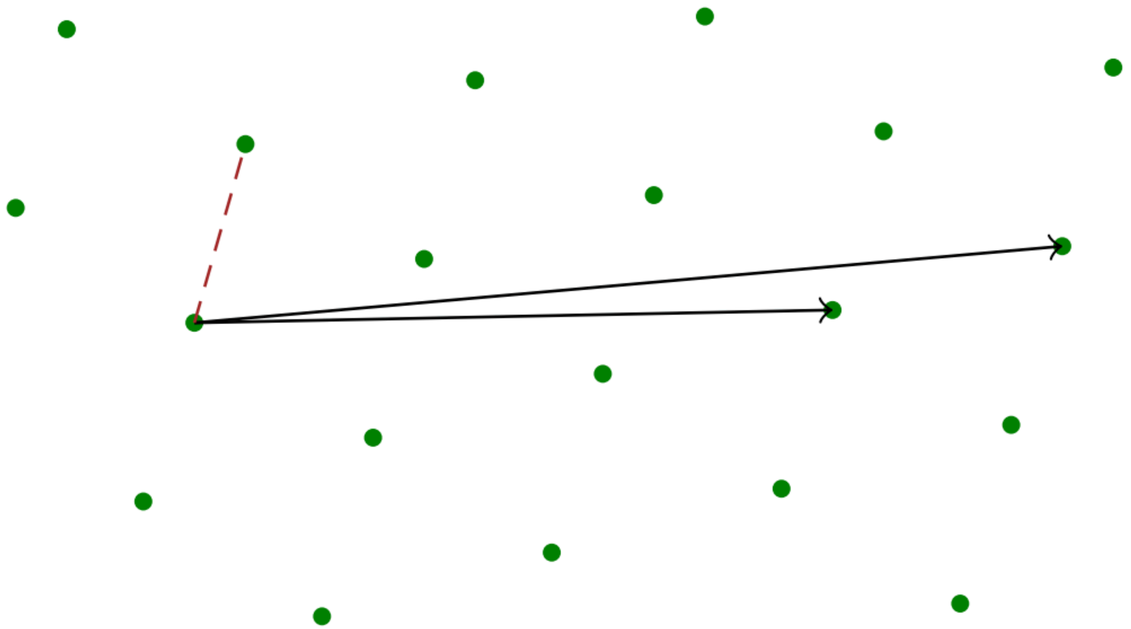
~1770s, 1850s, 1900s





- Lattice: ‘periodic grid’ in $\mathbb{R}^n$.
  Has (non-unique) *basis* of vectors.

- Conjectured hard problems:
  find ‘short’ lattice vectors,
  even *approximately*;
  find ‘closest’ lattice vector to target



(Point) Lattices

~1770s, 1850s, 1900s



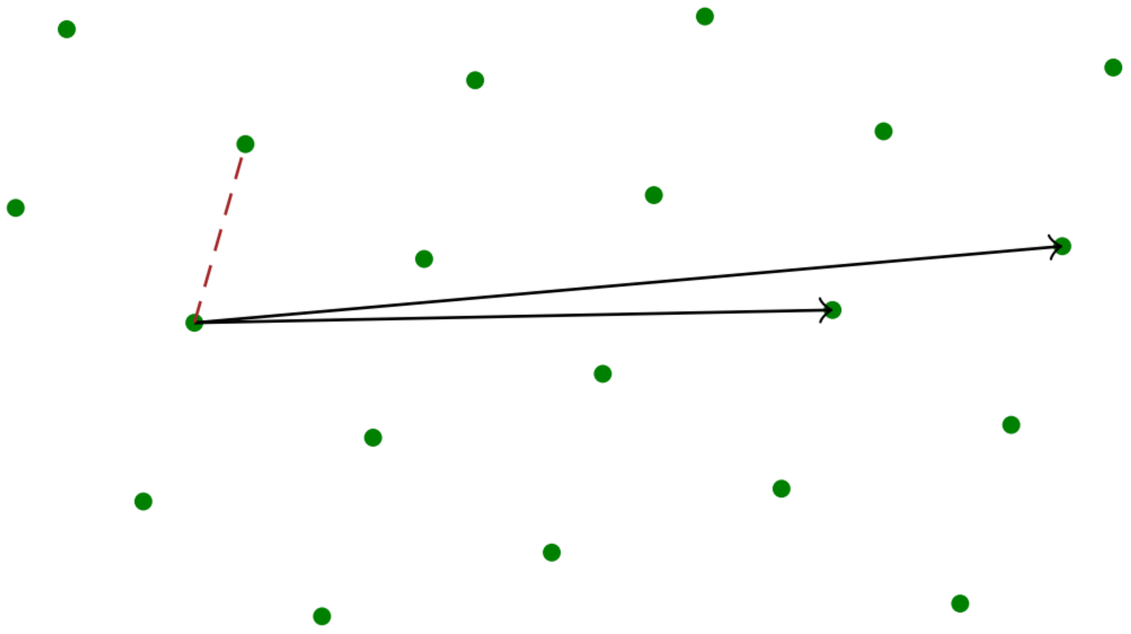




- Lattice: ‘periodic grid’ in $\mathbb{R}^n$.
  Has (non-unique) *basis* of vectors.

- Conjectured hard problems:
  find ‘short’ lattice vectors,
  even *approximately*;
  find ‘closest’ lattice vector to target

- As n grows, these *appear*
  exponentially hard—even for
  quantum!



Foundations Era: ’96–’06

a new paradigm, useful substrates

The Founding (’96)

The Founding (’96)

Generating Hard Instances of Lattice Problems
Extended abstract

M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Founding (’96)

Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

- Theoretically sound: provable *‘worst-case’* hardness

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Founding (’96)

Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

- Theoretically sound: provable *‘worst-case’* hardness
- Inefficient: huge keys, slow

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Founding (’96)

Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

- Theoretically sound: provable *‘worst-case’* hardness
- Inefficient: huge keys, slow
- Minimal functionality (no encryption)

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Founding (’96)

Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

- Theoretically sound: provable *‘worst-case’* hardness
- Inefficient: huge keys, slow

A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence

Miklós Ajtai * Cynthia Dwork *

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Founding (’96)

Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

- Theoretically sound: provable *‘worst-case’* hardness
- Inefficient: huge keys, slow

A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence

Miklós Ajtai * Cynthia Dwork *

- Fast encryption on *polynomial rings*

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Founding (’96)

Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

- Theoretically sound: provable *‘worst-case’* hardness
- Inefficient: huge keys, slow

A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence

Miklós Ajtai * Cynthia Dwork *

- Fast encryption on *polynomial rings*
- Heuristic security (lacks proofs)

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Founding (’96)

Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

- Theoretically sound: provable *‘worst-case’* hardness
- Inefficient: huge keys, slow

A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence

Miklós Ajtai * Cynthia Dwork *

- Fast encryption on *polynomial rings*
- Heuristic security (lacks proofs)
- Unexpected attacks were found

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Gaussian Revolution (’04—)

Generating Hard Instances of Lattice Problems
Extended abstract
M. Ajtai
IBM Almaden Research Center
650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence

Miklós Ajtai * Cynthia Dwork *

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Gaussian Revolution ('04—)

Generating Hard Instances of Lattice Problems

Worst-case to Average-case Reductions based on Gaussian Measures*

Daniele Micciancio † Oded Regev ‡

650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

A Public-Key Cryptosystem with
Worst-Case/Average-Case Equivalence

Miklós Ajtai * Cynthia Dwork *

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Gaussian Revolution ('04—)

Generating Hard Instances of Lattice Problems

Worst-case to Average-case Reductions based on Gaussian Measures*

Daniele Micciancio † Oded Regev ‡

650 Harry Road, San Jose, CA, 95120

e-mail: ajtai@almaden.ibm.com

On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Oded Regev *

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Gaussian Revolution ('04—)

Generating Hard Instances of Lattice Problems

Worst-case to Average-case Reductions based on Gaussian Meas

Daniele Micciancio † Oded Regev ‡

650 Harry Road, San Jose, CA, 95120
e-mail: ajtai@almaden.ibm.com

Generalized compact knapsacks, cyclic lattices, and efficient one-way functions*

Daniele Micciancio

On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Oded Regev *

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Gaussian Revolution ('04—)

Generating Hard Instances of Lattice Problems

Worst-case to Average-case Reductions based on Gaussian Meas

Daniele Micciancio † Oded Regev ‡

650 Harry Road, San Jose, CA, 95120

e-mail: ajtai@almaden.ibm.com

Generalized compact knapsacks, cyclic lattices, and efficient one-way functions*

Daniele Micciancio

Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices*

Chris Peikert† Alon Rosen‡

December 8, 2005

Generalized Compact Knapsacks are Collision Resistant *

Vadim Lyubashevsky Daniele Micciancio

On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Oded Regev *

NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

The Gaussian Revolution ('04—)

Generating Hard Instances of Lattice Problems

Worst-case to Average-case Reductions based on Gaussian Meas

Daniele Micciancio † Oded Regev ‡

650 Harry Road, San Jose, CA, 95120

e-mail: ajtai@almaden.ibm.com

Generalized compact knapsacks, cyclic lattices, and efficient one-way functions*

Daniele Micciancio

Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices*

Chris Peikert† Alon Rosen‡

December 8, 2005

Generalized Compact Knapsacks are Collision Resistant *

Vadim Lyubashevsky Daniele Micciancio

On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Oded Regev *

NT **em**

On Ideal Lattices and Learning with Errors Over Rings*

Vadim Lyubashevsky† Chris Peikert‡ Oded Regev§

Why ‘Re-Proving’ Seeded a Revolution

Why ‘Re-Proving’ Seeded a Revolution

- **Technical:** gave powerful, elegant Gaussian machinery that would later *migrate from hardness proofs to crypto constructions themselves*

Why ‘Re-Proving’ Seeded a Revolution

- **Technical:** gave powerful, elegant Gaussian machinery that would later *migrate from hardness proofs to crypto constructions themselves*
- **Conceptual:** *exported simple, accessible problems* (SIS/LWE) that constructions and attacks can use as a *common, modular substrate*

Why ‘Re-Proving’ Seeded a Revolution

- **Technical:** gave powerful, elegant Gaussian machinery that would later *migrate from hardness proofs to crypto constructions themselves*
- **Conceptual:** *exported simple, accessible problems* (SIS/LWE) that constructions and attacks can use as a *common, modular substrate*
- **Epistemic:** made results *easier to verify, understand, and trust*; systematically *explained and removed “sharp corners”*

Why ‘Re-Proving’ Seeded a Revolution

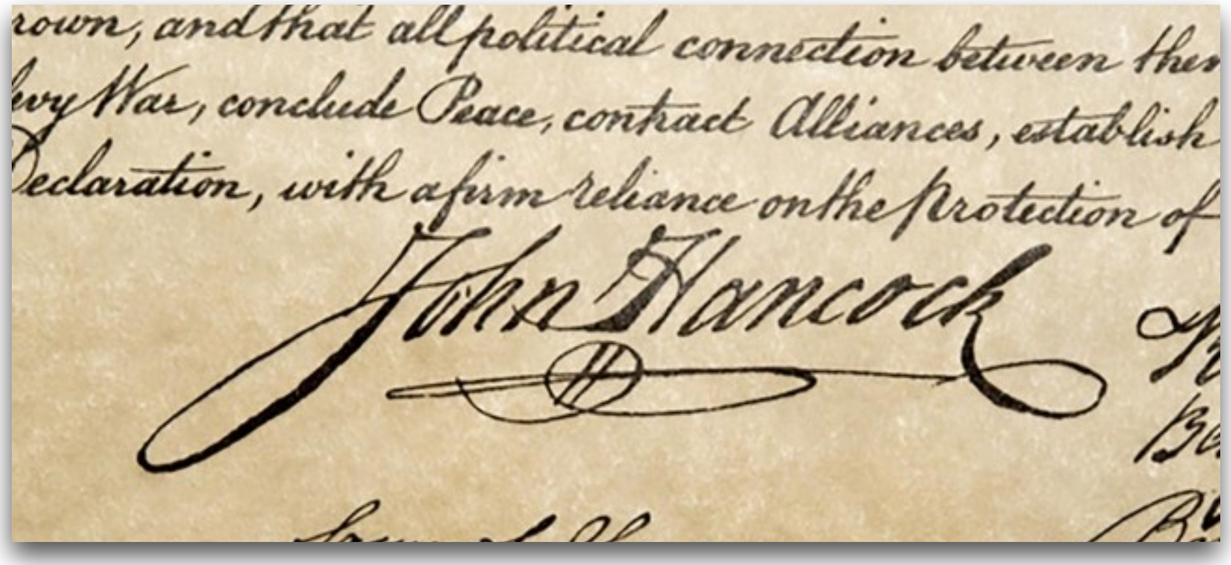
- **Technical:** gave powerful, elegant Gaussian machinery that would later *migrate from hardness proofs to crypto constructions themselves*
- **Conceptual:** *exported simple, accessible problems* (SIS/LWE) that constructions and attacks can use as a *common, modular substrate*
- **Epistemic:** made results *easier to verify, understand, and trust*; systematically *explained and removed “sharp corners”*
- **Social:** *lowered barriers to entry* for new researchers, *sparked joy*

Late Foundations Era: Digital Signatures

User signs w/ secret key; anyone can verify w/ public key

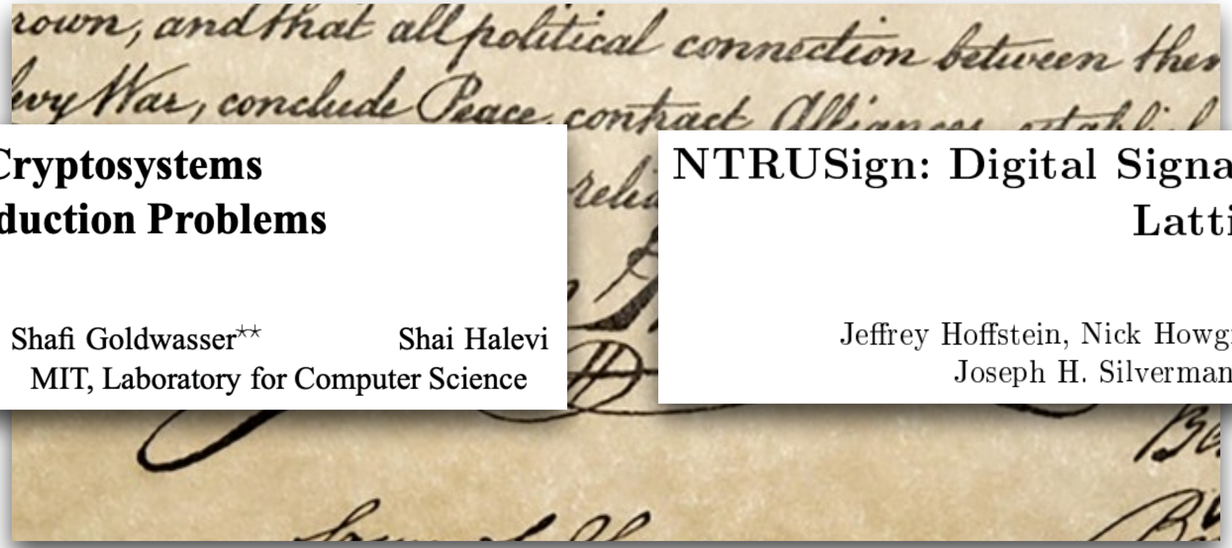
Late Foundations Era: Digital Signatures

User signs w/ secret key; anyone can verify w/ public key



Late Foundations Era: Digital Signatures

User signs w/ secret key; anyone can verify w/ public key



Public-Key Cryptosystems from Lattice Reduction Problems

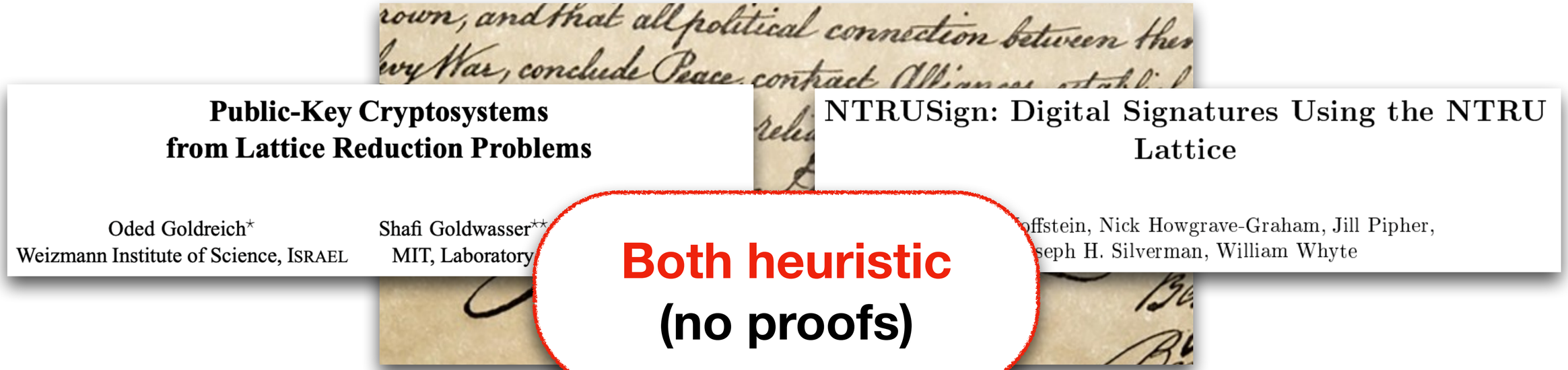
Oded Goldreich* Shafi Goldwasser** Shai Halevi
Weizmann Institute of Science, ISRAEL MIT, Laboratory for Computer Science

NTRUSign: Digital Signatures Using the NTRU Lattice

Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher,
Joseph H. Silverman, William Whyte

Late Foundations Era: Digital Signatures

User signs w/ secret key; anyone can verify w/ public key



Public-Key Cryptosystems from Lattice Reduction Problems

Oded Goldreich*
Weizmann Institute of Science, ISRAEL

Shafi Goldwasser**
MIT, Laboratory

NTRUSign: Digital Signatures Using the NTRU Lattice

offstein, Nick Howgrave-Graham, Jill Pipher,
seph H. Silverman, William Whyte

Both heuristic
(no proofs)

Late Foundations Era: Digital Signatures

User signs w/ secret key; anyone can verify w/ public key



Public-Key Cryptosystems from Lattice Reduction Problems

Oded Goldreich*
Weizmann Institute of Science,

NTRUSign: Digital Signatures Using the NTRU Lattice

ham, Jill Pipher,
Whyte

Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures

Phong Q. Nguyen*[1] and Oded Regev**[2]

Late Foundations Era: Digital Signatures

User signs w/ secret key; anyone can verify w/ public key



Public-Key Cryptosystems from Lattice Reduction Problems

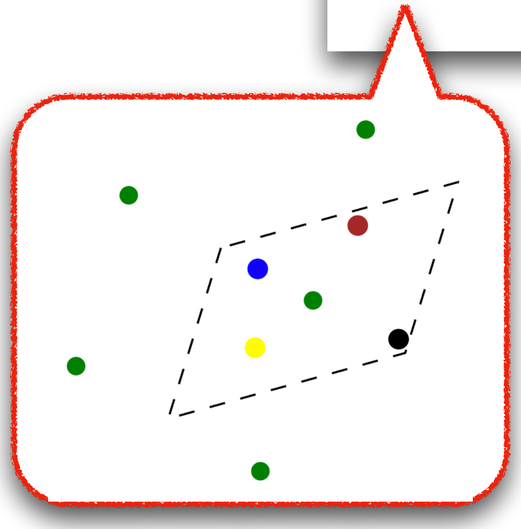
Oded Goldreich*
Weizmann Institute of Science,

NTRUSign: Digital Signatures Using the NTRU Lattice

...am, Jill Pipher,
Whyte

Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures

Phong Q. Nguyen*[1] and Oded Regev**[2]



Signatures leak the secret signing key

Late Foundations Era: Digital Signatures

User signs w/ secret key; anyone can verify w/ public key



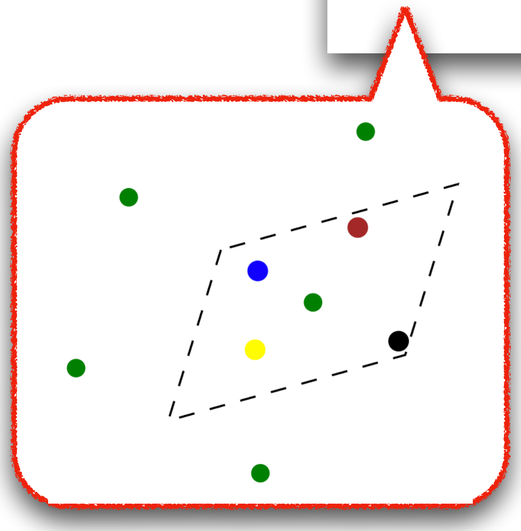
Public-Key Cryptosystems from Lattice Reduction Problems

Oded Goldreich*
Weizmann Institute of Science,

NTRUSign: Digital Signatures Using the NTRU Lattice

ham, Jill Pipher,
Whyte

Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures

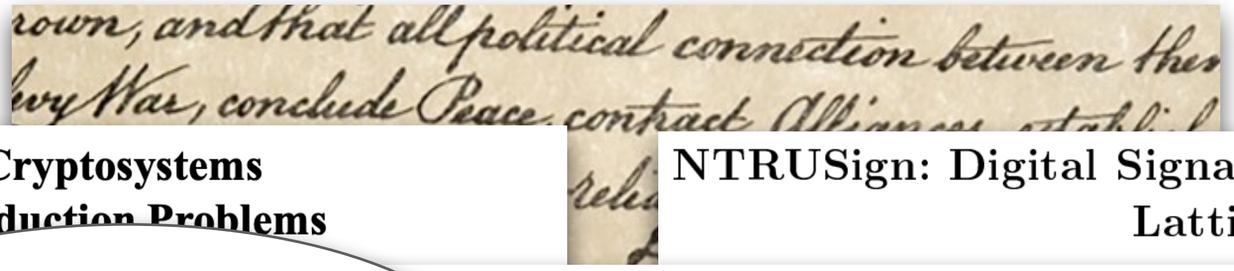




Signatures leak the secret signing key

Late Foundations Era: Digital Signatures

User signs w/ secret key; anyone can verify w/ public key



Public-Key Cryptosystems from Lattice Reduction Problems

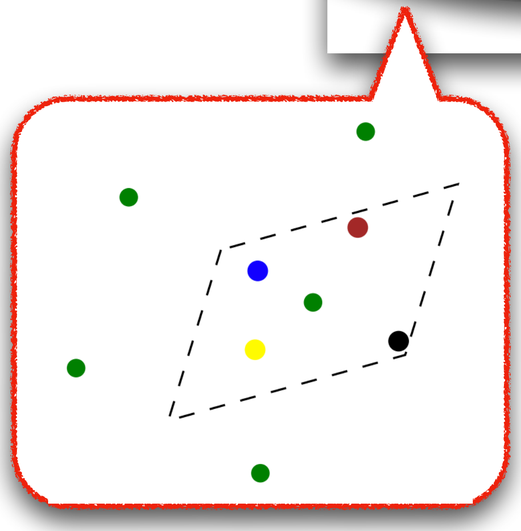
Oded Goldr
Weizmann Institute of

NTRUSign: Digital Signatures Using the NTRU Lattice

ham, Jill Pipher,
Whyte

a Parallelepiped:
GH and NTRU Signatures

We need ~~water~~ foundations!!





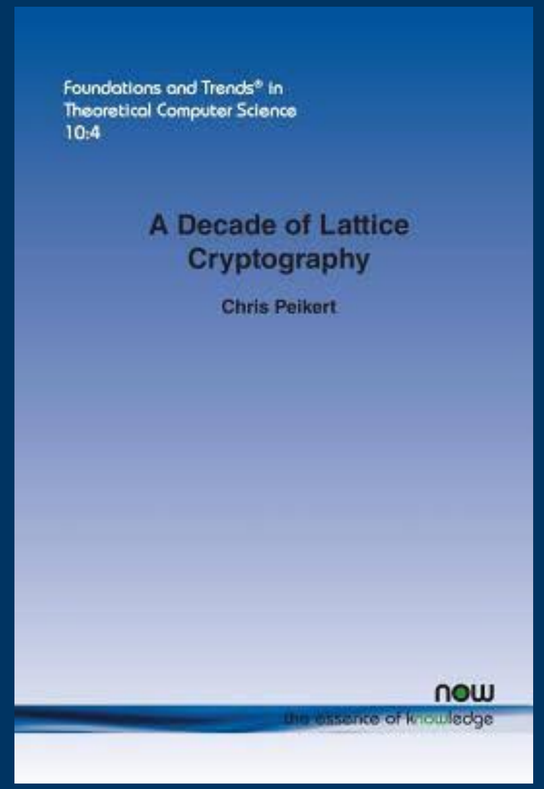
Signatures leak the secret signing key

Architecture Era: ’06–’16

rapid expansion, modular blueprints

Architecture Era: ’06–’16

rapid expansion, modular blueprints



Activities of the Architecture Era

Activities of the Architecture Era

- *Explosion of constructions and capabilities*, overwhelmingly based on the *shared substrates* (SIS, LWE, Gaussian analysis)
  - public-key encryption (w/active security), trapdoor functions, oblivious transfer/MPC, digital signatures, (constrained) pseudorandom functions, (hierarchical) identity-based encryption, attribute-based encryption, fully homomorphic encryption/signatures, …

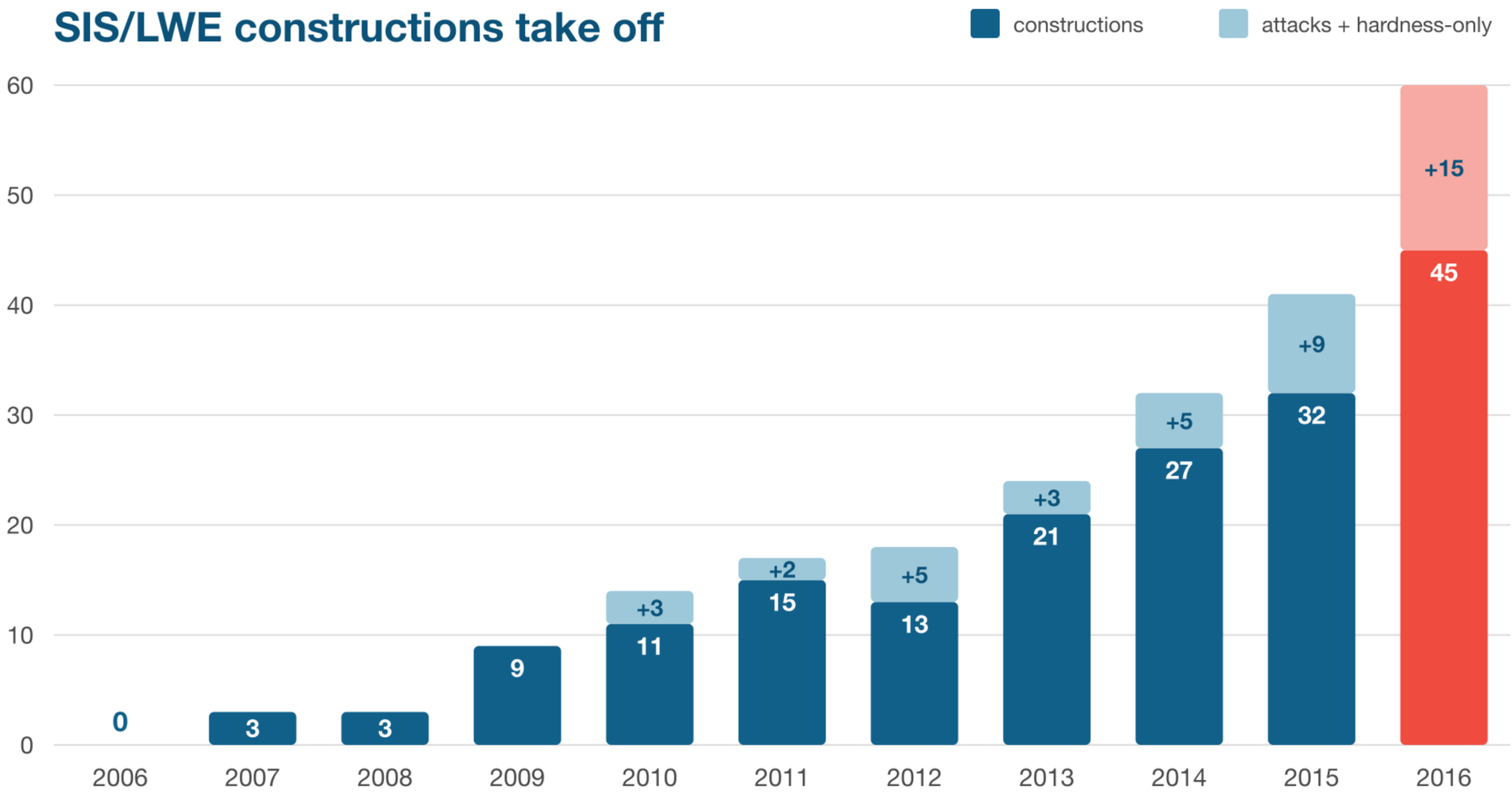
Activities of the Architecture Era

- *Explosion of constructions and capabilities*, overwhelmingly based on the *shared substrates* (SIS, LWE, Gaussian analysis)
  - public-key encryption (w/active security), trapdoor functions, oblivious transfer/MPC, digital signatures, (constrained) pseudorandom functions, (hierarchical) identity-based encryption, attribute-based encryption, fully homomorphic encryption/signatures, …
- *New, modular components*: trapdoors, discrete Gaussian samplers, protocols “with aborts”, gadget decompositions, rounding

Activities of the Architecture Era

- *Explosion of constructions and capabilities*, overwhelmingly based on the *shared substrates* (SIS, LWE, Gaussian analysis)
  - public-key encryption (w/active security), trapdoor functions, oblivious transfer/MPC, digital signatures, (constrained) pseudorandom functions, (hierarchical) identity-based encryption, attribute-based encryption, fully homomorphic encryption/signatures, …
- *New, modular components*: trapdoors, discrete Gaussian samplers, protocols “with aborts”, gadget decompositions, rounding
- Optimization and stabilization of *concrete cryptanalysis*

Architecture, Quantified



Conservative metadata census; distinct papers; ePrint year. See accompanying data and methodology.

Sound Lattice-Based Signatures

Sound Lattice-Based Signatures

How to Use a Short Basis:
Trapdoors for Hard Lattices and
New Cryptographic Constructions

Craig Gentry*
Stanford University
cgentry@cs.stanford.edu

Chris Peikert†
SRI International
cpeikert@alum.mit.edu

Vinod Vaikuntanathan‡
MIT
vinodv@mit.edu

Sound Lattice-Based Signatures

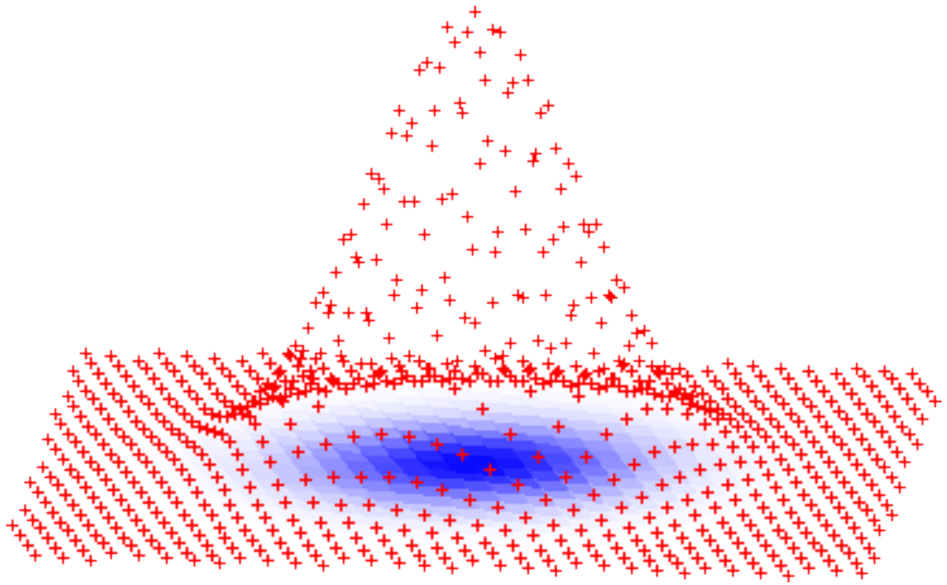
- Gave a *discrete Gaussian* sampler, & used it in *cryptosystem design*

How to Use a Short Basis:
Trapdoors for Hard Lattices and
New Cryptographic Constructions

Craig Gentry*
Stanford University
cgentry@cs.stanford.edu

Chris Peikert†
SRI International
cpeikert@alum.mit.edu

Vinod Vaikuntanathan‡
MIT
vinodv@mit.edu



Sound Lattice-Based Signatures

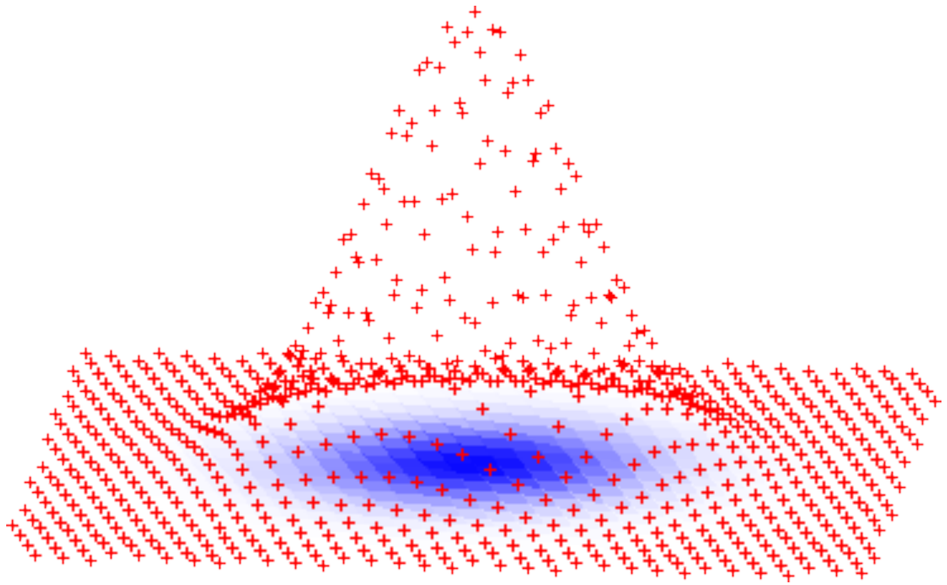
- Gave a *discrete Gaussian* sampler, & used it in *cryptosystem design*
- Key fact: DGS reveals nothing about the short basis; can be 'simulated'.
  ⇒ provably sound signatures

How to Use a Short Basis:
Trapdoors for Hard Lattices and
New Cryptographic Constructions

Craig Gentry*
Stanford University
cgentry@cs.stanford.edu

Chris Peikert†
SRI International
cpeikert@alum.mit.edu

Vinod Vaikuntanathan‡
MIT
vinodv@mit.edu



Sound Lattice-Based Signatures

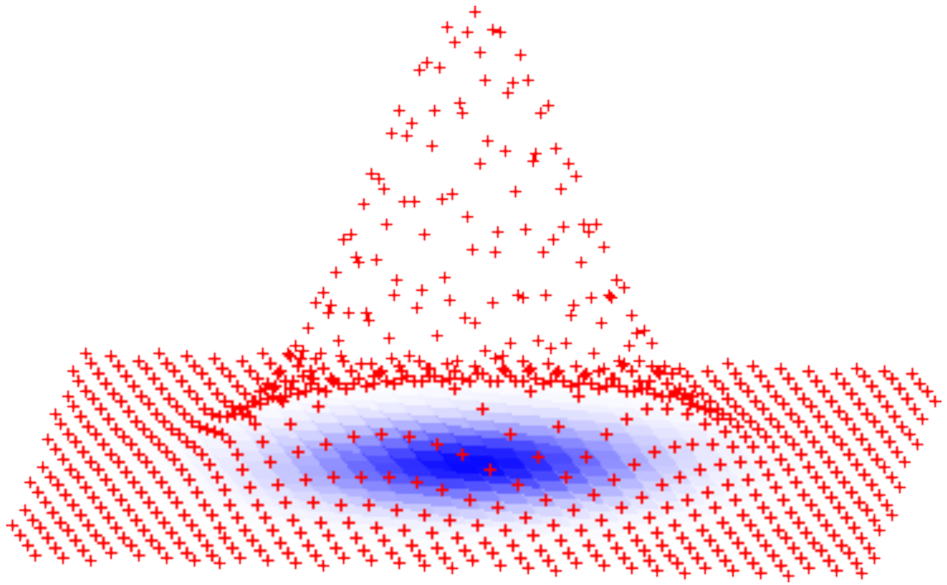
- Gave a *discrete Gaussian* sampler, & used it in *cryptosystem design*
- Key fact: DGS reveals nothing about the short basis; can be 'simulated'.
  ⇒ provably sound signatures
- Bonus: identity-based encryption & much more advanced functionality

How to Use a Short Basis:
Trapdoors for Hard Lattices and
New Cryptographic Constructions

Craig Gentry*
Stanford University
cgentry@cs.stanford.edu

Chris Peikert†
SRI International
cpeikert@alum.mit.edu

Vinod Vaikuntanathan‡
MIT
vinodv@mit.edu



Encrypted Computing

Encrypted Computing

- [RAD’78]: is computation on encrypted data possible?

  If so: no need to trust your cloud provider!

ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Ronald L. Rivest
Len Adleman
Michael L. Dertouzos

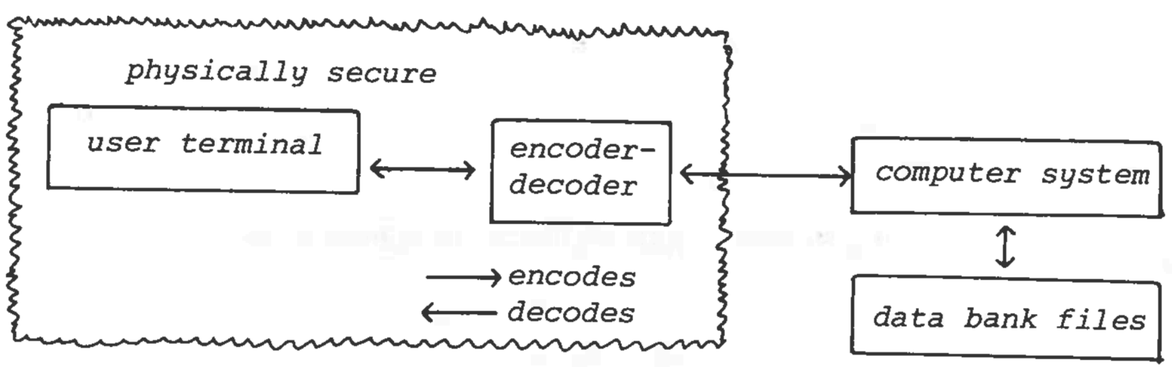
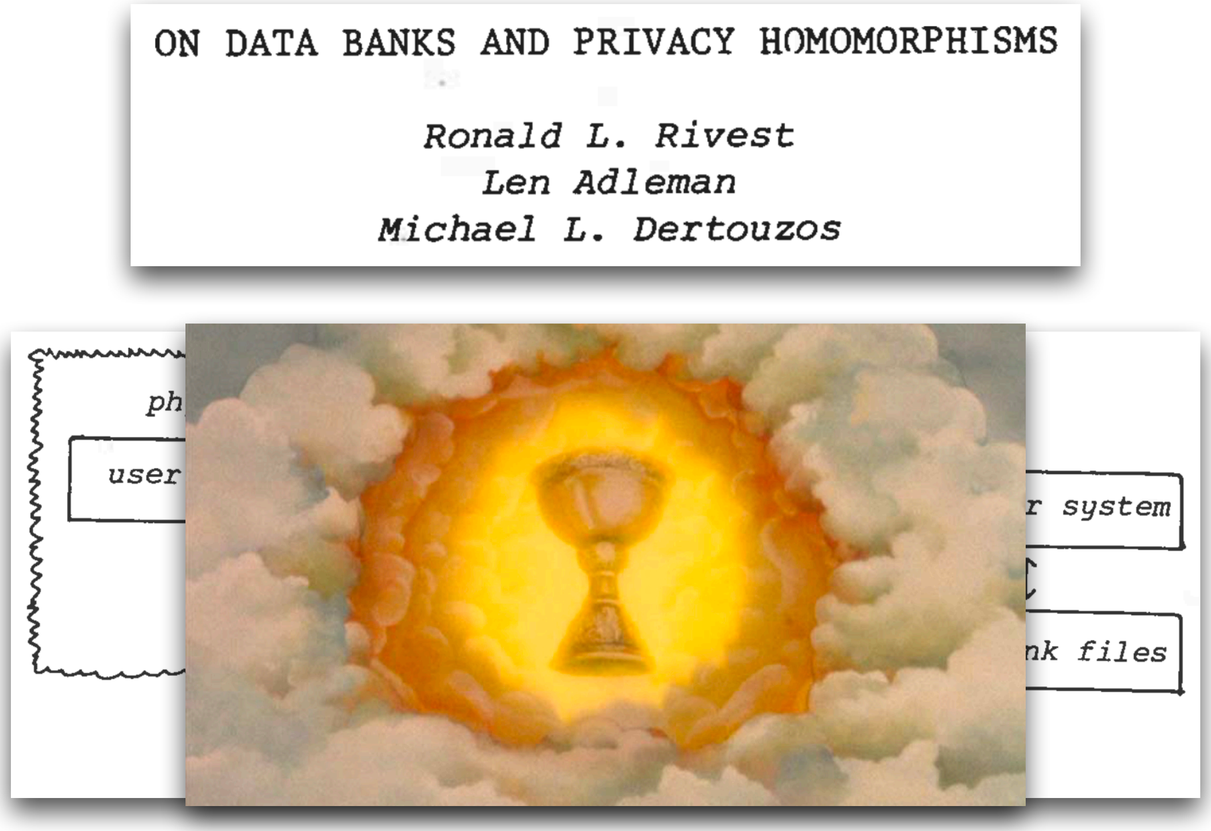


Figure 1

Encrypted Computing

- [RAD’78]: is computation on encrypted data possible?

  If so: no need to trust your cloud provider!



Encrypted Computing

- [RAD'78]: is computation on encrypted data possible?

  If so: no need to trust your cloud provider!

- [Gentry'09]: first plausible candidate! (Heuristic security, extremely inefficient.)

ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Ronald L. Rivest
Len Adleman
Michael L. Dertouzos



Fully Homomorphic Encryption Using Ideal Lattices

Craig Gentry
Stanford University and IBM Watson
cgentry@cs.stanford.edu

Encrypted Computing

- [RAD'78]: is computation on encrypted data possible?

  If so: no need to trust your cloud provider!

- [Gentry'09]: first plausible candidate! (Heuristic security, extremely inefficient.)

- Explosion of interest & improvements, mostly based on algebraic lattices.

ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Ronald L. Rivest
Len Adleman
Michael L. Dertouzos



Fully Homomorphic Encryption Using Ideal Lattices

Craig Gentry
Stanford University and IBM Watson
cgentry@cs.stanford.edu

Architecture → Artifacts

BLEEDING-EDGE PROTOTYPES (representative sample)

2008

SWIFFT / SWIFFTX

lattice hashing
at SIMD speed

2013

HElib

FHE as an “assembly language”

2013

BLISS

practical signatures
and Gaussian sampling

2014

SPRING

a lattice PRF in
software + hardware

2014

FHEW

bootstrapping:
minutes → ½ second

EXPERIMENTAL REAL-WORLD DEPLOYMENTS

strongSwan

2014–16

NTRU key exchange · BLISS signatures
then NewHope in an established VPN stack

OpenSSL / TLS

2015

Ring-LWE key exchange in a real TLS stack
measuring speed, bandwidth, compatibility

Chrome CECPQ1

2016

NewHope + X25519 on live Google traffic:
an Internet-scale experiment

Engineering Era: ’16–today

implementations, standards, deployments

Engineering Adds New Questions

Engineering Adds New Questions

- What are the precise security margins and failure probabilities?

Engineering Adds New Questions

- What are the precise security margins and failure probabilities?
- How to get constant-time and side-channel-resistant implementations?

Engineering Adds New Questions

- What are the precise security margins and failure probabilities?
- How to get constant-time and side-channel-resistant implementations?
- Can keys, ciphertexts, and signatures fit into real protocols?

Engineering Adds New Questions

- What are the precise security margins and failure probabilities?
- How to get constant-time and side-channel-resistant implementations?
- Can keys, ciphertexts, and signatures fit into real protocols?
- How to migrate safely and be crypto-agile?

NIST PQC: A Public Engineering and Stress Test

2016–17	2019	2020	2022	2024
69	26	15	4	3
CALL FOR PROPOSALS **first-round candidates** plurality lattice/LWE-based many approaches to **structure · parameters** **errors · rounding**	**ADVANCE** to Round 2	**ADVANCE** to Round 3	**INITIAL SELECTIONS** **3 are lattice-based**	**FIPS STANDARDS** **first 3 finalized**

Artifacts, Standards, Deployments

- **ML-KEM (Kyber)** — FIPS 203: algebraic (module-)LWE key establishment
- **ML-DSA (Dilithium)** — FIPS 204: module-lattice signatures “with aborts”
- **FN-DSA (Falcon)** — FIPS 206 draft: NTRU lattices + Gaussian sampling
- **FrodoKEM**: a conservative *unstructured*-LWE option endorsed by other orgs.
- Wide-scale deployments: **TLS** Chrome/Safari ↔ Cloudflare/AWS/Akamai/etc., **Signal** PQXDH, Apple **iMessage** PQ3, more.
- Apple **PIR** (“lightweight FHE”): private caller ID, spam detection, URL filter
- Cloudflare/Google target *full* internal PQC migration by **2029**.

Beyond NIST PQC: All Eras, All at Once

Beyond NIST PQC: All Eras, All at Once

- PQC is being deployed in other demanding applications (e.g., blockchains)

Beyond NIST PQC: All Eras, All at Once

- PQC is being deployed in other demanding applications (e.g., blockchains)
- Foundations/architecture/engineering of FHE, zero knowledge, and succinct proofs continue to improve

Beyond NIST PQC: All Eras, All at Once

- PQC is being deployed in other demanding applications (e.g., blockchains)
- Foundations/architecture/engineering of FHE, zero knowledge, and succinct proofs continue to improve
- Cryptanalysis continues to inform parameters and security margins

Beyond NIST PQC: All Eras, All at Once

- PQC is being deployed in other demanding applications (e.g., blockchains)
- Foundations/architecture/engineering of FHE, zero knowledge, and succinct proofs continue to improve
- Cryptanalysis continues to inform parameters and security margins
- Foundational work continues beneath all this
  (e.g., fine-grained/NP hardness, using new hard problems for crypto)

AI Era: ’26—

attacks, formalization, acceleration

This Slide Is Probably Already Obsolete

What a Week 😮‍💨

This Slide Is Probably Already Obsolete

What a Week 😮‍💨

- **July 28:** Claude Mythos *~halves the security strength of HAWK*, a NIST “on-ramp” proposal based on a newer kind of lattice problem
  - Driven by a non-expert, knocked down a chain of human-set dominoes

This Slide Is Probably Already Obsolete

What a Week 😮‍💨

- **July 28:** Claude Mythos *~halves the security strength of HAWK*, a NIST “on-ramp” proposal based on a newer kind of lattice problem
  - Driven by a non-expert, knocked down a chain of human-set dominoes
- **Aug 1:** OpenAI announces *10 Math/TCS breakthroughs* by Astra model
  - NP-hardness of CVP for polynomial approx factors: “out of the blue” shock

This Slide Is Probably Already Obsolete

What a Week 😮‍💨

- **July 28:** Claude Mythos *~halves the security strength of HAWK*, a NIST “on-ramp” proposal based on a newer kind of lattice problem
  - Driven by a non-expert, knocked down a chain of human-set dominoes
- **Aug 1:** OpenAI announces *10 Math/TCS breakthroughs* by Astra model
  - NP-hardness of CVP for polynomial approx factors: “out of the blue” shock
- **Aug 3-6:** 3x GPT-5.6-assisted, *exponentially faster* ***worst-case*** *SVP algorithm*

This Slide Is Probably Already Obsolete

What a Week 😮‍💨

- **July 28:** Claude Mythos *~halves the security strength of HAWK*, a NIST "on-ramp" proposal based on a newer kind of lattice problem
  - Driven by a non-expert, knocked down a chain of human-set dominoes
- **Aug 1:** OpenAI announces *10 Math/TCS breakthroughs* by Astra model
  - NP-hardness of CVP for polynomial approx factors: "out of the blue" shock
- **Aug 3-6:** 3x GPT-5.6-assisted, *exponentially faster* ***worst-case*** *SVP algorithm*
- **Aug 6:** Whatever appeared on ePrint/arXiv during this talk…

High-Velocity Era

High-Velocity Era

- *AI can rapidly produce* constructions, proofs, implementations, and attacks

High-Velocity Era

- *AI can rapidly produce* constructions, proofs, implementations, and attacks
- **Cryptanalysis** has historically received *much less attention* than construction

High-Velocity Era

- *AI can rapidly produce* constructions, proofs, implementations, and attacks
- **Cryptanalysis** has historically received *much less attention* than construction
  - There is *abundant low-hanging fruit* out there!

High-Velocity Era

- *AI can rapidly produce* constructions, proofs, implementations, and attacks
- **Cryptanalysis** has historically received *much less attention* than construction
  - There is *abundant low-hanging fruit* out there!
- Weak ideas may *fail faster*; strong ideas may *earn confidence faster*

High-Velocity Era

- *AI can rapidly produce* constructions, proofs, implementations, and attacks
- **Cryptanalysis** has historically received *much less attention* than construction
  - There is *abundant low-hanging fruit* out there!
- Weak ideas may *fail faster*; strong ideas may *earn confidence faster*
- **The most unique, scarce resource has shifted: from generation, to your *understanding, evaluation, and judgment***