NewHope, Frodo, in Between and Beyond

Instantiating and Implementing Lattice based Cryptography

Léo Ducas

CWI, Amsterdam, The Netherlands
Supported by an Public-Private Partnership grant from CWI, with NXP

October 3rd, Quantum-Safe Crypto Workshop, QTC@NUS, Singapoure

Outline

Outline

Lattice Based Crypto

Theory:

- Strong asymptotic security guarantees
- Resistant to known quantum attack
- Very versatile (e.g. Fully Homomorphic Encryption)

Lattice Based Crypto

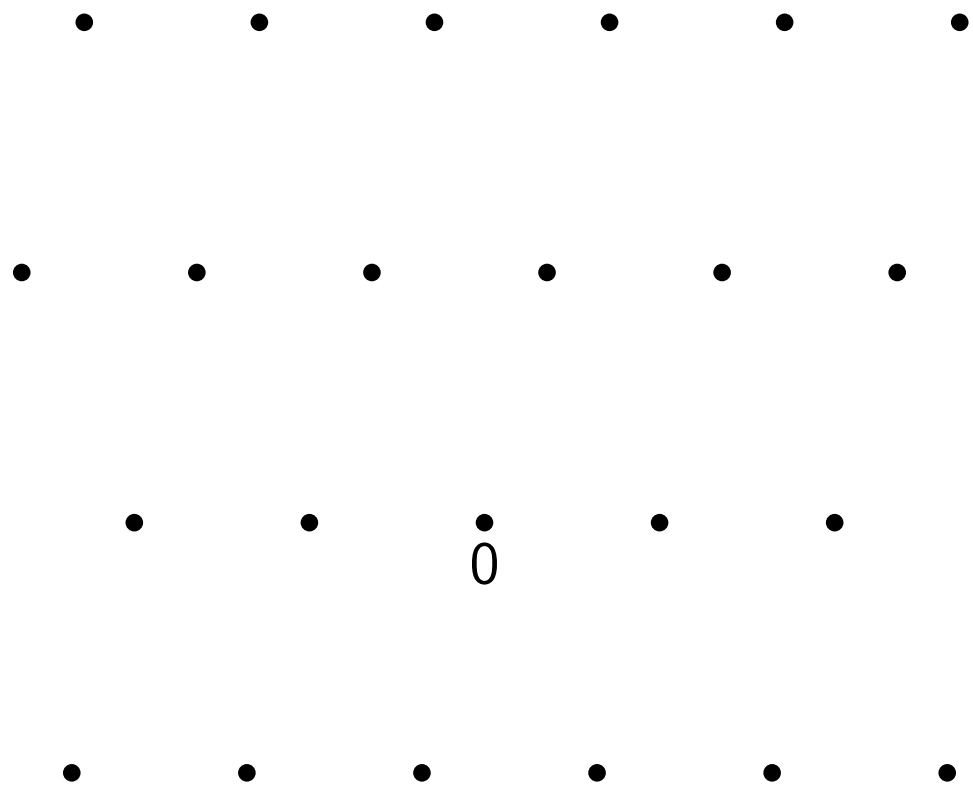
Theory:

- Strong asymptotic security guarantees
- Resistant to known quantum attack
- Very versatile (e.g. Fully Homomorphic Encryption)

Practice/Deployment:

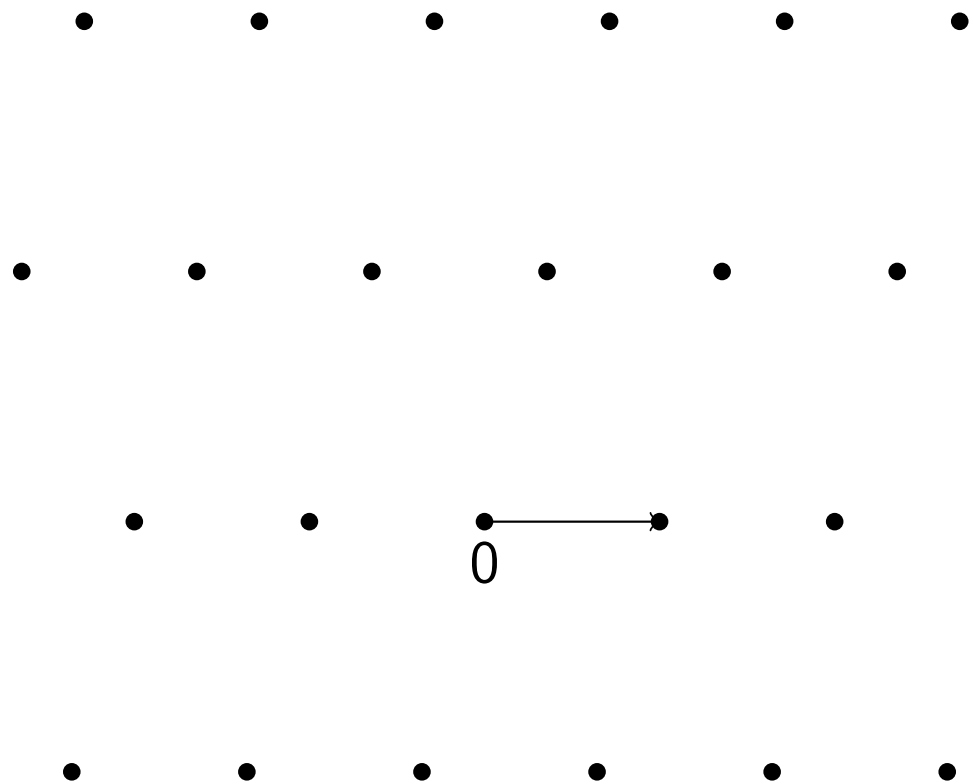
- NSA, NIST, CGS, recommend initiating transition to Post-Quantum crypto by 2020.
- Lattice based Crypto is (one of ?) the best candidate
- Far from ready for the real world

Lattices and hard problems



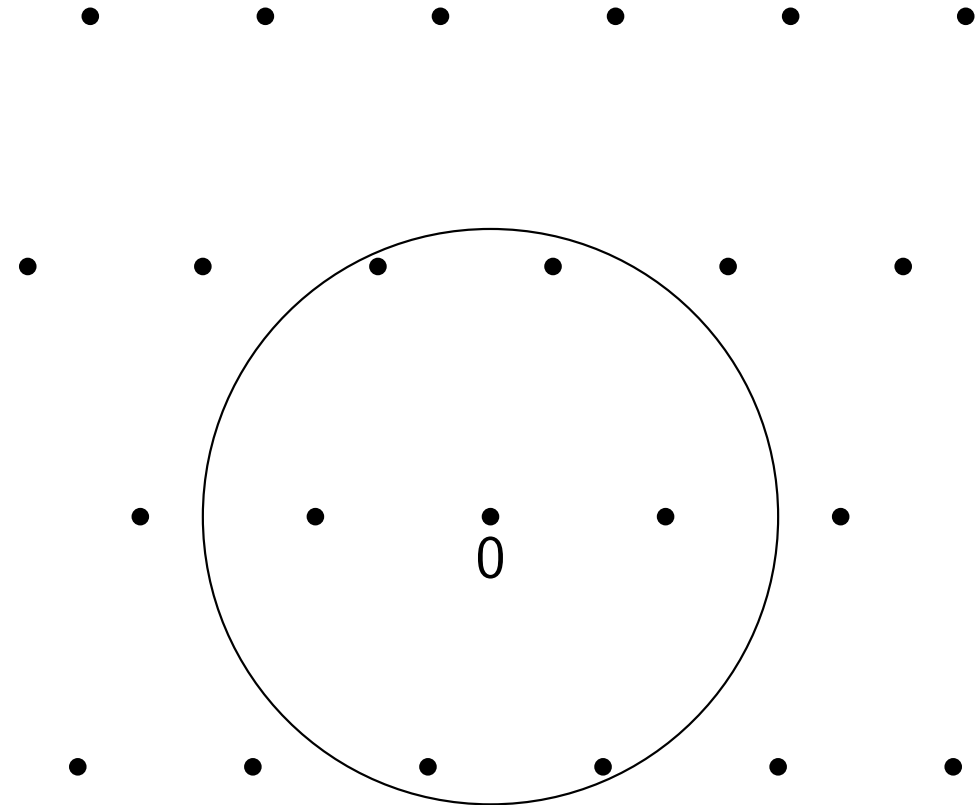
A lattice

Lattices and hard problems



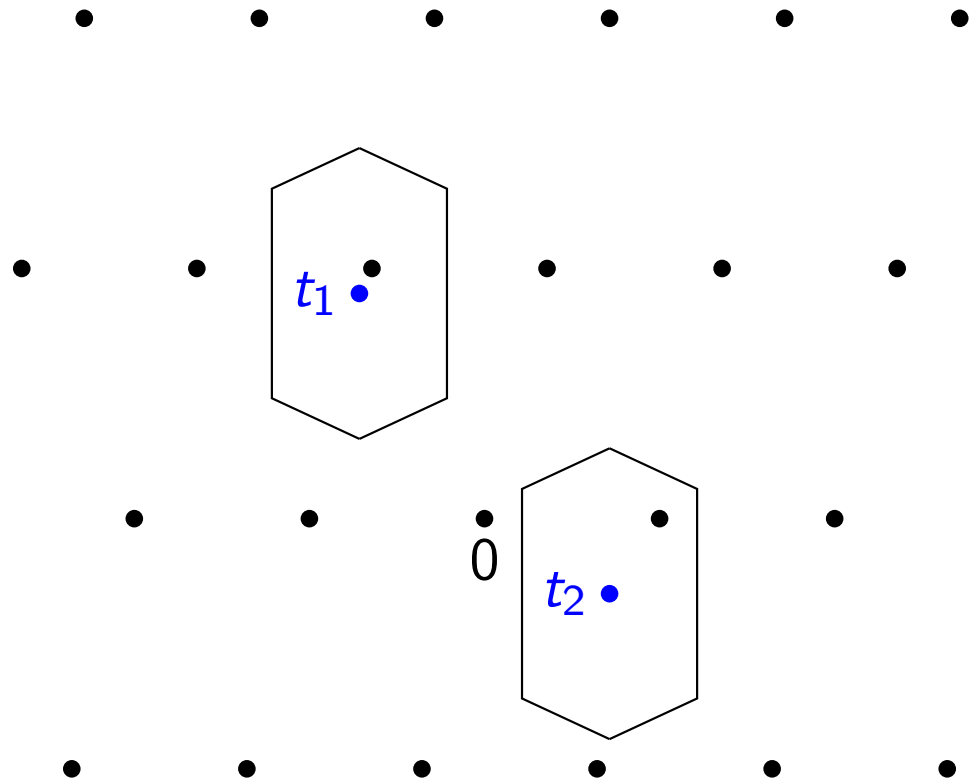
The Shortest Vector Problem (SVP)

Lattices and hard problems



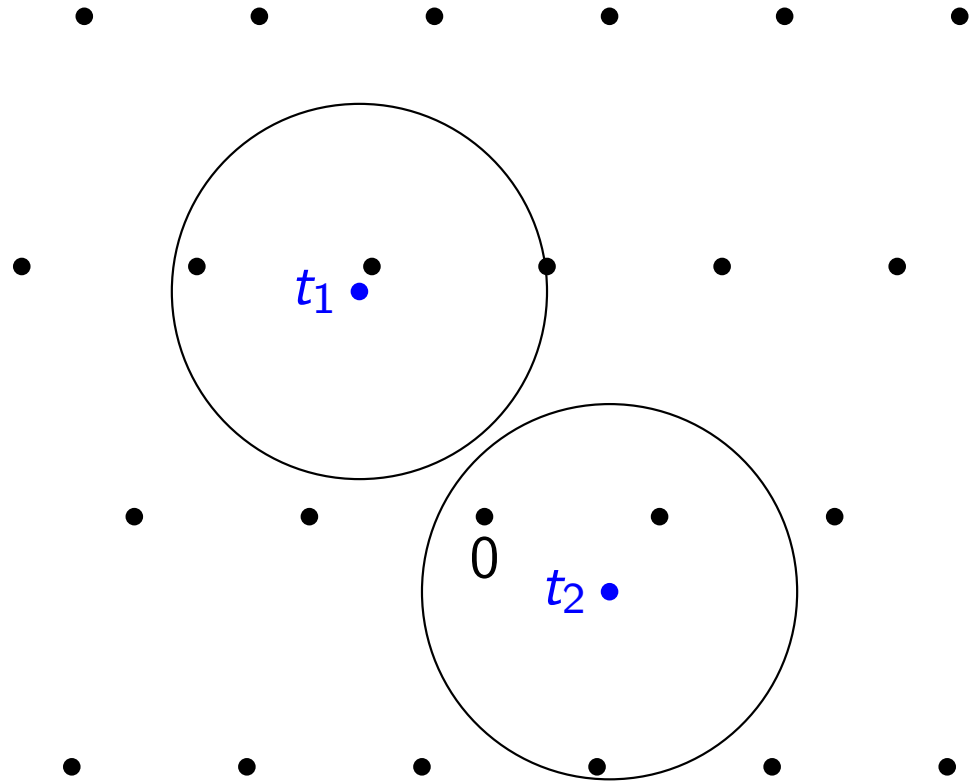
The Approximate Shortest Vector Problem (Approx-SVP)

Lattices and hard problems



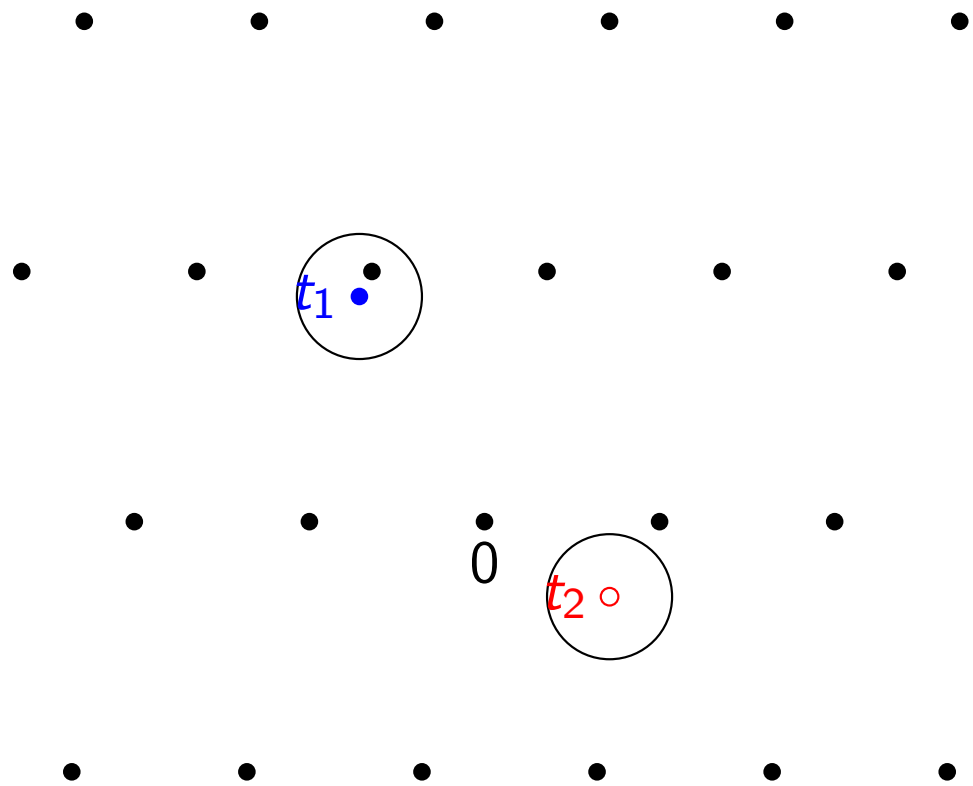
The Closest Vector Problem (CVP)

Lattices and hard problems



The Approximate Closest Vector Problem (Approx-CVP)

Lattices and hard problems



The Bounded Distance Decoding Problem (BDD)

Pre-Regev Lattice-based cryptography

Knowing a good basis (e.g. many approx-SVP solution) makes Approx-CVP and BDD easy

$\Rightarrow$ Public Key cryptography ?

BDD "based" encryption

pk A lattice L.

sk A good basis.

enc(m) View m as a lattice point $L(m)$.

$$c = L(m) + e$$

for some small e.

How to instantiate ?

What lattice ? What error distrib. ? Are messages random ?

Early approaches (NTRU / GGH) pretty heuristic [HPS98, GGH97]

Learning with Errors [BFKL94, Ale03, Reg05]

Definition (Learning with errors, Search and Decision)

Parameters: integers n, m, q, error distrib: ψ
Instance: $\mathbf{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{m \times n}), \mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \psi^m$ (or $\mathbf{s} \leftarrow \psi^n$)
Given: $(\mathbf{A}, \mathbf{As} + \mathbf{e})$
Find: $\mathbf{s}$ / Distinguish: from uniform $\mathcal{U}(\mathbb{Z}_q^{m \times n+1})$

search-LWE as a BDD instance:

- $\mathbf{As}$ is a point in the lattice $L = \{\mathbf{Ax} + q\mathbf{y}, \mathbf{x} \in \mathbb{Z}^n, \mathbf{y} \in \mathbb{Z}^m\}$

Theorem (Quantum reduction, [Reg05])

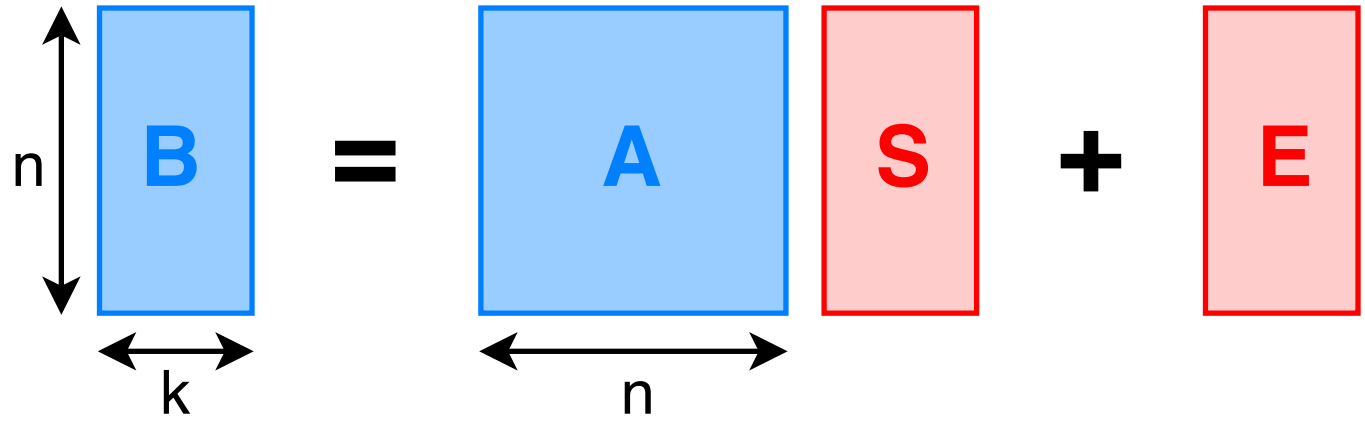
Search-LWE and Decision-LWE are at least as hard as Approx-SVP in the worst-case.

Note: Excellent theortical fundation, yet little practical meaning

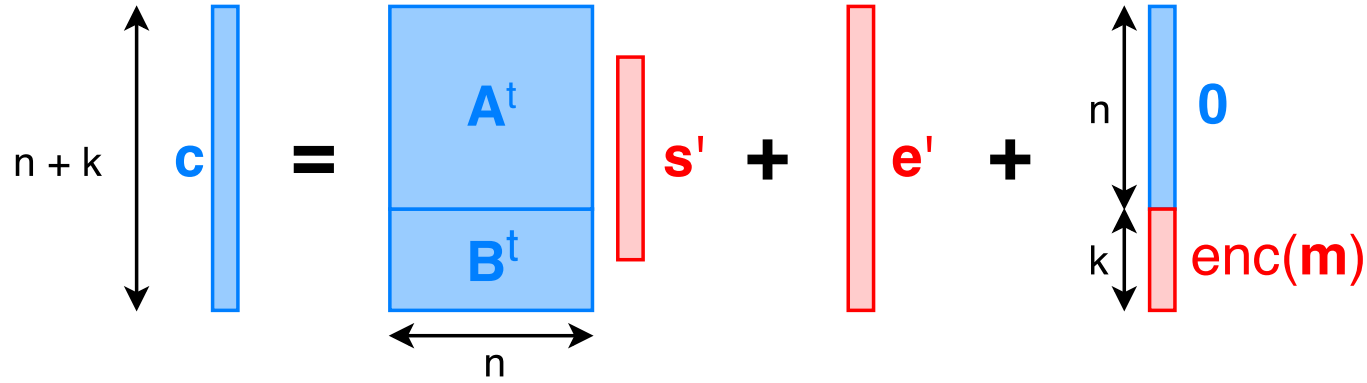
LWE-based encryption

Public parameter $\mathbf{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n \times n})$

KeyGen()



$Encrypt_{\mathbf{b}}(m \in \{0,1\})$



The ring variant [LPR10, LPR13]

Replace matrices and vectors by elements of a (abelian) ring $\mathcal{R} = \mathbb{Z}[X]/(P(X))$.

Definition ($\mathcal{R}$-LWE (over simplified))

Parameters: integers n, m, q, error distrib: ψ
Instance: $a \leftarrow \mathcal{R}, s \leftarrow \mathcal{R}, e \leftarrow \psi$ (or $s \leftarrow \psi$)
Given: $(a, as + e)$
Find: s / Distinguish: from uniform $\mathcal{U}(\mathcal{R}^2)$

The ring variant [LPR10, LPR13]

Replace matrices and vectors by elements of a (abelian) ring $\mathcal{R} = \mathbb{Z}[X]/(P(X))$.

Definition ($\mathcal{R}$-LWE (over simplified))

Parameters: integers n, m, q, error distrib: ψ
Instance: $a \leftarrow \mathcal{R}, s \leftarrow \mathcal{R}, e \leftarrow \psi$ (or $s \leftarrow \psi$)
Given: $(a, as + e)$
Find: s / Distinguish: from uniform $\mathcal{U}(\mathcal{R}^2)$

Theorem (Quantum reduction, [LPR10])

Search-$\mathcal{R}$-LWE are at least as hard as Ideal-Approx-SVP in the worst-case.
When $\mathcal{R}$ is cyclotomic ($\mathcal{R} = \mathbb{Z}[\omega_m]$), Decision-$\mathcal{R}$-LWE is at least as hard as Search-$\mathcal{R}$-LWE.

Outline

Ding et al. / Peikert's RLWE-based KEM

Parameters: q, n, χ

KEM.Setup() :

$\mathbf{a} \xleftarrow{\$} \mathcal{R}_q$

Alice (server)		Bob (client)
KEM.Gen($\mathbf{a}$) :		KEM.Encaps($\mathbf{a}, \mathbf{b}$) :
$\mathbf{s}, \mathbf{e} \xleftarrow{\$} \chi$		$\mathbf{s}', \mathbf{e}', \mathbf{e}'' \xleftarrow{\$} \chi$
$\mathbf{b} \leftarrow \mathbf{as} + \mathbf{e}$	$\xrightarrow{\mathbf{b}}$	$\mathbf{u} \leftarrow \mathbf{as}' + \mathbf{e}'$
		$\mathbf{v} \leftarrow \mathbf{bs}' + \mathbf{e}''$
		$\bar{\mathbf{v}} \xleftarrow{\$} \mathrm{dbl}(\mathbf{v})$
KEM.Decaps($\mathbf{s}, (\mathbf{u}, \mathbf{v}')$) :	$\xleftarrow{\mathbf{u}, \mathbf{v}'}$	$\mathbf{v}' = \langle \bar{\mathbf{v}} \rangle_2$
$\mu \leftarrow \mathrm{rec}(2\mathbf{us}, \mathbf{v}')$		$\mu \leftarrow \lfloor \bar{\mathbf{v}} \rceil_2$

BCNS key exchange

- Bos, Costello, Naehrig, Stebila, IEEE S&P 2015:
  - Instantiate with concrete parameters
  - Integrate with OpenSSL $\rightarrow$ post-quantum TLS key exchange
  - Also: combined ECDH+RLWE key exchange

BCNS key exchange

- Bos, Costello, Naehrig, Stebila, IEEE S&P 2015:
  - Instantiate with concrete parameters
  - Integrate with OpenSSL $\rightarrow$ post-quantum TLS key exchange
  - Also: combined ECDH+RLWE key exchange
- Parameters chosen by BCNS:
  - $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$
  - $n = 1024$
  - $q = 2^{32} - 1$
  - $\chi =$ Gaussian of parameter σ
  - $\sigma = 8\sqrt{2\pi} \approx 3.192$
- Total communications: 2×4 KBytes

BCNS key exchange

- Bos, Costello, Naehrig, Stebila, IEEE S&P 2015:
  - Instantiate with concrete parameters
  - Integrate with OpenSSL $\rightarrow$ post-quantum TLS key exchange
  - Also: combined ECDH+RLWE key exchange
- Parameters chosen by BCNS:
  - $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^n + 1)$
  - $n = 1024$
  - $q = 2^{32} - 1$
  - $\chi =$ Gaussian of parameter σ
  - $\sigma = 8\sqrt{2\pi} \approx 3.192$
- Total communications: 2×4 KBytes
- Claimed security level: 128 bits pre-quantum

A New Hope [Alkim, D., Poppelmann, Shwabe, 2016]

Awarded the **the Internet Defense Prize** (Usenix/Facebook)

Contributions:

- Improve failure analysis and error reconciliation
- Drastically reduce modulus q, **halving** communication
- Analysis of post-quantum security
- Use centered binomial noise ψ_k (reduction provided)
- Choose a fresh parameter **a** for every protocol run
- Provide C reference and fast AVX2 implementation

A New Hope [Alkim, D., Poppelmann, Shwabe, 2016]

Awarded the **the Internet Defense Prize** (Usenix/Facebook)

Contributions:

- Improve failure analysis and error reconciliation
- Drastically reduce modulus q, **halving** communication
- Analysis of post-quantum security
- Use centered binomial noise ψ_k (reduction provided)
- Choose a fresh parameter **a** for every protocol run
- Provide C reference and fast AVX2 implementation

Closer to real-world cryptography:

- Implemented in Boring-SSL, tested in **Google Chrome**

Why sampling fresh parameter **a** at each run ?

We know how to build undetectable backdoors !

It seems simpler and safer to just avoid p.p. than to mount nothing-up-my-sleeve countermeasure.

Other downfall:

- All-for-the-price-of-one attack (e.g. logjam attack): one very large computation can break all instances
- Multi-targets attack becomes easier

Yet, very easy to avoid, at a reasonable cost.

Newhope: Security levels

Attack	samples m	BKZ b	Known Classical	Known Quantum	Best Plausible
BCNS proposal [BCNS15]: $q = 2^{32} - 1$, $n = 1024$, $\sigma = 3.192$					
Primal attack	1062	296	86	**77**	61
JarJar: $q = 12289$, $n = 512$, $\sigma = \sqrt{12}$					
Primal attack	623	449	131	**117**	93
NewHope: $q = 12289$, $n = 1024$, $\sigma = \sqrt{8}$					
Primal attack	1100	967	282	**253**	200

Note: This is according to a very pessimistic security analysis. In particular, this does not invalidate the security claim of [BCNS15].

Newhope: Efficiency

Communications:

$$\text{Alice} \xrightarrow{1824\text{Bytes}} \text{Bob}$$

$$\text{Alice} \xleftarrow{2048\text{Bytes}} \text{Bob}$$

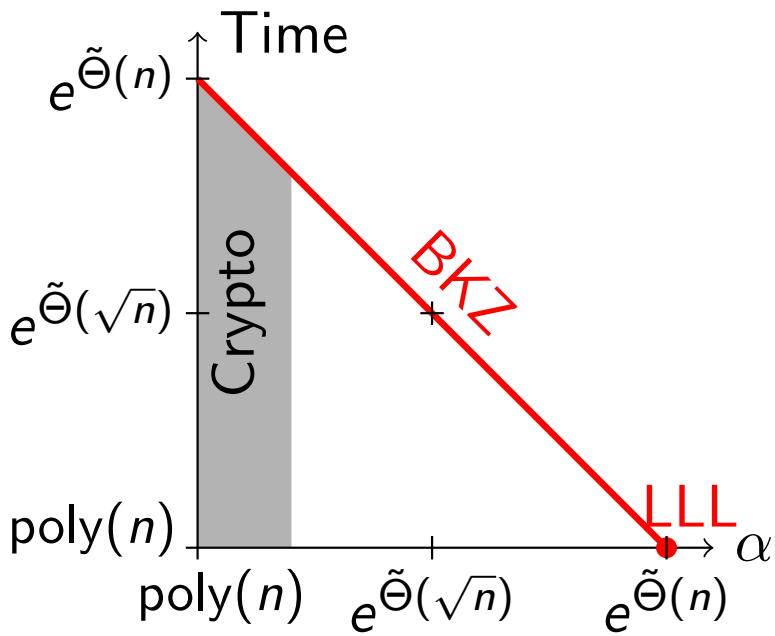
Cycle-count:

	BCNS	**Ours (C ref)**	**Ours (AVX2)**
KeyGen (server)	$\approx 2\,477\,958$	243 748 (243 561)	105 068 (104 874)
Key gen + shared key (client)	$\approx 3\,995\,977$	349 492 (349 686)	141 484 (141 656)
Shared key (server)	$\approx 481\,937$	82 076	29 816

Outline

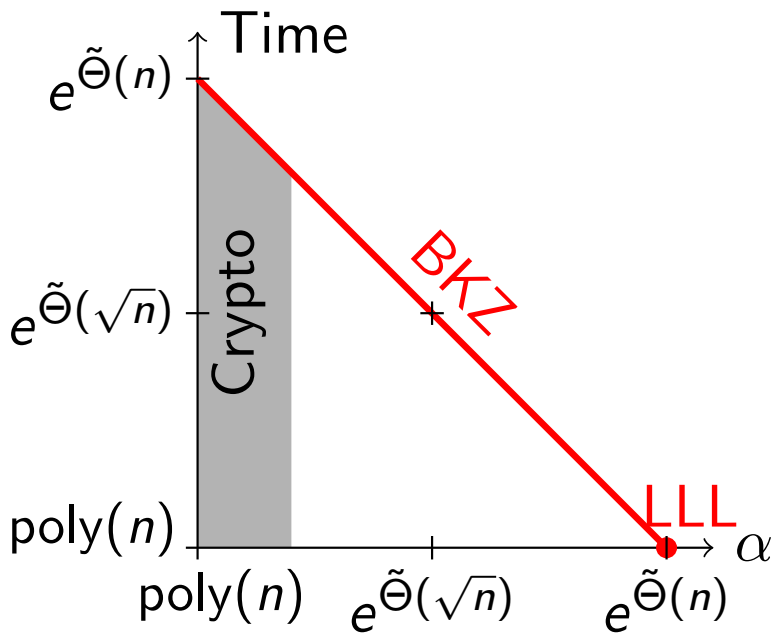
Best known attack on general lattices

Theoretically: α denotes the approximation factor



Best known attack on general lattices

Theoretically: α denotes the approximation factor



Concretely:

- Too little research compared to theoretical constructions
- Claims hard to reproduce (source code or data missing)
- Many avenue for improvements

Algebraic weaknesses ?

Several recent approaches:

- Evaluation attacks [ELOS15]
  Debunked: improper noise distribution [CIV16, Pei16]
- Overstretched NTRU with subfields [ABD16]
  Debunked: no ring nor subfield needed [KF16]
- Quantum SG-PIP algorithm [CGS14, BS16, CDPR16]
  Discussed next slide

Danger ?

Algebraic weaknesses ?

Several recent approaches:

- Evaluation attacks [ELOS15]
  Debunked: improper noise distribution [CIV16, Pei16]
- Overstretched NTRU with subfields [ABD16]
  Debunked: no ring nor subfield needed [KF16]
- Quantum SG-PIP algorithm [CGS14, BS16, CDPR16]
  Discussed next slide

Danger ?

Nothing on plain Ring-LWE or Ideal-SVP !

Algebraic weaknesses ?

Several recent approaches:

- Evaluation attacks [ELOS15]
  Debunked: improper noise distribution [CIV16, Pei16]
- Overstretched NTRU with subfields [ABD16]
  Debunked: no ring nor subfield needed [KF16]
- Quantum SG-PIP algorithm [CGS14, BS16, CDPR16]
  Discussed next slide

Danger ?

Nothing on plain Ring-LWE or Ideal-SVP ! So far...

Algebraic weaknesses ?

Several recent approaches:

- Evaluation attacks [ELOS15]
  Debunked: improper noise distribution [CIV16, Pei16]
- Overstretched NTRU with subfields [ABD16]
  Debunked: no ring nor subfield needed [KF16]
- Quantum SG-PIP algorithm [CGS14, BS16, CDPR16]
  Discussed next slide

Danger ?

Nothing on plain Ring-LWE or Ideal-SVP ! So far...

Quantum PIP and Short Generator recovery

A series of work has shown the following:

SG-PIP in Quantum Poly-time [CGS14, BS16, CDPR16]

Given a **principal ideal** $\mathfrak{I}$ recovering a **short** generator g s.t. $g\mathcal{R} = \mathfrak{I}$, can be done in classical poly-time for

$$m = p^k, \mathcal{R} = \mathbb{Z}[\omega_m], \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Quantum PIP and Short Generator recovery

A series of work has shown the following:

SG-PIP in Quantum Poly-time [CGS14, BS16, CDPR16]

Given a **principal ideal** $\mathfrak{I}$ recovering a **short** generator g s.t. $g\mathcal{R} = \mathfrak{I}$, can be done in classical poly-time for

$$m = p^k, \mathcal{R} = \mathbb{Z}[\omega_m], \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Obstacle toward attacks Ring-LWE

(i) Restricted to **principal** ideals.

(ii) The approximation factor in **too large** to affect Crypto.

(iii) Ring-LWE $\geqslant$ Ideal-SVP, but **equivalence is not known**.

Quantum PIP and Short Generator recovery

A series of work has shown the following:

SG-PIP in Quantum Poly-time [CGS14, BS16, CDPR16]

Given a **principal ideal** $\mathfrak{I}$ recovering a **short** generator g s.t. $g\mathcal{R} = \mathfrak{I}$, can be done in classical poly-time for

$$m = p^k, \mathcal{R} = \mathbb{Z}[\omega_m], \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Obstacle toward attacks Ring-LWE

(i) ~~Restricted to **principal** ideals.~~ [CDW16]

(ii) The approximation factor in **too large** to affect Crypto.

(iii) Ring-LWE $\geqslant$ Ideal-SVP, but **equivalence is not known**.

Short Stickelberger Class Relations & Application to Ideal-SVP [Cramer, D., Wesolowski, 2016]

Our result

$\Rightarrow$ Ideal-SVP **solvable** in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

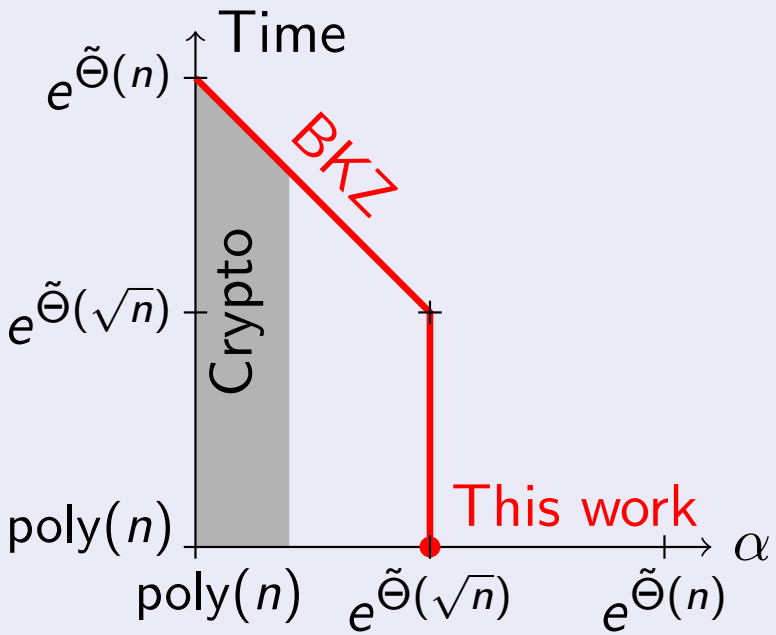
Short Stickelberger Class Relations & Application to Ideal-SVP [Cramer, D., Wesolowski, 2016]

Our result

$\Rightarrow$ Ideal-SVP **solvable** in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Better tradeoffs



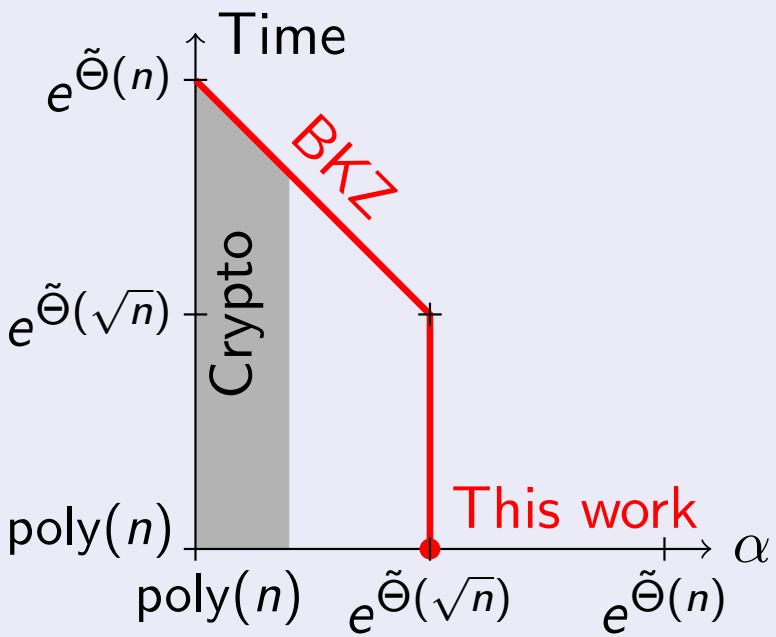
Short Stickelberger Class Relations & Application to Ideal-SVP [Cramer, D., Wesolowski, 2016]

Our result

$\Rightarrow$ Ideal-SVP **solvable** in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Better tradeoffs



Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

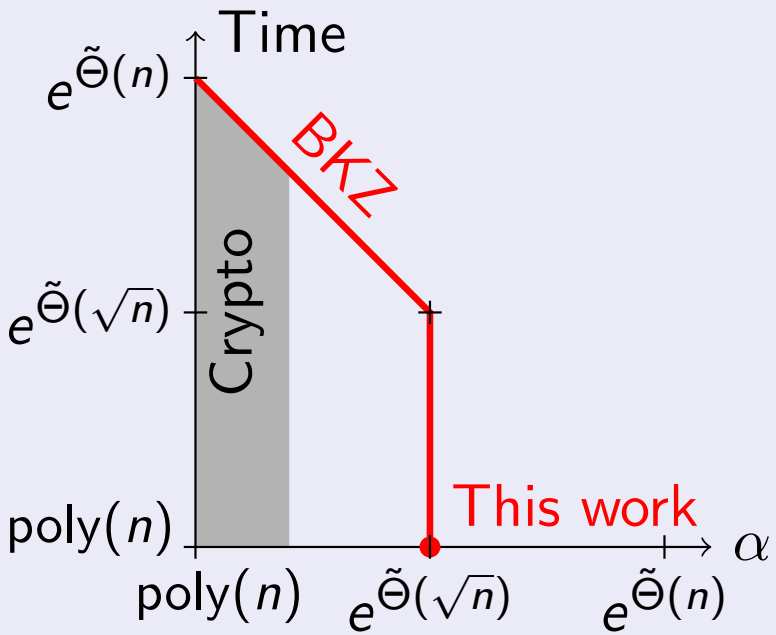
Short Stickelberger Class Relations & Application to Ideal-SVP [Cramer, D., Wesolowski, 2016]

Our result

$\Rightarrow$ Ideal-SVP **solvable** in Quantum poly-time, for

$$\mathcal{R} = \mathbb{Z}[\omega_m], \quad \alpha = \exp(\tilde{O}(\sqrt{n})).$$

Better tradeoffs



Impact and limitations

- No schemes broken
- **Hardness gap** between SVP and Ideal-SVP
- New cryptanalytic tools

$\Rightarrow$ start favoring **weaker assumptions** ?

Should we worry ?

Encryption/Key-Exchange/Signature

I don't: the approximation needed seems way too small to be reached by this approach.

Should we worry ?

Encryption/Key-Exchange/Signature

I don't: the approximation needed seems way too small to be reached by this approach.

Advanced Scheme (FHE, ABE, iO)

I do: most proposal way too aggressive, both in theory and practice (ignoring dual, sparse secret, ad-hoc assumptions . . .)

Should we worry ?

Encryption/Key-Exchange/Signature

I don't: the approximation needed seems way too small to be reached by this approach.

Advanced Scheme (FHE, ABE, iO)

I do: most proposal way too aggressive, both in theory and practice (ignoring dual, sparse secret, ad-hoc assumptions . . .)

Should you trust my gut feeling? **NO !**

- Be as conservative as you can afford to be
- Be patient, wait for the test of time avoid the MLM fiasco

Outline

Frodo [BCD+16]: Take off the ring (A fallback scheme)

Similar design principal applied without ring structure:
(Joint work with NXP, Google and Microsoft)

- Asymptotically, communication grows by $\tilde{\Theta}(\sqrt{\kappa})$
  Naively this would have been $\tilde{\Theta}(\kappa)$
- Can be a bit less conservative (less worries on new attacks)
- No NTT restriction on the choice of q and n
  $q = 2^k$ for efficiency, fine grained choice of n

Frodo [BCD+16]: Take off the ring (A fallback scheme)

Similar design principal applied without ring structure:
(Joint work with NXP, Google and Microsoft)

- Asymptotically, communication grows by $\tilde{\Theta}(\sqrt{\kappa})$
  Naively this would have been $\tilde{\Theta}(\kappa)$
- Can be a bit less conservative (less worries on new attacks)
- No NTT restriction on the choice of q and n
  $q = 2^k$ for efficiency, fine grained choice of n

Scheme	n	q	**dist.**	bit exchanged	**failure**	**bandwidth**
Challenge	352	2^{11}	D_1	$1 \cdot 8^2 = 64$	$2^{-41.8}$	7.75 KB
Classical	592	2^{12}	D_2	$2 \cdot 8^2 = 128$	$2^{-37.2}$	14.22 KB
Recommended	752	2^{15}	D_3	$4 \cdot 8^2 = 256$	$2^{-36.5}$	22.57 KB
Paranoid	864	2^{15}	D_4	$4 \cdot 8^2 = 256$	$2^{-35.8}$	25.93 KB

Frodo: Security and performances

Security:

Scheme	Attack	**Post-reduction** C	Q	P
Classical	Primal	**132**	120	95
	Dual	**130**	119	94
Recomm.	Primal	157	**143**	113
	Dual	156	**142**	112
Paranoid	Primal	192	175	**139**
	Dual	191	174	**138**

Performances :

TLS.ECDSA+Frodo only 1.6 slower than TLS.ECDSA

Outline

Other alternatives to Powers-of-two Cyclotomic Ring-LWE

Very little diversity so far, most practical scheme use:

$$\mathcal{R} = \mathbb{Z}[\zeta_{2^k}] = Z[X]/(X^{2^{k-1}} + 1))$$

- Theory exists [LPR13] for any cyclotomic ring $\mathcal{R} = \mathbb{Z}[\zeta_m]$
  with complications [DD12], sometime ignored in practice (Helib)
- Should extend to $\mathbb{Z}[\omega_p + \bar{\omega}_p]$, p a safe prime
  Related to cyclotomic, but has no subfields [ABD16]
- Other rings suggested [BCLvV16]: $\mathcal{R} = \mathbb{Z}[X]/(X^p + X + 1)$
  No automorphisms (so no security proof for decisional $\mathcal{R}$-LWE)
- Module-LWE [LS15]: a trade-off between Ring-LWE and LWE
  At least as hard as Ring-LWE, but less efficient.

A concrete Module-LWE based scheme (WIP)

Work in progress:

- $\mathcal{R} = \mathbb{Z}[\omega_{512}]$ module rank $r = 3$, $q = 7681$
  Communication $\approx$ 2.7KBytes, Security > 128 PQ-bits
- $\mathcal{R} = \mathbb{Z}[\omega_p + \bar{\omega}_p]$??
- $\mathcal{R} = \mathbb{Z}[X^p + X + 1]$, ??

Compared to NewHope:

Less structure $\Rightarrow$ more confidence, yet, BETTER performances !

Outline

An implicit error correcting code

LWE-Encrypt :

$$\mathbf{c} = \mathbf{A}\mathbf{s} + \mathbf{e} + \lfloor \frac{q}{2} \rfloor \mathbf{m}$$

LWE-Decrypt :

$$\mathbf{m} = \left\lfloor \frac{2}{q}(\mathbf{c} - \mathbf{A}\mathbf{s}) \right\rceil$$

Implicit encoding-decoding

$$\{0, 1\} \to \mathbb{Z}/q\mathbb{Z},$$

applied component-wise.

Don't we know better ?!

Binary codes

Add an outer binary ECC

+ Asymptotically efficient codes of maximal capacity (e.g. Turbo codes)
+ Very widespread
+ Well known by many cryptographers
– Beware of lack of independance between errors
? Resistance to timing/cache attacks

Lattice-codes

Equivalent of ECC for iscrete data over continuous channel

+ Interact optimally with lattice based crypto,
  no information wasted
+ Less understood, especially by cryptographers
− no good asymptotic construction
? Resistance to timing/cache attacks ?

Two Lattice-code tentatives

In NewHope:

- Root-lattice D_4 to encode 1 bit into 4 coordinates
  (256 bits key agreed, for a dimension $n = 1024$)
- No performance gain because of parameter constraints
  can only gain security, which was already overshot

Two Lattice-code tentatives

In NewHope:

- Root-lattice D_4 to encode 1 bit into 4 coordinates
  (256 bits key agreed, for a dimension $n = 1024$)
- No performance gain because of parameter constraints
  can only gain security, which was already overshot

Cryptographic decoding of the Leech Lattice [vanPoppelen, MSc]:

- Revisiting the best Leech Lattice Decoder
- Cache-attack resistant implementation ($\approx$ 100 000 cycles)
- Estimated bandwidth gain on a Frodo-like scheme 10 to 20%

Still a lot of nice theory and practice work to do on this topic !

Thanks

Questions ?


Martin Albrecht, Shi Bai, and Léo Ducas.
A subfield lattice attack on overstretched ntru assumptions: Cryptanalysis of some fhe and graded encoding schemes.
Technical report, Cryptology ePrint Archive, Report 2016/127, 2016.


Michael Alekhnovich.
More on average case vs approximation complexity.
In 44th FOCS, pages 298–307, Cambridge, Massachusetts, USA, October 11–14, 2003. IEEE Computer Society Press.


Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal.
Ntru prime.
Cryptology ePrint Archive, Report 2016/461, 2016.
http://eprint.iacr.org/2016/461.


Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila.
Post-quantum key exchange for the TLS protocol from the ring learning with errors problem.
In 2015 IEEE Symposium on Security and Privacy, pages 553–570, 2015.
http://eprint.iacr.org/2014/599.


Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton.
Cryptographic primitives based on hard learning problems.
In Douglas R. Stinson, editor, CRYPTO'93, volume 773 of LNCS, pages 278–291, Santa Barbara, CA, USA, August 22–26, 1994. Springer, Heidelberg, Germany.


J.-F. Biasse and F. Song.
A polynomial time quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields.
In SODA, 2016.


Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev.
Recovering short generators of principal ideals in cyclotomic rings.
Eurocrypt, 2016.


Ronald Cramer, Lo Ducas, and Benjamin Wesolowski.
Short stickelberger class relations and application to ideal-svp.
Cryptology ePrint Archive, Report 2016/885, 2016.
http://eprint.iacr.org/2016/885.


Peter Campbell, Michael Groves, and Dan Shepherd.
Soliloquy: A cautionary tale.
ETSI 2nd Quantum-Safe Crypto Workshop, 2014.
Available at http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf.


Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren.
Provably weak instances of ring-lwe revisited.
EUROCRYPT 16, Lecture Notes in Computer Science, 2016.


Léo Ducas and Alain Durmus.
Ring-LWE in polynomial rings.

In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, PKC 2012, volume 7293 of LNCS, pages 34–51, Darmstadt, Germany, May 21–23, 2012. Springer, Heidelberg, Germany.


Yara Elias, Kristin E. Lauter, Ekin Ozman, and Katherine E. Stange.
Provably weak instances of ring-LWE.
In Rosario Gennaro and Matthew J. B. Robshaw, editors, CRYPTO 2015, Part I, volume 9215 of LNCS, pages 63–92, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.


Oded Goldreich, Shafi Goldwasser, and Shai Halevi.
Public-key cryptosystems from lattice reduction problems.
In Burton S. Kaliski Jr., editor, CRYPTO'97, volume 1294 of LNCS, pages 112–131, Santa Barbara, CA, USA, August 17–21, 1997. Springer, Heidelberg, Germany.


Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
Ntru: A ring-based public key cryptosystem.
In Joe Buhler, editor, ANTS, volume 1423 of Lecture Notes in Computer Science, pages 267–288. Springer, 1998.


Paul Kirchner and Pierre-Alain Fouque.
Comparison between subfield and straightforward attacks on ntru.
Cryptology ePrint Archive, Report 2016/717, 2016.
http://eprint.iacr.org/2016/717.


Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
On ideal lattices and learning with errors over rings.

In Henri Gilbert, editor, EUROCRYPT 2010, volume 6110 of LNCS, pages 1–23, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany.

Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
A toolkit for ring-LWE cryptography.
In Thomas Johansson and Phong Q. Nguyen, editors, EUROCRYPT 2013, volume 7881 of LNCS, pages 35–54, Athens, Greece, May 26–30, 2013. Springer, Heidelberg, Germany.

Adeline Langlois and Damien Stehlé.
Worst-case to average-case reductions for module lattices.
Designs, Codes and Cryptography, 75(3):565–599, 2015.

Chris Peikert.
How (not) to instantiate ring-lwe.
Technical report, Cryptology ePrint Archive, Report 2016/351, 2016.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In Harold N. Gabow and Ronald Fagin, editors, 37th ACM STOC, pages 84–93, Baltimore, Maryland, USA, May 22–24, 2005. ACM Press.