

LEARNING WITH ERRORS

POST-QUANTUM CANDIDATES FROM NOISY LINEAR SYSTEMS

Martin R. Albrecht @martinralbrecht

15 June 2016 — Bletchley Park

OUTLINE

Motivation

Learning with Errors

Challenges

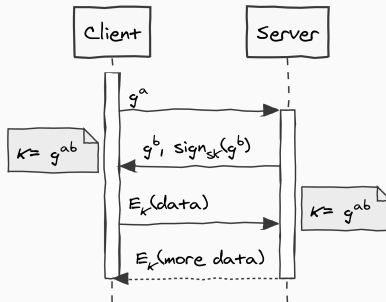
OUTLINE

Motivation

Learning with Errors

Challenges

A TYPICAL SCENARIO



- g^a, g^b, g^{ab} is a Diffie-Hellman triple
- $\text{sign}_{sk}(\cdot)$ typically realised using RSA signatures

BYE, BYE DDH AND RSA (?)

Both problems are easy on quantum computers

BYE, BYE DDH AND RSA (?)

Both problems are easy on quantum computers

- Matthew Campagna et al. [ETSI Whitepaper: Quantum Safe Cryptography and Security](http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf). <http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>. 2015

BYE, BYE DDH AND RSA (?)

Both problems are easy on quantum computers

- Matthew Campagna et al. [ETSI Whitepaper: Quantum Safe Cryptography and Security](http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf). <http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>. 2015
- National Security Agency: Information Assurance Directorate. [Cryptography Today](https://www.nsa.gov/ia/programs/suiteb_cryptography/). https://www.nsa.gov/ia/programs/suiteb_cryptography/. 2015

BYE, BYE DDH AND RSA (?)


Both problems are easy on quantum computers

- Matthew Campagna et al. [ETSI Whitepaper: Quantum Safe Cryptography and Security](http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf). <http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>. 2015
- National Security Agency: Information Assurance Directorate. [Cryptography Today](https://www.nsa.gov/ia/programs/suiteb_cryptography/). https://www.nsa.gov/ia/programs/suiteb_cryptography/. 2015
- CESG. [Quantum Key Distribution — A CESG White Paper](https://www.cesg.gov.uk/white-papers/quantum-key-distribution). <https://www.cesg.gov.uk/white-papers/quantum-key-distribution>. 2016

HELLO POST-QUANTUM


The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE SCIENCE BOOTNOTES FORUMS

 **Security**

NIST readies 'post-quantum' crypto competition

Are you Shor you want to try this?



4 May 2016 at 05:56, [Richard Chirgwin](#)


Your mission, should you choose to accept it, is to help the National Institute of Standards and Technology (NIST) defend cryptography against the onslaught of quantum computers.

It hasn't happened yet, but it's pretty widely agreed that quantum computers pose a significant risk to cryptography. All that's needed is either a quantum computer specifically built to implement [Shor's algorithm](#) (which sets out how to factor integers using quantum computers); or a truly quantum Turing machine that can be programmed to run whatever program it's asked to run.


More like this

Cryptography Nist


Most read




Why Oracle will win its Java copyright case – and why you'll be glad when it does




Even in remotest Africa, Windows 10 nagware ruins your day: Update burns satellite link cash



UK Home Office is creating mega database by stitching together ALL its gov records



UCLA shooter: I killed my prof over code theft



BOFH: What's your point, caller?

POST-QUANTUM FAMILIES

- Multivariate Quadratic Cryptography
- Code-based Cryptography
- Hash-based Signatures
- Lattice-based Cryptography

POST-QUANTUM FAMILIES

- Multivariate Quadratic Cryptography
- Code-based Cryptography
- Hash-based Signatures
- Lattice-based Cryptography

OUTLINE

Motivation

Learning with Errors

Challenges

LINEAR SYSTEM SOLVING

Given (\mathbf{A}, \mathbf{c}) with $\mathbf{c} \in \mathbb{Z}_q^m$, $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{s} \in \mathbb{Z}_q^n$ is

$$\begin{pmatrix} \mathbf{c} \end{pmatrix} = \begin{pmatrix} \leftarrow & n & \rightarrow \\ & \mathbf{A} & \end{pmatrix} \times \begin{pmatrix} \mathbf{s} \end{pmatrix}$$

or $\mathbf{c} \leftarrow_{\$} \mathcal{U}(\mathbb{Z}_q^m)$.

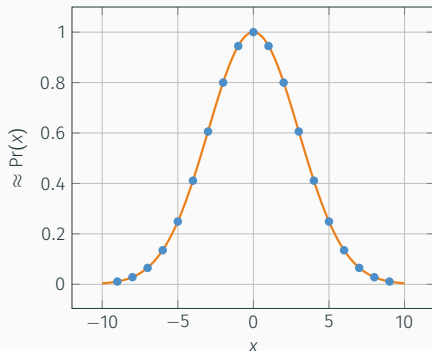
LEARNING WITH ERRORS

Given (\mathbf{A}, \mathbf{c}) with $\mathbf{c} \in \mathbb{Z}_q^m$, $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, $\mathbf{s} \in \mathbb{Z}_q^n$ and small $\mathbf{e} \in \mathbb{Z}^m$ is

$$\begin{pmatrix} \mathbf{c} \end{pmatrix} = \begin{pmatrix} \leftarrow n \rightarrow \\ \mathbf{A} \end{pmatrix} \times \begin{pmatrix} \mathbf{s} \end{pmatrix} + \begin{pmatrix} \mathbf{e} \end{pmatrix}$$

or $\mathbf{c} \leftarrow_{\$} \mathcal{U}(\mathbb{Z}_q^m)$.

PARAMETERS

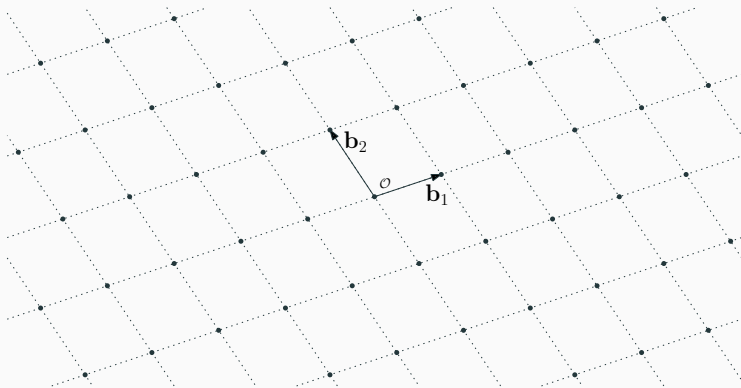


- Parameters are:
 - dimension n ,
 - modulus q (e.g. $q \approx n^2$),
 - noise size α (e.g. $\alpha q \approx \sqrt{n}$),
 - number of samples m .
- Elements of $\mathbf{A}, \mathbf{s}, \mathbf{e}, \mathbf{c}$ are in \mathbb{Z}_q .
- \mathbf{e} is sampled from χ_α , a discrete Gaussian with width

$$\sigma = \frac{\alpha q}{\sqrt{2\pi}}.$$

LATTICES

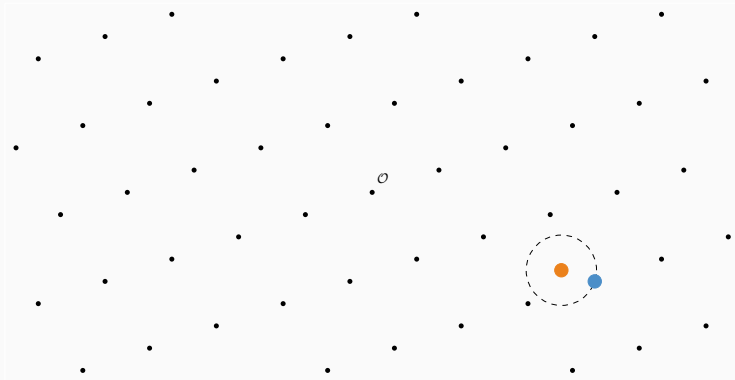
- A lattice is a discrete additive subgroup of \mathbb{R}^n .
- Let $\mathbf{B} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ be m linearly independent vectors in \mathbb{R}^n . Then $L(\mathbf{B}) = \{\sum_{i=1}^n x_i \mathbf{b}_i \mid x_i \in \mathbb{Z}\}$ is the lattice generated by \mathbf{B} .



Picture Credit: Joop van der Pol

BOUNDED DISTANCE DECODING

Let $B = [A|qI]^T$. LWE = BDD for \mathbf{c} and $L(B)$.

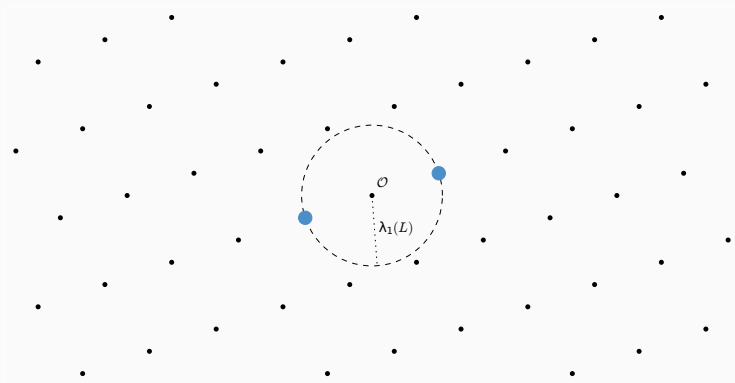


Picture Credit: Joop van der Pol

SHORTEST VECTOR PROBLEM

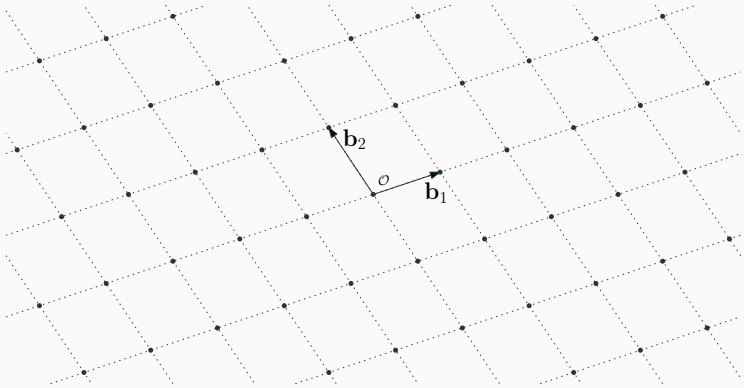
SVP Find the shortest non-zero vector in $L(\mathbf{B})$

GapSVP $_{\gamma}$ return YES if $\lambda_1(L(\mathbf{B})) \leq d$, and NO if $\lambda_1(L(\mathbf{B})) > \gamma \cdot d$.



GOOD AND BAD BASES

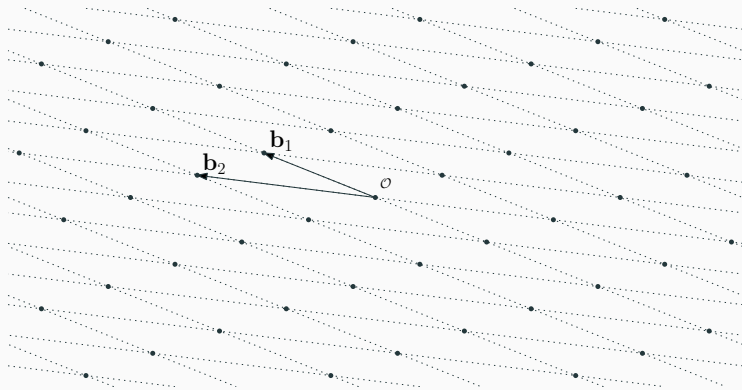
With a “good basis” many lattice problems are easy.



Picture Credit: Joop van der Pol

GOOD AND BAD BASES

With “bad basis” GapSVP_γ for polynomial γ assumed exponential.



Picture Credit: Joop van der Pol

Theorem

- Let e follow χ_α , a (discrete) Gaussian distribution over \mathbb{Z} with standard deviation $\sigma = \frac{\alpha q}{\sqrt{2\pi}}$.
- If $\sigma > \sqrt{n}$, worst-case $\text{GapSVP}_{\tilde{O}(n/\alpha)}$ reduces to average-case LWE.

Oded Regev. **On lattices, learning with errors, random linear codes, and cryptography.** In: 37th ACM STOC. ed. by Harold N. Gabow and Ronald Fagin. ACM Press, May 2005, pp. 84–93

ENCRYPTION

Public Key A, c with $c = A \cdot s + e$

Secret Key s

Encrypt $b \leftarrow_{\$} \{0, 1\}^m$ and return (a', c') with $a' = b \cdot A$,
 $c' = \langle b, c \rangle + m \cdot \lfloor q/2 \rfloor + e'$ for $m \in \{0, 1\}$

Decrypt $c' - \langle a', s \rangle = b \cdot A \cdot s + \langle b, e \rangle + \lfloor q/2 \rfloor \cdot m + e' - b \cdot A \cdot s$

KEY EXCHANGE: LWE NORMAL FORM

Given an LWE instance with $\mathbf{s} \leftarrow_{\$} \mathcal{U}(\mathbb{Z}_q^n)$, we can construct samples of the form $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s}' \rangle + e)$ with \mathbf{s}' sampled from the distribution of e .

- Take n rows and write $(\mathbf{A}, \mathbf{c}) = (\mathbf{A}, \mathbf{A} \cdot \mathbf{s} + \mathbf{e})$.
- With good probability \mathbf{A} is invertible.
- Get a row $(\mathbf{a}', c') = (\mathbf{a}', \langle \mathbf{a}', \mathbf{s} \rangle + e')$ and compute¹

$$\mathbf{a}' \cdot \mathbf{A}^{-1} \cdot \mathbf{c} - c' = \mathbf{a}' \cdot \mathbf{A}^{-1}(\mathbf{A} \cdot \mathbf{s} + \mathbf{e}_0) - \mathbf{a}'\mathbf{s} - e_1 = \mathbf{a}' \cdot \mathbf{A}^{-1} \cdot \mathbf{e} - e'.$$

- $(\mathbf{a}' \cdot \mathbf{A}^{-1}, \mathbf{a}' \cdot \mathbf{A}^{-1} \cdot \mathbf{c} - c')$ is your new sample.

¹Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. [Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems](#). In: *CRYPTO 2009*. Ed. by Shai Halevi. Vol. 5677. LNCS. Springer, Heidelberg, Aug. 2009, pp. 595–618.

KEY EXCHANGE²

Alice samples \mathbf{A} , $\mathbf{c}_a = \mathbf{A} \cdot \mathbf{s}_a + \mathbf{e}_a$ with $\mathbf{s}_a \leftarrow_{\$} \chi_{\alpha}^n$
sends (\mathbf{A}, \mathbf{c})

Bob samples $\mathbf{c}_b = \mathbf{s}_b \cdot \mathbf{A} + \mathbf{e}_b$ with $\mathbf{s}_b \leftarrow_{\$} \chi_{\alpha}^n$
sends \mathbf{c}_b

Shared Secret

$$\mathbf{s}_b \cdot (\mathbf{A} \cdot \mathbf{s}_a + \mathbf{e}_a) \approx (\mathbf{s}_b \cdot \mathbf{A} + \mathbf{e}_b) \cdot \mathbf{s}_a \approx \mathbf{s}_b \cdot \mathbf{A} \cdot \mathbf{s}_a$$

²Joppe 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*. IEEE Computer Society Press, May 2015, pp. 553–570. DOI: 10.1109/SP.2015.40; Erdem Alkim, Léoucas, Thomas Pöppelmann, and Peter Schwabe. [Post-quantum key exchange - a new hope](#). Cryptology ePrint Archive, Report 2015/1092. <http://eprint.iacr.org/2015/1092>. 2015.

SIGNATURES (FROM SIS)

SIS

Given $A \in \mathbb{Z}_q^{m \times n}$ find **small** s such that $s \cdot A = 0$

- Hash-and-Sign signatures³
- Fiat-Shamir signatures⁴

³Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. **Trapdoors for hard lattices and new cryptographic constructions**. In: *40th ACM STOC*. ed. by Richard E. Ladner and Cynthia Dwork. ACM Press, May 2008, pp. 197–206.

⁴Léo Ducas, Alain Durmus, Tancrede Lepoint, and Vadim Lyubashevsky. **Lattice Signatures and Bimodal Gaussians**. In: *CRYPTO 2013, Part I*. ed. by Ran Canetti and Juan A. Garay. Vol. 8042. LNCS. Springer, Heidelberg, Aug. 2013, pp. 40–56. DOI: 10.1007/978-3-642-40041-4_3.

OUTLINE

Motivation

Learning with Errors

Challenges

REGEV'S REDUCTION

- An algorithm solving LWE
 - for a fraction $1/n^{d_1}$
 - with advantage $1/n^{d_2}$
 - given $m = n^c$ samples

implies a polynomial-time algorithm solving GapSVP_γ calling LWE solving oracle $\mathcal{O}(n^{11+c+d_1+2d_2})$ times.⁵

⁵Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar. [Another Look at Tightness II: Practical Issues in Cryptography](#). In: *IACR Cryptology ePrint Archive* 2016 (2016), p. 360. URL: <http://eprint.iacr.org/2016/360>.

REGEV'S REDUCTION

- An algorithm solving LWE
 - for a fraction $1/n^{d_1}$
 - with advantage $1/n^{d_2}$
 - given $m = n^c$ samples

implies a polynomial-time algorithm solving GapSVP_γ calling LWE solving oracle $\mathcal{O}(n^{11+c+d_1+2d_2})$ times.⁵

- “Solving LWE n^{11+} times is hard”

⁵Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar. [Another Look at Tightness II: Practical Issues in Cryptography](#). In: *IACR Cryptology ePrint Archive* 2016 (2016), p. 360. URL: <http://eprint.iacr.org/2016/360>.

REGEV'S REDUCTION

- An algorithm solving LWE
 - for a fraction $1/n^{d_1}$
 - with advantage $1/n^{d_2}$
 - given $m = n^c$ samples

implies a polynomial-time algorithm solving GapSVP_γ calling LWE solving oracle $\mathcal{O}(n^{11+c+d_1+2d_2})$ times.⁵

- “Solving LWE n^{11+} times is hard”
- Best Known Attacks on LWE: $2^{\mathcal{O}(n)}$ time **and** $2^{\mathcal{O}(n)}$ memory

⁵Sanjit Chatterjee, Neal Koblitz, Alfred Menezes, and Palash Sarkar. [Another Look at Tightness II: Practical Issues in Cryptography](#). In: *IACR Cryptology ePrint Archive* 2016 (2016), p. 360. URL: <http://eprint.iacr.org/2016/360>.

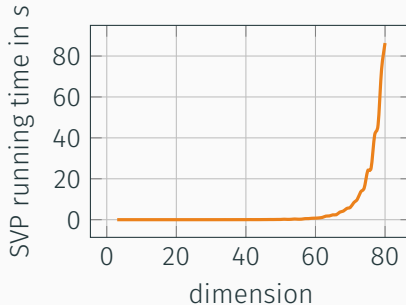
HOW HARD IS $2^{\mathcal{O}(n)}$ TIME AND $2^{\mathcal{O}(n)}$ MEMORY?

- How big should we choose n , q and the noise?
- Many problem formulations: SIS, BDD, uSVP, ...
- Many algorithms: combinatorial, algebraic, geometric
- Quantum attacks

Martin R Albrecht, Rachel Player, and Sam Scott. [On the concrete hardness of Learning with Errors](#). In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203

LATTICE REDUCTION

- Practically relevant algorithms rely on **lattice reduction** as a subroutine.
- Concrete performance of lattice reduction algorithms is not well understood.



Software

- <https://github.com/dstehle/fplll>
- <https://github.com/malb/fpylll>
- <http://perso.ens-lyon.fr/gilles.villard/hplll/>

- **Computational** cost for LWE is quite manageable because it only involves simple linear operations over \mathbb{Z}_q where q can be word-sized.
- Public-key and ciphertext **sizes** can be prohibitively expensive: $\mathcal{O}(n^2 \log_2 q)$ and $\mathcal{O}(n \log_2 q)$

- **Computational** cost for LWE is quite manageable because it only involves simple linear operations over \mathbb{Z}_q where q can be word-sized.
- Public-key and ciphertext **sizes** can be prohibitively expensive: $\mathcal{O}(n^2 \log_2 q)$ and $\mathcal{O}(n \log_2 q)$

Rule of Thumb

Post-quantum schemes are not slow, but they are big.

BETTER PERFORMANCE: RING-LWE

- Replace random \mathbf{A} by structured matrices, e.g. cyclic or nega-cyclic matrices.
- This is equivalent to computing in $\mathbb{Z}_q[x]/P(x)$.
- The problem is then called Ring-LWE.

BETTER PERFORMANCE: RING-LWE

- Replace random \mathbf{A} by structured matrices, e.g. cyclic or nega-cyclic matrices.
- This is equivalent to computing in $\mathbb{Z}_q[x]/P(x)$.
- The problem is then called **Ring-LWE**.

No Silver Bullet

$n = 1024, q \approx 2^{14} \rightarrow 1792$ bytes vs. MTU of 1500 bytes in Ethernet.

RINGS: NOT ALL PROBLEMS ARE HARD

- Let $n = 2^k$, sample some small $g \in \mathbb{Z}[x]/(x^n + 1)$.
- Consider the matrix \mathbf{G} spanned by the coefficient vectors of $\{x^i \cdot g \bmod x^n + 1\}$.
- Compute the Hermite normal form $\mathbf{H} = \text{HNF}(\mathbf{G})$.
- With good probability g is a shortest vector of the lattice $L(\mathbf{H})$.

Finding g takes polynomial time on a quantum computer.⁶

⁶Peter Campbell, Michael Groves, and Dan Shepherd. **SOLILOQUY: A CAUTIONARY TALE**. . ETSI 2nd Quantum-Safe Crypto Workshop. available at http://docbox.etsi.org/Workshop/2014/201410_CRYPT0/S07_Systems_and_Attacks/S07_Groves_Annex.pdf. 2014; Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. **Recovering Short Generators of Principal Ideals in Cyclotomic Rings**. In: *EUROCRYPT 2016*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Springer Berlin Heidelberg, 2016, pp. 559–585.

RINGS: NOT ALL PROBLEMS ARE AS HARD

- What if $\mathbb{Z}_q[x]/P(x)$ has subfields?
- Distinguishing $h = f/g \in \mathbb{Z}_q[x]/P(x)$ from random for small f and g and big q is easier than expected.⁷

⁷Craig Gentry and Michael Szydlo. *Cryptanalysis of the Revised NTRU Signature Scheme*. In: *EUROCRYPT 2002*. Ed. by Lars R. Knudsen. Vol. 2332. LNCS. Springer, Heidelberg, 2002, pp. 299–320; Martin Albrecht, Shi Bai, and Léoucas. *A subfield lattice attack on overstretched NTRU assumptions: Cryptanalysis of some FHE and Graded Encoding Schemes*. In: *IACR Cryptology ePrint Archive* 2016 (2016). URL: <http://ia.cr/2016/127>.

RINGS: NO KNOWN ATTACKS

There is **no known attack** which successfully exploits ring structure for properly chosen Ring-LWE parameters.

- The schemes described here (and in the literature) promise IND-CPA security, i.e. security against chosen-plaintext attacks.
- They do not promise IND-CCA security, i.e. security against chosen-ciphertext attacks.
- Building efficient CCA secure schemes from LWE is still open.⁸

⁸Chris Peikert. [Public-key cryptosystems from the worst-case shortest vector problem: extended abstract](#). In: 41st ACM STOC. ed. by Michael Mitzenmacher. ACM Press, 2009, pp. 333–342.

Thank You