Statement of Research

Noah Stephens-Davidowitz*

1 Summary

My research primarily uses the tools of *theoretical computer science* to answer fundamental questions about the security of widely deployed *real-world cryptography*.

Much of my work focuses on the foundations of *post-quantum cryptography*, that is, classical cryptographic schemes that are secure even against an adversary with a quantum computer. This particular line of research has some added urgency at the moment because such schemes are currently in the process of being standardized [NIS, Wika], with the goal of replacing much of our current (quantum-insecure) infrastructure in the near future [Bra16, NIS16, Moo18]. My co-authors and I study the fundamental computational problems underlying the security of these schemes by developing faster algorithms [DRS14, ADRS15, ADS15, AS18b, Ste19, ALNS19, MS19b, ALS19]; proving strong *fine-grained* hardness results [BGS17, AS18a, ABGS19, BSV19, SV19]; and studying the complexity of these problems more generally [Ste15, Ste16a, Ste16b, BDS16, PRS17].

I am also interested more broadly in theory, cryptography, and geometry. My co-authors and I have studied randomness extraction and (pseudo)random number generation [DSSW14, AGO+19, DGS19]; "post-Snowden" cryptography [MS15, DMS16] and other cryptographic constructions [HHSS17, APS18]; high-dimensional geometry [RS17a, RS17b, Ste17, MS19a, AS19]; and combinatorics [SC07, HCS07].

2 Selected Results

2.1 Lattices, codes, and post-quantum cryptography

Most of the post-quantum cryptographic constructions under consideration for standardization and widespread deployment use *lattice-based cryptography*, i.e., cryptography whose security relies on the presumed hardness of certain computational problems over n-dimensional geometric objects called *lattices*. Most of the remaining candidates are based on natural problems over *linear codes*.

The security of the proposed schemes relies crucially on the assumption that our current best algorithms (both classical and quantum) for these lattice and coding problems cannot be improved by even a relatively small amount.[1] However, these problems are not as well understood as the analogous problems behind the (quantum-insecure) cryptography that currently secures more than half of all internet traffic—factoring and the discrete logarithm. Indeed, my colleagues and I are still learning about these problems and discovering new algorithms for them [ADRS15, ADS15,

*Massachusetts Institute of Technology

[1] To maximize efficiency, practitioners typically choose key sizes and other parameters to be as small as possible while keeping the presumed security above some threshold, leaving very little margin for error in the security analysis.

AS18b, ALNS19, ALS19, MS19b], which might make one worry that further progress will break the proposed schemes after they are deployed.[2]

It is therefore imperative that we study these computational problems thoroughly *before* post-quantum cryptography is deployed at scale. Below, I list some of the many ways that my co-authors and I have attacked these problems.

SVP and CVP algorithms. Together with Aggarwal, Dadush, and Regev, we showed a new algorithm for the most important computational lattice problem, the *Shortest Vector Problem* (SVP) [ADRS15]. Our algorithm runs in $2^{n+o(n)}$ time, which improved upon the previous best proven running time of $4^{n+o(n)}$ [MV13].[3] The speed of such algorithms determines the security of lattice-based cryptography, as our current best attacks work via a reduction to SVP. With Aggarwal and Dadush, we later extended this result to an algorithm with the same running time for the *Closest Vector Problem* (CVP) [ADS15], which is the second-most important computational lattice problem and is known to be at least as hard as SVP.

Recently, we found a much simpler $2^{n+o(n)}$-time algorithm for SVP [AS18b], and we hope that this simpler algorithm will be easier to improve. Indeed, using ideas from [AS18b], we discovered a faster algorithm for a closely related problem [ALS19].

Lower bounds for SVP, CVP, and codes. Together with Bennett and Golovnev, we showed strong evidence that the algorithm for CVP mentioned above is essentially the fastest possible [BGS17] by proving *quantitative* lower bounds for CVP under certain well known complexity-theoretic conjectures.[4] With Aggarwal, we extended this to similar quantitative lower bounds for SVP [AS18a], proving that our current algorithms for SVP cannot be improved *too much*.[5] Such *fine-grained* hardness results give far stronger guarantees than, e.g., results that only rule out polynomial-time algorithms, and they therefore rule out certain attacks on lattice-based cryptography in practice. Both of these works answered long-standing open questions.

In recent work with Vaikuntanathan, we prove optimal lower bounds for the two most fundamental *coding problems* [SV19]. Again, this rules out some attacks on code-based post-quantum cryptographic schemes. Finally, in [ABGS19] we prove hardness of key variants of CVP.

The reverse Minkowski conjecture. With Regev, we proved Dadush's beautiful "reverse Minkowski" conjecture [RS17b]. The conjecture is closely related to Minkowski's celebrated theorem, which states that a dense lattice must have many short vectors. This is a foundational result in the study of lattices, and it has innumerable applications in fields as diverse as number theory, complexity theory, coding theory, and cryptography.

[2] Factoring and the discrete logarithm offer a cautionary tale, as there been multiple algorithmic breakthroughs for these problems since the first public-key encryption schemes were deployed. E.g., the original parameters chosen for the RSA encryption scheme are now known to be insecure. This was not a major issue at the time, but now we rely on secure communication far more and face far more determined and sophisticated adversaries.

[3] There are other algorithms that seem to perform better in practice but come with no proof of correctness [NV08, BDGL16].

[4] Setting aside some very important technical caveats, we showed that the fastest algorithm for CVP runs in time $2^{n+o(n)}$ under the Strong Exponential Time Hypothesis.

[5] Unlike for CVP, our lower bounds for SVP do not rule out *any* improvement. We actually expect to find faster algorithms for SVP, as I discuss a bit in Section 3.

Dadush conjectured a converse to this important theorem: that any (non-degenerate) lattice with many short vectors must be dense. Before it was proven, Dadush and Regev showed many implications of the conjecture in complexity theory, cryptography, integer programming, and Brownian motion [DR16], and even showed that it implies an earlier conjecture due to Kannan and Lovász [KL88]. Even more applications have appeared since, including work with my co-authors on new cryptographic proof systems [APS18], lattice algorithms [Ste19, ALS19], and hardness results [BSV19], as well as work by others in additive combinatorics [LR17], and convex geometry and complexity theory [Dad19]. The techniques in [RS17b] also yielded a new promising line of attack on a centuries-old question in algebraic number theory, as I discuss in Section 3.

This work has attracted attention from the larger community. [RS17b] was the subject of a Bourbaki Seminar [Wikb] given by Bost [Bos18]. And, Wigderson used our proof of a purely mathematical conjecture that arose from computer science as an example of the fruitful interplay between computer science and pure mathematics [Wig18].

Worst-case to average-case reductions. With Peikert and Regev, we showed *worst-case to average-case reductions* for a large class of lattice-based cryptographic schemes [PRS17]. Such reductions are one of the main selling points of lattice-based cryptography [Ajt04, MR07, Reg09] because they prove that cryptography is secure assuming the hardness of problems that are better understood theoretically, such as SVP.

Before our work, however, such reductions were only known for a small fraction of lattice-based cryptographic constructions. In [PRS17], we extend to essentially all plausible schemes[6] the strong hardness guarantees that we previously only knew in certain special cases. (Our results also subsume nearly all prior work.) In particular, we give the first such hardness guarantee for many of the cryptographic constructions based on *ideal lattices*, resolving a question posed in [LPR13]. These constructions are strongly preferred in practice because of their efficiency. (See Section 3.)

Additional work in lattices. My co-authors and I have also studied the geometry of lattices [RS17a, Ste17, MS19a, AS19]; developed additional lattice algorithms [DRS14, BDS16, Ste19, MS19b, ALNS19]; studied the complexity of other computational lattice problems [Ste15, Ste16a, Ste16b, BDS16]; and constructed lattice-based cryptographic schemes [HHSS17, APS18].

2.2 Other topics

Real-world RNGs. With Dodis, Shamir, and Wichs [DSSW14] and Dodis and Guo [DGS19], we study the *online (pseudo)Random Number Generators* (RNGs) that are widely used in practice. These RNGs are designed to slowly *accumulate* entropy from a sequence of random sources with unknown quality, such as thermal noise measurements or keystroke timings. This is in contrast to the pseudorandom generators typically studied by theoretical cryptographers, which require a truly random seed to start (or the "one-shot" extractors described below, which take a single input).

In [DSSW14], we provide the first formal security model for Ferguson and Schneier's celebrated *Fortuna* construction [FS03]. In [DGS19], we study the *high-speed online RNGs* used by operating systems. Such an RNG is run very frequently (e.g., on every keystroke) and therefore may only perform a few simple bit operations each time that it is run. In both cases, we provide the first

[6] Specifically, it works for all schemes based on versions of Regev's Learning with Errors problem [Reg09] (including Ring-LWE, Module-LWE, etc.).

theoretical justification (in quite strong models, using very diferent techniques) for RNGs that are widely used in practice. We also uncover surprising connections to number theory and harmonic analysis, and use these tools to improve on the current constructions.

Fine-grained hardness of average-case k-SUM. With Brakerski and Vaikuntanathan, we show strong lower bounds on algorithms for the *average-case* k-SUM problem (assuming a widely believed conjecture) [BSV19]. The *worst-case* fine-grained hardness of k-SUM has been extensively studied [Wil18] since the celebrated work of Gajentaan and Overmars [GO95, GO12] showed its close connection with many important problems in computational geometry.

Our work is the first to show fine-grained hardness for the *average-case* version of this problem (or for any natural problem). This has important applications in cryptography, such as in proof-of-work schemes [BRSV17, BRSV18]. In fact, our result yields the first fine-grained one-way function (and even a fine-grained collision-resistant hash function!), resolving open problems in [BRSV17].

Somewhere extractors. With Aggarwal, Guo, Obremski, and Ribeiro, we prove separations between *somewhere extractors* and *strong extractors* [AGO+19]. Extractors are deterministic functions that use a short random seed to convert any (single) entropic input string into a shorter uniformly random string. Optimal constructions of *strong* extractors have been known for decades and have innumerable applications. However, many of these applications only require a much weaker primitive known as *somewhere* extractors, which have gone largely unstudied.

We show a surprisingly simple construction of a somewhere extractor that is twice as efficient (in seed length) as the best possible strong extractor. This yields immediate improvements for many applications. We also prove lower bounds showing that our construction is nearly optimal.

Post-Snowden cryptography. The revelations of Snowden and the discovery of many high-profile security-breaking bugs in cryptographic constructions have led cryptographers [BPR14, DGG+15] to a rather paradoxical questions: "Can we provide meaningful security guarantees even if the users' machine is not behaving properly, either due to bugs or deliberate tampering?" With Mironov, we introduced the concept of a *cryptographic reverse firewall*, which allowed us to build powerful cryptographic constructions that remain secure even if the adversary has tampered with the user's machine [MS15]. With Dodis and Mironov, we then studied the fundamental problem of secure and efficient message transmission in this model [DMS16]. Since, others have used reverse firewalls to construct many "post-Snowden" cryptographic schemes [AMV15, CMY+16, MZY+18].

3 Directions for future work

In the future, I of course plan to continue studying real-world cryptography from a theorist's perspective. In particular, my colleagues' and my work on post-quantum cryptography has some added urgency at the moment, as we hope to identify any weaknesses in proposed schemes *before* they are widely deployed. We can also provide more evidence for the security of some schemes (as in much of the work described above), to provide better guidance to NIST and others.

I will also continue to study the geometry of lattices (which Wigderson recently declared to be "among the most 'universal' objects in mathematics" [Wig18]), cryptography more broadly, complexity theory, randomness and pseudorandomness, high-dimensional geometry, etc. Below, I describe a few of the specific open problems and directions that interest me.

Towards provable security. The holy grail for me would be a proof of the *quantitative* security of some specific public-key cryptographic scheme, i.e., a theorem of the form "no algorithm running in time 2^{128} can break this specific scheme." Such a statement would be a major theoretical breakthrough and allow cryptographers (and internet users) to rest easy. But, there are many major barriers to proving such a result, so that it seems very far out of reach at the moment (even if we are willing to make strong complexity-theoretic assumptions).

Nevertheless, we can make progress towards this ambitious goal and provide strong evidence for security. For example, the lower bounds in [BGS17, AS18a, ABGS19, SV19] rule out a large class of attacks on certain (post-quantum) cryptographic schemes. With many of my colleagues, we plan to continue in this direction. For lattice-based cryptography, we hope to prove lower bounds on problems that are progressively "closer" to cryptography—specifically, lower bounds on approximate SVP for progressively larger approximation factors. Another approach starts with the fine-grained cryptography that we built in [BSV19] and tries to "boost" the security.

Ideal lattices. Many lattice-based cryptographic schemes rely on a special class of lattices related to algebraic number fields, called ideal lattices [PR06, Mic07, LPR13]. (Ideal lattices were what originally motivated Minkowski, Hermite, and others to study lattices in the mid 19th century.) These schemes are remarkably efficient, and until recently, most experts believed that these more efficient schemes were just as secure as "plain lattice" schemes. Ideal lattices are therefore almost always used in practical applications. E.g., all but one of the NIST candidates use ideal lattices.

However, a recent series of unexpected algorithmic advances ([CGS14, CDPR16, CDW17, PHS19, LPSW19] and [Ste19, MS19b]) has brought the security of these schemes into question. These new algorithms do not yet yield attacks on any of the cryptographic schemes mentioned above, and most people think that they will not. However, we naturally fear that they could be our first glimpse of a huge security problem. My colleagues and I are working quickly to try to either extend these algorithms to attacks or to discover what barriers, if any, prevent this. Indeed, with Mukherjee, we recently showed some evidence for such barriers [MS19b].

Minkowski's conjecture. Minkowski's famous centuries-old conjecture in algebraic number theory posits a tight bound on the "algebraic distance" between an element in an algebraic number field and an ideal over its ring of integers. The conjecture has only been proven for low-degree fields using computer-assisted case analysis [HRS09, HRS11, KR16] that cannot work for larger-degree fields. In [RS17b] we found an entirely different way to attack Minkowski's conjecture. We proved (using a beautiful result of [SW16]) that the conjecture would follow from a positive resolution to another famous question in convex geometry (specifically, a special case of the slicing conjecture). With Dadush, Eldan, Regev, and Weiss, we are trying to use this approach to prove the conjecture.

Faster SVP algorithms. Currently, the fastest algorithms for SVP are still the $2^{n+o(n)}$-time algorithms from [ADRS15, AS18b]. However, this seems not to be the end of the story. There are heuristic algorithms that perform much better in practice [NV08, BDGL16], and there is strong reason to believe that the algorithmic techniques in [ADRS15] can be improved substantially [AS18b, ALS19]. Indeed, there is a natural candidate algorithm that runs in $2^{n/2+o(n)}$ time whose correctness we have been unable to prove so far. Nevertheless, we believe that a proof is possible. We are therefore working with Aggarwal, Li, and Regev, to find this proof, as well as to find alternative algorithms.

Work to Which I Contributed

[ABGS19] Divesh Aggarwal, Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. Fine-grained hardness of CVP(P)—Everything that we can prove (and nothing else). http://arxiv.org/abs/1911.02440, 2019.

[ADRS15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the Shortest Vector Problem in 2^n time via discrete Gaussian sampling. In *STOC*, 2015. http://arxiv.org/abs/1412.7994.

[ADS15] Divesh Aggarwal, Daniel Dadush, and Noah Stephens-Davidowitz. Solving the Closest Vector Problem in 2^n time–The discrete Gaussian strikes again! In *FOCS*, 2015. http://arxiv.org/abs/1504.01995.

[AGO+19] Divesh Aggarwal, Siyao Guo, Maciej Obremski, João Ribeiro, and Noah Stephens-Davidowitz. Extractor lower bounds, revisited. 2019.

[ALNS19] Divesh Aggarwal, Jianwei Li, Phong Q. Nguyen, and Noah Stephens-Davidowitz. Slide reduction, revisited–Filling the gaps in SVP approximation. http://arxiv.org/abs/1908.03724, 2019.

[ALS19] Divesh Aggarwal, Zeyong Li, and Noah Stephens-Davidowitz. Solving SVP faster via HermiteSVP. 2019.

[APS18] Navid Alamati, Chris Peikert, and Noah Stephens-Davidowitz. New (and old) proof systems for lattice problems. In *PKC*, 2018. https://eprint.iacr.org/2017/1226.

[AS18a] Divesh Aggarwal and Noah Stephens-Davidowitz. (Gap/S)ETH hardness of SVP. In *STOC*, 2018. http://arxiv.org/abs/1712.00942.

[AS18b] Divesh Aggarwal and Noah Stephens-Davidowitz. Just take the average! An embarrassingly simple 2^n-time algorithm for SVP (and CVP). In *SOSA*, 2018. http://arxiv.org/abs/1709.01535.

[AS19] Divesh Aggarwal and Noah Stephens-Davidowitz. An improved constant in Banaszczyk's transference theorem. http://arxiv.org/abs/1907.09020, 2019.

[BDS16] Huck Bennett, Daniel Dadush, and Noah Stephens-Davidowitz. On the Lattice Distortion Problem. In *ESA*, 2016. http://arxiv.org/abs/1605.03613.

[BGS17] Huck Bennett, Alexander Golovnev, and Noah Stephens-Davidowitz. On the quantitative hardness of CVP. In *FOCS*, 2017. http://arxiv.org/abs/1704.03928.

[BSV19] Zvika Brakerski, Noah Stephens-Davidowitz, and Vinod Vaikuntanathan. k-sum in the dense regime. 2019.

[DGS19] Yevgeniy Dodis, Siyao Guo, and Noah Stephens-Davidowitz. On very efficient online extractors. 2019.

[DMS16] Yevgeniy Dodis, Ilya Mironov, and Noah Stephens-Davidowitz. Message transmission with Reverse Firewalls—secure communication on corrupted machines. In *CRYPTO*, 2016. https://eprint.iacr.org/2015/548.

[DRS14] Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. On the Closest Vector Problem with a distance guarantee. In *CCC*, 2014. http://arxiv.org/abs/1409.8063.

[DSSW14] Yevgeniy Dodis, Adi Shamir, Noah Stephens-Davidowitz, and Daniel Wichs. How to eat your entropy and have it too – optimal recovery strategies for compromised RNGs. In *CRYPTO*, 2014. https://eprint.iacr.org/2014/167.

[HCS07] Fraser Chiu Kim Hong, Alex Cloninger, and Noah Stephens-Davidowitz. On link patterns and Alternating Sign Matrices. http://noahsd.com/papers/ASMLinks.pdf, 2007.

[HHSS17] Shai Halevi, Tzipora Halevi, Victor Shoup, and Noah Stephens-Davidowitz. Implementing BP-obfuscation using graph-induced encoding. In *CCS*, 2017. https://eprint.iacr.org/2017/104.

[MS15] Ilya Mironov and Noah Stephens-Davidowitz. Cryptographic Reverse Firewalls. In *Eurocrypt*, 2015. https://eprint.iacr.org/2014/758.

[MS19a] Stephen D. Miller and Noah Stephens-Davidowitz. Kissing numbers and transference theorems from generalized tail bounds. *SIDMA*, 2019. http://arxiv.org/abs/1802.05708.

[MS19b] Tamalika Mukherjee and Noah Stephens-Davidowitz. Lattice reduction for modules, or how to reduce ModuleSVP to ModuleSVP. https://eprint.iacr.org/2019/1142, 2019.

[PRS17] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of Ring-LWE for any ring and modulus. In *STOC*, 2017. https://eprint.iacr.org/2017/258.

[RS17a] Oded Regev and Noah Stephens-Davidowitz. An inequality for Gaussians on lattices. *SIDMA*, 2017. http://arxiv.org/abs/1502.04796.

[RS17b] Oded Regev and Noah Stephens-Davidowitz. A reverse Minkowski theorem. In *STOC*, 2017. http://arxiv.org/abs/1611.05979. Invited to the STOC 2018 special issue of SIAM JoC. Submitted to *Annals of Mathematics* on 2/28/17. Subject of a Bourbaki Seminar by Bost.

[SC07] Noah Stephens-Davidowitz and Alex Cloninger. The Cyclic Sieving Phenomenon on the Alternating Sign Matrices. http://noahsd.com/papers/ASMCSP.pdf, 2007.

[Ste15] Noah Stephens-Davidowitz. Dimension-preserving reductions between lattice problems. http://noahsd.com/latticeproblems.pdf, 2015.

[Ste16a] Noah Stephens-Davidowitz. Discrete Gaussian sampling reduces to CVP and SVP. In *SODA*, 2016. http://arxiv.org/abs/1506.07490.

[Ste16b] Noah Stephens-Davidowitz. Search-to-decision reductions for lattice problems with approximation factors (slightly) greater than one. In *APPROX*, 2016. http://arxiv.org/abs/1512.04138.

[Ste17] Noah Stephens-Davidowitz. *On the Gaussian measure over lattices*. Phd thesis, New York University, 2017. Winner of NYU's Dean's Outstanding Dissertation award in the sciences.

[Ste19] Noah Stephens-Davidowitz. A time-distance trade-off for GDD with preprocessing—Instantiating the DLW heuristic. In *CCC*, 2019. http://arxiv.org/abs/1902.08340.

[SV19] Noah Stephens-Davidowitz and Vinod Vaikuntanathan. SETH-hardness of coding problems. In *FOCS*, 2019. http://eccc.weizmann.ac.il/report/2019/159/.

Related Work

[Ajt04] Miklós Ajtai. Generating hard instances of lattice problems. *Quaderni di Matematica*, 13, 2004.

[AMV15] Giuseppe Ateniese, Bernardo Magri, and Daniele Venturi. Subversion-resilient signature schemes. In *CCS*, 2015.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *SODA*, 2016.

[Bos18] Jean-Benoît Bost. Séminaire N. Bourbaki: Réseaux euclidiens, séries thêta et pentes, 2018. See https://www.youtube.com/watch?v=j7YvtVvv3qs for a video of the lecture (in French).

[BPR14] Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway. Security of Symmetric Encryption against Mass Surveillance. In *CRYPTO*, 2014.

[Bra16] Matt Braithwaite. Experimenting with post-quantum cryptography. https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html, 2016.

[BRSV17] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Average-case fine-grained hardness. In *STOC*, 2017.

[BRSV18] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. Proofs of work from worst-case assumptions. In *CRYPTO*, 2018.

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Eurocrypt*, 2016.

[CDW17] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short Stickelberger class relations and application to Ideal-SVP. In *Eurocrypt*, 2017.

[CGS14] Peter Campbell, Michael Groves, and Dan Shepherd. Soliloquy: a cautionary tale. ETSI 2nd Quantum-Safe Crypto Workshop, 2014.

[CMY+16] Rongmao Chen, Yi Mu, Guomin Yang, Willy Susilo, Fuchun Guo, and Mingwu Zhang. Cryptographic reverse firewall via malleable smooth projective hash functions. In *ASIACRYPT*, 2016.

[Dad19] Daniel Dadush. On approximating the covering radius and finding dense lattice subspaces. In *STOC*, 2019.

[DGG+15] Yevgeniy Dodis, Chaya Ganesh, Alexander Golovnev, Ari Juels, and Thomas Ristenpart. A formal treatment of backdoored pseudorandom generators. In *Eurocrypt*, 2015.

[DR16] Daniel Dadush and Oded Regev. Towards strong reverse Minkowski-type inequalities for lattices. In *FOCS*, 2016.

[FS03] Niels Ferguson and Bruce Schneier. *Practical Cryptography*. John Wiley & Sons, Inc., New York, NY, USA, 1 edition, 2003.

[GO95] Anka Gajentaan and Mark H Overmars. On a class of $o(n^2)$ problems in computational geometry. *Computational Geometry*, 5(3), 1995.

[GO12] Anka Gajentaan and Mark H. Overmars. On a class of $o(n^2)$ problems in computational geometry. *Computational Geometry*, 45(4), 2012.

[HRS09] R. J. Hans-Gill, Madhu Raka, and Ranjeet Sehmi. On conjectures of Minkowski and Woods for n=7. *Journal of Number Theory*, 129(5), 2009.

[HRS11] R. J. Hans-Gill, Madhu Raka, and Ranjeet Sehmi. On conjectures of Minkowski and Woods for n= 8. *Acta Arithmetica*, 147, 2011.

[KL88] Ravi Kannan and László Lovász. Covering minima and lattice-point-free convex bodies. *Annals of Mathematics. Second Series*, 128(3), 1988.

[KR16] Leetika Kathuria and Madhu Raka. On conjectures of Minkowski and Woods for n = 9. In *Mathematical Sciences*, 2016.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *Journal of the ACM*, 60(6), 2013.

[LPSW19] Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. An LLL algorithm for module lattices. In *ASIACRYPT*, 2019.

[LR17] Shachar Lovett and Oded Regev. A counterexample to a strong variant of the polynomial Freiman-Ruzsa conjecture in Euclidean space. *Discrete Analysis*, 2017.

[Mic07] Daniele Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Computational Complexity*, 16(4), 2007.

[Moo18] Dustin Moody. Let's get ready to rumble—the NIST PQC "competition". https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/PQCrypto-April2018_Moody.pdf, 2018.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal of Computing*, 37(1), 2007.

[MV13] Daniele Micciancio and Panagiotis Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. *SIAM Journal on Computing*, 42(3), 2013.

[MZY+18] Hui Ma, Rui Zhang, Guomin Yang, Zishuai Song, Shuzhou Sun, and Yuting Xiao. Concessive online/offline attribute based encryption with cryptographic reverse firewalls—secure and efficient fine-grained access control on corrupted machines. In *ESORICS*, 2018.

[NIS] Computer Security Division NIST. Post-quantum cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[NIS16] NIST. NIST asks public to help future-proof electronic information. https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information, 2016.

[NV08] Phong Q. Nguyen and Thomas Vidick. Sieve algorithms for the Shortest Vector Problem are practical. *Journal of Mathematical Cryptology*, 2(2), 2008.

[PHS19] Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé. Approx-SVP in ideal lattices with pre-processing. In *Eurocrypt*, 2019.

[PR06] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *TCC*, 2006.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6), 2009.

[SW16] Uri Shapira and Barak Weiss. Stable lattices and the diagonal group. *Journal of the European Mathematical Society*, 18(8), 2016.

[Wig18] Avi Wigderson. *Math and Computation*. 2018. https://www.math.ias.edu/avi/book.

[Wika] Wikipedia. Post-quantum cryptography standardization. https://en.wikipedia.org/w/index.php?title=Post-Quantum_Cryptography_Standardization.

[Wikb] Wikipedia. Séminaire Nicolas Bourbaki. https://en.wikipedia.org/w/index.php?title=S%C3%A9minaire_Nicolas_Bourbaki.

[Wil18] Virginia Vassilevska Williams. On some fine-grained questions in algorithms and complexity. In *Proc. of the ICM*, 2018.