QIC 891 Topics in Quantum Safe Cryptography

Module 1: *Post-Quantum Cryptography*

# Lecture 4

*Lecturer: Fang Song* *May 19, 2016*

**Review**. PKE from trapdoor functions. Direct constructions: e.g., Regev's PKE.
**Today**. In the first part, we will introduce what *lattices* are and computational problems (directly) concerning them. In the second part (on slides), we will discuss the (quantum) security of the proposed post-quantum cryptosystems in two aspects: 1) investigate the hardness of solving the computational problems by classical and quantum algorithms; and 2) base security of the cryptosystems against (classical &) quantum attacks on the hard problems in the framework of provable security.

## 1 Lattices & lattice problems

**Definition 1** (Lattice)**.** An $n$-dimensional lattice $\mathscr{L}$ is a discrete (additive) subgroup of $\mathbb{R}$.

Probably the simplest example of a lattice is $\mathbb{Z}^n$. Note that a lattice contains infinitely many points. Nonetheless, it can be generated by *integer* linear combinations of a set of linearly independent (over $\mathbb{R}^n$) vectors $B = \{b_1, \ldots, b_k\}, b_i \in \mathbb{R}^n$ as

$$\mathscr{L} := \mathscr{L}(B) = B \cdot \mathbb{Z}^k = \left\{ \sum_{i=1}^{k} z_i b_i : z_i \in \mathbb{Z} \right\}.$$

$k$ is the *rank* of the latice and we will only be concerned with full-rank lattices (i.e. $k = n$). $B$ is called a basis of $\mathscr{L}$ and it's worth mentioning that a lattice basis is not unique. In fact for any unimodular matrix $U \in \mathbb{Z}^{n\times n}, \det(U) = \pm 1$, $B' = B \cdot U$ is also a basis of $\mathscr{L}(B)$.

A useful quantity is the *minimum distance* of a lattice, which is also the length of a shortest non-zero vector:

$$\lambda_1(\mathscr{L}) := \min_{v \in \mathscr{L}\setminus\{0\}} \|v\|.$$

For an arbitrary point $t \in \mathbb{R}^n$, we define its distance to $\mathscr{L}$ as

$$\mathrm{dist}(t, \mathscr{L}) := \min_{v\in\mathscr{L}} \|v - t\|.$$

### 1.1 Computational problems

The two most important problems in lattices are the *shortest vector problem* (SVP) and the *Bounded-Distance Decoding* (BDD).

**Definition 2** (Shortest Vector Problem (SVP))**.**

- **Given**: a basis of some lattice $\mathscr{L}$.
- **Find**: a shortest lattice vector, i.e. $v \in \mathscr{L}$ with $\|v\| = \lambda_1(\mathscr{L})$.

There are a few common variants of SVP. First of all, we often relax and only ask for an approximate solution.

**Definition 3** (Approximate Shortest Vector Problem ($\mathsf{SVP}_\gamma$))**.**

- **Given**: a basis of some lattice $\mathscr{L}$.
- **Find**: a short vector $v \in \mathscr{L}$ with $\|v\| \le \gamma \cdot \lambda_1(\mathscr{L})$.

$\gamma$ is called the approximation factor and is typically a function $\gamma(n)$ of the dimension $n$.
Of particular importance to cryptography is the decision version of $\mathsf{SVP}_\gamma$, denoted as $\mathsf{GapSVP}_\gamma$.

**Definition 4** (Decisional Approximate Shortest Vector Problem ($\mathsf{GapSVP}_\gamma$))**.**

- **Given**: a basis of some lattice $\mathscr{L}$.
- **Decide**: YES: $\lambda_1(\mathscr{L}) \le 1$ or NO: $\lambda_1(\mathscr{L}) > \gamma$.

The other important problem is called *Bounded-Distance Decoding* (BDD).

**Definition 5** (Bounded Distance Decoding Problem ($\mathsf{BDD}_\gamma$))**.**

- **Given**: a basis of some lattice $\mathscr{L}$ and a target vector $t \in \mathbb{R}^n$.
- **Promise**: $\mathrm{dist}(t, \mathscr{L}) \le d = \lambda_1(\mathscr{L})/(2\gamma(n))$.
- **Find**: the unique closest lattice vector to $t$, i.e., $v \in \mathscr{L}$ such that $\|v - t\| \le d$.

[Exercise: why $v$ is unique?]
BDD is a special case of the *closest vector problem* $\mathsf{CVP}_\gamma$, in which we do not have the distance promise.

## 1.2 Further observations on lattice-based & code-based problems

**$q$-ary lattices and connection to SIS & LWE.** For a matrix $A \in \mathbb{Z}_q^{n\times m}$, define the following two types of lattices

$$\Lambda_q^\perp(A) := \left\{v \in \mathbb{Z}^m : Av = 0 \pmod q\right\},$$
$$\Lambda_q(A) := \left\{v \in \mathbb{Z}^m : v = A^{\mathbf{T}} z \pmod q \text{ for some } z \in \mathbb{Z}^n\right\}.$$

Notice that $q\mathbb{Z}^m \subseteq \Lambda_q^\perp \subseteq \mathbb{Z}^n$ and $q\mathbb{Z}^m \subseteq \Lambda_q \subseteq \mathbb{Z}^n$. We call them $q$-ary lattices.
Then it is easy to see that the (homogeneous) SIS problem is equivalent to the $\mathsf{SVP}_\gamma$ problem in lattice $\Lambda_q^\perp$. Similarly, LWE can be viewed as a BDD instance in lattice $\Lambda_q$ with target $t = As + e \pmod q$ since $e$ is taken to be a "small" error. This means that SIS and LWE are no harder than some (average-case) lattice problems (e.g. $\mathsf{SVP}_\gamma$). More surprisingly and unique to lattice cryptography, we will see in part II (slides) that SIS and LWE are actually as hard as some worst-case lattice problem (e.g. $\mathsf{GapSVP}_\gamma$), i.e., as long as there exists some lattice on which $\mathsf{GapSVP}_\gamma$ is hard, the SIS problem is hard too for a randomly generated $A$.

*Remark* 1. Recall the Type-I trapdoor we defined last time: a "small" $S \in \mathbb{Z}_q^{m\times m}$ such that $AS = 0 \mod q$. Observe that $S$ is a "short-basis" for the lattice $\Lambda_q^\perp(A)$. This is why we ususally call $S$ a "short-basis" trapdoor, which one can use for solving BDD on $\Lambda_q^\perp(A)$ for instance.

**Duality**. Consider the functions induced by SIS and LWE:

$$A \in \mathbb{Z}_q^{n\times m} : f_A(x) := Ax \pmod q; \quad g_{A^T}(s,e) = A^T s + e \pmod q.$$

In fact, $f_A$ and $g_{A^T}$ are the same function under different parameter sets. Basically they are both derived from BDD where the distance is greater than the covering radius which leads to a surjective function $f_A$ in SIS, whereas in LWE the distance is smaller than $\lambda_1/2$, leading to a unique closest vector and hence an injective function. Detailed discussion can be found in [Mic10]. We show a similar equivalence for coding problems as a motivating example.

Let $H$ and $G$ be the parity check matrix and generating matrix for some binary linear code $(n, k, d)$ written in the systematic form:

$$H = \left(1_{n-k} | Q_{(n-k)\times k}\right) \in \mathbb{F}_2^{(n-k)\times n}; \quad G = (Q_{(n-k)\times k} | 1_k)^T \in \mathbb{F}_2^{n\times k}.$$

$1_j$ represents the identity matrix of dimension $j$.

Recall the functions induced from the syndrome decoding (SD) and codeword decoding (CD) problems:

$$f_H(x) := Hx; \quad g_G(s, e) = Gs + e.$$

- CD → SD ($g \to f$): Suppose we are given $y = f_H(x)$. Notice that $f_H(x) = \left(1_{n-k} | Q_{(n-k)\times k}\right) x = x_1 + Qx_2$ where $x_1$ and $x_2$ are the first $n-k$ and remaining $k$ coordinates of $x$ respectively. Hence this can be seen as a CD instance $g_Q(x_2, x_1)$, and we can recover $x$ if we can invert $g_Q$ to find $x_2$ and $x_1$.
- SD → CD ($f \to g$): Suppose we are given $y = g_G(s, e)$. If we multiply $H$, we get

  $$z := Hy = H(Gs + e) = He,$$

  since $HG = 0$. Therefore, we have a SD instance. We can compute $e$ if we can invert $f_H$ and recover $s$ as well.

## References for Part II in the slides

**Complexity and algorithms**.

- **Lattices**
  - **Hardness results**: NP-hard for approximate SVP [Ajt98, Mic01, Kho05, Pei08].
  - **worst-case to average-casae reductions**: worst-case lattice problems to SIS [Ajt96, MR07]. Worst-case lattice problems to LWE [Reg09, Pei09, BLP+13].
  - **Lattice reduction algorithms**: [LLL82, Sch87, CN11] and many more
  - **Exact SVP algorithms** enumeration, good performance in practice in small dimension [Kan83, GNR10], sieving [AKS01, MV10, MV13], Discrete Gaussian Sampling a special type of sieving which gives the best asymptotic performance ($2^n$ time & space) [ADRSD15].
  - **Quantum algorithms & attacks**: applying Grover search [LMVDP15]; quantum algorithms for problems in (high-degree) number fields including in particular the principal ideal problem (PIP) [EHKS14, BS16]; attacks on lattice cryptosystems based on the short-generator-PIP [CGS14, BS15, CDPR15]. unique-SVP and BDD reduces to dihedral coset problem [Reg04b].
- **Codes**
  - **Hardness results**: NP-hard to decode general linear codes [BMVT78, Var97]; NP-hard for approximate decoding [DMS03, FM04, REG04a]; NP-hard for (high-error) Reed-Solomon code [GV05].
  - **Algorithms**: Information set decoding [LB88, Leo88, Ste88, BJMM12]; a distinguisher for high-rate McEliece systems [FGUO+13]; support splitting algorithm for code equivalence [Sen00].

  - **Quantum algorithms**: Connection to (a seemingly hard instance of) the Hidden subgroup Problem, viewd as quantum-resistance of McEliece scheme [DMR11].

- **MQ**
  - **Hardness results**: NP-hard in worst-case [Stu02].
  - **Algorithms**: computing Gröbner basis [Buc06, BFS03, EF14], algorithms for isomporphism of polynomials [Pat96, BFV13].

**Provable Quantum Security**.

- **Quantum security models**: [Unr10, Son14, HSS15].
- **Quantum rewinding and cryptographic protocols**: a quantum rewinding lemma and zero-knowledge proofs for NP [Wat09]; 2-party computation [LN11, HSS11, FKS+13].
- **Quantum random-oracle**: proposed in [BDF+11], proof techniques developed in [Zha12, ES15, Unr15, HRS16].

## References


[ADRSD15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in $2^n$ time using discrete gaussian sampling. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 733–742. ACM, 2015.

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108. ACM, 1996.

[Ajt98] Miklós Ajtai. The shortest vector problem in l 2 is np-hard for randomized reductions. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pages 10–19. ACM, 1998.

[AKS01] Miklós Ajtai, Ravi Kumar, and Dandapani Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings of the Thirty-third annual ACM symposium on Theory of computing*, pages 601–610. ACM, 2001.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Advances in Cryptology–ASIACRYPT 2011*, pages 41–69. Springer, 2011.

[BFS03] Magali Bardet, Jean-Charles Faugere, and Bruno Salvy. Complexity of Gröbner basis computation for semi-regular overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$, 2003. Tech Report available at `https://hal.inria.fr/inria-00071534`.

[BFV13] Charles Bouillaguet, Pierre-Alain Fouque, and Amandine Véber. Graph-theoretic algorithms for the "isomorphism of polynomials" problem. In *Advances in Cryptology–EUROCRYPT 2013*, pages 211–227. Springer, 2013.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How 1+ 1= 0 improves information set decoding. In *Advances in Cryptology–EUROCRYPT 2012*, pages 520–536. Springer, 2012.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the Forty-Fifth annual ACM symposium on Theory of computing*, pages 575–584. ACM, 2013.

[BMVT78] Elwyn R Berlekamp, Robert J McEliece, and Henk CA Van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

[BS15] Jean-François Biasse and Fang Song. On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in $\mathbb{Q}(\zeta_{p^n})$. Tech Report CACR 2015-12, September 2015.

[BS16] Jean-François Biasse and Fang Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 893–902. SIAM, 2016.

[Buc06] Bruno Buchberger. Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of symbolic computation*, 41(3):475–511, 2006.

[CDPR15] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. Cryptology ePrint Archive, Report 2015/313, October 2015.

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

[CN11] Yuanmi Chen and Phong Q Nguyen. Bkz 2.0: Better lattice security estimates. In *Advances in Cryptology–ASIACRYPT 2011*, pages 1–20. Springer, 2011.

[DMR11] Hang Dinh, Cristopher Moore, and Alexander Russell. Mceliece and Niederreiter cryptosystems that resist quantum fourier sampling attacks. In *Advances in Cryptology–Crypto 2011*, pages 761–779. Springer, 2011.

[DMS03] Ilya Dumer, Daniele Micciancio, and Madhu Sudan. Hardness of approximating the minimum distance of a linear code. *Information Theory, IEEE Transactions on*, 49(1):22–37, 2003. Preliminary version in FOCS 1999.

[EF14] Christian Eder and Jean-Charles Faugere. A survey on signature-based Gröbner basis computations. *arXiv preprint arXiv:1404.1774*, 2014.

[EHKS14] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *Proceedings of the 46th STOC*, pages 293–302. ACM, 2014.

[ES15] Edward Eaton and Fang Song. Making existential-unforgeable signatures strongly unforgeable in the quantum random-oracle model. In *10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)*, pages 147–162, 2015.

[FGUO$^+$13] Jean-Charles Faugere, Valérie Gauthier-Umana, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. A distinguisher for high-rate McEliece cryptosystems. *Information Theory, IEEE Transactions on*, 59(10):6830–6844, 2013.

[FKS$^+$13] Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou, and Vassilis Zikas. Feasibility and completeness of cryptographic tasks in the quantum world. In *Theory of Cryptography*, pages 281–296. Springer, 2013.

[FM04] Uriel Feige and Daniele Micciancio. The inapproximability of lattice and coding problems with preprocessing. *Journal of Computer and System Sciences*, 69(1):45–67, 2004. Preliminary version in CCC 2002.

[GNR10] Nicolas Gama, Phong Q Nguyen, and Oded Regev. Lattice enumeration using extreme pruning. In *Advances in Cryptology–EUROCRYPT 2010*, pages 257–278. Springer, 2010.

[GV05] Venkatesan Guruswami and Alexander Vardy. Maximum-likelihood decoding of reed-solomon codes is NP-hard. *Information Theory, IEEE Transactions on*, 51(7):2249–2256, 2005. Preliminary version in SODA 2005.

[HRS16] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. In *Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I*, pages 387–416, 2016.

[HSS11] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. In *Advances in Cryptology–Crypto 2011*, pages 411–428, 2011.

[HSS15] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. *International Journal of Quantum Information*, 13(04):1550028, 2015. Preliminary version appeared in Crypto'11.

[Kan83] Ravi Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the Fifteenth annual ACM symposium on Theory of computing*, pages 193–206. ACM, 1983.

[Kho05] Subhash Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM (JACM)*, 52(5):789–808, 2005. Preliminary version in FOCS 2003.

[LB88] Pil Joong Lee and Ernest F Brickell. An observation on the security of mceliece's public-key cryptosystem. In *Advances in Cryptology–EUROCRYPT 1988*, pages 275–280. Springer, 1988.

[Leo88] Jeffrey S Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. *IEEE Transactions on Information Theory*, 34(5):1354–1359, 1988.

[LLL82] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[LMVDP15] Thijs Laarhoven, Michele Mosca, and Joop Van De Pol. Finding shortest lattice vectors faster using quantum search. *Designs, Codes and Cryptography*, 77(2-3):375–400, 2015.

[LN11] Carolin Lunemann and Jesper Buus Nielsen. Fully simulatable quantum-secure coin-flipping and applications. In *AFRICACRYPT*, pages 21–40, 2011.

[Mic01] Daniele Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM journal on Computing*, 30(6):2008–2035, 2001. Preliminary version in FOCS 1998.

[Mic10] Daniele Micciancio. Duality in lattice cryptography. Invited talk at Public Key Cryptography, 2010. Slides available at `https://cseweb.ucsd.edu/~daniele/papers/DualitySlides.pdf`.

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007. Preliminary version in FOCS 2004.

[MV10] Daniele Micciancio and Panagiotis Voulgaris. Faster exponential time algorithms for the shortest vector problem. In *Proceedings of the Twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, pages 1468–1480. Society for Industrial and Applied Mathematics, 2010.

[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):1364–1391, 2013. Preliminary version in STOC 2010.

[Pat96] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *Advances in Cryptology–EUROCRYPT 1996*, pages 33–48. Springer, 1996.

[Pei08] Chris Peikert. Limits on the hardness of lattice problems in $\ell_p$ norms. *Computational Complexity*, 17(2):300–351, 2008.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of the Forty-First annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2009.

[REG04a] Oded REGEV. Improved inapproximability of lattice and coding problems with preprocessing. *IEEE transactions on information theory*, 50(9):2031–2037, 2004. Preliminary version in CCC 2003.

[Reg04b] Oded Regev. Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760, 2004.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.

[Sch87] Claus-Peter Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical computer science*, 53(2):201–224, 1987.

[Sen00] Nicolas Sendrier. Finding the permutation between equivalent linear codes: The support splitting algorithm. *Information Theory, IEEE Transactions on*, 46(4):1193–1203, 2000.

[Son14] Fang Song. A note on quantum security for post-quantum cryptography. In *Proceedings of the 6th International Workshop on Post-Quantum Cryptography*, volume 8772 of *Lecture Notes in Computer Science*, pages 246–265. Springer, 2014.

[Ste88] Jacques Stern. A method for finding codewords of small weight. In *Coding theory and applications*, pages 106–113. Springer, 1988.

[Stu02] Bernd Sturmfels. *Solving systems of polynomial equations*. Number 97. American Mathematical Soc., 2002.

[Unr10] Dominique Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology–EUROCRYPT 2010*, pages 486–505. Springer, 2010.

[Unr15] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Advances in Cryptology-EUROCRYPT 2015*, pages 755–784. Springer, 2015.

[Var97] Alexander Vardy. The intractability of computing the minimum distance of a code. *IEEE Transactions on Information Theory*, 43(6):1757–1766, 1997.

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version in STOC 2006.

[Zha12] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In *Proceedings of CRYPTO 2012*, 2012.