Post Quantum Cryptography: An Introduction

Shweta Agrawal*

IIT Madras

1 Introduction

Cryptography is a rich and elegant field of study that has enjoyed enormous success over the last few decades. At a very high level, cryptography is the science of designing methods to achieve certain secrecy goals, for instance that of hiding information, so that learning the message from a cryptographically sealed envelope implies a solution to some well known mathematical problem. By suitably choosing the underlying mathematical problems to be intractable, we may rest assured that an attacker's chances of learning secret information are extremely small: in particular, she must outperform all the mathematical minds that have attempted without success to solve the underlying problem in order to learn the secret. Choosing the underlying hard problem is thus of paramount importance, and we would like to have strong evidence that current day computing resources do not permit an attacker to solve the problem in any reasonable time.

Here, the terms "current day computing resources" and "reasonable time" warrant further investigation. What is considered as reasonable time depends on the application: for securing credit card transactions, we may expect that an attacker will not spend ten years to break secrecy, but this may not be reasonable for highly sensitive defence communications. The question of computing resources is even more delicate: does the adversary have access to a mobile phone, a laptop, a cluster of computers or a supercomputer? While again the answer to this question depends on the application, the subject of this note is the very model of computation. Traditionally, cryptography has been based on problems that are conjectured to be infeasible in the realm of classical computers. However, recent times have seen significant advances in

*Email: shweta@iitm.ac.in

the design and construction of *quantum computers*, which are more powerful than classical computers. If an attacker has access to a quantum computer, are known cryptosystems safe?

Two of the most popular problems underlying most current day cryptography are the integer factorization problem and the discrete logarithm problem, please see [Gol00] for a discussion. While the best known classical algorithms to solve these problems take exponential time, a breakthrough work by Shor [Sho94] demonstrated that they can be solved in *quantum* polynomial time. Thus, in the realm of quantum computers, most current day cryptography breaks down. It is therefore necessary to base cryptography of the future on problems that remain intractable against quantum computers. While it is unclear when quantum computers will become a reality, recent times have seen significant strides in this area and it is widely accepted that developing cryptosystems that are secure against quantum computers is an urgent need. To address this, the "National Institute of Standards and Technology" (NIST), a unit of the U.S. commerce department, initiated a process to "solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms" [CJL+].

In this note, we do not discuss the progress made in constructing quantum computers, nor the differences between classical and quantum computing. Instead, we study some problems that are conjectured to be quantum hard, and discuss some applications to cryptography.

2 Directions for Post Quantum Cryptography

At a high level, the mathematical problems underlying post-quantum cryptography may be categorized into the following broad families:

Lattice Based Cryptography. Of all known candidates for post quantum cryptography, perhaps the most popular is lattice based cryptography. Informally, a lattice is a set of points in an n dimensional space with a periodic structure. Lattices occur everywhere, from crystals to stacks of fruit to ancient Islamic art, and have been widely studied, starting with ancient mathematicians such as Lagrange, Minkowski and Gauss upto modern computer scientists. A lattice may be represented using a basis that generates its points, and given a basis, the most basic question that may be posed is that of finding the smallest nonzero point in the corresponding lattice. This classic problem is known as the shortest vector problem (or SVP) and is related to many other lattice problems as we shall see subsequently.

Despite substantial research effort, no efficient quantum algorithms are known for lattice problems that outperform classical ones significantly. In fact, the only advantage quantum computers offer in this regard are modest generic speedups. Besides, lattice based cryptography has many other advantages. Cryptosystems based on lattices are often algorithmically simple, efficient and highly paralellizable. Moreover, lattice based cryptography enjoys a surprising connection between average case and worst case hardness [Ajt96] which makes it especially attractive. In more detail, cryptography is based on average case intractable problems, which means that randomly chosen instances of problem must be difficult to solve. On the other hand, complexity theory usually studies worst case hardness, where a problem is considered hard if there merely exists an intractable instance of the problem. In a surprising work, Ajtai [Ajt96] showed that certain lattice problems are hard on the average if some related lattice problems are hard in the worst case. This allows for the design of cryptographic schemes that are infeasible to break unless *all* instances of certain lattice problems are hard to solve.

We discuss hard lattice problems and their application to cryptography in more detail in subsequent sections.

Multivariate Polynomial Cryptography. Another family of problems that is believed to resist quantum computers is related to solving nonlinear equations over a finite field. Cryptosystems that rely on such problems for their security are clubbed under the banner of "multivariate polynomial cryptography" [MI88, BFSS13, Wol05, DY09]. In more detail, the multivariate quadratic polynomial problem, denoted by MQ, is: given m quadratic polynomials $f_1, \ldots, f_m$ in n variables $x_1, \ldots, x_n$, with coefficients chosen from a field $\mathbb{F}$, find a solution $\mathbf{z} \in \mathbb{F}^n$ such that $f_i(\mathbf{z}) = 0$ for $i \in [m]$. Evidently, the parameters are chosen so that simple attacks such as linearization do not apply. Indeed, in the worst case, this problem is known to be NP hard.

The birth of multivariate polynomial cryptography took place in 1988, in an encryption scheme proposed by T. Matsumoto and H. Imai [MI88]. While this scheme was subsequently broken, the general principle found applicability in many subsequent constructions, such as the "Hidden Field Equations" by Patarin [Pat96] or "Unbalanced Oil and Vinegar" [KPG99]. Presently, there exist candidates for secure cryptosystems based on this class of problems that are believed to be quantum secure.

We refer the reader to [Has18] for a detailed survey.

Code Based Cryptography. Code based cryptography uses the theory of error correcting codes to construct cryptosystems. The first candidate of such a cryptosystem was by McEliece [McE78], based on the hardness of decoding a general linear code, a problem which is known to be NP-hard. To construct the secret key, an error-correcting code is chosen for which an efficient decoding algorithm is known, and which is able to correct up to t errors. The public key is derived from the private key by disguising the selected code as a general linear code. The encryptor generates a codeword using the public key, perturbed by upto t errors. The decryptor recovers the message by performing error correction and efficient decoding of the codeword. The security of the above construction depends heavily on the choice of the error correcting code used in the construction: to the best of our knowledge, constructions using Goppa codes have remained resilient to attack [OS09]. Traditionally the McEliece cryptosystem did not find much deployment due to its large keys and ciphertexts. But there is renewed interest in this family of constructions due to their quantum resilience.

Hash Based Cryptography. Hash based cryptography is a general name given to cryptosystems which derive their hardness from hash functions. The simplest and most well known example of a hash based cryptosystem is the signature scheme by Merkle [Mer79], which converts a weak signature scheme to a strong one, using hash functions. In more detail, the transformation begins with a signature scheme which is only secure for signing a single message and converts it into a many time signature scheme using the so called "Merkle tree structure" and by relying only on the existence of hash functions. Since one time signatures can be based simply on the existence of one way functions, the security of these constructions is well understood even in the quantum setting. However, the efficiency and generality of hash based cryptography is restricted, and this limits its popularity.

3 Lattice Based Cryptography

To give the reader a deeper taste of post quantum cryptography, we focus our attention on lattice based cryptography for the remainder of this note. To begin, let us define a lattice formally.

Definition 3.1. An *m-dimensional lattice* Λ is a full-rank discrete subgroup of $\mathbb{R}^m$. A *basis* of Λ is a linearly independent set of vectors whose integer linear combinations generate Λ. In cryptography, we are usually concerned with *integer lattices*, i.e., those whose points have coordinates in $\mathbb{Z}^m$.

Among these lattices are the "q-ary" lattices defined as follows: for any integer $q \geq 2$ and any $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, we define

$$:= \quad \left\{ \mathbf{e} \in \mathbb{Z}^m : \mathbf{A} \cdot \mathbf{e} = \mathbf{0} \bmod q \right\}$$

These lattices are of special interest in cryptography.

The *minimum* distance of a lattice Λ is the length of a shortest nonzero vector:

$$\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \{0\}} \|\mathbf{v}\|$$

Here, $\|\cdot\|$ denotes the Euclidean norm. In general, the i^{th} successive minima $\lambda_i(\Lambda)$ is the smallest radius r such that Λ has i linearly independent vectors of norm at most r.

3.1 Classic Computational Lattice Problems

In this section, we discuss some classic computational problems over lattices.

Definition 3.2 (Shortest Vector Problem (SVP))**.** Given an arbitrary basis $\mathcal{B}$ of some lattice $\Lambda = \Lambda(\mathcal{B})$, find a nonzero vector $\mathbf{v} \in \Lambda(\mathcal{B})$ such that $\|\mathbf{v}\| = \lambda_1(\Lambda(\mathcal{B}))$.

We note that there is a bound on $\lambda_1(\Lambda(\mathcal{B}))$ by Minkowski's first theorem, which states that for any full rank lattice $\Lambda(\mathcal{B})$ of rank n,

$$\lambda_1(\Lambda(\mathcal{B})) \leq \sqrt{n} \ (\det(\Lambda(\mathcal{B}))^{\frac{1}{n}}$$

Next, we define the approximate version of this problem. Let $\gamma \geq 1$ be an approximation factor; this is typically taken as a function of the lattice dimension n.

Definition 3.3 (Approximate Shortest Vector Problem (SVP_γ))**.** Given a basis $\mathcal{B}$ of an n dimensional lattice $\Lambda = \Lambda(\mathcal{B})$, find nonzero vector $\mathbf{v} \in \Lambda(\mathcal{B})$ s.t. $\|\mathbf{v}\| \leq \gamma \cdot \lambda_1(\Lambda(\mathcal{B}))$.

Of particular importance in cryptography is the decision version of the approximate shortest vector problem, which we define next.

Definition 3.4 (Decisional Shortest SVP (GapSVP_γ))**.** Given a basis $\mathcal{B}$ of an n dimensional lattice and the promise that either $\lambda_1(\Lambda(\mathcal{B})) \leq 1$ or $\lambda_1(\Lambda(\mathcal{B})) \geq \gamma$, determine which is the case.

Definition 3.5 (Shortest Independent Vector Problem (SIVP_γ))**.** Given a basis $\mathcal{B}$ of a full rank, n dimensional lattice $\Lambda = \Lambda(\mathcal{B})$, output a set of n linearly independent lattice vectors vectors $S = \{\mathbf{s}_i\}_{i \in [n]}$ s.t. for $i \in [n]$,

$$\|\mathbf{s}_i\| \leq \gamma \cdot \lambda_n(\Lambda(\mathcal{B}))$$

Finally, we define the "bounded distance decoding" problem, which takes as input a lattice Λ and a target point $\mathbf{t}$, with the promise that $\mathbf{t}$ is "close" to Λ, and asks to find the lattice point closest to $\mathbf{t}$.

Definition 3.6 (Bounded Distance Decoding Problem (BDD_γ))**.** Given a basis $\mathcal{B}$ of an n dimensional lattice $\Lambda = \Lambda(\mathcal{B})$ and a target point $\mathbf{t} \in \mathbb{R}^n$ with the promise that $dist(\Lambda, \mathbf{t}) < d = \lambda_1(\Lambda(\mathcal{B}))/(2 \cdot \gamma)$, find the unique lattice point $\mathbf{v}$ such that $\|\mathbf{t} - \mathbf{v}\| < d$.

Hardness and effect on cryptography. Most of the above problems are known to be NP-hard to solve exactly as well as for sub-polynomial approximation factors. However, cryptographic constructions rely on the hardness of the above problems for polynomial approximation factors, which place them in the realm of NP $\cap$ co-NP. Even for polynomial approximation factors however, we believe these problems are intractable; indeed, no efficient algorithms are known even for sub-exponential approximation factors despite significant research effort by the community. We refer the reader to [Pei16] for an in-depth discussion.

Early lattice based cryptosystems such as by Ajtai and Dwork [AD97], Goldreich, Goldwasser and Halevi [GGH97], and Regev [Reg04] were based on the above problems or variants thereoff. While these were important theoretical breakthroughs and introduced ideas that form the cornerstone of lattice based cryptographic design even today, they were subsequently replaced by simpler systems relying on hardness of a different set of lattice problems, which may be seen as "better suited" for cryptographic design. We discuss these next.

3.2 Modern Computational Lattice Problems

Most modern cryptosystems rely on the hardness of the following problems.

Short Integer Solution Problem (SIS). The short integer solution problem was introduced by Ajtai [Ajt96] and is defined below.

Definition 3.7 (Short Integer Solution ($\mathsf{SIS}_{\mathsf{n},\mathsf{m},\mathsf{q},\beta}$))**.** Given a uniformly chosen matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and a real valued parameter β, find a nonzero integer vector $\mathbf{e} \in \mathbb{Z}^m$ s.t.

$$\mathbf{A}\,\mathbf{e} = 0 \mod q \quad \text{and} \quad \|\mathbf{e}\| \leq \beta$$

Note that the SIS problem can be seen as an average case short vector problem on the q-ary lattice $\Lambda_q^{\perp}(\mathbf{A})$ defined above.

Definition 3.8 (Inhomogeneous Short Integer Solution ($\mathsf{ISIS}_{\mathsf{n},\mathsf{m},\mathsf{q},\beta}$))**.** Given a uniformly chosen matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, a uniformly chosen vector $\mathbf{u} \leftarrow \mathbb{Z}_q^n$ and a real valued parameter β, find a nonzero integer vector $\mathbf{e} \in \mathbb{Z}^m$ s.t.

$$\mathbf{A}\,\mathbf{e} = \mathbf{u} \mod q \quad \text{and} \quad \|\mathbf{e}\| \leq \beta$$

The SIS and ISIS problem can be seen as essentially equivalent, and related to the classic GapSVP problem as follows.

Theorem 3.9. *[Ajt96, MR07, GPV08, MP13] For $m = \mathrm{poly}(n)$, any $\beta > 0$, and sufficiently large $q \geq \beta \cdot \mathrm{poly}(n)$, solving the (average case) $\mathsf{SIS}_{\mathsf{n},\mathsf{m},\mathsf{q},\beta}$ (or $\mathsf{ISIS}_{\mathsf{n},\mathsf{m},\mathsf{q},\beta}$) problem with non-negligible probablity is at least as hard as solving the decisional approximate shortest vector problem GapSVP_γ and the approximate shortest independent vectors problem SIVP_γ on arbitrary n-dimensional lattices (i.e. in the worst case) with overwhelming probability, for some $\gamma = \beta \cdot \mathrm{poly}(n)$.*

We refer the reader to [Pei16] for a detailed discussion regarding the reductions.

While the SIS and ISIS problem can be used to construct primitives like one way functions, collision resistant hash functions and signatures, public-key encryption (and beyond) require the so-called "Learning With Errors" problem LWE [Reg09] or its ring variant RLWE [LPR10]. We define these next.

Definition 3.10 (LWE)**.** Let $q = q(n) \geq 2$ be an integer and let $\chi = \chi(n)$ be a distribution over $\mathbb{Z}$. The $\mathsf{LWE}_{\mathsf{n},\mathsf{q},\chi}$ problem is to distinguish the following two distributions: in the first distribution, sample $(\mathbf{a}_i, b_i)$ uniformly from $\mathbb{Z}_q^{n+1}$. In the second distribution, one first draws $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ uniformly and then samples $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^{n+1}$ by sampling $\mathbf{a}_i \leftarrow \mathbb{Z}_q^n$ uniformly, $e_i \leftarrow \chi$ and setting $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i$. The $\mathsf{LWE}_{\mathsf{n},\mathsf{q},\chi}$ assumption is that the $\mathsf{LWE}_{\mathsf{n},\mathsf{q},\chi}$ problem is infeasible.

We will also need the definition of a B-bounded distribution.

Definition 3.11 (B-bounded distribution)**.** A distribution ensemble $(\chi_n)_{n\in\mathbb{N}}$ is called B-bounded if

$$\Pr_{e\leftarrow\chi_n}(\|e\| > B) = \mathrm{negl}(n)$$

Here, $\mathrm{negl}(\cdot)$ refers to a function that decreases faster than the inverse of any polynomial.

Regev [Reg09] proved that for certain moduli q and certain bounded error distributions χ, the $\mathsf{LWE}_{\mathsf{n},\mathsf{q},\chi}$ assumption is true as long as certain worst-case lattice problems are hard to solve using a quantum algorithm. This result was de-quantized by Peikert for exponential modulus [Pei09] and by Brakerski, Langlois, Peikert, Regev, Oded and Stehlé for polynomial modulus [BLP+13].

Theorem 3.12. *For integer dimension n, prime integer q and integer $B \geq 2n$, there is an efficiently sampleable B bounded distribution χ such that if there exists an efficient (possibly quantum) algorithm that solves $\mathsf{LWE}_{\mathsf{n},\mathsf{q},\chi}$, then there is an efficient quantum algorithm for solving $\tilde{O}(qn^{1.5}/B)$ approximate worst case* SIVP *and* GapSVP*.*

Next, we define the ring variant of the LWE problem, which yields more efficient cryptosystems than LWE.

Definition 3.13 (Ring Learning With Errors (RLWE))**.** Let $f(x) = x^n + 1$ where n is a power of 2. Let $q = q(n)$ be an integer. Let $R = \mathbb{Z}[x]/f(x)$ and let $R_q = R/qR$. Let χ be a probability distribution on R. For $s \in R_q$, let $A_{s,\chi}$ be the probability distribution on $R_q \times R_q$ obtained by choosing an element $a \in R_q$ uniformly at random, choosing $e \leftarrow \chi$ and outputting $(a, a \cdot s + e)$. The decision $\mathsf{RLWE}_{n,q,\chi}$ problem is to distinguish between samples that are either (all) from $A_{s,\chi}$ or (all) uniformly random in $R_q \times R_q$. The $\mathsf{RLWE}_{\mathsf{n},\mathsf{q},\chi}$ assumption is that the $\mathsf{RLWE}_{\mathsf{n},\mathsf{q},\chi}$ problem is infeasible.

Theorem 3.14 ([LPR10])**.** *Let $r \geq \omega(\sqrt{\log n})$ be a real number and let R, q be as above. Then, there is a randomized reduction from $2^{\omega(\log n)} \cdot (q/r)$ approximate* RSVP *to $\mathsf{RLWE}_{n,q,\chi}$ where χ is the discrete Gaussian distribution with parameter r. The reduction runs in time* $\mathrm{poly}(n, q)$*.*

NTRU. Another popular hardness assumption is the **NTRU** assumption defined by [HPS98] which roughly states that it is hard to distinguish a fraction of small elements over R_q from random.

Definition 3.15 ($\mathsf{NTRU}_{q,\chi}$)**.** The NTRU problem $\mathsf{NTRU}_{q,\chi}$ is to distinguish between the following two distributions: in the first distribution sample a polynomial $h = g/f$ where $f, g \leftarrow \chi$, conditioned on f being invertible in R_q and in the second distribution sample a polynomial h uniformly over R_q.

Stehlé and Steinfeld [SS11] showed that the $\mathsf{NTRU}_{q,\chi}$ problem is hard even for unbounded adversaries for χ chosen as the discrete Gaussian distribution with parameter $r > \sqrt{q} \cdot \mathrm{poly}(n)$. However, it is more useful to make the assumption for much smaller $r = \mathrm{poly}(n)$ as in [LATV12].

4 Cryptographic Constructions

In this section, we discuss how the aforementioned hardness assumptions can be used to design cryptosystems. Due to space constraints we restrict our attention to the primitive of encryption. We describe the public key encryption system based on LWE defined by Regev [Reg09].

4.1 Public Key Encryption

Recall the notion of public key encryption. At a high level, a public key encryption scheme consists of the following algorithms:

$\mathsf{Setup}(1^n)$: This algorithm takes as input the security parameter (which can be used to fine tune the efficiency-security tradeoff in any construction) and outputs a public key PK and a secret key SK.

$\mathsf{Encrypt}(\mathsf{PK}, M)$: This algorithm takes as input public key PK and a message $M \in \{0,1\}$, and outputs a ciphertext CT.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}, \mathsf{CT})$: This algorithm takes as input the public key PK, the secret key SK and a ciphertext CT and outputs a message M or $\perp$.

Correctness requires that if $(\mathsf{PK}, \mathsf{SK})$ are generated honestly using Setup and CT is generated honestly using $\mathsf{Encrypt}$ on inputs (PK, M), then $\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}, \mathsf{CT})$ yields M as desired. Security requires that an encryption of M_0 is indistinguishable from an encryption of M_1 for any M_0, M_1.

We proceed to describe a public key encryption system designed by Regev [Reg09], whose hardness is based on the LWE problem.

$\mathsf{Setup}(1^n)$: On input a security parameter n do:

1. Choose a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$.
2. Choose a uniformly random $\mathbf{s} \xleftarrow{\mathrm{R}} \mathbb{Z}_q^n$.
3. Choose a noise vector $\mathbf{e} \leftarrow \chi^m$.
4. Set $\mathbf{b} = \mathbf{A}^\mathsf{T} \cdot \mathbf{s} + \mathbf{e}$.

Output $\mathsf{PK} = (\mathbf{A}, \mathbf{b})$ and $\mathsf{SK} = \mathbf{s}$.

$\mathsf{Encrypt}(\mathsf{PK}, M)$: On input public parameters PK and a message $M \in \{0,1\}$, do:

1. Choose a uniformly random vector $\mathbf{r} \xleftarrow{\mathrm{R}} \{0,1\}^m$.
2. Compute $\mathbf{c}_0 = \mathbf{A} \cdot \mathbf{r}$ and $c_1 = \mathbf{r}^\mathsf{T}\mathbf{b} + M\lfloor \frac{q}{2} \rfloor$.

Output the ciphertext $\mathsf{CT} := (\mathbf{c}_0, c_1)$.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}, \mathsf{CT})$: On input the public parameters PK, the secret key $\mathsf{SK} = \mathbf{s}$ and a ciphertext $\mathsf{CT} = (\mathbf{c}_0, c_1)$, do:

1. Let $d = c_1 - \mathbf{c}_0^\mathsf{T}\mathbf{s}$.
2. If d is closer to $q/2$ than to 0 output 1, else output 0.

Correctness. To see that the encryption scheme is correct, we walk through the steps of decryption:

$$\begin{aligned} d &= c_1 - \mathbf{c}_0^\mathsf{T}\mathbf{s} \\ &= \left(\mathbf{r}^\mathsf{T}\mathbf{b} + M\lfloor \frac{q}{2} \rfloor\right) - \left(\mathbf{A} \cdot \mathbf{r}\right)^\mathsf{T}\mathbf{s} \\ &= \mathbf{r}^\mathsf{T}(\mathbf{A}^\mathsf{T} \cdot \mathbf{s} + \mathbf{e}) + M\lfloor \frac{q}{2} \rfloor - \mathbf{r}^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{s} \\ &= \mathbf{r}^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{r}^\mathsf{T}\mathbf{e} + M\lfloor \frac{q}{2} \rfloor - \mathbf{r}^\mathsf{T}\mathbf{A}^\mathsf{T}\mathbf{s} \\ &= \mathbf{r}^\mathsf{T}\mathbf{e} + M\lfloor \frac{q}{2} \rfloor \end{aligned}$$

Since $\mathbf{r}$ is binary and $\mathbf{e}$ is chosen from a bounded distribution, it is possible to set the parameters so that $\mathbf{r}^\mathsf{T}\mathbf{e}$ is significantly smaller than $q/2$ and can be rounded off to recover the bit M.

Security. Security relies on the LWE assumption. Note that by the leftover hash lemma [BDK+11], for $m > 2n \log q$ and randomly chosen $\mathbf{r}$, the product $\mathbf{A} \cdot \mathbf{r} = \mathbf{u}$ (say) is uniform. Then, we observe that the ciphertext $(\mathbf{c}_0, c_1)$ is sampled from the LWE distribution as $(\mathbf{u}, \mathbf{u}^\intercal \mathbf{s} + \mathbf{r}^\intercal \mathbf{e} + M\lfloor \frac{q}{2} \rfloor)$, which by the LWE assumption is indistinguishable from uniform $(\mathbf{u}, v)$ which implies that M is hidden.

5 Conclusions

We presented a very high level overview of post quantum cryptography, with a focus on lattice based cryptography. This note is too short to contain anything beyond a flavour of the topic of discussion, which is as deep as it is beautiful. We refer the reader to [Pei16] for an excellent survey of lattice based cryptography and to [CJL+, OS09] for more details on post quantum cryptography at large.

References

[AD97] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 284–293. ACM, 1997.

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, 1996.

[BDK+11] Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, François-Xavier Standaert, and Yu Yu. Leftover hash lemma, revisited. In *Annual Cryptology Conference*, pages 1–20. Springer, 2011.

[BFSS13] Magali Bardet, Jean-Charles Faugere, Bruno Salvy, and Pierre-Jean Spaenlehauer. On the complexity of solving quadratic boolean systems. *Journal of Complexity*, 29(1):53 – 75, 2013.

[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*, STOC '13. ACM, 2013.

[CJL+] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. Report on post-quantum cryptography. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf.

[DY09] Jintai Ding and Bo-Yin Yang. *Multivariate Public Key Cryptography*, pages 193–241. Springer Berlin Heidelberg, 2009.

[GGH97] Oded Goldreich, Shafi Goldwasser, and Shai Halevi. Public-key cryptosystems from lattice reduction problems. In *Annual International Cryptology Conference*, pages 112–131. Springer, 1997.

[Gol00] Oded Goldreich. *Foundations of Cryptography: Basic Tools*. Cambridge University Press, New York, NY, USA, 2000.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206, 2008.

[Has18] Yasufumi Hashimoto. Multivariate public key cryptosystems. In *Mathematical Modelling for Next-Generation Cryptography*, pages 17–42. Springer, 2018.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru: A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory: Third International Symposiun, ANTS-III Portland, Oregon, USA, June 21–25, 1998 Proceedings*, 1998.

[KPG99] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In Jacques Stern, editor, *Advances in Cryptology — EUROCRYPT '99*, 1999.

[LATV12] Adriana López-Alt, Eran Tromer, and Vinod Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, 2012.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *EUROCRYPT*, volume 6110, 2010.

[McE78] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44:114–116, January 1978.

[Mer79] Ralph Merkle. *Secrecy, authentication and public key systems / A certified digital signature*. PhD thesis, Stanford University, 1979.

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in Cryptology — EUROCRYPT '88*, pages 419–453, Berlin, Heidelberg, 1988. Springer Berlin Heidelberg.

[MP13] Daniele Micciancio and Chris Peikert. Hardness of sis and lwe with small parameters. In *Crypto*, 2013.

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

[OS09] Raphael Overbeck and Nicolas Sendrier. *Code-based cryptography*. 2009.

[Pat96] Jacques Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, 1996.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *STOC*, pages 333–342, 2009.

[Pei16] Chris Peikert. *A Decade of Lattice Cryptography*, volume 10, pages 283–424. 03 2016.

[Reg04] Oded Regev. New lattice-based cryptographic constructions. *Journal of the ACM (JACM)*, 51(6):899–942, 2004.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J.ACM*, 56(6), 2009. extended abstract in STOC'05.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 124–134, 1994.

[SS11] Damien Stehlé and Ron Steinfeld. Making ntru as secure as worst-case problems over ideal lattices. In *Proceedings of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT'11, 2011.

[Wol05] Christopher Wolf. *Multivariate Quadratic Polynomials In Public Key Cryptography*. PhD thesis, KATHOLIEKE UNIVERSITEIT LEUVEN, 2005.