Editors' Suggestion

Learning-with-errors problem is easy with quantum samples

Alex B. Grilo,[1] Iordanis Kerenidis,[2] and Timo Zijlstra[3]
[1]*QuSoft and CWI, Amsterdam 1098XG, The Netherlands*
[2]*IRIF, CNRS, Université Paris Diderot, 75013 Paris, France*
[3]*Lab-STICC, Université Bretagne Sud, 56321 Lorient, France*

(Received 8 September 2018; published 11 March 2019)

The learning-with-errors (LWE) problem is one of the fundamental problems in computational learning theory and has in the last years become the cornerstone of postquantum cryptography. In this work, we study the quantum sample complexity of learning with errors and show that there exists an efficient quantum learning algorithm (with polynomial sample and time complexity) for the learning-with-errors problem where the error distribution is the one used in cryptography. While our quantum learning algorithm does not break the LWE-based encryption schemes proposed in the cryptography literature, it does have some interesting implications for cryptography: if a quantum adversary has access to a particular superposition of quantum states, a LWE-based encryption scheme becomes insecure. In particular, if a quantum sample state could be created from classical samples, then it would be possible to break LWE-based schemes using our learning algorithm. Finally, we extend our results and show quantum learning algorithms for three related problems: learning parity with noise, learning with rounding, and short integer solution.

DOI: 10.1103/PhysRevA.99.032314

I. INTRODUCTION

The large amount of data arising in the real world, for example through scientific observations, large-scale experiments, internet traffic, social media, etc., makes it necessary to be able to predict some general properties or behaviors of the data from a limited number of samples. In this context, computational learning theory provides rigorous models for learning and studies the necessary and sufficient resources, for example, the number of samples or the running time of the learning algorithm. In his seminal work, Valiant [1] introduced the model of PAC learning, and since then this model has been extensively studied and has given rise to numerous extensions.

In another revolutionary direction, quantum computing takes advantage of the quantum nature of small-scale systems as a computational resource. In this field, the main question is to understand what problems can be solved more efficiently in a quantum computer than in classical computers. In the intersection of the two fields, we have quantum learning theory, where we ask if quantum learning algorithms can be more efficient than classical ones.

One of course needs to be careful about defining quantum learning and more precisely, what kind of access to the data a quantum learning algorithm has. On one hand, we can just provide classical samples to the quantum learning algorithm that can then use the quantum power in processing these classical data. In the more general scenario, we allow the quantum learning algorithm to receive quantum samples of the data, for a natural notion of a quantum sample as a superposition that corresponds to the classical sample distribution.

More precisely, in classical learning, the learning algorithm is provided with samples of $(x, f(x))$, where x is drawn from some (possibly unknown) distribution D and f is the function we wish to learn. The goal of the learner in this case is to output a function g such that with high probability (with respect to the samples received), f and g are close, i.e., $Pr[f(x) \neq g(x)]$ is small when x is drawn from the same distribution D.

The extension of this model to the quantum setting is that the samples now are given in the form of a quantum state $\sum_x \sqrt{D(x)}|x\rangle|f(x)\rangle$. Note that one thing the quantum learner can do with this state is simply measure it in the computational basis and get a classical sample from the distribution D. Hence, a quantum sample is at least as powerful as a classical sample. The main question is whether the quantum learner can make better use of these quantum samples and provide an advantage in the number of samples and/or running time compared to a classical learner.

In this work we focus on one of the fundamental problems in learning theory, learning with errors (LWE). In LWE, one is given samples of the form

$$(a, a \cdot s + e \pmod q),$$

where $s \in \mathbb{F}_q^n$ is fixed, $a \in \mathbb{F}_q^n$ is drawn uniformly at random and $e \in \mathbb{F}_q$ is an error term drawn from some distribution χ. The goal is to output s, while minimizing the number of samples and the computation time.

First, LWE is the natural generalization of the well-studied learning-parity-with-noise problem (LPN), which is the case of $q = 2$. Moreover, a lot of attention was drawn to this problem when Regev [2] reduced some (expected to be) hard problems involving lattices to LWE. With this reduction, LWE has become the cornerstone of current postquantum cryptographic schemes. Several cryptographic primitives proposals such as fully homomorphic encryption [3], oblivious transfer [4], identity-based encryption [5–7], and other schemes are

based in the hardness of LWE (for a more complete list see Ref. [8] and Ref. [9]).

Classically, Blum *et al.* [10] proposed the first subexponential algorithm for this problem, where both sample and time complexities are $2^{O(n/\log n)}$. Then, Arora and Ge [11] improved the time complexity for LWE with a learning algorithm that runs in $2^{\tilde{O}(n^{2\varepsilon})}$ time, for some $\varepsilon < \frac{1}{2}$, and it uses at least $\Omega(q^2 \log q)$ samples. For LPN, Lyubashevsky [12] has proposed an algorithm with sample complexity $n^{1+\varepsilon}$ at the cost of increasing computation time to $O(2^{n/\log\log n})$.

II. QUANTUM LEARNING MODEL

In this work, we use the model of exact learning under the uniform distribution where the learner receives samples according to the uniform distribution and outputs the exact function with high probability. In the quantum setting, the learning algorithm is given quantum samples, namely a uniform superposition of the inputs and function values,

$$\sum_{x\in X} \frac{1}{\sqrt{|X|}} |x\rangle|f(x)\rangle.$$

In this work, we are interested in noisy samples, which can be modeled by setting $f(x) = g(x) + e(x, r)$, where g and e are deterministic functions, $x \in X$ and $r \in R$ is the randomness necessary to generate the noise. For defining the quantum sample, we start with the superposition

$$\frac{1}{\sqrt{|R|}} \sum_{r\in R} |r\rangle \left(\frac{1}{\sqrt{|X|}} \sum_{x\in X} |x\rangle|g(x) + e(x, r)\rangle \right),$$

and then by tracing out the register corresponding to the randomness, the reduced density matrix is

$$\frac{1}{|R||X|} \sum_{\substack{r\in R \\ x,x'\in X}} |x\rangle\langle x'||g(x) + e(x, r)\rangle\langle g(x') + e(x', r)|,$$

which can be seen as having the following quantum sample with probability $\frac{1}{|R|}$, for each $r \in R$:

$$\frac{1}{\sqrt{|X|}} \sum_{x\in X} |x\rangle|g(x) + e(x, r)\rangle.$$

We consider the noise model defined in Bshouty and Jackson [13], where independent noise is added for each element in the superposition, in other words, $r = (r_1, \ldots, r_{|X|})$ and $e(x, r) = e'(r_x)$. This model is a natural generalization for quantum samples with noise since it can be seen as a superposition of the classical samples.

In contrast, Cross *et al.* [14] proposed a noise function that is independent of x. Although our noise model might require exponentially more resources to implement quantum samples, we show that this does not make the problem intractable. Also, this is the kind of state we could get after solving the index erasure problem[1].

[1]See Sec. III B for a more detailed discussion.

III. OUR CONTRIBUTIONS

In this work we study quantum algorithms for solving LWE with quantum samples. Let us be more explicit on the definition of a quantum sample for the LWE problem. We assume that the quantum learning algorithm receives samples in the form

$$\frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{F}_q^n} |a\rangle|a \cdot s + e_a \pmod q\rangle, \tag{1}$$

where e_a are iid random variables from some distribution χ over $\mathbb{F}_q$.

As expected, the performance of the learning algorithm, both in the classical and quantum case, is sensitive to the noise model adopted, i.e., to the distribution χ. When LWE is used in cryptographic schemes, the distribution χ has support on a small interval around 0, either uniform or a discrete Gaussian. We prove that for such distributions, there exists an efficient quantum learner for LWE.

Main Result (informal). For error distributions χ used in cryptographic schemes, and for any $\eta > 0$, there exists a quantum learning algorithm that solves LWE with probability $1 - \eta$ using $O(n \log \frac{1}{\eta})$ samples and running time $poly(n, \log \frac{1}{\eta})$.

Another interesting feature of our quantum learner is that it is conceptually a very simple algorithm based on one of the basic quantum operations, the quantum Fourier transform. Such algorithms have even started to be implemented, of course for very small input sizes and for the binary case [15]. Nevertheless, as far as quantum algorithms are concerned, our learner is quite feasible from an implementation point of view.

The approach to solve the problem is a generalization of Bernstein-Vazirani algorithm [16]: we start with a quantum sample, apply a quantum Fourier transform over $\mathbb{F}_q$ on each qudit, and then we measure in the computational basis. Our analysis shows that, when the last qudit is not 0, which happens with high probability, the value of the remaining registers gives s with constant probability. We can then repeat this process so that our algorithm outputs s with high probability.

Finally, the hardness of LWE has been proved to be equivalent to several other problems, when considering classical samples. Unfortunately, this does not imply equivalence of the hardness of LWE and these problems with quantum samples. This happens because the classical reduction can be randomized, which could cause problem when reducing a quantum sample of LWE to a quantum sample of another problem. In this work, we are able to show quantum learning algorithms for three problems related to LWE.

First, we study the learning-parity-with-noise (LPN) problem with quantum samples. This problem is an instance of LWE with $q = 2$, and the main difference with LWE is that the noise model is different: while in LWE the noise is sampled from a range, in an LPN sample, the value of the function is flipped with some probability. LPN is also very important in cryptography since since the security of several cryptographic schemes is based on its hardness [17–20]. In our work we extend the noise model of previous results [14,15], and we show that our algorithm still works for LPN with quantum samples in this extended noise model.

Second, we study the learning with rounding problem, which is a derandomized version of LWE. The LWR

problem is used in cryptographic primitives where the randomness needed by LWE samples is prohibitive, such as pseudorandom-number generators [21]. We are able to show that LWR samples can be seen as LWE samples, and then we can also prove the correctness of our algorithm for this problem.

At last, we study the shortest integer solution problem (SIS), where we search a short integer solution of a linear system. The hardness of SIS is a common cryptographic assumption in postquantum cryptographic schemes [22,23]. The quantum algorithm that we propose for SIS is slightly different and it is based on the entanglement between the input and the function registers.

A. Related work

We now review some results on quantum algorithms for learning problems. For a more extended introduction, see the survey by Arunachalam and de Wolf [24].

The first approach on trying to solve learning problems with quantum samples was proposed by Bshouty and Jackson [13], where they prove that DNFs[2] can be learned efficiently, even when the samples are noisy. No such efficient learners are known classically.

Despite not presenting it as a learning problem, Bernstein and Vazirani [16] show how to learn parity using a single quantum sample, while classically we need a linear number of samples.

Some years later, Servedio and Gortler [25] showed that classical and quantum sample and query complexity of learning problems are polynomially related, but they showed that for time complexity there exist exponential separations between classical and quantum learning (assuming standard computational hardness assumptions).

Then, Ambainis *et al.* [26], Atici and Servedio [27], and Hunziker *et al.* [28] provided general upper bounds on the query complexity for learning problems that depend on the size of the concept class being learned.

On specific problems, Atici and Servedio [29] and Belovs [30] provided quantum algorithms for learning juntas and Cross *et al.* [14] proposed and implemented quantum algorithms for LPN in a different noise model. Arunachalam and de Wolf [31] proved optimal bounds for the quantum sample complexity of the quantum PAC model.

B. Relation to LWE-based cryptography

As we have mentioned, LWE is used in cryptography for many different tasks. Let us briefly describe how one can build an encryption scheme based on LWE [2]. The key generation algorithm produces a secret key $s \in \mathbb{F}_q$, while the public key consists of a sequence of classical LWE samples $(a_1, a_1 \cdot s + e_1 \pmod q), \ldots, (a_m, a_m \cdot s + e_m \pmod q)$, where the error comes from a distribution with support in a small interval around 0. For the encryption of a bit b, the party picks a subset S of $[m]$ uniformly at random and outputs

$$\left(\sum_{i\in S} a_i \pmod q, b\left\lceil \frac{q}{2}\right\rceil + \sum_{i\in S} a_i \cdot s + e_i \pmod q\right).$$

For the decryption, knowing s allows one to find b. On the other hand, Regev showed that if s is unknown and it is possible to distinguish encryptions of 0 from encryptions of 1, i.e., to break the encryption scheme, then it is possible to solve the LWE problem [2].

The algorithm we present here does not break the above LWE-based encryption scheme. Nevertheless, it has interesting implications for cryptography.

First, if quantum samples could be approximated from classical samples, our algorithm could then be used for attacking LWE-based encryption. One potential way for this would be to start with m classical samples and create the following superposition

$$\sum_{S\subseteq[m]} |S\rangle \left|\sum_{i\in S} a_i \pmod q\right\rangle \left|\sum_{i\in S} a_i \cdot s + e_i \pmod q\right\rangle.$$

This operation is in fact efficient: from the superposition of all subsets $\sum_{S\subseteq[m]} |S\rangle$, we can use, in a coherent way, the classical algorithm that creates $|\sum_{i\in S} a_i \pmod q\rangle |\sum_{i\in S} a_i \cdot s + e_i \pmod q\rangle$ from the classical samples for a fixed S. Then, in order to approximate the quantum sample state, one would need to forget the register containing the index information about which subset of the m classical samples. In the most general case, such an operation of forgetting the index of the states in a quantum superposition, known as index erasure (see Aharonov and Ta-Shma [32] and Ambainis *et al.* [26]), is exponentially hard, and a number of problems, such as graph nonisomorphism, would have an efficient quantum algorithm, if we could do it efficiently. Therefore, if the structure of LWE allows such operation to be performed efficiently, then one could combine it with our learning algorithm to solve LWE with classical samples, which would have a major impact in postquantum cryptography.

A second concern that our algorithm raises is that when building an LWE-based scheme, the access to a particular superposition of quantum states could make the scheme insecure. It is well known that for example, even in the classical case, if the adversary can ask classical queries to the LWE oracle, then he can easily break the scheme: by asking the same query many times one can basically average out the noise and find the secret s. However, if we just assume that the public key is given as a box that an agent has passive access to it, in the sense that he can request a random sample and receive one, then the encryption scheme is secure classically as long as LWE is difficult. However, imagine that the random sample from LWE is provided by a device that creates a superposition $\frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{F}_q^n} |a\rangle |a \cdot s + e_a \pmod q\rangle$ and then measures it. Then a quantum adversary that has access to this quantum state can break the scheme by using our quantum algorithm to learn the secret s, and therefore being able to decrypt any encrypted message of the proposed scheme. Again, our claim is, by no means, that our algorithm breaks the proposed LWE-based encryption schemes, but more that LWE-based schemes,

[2]A boolean formula is called a DNF if it is described as ORs ($\vee$) of ANDs ($\wedge$). An example of a DNF over the variables $x_1, \ldots x_4$ would be $\overline{x_1} \vee (x_2 \wedge x_4) \vee (x_2 \wedge x_3 \wedge x_4)$, where $\overline{y}$ is the negation of a variable y.

which are secure classically (assuming the hardness of LWE) may stop being secure against quantum adversaries if the access to the public key generation algorithm becomes also quantum.

A similar situation has also appeared in the symmetric key cryptography with the so-called superposition attacks [33–36]. There, the attacker has the ability to query the encryption oracle in superposition, and in this way, she can in fact break many schemes that are assumed to be secure classically. While in the case of symmetric cryptography, the attacker must have quantum access to the encryption oracle in order to break the system, our results show that in the case of LWE-based public-key encryption, the attacker must have quantum access to the public-key generation algorithm.

Recently, Alagic, Jeffery, Ozols, and Poremba [37] proposed quantum attacks to LWE encryption schemes where the attacker has quantum access to encryption and decryption oracles.

IV. ALGORITHM FOR LWE

In this section we present the extension of the Bernstein-Vazirani algorithm for higher-order fields and analyze its behavior with LWE samples. We describe now the Field Bernstein-Vazirani algorithm [16], whose main component is the quantum Fourier transform over $\mathbb{F}_q$, $QFT|j\rangle = \frac{1}{\sqrt{q^n}} \sum_{k=0}^{q^n-1} \omega^{jk}|k\rangle$.

Field Bernstein-Vazirani algorithm
Input: $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n+1}$
Output: $\tilde{s} \in \mathbb{F}_q^n \cup \{\perp\}$
Apply $QFT^{\otimes n+1}$ on $|\psi\rangle$.
Measure in the computational basis
Let $|j\rangle|j^*\rangle$ be the output
If $j^* \neq 0$, return $-(j^*)^{-1} j \pmod q$
Else, return $\perp$

For warming up, we show the behavior of Field Bernstein-Vazirani for learning linear functions without noise in Sec. IV A and then in Sec. IV B we analyze it for LWE samples.

A. Quantum algorithm for learning a linear function without error

If the input $|\psi\rangle$ is a noiseless quantum sample of a linear function, namely

$$|\psi\rangle = \frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{F}_q^n} |a\rangle|a\cdot s \pmod q\rangle. \tag{2}$$

Then the Field Bernstein-Vazirani algorithm outputs the correct value with probability $\frac{q-1}{q}$: after applying the QFT on each qudit of Eq. (2), we get the state

$$\frac{1}{q^{n+\frac{1}{2}}} \sum_{a,j\in\mathbb{F}_q^n} \sum_{j^*\in\mathbb{F}_q} \omega^{a\cdot(j+j^*s)}|j\rangle|j^*\rangle.$$

It is not hard to see that the probability that for all $i \in [n]$, we have $j = -j^*s \pmod q$ and $j^* \neq 0$ is

$$\left\| \frac{1}{q^{n+\frac{1}{2}}} \sum_{j^*\in\mathbb{F}_q^*} \sum_{a\in\mathbb{F}_q^n} \omega^{0}|-j^*s \pmod q\rangle|j^*\rangle \right\|^2$$

$$= \frac{1}{q^{2n+1}} \sum_{j^*\in\mathbb{F}_q^*} \left(\sum_{a\in\mathbb{F}_q^n} 1 \right)^2 = \frac{q-1}{q}.$$

Therefore, if $j^* \neq 0$, we can retrieve s by outputting $-(j^*)^{-1} j_i$ (all operations mod q).

B. Analysis of the algorithm for noisy samples

In this section we show that the Field Bernstein-Vazirani algorithm works even if the input is noisy. Instead of the superposition of all elements in $\mathbb{F}_q^n$, we prove our result here for a more general case where the quantum sample has the form

$$|\psi\rangle = \frac{1}{\sqrt{v}} \sum_{a\in V} |a\rangle|a\cdot s + e_a \pmod q\rangle,$$

where $v \in [q^n]$ is a fixed value, V be a random subset of $\mathbb{F}_q^n$ of size v and e_a is a random noise. In this case, for every quantum sample, a new subset V of size v is picked independently at random. This model could be useful, for instance, to learn s on quantum samples generated from classical samples[3] and it also allows us to understand the tradeoff between the quality of the quantum sample and the probability that the algorithm outputs the correct answer.

Theorem 1. Fix $v \in [q^n]$. Let $V \subseteq \mathbb{F}_q^n$ be a random subset of $\mathbb{F}_q^n$ such that $|V| = v$, and let

$$|\psi\rangle = \frac{1}{\sqrt{v}} \sum_{a\in V} |a\rangle|a\cdot s + e_a \pmod q\rangle,$$

where the e_a are random variables with absolute value at most k. The Field Bernstein-Vazirani ($|\psi\rangle$) outputs s with probability $\frac{v}{20kq^n}$.

Proof. If we apply QFT on the state $|\psi\rangle$, we have

$$\frac{1}{\sqrt{q^{n+1}v}} \sum_{a\in V} \sum_{j\in\mathbb{F}_q^n, j^*\in\mathbb{F}_q} \omega^{e_a j^* + a\cdot(j+j^*s)}|j\rangle|j^*\rangle.$$

From the last equation, we have that the probability that $j = -j^*s \pmod q$ and $j^* \neq 0$ is:

$$\frac{1}{q^{n+1}v} \left\| \sum_{a\in V} \sum_{j^*\in\mathbb{F}_q^*} \omega^{e_a j^*}|-j^*s \pmod q\rangle|j^*\rangle \right\|^2$$

$$= \frac{1}{q^{n+1}v} \sum_{j^*\in\mathbb{F}_q^*} \left(\sum_{a\in V} \mathrm{Re}(\omega^{e_a j^*}) \right)^2 + \left(\sum_{a\in V} \mathrm{Im}(\omega^{e_a j^*}) \right)^2$$

$$\geqslant \frac{1}{q^{n+1}v} \sum_{\substack{j^*\in\mathbb{F}_q^* \\ j^* \leqslant \frac{\gamma q}{k}}} \left(\sum_{a\in V} \mathrm{Re}(\omega^{e_a j^*}) \right)^2 \geqslant \frac{\gamma v \cos(2\pi\gamma)^2}{kq^n}, \tag{3}$$

[3] See Sec. III B for a more detailed discussion on such approach.

where $\gamma \in (0, \frac{1}{4})$ will be fixed later and $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ are the real and imaginary part of z, respectively. The first equality holds since

$$\left\| \sum_x \alpha_x |x\rangle \right\|^2 = \sum_x |\alpha_x|^2 = \sum_x \mathrm{Re}(\alpha_x)^2 + \mathrm{Im}(\alpha_x)^2.$$

For the first inequality, we have removed some positive quantities, and the last inequality follows from the fact that $\mathrm{Re}(\omega^{e_a j^*}) \leqslant \cos(2\pi\gamma)$ for $j^* \leqslant \frac{\gamma q}{k}$ and $|e_a| \leqslant k$.

By maximizing it over all $\gamma \in (0, \frac{1}{4})$, we have that Eq. (3) can be upper-bounded by $\frac{v}{20kq^n}$, proving the statement. ■

We now propose an algorithm that tests a candidate solution.

Test Candidate
Input: $\tilde{s} \in \mathbb{F}_q^n$, $M \in \mathbb{Z}^+$
Output: Accept/reject
Repeat M times.
Pick sample $|\psi\rangle = \frac{1}{\sqrt{v}} \sum_{a \in V} |a\rangle |a \cdot s + e_a \mod q\rangle$.
Measure the sample in the computational basis
Let $(a', a' \cdot s + e_{a'})$ be the output
If $|a' \cdot s + e_{a'} - a' \cdot \tilde{s}| > k$, reject
Accept

Lemma 1. For $\tilde{s} = s$, Test Candidate $(\tilde{s}, M)$ accepts with probability 1, while for $\tilde{s} \neq s$, Test Candidate $(\tilde{s}, M)$ accepts with probability probability at most $(\frac{2k+1}{q})^M$.

Proof. Since $|a' \cdot s + e_{a'} - a' \cdot s| = |e_{a'}| \leqslant k$ by the noise distribution, it follows that the test passes with probability 1 when $\tilde{s} = s$.

For a value a' picked uniformly random from $\mathbb{F}_q^n$, it follows that $a' \cdot (s - \tilde{s}) + e_{a'} \mod q$ is uniformly distributed over $\mathbb{F}_q$ if $\tilde{s} \neq s$. Therefore, the probability that it lies in the interval $[-k, k]$ is $\frac{2k+1}{q}$. Since the probability is independent for every iteration, the probability that $\tilde{s}$ is accepted on M iterations is $(\frac{2k+1}{q})^M$. ■

We show now how to use Theorem 1 and Lemma 1 in order to solve solve LWE with quantum samples using noise distributions proposed in Brakerski and Vaikuntanathan [3]. There, the field order q is subexponential in the dimension n, generally in $[2^{n^\gamma}, 2 \cdot 2^{n^\gamma})$ for some constant $\gamma \in (0, 1)$, while the noise distribution χ produces samples with magnitude at most polynomial in n (for instance linear).

LWE Algorithm(L, M)
Input: $L, M \in \mathbb{Z}^+$
Output: $\tilde{s} \in \mathbb{F}_q^n \cup \{\perp\}$
Repeat L times:
Pick a quantum sample $|\psi\rangle$
Run the Field Bernstein-Vazirani ($|\psi\rangle$) to get output $\tilde{s}$
Run Test Candidate $(\tilde{s}, M)$
If $\tilde{s}$ passes the test, return $\tilde{s}$
Return $\perp$.

Theorem 2. For dimension n, let q be a prime in the interval $[2^{n^\gamma}, 2 \cdot 2^{n^\gamma})$. Let

$$|\psi\rangle = \frac{1}{\sqrt{q^n}} \sum_{a \in \mathbb{F}_q^n} |a\rangle |a \cdot s + e_a\rangle,$$

where the e_a are random variables drawn from a noise distribution with noise magnitude at most $k = poly(n)$. There is an algorithm that outputs s with probability $1 - \eta$ with sample complexity $O(k \log \frac{1}{\eta})$ and running time $poly(n, \log \frac{1}{\eta})$.

Proof. We start the proof by analyzing the LWE Algorithm(L, M) and then we choose the parameters L and M in order to prove the statement.

LWE Algorithm(L, M) does not output s if either Test Candidate $(\tilde{s}, \log \frac{1}{\eta})$ accepts some $\tilde{s} \neq s$ before an iteration where Field Bernstein-Vazirani outputs s, or LWE algorithm outputs $\perp$. We can upper bound the probability of this event by the probability that at least one of L independent calls to Test Candidate $(\tilde{s}, \log \frac{1}{\eta})$ accepts some $\tilde{s} \neq s$ or that L independent calls to Field Bernstein-Vazirani do not output s.

From Lemma 1 and using the union bound, the probability that at least one of L independent calls to Test Candidate $(\tilde{s}, \log \frac{1}{\eta})$ accepts some $\tilde{s} \neq s$ is at most

$$\left(\frac{2k+1}{q}\right)^M L \leqslant \left(\frac{3k}{q}\right)^M L.$$

From Theorem 1, the probability that s is not the output of L independent calls to Field Bernstein-Vazirani is at most

$$\left(1 - \frac{v}{20kq^n}\right)^L.$$

By union bound, LWE algorithm(L, M) does not output s with probability at most

$$\left(1 - \frac{v}{20kq^n}\right)^L + \left(\frac{3k}{q}\right)^M L. \tag{4}$$

Finally, by picking $v = q^n$, $L = 20k \ln \frac{1}{\eta}$ and $M = 1$, the statement follows from Eq. (4). ■

We show in Appendix B how to extend the result to related problems: the learning parity with noise problem, the learning with rounding problem, and the short integer solution problem.[4]

V. OPEN PROBLEMS

A. Generalizing from linear functions

Learning linear functions can be seen as finding a hidden subgroup $H = a|a \cdot s = 0$ of $\mathbb{Z}_q^n$. Efficient algorithms for general Abelian hidden subgroup problem are known [38,39], and we leave as an open question if these algorithms are also tolerant to noise.

B. LWE over rings

Due to technical reasons regarding the representation of polynomials in Ring-LWE instances (see Appendix B 2 for

[4]See Sec. III for a discussion on such problems.

more details), our LWE algorithm cannot be used to solve Ring-LWE with quantum samples and we leave this question as an open problem.

ACKNOWLEDGMENTS

Most of this work was done when A.B.G. and T.Z. were supported by IRIF, Université Paris Diderot, Paris, France. A.B.G. and I.K. thank Ronald de Wolf for helpful discussions. A.B.G. thanks also Lucas Boczkowski, Brieuc Guinard, Franois Le Gall, and Alexandre Nolin for helpful discussions. Supported by ERC QCC Grant No. 306537 and French Programme d'Investissement d'Avenir RISQ P141580. A.B.G. was also supported by ERC Consolidator Grant No. 615307-QPROGRESS.

APPENDIX A: NOTATION

For $n \in \mathbb{N}$, we define $[n] := \{1, \ldots, n\}$. For a complex number $x = a + ib$, $a, b \in \mathbb{R}$, we define its norm $|x|$ by $\sqrt{a^2 + b^2}$, its real part $\mathrm{Re}(x) = a$, and its imaginary part $\mathrm{Im}(x) = b$. We denote ω as the qth root of unity, where q will be clear by the context. For a field $\mathbb{F}_q$ and element $a \in \mathbb{F}_q$, we denote $|a|$ as the unique value $b \in [\frac{-(q-1)}{2}, \frac{q-1}{2}]$ such that $b \equiv a \pmod q$.

We remind now the notation for quantum information and computation. For readers not familiar with these concepts we refer to Ref. [40]. Let $\{e_i\}$ be the standard basis for the q-dimensional Hilbert space $\mathbb{C}^q$. We denote here $|i\rangle = e_i$ and a q-dimensional qudit is a unit vector in this space, i.e., $|\psi\rangle = \sum_{i \in \mathbb{F}_q} \alpha_i |i\rangle$, for $\alpha_i \in \mathbb{C}$ and $\sum_{i \in \mathbb{F}_q} |\alpha_i|^2 = 1$. We call the state a qubit when $q = 2$. A k-qudit quantum state is a unit vector in the complex Hilbert space $\mathbb{C}^{q^k}$ and we shorthand the basis states for this space $|i_1\rangle \otimes \ldots \otimes |i_k\rangle$ with $|i_1\rangle \ldots |i_k\rangle$.

APPENDIX B: QUANTUM LEARNING COMPLEXITY OF RELATED PROBLEMS

In this Appendix we present learning algorithms for problems that are related to LWE.

1. Learning parity with noise

We show here our result for learning parity with noise (LPN) problem, which is the LWE problem for $q = 2$.

Here, the parity bit is flipped independently for each element in the superposition with probability η. This is the same noise model proposed by Bshouty and Jackson [13]. Note that Cross *et al.* [14] studied LPN with different noise models. In the first, all parities in the superposition are flipped at the same time with probability η. In the second one, each qubit passed through a depolarizing channel. Our algorithm and analysis also works for both of the noise models proposed by Cross *et al.* [14]. The algorithm is the same as in the previous section, where now the QFT is over $\mathbb{F}_2$ (also called the Hadamard transform H).

Lemma 2. Let $\frac{1}{\sqrt{2^n}} \sum_{a \in \{0,1\}^n} |a\rangle |a \cdot s + e_a \pmod 2\rangle$ be a quantum sample where e_a are iid random variables with value 0 with probability $1 - \eta$ and 1 with probability η. There exists a quantum algorithm that outputs s with probability exponentially close to 1 with sample complexity $O(n \log \frac{1}{\eta})$ and running time $poly(n, \log \frac{1}{\eta})$.

Proof. Let us analyze the behavior of the Bernstein-Vazirani algorithm on the previous state.

If we apply Hadamards on each qubit of the sample state, we have

$$\frac{1}{2^{n+\frac{1}{2}}} \sum_{a \in \{0,1\}^n} \sum_{j \in \{0,1\}^{n+1}} (-1)^{e_a j^* + a \cdot (j + j^* s)} |j\rangle |j^*\rangle$$

We now calculate the probability that $j^* = 1$ and the first qubits are in the state $|s\rangle$:

$$\left\| \frac{1}{2^{n+\frac{1}{2}}} \sum_{a \in \{0,1\}^n} (-1)^{e_a + a \cdot (s+s)} |s\rangle \right\|^2 = \frac{1}{2^{2n+1}} \Big(\sum_{a \in \{0,1\}^n} (-1)^{e_a} \Big)^2$$

From the distribution of each e_a, we have that $(-1)^{e_a}$ is 1 w.p. $1 - \eta$ and -1 w.p. η, independently. Therefore $\mathbb{E}[(-1)^{e_a}] = 1 - 2\eta$ and using Hoeffding's bound we have that for every $0 < \delta < 1$

$$Pr\left[\sum_{a \in \{0,1\}^n} (-1)^{e_a} \leqslant (1 - \delta)(1 - 2\eta) 2^n \right] < e^{\delta^2 (1-2\eta)^2 2^{2n}/4}.$$

Therefore, with probability exponentially close to 1, the probability that $j = s$ is at least

$$\frac{1}{2^{2n+1}} [(1 - \delta)(1 - 2\eta) 2^n]^2 = \tfrac{1}{2}(1 - \delta)^2 (1 - 2\eta)^2.$$

We bound now the expected probability that the output is a fixed $\tilde{s} \neq s$.

Let $Y = \sum_a (-1)^{e_a + a \cdot (s + \tilde{s})}$ be a random variable and then we can calculate that $\mathbb{E}[Y] = 0$ and $\mathrm{Var}[Y] = 2^n (4\eta - 4\eta^2)$. It follows that the probability of outputting $\tilde{s}$ is

$$\mathbb{E}\left[\left\| \frac{1}{2^{n+\frac{1}{2}}} \sum_{a \in \{0,1\}^n} (-1)^{e_a + a \cdot (s+\tilde{s})} |\tilde{s}\rangle \right\|^2 \right] = \frac{1}{2^{2n+1}} \mathbb{E}[Y^2] = \frac{1}{2^{2n+1}} (\mathrm{Var}[Y] + \mathbb{E}[Y]^2) = \frac{4\eta - 4\eta^2}{2^{n+1}}.$$

If we repeat the process $O(n \log \frac{1}{\eta})$ times, by Chernoff bounds, s is the most common string among all outputs with probability exponentially close to 1. ∎

2. LWE over rings

The ring-LWE problem [41], a variant of LWE over the ring of polynomials, has been proposed in order to improve the performance of cryptographic constructions using LWE, at the cost of stronger hardness assumptions.

The ring-LWE problem uses the structure of the ring $\mathcal{R}_q = \mathcal{R}/q\mathcal{R}$ for a prime q, $\mathcal{R} = \mathbb{Z}[x]/f(x)$ and a cyclotomic polynomial $f(x)$. As in LWE, a ring-LWE sample is the pair $(a, as + e \pmod q)$ for random $s, a \in \mathcal{R}_q$ and e is picked according to some error distribution χ.

Unfortunately, our algorithm cannot be used to solve ring-LWE with the noise model proposed by Bshouty *et al.* [13], due to technical issues on representing the polynomials. In order to use the quantum learning algorithm for LWE, we need to find an isomorphism ϕ from $\mathcal{R}_q$ to $\mathbb{Z}_q^n$, where $n = \varphi(m)$ is the number of invertible elements modulo m. With this isomorphism, we can consider a sample $(a, as + e) \in \mathcal{R}_q^2$ as two vectors in $\mathbb{Z}_q^n$, and a superposition of quantum states representing these vectors can be written as:

$$|\psi\rangle = \frac{1}{\sqrt{q^n}} \sum_{a\in\mathcal{R}_q} |\phi(a)\rangle|\phi(as + e_a)\rangle,$$

and applying the QFT over every register of this state results in

$$QFT^{\otimes 2n}|\psi\rangle \tag{B1}$$

$$= \frac{1}{\sqrt{q^{3n}}} \sum_{a\in\mathcal{R}_q} \sum_{x,y\in\mathbb{Z}_q} \omega^{\phi(a)\cdot x}|x\rangle \otimes \omega^{\phi(as+e_a)\cdot y}|y\rangle$$

$$= \frac{1}{\sqrt{q^{3n}}} \sum_{a\in\mathcal{R}_q} \sum_{x,y\in\mathbb{Z}_q} \omega^{\phi(a)\cdot(x+y\phi(s))+y\cdot\phi(e_a)}|x\rangle|y\rangle, \tag{B2}$$

where the second equality holds because ϕ is a homomorphism.

We consider two ways of representing elements in $\mathcal{R}_q$ as integer vectors. The first one consists of identifying a polynomial in $\mathcal{R}_q$ with the vector containing its coefficients. However, this coefficient embedding is not a homomorphism to $\mathbb{Z}_q^n$, and the following identity, used in Eq. (5), does not hold

$$\phi(a)\cdot x + \phi(a\cdot s + e_a)y = \phi(a)(x + y\phi(s)) + y\phi(e_a).$$

Therefore, this representation of polynomials cannot be used within our learning algorithm.

The second way of representing a polynomial is through the map

$$\phi(p(x)) = [p(\omega_m), \ldots, p(\omega_m^{m-1})],$$

where $\omega_m \in \mathbb{Z}_q$ be a primitive mth root of unity. This map is particularly interesting since multiplication $\mathbb{Z}_q^n$ is done componentwise [42] and therefore it can be used in implementations of ring-LWE with efficient multiplication [43]. However, in these constructions, the error is sampled from a distribution over polynomials with small coefficients and when after applying the isomorphism, $\phi(e_a)$ can be arbitrarily large in $\mathbb{Z}_q^n$, which cannot be handled by our algorithm if the error is independent for each element in the superposition. Finally, we show now how to do solve ring-LWE for the error model presented in Cross *et al.* [14], namely, the noise is the same for all elements in the superposition.

Let ϕ be any isomorphism from $\mathcal{R}_q$ to $\mathbb{Z}_q^n$. We can map the original quantum sample using ϕ resulting in

$$\frac{1}{\sqrt{q^n}} \sum_{a\in\mathcal{R}_q} |\phi(a)\rangle \otimes |\phi(as + e)\rangle,$$

and using the Field-Bernstein-Vazirani algorithm on this state we have

$$QFT^{\otimes 2n}|\psi\rangle = \frac{1}{\sqrt{q^{3n}}} \sum_{a\in\mathcal{R}_q} \sum_{x,y\in\mathbb{Z}_q} \omega^{\phi(a)\cdot x}|x\rangle \otimes \omega^{\phi(as+e)\cdot y}|y\rangle$$

$$= \frac{1}{\sqrt{q^{3n}}} \sum_{y\in\mathbb{Z}_q} \omega^{y\cdot\phi(e)} \sum_{a\in\mathcal{R}_q} \sum_{x\in\mathbb{Z}_q} \omega^{\phi(a)\cdot(x+y\phi(s)))}|x\rangle|y\rangle.$$

By measuring the last register, the error becomes a global phase and we are able to retrieve s as shown in Sec. IV A.

3. Learning with rounding

LWE has been used in the construction of several cryptographic primitives. However, its usage sometimes is limited. For instance, in the implementation of pseudorandom functions, the output must use little or no randomness, which does not correspond to the inherent randomness in LWE's input.

For this purpose, Banerjee, Peikert, and Rosen [21] proposed a derandomized version of LWE called learning with rounding (LWR), which does not compromise hardness. LWR has been used in the construction of pseudorandom functions [21] and deterministic public-key encryption [44].

The main idea of LWR consists in replacing $a \cdot s + e_a$ by the rounding of $a \cdot s$ with respect to some modulus $p \ll q$, which can be seen as a deterministic noise. More precisely, the rounding function is defined as follows:

$$\lfloor\cdot\rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p, \text{ with} \lfloor x\rceil_p = \left\lfloor \frac{p}{q}x \right\rceil \pmod p.$$

An LWR sample is then given by $(a, \lfloor a\cdot s\rceil_p)$ for some a sampled from the uniform distribution on $\mathbb{F}_q^n$.

Corollary 1. Let

$$|\psi\rangle = \frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{F}_q^n} |a\rangle|\lfloor a\cdot s\rceil_p\rangle,$$

be a quantum LWR sample. Let $|\phi\rangle$ be the state when we multiply the last register of $|\psi\rangle$ with $\frac{q}{p}$. The Field Bernstein-Vazirani ($|\phi\rangle$) outputs s with probability at least $\frac{p}{12(q-1)}$.

Proof. For a fixed a, we have that

$$\frac{q}{p}\lfloor a\cdot s\rceil_p = a\cdot s + \left(\frac{q}{p}\lfloor a\cdot s\rceil_p - a\cdot s\right) \pmod q.$$

Since $\frac{-q}{2p} \leqslant \frac{q}{p}\lfloor a\cdot s\rceil_p - a\cdot s \leqslant \frac{q}{2p} \pmod q$, the result follows by Theorem 1 for $k = \frac{q}{2p}$. ∎

4. Quantum samples for SIS problem

We present in this section a learning algorithm for another relevant problem in cryptography, the short integer solution problem. As the name indicates, the short integer solution problem (SIS) consists in finding a short integer solution for a system of linear equations, and we present now its formal definition.

Definition 1 (short integer solution). Given a random matrix $A \in \mathbb{F}_q^{m\times n}$, a random vector $z \in \mathbb{F}_q^m$, the $\text{SIS}_{n,m,q,\beta}$ problem is to find a vector $x \in \mathbb{F}_q^n$ such that $Ax = z \pmod q$ with $\|x\| < \beta$.

As in the LWE case, the hardness of SIS is also proved through the reduction of (expected to be) hard lattice problems [7,45–47]. We remark that if we drop either the constraint of having an integer solution or having a short solution, the problem can be easily solved using Gaussian elimination.

The SIS problem and its variants have been used to prove security of constructions of signature schemes [22,48], and hash functions [49]. In these schemes, samples in the form (A, Av) are public, where v is a small random vector and A is a random matrix.

Inspired in the LWE case, we can define a quantum sample for SIS problem as

$$|\psi\rangle = \frac{1}{\sqrt{q^{nm}}} \sum_{A\in\mathbb{F}_q^{m\times n}} |A\rangle|Av\rangle \pmod q,$$

and we are interested in the sample complexity of finding the (fixed) short solution v. Using Field Bernstein-Vazirani brings the same problem of Gaussian elimination: there is no guarantee of finding a short solution instead of an arbitrary one.

We notice that tracing out $m-1$ rows of A and the corresponding positions of Av, we remain with

$$\frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{F}_q^n} |a\rangle|a\cdot v\rangle,$$

and we show an algorithm that works even for this type of quantum sample.

The algorithm consists by testing all possible values $j \in \{-k,\dots,k\}$ of $-v_i$. The test on $j=-v_i$ passes with probability 1, while the test rejects with constant probability for $j\neq -v_i$. By repeating the test L times, the probability of finding the correct value is amplified.

SIS Algorithm(L)
Input: $L\in\mathbb{Z}^+$
Output: $\tilde{v}\in\mathbb{F}_q^n$
For $i\in[n]$ do:
For $j\in\{-k,\dots,k\}$ do:
  For $l\in[L]$:
    Pick a quantum sample $\frac{1}{\sqrt{q^n}}\sum_{a\in\mathbb{F}_q^n}|a\rangle|a\cdot v\rangle$.
    Add ja_i to the last register
    Apply QFT on the ith qudit of a and measure it
    Test next value of j if outcome is not $|0\rangle$
  Set $\tilde{v}_i=-j$ and continue with the next value of i.
Output $\tilde{v}$

Theorem 3. Let $v\in\mathbb{F}_q^n$ whose coefficients are all smaller in absolute value than some bound k. Given the quantum samples in the form

$$|\psi\rangle = \sum_{a\in\mathbb{F}_q^n} |a\rangle|a\cdot v\rangle,$$

SIS Algorithm(L) outputs v with probability $1-\frac{2km}{q^L}$.

Proof. We start by doing the analysis of SIS algorithm for $i=1$. After adding ja_1 to the last register of the quantum sample, we have

$$\frac{1}{\sqrt{q^n}} \sum_{a\in\mathbb{F}_q^n} |a\rangle|a\cdot v + a_1 j\rangle$$
$$= \frac{1}{\sqrt{q^n}} \sum_{a_1\in\mathbb{F}_q} \sum_{\overline{a}\in\mathbb{F}_q^{n-1}} |a_1\rangle|\overline{a}\rangle|a_1(v_1+j)+\overline{a}\cdot\overline{v}\rangle.$$

If $j=-v_1$, then the previous state is the product state

$$\frac{1}{\sqrt{q}} \sum_{a_1\in\mathbb{F}_q} |a_1\rangle \otimes \frac{1}{\sqrt{q^{n-1}}} \sum_{\overline{a}\in\mathbb{F}_q^{n-1}} |\overline{a}\rangle|\overline{a}\cdot\overline{v}\rangle.$$

and since $QFT\sum_{a_1\in\mathbb{F}_q}|a_1\rangle = |0\rangle$, the test passes for all $l\in[L]$.

On the other hand, if $j\neq -v_1$, then the state is entangled, and the reduced density matrix of the first register is

$$\frac{1}{q}\sum_{a_1\in\mathbb{F}_q} |a_1\rangle\langle a_1|.$$

In this case, after applying the QFT on the first register and measuring it, the output is $|0\rangle$ with probability $\frac{1}{q}$. Therefore, we have $\tilde{v}_1=-j$ if for all L independent samples the measurement outcome after the QFT is $|0\rangle$, and this happens with probability $\frac{1}{q^L}$. By the union bound, the probability that the test passes for any value $j\neq -v_i$ is at most $\frac{2k}{q^L}$.

Finally, the previous analysis holds for every $i\in[n]$. Since $v\neq\tilde{v}$ if and only if there exists an $i\in[n]$ such that $\tilde{v}_i\neq v_i$, we can use union bound again to show that this happens with probability at most $\frac{2km}{q^L}$. ∎

By picking $L=\max\{1, \frac{\log\frac{2km}{\eta}}{\log q}\}$, the algorithm outputs the correct v with probability at least $1-\eta$.

[1] L. G. Valiant, A theory of the learnable, Commun. ACM **27**, 1134 (1984).

[2] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, STOC 2005*, edited by R. A. Servedio and R. Rubinfeld (ACM, New York, 2005), pp. 84–93.

[3] Z. Brakerski and V. Vaikuntanathan, Efficient fully homomorphic encryption from (standard) LWE, SIAM J. Comput. **43**, 831 (2014).

[4] C. Peikert, V. Vaikuntanathan, and B. Waters, A framework for efficient and composable oblivious transfer, in *Advances in Cryptology - CRYPTO 2008*, edited by D. Wagner, Lecture Notes in Computer Science Vol. 5157 (Springer, Berlin, Heidelberg, 2008), pp. 554–571.

[5] S. Agrawal, D. Boneh, and X. Boyen, Efficient lattice (H)IBE in the standard model, in *Advances in Cryptology - EUROCRYPT 2010*, edited by H. Gilbert, Lecture Notes in Computer Science Vol. 6110 (Springer, Berlin, Heidelberg, 2010), pp. 553–572.

[6] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, Bonsai trees, or how to delegate a lattice basis, J. Cryptology **25**, 601 (2012).

[7] C. Gentry, C. Peikert, and V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008*, edited by I. Diakonikolas, D. Kempe, and M. Henzinger (ACM, New York, 2008), pp. 197–206.

[8] D. Micciancio and O. Regev, Lattice-based cryptography, in *Post Quantum Cryptography*, edited by J. A. Buchmann and J. Ding, Lecture Notes in Computer Science Vol. 5299 (Springer, Berlin, Heidelberg, 2008).

[9] C. Peikert, A decade of lattice cryptography, Foundations and Trends in, Theor. Comput. Sci. **10**, 283 (2016).

[10] A. Blum, A. Kalai, and H. Wasserman, Noise-tolerant learning, the parity problem, and the statistical query model, J. ACM **50**, 506 (2003).

[11] S. Arora and R. Ge, New algorithms for learning in presence of errors, in *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011*, edited by L. Aceto, M. Henzinger, and J. Sgall, Lecture Notes in Computer Science Vol. 6755 (Springer, Berlin, Heidelberg, 2011), pp. 403–415.

[12] V. Lyubashevsky, The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem, in *Approximation, Randomization and Combinatorial Optimization, Algorithms and Techniques, APPROX-RANDOM 2005*, edited by C. Chekuri, K. Jansen, J. D. P. Rolim, and L. Trevisan, Lecture Notes in Computer Science Vol. 3624 (Springer, Berlin, Heidelberg, 2005), pp. 378–389.

[13] N. H. Bshouty and J. C. Jackson, Learning dnf over the uniform distribution using a quantum example oracle, in *Proceedings of the Eighth Annual Conference on Computational Learning Theory, COLT '95*, edited by W. Maass (ACM, New York, 1995), pp. 118–127.

[14] A. W. Cross, G. Smith, and J. A. Smolin, Quantum learning robust against noise, Phys. Rev. A **92**, 012327 (2015).

[15] D. Ristè, M. P. da Silva, C. A. Ryan, A. W. Cross, J. A. Smolin, J. M. Gambetta, J. M. Chow, and B. R. Johnson, Demonstration of quantum advantage in machine learning, arXiv:1512.06069 (2015).

[16] E. Bernstein and U. Vazirani, Quantum complexity theory, SIAM J. Comput. **26**, 1411 (1997).

[17] M. Alekhnovich, More on average case vs approximation complexity, in *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, FOCS '03* (IEEE, 2003).

[18] B. Applebaum, D. Cash, C. Peikert, and A. Sahai, Fast cryptographic primitives and circular-secure encryption based on hard learning problems, in *Advances in Cryptology - CRYPTO 2009*, edited by S. Halevi, Lecture Notes in Computer Science Vol. 5677 (Springer, Berlin, Heidelberg, 2009), pp. 595–618.

[19] A. Blum, M. L. Furst, M. J. Kearns, and R. J. Lipton, Cryptographic primitives based on hard learning problems, in *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '93*, edited by D. R. Stinson, Lecture Notes in Computer Science Vol. 773 (Springer, Berlin, Heidelberg, 2008).

[20] N. J. Hopper and M. Blum, Secure human identification protocols, in *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security*, edited by C. Boyd, Lecture Notes in Computer Science Vol. 2248 (Springer, Berlin, Heidelberg, 2001), pp. 52–66.

[21] A. Banerjee, C. Peikert, and A. Rosen, Pseudorandom functions and lattices, in *Advances in Cryptology – EUROCRYPT* 2012, edited by D. Pointcheval and T. Johansson, Lecture Notes in Computer Science Vol. 7237 (Springer, Berlin, Heidelberg, 2012), pp. 719–737.

[22] V. Lyubashevsky, Lattice signatures without trapdoors, in *Advances in Cryptology – EUROCRYPT 2012*, edited by D. Pointcheval and T. Johansson, Lecture Notes in Computer Science Vol. 7237 (Springer, Berlin, Heidelberg, 2012).

[23] V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen, Swifft: A modest proposal for fft hashing, in *Fast Software Encryption*, edited by K. Nyberg, Lecture Notes in Computer Science Vol. 7237 (Springer, Berlin, 2008), pp. 54–72.

[24] S. Arunachalam and R. de Wolf, Guest column: A survey of quantum learning theory, SIGACT News **48**, 41 (2017).

[25] R. A. Servedio and S. J. Gortler, Equivalences and separations between quantum and classical learnability, SIAM J. Comput. **33**, 1067 (2004).

[26] A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R. H. Putra, and S. Yamashita, Quantum identification of boolean oracles, in *21st Annual Symposium on Theoretical Aspects of Computer Science, STACS 2004*, edited by V. Diekert and M. Habib, Lecture Notes in Computer Science Vol. 2996 (Springer, Berlin, Heidelberg, 2004), pp. 105–116.

[27] A. Atici and R. A. Servedio, Improved bounds on quantum learning algorithms, Quant. Info. Proc. **4**, 355 (2005).

[28] M. Hunziker, D. A. Meyer, J. Park, J. Pommersheim, and M. Rothstein, The geometry of quantum learning, Quant. Info. Proc. **9**, 321 (2010).

[29] A. Atici and R. A. Servedio, Quantum algorithms for learning and testing juntas, Quant. Info. Proc. **6**, 323 (2007).

[30] A. Belovs, Quantum algorithms for learning symmetric juntas via the adversary bound, Comput. Complex. **24**, 255 (2015).

[31] S. Arunachalam and R. de Wolf, Optimal quantum sample complexity of learning algorithms, in *32nd Computational Complexity Conference, CCC 2017*, edited by R. O'Donnell, LIPIcs (Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017), Vol. 79, pp. 1–31.

[32] D. Aharonov and A. Ta-Shma, Adiabatic quantum state generation and statistical zero knowledge, in *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing, STOC '03*, edited by L. L. Larmore and M. X. Goemans (ACM, New York, 2003), pp. 20–29.

[33] D. Boneh and M. Zhandry, Secure signatures and chosen ciphertext security in a quantum computing world, in *Advances in Cryptology – CRYPTO 2013*, edited by R. Canetti and J. A. Garay, Lecture Notes in Computer Science Vol. 8043 (Springer, Berlin, Heidelberg, 2013), pp. 361–379.

[34] I. Damgård, J. Funder, J. B. Nielsen, and L. Salvail, Superposition attacks on cryptographic protocols, in *Information Theoretic Security: 7th International Conference, ICITS 2013*, edited by C. Padró, Lecture Notes in Computer Science Vol. 8317 (Springer, Berlin, Heidelberg, 2008).

[35] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, Breaking symmetric cryptosystems using quantum period finding, in *Advances in Cryptology – CRYPTO 2016*, edited by M. Robshaw and J. Katz, Lecture Notes in Computer Science Vol. 9815 (Springer, Berlin, Heidelberg, 2008).

[36] M. Zhandry, How to construct quantum random functions, in *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012* (IEEE, 2012), pp. 679–687.

[37] G. Alagic, S. Jeffery, M. Ozols, and A. Poremba, On nonadaptive quantum chosen-ciphertext attacks and Learning with Errors, arXiv:1808.09655 (2018).

[38] K. K. H. Cheung and M. Mosca, Decomposing finite abelian groups, Quantum Inf. Comput. **1**, 26 (2001).

[39] M. Mosca, *Abelian Hidden Subgroup Problem* (Springer, Berlin, 2014), pp. 1–6.

[40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, New York, 2011).

[41] V. Lyubashevsky, C. Peikert, and O. Regev, On ideal lattices and learning with errors over rings, J. ACM **60**, 1 (2013).

[42] V. Lyubashevsky, C. Peikert, and O. Regev, A toolkit for ring-LWE cryptography, in *Advances in Cryptology – EUROCRYPT 2013*, edited by T. Johansson and P.Q. Nguyen, Lecture Notes in Computer Science Vol. 7881 (Springer, Berlin, Heidelberg, 2013), pp. 35–54.

[43] C. M. Mayer, Implementing a toolkit for ring-LWE based cryptography in arbitrary cyclotomic number fields, IACR Cryptology ePrint Archive **2016**, 49 (2016).

[44] X. Xie, R. Xue, and R. Zhang, Deterministic public key encryption and identity-based encryption from lattices in the auxiliary-input setting, in *Security and Cryptography for Networks, SCN 2012*, edited by I. Visconti and R. De Prisco, Lecture Notes in Computer Science Vol. 7485 (Springer, Berlin, Heidelberg, 2012), pp. 1–18.

[45] 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* (ACM, New York, 1996), pp. 99–108.

[46] D. Micciancio and C. Peikert, Hardness of sis and lwe with small parameters, in *Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013*, Part I, edited by R. Canetti and J. A. Garay, Lecture Notes in Computer Science Vol. 8042 (Springer, Berlin, Heidelberg, 2013), pp. 21–39.

[47] D. Micciancio and O. Regev, Worst-case to average-case reductions based on gaussian measures, SIAM J. Comput. **37**, 267 (2007).

[48] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, Lattice signatures and bimodal Gaussians, in *33rd Annual Cryptology Conference, CRYPTO 2013*, edited by R. Canetti and J. A. Garay, Lecture Notes in Computer Science Vol. 8042 (Springer, Berlin, Heidelberg, 2013), pp. 40–56.

[49] V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen, Swifft: A modest proposal for fft hashing, in *Fast Software Encryption, 15th International Workshop, FSE 2008*, edited by K. Nyberg, Lecture Notes in Computer Science Vol. 5086 (Springer, Berlin, Heidelberg, 2008), pp. 54–72.