Quantum and Post-Quantum Cryptography

Venkata Koppula[*]

January 2nd, 2023

Contents

Many thanks to Ramprasad Saptarishi for this LaTeX template.

[*]kvenkata@cse.iitd.ac.in

Course Introduction

Lecture 1:
January 3rd, 2023

COL759 Recap

Let us start with a quick recap of a few basic principles of provable security from COL759. For any cryptographic primitive, recall the four-step recipe for a provably secure construction:

1. (Syntax and security definition) The first step is to define the syntax. This involves defining the various algorithms involved, as well as the correctness condition. For example, in the case of public key encryption, there is a setup algorithm that outputs a public key and a secret key, an encryption algorithm that uses the public key to encrypt a message (producing a ciphertext), and a decryption algorithm that uses the secret key to decrypt the ciphertext. Correctness requires that if a message m is encrypted using a public key, then decryption of the ciphertext using the corresponding secret key must produce m.

   Once the syntax is defined, we define security for the cryptographic primitive. This is usually done via a security game. For public key encryption, we defined the semantic security game between a challenger and an adversary. The challenger runs the setup algorithm to sample a secret key and a public key. It sends the public key to the adversary. Next, the adversary picks two distinct messages m_0 and m_1 (adversarially), and sends them to the challenger. The challenger encrypts one of them (using the public key) and sends the resulting ciphertext to the adversary. In order to win the game, the adversary must guess whether m_0 was encrypted, or m_1. An encryption scheme is secure if no polynomial time adversary can win this game with noticeable advantage.

2. (Choosing an appropriate cryptographic assumption) Most cryptography is based on cryptographic assumptions. These are computational problems which are believed to be 'hard'. For example, we saw computational problems such as RSA, DDH. The second step, therefore, is to choose an appropriate cryptographic assumption.

3. (Proposing a construction) Once we have chosen a cryptographic assumption, we propose a construction. Depending on the structure present in our cryptographic assumption, the constructions can be very different. For instance, compare the RSA based PKE scheme and the El-Gamal encryption scheme.

4. (Proof of security) The final step ties together the first three steps. We show that if there exists a polynomial time adversary that wins the security game (defined in Step 1) against our construction (given in Step 3), then there exists a polynomial time algorithm that solves the 'hard' computation problem (chosen in Step 2).

This recipe has worked very well so far (at least in theory). Decades of research in algorithms and complexity theory have given us many hard compu-

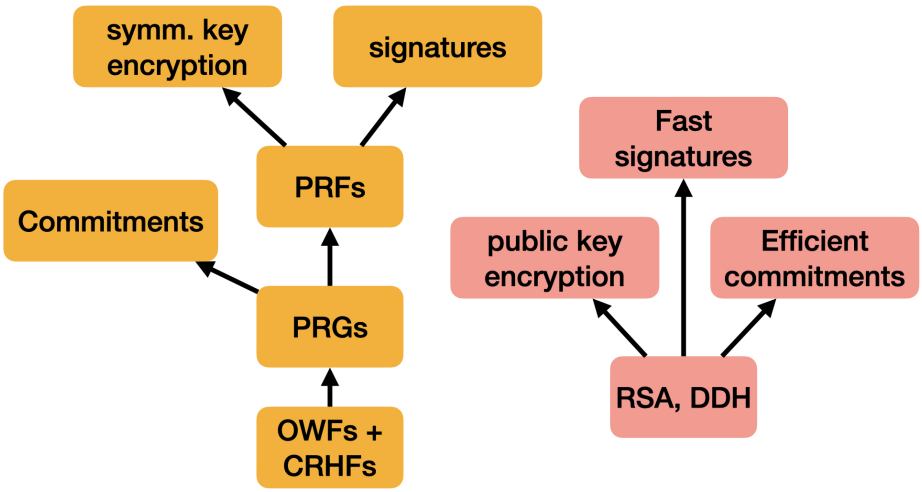


Figure 1: COL759: summarized in one figure. Some cryptographic primitives that can be built from OWFs and CRHFs. In practice, we have very efficient OWFs, PRGs, PRFs and CRHFs. Others such as public key encryption and key agreement rely on computational number-theoretic problems such as RSA or DDH.

tational problems, and some of them are well suited for building cryptographic primitives. Thanks to these hard computational problems, we have good confidence in our security systems.

What happens if someone finds an efficient algorithm for one of these hard problems? The natural idea then is to use a different hard problem, and hope that (a) it is structurally very different so that it doesn't succumb to the same attack (b) it still has enough structure to be useful for cryptography. This is the reason why we have different constructions for the same cryptographic primitive under a diverse set of assumptions.

Quantum computers are coming

In the recent years, there has been tremendous progress in the area of quantum computing. A couple of years ago, Google announced a 53 qubit quantum computer. Even though this quantum device was extremely noisy, Google claimed that it could solve certain computational problems within seconds, which would require much more time on a classical computer. While this demonstration is exciting news (and quantum computing has received much media attention due to this), this is bad news for cybersecurity. A lot of our modern protocols rely on number-theoretic problems such as RSA and DDH, and there exist efficient quantum algorithms for solving RSA and DDH. As a result, if we have a crypto primtive whose security is based on RSA/DDH, the security proof is useless in the presence of quantum adversaries.

Since then, other research groups have built quantum processors with 100+ qubits.

Fortunately, we do have computational problems which (a) are potentially quantum-resilient, (b) can be used for building cryptography (see Part I for

more details). In Section 1, we discuss how to build quantum resilient one-way functions and quantum-resilient collision resistant hash functions. In Section 2, we discuss how to build quantum-resilient public key encryption schemes. As a result, have we successfully dealt with all quantum adversaries (assuming the computational problems used in Section 1 and 2)? For instance, we saw (in the last two lectures of COL759) that OWFs + CRHFs suffice for building (classical) zero knowledge proofs. Does that mean that quantum-resilient OWFs + quantum-resilient CRHFs imply quantum-resilient zero knowledge proofs? Similarly, it is easy to show that the existence of secure public key encryption implies the existence of secure commitment schemes. Does this mean that quantum-resilient PKE implies quantum-resilient commitment schemes? The next section explores these questions in a bit more detail, and most of this course will revolve around such questions.

Challenges in the presence of quantum adversaries

This section will briefly discuss two scenarios where a classical proof/definition is not very useful in the presence of quantum adversaries.

Rewinding issue in quantum zero knowledge proofs

Towards the end of COL759, we saw the notion of zero knowledge proofs, and also saw that public key encryption can be used to build a secure zero knowledge protocol for the 3COL problem, and therefore we get a zero knowledge protocol for all of NP.

We will discuss these protocols in detail next week.

Suppose now we want a zero knowledge protocol in the presence of quantum adversaries. Let us focus on the zero-knowledge property. This involves cheating verifiers. Suppose we want to deal with cheating quantum verifiers. The security definition stays the same, except for a minor modification — we will need to allow the simulator to be a quantum polynomial time algorithm.

Definition Attempt (ZK property wrt quantum poly. time adversaries, informal)**.** *For every quantum polynomial time verifier $\mathbf{V}^*$, there exists a quantum polynomial time simulator S such that the verifier's view in the real protocol is indistinguishable from the simulator's output.*

Given this reasonable looking definition, can we replicate the classical proof for zero-knowledgeness? Unfortunately, no. The proof crucially relied on rewinding the verifier, and in the quantum setting, one needs to be very careful with regard to such arguments (and in particular, many of the classical proofs simply don't have an analogue in the quantum setting).

The curious case of commitments

In the last section, we saw that proofs of security may not translate to the quantum setting. For some cryptographic primitives, we might need new security definitions too. We will illustrate this using cryptographic commitments.

Recall the following toy motivation for commitments: there is a professor who gives very difficult assignments. The students want some 'proof' that the professor can solve the assignment. Commitments can be used in this scenario. The professor, when giving out the assignment, also produces a 'commitment'

to the solutions. This commitment must not reveal the committed solutions. Additionally, we also want the commitment to be binding. After the assignment deadline, the professor must produce an 'opening' which proves that he/she indeed committed to the solutions. Informally, we don't want the following scenario: the students submit solutions, and the professor uses one of those (correct) solutions to produce a matching opening. Let us formally define the syntax for commitments, and focus on the binding security game.

Last semester, we defined commitments as a one-round interactive protocol. Here, we are looking at a slightly weaker notion which is easier to work with. There is a honestly chosen public key, and the sender/receiver must use this public key. This allows us a 'non-interactive' commitment scheme.

NON-INTERACTIVE COMMITMENTS WITH SETUP : A non-interactive commitment scheme with setup consists of the following two algorithms:

- $\mathsf{Setup}(1^n)$: The setup algorithm takes as input the security parameter, and outputs a public key pk.
- $\mathsf{Commit}(\mathsf{pk}, m; r)$: The commitment algorithm takes as input a public key pk, message m and randomness r. It outputs a commitment com. The randomness r is used as the opening.

Last semester, we defined the following (strong) security game for binding:

Binding-Game

- Challenger chooses a public key pk using Setup and sends it to the adversary.
- Adversary produces a commitment com, and two messages m_0, m_1 and randomness r_0, r_1. The adversary wins if $\mathsf{Commit}(\mathsf{pk}, m_0; r_0) = \mathsf{Commit}(\mathsf{pk}, m_1; r_1) = \mathsf{com}$.

Figure 2: The Binding Security Game

Note, for our toy scenario, we only require a weaker security requirement for binding. I'll call this 'prof-binding':

In our informal lingo, weaker security requirement implies the adversary's job is harder, and therefore our 'expectations' from the commitment scheme are 'weaker'.

Prof-binding is not a standard notion; please don't use this outside our classroom :) We will give this a proper name when we discuss this in more detail.

Prof-Binding-Game

- Challenger chooses a public key pk using Setup and sends it to the adversary.
- Adversary produces a commitment com.
- Challenger picks a random message m and sends it to the adversary.
- Adversary produces randomness r and wins if $\mathsf{Commit}(\mathsf{pk}, m; r) = \mathsf{com}$.

Figure 3: The Prof-Binding Security Game

Prof-binding a weaker security requirement than (standard) binding, because if a commitment scheme satisfies binding, then it also satisfies prof-binding.

Claim. *Let $\mathcal{C} = (\mathsf{Setup}, \mathsf{Commit})$ be a commitment scheme. If there exists a p.p.t. adversary that wins the* Prof-Binding-Game *w.r.t. $\mathcal{C}$, then there exists a p.p.t. adversary that wins the* Binding-Game *w.r.t. $\mathcal{C}$.*

Sketch of Proof. Suppose there exists an adversary that wins the Prof-Binding-Game w.r.t. $\mathcal{C}$. The reduction algorithm works as follows:

- The reduction algorithm receives public key pk from the challenger, which it forwards to the adversary.
- Next, the adversary sends a commitment com. The reduction algorithm picks a uniformly random message m and sends to the adversary. The adversary sends opening r.
- The reduction then 'rewinds' the adversary to the point immediately after it sends com. The reduction chooses a new random message m' and sends it to this rewinded adversary. It receives r' as the new opening. Note that if the adversary successfully wins the Prof-Binding-Game, then $\mathsf{Commit}(\mathsf{pk}, m; r) = \mathsf{Commit}(\mathsf{pk}, m'; r') = \mathsf{com}$.
- The reduction algorithm sends (m, r) and (m', r') to the challenger, and wins the Binding-Game.

□

Note: It is important to rewind the adversary in this proof, and not restart the adversary's execution. This is because we want two (message, randomness) pairs *for the same commitment* com.

This claim, together with the claim you proved in Assignment 1 of COL759, give us the following result:

Claim. *Assuming the existence of secure PRGs, there exists a commitment scheme that satisfies binding security. Using the above claim, there also exists a commitment scheme that satisfies prof-binding security (assuming the existence of secure PRGs).*

Let us now focus our attention on the quantum analogues of these security definitions. The definition is quite natural — replace the 'p.p.t. adversary' with a 'quantum polynomial time adversary'. Your COL759 Assignment 1 proof can be adapted to get a commitment scheme that satisfies binding security w.r.t. quantum adversaries, assuming quantum-secure PRGs. However, the existence of quantum-secure PRGs **does not** immediately imply the existence of commitment schemes that satisfies prof-binding security w.r.t. quantum adversaries. Again, the issue is that we cannot rewind a quantum adversary. This brings us to the following questions:

What is the 'correct' definition for binding security in the presence of quantum adversaries? And if we care about prof-binding, then how do we construct such commitment schemes?

Going beyond classical messages

So far, we have considered classical crypto primitives in the presence of quantum adveraries. What happens if the messages themselves are *qubits* instead of classical bit strings? Can we commit to a quantum state, or encrypt a quantum state? Can we commit to a quantum state using only classical communication? These are some of the questions that we will consider in the final segment of our course.

Part I: Lattice-based Cryptography

Introduction to Lattice-based Cryptography

Notations We will use the following notations for this chapter (and most other chapters, unless specified otherwise).

- For any two integers $a < b$, $[a, b]$ denotes the set of integers $\{a, a+1, \ldots, b\}$.
- For a finite set S, Unif_S denotes the uniform distribution over S.
- For a finite set $\mathcal{S}$, $x \leftarrow \mathcal{S}$ denotes a uniformly random element drawn from $\mathcal{S}$. Similarly, for a distribution $\mathcal{D}$ over $\mathcal{S}$, $x \leftarrow \mathcal{D}$ denotes an element drawn from distribution $\mathcal{D}$.
- For any two distributions $\mathcal{D}_1, \mathcal{D}_2$ over a finite set $\mathcal{X}$, the statistical distance between $\mathcal{D}_1$ and $\mathcal{D}_2$, denoted by $\mathsf{SD}(\mathcal{D}_1, \mathcal{D}_2)$ is defined as follows:

  $$\mathsf{SD}(\mathcal{D}_1, \mathcal{D}_2) = \frac{1}{2}\left(\sum_{a \in \mathcal{X}} \left| \Pr_{x \leftarrow \mathcal{D}_1}[x = a] - \Pr_{x \leftarrow \mathcal{D}_2}[x = a] \right|\right)$$

  We say that two distributions are statistically indistinguishable, denoted by $\mathcal{D}_1 \approx_s \mathcal{D}_2$ if $\mathsf{SD}(\mathcal{D}_1, \mathcal{D}_2)$ is negligible in $n = \log|\mathcal{X}|$.

  If two distributions are statistically indistinguishable, then no algorithm can distinguish between these two distributions with non-negligible advantage.
- Let $\{\mathcal{X}_n\}_n$ be a family of finite sets, where $|\mathcal{X}_n| \leq 2^{\mathrm{poly}(n)}$ for some fixed polynomial $\mathrm{poly}(\cdot)$. For any two efficiently sampleable distributions $\mathcal{D}_1, \mathcal{D}_2$ over $\mathcal{X}_n$, the shorthand notation $\mathcal{D}_1 \approx_c \mathcal{D}_2$ indicates that the two distributions are computationally indistinguishable. That is, for any p.p.t. adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n,

  $$\Pr[\mathcal{A}(x) = 1 : x \leftarrow \mathcal{D}_1] - \Pr[\mathcal{A}(x) = 1 : x \leftarrow \mathcal{D}_2] \leq \mu(n).$$

1 The Short-Integer-Solutions Problem

The first (potentially) quantum-resilient assumption of this course is the Short Integer Solutions problem.

Computational Problem 1 (Short Integer Solution Problem ($\mathsf{SIS}_{n,m,q}$))**.** *Given a uniformly random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, output a nonzero vector $\mathbf{x} \in \{-1, 0, 1\}^m$ such that $\mathbf{A} \cdot \mathbf{x} \pmod q = \mathbf{0}$.*

The 'interesting' regime for this problem is when $n^{1.5} \leq q \leq \exp(n)$ and $m \geq \Omega(n \log q)$. If we did not have the constraint that $\mathbf{x} \in \{-1, 0, 1\}$, then this problem can be solved easily using Gaussian elimination. However, once we

add this restriction for $\mathbf{x}$, this problem is no longer easy. If m is large enough, then such a 'short integer solution' is guaranteed to exist (see exercise below).

Exercise 1.1. *Show that if $2^m > q^n$, then for every matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, there exists a vector $\mathbf{x} \in \{-1, 0, 1\}^m$ such that $\mathbf{A} \cdot \mathbf{x} \pmod q = \mathbf{0}$.*[a]

[a] An earlier version of this exercise had a 3^m instead of 2^m. As pointed out by one of the students in class, the old version was incorrect. Thanks for the correction.

However, finding such a short integer solution is believed to be hard (even given a quantum computer). Ajtai [Ajt96] showed that, in the interesting regime, if there exists an efficient algorithm for the SIS problem, then there exists an efficient algorithm for certain lattice problems in the *worst-case*.

The main parameters that govern the hardness of SIS: n and the size of modulus q. The exact form of q does not matter. The parameter m should be polynomial in n and $\log q$, but the exact value of m does not alter the hardness of SIS.

1.1 One-Way Functions and Collision Resistance from SIS

Recall, a collision resistant hash function family is a set of keyed functions such that, given a random function from this family, it is hard to find two inputs that map to the same output. Let q be a power of 2, and $m > 2n \log q$. Consider the following function family $\mathcal{H} = \left\{ H_{\mathbf{A}} : \{0,1\}^m \to \mathbb{Z}_q^n \right\}_{\mathbf{A} \in \mathbb{Z}_q^{n \times m}}$ where

$$H_{\mathbf{A}}(\mathbf{x}) = \mathbf{A} \cdot \mathbf{x} \pmod q$$

This is a compressing function since $m > 2n \log q$, and if there exist distinct bit-vectors $\mathbf{x}$ and $\mathbf{y}$ such that $\mathbf{A} \cdot \mathbf{x} = \mathbf{A} \cdot \mathbf{y}$, then $\mathbf{A} \cdot (\mathbf{x} - \mathbf{y}) = \mathbf{0}$, and $\mathbf{x} - \mathbf{y} \in \{-1, 0, 1\}^m$.[1]

Since this function family is sufficiently compressing, collision resistance implies one-wayness.

Exercise 1.2. *Show that if $\mathcal{H} = \left\{ H_k : \{0,1\}^{2n} \to \{0,1\}^n \right\}_{k \in \mathcal{K}}$ is a collision-resistant hash function family, then $\mathcal{H}$ is also a one-way function family.*

However, this does not hold true if $\mathcal{H}$ is only mildly-compressing. That is, suppose $\mathcal{H} = \left\{ H_k : \{0,1\}^{n+1} \to \{0,1\}^n \right\}_{k \in \mathcal{K}}$ is a collision-resistant hash function family. Construct a new hash function family $\mathcal{H}'$ that is also collision-resistant, but $\mathcal{H}'$ is not one-way.

1.2 Commitment Scheme from SIS

In this section, we will present a non-interactive commitment scheme with setup, based on SIS. For this construction, we will consider a variant of SIS, called 'inhomogeneous SIS' (iSIS).

Computational Problem 2 (Inhomogeneous Short Integer Solution Problem ($\mathsf{iSIS}_{n,m,q}$))**.** *Given a uniformly random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and a uniformly random vector $\mathbf{b} \leftarrow \mathbb{Z}_q^n$, output a nonzero vector $\mathbf{x} \in \{-1, 0, 1\}^m$ such that $\mathbf{A} \cdot \mathbf{x} \pmod q = \mathbf{b}$.*

[1] All these equalities are modulo q, I will ignore $\pmod q$ when it is clear from the context.

It is easy to show that this variant is as hard as SIS.

Exercise 1.3. *Show that there exists a p.p.t. adversary that solves* $\mathsf{iSIS}_{n,m,q}$ *with non-negligible probability, if and only if there exists a p.p.t. adversary that solves* $\mathsf{SIS}_{n,m,q}$ *with non-negligible probability.*

The iSIS gives a direct proof of one-wayness of $\{H_{\mathbf{A}} \equiv \mathbf{A} \cdot \mathbf{x}\}_{\mathbf{A}}$. This proof goes via the *leftover hash lemma*, a useful lemma that we'll encounter multiple times in this course. Essentially, this lemma says that if m is sufficiently larger than $n \log q$, then given a random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, the vector $\mathbf{A} \cdot \mathbf{x}$, where $\mathbf{x}$ is drawn from a distribution with enough randomness, looks like a uniformly random vector in $\mathbb{Z}_q^n$. We will not prove this lemma here (you can refer to [AB09] for a proof of the lemma).

Fact 1 (Leftover Hash Lemma)**.** *Let $S \subset \mathbb{Z}_q$, $|S| = B$. If $m \geq n \log_B q + n$, then the statistical distance between the following distributions is a negligible funtion of n:*

$$\mathcal{D}_1 = \left\{ (\mathbf{A}, \mathbf{A} \cdot \mathbf{x}) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}, \\ \mathbf{x} \leftarrow S^m \end{array} \right\} \qquad \mathcal{D}_2 = \left\{ (\mathbf{A}, \mathbf{u}) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}, \\ \mathbf{u} \leftarrow \mathbb{Z}_q^n \end{array} \right\}$$

This is a simplified version of the leftover hash lemma. The 'full version' states that for any distribution $\mathcal{D}$ over $\mathbb{Z}_q^m$ with sufficient entropy, if $\mathbf{x} \leftarrow \mathcal{D}$, then $(\mathbf{A}, \mathbf{A} \cdot \mathbf{x}) \approx_s (\mathbf{A}, \mathbf{U})$.

A short discussion on LHL: First, let us understand where the name of this lemma comes from. The 'hash' in the name arises because the function $\mathbf{x} \to \mathbf{A} \cdot \mathbf{x}$ is a pairwise independent hash function mapping $\{0,1\}^m$ to $\mathbb{Z}_q^n$. The 'leftover' in the name comes from the following scenario that arises often in crypto/-complexity: suppose you have a source of randomness X that outputs t bits of randomness, and you know that there is an adversary that has somehow learnt k out of t bits. You don't know which bits the adversary knows. Given that the adversary has only k bits of information, you still have $t - k$ bits of randomness *left over*. The leftover hash lemma says that by choosing an appropriate hash function, you can indeed extract somme pure randomness out of this corrupted source.

A more concrete scenario: Alice and Bob are performing the Diffie-Hellman key exchange protocol. Alice chooses a group generator g, an integer $a \leftarrow \mathbb{Z}_q$ and sends (g, g^a) to Bob. Bob chooses $b \leftarrow \mathbb{Z}_q$ and sends g^b to Alice. Both can now compute g^{ab} (and therefore both have $\log q$ random bits). But suppose the adversary can learn t bits about b. Such things can happen in practice, and are known as *side channel attacks*. For instance, maybe the adversary is close to Bob's computer and is monitoring the electromagnetic radiations when Bob is computing g^b. Now we cannot conclude that Bob has no information about the shared key g^{ab}. To take care of this situation, Alice also sends an appropriate hash function (say a matrix $\mathbf{A}$). Instead of using g^{ab} as the shared key, both Alice and Bob must first express g^{ab} as a bit string $\mathbf{x}$, and then use the hash of $\mathbf{x}$ (that is, $\mathbf{A} \cdot \mathbf{x}$) as the shared key.

Exercise 1.4. *Let $m = n$. Compute a lower bound on the statistical distance*

between the following distributions:

$$\mathcal{D}_1 = \left\{ (\mathbf{A}, \mathbf{A}\cdot\mathbf{x}) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}, \\ \mathbf{x} \leftarrow \{0,1\}^m \end{array} \right\} \quad \mathcal{D}_2 = \left\{ (\mathbf{A}, \mathbf{u}) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}, \\ \mathbf{u} \leftarrow \mathbb{Z}_q^{n} \end{array} \right\}$$

Let us put the leftover hash lemma to good use. Recall, last semester we had discussed that OWFs can be used to build PRGs, and in one of your assignments, you had constructed a commitment scheme using PRGs. Therefore, following this approach, we have a commitment scheme whose security is based on SIS. There is a simpler direct construction based on SIS, which is described below.

Lecture 2: January 6th, 2023

Construction 1.5 (Commitment scheme from SIS)**.** *The message space for our commitment scheme is $\{0,1\}^m$, and the sender's commitment algorithm uses m bits of randomness.*

- $\mathsf{Setup}(1^n)$: *The setup algorithm samples two matrices $\mathbf{A}_1, \mathbf{A}_2 \leftarrow \mathbb{Z}_q^{n\times m}$ and sets $\mathsf{pk} = (\mathbf{A}_1, \mathbf{A}_2)$.*
- $\mathsf{Commit}(\mathsf{pk}, \mathsf{msg})$: *The commit algorithm chooses a uniformly random bit string $\mathbf{r} \leftarrow \{0,1\}^m$ and sets $\mathsf{s\text{-}msg} = \mathbf{A}_1 \cdot \mathsf{msg} + \mathbf{A}_2 \cdot \mathbf{r}$.*

$\Diamond$

The binding property is similar to the collision-resistance of $\mathcal{H}$ (discussed in Section 1.1 above). The reduction algorithm receives a matrix $\mathbf{A} = [\mathbf{A}_1 \mid \mathbf{A}_2]$ from the SIS challenger. It sends $\mathsf{pk} = (\mathbf{A}_1, \mathbf{A}_2)$ and sends it to the adversary. The adversary then produces $\mathsf{msg}_0, r_0, \mathsf{msg}_1, r_1$ (each of which is an m bit string) and wins if $\mathbf{A}_1 \cdot \mathsf{msg}_0 + \mathbf{A}_2 \cdot r_0 = \mathbf{A}_1 \cdot \mathsf{msg}_1 + \mathbf{A}_2 \cdot r_1$. The reduction algorithm sends $\mathbf{x} = [\mathsf{msg}_0 \mid r_0]^\top - [\mathsf{msg}_1 \mid r_1]^\top$ to the SIS challenger.

For hiding, note that the commitment $\mathsf{com} = \mathbf{A}_1 \cdot \mathsf{msg} + \mathbf{A}_2 \cdot r$. Using the leftover hash lemma, it follows that $\left\{ (\mathbf{A}_2, \mathbf{A}_2 \cdot r) : \mathbf{A}_2 \leftarrow \mathbb{Z}_q^{n\times m}, r \leftarrow \{0,1\}^m \right\} \approx_s \left\{ (\mathbf{A}_2, \mathbf{u}) : \mathbf{A}_2 \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{u} \leftarrow \mathbb{Z}_q^n \right\}$. As a result, com is statistically indistinguishable from a uniformly random vector, and as a result, even an exponential time adversary cannot recover the message given the commitment.

Summing it up, we have the following claim.

Claim 1.6. *Let $m = 2n \log q$. Assuming $\mathsf{SIS}_{n,2m,q}$ is computationally hard, the non-interactive commitment scheme with setup described in Construction 1.5 is computationally binding (that is, no polynomial time adversary can win* Binding-Game *defined in Figure 4) and statistically hiding (no adversary can win the hiding game defined in Figure 5).*

Exercise 1.7. *The commitment scheme in Construction 1.5 involves a honest setup. In COL759 Assignment 1, you had built a stronger commitment scheme. In that scheme, the receiver chooses the first message (there is no trusted setup). Would the above construction satisfy that stronger definition?*

Another way to remove honest setup is to allow the sender to run the setup (in this case, choose matrices $\mathbf{A}_1, \mathbf{A}_2$). Would that be secure?

Exercise 1.8. *The commitment scheme described in Construction 1.5 is computationally binding and statistically hiding. Similarly, one can define and construct commitment schemes that are statistically binding and computationally hiding.*

Prove that it is impossible to construct a commitment scheme that is statistically binding and statistically hiding.

2 The Learning-with-Errors Problem

The SIS problem can be used to build OWFs, CRHFs, but the real quantum threat is for public key encryption (and other crypto primitives that rely on RSA/DDH). Fortunately, we have another computational problem that is also believed to be quantum-resilient, and has enough structure to give us public key encryption (and much more). This problem is closely related to the SIS problem, and is called the 'Learning with Errors' problem. The (decisional) Learning with Errors problem is parameterized by matrix dimensions n, m, modulus q and a 'noise distribution' χ over $\mathbb{Z}_q$.

For the purpose of this course, it suffices to think of q as a $\sqrt{n}$-bit prime and χ as uniform distribution over $\{-B, B\}$, where B is much smaller than q. For instance, take $B = \sqrt{q}$.

Computational Problem 3 (Learning with Errors Problem ($\mathsf{LWE}_{n,m,q,\chi}$))**.** *Distinguish between the following distributions:*

$$\mathcal{D}_1 = \left\{ (\mathbf{A}, \mathbf{s}^\top \cdot \mathbf{A} + \mathbf{e}^\top) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m} \\ \mathbf{s} \leftarrow \mathbb{Z}_q^n \\ \mathbf{e} \leftarrow \chi^m \end{array} \right\} \quad \mathcal{D}_2 = \left\{ (\mathbf{A}, \mathbf{u}^\top) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{m \times n} \\ \mathbf{u} \leftarrow \mathbb{Z}_q^m \end{array} \right\}$$

We will call samples from $\mathcal{D}_1$ as 'LWE pairs'.

A few noteworthy points about this problem:

- The vector $\mathbf{e}$ is the 'error vector'. If there was no error vector, then it is easy to distinguish between the two distributions (using Gaussian elimination).
- There is a corresponding 'search' version of this problem, where given $(\mathbf{A}, \mathbf{s}^\top \cdot \mathbf{A} + \mathbf{e}^\top)$, one must learn $\mathbf{s}$ (hence the name 'learning with errors'). We have a search-to-decision reduction for LWE, and therefore it suffices to restrict our attention to the decision version.
- Suppose $q = O(2^{\sqrt{n}})$, and let χ be the uniform distribution over $[-\sqrt{q}, \sqrt{q}]$. Let us compute the amount of randomness needed to get one sample from each of the distributions. In the distribution $\mathcal{D}_2$, we require $(n \cdot m + m) \cdot \log q \approx (n \cdot m + m) \cdot \sqrt{n}$ bits of randomness (per sample). In $\mathcal{D}_1$, the amount of randomness (per sample) is $n \cdot m \cdot \sqrt{n} + n \log q + m \cdot \log B \approx n \cdot m \cdot \sqrt{n} + n \cdot \sqrt{n} + m \cdot \sqrt{n}/2$. As a result, if m is larger than $2n$, these two distributions are statistically far-apart (and hence an unbounded adversary can distinguish between these two distributions). However, a computationally bounded adversary cannot distinguish between the two distributions (assuming $\mathsf{LWE}_{n,m,q,\chi}$ is hard).

- Just like the SIS problem, LWE is interesting only when m is larger than n. For instance, if $m \leq n$, then the two distributions are statistically indistinguishable.

The Learning with Errors problem was introduced in the landmark paper of Regev [Reg09]. The key contributions of this paper are as follows:

- Regev showed that the search version of LWE is as hard as some well studied lattice problems. His reduction was a **quantum** reduction. That is, he showed that if there exists an algorithm (classical or quantum) that solves the search version of LWE, then there exists a quantum algorithm for solving all instances of hard lattice problems.

The main parameters that govern the hardness of LWE: size of q and the modulus/noise ratio. Again, it does not depend much on the parameter m. Similarly, it does not depend on the form of q.

- Next, he showed that decisional LWE is as hard as the search version. His reduction was for modulus having certain properties, but this was later extended to work for all moduli.
- Finally, Regev showed that this is a very useful assumption for cryptography. Regev showed how to build public key encryption from decisional LWE. Soon after, researchers realized that this is a very useful assumption for crypto.

Thanks to one of the students for raising this question in class.

If the error is very small, say each coordinate is bounded by some constant value B, then there is a polynomial time attack on LWE, shown by Arora and Ge [AG11]. There are other subexponential time attacks for specialized parameter settings. However, for the version described above, currently there is no known algorithm that runs in time $o(2^n)$.

2.1 *LWE and SIS*

SIS and LWE are closely related problems. Both these problems, with minor modification, become 'easy' problems via Gaussian elimination. In SIS, if we remove the restriction that $x \in \{-1, 0, 1\}^m$, then the problem can be solved efficiently. Similarly, in LWE, if we remove the error, then this problem can also be solved efficiently.

The following observation shows that SIS is as hard as LWE.

Observation 2.1 (SIS $\geq$ LWE)**.** *If there exists a p.p.t. algorithm that solves* $\mathsf{SIS}_{n,m,q}$ *(as defined in Section 1), then there exists a p.p.t. algorithm that solves* $\mathsf{LWE}_{n,m,q,\chi}$*.*

Sketch of Proof. The reduction algorithm receives $(\mathbf{A}, \mathbf{b})$ from the LWE challenger. It sends $\mathbf{A}$ to the SIS adversary, and receives $\mathbf{x} \in \{-1, 0, 1\}^m$. If $\mathbf{A} \cdot \mathbf{x} = \mathbf{0}$, then the reduction checks if $\mathbf{b}^\top \cdot \mathbf{x}$ is in $[0, q/4] \cup [3q/4, q]$. If so, it concludes that $(\mathbf{A}, \mathbf{b})$ is an LWE pair. Else it concludes that $(\mathbf{A}, \mathbf{b})$ are uniformly random. □

The other direction (LWE $\geq$ SIS) is interesting. Currently, we don't know a classical reduction, but a quantum reduction follows from Regev's work. I do not plan to discuss this reduction in this course. However, if there's sufficient interest in seeing this reduction, I am happy to include it in one of the later lectures.

2.2 *Cryptographic Primitives from LWE*

LWE is a very versatile cryptographic assumption. When it was proposed by Regev, it was introduced as a post-quantum hardness assumption that implies public key encryption. However, over the next few years, researchers showed various advanced cryptographic primitives that can be built using LWE. We will see a few of them in this course.

First, note that LWE immediately gives us a pseudorandom generator. This is because the LWE distribution uses fewer random bits than the uniform distribution, yet is computationally indistinguishable from the uniform distribution. PRGs imply PRFs, which in turn imply semantically secure symmetric-key encryption. However, let us look at a direct construction of symmetric key encryption based on LWE. This will serve as a warm-up for public-key encryption.

Lecture 3: January 10th, 2023

Symmetric Key Encryption using LWE

Construction 2.2 (Symmetric key encryption scheme based on LWE)**.** *Let $q = 2^{\sqrt{n}}$, $m = O(n \log q)$, $\chi \equiv \mathsf{Unif}_{[-\sqrt{q},\sqrt{q}]}$ be the LWE parameters. The message space is $\{0,1\}$, and the secret key is a vector $\mathbf{s} \in \mathbb{Z}_q^n$.*

- $\mathsf{Enc}(\mathbf{s}, \mathsf{msg})$*: Choose a random vector $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ and $e \leftarrow \chi$, output* $\mathsf{ct} = \left(\mathbf{c}_1 = \mathbf{a}, c_2 = \mathbf{s}^\top \cdot \mathbf{a} + e + \mathsf{msg} \cdot \frac{q}{2}\right)$.
- $\mathsf{Dec}(\mathbf{s}, \mathsf{ct} = (\mathbf{c}_1, c_2))$*: If $c_2 - \mathbf{s}^\top \cdot \mathbf{c}_1$ is in the range $[q/4, 3q/4]$, then output* 1*, else output* 0*.*

$\Diamond$

Perfect correctness: The correctness of this scheme follows immediately. Since χ is the uniform distribution over $[0, \sqrt{q}] \cup [q - \sqrt{q}, q]$, if $e \leftarrow \chi$, then $e + q/2 \pmod q$ will be in the range $[q/4, 3q/4]$.

Semantic security proof sketch: Suppose an adversary $\mathcal{A}$ makes at most t queries and breaks the semantic security of this scheme. Then there exists a reduction algorithm that breaks the $\mathsf{LWE}_{n,t,q,\chi}$ assumption. The reduction receives an $n \times t$ matrix $\mathbf{A}$ and a vector $\mathbf{b} \in \mathbb{Z}_q^t$ from the LWE challenger. For the i^{th} encryption query by $\mathcal{A}$, the reduction uses the i^{th} column of $\mathbf{A}$ and the i^{th} entry of $\mathbf{b}$.

Additive homomorphism The above scheme has the following property (which is easy to verify): we can 'add' ciphertexts, and the underlying messages get added $\pmod 2$. Given encryption $\mathsf{ct} = (\mathbf{c}_1, c_2)$ of message msg and encryption $\mathsf{ct}' = (\mathbf{c}_1', c_2')$ of message msg', we can produce an encryption of $\mathsf{msg} \oplus \mathsf{msg}'$. This is simply $(\mathbf{c}_1 + \mathbf{c}_1', c_2 + c_2')$.[2] Note that the error grows slightly, but perfect decryption still holds.

[2] Again, I am ignoring the $\bmod\ q$ here.

Similarly, given an encryption ct of msg, we can also produce an encryption of the negation $1 \oplus \mathsf{msg}$ (without knowing msg).

I will refer to this as 'homomorphic negation'.

Later in the course, we will see how to perform arbitrary computations over ciphertexts.

Another approach for building symmetric key encryption from LWE The following scheme was proposed in class:

Construction 2.3 (Another SKE scheme based on LWE)**.** *Let $q = 2^{\sqrt{n}}$, $m = O(n \log q)$, $\chi \equiv \mathsf{Unif}_{[-\sqrt{q},\sqrt{q}]}$ be the LWE parameters. The message space is $\{0,1\}$, and the secret key is a vector $\mathbf{s} \in \mathbb{Z}_q^n$.*

- $\mathsf{Enc}(\mathbf{s}, \mathsf{msg})$*: Choose two random matrices $\mathbf{A}_0, \mathbf{A}_1$ of dimensions $n \times n$ and an error vector $\mathbf{e} \leftarrow \chi^n$. Compute $\mathbf{c} = \mathbf{s}^\top \cdot \mathbf{A}_{\mathsf{msg}} + \mathbf{e}$ and output $(\mathbf{A}_0, \mathbf{A}_1, \mathbf{c})$ as the ciphertext.*
- $\mathsf{Dec}(\mathbf{s}, \mathsf{ct} = (\mathbf{A}_0, \mathbf{A}_1, \mathbf{c}))$*: If $\|\mathbf{c} - \mathbf{s}^\top \cdot \mathbf{A}_0\| \le q/4$, output 0, else output 1.*

$\Diamond$

Suppose the adversary makes at most t queries. This scheme is semantically secure, assuming $\mathsf{LWE}_{n,nt,q,\chi}$ is hard. However, this scheme has a small (negligible) decryption error. Negligible decryption error is mostly fine. However, for certain applications (see Section 2.2), we require perfect correctness. Also, this scheme does not seem to have the homomorphism property (which will be useful in the following section).

Why is it reasonable to assume that we know a bound on the adversary's running time/number of queries? The reduction can always 'guess' a bound on the number of queries. As long as the adversary's view is unaffected by this guess, we are fine.

Exercise 2.4. *Modify the above construction (Construction 2.3) to achieve perfect correctness.*

Public Key Encryption using LWE

Let us now extend Construction 2.2 to build a public key encryption scheme. We will first propose an abstract framework for going from SKE to PKE, and then present a concrete LWE-based construction. Suppose there is a symmetric key encryption scheme $\mathcal{E}_{\mathrm{SKE}} = (\mathsf{Setup}_{\mathrm{SKE}}, \mathsf{Enc}_{\mathrm{SKE}}, \mathsf{Dec}_{\mathrm{SKE}})$ with perfect correctness, and supporting additive homomorphism and homomorphic negation. The message space is $\{0,1\}$, and the ciphertext space is $\{0,1\}^\ell$.

$\mathcal{E}_{\mathrm{SKE}} \to \mathcal{E}_{\mathrm{PKE}}$ framework: In our public key encryption scheme, the setup algorithm runs the symmetric key setup $\mathsf{Setup}_{\mathrm{SKE}}$, generating a secret key sk. Next, it produces *many* encryptions of 0. How many depends on the ciphertext size (which is ℓ). Suppose it produces m ciphertexts. The public key consists of these m encryptions of zero.

To encrypt a bit msg using this public key, we do the following: if $\mathsf{msg} = 0$, pick a random subset S of these ciphertexts, and 'add' them together. Thanks to the additive homomorphism, this resulting ciphertext will also be an encryption of

0. If $\mathsf{msg} = 1$, we will again pick a random subset S of these ciphertexts, and add them together. Finally, we will homomorphically negate the resulting ciphertext, resulting in an encryption of 1.

It follows, from the additive homomorphism and perfect correctness, that the resulting public key encryption scheme is also perfectly correct. Why is it secure? Here again, leftover hash lemma is our friend. Note, we are mapping the random subset S (which can be described using m bits) to an ℓ bit string. If this mapping is a 'nice' hash such that LHL can be applied, then the resulting ciphertext looks like a uniformly random string.

An instantiation of the above framework - Regev's encryption scheme Below we discuss the public key encryption scheme proposed by Regev.

In Regev's scheme, the modulus was polynomial, and hence there was a small decryption error.

Construction 2.5 (Regev's PKE scheme based on LWE)**.** *Let $q = 2^{\sqrt{n}}$, $m = O(n \log q)$, $\chi \equiv \mathsf{Unif}_{[-\sqrt{q},\sqrt{q}]}$ be the LWE parameters.*
Regev encryption scheme for message space $\{0,1\}$ can be specified as follows:

- $\mathsf{Setup}(1^n)$*: It sets m, q, χ as above. It sample a random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, a random secret vector $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, and a random error vector $\mathbf{e} \leftarrow \chi^m$. It outputs the public-secret key pair as:*

$$\mathsf{pk} = (\mathbf{A}, \mathbf{b}) \text{ where } \mathbf{b}^\top = \mathbf{s}^\top \cdot \mathbf{A} + \mathbf{e}^\top, \quad \mathsf{sk} = \mathbf{s}.$$

- $\mathsf{Enc}(\mathsf{pk}, \mathsf{msg})$*: Let $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$. It samples a random vector $\mathbf{r} \leftarrow \{0,1\}^m$. It outputs the ciphertext as:*

$$\mathsf{ct} = \left(\mathbf{A} \cdot \mathbf{r}, \mathbf{b}^\top \cdot \mathbf{r} + \mathsf{msg} \cdot \frac{q}{2}\right).$$

- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$*: Let the ciphertext $\mathsf{ct} = (\mathbf{c}_1, c_2)$. It outputs the message bit as:*

$$\mathsf{round}^{q/2}(c_2 - \mathbf{c}_1^\top \cdot \mathbf{s}),$$

where $\mathsf{round}^{q/2}(z)$ rounds an element $z \in \mathbb{Z}_q$ to 1 if $z \in [q/4, 3q/4]$ and 0 otherwise.

$\Diamond$

Perfect correctness: The correctness of this scheme relies on the following observation: the quantity $\mathbf{e}^\top \cdot \mathbf{r} \bmod q$ will never be in the range $[q/4, 3q, 4]$. This is because $\mathbf{e} \in [-\sqrt{q}, \sqrt{q}]^m$ and $\mathbf{r} \in \{0,1\}^m$.

Similarly, $(q/2 + \mathbf{r}^\top \cdot \mathbf{e}) \bmod q$ will never be in the range $[0, q/4] \cup [3q/4, q]$. Therefore, $\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, \mathsf{msg})) = \mathsf{msg}$ for $\mathsf{msg} \in \{0,1\}$.

Semantic security proof sketch: Using LWE, we can first switch $\mathbf{b}$ to be a uniformly random vector. Once we have done that, note that using the leftover hash lemma (Fact 1), $(\mathbf{A} \cdot \mathbf{r}, \mathbf{b}^\top \cdot \mathbf{r})$ looks like a uniformly random vector in $\mathbb{Z}_q^{n+1}$. This concludes our proof sketch.

Viewing Regev's scheme via the $\mathcal{E}_{\text{SKE}} \to \mathcal{E}_{\text{PKE}}$ framework: The public key in Regev's scheme is a matrix $\mathbf{A}$ and vector $\mathbf{b}^\top = \mathbf{s}^\top \cdot \mathbf{A} + \mathbf{e}^\top$. We can view the public key as m encryptions of 0, using the secret vector $\mathbf{s}$.

To encrypt a message bit msg, Regev's scheme computes $\mathbf{A} \cdot \mathbf{r}$ and $\mathbf{b}^\top \cdot \mathbf{r} + \mathsf{msg} \cdot \frac{q}{2}$, where $\mathbf{r} \leftarrow \{0,1\}^m$. Note that $\mathbf{r}$ is used to sample a subset of the columns of $\mathbf{A}$ (and similarly the same subset of the entries of $\mathbf{b}$). As a result, we are taking a random subset of the zero encryptions present in the public key, and adding them together. If $\mathsf{msg} = 0$, then this is our final ciphertext. Otherwise we add $\frac{q}{2}$.

Finally, we need to argue security. The random set (viewed as an m bit string) is mapped to a ciphertext (which consists of $n+1$ integers in $\mathbb{Z}_q$). Therefore, if m is sufficiently larger than $n \log q$, then there's some hope of using LHL. The hashing from the set to $n+1$ integers uses $(\mathbf{A}, \mathbf{b})$, but they're not uniformly random. However, using the LWE assumption, we argue that $\mathbf{A}, \mathbf{b}$ are computationally indistinguishable from uniformly random, and once that is done, we can use LHL.

Thanks to one of the students for raising this question in class.

Exercise 2.6. *Suppose an encryption scheme has message space $\{0,1\}^t$ and ciphertext space $\{0,1\}^\ell$. The* encryption rate *of this scheme is defined as t/ℓ. Clearly, high-rate would be desirable for efficiency reasons.*

Note that the rate of Regev's encryption scheme (as described in Construction 2.9) is $\Theta(1/n \log q) = 1/n\sqrt{n}$. Modify the construction to improve the rate to $\Theta(1/\sqrt{n})$.

Non-interactive commitments (without setup) from LWE

In Construction 1.6, we built a commitment scheme (based on SIS) that required an honest setup. In this section, we will see a simple construction that does not require any setup or interaction. This commitment scheme can be built *generically from any PKE with perfect correctness*. Therefore, using Regev's encryption scheme, we have a noninteractive commitment scheme without setup.

Construction 2.7 (Noninteractive commitments without setup)**.** *Let $\mathcal{E}_{\text{PKE}} = (\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme with message space $\mathcal{M}$, and having perfect correctness.*

- $\mathsf{Commit}(\mathsf{msg} \in \mathcal{M}, 1^n)$*: The commitment algorithm takes as input the message* msg *and security parameter n. It chooses* $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^n)$*, computes* $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{msg})$ *and sends* $(\mathsf{pk}, \mathsf{ct})$ *as the commitment.*

The opening for the commitment is the randomness used by Setup *and* Enc. ◊

The hiding property follows immediately from the semantic security of $\mathcal{E}_{\text{PKE}}$. However, we need to be careful with the binding property. Recall, in Construction 1.5, when we allowed the sender to choose $(\mathbf{A}_1, \mathbf{A}_2)$, then we could not guarantee the binding property. Here also, the same issue could arise: *what if the adversarial sender can choose 'malicious' public key* pk *and ciphertext* ct *such that there exist two secret keys* $\mathsf{sk}_0, \mathsf{sk}_1$ *with the property that both can be tied to* pk*, and* $\mathsf{Dec}(\mathsf{sk}_b, \mathsf{ct}) = \mathsf{msg}_b$*?*

Here, we will use the perfect correctness of $\mathcal{E}_{\text{PKE}}$. Since the scheme is perfectly correct, for every $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Setup}(1^n)$, every message $\mathsf{msg} \in \mathcal{M}$ and every $\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$, $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) = \mathsf{msg}$. Suppose an adversary can break the binding property. Then it can output a public key pk, a ciphertext ct and randomness pairs $(r_{\mathsf{Setup},0}, r_{\mathsf{Enc},0})$ and $(r_{\mathsf{Setup},1}, r_{\mathsf{Enc},1})$ such that

- $\mathsf{Setup}(1^n; r_{\mathsf{Setup},b}) = (\mathsf{pk}, \mathsf{sk}_b)$
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{msg}_0; r_{\mathsf{Enc},0}) = \mathsf{Enc}(\mathsf{pk}, \mathsf{msg}_1; r_{\mathsf{Enc},1}) = \mathsf{ct}$.

This would violate the perfect correctness. There exists a public key/secret key pair $(\mathsf{pk}, \mathsf{sk}_0)$, a message msg_1, a ciphertext $\mathsf{ct} = \mathsf{Enc}(\mathsf{pk}, \mathsf{msg}_1; r_{\mathsf{Enc},1})$ such that $\mathsf{Dec}(\mathsf{sk}_0, \mathsf{ct}) = \mathsf{msg}_0$.

2.3 *Variants of LWE*

Just like we saw for SIS, there are a number of variants of LWE that are as hard as vanilla LWE. Here, we discuss one variant where the secret vector, instead of being a uniformly random vector, is drawn from the noise distribution. This is called *small-secrets LWE*, since the secret vector consists of small entries.

Computational Problem 4 (Small Secrets Learning with Errors Problem ($\mathsf{ss\text{-}LWE}_{n,m,q,\chi}$))**.** *Distinguish between the following distributions:*

$$\mathcal{D}_1 = \left\{ (\mathbf{A}, \mathbf{s}^\top \cdot \mathbf{A} + \mathbf{e}^\top) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m} \\ \mathbf{s} \leftarrow \chi^n \\ \mathbf{e} \leftarrow \chi^m \end{array} \right\} \quad \mathcal{D}_2 = \left\{ (\mathbf{A}, \mathbf{u}^\top) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m} \\ \mathbf{u} \leftarrow \mathbb{Z}_q^{m} \end{array} \right\}$$

Clearly, LWE is as hard as ssLWE, since $\mathsf{uniform} + \chi \equiv \mathsf{uniform}$. The following claim shows that small-secret LWE is as hard as LWE (albeit with a slight increase in m - the number of columns).

Claim 2.8 ($\mathsf{ss\text{-}LWE} \geq \mathsf{LWE}$)**.** *Let q be a prime. If there exists a p.p.t. algorithm $\mathcal{A}$ that solves $\mathsf{ss\text{-}LWE}_{n,m-n,q,\chi}$, then there exists a p.p.t. algorithm $\mathcal{B}$ that solves $\mathsf{LWE}_{n,m,q,\chi}$.*

Sketch of Proof. The reduction algorithm receives $(\mathbf{A}, \mathbf{b})$ from the LWE challenger. Let $\mathbf{A}_1$ denote the first n columns of $\mathbf{A}$, and $\mathbf{A}_2$ the last $m - n$ columns. Since $\mathbf{A}$ is chosen uniformly at random, $\mathbf{A}_1$ is invertible (with high probability). Let $\mathbf{b}_1$ denote the first n entries of $\mathbf{b}$, and $\mathbf{b}_2$ the remaining $m - n$ entries. If $(\mathbf{A}, \mathbf{b})$ is a $\mathsf{LWE}_{n,m,q,\chi}$ pair and $\mathbf{b}^\top = \mathbf{s}^\top \cdot \mathbf{A} + \mathbf{e}^\top$, then $\mathbf{b}_1 = \mathbf{s}^\top \cdot \mathbf{A}_1 + \mathbf{e}_1^\top$ and $\mathbf{b}_2 = \mathbf{s}^\top \cdot \mathbf{A}_2 + \mathbf{e}_2^\top$.

Computing the inverse of $\mathbf{A}_1$ is the only place where we've used the primality of q.

Let $\mathbf{A}' = -\mathbf{A}_1^{-1} \cdot \mathbf{A}_2$. This is a matrix of dimension $(m - n) \times n$. Since $\mathbf{A}_1$ and $\mathbf{A}_2$ are uniformly random matrices, $\mathbf{A}'$ is also uniformly random.

Let $\mathbf{b}' = \mathbf{b}_1^\top \cdot \mathbf{A}' + \mathbf{b}_2^\top$ be a vector of dimension $(m - n)$. If $(\mathbf{A}, \mathbf{b})$ is a $\mathsf{LWE}_{n,m,q,\chi}$ pair, then $(\mathbf{A}', \mathbf{b}')$ is a $\mathsf{ss\text{-}LWE}_{n,m-n,q,\chi}$ pair, since $\mathbf{b}' = \mathbf{e}_1^\top \cdot \mathbf{A}' + \mathbf{e}_2^\top$. If $\mathbf{b}$ is uniformly random, then so is $\mathbf{b}'$. Therefore the adversary $\mathcal{A}$ can be used to decide whether $(\mathbf{A}', \mathbf{b}')$ is an ssLWE pair or not. □

Here is another LWE variant that was proposed in the lecture, where the secret is a binary vector, and noise is same as above. This variant is also as hard as LWE (although in this case, the LWE parameters will be worse; there will be a $\log q$ factor loss in n).

Thanks to one of the students for bringing this up. I had mistakenly said that we don't know a hardness proof for this variant.

Computational Problem 5 (Binary Secrets Learning with Errors Problem ($\mathsf{bin\text{-}LWE}_{n,m,q,\chi}$)). *Distinguish between the following distributions:*

$$\mathcal{D}_1 = \left\{ (\mathbf{A}, \mathbf{s}^\top \cdot \mathbf{A} + \mathbf{e}^\top) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m} \\ \mathbf{s} \leftarrow \{0,1\}^n \\ \mathbf{e} \leftarrow \chi^m \end{array} \right\} \quad \mathcal{D}_2 = \left\{ (\mathbf{A}, \mathbf{u}^\top) : \begin{array}{c} \mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m} \\ \mathbf{u} \leftarrow \mathbb{Z}_q^{m} \end{array} \right\}$$

One can show that $\mathsf{bin\text{-}LWE}_{n,m,q,\chi}$ is as hard as $\mathsf{LWE}_{n/\log q,m,q,\chi}$, see this paper [Mic18] for reference. I might include a simplified version in one of the future problem sets.

Regev's encryption scheme with smaller public keys

Recall, the public key in Regev's encryption scheme consists of a matrix of dimension $n \times m$, where $m \geq n \log q$. Can we use an $n \times n$ matrix instead? As you may have noticed, this immediately leads to a problem: we cannot use LHL (since LHL requires $m \geq n \log q + n$). LHL was needed to argue that $(\mathbf{A} \cdot \mathbf{r}, \mathbf{b}^\top \cdot \mathbf{r})$ is indistinguishable from a uniformly random vector in $\mathbb{Z}_q^{n+1}$. However, instead of a statistical hammer (LHL), can we use a computational assumption?

This leads us to the following attempt: set the public key as $(\mathbf{A}, \mathbf{s}^\top \cdot \mathbf{A} + \mathsf{noise})$ where $\mathbf{A}$ is an $n \times n$ matrix. To encrypt a bit msg, we choose a low-norm vector $\mathbf{r}$, and output $\mathbf{c}_1 = \mathbf{A} \cdot \mathbf{r} + \mathsf{noise}$, $c_2 = \mathbf{b}^\top \cdot \mathbf{r} + \mathsf{noise}$.

As you may have noticed, decryption will not be correct. This is because there is noise in the ciphertext, and $\mathbf{s}^\top \cdot \mathsf{noise}$ will blow up. The fix, therefore, is to choose $\mathbf{s}$ also from the noise distribution (and use ssLWE instead of LWE). We will have to reduce the noise bound slightly. The full construction is described below.

Note that the error bound here is slightly less than $q^{0.5}$. Thanks for pointing out during the lecture.

Construction 2.9 (LWE-based PKE scheme with smaller public keys). *Let $q = 2^{\sqrt{n}}$, $m = n$, $\chi \equiv \mathsf{Unif}_{[-q^{0.4},q^{0.4}]}$ be the ssLWE parameters.*
The encryption scheme for message space $\{0,1\}$ can be specified as follows:

- $\mathsf{Setup}(1^n)$*: It sample a random matrix $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times n}$, a random secret vector $\mathbf{s} \leftarrow \chi^n$, and a random error vector $\mathbf{e} \leftarrow \chi^n$. It outputs the public-secret key pair as:*

$$\mathsf{pk} = (\mathbf{A}, \mathbf{b}) \text{ where } \mathbf{b}^\top = \mathbf{s}^\top \cdot \mathbf{A} + \mathbf{e}^\top, \quad \mathsf{sk} = \mathbf{s}.$$

- $\mathsf{Enc}(\mathsf{pk}, \mathsf{msg})$*: Let $\mathsf{pk} = (\mathbf{A}, \mathbf{b})$. It samples a random vector $\mathbf{r} \leftarrow \chi^n$, error vector $\mathbf{e}_1 \leftarrow \chi^n$ and $e_2 \leftarrow \chi$. It outputs the ciphertext as:*

$$\mathsf{ct} = \left(\mathbf{A} \cdot \mathbf{r} + \mathbf{e}_1, \mathbf{b}^\top \cdot \mathbf{r} + e_2 + \mathsf{msg} \cdot \frac{q}{2} \right).$$

- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$*: Let the ciphertext $\mathsf{ct} = (\mathbf{c}_1, c_2)$. It outputs the message bit as:*

$$\mathsf{round}^{q/2}(c_2 - \mathbf{c}_1^\top \cdot \mathbf{s}),$$

where $\mathsf{round}^{q/2}(z)$ *rounds an element* $z \in \mathbb{Z}_q$ *to* 1 *if* $z \in [q/4, 3q/4]$ *and* 0 *otherwise.*

$\Diamond$

The scheme satisfies perfect correctness. For semantic security, we first switch the public key to uniformly random using the ss-$\mathsf{LWE}_{n,n,q,\chi}$ assumption. Next, we switch $(\mathbf{A} \cdot \mathbf{r} + \mathbf{e}_1, \mathbf{b}^\top \cdot \mathbf{r} + e_2)$ to uniformly random using the ss-$\mathsf{LWE}_{n,n+1,q,\chi}$ assumption.

Can we further reduce the public key size? One natural question is whether we need a uniformly random matrix? Can we choose one column vector $\mathbf{a}$, and deterministically generate the remaining columns from $\mathbf{a}$? This is an active area of research. The resulting security cannot be based on LWE, but instead relies on a family of assumptions called Ring-LWE. Unfortunately this is beyond the scope of this course.

Part II: Interactive Proofs

In the previous part, we saw two post-quantum hardness assumptions, and used them to build a few post-quantum cryptographic primitives. In this part, we will see the first scenario where a classical proof technique doesn't translate to the quantum setting. This is in the context of zero knowledge proofs (ZKPs). We will spend a couple of lectures on a more general primitive called interactive proofs. Besides being a very useful and well-studied generalization of ZKPs, interactive proofs will also be useful later in the semester, when we discuss *quantum cryptography*.

Post-quantum security refers to security of classical crypto primitives in the presence of a quantum adversary. The syntax and security definition stays the same, except that 'p.p.t. adversary' is replaced with 'efficient quantum adversary'.

Introduction to Interactive Proofs

The complexity class NP consists of problems (such as SAT, 3COL) whose solutions are efficiently and deterministically verifiable. For every problem, there is a deterministic verification process $\mathbf{V}$ such that if an instance is a 'yes' instance, then there exists a 'certificate' that $\mathbf{V}$ can check efficiently. For example, let us consider 3COL. The 'yes' instances consist of all graphs that can be colored using three distinct colors such that no two neighboring vertices have the same color. As a result, for every 'yes' instance, there is a very simple certificate: an assignment of colors to the vertices. Given a yes instance graph G and such a valid coloring, the verifier can check that only three colors are used, and that no neighboring vertices in the graph have the same color.

However, what if someone wants to prove that there exists **no** three coloring for a graph? It is unlikely that such statements will have short certificates. The lack of short certificates does not mean that such statements cannot be efficiently verified. A series of remarkable works showed that such statements (and much harder problems) can be verified if we allow interaction and a small error probability.

An interesting (non-technical) summary of the rich history of interactive proofs can be found here.

3 Interactive Proofs for Problems outside NP

Let us start with the formal definitions, and some notations that will be useful for this section.

Notations

- An interactive protocol consists of interactive algorithms $\mathbf{P}, \mathbf{V}$ (the prover and verifier) sending messages back and forth, and at the end, the verifier outputs a single bit. For a k message protocol, if the prover sends the first message, think of these as k Turing machines $\mathbf{P}_1, \mathbf{V}_2, \mathbf{P}_3, \ldots, \mathbf{P}_k$. The prover consists of $(\mathbf{P}_1, \mathbf{P}_3, \ldots, \mathbf{P}_k)$, and the verifier consists of $(\mathbf{V}_2, \ldots, \mathbf{V}_{k-1})$. On input x, $\mathbf{P}_1(x)$ outputs the first message m_1. The verifier uses x, m_1 and outputs $m_2 \leftarrow \mathbf{V}_2(x, m_1)$. Next, the prover outputs $m_3 = \mathbf{P}_3(x, m_1, m_2)$ and so on.

- Let $\mathsf{out}\langle \mathbf{P}, \mathbf{V}\rangle(x)$ denote the final output of $\mathbf{V}$. The verifier Turing machines are randomized, and therefore this output is a random variable.
- The transcript of the protocol, denoted by $\mathsf{trans}\langle \mathbf{P}, \mathbf{V}\rangle(x)$ consists of all the messages exchanged between $\mathbf{P}$ and $\mathbf{V}$. Again, this is a random variable.

Definition 3.1 (Interactive Proofs)**.** *Let* $\mathsf{L} = (\mathsf{L}_{\text{yes}}, \mathsf{L}_{\text{no}})$ *denote a language, where* L_{yes} *consists of all the 'yes' instances, and* L_{no} *consists of all the 'no' instances. An interactive proof system for* L *with completeness error* c *and soundness error* s *consists of a pair of interactive algorithms* $(\mathbf{P}, \mathbf{V})$ *with the following properties:*

- *Completeness: For every* $x \in \mathsf{L}_{\text{yes}}$, $\Pr[\mathsf{out}\langle \mathbf{P}, \mathbf{V}\rangle(x) = 1] \geq 1 - c$
- *Soundness: For every* $x \in \mathsf{L}_{\text{no}}$ *and every prover* $\mathbf{P}^*$ *(including malicious provers),* $\Pr[\mathsf{out}\langle \mathbf{P}^*, \mathbf{V}\rangle(x) = 1] \leq s$.

◊

For example, consider the *graph nonisomorphism* problem. Here the 'yes' instances set L_{yes} consists of graph pairs (G_0, G_1) that are not isomorphic, and the 'no' instances set L_{no} consists of graph pairs (G_0, G_1) such that G_0 and G_1 are isomorphic.

A few comments regarding this definition:

- If we have completeness error c and soundness error s where $1 - c$ and s are at least $1/\text{poly}$ apart, then we can boost the gap by sequential/parallel repetition, resulting in a protocol with negligible completeness and soundness errors.
- Using the above definition of interactive protocols, we can define the complexity class IP, which is the set of all languages that have probabilistic polynomial time verifiers. Note that in the definition of IP, the prover is allowed to run for unbounded time. There are also other complexity classes that capture protocols that have prover/verifier with certain resource restrictions.

Error reduction for sequential repetition is easy to prove; the case of parallel repetition requires a careful argument. See [Gol98], Appendix C for a formal proof.

3.1 *Interactive proof for Graph Non-Isomorphism*

Lecture 4: January 13th, 2023

The first interactive protocol (for a problem outside NP) will be for the graph nonisomorphism problem. Recall, the 'yes' instances here are pairs of graphs (on the same set of vertices) that are not isomorphic. The protocol for graph non-isomorphism is described below.

Common Input: graphs $G_0 = (V, E_0)$, $G_1 = (V, E_1)$.

Claim to prove: G_0 and G_1 are not isomorphic.

Protocol 1: Graph Non-Isomorphism: Private Coins Protocol

1 Verifier chooses a bit $b \leftarrow \{0,1\}$ and a uniformly random permutation $\pi \leftarrow S_n$. It computes a new graph $H = (V, E_H)$ where H is a random isomorphism of the graph G_b. More formally, $(\pi(u), \pi(v)) \in E_H$ if and only if $(u, v) \in E_b$. Verifier sends H to the prover.
2 Prover checks which of G_0 or G_1 is isomorphic to H (since the prover is unbounded, it can iterate over all permutations in S_n). It sends the corresponding bit $b' \in \{0,1\}$.
3 Verifier outputs 1 if $b = b'$, else it outputs 0.

S_n is the set of all permutations of $[n]$.

Completeness: If G_0 and G_1 are not isomorphic, then the graph H is isomorphic to exactly one of the two graphs. The prover can correctly find the graph that is isomorphic to H.

Soundness: For soundness, we require that if G_0 and G_1 are both isomorphic to each other, then H is a random isomorphism of both G_0 and G_1. Therefore, the graph H contains no information about the bit b sampled by the verifier. As a result, the prover's guess b' is correct with probability equal to $1/2$.

Reducing the soundness error: The k parallel repetition of the above protocol results in soundness error being $1/2^k$.

3.2 *Public-coins Interactive proof for Graph Non-Isomorphism*

The protocol described in Section 3.1 is a 'private coins' protocol. In that protocol, it was crucial that the verifier's randomness remains hidden from the prover. A surprising result by Goldwasser and Sipser [GS86] showed that any interactive protocol can be transformed into one where the verifier reveals all its randomness. Such protocols are called 'public coins' protocol. Public coins protocols are interesting because they have a nice structural property: for any constant k, a k round public coins protocol can be transformed into a two round public coins protocol.

In this section, we will discuss a public coins protocol for graph nonisomorphism. This protocol uses pairwise independent hash functions, which are defined below.

Definition 3.2 (Pairwise Independent Hash Functions)**.** *Let $\mathcal{H}$ be a family of hash functions with domain $\mathcal{X}$ and co-domain $\mathcal{Y}$. We say that $\mathcal{H}$ is a pairwise independent hash function family if the following properties hold:*

- *for any $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, $\Pr_{h \leftarrow \mathcal{H}}[h(x) = y] = 1/|\mathcal{Y}|$.*
- *for any distinct $x, x' \in \mathcal{X}$ and $y, y' \in \mathcal{Y}$, $\Pr_{h \leftarrow \mathcal{H}}[h(x) = y \text{ and } h(x') = y'] = 1/|\mathcal{Y}|^2$*

◊

The second property says that knowing the value at x tells you no information about the value at x'. A uniformly random function from $\mathcal{X}$ to $\mathcal{Y}$ would be k-wise independent (for any k). However, sampling and storing a uniformly random function is very expensive. Instead, for many applications, just pairwise independence suffices, in which case we can use a pairwise independent hash function family. These hash functions can be sampled/stored efficiently.

Example 3.3 (Pairwise Independent Hash Function)**.** *Let m, n be integers, $m > n$. Consider the hash family $\left\{f_{\mathbf{A},\mathbf{b}} : \{0,1\}^m \to \{0,1\}^n\right\}_{\mathbf{A}\in\mathbb{Z}_2^{n\times m},\mathbf{b}\in\mathbb{Z}_2^n}$ where*

$$f_{\mathbf{A},\mathbf{b}}(\mathbf{x}) = \mathbf{A}\cdot\mathbf{x} + \mathbf{b} \pmod 2.$$

Check that this satisfies the two requirements of pairwise independent hash functions. ◊

Back to our public coins protocol for GNI: the key idea here is to consider the set of graphs that are isomorphic to either G_0 or G_1. Intuitively, in the 'yes' case, the size of this set is larger than the size of the set in the 'no' case. A natural first guess is that the size will be $2n!$ in the 'yes' case, and $n!$ in the 'no' case.

However, strictly speaking, this statement is not true. Consider for instance, a 'yes' instance on three vertices, where G_0 is the triangle graph, and G_1 is the empty graph on three vertices. These two graphs are non-isomorphic. However, the set of graphs that are isomorphic to one of these two has only two graphs. On the other hand, if we take a 'no' instance where G_0 and G_1 are both path graphs on three vertices, then there are three graphs that are isomorphic to either G_0 or G_1.

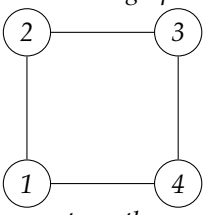
The main issue is that for certain graphs (such as the triangle and empty graphs), the set of graphs isomorphic to such graphs are identical to the graph. Such permutations are called *automorphisms* of the graph.

Definition 3.4 (Automorphism of a graph)**.** *Given a graph $G = (V, E)$ on n vertices, an automorphism of G is a permutation $\pi \in S_n$ such that for all (u, v) pairs,*

$$(u, v) \in E \iff (\pi(u), \pi(v)) \in E.$$

◊

Example 3.5 (Automorphisms of the 4-cycle)**.** *Consider the cycle graph on 4 vertices. Check that this graph has 8 automorphisms:*



$(1\to1, 2\to2, 3\to3, 4\to4)$ $(1\to1, 2\to4, 3\to3, 4\to2)$
$(1\to2, 2\to1, 3\to4, 4\to3)$ $(1\to2, 2\to3, 3\to4, 4\to1)$
$(1\to3, 2\to2, 3\to1, 4\to4)$ $(1\to3, 2\to4, 3\to1, 4\to2)$
$(1\to4, 2\to3, 3\to2, 4\to1)$ $(1\to4, 2\to1, 3\to2, 4\to3)$

There are two other graphs isomorphic to the 4-vertex graph.

◊

For any graph G, the set $\mathsf{aut}(G)$ consists of all automorphisms of G. Note that this set is non-empty, since $\mathsf{aut}(G)$ always contains the identity permutation. Similarly, let $\mathsf{iso}(G)$ denote the set of all graphs isomorphic to G (this set includes G). From the definitions of $\mathsf{aut}(G)$ and $\mathsf{iso}(G)$, we get the following observation for graphs on n vertices:

Observation 3.6. *For any graph on n vertices, $|\mathsf{iso}(G)| \cdot |\mathsf{aut}(G)| = n!$.*

This observation follows because there is a bijection between S_n (the set of all permutations over $[n]$) and $\mathsf{iso}(G) \times \mathsf{aut}(G)$.

The above observation gives us the following distinction between the 'yes' and 'no' instances. Instead of looking at all graphs that are isomorphic to either G_0 or G_1, we should look at the following set:

$$\mathsf{S}_{G_0,G_1} = \left\{ (H,\pi) : \begin{array}{c} H \text{ is isomorphic to } G_0 \text{ or } G_1 \\ \pi \in \mathsf{aut}(H) \end{array} \right\}$$

For the 'yes' case, this set has size $2n!$, while in the 'no' case, it has size $n!$.

The protocol

With all tools in place, we are ready to see the public-coins protocol for graph non-isomorphism. The set S_{G_0,G_1} has two properties:

- Given graphs (G_0, G_1), the set S_{G_0,G_1} has size $2n!$ if G_0 and G_1 are non-isomorphic, and size $n!$ if the sets are isomorphic.
- Given graphs (G_0, G_1), in both the 'yes' and 'no' case, for every $(H,\pi) \in \mathsf{S}_{G_0,G_1}$, there exists a short 'certificate' for proving that (H,π) is an element in S_{G_0,G_1}. The certificate simply consists of a bit b and a permutation σ mapping G_b to H. Given b, σ, one can efficiently verify that H is an isomorphism of G_b. (Checking that $\pi \in \mathsf{aut}(H)$ can be performed efficiently without any witness).

Let $\mathcal{U}$ denote the 'universe set' containing S_{G_0,G_1} (take $\mathcal{U} = \{\text{ALL GRAPHS} \times S_n\}$ for instance). The verifier picks a random hash function h mapping $\mathcal{U}$ to a suitable co-domain, and a random point y in the co-domain. The hope is the following:

- if we are in the 'yes' case, then with high probability, there exists a point x in the set S_{G_0,G_1} such that $h(x) = y$.
- in the 'no' case, since S_{G_0,G_1} is a small set, y will have no preimage in S_{G_0,G_1}.

Of course, it is important to choose the size of our co-domain carefully. Consider the first extreme: we choose the co-domain to be very large, say equal to $\mathcal{U}$). Note that S_{G_0,G_1} is much smaller than $\mathcal{U}$, and therefore a random point in the co-domain will not have a preimage in S_{G_0,G_1}. On the other hand, if we choose the co-domain to be very small, then y will have a preimage in S_{G_0,G_1} even in the 'no' case.

Let ℓ be an integer such that $2^{\ell-2} < 2n! < 2^{\ell-1}$, and let $\mathcal{H}$ denote a pairwise independent hash function family with domain $\mathcal{U}$ and co-domain $\{0,1\}^\ell$.

Common Input: Graphs (G_0, G_1)

Claim to prove: $|\mathsf{S}_{G_0,G_1}| = 2n!$

Protocol 2: Graph Non-Isomorphism : Public-coins Protocol

1 Verifier chooses $h \leftarrow \mathcal{H}$ and $y \leftarrow \{0,1\}^{\ell}$. It sends (h, y) to the prover.
2 Prover finds an $x = (H, \pi) \in \mathsf{S}_{G_0,G_1}$ such that $h(x) = y$. If no such x exists, prover outputs $\perp$. Else, it provides a certificate (b, σ), certifying that $H = \sigma(G_b)$.
3 Verifier, on receiving $(x = (H, \pi), (b, \sigma))$, checks that $h(x) = y$, $H = \sigma(G_b)$ and $\pi \in \mathsf{aut}(H)$. If these checks pass, it outputs 1, else outputs 0.

Clearly, this is a public-coins two-round protocol. Let us now analyze the completeness and soundness error probabilities.

Completeness: This bound follows from inclusion-exclusion, and uses the pairwise independence property.

$$\begin{aligned}
&\mathsf{Pr}_{h,y}\left[\exists x \in \mathsf{S}_{G_0,G_1} \text{ s.t. } h(x) = y\right] \\
&\geq \sum_{x \in \mathsf{S}_{G_0,G_1}} \mathsf{Pr}_{h,y}\left[h(x) = y\right] - \sum_{\substack{x,x' \in \mathsf{S}_{G_0,G_1} \\ x \neq x'}} \mathsf{Pr}_{h,y}\left[h(x) = h(x') = y\right] \\
&= \left(\frac{2n!}{2^{\ell}}\right) \cdot \left(\frac{(2n!)(2n!-1)}{2 \cdot 2^{2\ell}}\right) = \left(\frac{2n!}{2^{\ell}}\right) \cdot \left[1 - \left(\frac{(2n!-1)}{2 \cdot 2^{\ell}}\right)\right] > \left(\frac{2n!}{2^{\ell}}\right) \cdot \left(\frac{3}{4}\right)
\end{aligned}$$

The first step follows from inclusion-exclusion, and the second step follows from the pairwise independence property.

Soundness: The soundness bound is easier to prove. Note that in the 'no' case, $|\mathsf{S}_{G_0,G_1}| = n! < 2^{\ell-2}$. As a result, with probability at least $1 - n!/2^{\ell}$, a randomly picked string $y \leftarrow \{0,1\}^{\ell}$ has no preimage in S_{G_0,G_1}. The soundness error is at most $n!/2^{\ell}$.

A few remarks about the protocol:

- Note there is a gap in the completeness and soundness error probabilities. Since the gap is at least $1/\mathrm{poly}$, this can be amplified by parallel repetition.
- It is possible to make the completeness 'perfect' (that is, in the 'yes' case, the verifier always accepts).

Exercise 3.7. *Modify the above protocol so that the prover chooses the hash function h.*

4 Interactive Proofs for Very Hard Problems

In this section, we will present an interactive proof for a large class of very hard problems. Recall the NP-complete problem 3SAT. Given an instance ϕ, we want

to know if there *exists* a satisfying assignment. What if we want to count the number of satisfying solutions? Here, we will present an interactive protocol between an unbounded prover and a polynomial time verifier for verifying that a 3SAT instance ϕ has exactly t satisfying inputs.

Note, for instance, this protocol can be used to prove that a formula ϕ has no satisfying inputs. For quite some time, it was believed that such a protocol is not possible, and therefore it was a big surprise when this protocol was proposed.

4.1 *Arithmetization*

The first key idea in this protocol is to *arithmetize* the SAT instance. Given a 3SAT instance ϕ over n variables, one can efficiently produce an n-variate polynomial g_ϕ over $\mathbb{Z}_q$ (for some large q) such that

All coefficients of g_ϕ are from $\mathbb{Z}_q$, and when we evaluate g_ϕ on any $(x_1, \ldots, x_n)$, the evaluation is modulo q.

(*) for any input $(x_1, \ldots, x_n) \in \{0,1\}^n$, $\phi(x_1, \ldots, x_n) = g_\phi(x_1, \ldots, x_n)$

Note that this polynomial g_ϕ needs to agree with ϕ over the Boolean hypercube, but the polynomial can be evaluated at other points too.

The formula ϕ consists of m clauses. For the i^{th} clause over variables $x_{i_1}, x_{i_2}, x_{i_3}$, we will produce a 3-variate polynomial g_i over variables $x_{i_1}, x_{i_2}, x_{i_3}$ such that if clause is satisfied, $g_i(x_{i_1}, x_{i_2}, x_{i_3}) = 1$, otherwise $g_i(x_{i_1}, x_{i_2}, x_{i_3}) = 0$. If we can produce such a polynomial for each clause, then note that $g_\phi(x_1, \ldots, x_n) = \prod_i g_i(x_{i_1}, x_{i_2}, x_{i_3})$ satisfies (*).

Arithmetizing a clause: Given a clause $C(x, y, z)$, a *valid arithmetization* of the clause is a polynomial p_C over $\mathbb{Z}_q$ such that $C(x, y, z) = p_C(x, y, z)$ for all $(x, y, z) \in \{0,1\}^3$. Let $C_i = (x_{i_1} \vee x_{i_2} \vee x_{i_3})$ be a clause. Check that the polynomial

$$g_i(x_{i_1}, x_{i_2}, x_{i_3}) = 1 - \big(1 - x_{i_1}\big) \cdot \big(1 - x_{i_2}\big) \cdot \big(1 - x_{i_3}\big)$$

is equal to 1 if at least one of the variables is set to 1. If all the variables are set to 0 in C_i, then g_i evaluates to 0. If one or more of the variables are negated, then we can replace the $(1 - x)$ with x. For example, if $C_i = (\neg x_{i_1} \vee x_{i_2} \vee x_{i_3})$, then check that the following polynomial

$$g_i(x_{i_1}, x_{i_2}, x_{i_3}) = 1 - x_{i_1} \cdot \big(1 - x_{i_2}\big) \cdot \big(1 - x_{i_3}\big)$$

is a valid arithmetization of this clause.

We will call this the *canonical arithmetization* of the formula ϕ.

Important note: Given a formula ϕ, one can efficiently 'write down' the canonical arithmetization g_ϕ. The polynomial g_ϕ can also be efficiently evaluated at any point $(x_1, \ldots, x_n) \in \mathbb{Z}_q^n$.

Example 4.1. *Consider the formula $\phi(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (\neg x_1 \vee x_3)$. The canonical arithmetization is*

$$g_\phi(x_1, x_2, x_3) = (1 - (1 - x_1) \cdot (1 - x_2)) \cdot (1 - x_1 \cdot (1 - x_3))$$

Note that this is not the unique 3-variate polynomial that agrees with ϕ on the Boolean hypercube. Verify that the simplified polynomial $g'_\phi = x_2 - x_1x_2 + x_1x_3$ also agrees with ϕ on the Boolean hypercube. ◊

Observation 4.2. *For any* 3SAT *instance ϕ over n variables and having m clauses, the canonical arithmetization g_ϕ has degree at most $3m$. The degree of g_ϕ in any variable x is at most m (assuming none of the clauses have repeated variables).*

4.2 *The sum-check protocol*

Now that we have seen how to arithmetize a formula, we can cast the original 'logic' problem (counting the number of satisfying inputs) as an 'arithmetic problem' : compute $\sum g_\phi(x_1, \ldots, x_n)$ where the sum is over all $(x_1, \ldots, x_n) \in \{0,1\}^n$. As a result, in our protocol, if a prover needs to prove that ϕ has exactly t satisfying solutions, then it suffices for the prover to prove that $\sum g_\phi(x_1, \ldots, x_n) = t$. Thus, this is a *sum-check* protocol - the verifier must efficiently check that the sum of $g_\phi(x_1, \ldots, x_n)$ over all $(x_1, \ldots, x_n) \in \{0,1\}^n$ is indeed t.

The verifier can efficiently compute g_ϕ at any point $(x_1, \ldots, x_n)$. Using this protocol, it can check the sum of g_ϕ over all $\{0,1\}^n$.

Protocol intuition: First, let us start with the easy case: g_ϕ is a univariate polynomial. In this case, the verifier doesn't need the prover. It can simply check $g_\phi(0) + g_\phi(1) = t$. This suggests that if we have a means of reducing the number of variables one-by-one, then the problem can be solved easily when base case $n = 1$.

Reducing the number of variables: Suppose our verifier could check, for all $(n-1)$ variate polynomials $\tilde{g}$ and integers $\tilde{t}$, if $\sum_{(x_1,\ldots,x_{n-1}) \in \{0,1\}^{n-1}} \tilde{g}(x_1, \ldots, x_{n-1})$ is equal to $\tilde{t}$. Here is the first natural idea to reduce the n-variate case to the $(n-1)$ variate case: given $g(x_1, \ldots, x_n)$, the verifier can ask the prover for the values $t_0 = \sum_{(x_2,\ldots,x_n)} g(0, x_2, \ldots, x_n)$ and $t_1 = \sum_{(x_2,\ldots,x_n)} g(1, x_2, \ldots, x_n)$. Note that $h_0(x_2, \ldots, x_n) \equiv g(0, x_2, \ldots, x_n)$ and $h_1(x_2, \ldots, x_n) \equiv g(1, x_2, \ldots, x_n)$ are both $(n-1)$ variate polynomials, and given these values, the verifier needs to check:

- $t = t_0 + t_1$
- $t_0 = \sum_{x_2,\ldots,x_n} h_0(x_2, \ldots, x_n)$
- $t_1 = \sum_{x_2,\ldots,x_n} h_1(x_2, \ldots, x_n)$

While the first check is easy, there are two recursive calls, and therefore the verifier's work doubles up in each recursive call.

As mentioned by one of the students in class, if the verifier proceeds this way, it is essentially asking the prover for $g_\phi(x_1, \ldots, x_n)$ for all $(x_1, \ldots, x_n) \in \{0,1\}^n$.

Instead of asking the prover for t_0 and t_1 as above, the verifier can ask the prover for a univariate polynomial g_1 such that

$$g_1(X) \equiv \sum_{(x_2,\ldots,x_n) \in \{0,1\}^{n-1}} g(X, x_2, \ldots, x_n)$$

Given this polynomial, the verifier can compute $t_0 = g_1(0)$ and $t_1 = g_1(1)$ and check $t_0 + t_1 = t$. However, the verifier also needs to check that this polynomial is identical to $\sum_{(x_2,\ldots,x_n) \in \{0,1\}^{n-1}} g(X, x_2, \ldots, x_n)$. Can this be done using a single recursive call to sum-check over $(n-1)$ variables? Checking that two polynomials are identical can be very expensive. Note that one polynomial (g_1) is given explicitly in coefficient representation, but the other one $(\sum_{(x_2,\ldots,x_n)} g(X, x_2, \ldots, x_n))$ is implicit, and the verifier cannot compute its coefficient representation.

This brings us to the main observation of the protocol: both these polynomials are low-degree polynomials. Their degree is bounded by m, and *if two low-degree*

polynomials are not identical, they can agree on at most m points. As a result, the verifier picks a random number θ_1, and asks the prover to prove that

Given two degree d polynomials p_1, p_2, consider the polynomial $p = p_1 - p_2$. If $p_1 \neq p_2$, p has at most d roots.

$$\mathsf{Stmt}_1 : \sum_{(x_2,\ldots,x_n)\in\{0,1\}^{n-1}} g(\theta_1, x_2, \ldots, x_n) = g_1(\theta_1).$$

If the prover had lied in the first step (by sending an incorrect g_1), with high probability, it will get caught when it proves Stmt_1. Note that Stmt_1 is a sum-check statement over $(n-1)$ variables, and we can use recursion now.

Before stating the full protocol, we will describe the high-level template. The reader is encouraged to figure out the protocol based on the template.

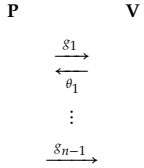
Common Input: 3CNF formula ϕ and integer $t \leq 2^n$. Equivalently, we can think of the common input as a prime $q > 2^n$, a number $t \leq 2^n$ and the canonical arithmetization g_ϕ, a polynomial over $\mathbb{Z}_q$.

Claim to prove: $\sum_{(x_1,\ldots,x_n)\in\{0,1\}^n} g_\phi(x_1, \ldots, x_n) = t \mod q$

Protocol 3: Sum-Check Protocol

1 Set $\gamma_0 = t$ and statement $\mathsf{Stmt}_0 : \sum_{(x_1,\ldots,x_n)\in\{0,1\}^n} g_\phi(x_1, \ldots, x_n) = \gamma_0$;
2 **for** $i = 1$ *to* $n-1$ **do**
3 Prover needs to prove statement Stmt_{i-1}. It sends a *univariate* polynomial g_i of degree at most m ;
4 Verifier checks that g_i has degree at most m and $g_i(0) + g_i(1) = \gamma_{i-1}$. **if** *check passes* **then**
5 verifier samples a random $\theta_i \leftarrow \mathbb{Z}_q$, sets $\gamma_i = g_i(\theta_i)$ and sends θ_i to the prover. The statement Stmt_i for the next round is $\sum_{(x_{i+1},\ldots,x_n)\in\{0,1\}^{n-i}} g_\phi(\theta_1, \ldots, \theta_i, x_{i+1}, \ldots, x_n) = \gamma_i$.
6 **else**
7 Verifier rejects and outputs 0;
8 Finally, verifier checks $g_\phi(\theta_1, \ldots, \theta_{n-1}, 0) + g_\phi(\theta_1, \ldots, \theta_{n-1}, 1) = \gamma_{n-1}$ and outputs 1 if this check passes, else outputs 0.

A few points to note before we discuss the protocol details:



- This is a 'public coins' protocol. Note that the verifier's messages $\{\theta_i\}_{i\in[n-1]}$ are all random numbers sampled from $\mathbb{Z}_q$. Other than this, the verifier uses no other randomness.
- In our protocol description, the verifier also sends θ_{n-1} in the last round. However, this is not needed.
- The verifier's work mainly consists of evaluating polynomials of degree at most m, and finally evaluating an n-variate polynomial of degree at most m.

The main step that is left to describe is Step 2 of the protocol.

Step 2 of the Sum-Check Protocol

In the i^{th} iteration of the protocol, the prover needs to prove statement

$$\mathsf{Stmt}_{i-1} : \sum_{x_i \in \{0,1\}} \sum_{(x_{i+1},\ldots,x_n) \in \{0,1\}^{n-i}} g_\phi(\theta_1, \ldots, \theta_{i-1}, x_i, \ldots, x_n) = \gamma_{i-1}$$

Note that the prover has $g_1, \theta_1, \ldots, g_{i-1}, \theta_{i-1}$ from the previous rounds, and can compute γ_{i-1} given θ_{i-1}.

Consider the univariate polynomial

$$g_i(X) = \sum_{(x_{i+1},\ldots,x_n) \in \{0,1\}^{n-i}} g_\phi(\theta_1, \ldots, \theta_{i-1}, X, x_{i+1}, \ldots, x_n)$$

This polynomial has degree at most m (since the overall degree of g_ϕ is m, the degree of any variable is also at most m). Moreover, if statement Stmt_{i-1} is true, then $g_i(0) + g_i(1) = \gamma_{i-1}$. Hence the verifier's check in Step 3 passes.

From the definition of g_i, it follows that for all $\theta \in \mathbb{Z}_q$,

$$g_i(\theta) = \sum_{(x_{i+1},\ldots,x_n) \in \{0,1\}^{n-i}} g_\phi(\theta_1, \ldots, \theta_{i-1}, \theta, x_{i+1}, \ldots, x_n)$$

Therefore statement Stmt_i (which is defined using a random $\theta_i \leftarrow \mathbb{Z}_q$) is true.

Soundness Error

Before we analyze the behavior of malicious provers, let us see where the honest prover gets stuck if we try to prove an incorrect statement. Let us consider the formula in Example 4.1. There are four satisfying assignments for $\phi(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (\neg x_1 \vee x_3)$. Suppose we try to prove the false statement $\mathsf{Stmt}_0 : \sum_{(x_1,x_2,x_3) \in \{0,1\}^3} g_\phi(x_1, x_2, x_3) = 3$, and suppose the prime $q = 43$.

Nothing special about 43, picked an arbitrary large prime.

In the first iteration, the prover sends the univariate polynomial g_1 obtained by summing over x_2 and x_3. This polynomial is

$$g_1(x) = 2 + x - x^2$$

and recall $\gamma_0 = 3$. In the first round itself, the verifier can realize that this statement is incorrect, since $g_1(0) + g_1(1) = 4 \neq \gamma_0$.

Suppose that the prover is malicious and sends $g_1'(x) = 2 - x^2$. Now, when the verifier checks $g_1'(0) + g_1'(1) = \gamma_0$, the first check passes. The verifier then picks a random number θ_1, say 5. The statement for the next round is

$$\mathsf{Stmt}_1 : \sum_{(x_2,x_3) \in \{0,1\}^2} g_\phi(5, x_2, x_3) = g_1'(5) = -23 = 20$$

If the prover is honest in the next round, then it must send

$$g_2(x) = 12x - 15$$

However, with this polynomial, the prover will get caught, since $g_2(0) + g_2(1) \neq 20$. Therefore, the prover must again lie. Suppose it sends $g_2'(x) = 2x + 9$. Now,

check that $g_2'(0) + g_2'(1) = 20$. The verifier again chooses a random number θ_2, say 3, and checks if $g_\phi(5,3,0) + g_\phi(5,3,1) = g_2'(3)$. At this point, the prover is caught, since the LHS is 21 and the RHS is 15.

Exercise 4.3. *In the sum-check protocol, it is essential that in the i^{th} round, θ_i is sent to the prover **after** the prover sends g_i. What would happen if θ_i is sent before the prover sends g_i?*

Exercise 4.4. *In the sum-check protocol, it is essential that the verifier checks the degree bound on each g_i sent by the prover. Show that the prover can cheat successfully if this check is removed.*

Formal proof of soundness The formal proof of soundness relies on a simple mathematical fact: any degree d polynomial has at most d roots. A useful corollary of this simple fact: any two distinct degree d polynomials can agree on at most d points. As a result, if we have two distinct polynomials, and we pick a random integer $\theta \leftarrow \mathbb{Z}_q$, the two polynomials will not agree at θ with probability at least $1 - d/q$.

In class, we saw a slightly stronger bound: for a false statement, the verifier outputs 0 with probability at least $\left(1 - \frac{d}{q}\right)^n$.

Lemma 4.5. *Suppose $g_\phi \in \mathbb{Z}_q[x_1, \ldots, x_n]$ is a degree d polynomial (over n variables), and the statement $\mathsf{Stmt}_0 : \sum_{(x_1,\ldots,x_n)\in\{0,1\}^n} g_\phi(x_1, \ldots, x_n) = \gamma_0$ is false. Then*

$$\Pr\left[\mathbf{V} \text{ outputs } 1 \text{ at end of } n \text{ rounds }\right] \leq \frac{nd}{q}$$

Sketch of Proof.

... to be continued in next lecture

Lecture 5: January 17th, 2023

□

References

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, USA, 1st edition, 2009.

[AG11] Sanjeev Arora and Rong Ge. New Algorithms for Learning in Presence of Errors. In Luca Aceto, Monika Henzinger, and Jirí Sgall, editors, *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I*, volume 6755 of *Lecture Notes in Computer Science*, pages 403–415. Springer, 2011.

[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, page 99–108, New York, NY, USA, 1996. Association for Computing Machinery.

[Gol98] Oded Goldreich. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, volume 17 of *Algorithms and Combinatorics*. Springer, 1998.

[GS86] S Goldwasser and M Sipser. Private Coins versus Public Coins in Interactive Proof Systems. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, STOC '86, page 59–68, New York, NY, USA, 1986. Association for Computing Machinery.

[Mic18] Daniele Micciancio. On the Hardness of Learning With Errors with Binary Secrets. *Theory of Computing*, 14(13):1–17, 2018.

[Reg09] Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *J. ACM*, 56(6), sep 2009.

Appendix: Cryptographic Primitives

Definition 1 (Non-interactive commitment scheme with setup)**.** *A non-interactive commitment scheme with setup consists of two algorithms:* Setup *and* Commit *with the following syntax:*

- $\mathsf{Setup}(1^n)$*: takes as input the security parameter, and outputs a public key* pk*.*
- $\mathsf{Commit}(\mathsf{pk}, \mathsf{msg}; r)$ *: takes as input the public key* pk*, the message* msg *to be committed, randomness* r*, and outputs a commitment* com*.*

A non-interactive commitment scheme with setup must satisfy the following two security properties:

- ***Binding property****: A commitment scheme satisfies the binding property if for any prob. poly. time adversary* $\mathcal{A}$*, there exists a negligible function* $\mu(\cdot)$ *such that for all* n*,* $\Pr[\mathcal{A}$ *wins the binding security game*$] \leq \mu(n)$ *where the binding security game is defined below:*

Binding-Game
– Challenger chooses $\mathsf{pk} \leftarrow \mathsf{Setup}(1^n)$ and sends pk to $\mathcal{A}$.
– Adversary sends a commitment com, together with two (message, opening) pairs (msg_0, r_0) and (msg_1, r_1). The adversary wins if $\mathsf{Commit}(\mathsf{pk}, \mathsf{msg}_0; r_0) = \mathsf{Commit}(\mathsf{pk}, \mathsf{msg}_1; r_1) = \mathsf{com}$.

Figure 4: The Binding Security Game

- ***Hiding property****: A commitment scheme satisfies the hiding property if for any prob. poly. time adversary* $\mathcal{A}$*, there exists a neglibile function* $\mu(\cdot)$ *such that for all* n*,* $\Pr[\mathcal{A}$ *wins the hiding security game*$] \leq 1/2 + \mu(n)$ *where the binding security game is defined below:*

Hiding-Game
– Challenger chooses $\mathsf{pk} \leftarrow \mathsf{Setup}(1^n)$ and sends it to the adversary.
– The adversary sends two messages $\mathsf{msg}_0, \mathsf{msg}_1$.
– Challenger chooses $b \leftarrow \{0,1\}$, computes $\mathsf{com} \leftarrow \mathsf{Commit}(\mathsf{pk}, \mathsf{msg}_b)$ and sends com to $\mathcal{A}$.
– Adversary sends guess b' and wins if $b = b'$.

Figure 5: The Hiding Security Game

$\Diamond$