University of Illinois, Urbana Champaign
CS 598DK Special Topics in Cryptography

Instructor: Dakshita Khurana
Scribe: Ima Student
Date: August 28, 2019

LECTURE
11

Instructions for Preparing Scribe Notes

More and more computation is being outsourced to public clouds nowadays. However, traditional encryption schemes requires that data must be decrypted before it can be analyzed or manipulated. It would be better the outsourced computation can be done on encrypted data if the encryption has some "special" property that having the same effect as firstly computing on meta data and then encrypting it and data privacy is protected. Such property is called homomorphic. In today's lecture, we will see what is fully homomorphic encryption (FHE) scheme and how to build a FHE scheme achieving homomorphic addition and multiplication based on learning with errors (LWE) problems.

11.1 Recap

Before stepping into how to build LWE-based FHE schemes, let's briefly recap how to build private and public encryption scheme with LWE problem.

Definition 11.1. ***Decisional LWE***$_{n,m,q,\mathcal{X}}$

For all non-uniform probabilistic polynomial time adversary $\mathcal{A}$

$$|\underset{\substack{\boldsymbol{s}\leftarrow\mathbb{Z}_q^{n\times 1}\\ \boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}\\ \boldsymbol{e}\leftarrow\mathcal{X}^m}}{Pr}[\mathcal{A}(\boldsymbol{A},\boldsymbol{s}^T\boldsymbol{A}+\boldsymbol{e}^T)=1]-\underset{\substack{\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}\\ \boldsymbol{b}\leftarrow\mathbb{Z}_q^m}}{Pr}[\mathcal{A}(\boldsymbol{A},\boldsymbol{b})=1]|=negl(n)$$

where q is a prime within $O(2^n)$, $m = O(n\log q)$ and norm $\parallel \boldsymbol{e} \parallel= \omega(\log n)$.

Next we present the secret key encryption (SKE) built with LWE which has $m = 1$:

- $KeyGen(1^n) : \boldsymbol{s} \leftarrow \mathbb{Z}_q^n$
- $Enc(\boldsymbol{s}, \mu \in \{0,1\}) : (\boldsymbol{A}, (\boldsymbol{s}^T\boldsymbol{A} + e + \mu\lfloor\frac{q}{2}\rfloor) \mod q)$
  - * $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times 1}$
  - * $e \leftarrow \mathcal{X}$

- $Dec(\boldsymbol{s}, \boldsymbol{a}, b) : b - \langle \boldsymbol{s}^T, \boldsymbol{a} \rangle = (e + \mu \lfloor \frac{q}{2} \rfloor) \mod q$

LWE can also be used to build public key encryption (PKE):

-

- $KeyGen(1^n) : (sk = \boldsymbol{s}, pk = (\boldsymbol{A}, \boldsymbol{b}^T = \boldsymbol{s}^T \boldsymbol{A} + \boldsymbol{e}^T))$

  * $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$
  * $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n \times m}$
  * $\boldsymbol{e} \leftarrow \mathcal{X}^m$

- $Enc(pk, \mu \in \{0,1\}) : (\boldsymbol{c_1} = \boldsymbol{Ar}, c_2 = (\boldsymbol{b}^T \boldsymbol{r} + \mu \lfloor \frac{q}{2} \rfloor) \mod q)$

  * $\boldsymbol{r} \longleftarrow \{0,1\}^m$

- $Dec(sk, (\boldsymbol{c_1}, c_2)) : c_2 - \boldsymbol{s}^T \boldsymbol{c_1} = \boldsymbol{e}^T \boldsymbol{r} + \mu \lfloor \frac{q}{2} \rfloor$

11.2 Fully Homomorphic Encryption (FHE)

Let us consider the scenario shown in **??**. A client has a secret value x. The client wants the server do some computation on x without revealing what x is. Firstly, a ciphertext $ct = Enc(x)$ is sent to the server along with the desired function f. Then the server could compute a new ciphertext $ct^* = Enc(f(x))$ by evaluating x on another function g which is publicly computable from f. After receiving ct^* from the server, the client can use its secret key sk to get the desired result of $f(x)$.

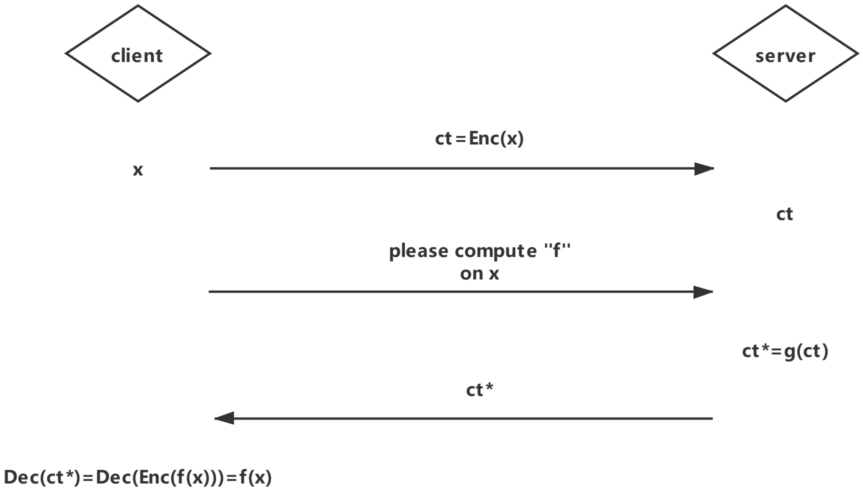

Figure 11.1: Outsourced Computation

A homomorphic encryption can be used for privacy-preserving outsourced storage and computation. It allows operations and analysis on encrypted data without revealing the original one, which removes the privacy barriers in several real-life applications.

Definition 11.2. Let $\mathcal{C}$ be a class of circuits where for each $f \in \mathcal{C}$, $f : \{0,1\}^n \to \{0,1\}$. An encryption scheme $(KeyGen, Enc, Dec, Eval)$ is **$\mathcal{C}$-homomorphic** if $\forall f \in \mathcal{C}$, all ciphertexts $ct_1, \ldots, ct_n$, $Eval(f, ct_1, \ldots, ct_n) = ct^*$ such that if $\forall i$, $\exists m_i, r_i$ s.t. $ct_i = Enc(m_i; r_i)$, then $Dec_{sk}(ct^*) = f(m_1, \ldots, m_n)$ and the scheme is IND-CPA secure.

At a high level, given ciphertexts $ct_1, \ldots, ct_n$ that encrypt $m_1, \ldots, m_n$, FHE should allow anyone to output a ciphertext ct^* that encrypts $f(m_1, \ldots, m_n)$ for any desired function f by evaluating another function g which is publicly computable from f. Thus, the key holder could use the secret key sk to decrypt ct^* and get the result of $f(m_1, \ldots, m_n)$.

Note that each function $f : \{0,1\}^n \to \{0,1\}^k$ can be split into $f_1, \ldots, f_k$ where $\forall i$, $f_i : \{0,1\}^n \to \{0,1\}$ and also we can generalized the definition by regulating the input length of circuits in $\mathcal{C}$ from n to $poly(n)$.

11.3

Using the provided `\makeheader` command, customize the above header with your name, lecture date, lecture number, and lecture title. For example, the above header was generated by typing `\makeheader{Ima Student}{August 28, 2019}{10}{Instructions for Preparing Scribe Notes}`. Your scribe notes should start with a high-level description of the lecture, its goal and techniques, and how it fits in the broader context of the course. In particular, explain its relation to the previous lecture if appropriate. This high-level description should be two or three solid paragraphs in length.

11.4 Organization

Lecture proper should be presented in a sequence of sections. For example, you might choose to present background or preparatory work in one section, the main results in another section, and any generalizations or conclusions in a third section. Do *not* use any subdivisions within sections (subsections, subsubsections, etc.). Use normal capitalization in section headings rather than initial caps.

11.5 Some do's

The single most important thing to keep in mind when preparing scribe notes is that they should be a self-contained record of the lecture. In particular, it is *entirely inadequate* to simply typeset the contents of the blackboard— this will be rewarded with a flat grade of 1 point. The lecture is much more than the contents of the blackboard; I do not just walk in the classroom and write on the blackboard for two hours. The lecture has a *soundtrack*, which supplies a motivation for the material, intuitive descriptions of the proofs, and answers to questions from the audience. This component of the lecture is vital to understanding the subject matter and should be prominently present in your scribe notes. Here are some other things to keep in mind.

FIGURE 11.2: A triangle and a circle.

- Always preface a formal statement (theorem, lemma, proposition) with a discussion of its purpose and a brief and intuitive outline of the proof.
- We all know from experience that a picture is worth a thousand words, so be generous with figures. See Figure 11.2 for an example usage of the figure environment.
- Write in complete sentences. Mathematical writing is not fundamentally different from any other form of expository prose. Take pride in your work.
- As with any writing, make sure to spell check your scribe notes.
- Be sure to include all bibliographic references, like so [1]. You will find all the needed references at the end of the corresponding chapter in the textbook. The bibliography must be incorporated using BibTex. When finished, please send me the following files by email: your LaTeX source file (`.tex`), your bibliography file (`.bib`) if you used one, any figures (ideally in `.pdf` format), and the resulting typeset document (`.pdf`). I prefer to receive a single ZIP archive rather than several individual attachments.

11.6 Some don'ts

Here are the most common pitfalls to watch out for.

- Copying or paraphrasing material from the textbook is emphatically *not* OK because it defeats the pedagogical purpose of scribe notes. What I am looking for is *your* personal perspective on the material. A good way to proceed is to master the material from the lecture and textbook, wait a day for it to sink in, and then typeset your scribe notes without consulting any sources. This approach brings out your personal take on the material and allows you to truly internalize it to a point when you yourself could teach it.
- You must not change the format of the scribe notes in any way, including font type, font size, pagination, section numbering, margins, or bibliography style.
- No content should spill over into the margins.
- You should not need to include any LaTeX packages in addition to those already included in the template file. One exception, if you want to be extra creative, is tikz-people (`http://tex-talk.net/2016/11/tikz-people/`).

11.7 Mathematical environments

For your convenience, the scribe note style file comes with the following mathematical environments predefined: theorem, lemma, corollary, proposition, fact, claim, definition, example, assumption, remark, conjecture, open problem, problem. The environments are illustrated below. Please limit yourself to these environments.

Theorem 11.3. *Statement here*

Lemma 11.4. *Statement here*

Corollary 11.5. *Statement here*

Proposition 11.6. *Statement here*

Fact 11.7. *Statement here*

Claim 11.8. *Statement here*

Definition 11.9. Statement here

Example 11.10. Statement here

Assumption 11.11. Statement here

Remark 11.12. Statement here

Conjecture 11.13. Statement here

Open Problem 11.14. Statement here

Problem 11.15. Statement here

Note that LaTeX automatically numbers these environments within the lecture number (11 in this case). The same applies to the numbering of pages (this page being page 11-5), figures (Figure 11.2 above), and equations:

$$a = a_1 + a_2 + \cdots + a_n. \tag{11.1}$$

For proofs, use the provided `proof` environment, illustrated below.

Proof. Proof goes here. □

Acknowledgement

These scribe notes were prepared by editing a light modification of the template designed by Alexander Sherstov.

References

[1] E. Kushilevitz and N. Nisan. *Communication complexity.* Cambridge University Press, 2nd edition, 2006.