King Fahd University of Petroleum and Minerals

College of Computing and Mathematics
Information and Computer Science Department

SEC 595: Encrypted Computing

Term 241

Course Information

- Lectures: Sunday & Tuesday, 18:45-20:00 PM
- Location: Building 22-134

Course Description

Homomorphic Encryption: Partial homomorphic encryption, Leveled homomorphic encryption, Full homomorphic encryption. Bootstrapping. FHE schemes: BGV, BFV, CKKS. Optimization and acceleration of FHE. Secret sharing. Oblivious transfers. Secure multiparty computation (MPC). Garbled circuits. Privacy-Preserving machine learning.

Prerequisites

Graduate standing

Course Objectives

The objectives of this course are:

i. Introduce the students to the emerging field of encrypted computing.
ii. Expose students to the state-of-the-art algorithms in homomorphic encryption and secure multiparty computation

Learning Outcomes

After taking this course, students will have the ability to:

1. Explain various encrypted computing techniques and algorithms.
2. Identify the advantages and challenges of different encrypted computing algorithms.
3. Apply appropriate encrypted computing techniques based on the application's requirements.
4. Design new encrypted computing techniques and protocols.

Textbook and references

1. Chen K, Yang Q. Privacy-Preserving Computing: For Big Data Analytics and AI. Cambridge University Press; 2023.
2. Dan Boneh and Victor Shoup, A Graduate Course in Applied Cryptography. (link)
3. A Pragmatic Introduction to Secure Multi-Party Computation (link)
4. List of papers
    a. Computing Arbitrary Functions of Encrypted Data https://people.csail.mit.edu/vinodv/6892-Fall2013/GentryCACM.pdf
    b. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography https://people.csail.mit.edu/vinodv/6892-Fall2013/regev.pdf
    c. The Learning with Errors Problem https://people.csail.mit.edu/vinodv/6892-Fall2013/lwesurvey.pdf
    d. Homomorphic Encryption for Arithmetic of Approximate Numbers https://eprint.iacr.org/2016/421.pdf

e. Carig Gentry's thesis https://crypto.stanford.edu/craig/craig-thesis.pdf
f. (Leveled) Fully Homomorphic Encryption without Bootstrapping https://people.csail.mit.edu/vinodv/6892-Fall2013/BGV.pdf
g. https://files.boazbarak.org/crypto/lec_15_FHE.pdf
h. https://securecomputation.org/docs/pragmaticmpc.pdf

Useful Links (Libraries and curated lists)

1. OpenMind https://blog.openmined.org/private-machine-learning-explained/
2. Aweseom HE https://github.com/jonaschn/awesome-he
3. HElib library https://github.com/shaih/HElib
4. Microsoft SEAL https://www.microsoft.com/en-us/research/project/microsoft-seal/
5. MIT HE List https://people.csail.mit.edu/vinodv/FHE/FHE-refs.html
6. OpenFHE Community https://www.openfhe.org/

Evaluation

Paper Presentation	10%
Project	30%
Midterm Exam	30%
Final Exam	30%

List of Topics

List of Topics	Weeks
Review of number theory/Introduction to Lattice	2
Homomorphic encryption: PHE, LHE, FHE. Bootstrapping	2
FHE schemes: BGV, BFV, CKKS	3
Optimization and acceleration of FHE	1
Secret sharing	1
Oblivious transfer	1
Secure multiparty computation	1
Garbled circuits	1
Secure and privacy-preserving machine learning	2

Course Policies

- ***Course Website & Participation***: Students are required to periodically check the course website on Blackboard the MS Teams.
- ***Attendance***: Regular attendance is a university requirement; hence attendance will be taken at the beginning of each lecture.
    - Missing more than **6 lectures** will result in a DN grade without warning.
    - Official excuses must be presented to the instructor no later than one week of returning to classes.
- ***Re-grading policy***: If you have a complaint about any of your grades, discuss it with the instructor no later than a week from distributing the grades (except for the final). Only legitimate concerns on grading should be discussed.
- ***Office Hours***: Students are encouraged to visit faculty in the office hours to clarify any part of the material that is not clear.
- ***Academic honesty***: Students are expected to abide by all the university regulations on academic honesty. **Cheating will be reported to the Department Chairman** and will be severely penalized. Although collaboration and sharing knowledge is highly encouraged, copying others' work (classmates, others or from the web) without proper citation, either in part or full, is considered plagiarism. Whenever in doubt, review the university guidelines or consult the instructor. **Cheating in whatever form will result in an F grade.**
- Absolute academic integrity is expected of every KFUPM student in all academic undertakings. Most essential values academia are grounded on the concept of honesty with respect to the intellectual efforts of oneself and others. While both students and faculty of KFUPM assume the responsibility of maintaining and furthering these values, this memo is concerned specifically with the conduct of students. The KFUPM have a zero-tolerance policy towards cheating, plagiarism or any other violation to the Code of Honesty.
    - Examples of Violations of Code of Academic Honesty
        - Knowingly representing the work of others as one's own.
        - Using, obtaining, or providing unauthorized assistance on examinations, quizzes, assignment, or any other academic work.
        - Fabricating results in support of laboratory or field work.
    - Examinations.
        - No student may take an examination for another student. The student is responsible for understanding the conditions and rules under which the examination will be taken.
        - Dishonesty or cheating in examinations which is defined as the use of inappropriate or unauthorized materials, information, or study aids in an exam. Unless the instructor directs otherwise, an examination is assumed to be solely a student's own work.
        - No communication is allowed among students either through voice, written, electronic, or any other form of transmission, nor are students permitted to consult books, papers, study aids or notes without explicit permission of the course instructor.
        - Violating exam rules and regulations by bringing smart electronic devices (such as mobile phones, smart watches, earbuds, etc.) to the exam venue is considered a cheating attempt.