CS4192: ALGORITHMS FOR PRIVATE DATA ANALYTICS

Effective Term
Semester A 2025/26

Part I Course Overview

Course Title
Algorithms for Private Data Analytics

Subject Code
CS - Computer Science
Course Number
4192

Academic Unit
Computer Science (CS)

College/School
College of Computing (CC)

Course Duration
One Semester

Credit Units
3

Level
B1, B2, B3, B4 - Bachelor's Degree

Medium of Instruction
English

Medium of Assessment
English

Prerequisites
CS3104 Applied Cryptographic Systems

Precursors
Nil

Equivalent Courses
Nil

Exclusive Courses
Nil

Part II Course Details

Abstract

Large amounts of data containing sensitive personal information are being constantly collected in today's digitized world. This course aims at providing students with a solid understanding of a set of core and emerging techniques for privacy-preserving data analytics. Topics include data anonymization techniques, differential privacy, multi-party computation protocols, zero-knowledge proofs, privacy-preserving machine learning algorithms, and encrypted databases and searchable encryption schemes. Learning activities include lectures, tutorials, case studies, and assignments.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	Understand common privacy metrics and their implications, and apply them to evaluate privacy risks in datasets.	20	x	x	
2	Explain the fundamental concepts, principles, and algorithms of privacy-preserving data analytics.	20	x	x	
3	Describe and analyse appropriate privacy-preserving algorithms to protect sensitive information during various data analytics tasks.	20	x	x	x
4	Identify and evaluate the effectiveness of different privacy-preserving algorithms in various scenarios, considering factors such as data sensitivity, computational overhead, and legal requirements.	20	x	x	x
5	Understand the latest developments in the field of private data analytics, including the emerging trends, challenges, and novel algorithms.	20	x	x	x

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Learning and Teaching Activities (LTAs)

	LTAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lecture	Lectures will be supplemented with case studies for identifying the security and privacy issues in digitised world, and exploring countermeasures that support privacy-assured applications.	1, 2, 3, 4, 5	3 hours/ week

2	Tutorials	Tutorials will be conducted to help the students to understand and practise what they have learned in lectures.	1, 2, 3, 4	8 hours/ semester
3	Assignments	Require students to develop the ability to think in depth about private data analytics algorithms, and the ability to solve problems independently.	1, 2, 3, 4, 5	

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks ("-" for nil entry)	Allow Use of GenAI?
1	Assignments	1, 2, 3, 4, 5	15	3 assignments	Yes
2	Quiz	1, 2, 3, 4	15	One hour	No

Continuous Assessment (%)

30

Examination (%)

70

Examination Duration (Hours)

2

Minimum Examination Passing Requirement (%)

30

Additional Information for ATs

For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task

Assignments

Criterion

Ability to explain and use concepts, algorithms and protocols, and the ability to solve problems independently

Excellent (A+, A, A-)

High

Good (B+, B, B-)

Significant

Fair (C+, C, C-)

Moderate

Marginal (D)

Basic

Failure (F)

Not even reaching marginal levels

Assessment Task
Quiz

Criterion
Ability to explain and use concepts, algorithms and protocols

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Assessment Task
Examination

Criterion
Ability to explain and use concepts, algorithms and protocols

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Part III Other Information

Keyword Syllabus
Data anonymization techniques, k-anonymity, l-diversity, t-closeness, differential privacy, privacy budget, Laplace mechanism, composition theorems, privacy-preserving data publishing, privacy-preserving data analytics, trustworthy

machine learning, multi-party computation (MPC), secret sharing, zero-knowledge proofs (ZKPs), non-interactive zero-knowledge proofs (NIZKs), zk-SNARKs, federated learning, encrypted databases, searchable encryption.

Reading List

Compulsory Readings

	Title
1	Cynthia Dwork, Aaron Roth. The Algorithmic Foundations of Differential Privacy. Now Publishers, ISBN 1601988184, Available online at https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf, 2014.
2	Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography, Part III. CRC Press, ISBN 0849385237, version 0.6 in Jan. 2023, Available online at https://toc.cryptobook.us/, 2023.

Additional Readings

	Title
1	Kui Ren, Cong Wang. Searchable Encryption: From Concepts to Systems. Springer, ISBN 3031213769, 1st edition, 2023.