UFMG/ICEx/DCC — Prof: Mário S. Alvim
Quantitative Information Flow (QIF)
1st Semester of 2021

Instructions Regarding the Seminar

General goals

- **All students** have to investigate a new topic on QIF, or explore in deeper depth a topic on QIF covered in the course, understanding its fundamentals and possible applications, and communicating their discoveries to their colleagues in class.
- **Graduate students** are encouraged, when possible, to apply the knowledge obtained in the course to some aspect of their research, be it directly related to their thesis/dissertation or not.
- **Everyone** should have some fun investigating new and intriguing subjects! ☺

Organization and evaluation

- Seminars will be presented by groups of 1 student (for graduate students) or 2 students (for undergraduate students).
- The seminar is worth 30 marks distributed as follows:
  1. A **written report**, in the format of a short paper with **at most 5 pages** (excuding bibliographic references), **single column**, **font size of 11pt**. You are **strongly encouraged to use LaTeX**, and if you do so, please **use the SBC template for papers available here**: `http://www.sbc.org.br/documentos-da-sbc/summary/169-templates-para-artigos-e-capitulos-de-livros/878-modelosparapublicaodeartigos`. **(12 marks)**
  2. An **oral presentation** in class, with duration of at most 12 minutes, followed by 5 minutes dedicated to questions and discussion (time constraints may vary depending on the number of students enrolled for the seminar). **(18 marks)**
- Both the written report and the oral presentation will be evaluated according to:
  1. depth and relevance of the students' coverage of the topic,
  2. clarity and conciseness, and
  3. ability to communicate to your peers the knowledge you acquired.
- Important remarks:
  - In the written report the students must use **their own words** to explain the topics studied. Any plagiarism detected will be severely punished.
  - All students must be present at every other students' presentations. Students who skip a colleague's presentation without a valid justification will have their grade reduced.

Suggested topics

- **Graduate students** are encouraged (but not mandated) to apply the knowledge obtained in the course to a problem in their research area. A great seminar would ideally lead to a formal modeling or to a solution in terms of QIF of some problem in the student's thesis/dissertation.
- If you cannot directly apply QIF to your research problem quite yet (or if you are not a Graduate student with a research problem to begin with), an alternative is to choose relevant papers on your area of interest that use QIF and understand why and how they do it, explaining the advantages and shortcomings of their approach.

  E.g.: How is QIF used in Machine Learning, Security and Privacy, Pattern Recognition, Robotics, Artificial Intelligence, etc.? What information measures are used? Do the measures chosen really capture the intuitive notion of "information" in that specific problem? Is the concept of a information-theoretic channel used in their modeling? Etc...
- If you believe that what you need from QIF to apply to your area of interested was not yet covered in this course (the course will still go on for a couple of months), an option for your seminar is study a topic on QIF and report on it. Table 1 contains a list of suggestions for topics. **This list is not exhaustive:** you may propose your own topic!

Important dates

Task	Due date	Observations
Inform the professor about chosen groups and topics	**Before 10:00 PM of July 26th 2021**	• One member per group must fill in the form https://forms.gle/ya9s45j39UnrEH8E9, before the deadline, informing: a) the group members (E.g.: Ana Alves, Breno Brito, Clara Campos); b) in case the group wants to choose from the table of suggested topics, inform a list of priorities ordered from the most preferable topic to the least preferable one: (E.g.: B A D E C G I H J F). • Ties, if any, will be broken using the group's grades so far in this course.
Discussions about topics	**July 27th 2021 during class**	• This is the time for groups to discuss their topics with the professor. • In this day the order of presentation among groups will be defined.
Submission of written report	**Before 10:00 PM of August 22nd 2021**	• One member per group must submit the report in PDF format via Moodle.
Lightning oral presentations	**August, 26th–31st and September 2nd, 2021 during class**	• Presentation days will be defined randomly. • Groups are encouraged to present live. However, if needed, they can pre-record their presentation and make it available to the whole class on YouTube. In this case the video will be played by the professor during class. • In all cases, the questions & answers part of the seminar will happen during class for all groups, independently of whether their presentations were live or pre-recorded.

The Science of QIF Book	
Chapter 13	Quantitative information flow in sequential computer programs
Chapter 19	Timing attacks on blinded and bucketed cryptography
Chapter 20	Defense against side channels
Chapter 21	Multi-party computation: The Three Judges protocol
Chapter 22	Voting systems
Chapter 23	Differential privacy
Scientific papers	
Paper A	LeakWatch: Estimating Information Leakage from Java Programs [7] (Estimating leakage in real programs.)
Paper B	F-BLEAU: Fast Black-Box Leakage Estimation [6] (How to estimate leakage in a black-box system?)
Paper C	The thermodynamics of confidentiality [8] (What do QIF and the 2^{nd} law of thermodynamics have in common?)
Paper D	Information Leakage Games [1] (QIF meets game theory.)
Paper E	Anonymity protocols as noisy channels [5] (Understanding anonymity in QIF.)
Paper F	QQIF: Quantum Quantitative Information Flow [3] (Just like QIF, but quantum!)
Paper G	Quantifying Vulnerability of Secret Generation Using Hyper-Distributions [2] (When the prior is not only a distribution, but a hyper...)
Paper H	Comparing Systems: Max-Case Refinement Orders and Application to Differential Privacy [4] (Refinement for max-case vulnerabilities.)

Table 1: Suggested topics for the seminar. This list is not exhaustive: you may propose your own topic of interest.

References

[1] Mário S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi. Information leakage games. In Stefan Rass, Bo An, Christopher Kiekintveld, Fei Fang, and Stefan Schauer, editors, Proceedings of the 8th Int. Conf. on Decision and Game Theory for Security (GameSec), volume 10575 of LNCS, pages 437–457. Springer, 2017.

[2] Mário S. Alvim, Piotr Mardziel, and Michael W. Hicks. Quantifying vulnerability of secret generation using hyper-distributions. In Matteo Maffei and Mark Ryan, editors, Principles of Security and Trust - 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings, volume 10204 of Lecture Notes in Computer Science, pages 26–48. Springer, 2017.

[3] Arthur Américo and Pasquale Malacaria. QQIF: quantum quantitative information flow (invited paper). In IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2020, Genoa, Italy, September 7-11, 2020, pages 261–270. IEEE, 2020.

[4] Konstantinos Chatzikokolakis, Natasha Fernandes, and Catuscia Palamidessi. Comparing systems: Max-case refinement orders and application to differential privacy. In 32nd IEEE Computer Security Foundations Symposium, CSF 2019, Hoboken, NJ, USA, June 25-28, 2019, pages 442–457. IEEE, 2019.

[5] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Prakash Panangaden. Anonymity protocols as noisy channels. Inf. and Comp., 206(2–4):378–401, 2008.

[6] Giovanni Cherubin, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. F-BLEAU: fast black-box leakage estimation. In 2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019, pages 835–852. IEEE, 2019.

[7] Tom Chothia, Yusuke Kawamoto, and Chris Novakovic. Leakwatch: Estimating information leakage from java programs. In Mirosław Kutyłowski and Jaideep Vaidya, editors, Computer Security - ESORICS 2014, pages 219–236, Cham, 2014. Springer International Publishing.

[8] Pasquale Malacaria and Fabrizio Smeraldi. The thermodynamics of confidentiality. In 2012 IEEE 25th Computer Security Foundations Symposium, pages 280–290, 2012.