INFO-F514: protocols, cryptanalysis and mathematical cryptology

Liran Lerman and Christophe Petit
Université libre de Bruxelles

January 26, 2026

In this course, we will study some advanced cryptography concepts, and relate them to the design of e-voting systems.

Voting represents one of the most important process in democratic elections. In Belgium, elections are held to elect representatives at local, regional, national and European levels. Elections are also routinely organized at unions, and multiples decisions are taken in countless organizations by letting qualified people vote. At ULB level, there were also rectoral elections in 2025, with students, administrative and scientific staff eligible to vote for the first time. Interestingly, these elections also used cryptographically designed election systems.

In recent years, several solutions were proposed in order to improve voting systems, among others electronic systems (a.k.a., e-voting). Cryptographers aim to design end-to-end verifiable voting systems, where voters can verify that their votes are cast as intended; recorded as cast; and counted as recorded. By essence, e-voting requires to handle highly personal data. This information must then be protected from hackers, individual users and potentially wannabe authoritarian governments.

Prerequisites: INFO-F415 Introduction to Cryptography
Evaluation: oral exam based on a the course material (50%) and a group project (50%).

Contents

1 Course content and organization

1.1 Content

After a general introduction, we will cover various aspects relevant to the design of e-voting systems. The first part of the course will be dedicated to theoretical cryptography concepts and the second part to applied concepts.

1.2 Organization

Our learning approaches will combine 12x2h "theory" lectures with significant individual and group work during the term.

A tentative schedule for the lectures is as below:

Week	Topic	Lecturer	Paper	Date	On-campus/Teams
1	Introduction to the course and to e-voting systems	CP & LL	[2]	06/02	OC
2	"Provable security"	CP	[5]	13/02	OC
3	Homomorphic encryption	CP	[9]	20/02	OC
4	Zero-knowledge proofs	CP	[7]	27/02	OC
5	Cryptanalysis	CP	[4]	06/03	OC
6	Post-quantum cryptography	CP	[1]	13/03	OC
7	Differential fault analysis	LL (K. Papagiannopoulos)		20/03	OC
8	Security of AI	LL (S. Picek)		27/03	Teams
9	Security/Crypto in industry (Part 1)	LL	[10]	03/04	Teams
10	Security/Crypto in industry (Part 2)	LL	[10]	10/04	Teams
11	Threat model	LL	[8]	17/04	Teams
12	Secure software implementation	LL	[11]	08/05	Teams

Some of the lectures will be delivered on-campus and others will be online (over Teams). Exceptionally, some lectures might be pre-recorded. Lectures will usually take place on Fridays.

The lectures will cover significant material in a short amount of time. To make the most of them, or simply be able to follow them, you are also expected to complete significant individual work during the term. More precisely *before* each lecture takes place, you are expected to read a research paper associated to it and to answer a few questions related to the paper (see Section 2). The paper will be briefly discussed during the lecture. This preparatory work does not count towards your final mark, and neither are you requested to submit your answers. However, completing it will introduce you to the content of the lectures, hence help you follow them smoothly. It will also train you to a critical reading of research papers, which will be useful for the project.

1.3 Evaluation

The course evaluation will take the form of an oral examination, covering both the course content and the group project, each of them contributing to 50% of the mark. You will be allowed to take your project group report at the exam.

2 Lecture preparation

2.1 Introduction to the course and to e-voting systems

Main reference: Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater *Electing a university president using open-audit voting: Analysis of real-world use of Helios.* [2].

- What were the main technical and non technical challenges in this election?
- The paper is now 15 year old. What are the existing free or commercial solutions available today to carry a university rector election? How do they compare with Helios?
- Which solution would you choose for ULB elections?

2.2 Provable security

Main reference: Koblitz-Menezes, *Critical perspectives on provable security: Fifteen years of "another look at" papers* [5].

- What is generally meant by "security proof" in cryptography?
- What is the value of a security proof?
- Cite three ways a protocol that is "provably secure" can nevertheless be broken in practice
- Search the web for a proof that "ElGamal encryption protocol is IND-CPA secure if Decisional Diffie-Hellman problem is hard", and study this proof.
- Suggest two attacks on ElGamal encryption, and explain why these attacks are feasible in spite of the above security proof.
- In your opinion, should we only deploy and use e-voting systems that are "provably secure"?

2.3 Homomorphic encryption

Main reference: Alice Silverberg, *Fully homomorphic encryption for mathematicians* [9], particularly Sections 1-3.

- Define (fully) homomorphic encryption
- Describe and prove the homomorphic properties of RSA encryption and ElGamal encryption.
- Describe the homomorphic properties of Paillier cryptosystem [6].
- What is a somewhat homomorphic encryption scheme? Explain how to use such a protocol to build a fully homomorphic encryption scheme.
- Can a (fully) homomorphic encryption scheme be IND-CCA secure ?
- Verify that the encryption protocols described in [9, Section 3] are somewhat homomorphic. Why are they not fully homomorphic?
- Give one potential application of such a scheme for e-voting systems.

2.4 Zero-knowledge proofs

Main reference: Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou, Thomas A. Berson, *How to Explain Zero-Knowledge Protocols to Your Children* [7].

- Explain how Mic Ali's protocol works, what security properties it aims to achieve, and why these properties are achieved.
- Zero-knowledge proofs must be *correct*, *sound* and *zero-knowledge*. Search the web for definitions of those properties.
- Explain in your own words what the title of [3] means.
- Suggest a potential application of zero-knowledge proofs for e-voting systems.

2.5 Cryptanalysis

Main reference: Antoine Joux, Andrew M. Odlyzko, Cécile Pierrot, *The Past, Evolving Present, and Future of the Discrete Logarithm* [4].

- What is a generic discrete logarithm algorithm? What do we know about the complexity of such an algorithm? What does it tell us about the complexity of a specific instance (say ECDLP).
- What does the Pohlig- Hellman algorithm tell us about the security of a specific discrete logarithm problem?
- Study the Baby Step - Giant Step algorithm.
- Study Pollard's rho algorithm for discrete logarithms.
- Implement one of these algorithms in SageMath.
- Understand the L (subexponential) notation, and the impact of the α and c parameters on the value of $L_q(\alpha, c)$.
- Browse the website `www.keylength.com`. What are the key lengths recommended for security in 5, 10, 20, 50 years time from now? How are those key lengths estimated?
- If you could base the security of an e-voting system entirely on discrete logarithm-based protocols, how would you choose your group?

2.6 Post-quantum cryptography

Main reference: Daniel J. Bernstein, Tanja Lange, *Post-quantum cryptography—dealing with the fallout of physics success* [1].

- Explain what will be the main consequences of quantum computers on the cryptographic algorithms and protocols in use today.
- What are the mathematical problems suggested to replace factoring and discrete logarithms in a post-quantum world? What is the evidence that these problems are hard for classical and quantum computers?
- Besides computational hardness, what makes a good hard problem for cryptography?

- What are the main pros and cons of lattice-based, code-based, multivariate and hash-based cryptography?
- What is the purpose of NIST's ongoing post-quantum cryptography project ?
- In a e-voting system, would you rather use on DLP protocols or on a newly developed post-quantum protocol?

2.7 Security/Crypto in industry

Main reference: Sergei Skorobogatov, *How microprobing can attack encrypted memory* [10].

- What are the differences between black-box model and white-box model?
- What are the sensitive assets in e-voting systems?
- Which software countermeasures should we add to a e-voting system in order to reduce the success probability of microprobing attacks?

2.8 Threat model

Main reference: Adam Shostack Adam, *Threat modeling: Designing for security* [8].

- What does STRIDE mean?
- What does LINDDUN mean?

3 Project

The project's main purpose is to expand your knowledge and understanding of Cryptography beyond what is covered during the regular lectures, in a direction of your choice. You are requested to form a small group, choose a research problem related to the course and a research paper addressing that question, study that paper and write two reports (a group report and an individual report) on your findings. The remaining of this document describes the successive tasks associated to this project.

We expect that all group members contribute equally to the project (quantitatively and qualitatively). We will assess this based on individual reports and interactions with you; please do get in touch as early as possible if any issue arises. The project mark will be based on the group report, the individual reports and the oral examination, taking into account individual contributions. Each group member is expected to understand and be able to defend the whole report, even if project tasks have been distributed among team members.

A research project? For this project you will have to study at least one research paper published in the literature. This will involve verifying the arguments and results presented in the paper, sometimes by writing your own code or running your own tests on existing code. To be clear, it is not expected that you will produce new scientific results of a publishable level here, but instead that you use your knowledge, judgment and skills to evaluate previous work.

3.1 Build your Group and choose a project (deadline 27/02)

The majority of groups must have 5 students. You are free to group yourselves as you wish. It may make sense to group yourselves according to your interests (see next section).

Once you have formed a group, you should identify a topic of interest and at least one (good) research paper that relates to it. The topic must of course be related to Cryptography.

How to identify good research papers? Good papers tend to be published at good venues, be written by authors from recognized institutions, have a high number of citations (relative to their age) and a high editorial quality. Use your common sense and critical skills, and ask us if in doubt.

We would suggest that you either start from a question of interest to you and search for good papers related to it, or that you browse the program of some top cryptography venues (mostly the IACR conferences eg CRYPTO, EUROCRYPT, ASIACRYPT) to identify topics of interest to you.

Assignment. You are asked to submit a one-page description of your project by the deadline in the Section "Projects" available on UV[1]. The description must include the topic description, why it is an important Cryptography question and why you chose it. It should also include a tentative workplan, describing the work you will do and how it will be organized during the term and distributed to the group members. It should of course clearly reference the research paper(s) that you will be focusing on to address your problem, as well as any other source used.

Priority claims and early feedback. All groups must have clearly distinct projects. Your group can claim priority for a particular project by proposing it ahead of the submission deadline on the relevant discussion page on UV. In case of conflict, the first group to post their idea on this page will get the priority on the project, and the other group will have to find a new project.

Evaluation. This is a formative assignment; we will provide feedback on your proposal to ensure you are on good tracks for the project. The assignment does not count towards the final mark, but a penalty of up to 5% of the project mark can be applied if you do not submit your project proposal by the deadline.

3.2 Study the paper

Some questions you may want to consider when reading a research paper:

- What is the problem considered? How important is it? Does it relate to other more important problems? What is the evidence that the problem is important?
- How much work had been done previously on that problem? What were the limitations in previous works? Is the paper providing a fair description of the state-of-the-art?
- Have the papers cited appeared in good venues?
- What is exactly the gap that the paper aims to fill in? Judging from the abstract, introduction and conclusion, does it succeed in doing that?
- What is the most important idea in the paper?
- What is the methodology employed in the paper? Is this methodology sound? Had it been used before?
- Does the paper make any assumption or restrict the context? How realistic are those assumptions and restrictions?
- Are the results impressive? Should they be complemented with more results to provide definitive evidence? What are the main weaknesses of the results?
- Are the weakness fundamental, are they due to the methodology? could they be avoided using other techniques?
- Can you reproduce the results? If not then why is is not possible? Could you improve the results?

[1] `https://uv.ulb.ac.be`

- Are there other papers citing this one? how do they describe its contributions? do they agree with the overall conclusions? Do they identify further weaknesses? do they improve it?
- Will the paper become/remain influential in the field, or will it be quickly forgotten?

Sometimes you will not be able to verify all the authors' claims only by reading the paper and other literature items, in which case you may want to write your own code, or run your own tests on existing code to verify certain assumptions and results.

3.3 Submit progress report (deadline 27/03)

Provide an update on your progress, work distribution, and any difficulty you have faced so far.

Evaluation. This is a formative assignment; we will provide feedback on your report, sometimes clarify our expectations and sometimes suggest additional directions, to help you produce a better final report. The assignment does not count towards the final mark, but a penalty of up to 5% of the project mark can be applied if you do not submit your report proposal by the deadline.

3.4 Submit group report (deadline 30/04)

Assignment. You are asked to submit a group report by the deadline on the UV. The report must be at most 10 pages including references and appendices.

The report should summarize the question you are considering and how the paper(s) contribute to it.

It should start with an introduction motivating and defining the problem. It can then go on describing the paper's main contribution(s), explaining their assumptions, methodology, main ideas and results. When appropriate, the report can then describe your own attempts at reproducing (part of) their findings. Finally, it should put the results in perspective, explain why they are important and what are their current limitations, and possibly compare the paper(s) to other approaches in the literature. It should of course reference any source you have used.

Be critical: not every paper published at a good conference will completely solve a major open problem, and very often you will find that they have crucial limitations. You may find that authors tend to downplay the limits of their papers and highlight their advantages; in this case you should of course be more critical and justify your claims.

Attention should be paid to the editorial quality, including the overall structure, English language quality, and the proper use of scientific conventions.

The University takes plagiarism issues very seriously. See `https://bib.ulb.be/fr/support/boite-a-outils/plagiat`.

Evaluation. The report will be assessed based on technical content, editorial quality and investigation effort. See Appendix A for an indicative mark grid.

3.5 Submit individual report (deadline 08/05)

Assignment. Every student must submit an individual report by the deadline on UV. The report should be no longer than five pages. It should summarize the project (3 pages) and explain how the work was distributed between the group members (1 page).

Evaluation. Individual reports will be used to assess your individual contributions and understanding of the project. We will also assess their editorial quality. See Appendix A for an indicative mark grid.

3.6 Oral exam

In addition to the group and individual reports, your understanding of, and contribution to the project will be assessed during an oral exam. This examination will be individual.

3.7 A note on team working

Working in groups can be very stimulating and rewarding, but it can sometimes also present significant challenges. Please get in touch with us as soon as possible if you are experiencing a significant problem of this nature, which you are not able to solve within the group.

References

[1] Tanja Lange Daniel J. Bernstein. Post-quantum cryptography - dealing with the fallout of physics success. *Nature*, 549:188–194, 2017.

[2] Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a university president using open-audit voting: Analysis of real-world use of helios. In David Jefferson, Joseph Lorenzo Hall, and Tal Moran, editors, *2009 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, EVT/WOTE '09, Montreal, Canada, August 10-11, 2009*. USENIX Association, 2009.

[3] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to prove all np-statements in zero-knowledge, and a methodology of cryptographic protocol design. In Andrew M. Odlyzko, editor, *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, volume 263 of *Lecture Notes in Computer Science*, pages 171–185. Springer, 1986.

[4] Antoine Joux, Andrew M. Odlyzko, and Cécile Pierrot. The past, evolving present, and future of the discrete logarithm. In Çetin Kaya Koç, editor, *Open Problems in Mathematics and Computational Science*, pages 5–36. Springer, 2014.

[5] Neal Koblitz and Alfred Menezes. Critical perspectives on provable security: Fifteen years of "another look" papers. *Adv. Math. Commun.*, 13(4):517–558, 2019.

[6] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 1999.

[7] Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou, and Thomas A. Berson. How to explain zero-knowledge protocols to your children. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 628–631. Springer, 1989.

[8] Adam Shostack. *Threat modeling: Designing for security.* John Wiley & Sons, 2014.

[9] Alice Silverberg. Fully homomorphic encryption for mathematicians. *IACR Cryptol. ePrint Arch.*, 2013:250, 2013.

[10] Sergei Skorobogatov. How microprobing can attack encrypted memory. In Hana Kubátová, Martin Novotný, and Amund Skavhaug, editors, *Euromicro Conference on Digital System Design, DSD 2017, Vienna, Austria, August 30 - Sept. 1, 2017*, pages 244–251. IEEE Computer Society, 2017.

[11] Ken Thompson. Reflections on trusting trust. *Commun. ACM*, 27(8):761–763, 1984.

A Indicative mark grid for reports

We will use the following grid to consistently and fairly assess all the reports. The grid is taken (nearly verbatim) from the evaluation grid used at the University of Oxford for the Master in Mathematics and Foundations of Computer Science (MFoCS).

- 70 - 100 Excellent - the candidate has demonstrated an excellent understanding of almost all the material covered with a commensurate quality of presentation, and has completed almost all of the assignment satisfactorily; further subdivided by
  - 90-100 - the candidate has shown originality or insight that goes beyond a basic completion of the task set
  - 80-89 – the work submitted shows a near-perfect completion of the task in hand, whether a mini project or dissertation, but does not meet the additional requirements above, or does but has defects in presentation
  - 70-79 - the work submitted is of a generally high order, but may have minor errors in content and/or deficiencies in presentation
- 60 - 69 Good - the candidate has demonstrated a good understanding of much of the material, and has completed most of the assignment satisfactorily
- 50 - 59 Adequate - the candidate has demonstrated an understanding of the material and an ability to apply his or her understanding that together are sufficient to pass;
- and at levels that fail
  - 40 - 49 The work submitted, while sufficient in quantity, suffers from sufficient defects to show a lack of adequate understanding or ability to apply results
  - 30 - 39 – the candidate, while attempting a significant part of the mini project or in writing a dissertation, has displayed a very limited knowledge or understanding at the level required for a master's degree
  - 0 – 29 - the candidate has either attempted only a fragment of a mini project / dissertation or has shown an inadequate grasp of basic material.

Note that the project mark will also depend on your individual contributions and on your performance at the oral examination, and that your understanding of the course content will also be separately assessed at the oral examination.