CS/BiRC
PhD & postdoc retreat 2019
Program for CS/BiRC PhD Retreat 2019

9:15 PowerPoint karaoke
10:00 Welcome (Sofia Rasmussen, Ira Assent, Anders Møller)
   Tips & tricks for writing progress report and PhD thesis (Anders Møller)
11:00 Mindfulness as stress relief (Niels Viggo Hansen, Center for Mindfulness)
12:00 Lunch
12:30 Track 1: Advice for writing research grant applications (Mogens Nielsen)
   Track 2: How (not) to present a paper (Anders Møller)
13:30 Track 1: Alternative career paths (Aino Corry, Metadeveloper)
   Track 2: Group work on presentations
15:00 Coffee break, guided tours and free time at Moesgaard
   Guided tour (15:00 – 16:00):
     • Option 1: The first Immigrants
     • Option 2: People of the Sun
17:00 Departure from Moesgaard
18:30 Dinner at Chemistry Canteen, AU
PhD partner at GSST

• Maia Høyer Monod is PhD partner for Computer Science and Bioinformatics

• Office in Nymunkegade, Building 1521, room 113

• CS office (Mondays 12:30-15:30) Hopper-131
Juniorklubben

• Arranges social events for PhD students from all research groups

• Budget for events, and practical support from student helpers and PhD administrator

• Currently managed by Lau Skorstengaard and Aina Georges, but Lau will soon hand in his thesis

• Looking for one or two people to help Aina
Areas to work with:

- **Stress and general well-being**
  - Teaching can be stressful → remember you can opt out
  - Support groups are not always taken seriously by staff members

- **Community-feeling**
  - Break down prejudices between research groups → events and study groups that create bonds across research groups
  - Keep a positive mindset about all research groups

- **Relationship with manager**
  - Lack of acknowledgement and matching of expectations lead to insecurities → Remember to talk to your supervisor
  - Make use of the staff development dialogue which is offered annually

If you want the full report email Sofia
Writing a Progress Report

Goals:
- demonstrate solid progress on the research project
- present an ambitious and realistic plan for Part B
- show an ability to communicate scientific work

Recommended structure:
- Short introduction to the field of research and aims of the project
- Overview of results obtained so far (reuse of material is permitted)
  - Can be partial results, or research techniques acquired
- Ideas for Part B, tentative work plan ← OFTEN TOO LITTLE EMPHASIS!
  (Max. 30 pages)

An opportunity for
- Reflecting on where you are heading and how to get there
- Getting feedback from experienced researchers
Writing a PhD thesis

“The PhD thesis must document the academic independence of the PhD student and that the PhD student has contributed to the development of new knowledge that meets the international standards of the field. Therefore, the thesis must demonstrate the PhD student’s ability to independently plan, initiate and carry out research as well as participate in international discussions within the chosen research field.”

https://phd.scitech.au.dk/about-us/basic-principles/
“If the thesis is composed mainly of manuscripts or papers (regardless of whether the complete texts are included, or they have been edited to form a coherent monograph-like thesis), the thesis must include one or several introductory sections in the student's own words (i.e., not re-using text from papers not solely written by the student) encompassing the following elements (not necessarily in this order):

- A brief description of the proposed research questions in the papers
- A summary of the results and an assessment of the applied methodologies
- A clear description of the student's own contributions to the work, including an outline of the student's role in writing manuscripts or papers included in the thesis
- A critical review in which the PhD student relates his or her own work to the most state-of-the-art work within the field. The PhD student must also demonstrate that he or she has an up-to-date knowledge hereof and is able to put this knowledge into a broader perspective”

Note: rules and guidelines are different at other universities, especially in other countries!
Recommendations for your thesis

- Typical (recommended) structure:
  - Part I: Overview
    - Your(!) new text, puts your work in a broader perspective
    - Provide a “reading guide” – how are the different sections in Part I related to the sections in Part II, emphasize what’s different compared to the papers
    - Background material
    - Overview of results
    - Related work
  - Part II: Papers

- If you prefer to reorganize the parts to obtain a more coherent flow:
  - Extreme case: monograph style (highly uncommon at CS.AU)
  - Be explicit about what parts (chapters/sections/paragraphs/figures) are identical to published papers, and which parts are “new”!

  - Prevents concerns about self-plagiarism!
  - Helps the readers (≥ the evaluation committee)!
  - (Reuse of material from your Master’s thesis is not permitted, but it is perfectly fine to reuse material from your progress report)
iThenticate – (self-)plagiarism detection

http://www.au.dk/en/research/responsible-conduct-of-research/

Low Overhead

In this section, we discuss our results on fully homomorphic UC commitments with low overhead that we first presented in [34, 36] (from where we have taken this discussion almost verbatim).

We first observe that even if we cannot build practical UC commitments without using public-key technology, we might still confine the use of it to a small once-and-for-all set-up phase. This is exactly what we achieve: given initial access to a small number of oblivious transfers, we show a UC secure commitment scheme where the only computation required is pseudorandom bit generation and a few elementary operations in a finite field. The number of oblivious transfers we need does not depend on the number of commitments we make later. The main observation we make is that we can reach our goal by combining the oblivious transfers with a “sufficiently compact” Verifiable Secret Sharing Scheme (VSS) that we then construct. The VSS has applications on its own as we detail below.

To commit to a $k$-bit string, the amortized communication cost is $O(k)$ bits. The computational complexity is $O(k)$ for the verifier and $O(k^{1+\epsilon})$ for the committer (where $\epsilon < 1$ is a constant). This assumes a pseudorandom generator with linear overhead per generated bit. In an alternative variant of the construction, all complexities are $O(k \cdot \text{polylog}(k))$. After the set-up phase is done, the prover can commit by sending a single string. Our construction extends to commitment to strings over any finite field and is additively homomorphic. Moreover, if the prover sends one extra string, the verifier can also check that committed vectors $a, b, c$ satisfy $c = a \cdot b$, the component-wise product. Finally, again by sending one extra string and allowing one extra opening, the verifier can compute a commitment to $\varphi(a)$, given the commitment to $a$, for any linear function $\varphi$. These extra strings have the same size as a commitment, up to a constant factor.

On the technical side, we take the work from [50] as our point of departure. As part of their protocol for secure 2-party computation, they construct an imperfect scheme (which is not 2

2This seems a very plausible assumption as a number of different sufficient conditions for such PRGs are known. In [63] it is observed that such PRGs follow Alekhnovich’s variant of the Learning Parity with Noise assumption. Applebaum [5] shows that such PRGs can be obtained from the assumption that a natural variant of Goldreich’s candidate for a one-way function in NCK is indeed one-way. The improved HILL-style result of Vadhan and Zheng [90] implies that such PRGs can be obtained from any exponentially strong OWF that can be computed by a linear-size circuit.
3.1 Udtalelse af 30. januar 2018 og 31. januar 2018

Tema: Selvplagiat

De videnskablelige produkter i sagerne var to såkaldte artikelbaserede ph.d.-afhandlinger indleveret til bedømmelse hver især bestående af en sammenfatning (kappe) og 4 studier beskrevet i artikler/manuskripter. Sagerne var nærmest identiske, og udvalgets udtalelse i de to sager var derfor enslydende.

Praksisudvalget var af den opfattelse, at kappen og de fire studier måtte anses som 5 selvstændige publikationer, da de er publiceret enkeltvis i hver sin kanal.

Praksisudvalget fandt, at det i kapperne indledninger tydeligt var angivet, hvilke studier afhandlinger byggde på. Der var for Praksisudvalget ingen tvivl om, hvorledes studierne og disse resultater var afspejlet i de sammenfattende dele af kapperne, hvor artiklerne blev sat i relation til hinanden. Spørgsmålet var derfor, om der forelå selvplagiering og dermed tvivl som forskningspraksis, når forskere under de i sagerne foreliggende omstændigheder citerede sig selv ordet uden at markere dette ved anførselsstegn, kursivering, indrykning eller anden tydelig markering med angivelse af kilden.

Udvalget fandt, at der i begge afhandlinger var flere eksempler på tekst, der var kopieret ordret fra en publikation til en anden (kapperne), uden angivelse af, at det var kopieret tekst. Der var f.eks. manglende selvfreference i kappernes diskussion, hvor der var kopieret substantielle tekstafsnit fra manuskripter/artikler direkte ind i kapperne, uden at det gengivne var markeret med anførselsstegn, kursivering, indrykning eller anden tydelig markering. Udvalget vurderede, at kopiering af substantielle afsnit fra en selvstændig publikation til en anden, ikke var i overensstemmelse med god forskningspraksis på dette forskningsområde.

“Results, data, figures, and ideas taken from other sources should always be indicated by detailed references to the original source, even if you were the author yourself.”

“Text copied (or paraphrased) from other sources should be clearly marked, and the original source indicated. This includes text copied (or paraphrased) from your own previous work. For smaller excerpts, give explicit references where the re-used text appears. When re-using larger sections (e.g., if a published or submitted paper is incorporated as a thesis chapter—perhaps with some re-phrasing to fit into a coherent thesis set-up) indicate this explicitly with a reference to the source at the beginning of the re-used material, and/or in the thesis introduction. Do not just state that Chapter X is based on Paper Y, but state more explicitly, for example, that the chapter is identical to the paper except for page layout, or that specific sections have been added or removed.”
How to give an overview of your results without self-plagiarizing?

- Don’t copy-paste large pieces of text from the papers (even with proper references)
  - The readers don’t want to read the same thing twice
- If you feel that you are trying to rephrase sentences from the papers, just to “write new text in your own words” but really saying the same as the sentences in the papers, you are doing it wrong!
  - The purpose of the introduction chapters is to put your work in a broader perspective, not to repeat what’s in the papers
- Ask yourself,
  - what common themes tie together your results?
  - what work of others does your work build upon? (in research papers, there’s usually not much space for this)
  - how does your results differ from related techniques by others?
  - what can your results be used for by others?
Other things to think about

- The introduction should properly motivate your work
- The central research challenge should be clear from the very first paragraphs
- What new knowledge have you produced? (vs. what have you done)
- Explain your research methodology and why is it appropriate
  - Importance of this depends on the field
- Define (and motivate) your focus: what is relevant and what is not?
  - The reader may be interested in the same topics but with a different focus
- Which questions remain unresolved? What future work does your thesis pave the way for?
  - Relevant for the Conclusion chapter
- Has the state-of-the-art changed over the duration of your work? If so, how?
  - In some cases there can be substantial developments within short time
Exercises (for PhD students)

Examine the structure of one or more theses from http://cs.au.dk/education/phd/phds-produced/

- Is the structure of the thesis explained to the reader?
- Is the research methodology explained?
- Is there an explicit “thesis statement” or a list of “hypotheses” or “research questions”?
- Is it clear which parts of the thesis have also been published at conferences/workshops/journals?
- Can you easily identify which sections or paragraphs contain background material (that the thesis work builds upon)?
- Can you easily identify which sections or paragraphs discuss related work (and how the contributions of the thesis are positioned)?
- If the thesis is structured in two parts (with papers in Part II), to what extent are the results from the papers repeated or summarized in Part I?

Note: All the theses were accepted, but not all of them are role models ;-) Also, just a few years ago, there wasn’t as much focus on self-plagiarism
Exercises (for postdocs)

- What were the main questions or concerns you had when writing your thesis?
- As a (future) supervisor of PhD students, how do you teach your students how to write a thesis? What is important for your students to be aware of?
- In case you have supervision experience, what were you/the student struggling with when writing a thesis (or project report)?
Exercises for *How (not) to present a paper*

Study one or more presentations you or another student/postdoc have given at a conference or workshop

- How much of the presentation is spent on
  - motivating and explaining the research problem?
  - the proposed solution?
  - examples?
  - technicalities (formal definitions, theorems, proofs, …)
  - (experimental) results?
  - related work? future work?
  - ..or other purposes?

- What is assumed from the audience?

- How did you practice before the conference/workshop?

- How did you prepare for questions?

- Did you violate some of the advice given by Anders? If so, why?

- What should be done differently if you only had half the amount of time available for the talk?

- What should be done differently if the audience was broader, for example covering all of Computer Science (or Bioinformatics)?

- Do you recall any terrific (or terrible) talks you have seen? What made them memorable?