COS 597C Final Project

Mark Zhandry

1 Assignment

You final project will be to survey some research on obfuscation that was not directly covered in the course. Specifically, you will read 2-3 research papers on a subject relating to obfuscation, write a report, and give an in class presentation during the final week of class. You are encouraged, but not required, to have some open problem in mind when selecting the papers to survey — solving an open problem in obfuscation would make for an excellent report!

1.1 Guidelines

The report should cover the most interesting or important parts of the papers surveyed, and should *not* strive to cover all of the technical details. The goal is to distill the papers down into a concise and easy-to-read report that delivers the main ideas. You should take some time to think about what are the essential contributions of the papers and how the papers relate to the broader study of obfuscation.

If you choose, you may work in pairs. Naturally, the scope of the project should be correspondingly expanded.

1.2 Minutia

Project Proposal:

- Before starting your project, please send me an email stating which papers you would like read and any open problems you would like to potentially explore in this project. This way, I can give you feedback and suggestions before you embark on your project.

Project Report:

- There is no page minimum or maximum for the report, but reports will probably be in the range of 5-10 pages.
- The report should contain at least one precise theorem statement along with corresponding proof for one of the main results of the papers surveyed. If you are able to solve an important open problem, the statement of the problem and proof can satisfy this item.
- The paper should be readable to anyone who has taken the course. This means any concepts not covered in class should be properly defined.
- Your report should be typeset using LaTeX.

Final Presentation:

- The presentation will be 20 minutes (40 minutes if working in pairs), including a couple minutes at the end for questions.
- The presentation can be either slides or a whiteboad talk.
- As above, the presentation should be understandable to anyone who has taken the course.
- The presentations will be held in class during the last week of class.

Deadlines and submission instructions:

- **Proposals: Monday, November 12, 11:59pm.** You are also encouraged to discuss your project idea with me prior to the proposal deadline.
- **Presentation: In class during the last week of class.**
- **Report: Dean's Date, Tuesday, January 17, 11:59pm.**

2 Project Ideas

The following are just a handful of papers relating to obfuscation. You can select from these, or try to find others. The best way to find other papers is to search the IACR eprint archives: https://eprint.iacr.org.

- Notions of obfuscation not discussed in class:
  - Public Coin Differing Inputs Obfuscation (diO): https://eprint.iacr.org/2014/942.pdf.

  - Virtual Gray Box (VGB) Obfuscation: https://eprint.iacr.org/2014/554.pdf.
  - Obfuscation for evasive functions: https://eprint.iacr.org/2013/668.pdf.
  - Point Obfuscation: https://eprint.iacr.org/1997/007.
- Other applications
  - Trapdoor permutations: https://eprint.iacr.org/2015/126.pdf
  - Traitor tracing: http://eprint.iacr.org/2013/642.pdf
  - Leakage resilient cryptography: https://eprint.iacr.org/2016/730.pdf
  - Watermarking: https://eprint.iacr.org/2015/344.pdf, https://eprint.iacr.org/2015/373.pdf
  - Multiparty Computation: https://eprint.iacr.org/2013/601
- One-out-of-two impossibility results: https://eprint.iacr.org/2015/487.pdf, http://eprint.iacr.org/2014/405.pdf, https://eprint.iacr.org/2014/402.pdf, http://eprint.iacr.org/2013/703.pdf
- Obfuscating NC^1 circuits directly: https://eprint.iacr.org/2015/025.pdf, https://eprint.iacr.org/2014/776.pdf, https://eprint.iacr.org/2016/418.pdf
- Using weaker tools for specific applications:
  - Witness Encryption: https://eprint.iacr.org/2013/258.pdf
  - LWE: https://eprint.iacr.org/2016/418.pdf, https://eprint.iacr.org/2016/117.pdf, https://eprint.iacr.org/2015/715.pdf, https://eprint.iacr.org/2016/110
  - Witness PRFs: http://eprint.iacr.org/2014/301
  - ELFs: https://eprint.iacr.org/2016/114
- Connections to differential privacy: http://eprint.iacr.org/2013/642, https://eprint.iacr.org/2016/721
- Universal Obfuscation: https://eprint.iacr.org/2016/281.pdf, http://eprint.iacr.org/2016/289.pdf
- Obfuscation from concrete MMap assumptions: https://eprint.iacr.org/2014/309.pdf, https://eprint.iacr.org/2013/781.pdf
- Functional Encryption (FE)

  - iO from FE: https://eprint.iacr.org/2015/163.pdf, https://eprint.iacr.org/2015/173.pdf
  - iO applications from FE: https://eprint.iacr.org/2015/1078.pdf, https://eprint.iacr.org/2016/102.pdf
- Other MMap candidates
  - CLT13: https://eprint.iacr.org/2013/183.pdf
  - GGH15: https://eprint.iacr.org/2014/645.pdf
- Attacks on other MMap candidates: http://eprint.iacr.org/2014/906, https://eprint.iacr.org/2015/1037.pdf