KTH Computer Science and Communication

Presentation of advanced topic
Foundations of Cryptography 2015

Goal

Recall that one of the learning outcomes of the course is to "read and understand technical articles in cryptography". How well you meet this goal is mainly assessed using some of the implementation exercises and your talk.

Topics

This year you can choose one of the following topics for your presentation.

- Yao's garbled circuits.
- Lattice-based cryptography.
- Bilinear pairing-based cryptography.
- The SHA-3 (Keccak) hash function.

Do not ask me for pointers to literature, I am sure that you can find sufficient material online on your own and part of the exercise is for you to use your own judgement and choose interesting material.

In class we discussed restricting the number of students picking the same topic. There are no such restrictions, but you may not pick the same topic as another member of your study group for the presentation.

Rules

Presentations not adhering to the following requirements may be cancelled, interrupted, or awarded zero points.

- The presentation must be prepared and given individually in English.
- The presentations will be given in blocks of up to 4 presentations in a 1 hour session. Each student is required to attend the other presentations in the session in which he gives his own presentation.
- The time allowed for the presentation is 12 minutes. Timing is important and normally a warning is given when 3 minutes remain. After 15 minutes the talk is interrupted.
- You may discuss your presentations and give practice talks in study groups of three students. You may be involved in a different study group for your presentation than those for the homeworks. The members of the study group should be stated at the beginning of your presentation (on the first slide if you use slides, and on the whiteboard otherwise).

Grading

You can get 30-80 P-points for your presentation. Keep in mind that this is $80/281 \approx 28\%$ of the maximal number of points awarded, so take it seriously. Your grade is broken down into grades for the following aspects.

- **(20P) Choice of content.** Focus on *your topic* and not on cryptography in general. Choose things that you are excited about, and that are interesting to and can be explained to your fellow students in 12 minutes.
- **(20P) Understanding of the content.** Develop your own understanding of the subject. Use your own phrases during the presentation and prepare your own images and examples to show that you understand what you are doing. You should also be ready to answer questions related to what you present.
- **(20P) Quality of slides (or whiteboard).** A non-exhaustive list of basic things that you should think about is:
  - Do not put everything you say on the slides.
  - Use images, but make sure that they are tidy and don't look like bitmaps.
  - Do not put too much text or images on a single slide.
  - Do not confuse the audience with irrelevant text or information in images.
- **(20P) Presentation skills.** A non-exhaustive list of basic things that you should think about during your talk is:
  - Make sure that we hear what you are saying.
  - Make sure that you know what you are going to say, but don't use any written notes.
  - If your native tongue is not English, then the previous two points are even more important.
  - Don't read the text on your slides out loud.
  - Focus your attention on the audience, not only on the lecturer, and not on your slides.
  - Show your enthusiasm! You chose the content so you should like it.
  - Respect the time limit, but use your alotted 12 minutes fully.

Equipment

Presentations can be given on the blackboard/whiteboard (whatever is available in the allocated room) and/or using slides projected from a computer (and blackboard/whiteboard). We bring a projector and a computer with Windows 7, but if you want to use our computer to present your slides you must email them to `dog@csc.kth.se` before 08:00 the day of your talk.

We strongly recommend that you give at least 5 complete timed practice talks on your own and/or in front of your

study group/friends before showing up to the session!!!!!