CS 519.003, ECE 599.003: Special Topics in Cryptography
Presentation & paper summary guidelines

Presentation guidelines

What to present:

- Don’t try present everything that is contained in the paper. Present what you think are the most important results relevant to the class.
- Better yet, instead of thinking in terms of results, think in terms of ideas. What are the most important ideas in the paper? What are the clever tricks or insights used to obtain the results?
- Don’t present things in their full generality. Instead, present the simplest concrete example / special case that illustrates the important tricks. Then you can just simply state (without explaining fully) what the fully general result is, with the understanding that the tricks you showed can be used to get the fully general result.

How to present it:

- Plan for 40 minutes of presentation, to allow time for questions and setup.
  I aim for a correspondence of “1 slide ≈ 1.5 minutes” (excluding content-free slides like title slide, table of contents etc). If your talk satisfies “# slides > # minutes allowed”, this is a red flag for disaster!
- Keep text on the slide to a minimum. There is no need to use complete sentences.
- Favor diagrams/pictures over text/formulas, especially for complicated things. Only use formulas for the most important or easy-to-digest pieces.
- Uri Alon suggests (in this multi-part youtube video, and this text summary thereof) that each slide should have a single premise, where a premise is a single complete sentence. Everything on that slide should directly address that premise.
  I find this a useful exercise for organizing and planning the presentation. He also suggests putting the premise on each slide as the actual title of the slide, which I don’t do, but you are welcome to.

Paper summary guidelines

- For constructions: Describe the main idea behind results/instantiations. State the security model, hardness assumptions, and efficiency analysis if relevant. State the instantiations of easy-to-state things like gate-level ciphers.
- For definitions: If a main contribution of paper, give an overview (see example in BHR12)
- Refer to the “model” summary/summaries written by me
- Include a one-sentence summary in the page source. It will be used in the index pages that display lists of all papers.
• Link to glossary terms, unless this is the paper that defines the term (in that case, the glossary entry will just direct to the more detailed explanation in that paper's summary).

• Stick to facts, avoid subjective evaluation