591Cybersecurity Class Syllabus

Jared Saia

1 Class Deliverables

The deliverables for the class will consist of a project and presentation and presentations of papers. The tentative weighting of grades will be as follows.

1. Project (60%)
2. Presentations (30%)
3. Participation (10%) (participation in class discussions via asking questions, making comments, etc.)

1.1 Project

A significant part of this class is the class project. In this project, you will apply mathematical tools learned in this class to solve an algorithmic problem. The project must have some analytical component to it where you demonstrate mastery of mathematical tools learned in this class. I also recommend that the project have an empirical component where you do empirical tests which support or complement your analytical results (It's good to have an empirical component in case you don't get the theoretical results you're trying for).

There will be two main deliverables for the project: a paper and an in-class presentation. The paper should be no more than twelve pages in length (not including bibliography and appendix). This paper should be structured as a standard research paper in that it should have an abstract, an introduction, a related work section, a body (this could contain for example a section on algorithms, a separate section on analysis and a separate section on empirical results), and a conclusion and future work section. The presentation will be 20 minutes in-class with 10 minutes for questions and answers.

You can choose to do a project with more of an empirical or theoretical focus. One type of empirical project would involve implementing an algorithm or protocol described in class, then empirically determining how this algorithm performs (e.g. in terms of robustness and resource costs) under a certain set of attacks, and then finally comparing these empirical results with the analytical results. Another more challenging (and perhaps

more interesting) project would involve simplifying an algorithm discussed in class so as to improve its resource costs empirically and/or analytically. To do this, you may need to make some additional (hopefully not too strong) assumptions. The theoretical component of such a project would be to prove that your new algorithm is still secure and the empirical component would be to implement your new algorithm to verify that it performs well empirically. Another type of project would involve designing an algorithm for a variant of some problem discussed in class (or a new security problem of your own formulation) and then proving that your algorithm is secure for some definition of security.

In general, for the class projects, I will be more excited about partial progress on a hard problem than a complete solution to an easier problem. You may work in groups of 2 or 3 on the project or you may work individually.

1.2 Presentations

Another significant component of the class is presentation of research papers. I will expect each student (again working in groups of 2-3) to present at least one paper a month in class. These presentations should be done with the help of slides or lecture notes. The presentations should present not only the main ideas and results of the paper but also give a critical analysis of the paper. Following are some of the questions you should ask about the paper you're presenting.

- What is the abstract problem being solved? How closely does this problem relate to a real-world problem of interest? Can you think of a new problem formulation that more closely matches an interesting real-world problem and is still simple enough that it's likely to yield to mathematical solution.

- Assumptions: What are the key assumptions being made? Are they realistic and simple to state?

- Results: What are the major results of the paper? If the paper describes an algorithm, is the result primarily theoretical, e.g "proof of concept", in that it shows the problem can be solved in theory, but the algorithm proposed is too complicated or slow to be useful. Alternatively, is there a reasonable chance that the algorithm could be used in practice? If the paper gives a negative result, how surprising and pertinent is the negative result?

- Mathematical Tools: What are the main mathematical tools used in the paper? Are there new tools introduced from other fields? Old tools used in new ways? New mathematical machinery created to solve the problem?(note: this is rare)

- Open Problems: How would you extend or improve the results of the paper? Don't just copy from the future work section of the paper. Think about oversimplifications the authors may have made. Are the algorithms overly complicated? Is it possible to

improve on the resource costs achieved? Can you apply the tools used in the paper to another interesting problem?

1.3 Policies

Assignment deadlines are strict: late homework will automatically receive a grade of zero, unless reasonable cause can be shown (which is easy for one, possible for two, and very hard for three or more!); no make-up.

Collaboration is encouraged on all of the homeworks. Usual university policies for withdrawals, incompletes and academic honesty.

2 Class Outline

Topics will include but will not be limited to:

- Linear Algebra and applications to Quantum Agreement and Quantum Cryptography
- Ramsey Theory and applications to privacy preservation
- Spectral Methods and applications to robust web search and robust collaborative filtering
- Sperner's Lemma and applications to Fair Division Algorithms
- The Probabilistic Method and applications to robust network creation and robust computation
- Graph Theory and applications to self-healing algorithms
- Number Theory and applications to cryptography and secret sharing

The list of papers for each of these topics is available on the class web site.