Name: Nate Chenette
Email: chenett1@rose-hulman.edu

Ideas for senior thesis topics

Areas of research interest
Cryptography
Algorithms
Combinatorics
Theoretical computer science / discrete math
Cryptocurrencies/blockchain [to an extent]

Past theses advised

- Convergence of a Continuous Ant Colony Optimization Algorithm on the Hyperplane Model [mathematical proofs that an a certain heuristic converges under certain circumstances]
- Alternatives to Conventional Heuristics Used in Contraction Hierarchies [modern shortest-path algorithms]
- A Chaos-Based Hashing Algorithm Using the Tent Map [using ideas from chaos theory to construct and test security of a hash function]
- Comparison between Two Group Signature Schemes [comparing cryptographic schemes involved in cryptocurrency protocols]
- Improvement to the PKZip Stream Cipher [a tweak to an insecure stream cipher that appears to thwart the known attack]

Thoughts about senior theses in CS theory
I am a natural person to advise theses in computer science theory. However, as can be expected from mathematical subjects, the hardest part of research in this area is coming up with an appropriate problem: one hard enough that it hasn't been solved, but approachable enough that some progress can be made in a 1-year undergraduate thesis. Often this means looking for "small" problems that piggyback on old results or extend ideas in some way. Since this is a big part of the challenge, I don't expect senior thesis students to know the appropriate problem by the time of their research proposal. However, they should have an idea of what narrow topic they want to study, including which existing papers they would start by reading and understanding. That area of research should be of relatively recent vintage, and the topic should align well with the student's interests.

How to get ideas for research problems in CS theory?
Think about theory courses you've taken (CSSE230, CSSE/MA473, CSSE/MA474, CSSE/MA479, etc.) What topics intrigued you and left you wishing you could learn more? Do a search for recent academic research in this area. Note that most of the core of these courses date from several decades ago, so see how these ideas are being extended, improved upon, or implemented in practice in the modern day. (A good example is the Contraction Hierarchies technique for finding shortest paths.)

How to get ideas for research problems in Cryptography?
Hopefully you've taken, or are currently taking, CSSE/MA479.
Look at the topics and paper titles for recent research published in the major crypto conferences. This includes the conferences (Crypto, Eurocrypt, Asiacrypt, etc.) sponsored by the IACR. Real World Cryptography is a good one for Rose students as we like real-world applicability at Rose. Looking at these gives you a sense of what crypto topics are actively studied now. What interests you, and seems within your abilities to master given a few months of study? Try to get as specific as possible—you can always branch out later.

My research background

Government research
Most of my research in the past 7 years has been summers (2016, 2017, 2019, 2022) and sabbatical (2022–23) working on interesting math/CS problems for the government in a classified setting. Unfortunately, it is impossible to involve students in this research—in fact, I can't even do it unless I'm at a secure facility. Moreover, it's best if my "outside" and "inside" work are as disjoint as possible. However, I can advise students who are interested in a career with the National Security Agency or another intelligence organization.

Academic research
My academic research expertise is in cryptography;
more specifically, searchable encryption;
more specifically, "order-revealing encryption" and "order-preserving encryption"

- Essentially, my work has studied whether it's possible for a database to allow efficient range queries, while having that data encrypted in some way. (Short answer: the security that is possible is very weak.) Here are the main three papers I've published on these topics.
    - Order-Preserving Symmetric Encryption (EUROCRYPT 2009)
    - Order-Preserving Encryption Revisited (CRYPTO 2011)
    - Practical Order-Revealing Encryption with Limited Leakage (FSE 2016)
- Since they were published, these papers have been cited hundreds of times. This is what happens when you publish constructions of very weakly-secure encryption schemes: lots of people like to break them! I have not kept up with the pace of papers being published in this area, due to a teaching-centered career and pivoting to government research as mentioned above . However, any paper citing one of mine, especially the more recent FSE 2016 paper, would be an interesting read and would potentially open doors for further research problems.
- To work on these types of problems, it would be best if the student has taken the CSSE/MA479 Cryptography course and/or the CSSE482 Applied Modern Cryptography course. That said, there will still be a learning curve in reading and understanding these papers. The math is not difficult, but there is a lot of cryptography jargon that takes some getting used to.

- Here's a nice blog post with a soft intro to searchable encryption and the state of the field of research (focusing on a particular paper from 2019, which you can skip if you like.)