Suggested topics:

**Parallel algorithms** Look at how algorithms for basic problems like matrix multiplication and sorting need to be modified to take advantage of parallelism. Starting place: see Scott Baden’s CSE 260 syllabus.

**Cryptanalysis: lattice reductions** How is the lattice reduction algorithm of Lenstra, Lenstra and Lovasz used in cryptanalysis?

**Cryptanalysis: factoring** The quadratic sieve method for factoring large integers.

**Cryptography: batch verification** How to gain efficiency in verifying multiple signatures simultaneously. Starting place: Fast verification for modular exponentiation and digital signatures. Bellare, Garay, and Rabin.

**Vision** Shape recognition and object recognition using shape contexts. Belongie, Malik, Puzichar. Concentrate on the problem of finding the closest match spatial transformation.

**Data Structures** Double hashing with pass bits. Burkhard, IPL 2005.

**Graphics** Inverse Kinetics. See Sam Buss’s website.


**Bioinformatics**


Circuit design Arithmetic algorithms for hardware implementation. See CSE 246 syllabus.

Circuit design Wang, Zhang, Chen, Yang, Cheng, Graham. Bus Matrix synthesis ased on Steiner Graphs for Power Efficient System on a chip

Circuit design Albrecht, Kahng, Mandiou, Zelikowsky, Multicommodity Flow Algorithm for Buffering Global Routing, 2005. See also prior ISPD paper by Albrecht.


Data Mining and other applications The Johnson-Lindenstrauss transform. Starting place: Dasgupta paper.
**Data Mining** Differential privacy. Starting place: papers by Cynthia Dwork.


**On-line algorithms** Starting place: Online computation and Competitive Analysis, Borodin and El-Yaniv (book, project should be based on e.g., first chapter).

**Streaming algorithms** Starting place: S. Muthukrishnan, Data Streams: Algorithms and Applications, Foundations and Trends in TCS. (Pick one problem.)

**Computational economics** Algorithmic mechanism design. Starting place: Nisan and Ronen, 1999.


**Coding** Achyara, Das, Orlitsky, Pan. Algebraic computation of pattern maximum likelihood.

**Network routing** Levchenko, Voelker, Paturi, Savage: XI: an efficient network routing algorithm.

**Improved SAT algorithms** Compare approaches of Paturi, Pudlak, Zane and of Schoning.