Fall 2018 Systems Prelim Proposal

Ian Martiny

September 19, 2018

1 Preparations

My classes related to my Preliminary exam include: CSCI 7000 - Topics in Computer Science (Fall 2015, Cryptography and Cryptanalysis), CSCI 5573 - Advanced Operating Systems (Spring 2016), ECEN 5014 - Special Topics (Spring 2016, Computer Security and Privacy), CSCI 5273 - Networks Systems (Fall 2016), MATH 5440 - Coding and Cryptography (Fall 2016). CSCI 7000 - Topics in Computer Science (Fall 2017, Censorship Circumvention and Prevention), ECEN 5008 - Special Topics (Fall 2017, Adv Computer/Network System Security)

Over the last two years I have also been involved in a Network Security Reading group and worked on research projects with Dr. Eric Wustrow.

2 Topic Area

I will complete my Preliminary exam in the intersection of a few areas, including: Secure messaging, privacy, and web security.

Dr. Eric Wustrow has approved this preliminary exam.

3 Papers

The foundation of papers I will base my review on include: Dissent in Numbers: Making Strong anonymity scale [9]. DP5: A Private Presence Service [3]. Secure Multi-party computation for privacy preserving data mining [6]. Pinocchio: Nearly practical verifiable computation [8]. SNARKs for C: Verifying program executions succinctly and in zero knowledge [1]. Zerocoin: Anonymous distributed e-cash from bitcoin [7]. Secure Multi-party computation goes live [2]. Protocols for Secure Computations [10]. Differential privacy: A survey of results [4]. Rappor: Randomized aggregatable privacy-preserving ordinal response [5]

References

[1] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. Snarks for c: Verifying program executions succinctly and in zero knowledge. In *Advances in Cryptology–CRYPTO 2013*, pages 90–108. Springer, 2013.

[2] Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, et al. Secure multiparty computation goes live. In *International Conference on Financial Cryptography and Data Security*, pages 325–343. Springer, 2009.

[3] Nikita Borisov, George Danezis, and Ian Goldberg. Dp5: A private presence service. *Proceedings on Privacy Enhancing Technologies*, 2015(2):4–24, 2015.

[4] Cynthia Dwork. Differential privacy: A survey of results. In *International Conference on Theory and Applications of Models of Computation*, pages 1–19. Springer, 2008.

[5] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 1054–1067. ACM, 2014.

[6] Yehida Lindell. Secure multiparty computation for privacy preserving data mining. In *Encyclopedia of Data Warehousing and Mining*, pages 1005–1009. IGI Global, 2005.

[7] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Security and Privacy (SP), 2013 IEEE Symposium on*, pages 397–411. IEEE, 2013.

[8] Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova. Pinocchio: Nearly practical verifiable computation. *Communications of the ACM*, 59(2):103–112, 2016.

[9] David Isaac Wolinsky, Henry Corrigan-Gibbs, Bryan Ford, and Aaron Johnson. Dissent in numbers: Making strong anonymity scale. In *OSDI*, pages 179–182, 2012.

[10] Andrew C Yao. Protocols for secure computations. In *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*, pages 160–164. IEEE, 1982.