Proposal: “A Multiplicative Weights Mechanism for Privacy-Preserving Data Analysis”

Team: Roger Hallman, TBD

Why I chose this paper: Data privacy has been a topic of interest throughout my my career with the Dept. of the Navy. Beyond my early work supporting research on applied homomorphic encryption, I was the Technical Agent for DARPA’s Brandeis Program, a 54-month program which sought to further develop privacy-preserving and privacy enhancing technologies. The ultimate goal of this program was to enable scalable capabilities which would enable the adoption of new technological paradigms (e.g., big data analytics, IoT, etc.) while providing some guarantee of privacy protection for individuals who had data in these systems. Differential privacy, which the paper above builds upon, whas a major focus of the Brandeis ‘Technical Area 1’, which focused on privacy preserving computation. This paper shows what appears to be a successful application of a scheme with which I have some familiarity and falls within an area that I greatly care about.

What will I do with this paper: This paper may be seen as something of a “starting off” point. The final report will summarize the paper according to a number of the guidelines on the class project page (e.g., the main problem addressed and its importance, previous approaches to the problem, main results), however the report will look at at least one stream of research that has been built off of this paper’s results. According to Google Scholar, this paper was published in 2010 and has nearly 300 citations (not the citation count for a groundbreaking paper in the privacy/security field, but very respectable nonetheless); indeed, searching through the citations turns up authors on at least one award which I oversaw. This paper has been routinely cited in the ongoing research of many of the top differential privacy researchers, and I believe that it would be interesting to look at it in the context of how it has contributed that lead to the current state of the art.