CS208 Annotated Bibliography

Spring 2019

1. Background Material
   (a) Discrete math and proofs: Solow [2013], Rosen [2012]
   (b) Algorithms and complexity: Cormen et al. [2009], Mitzenmacher and Upfal [2005]

2. Reidentification Attacks
   (a) (required) Forbes article on Sweeney’s reidentification of Personal Genome Project participants: Tanner [2013]
   (b) (required) New York Times article on reidentification from AOL Search Log release: Barbaro and Zeller [2006]
   (c) (required) Narayanan-Shmatikov opinion piece on the concept of PHI: Narayanan and Shmatikov [2010]
   (d) Sweeney’s original re-identification: Sweeney [1997]
   (e) Statistics on reidentification by DOB, ZIP, and Sex: Sweeney [2000], Golle [2006]
   (f) Paper on the Personal Genome Project reidentification: Sweeney et al. [2013]
   (g) Paper introducing $k$-anonymity: Sweeney [2002]
   (h) Composition attack on $k$-anonymity: Ganta et al. [2008]
   (i) Biases introduced by de-identification of EdX data: Daries et al. [2014]
   (j) Netflix reidentification: Narayanan and Shmatikov [2008]
   (k) Cancellation of 2nd Netflix Challenge after Lawsuit: Singel [2010]

3. Reconstruction Attacks
   (a) (required) Linear programming attack on Diffix: Cohen and Nissim [2018]
   (b) (required) SAT Solver attack on Census data: Garfinkel et al. [2018]
   (c) Survey paper on attacks on aggregate statistics: Dwork et al. [2017, §1.2]
(d) Paper introducing reconstruction attacks: Dinur and Nissim [2003]
(e) Differencing attack on Israeli Census: Ziv [2013]

4. Membership Attacks

(a) (required) P3G Consortium responses to membership attacks on genomic data: Consortium et al. [2009]
(b) (required) Privacy attacks on microtargeted ads: Korolova [2011, §1,4,6,8]
(c) Survey paper on attacks on aggregate statistics: Dwork et al. [2017, §3]
(d) Membership attack on means in genomic data: Homer et al. [2008]
(e) Membership attack on noisy means: Dwork et al. [2015]
(f) Membership attack on ML as a Service: Shokri et al. [2017]
(g) Attribute inference attacks on ML: Fredrikson et al. [2014]
(h) Blog post in response to inference attacks on ML: McSherry [2016]

5. Foundations of Differential Privacy

(a) (extracts required) Primer for non-technical audiences: Wood et al. [2018]
(b) (extracts required) The standard textbook: Dwork and Roth [2013]
(c) Survey on complexity-theoretic aspects of differential privacy: Vadhan [2017]
(d) Attacks on floating-point implementations of differential privacy and remedies: Mironov [2012], Balcer and Vadhan [2018]

References


Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page, and Thomas Ristenpart. Privacy in pharmacogenetics: An end-to-end


