

Review of *Local Private Hypothesis Testing*: χ^2 tests.

May 30, 2018

1 The BibTeX

First, this has the following BibTeX:

```
@ARTICLE{2017arXiv170907155G ,
  author = {{Gaboardi}, M. and {Rogers}, R.},
  title = "{Local Private Hypothesis Testing: Chi-Square Tests}",
  journal = {ArXiv e-prints},
  archivePrefix = "arXiv",
  eprint = {1709.07155},
  primaryClass = "math.ST",
  keywords = {Mathematics - Statistics Theory, Computer Science - Cryptography and Security},
  year = 2017,
  month = sep,
  adsurl = {http://adsabs.harvard.edu/abs/2017arXiv170907155G},
  adsnote = {Provided by the SAO/NASA Astrophysics Data System}
}
```

2 The Paper

We'll try to answer the following questions:

1. *What new background is needed for this article?*

This uses the concept of *concentrated differential privacy*. This is a variant of differential privacy where the “defining inequality” doesn’t hold for *all events*. Recall that for (ϵ, δ) differential privacy, we say that for any two neighboring databases that:

$$\Pr[M(x) \in S] \leq e^\epsilon \Pr[M(y) \in S] + \delta \tag{1}$$

must hold for *all* subsets $S \subseteq \text{Range}(M(x))$.

Concentrated differential privacy instead says that:

$$\mathbb{E}_{y \sim \mathcal{M}(x)}[\exp(t \ln(\frac{\Pr[M(x) = y]}{\Pr[M(y) = y]} - \rho))] \leq e^{t^2 \rho}, \quad \forall t \geq 0 \quad (2)$$

Note that the $\ln \frac{f(x)}{f(y)} - \rho$ quantity is *essentially* the same thing as ϵ in the definition of (ϵ, ρ) differential privacy. If $M(x)$ was (ϵ, ρ) differentially private, we'd have that this inequality is just (bounded by):

$$\mathbb{E}[\exp(t\epsilon)] \leq \exp(t^2 \rho) \quad (3)$$

We can view the Advanced Composition Theorem as a *concentration inequality*, saying that *privacy loss* is concentrated about the mean.

Concentrated Differential privacy makes a *new* (incomparable) definition of differential privacy, with the intent that it satisfies a concentration inequality under composition. The tradeoffs are that in (ϵ, δ) DP, with probability δ privacy loss can be *arbitrarily bad*. Concentrated differential privacy essentially says that the *privacy loss* is small mean, and sub-gaussian.

2. *What new techniques do the authors apply?*
3. *What new results do the authors get?*

They develop a χ^2 test for *local, concentrated* differential privacy. This is the first of its kind (other concentrated differential privacy ones existed,