Errata Slip #2

14th USENIX Symposium on Networked Systems Design and Implementation (NSDI ’17)

In the paper “Prio: Private, Robust, and Scalable Computation of Aggregate Statistics” by Henry Corrigan-Gibbs and Dan Boneh, *Stanford University* (Tuesday session, “Privacy and Security,” pp. 259–282 of the Proceedings) the authors wish to make the following corrections to Section 4.2 of their paper:

- In Step 1 of the protocol, the client must set the constant terms $f(0)$ and $g(0)$ of the polynomials f and g to be values sampled independently and uniformly at random from $\mathbb{F}$. This is necessary for the zero-knowledge property to hold.
- In Step 3a of the protocol, the servers must sample a random point r in the field and test whether $r \cdot (\hat{f}(r)\cdot \hat{g}(r) - \hat{h}(r)) = 0$. This is necessary for the soundness property to hold.

A corrected version of the paper, and the accompanying security analysis, is in the extended version of the paper on arXiv (https://arxiv.org/pdf/1703.06255.pdf).