Dear Editor,

This document lists minor changes made in response to reviews for the manuscript “Impossibility of Efficient Information-Theoretic Fuzzy Extraction.” Below we list the review comments and the response in blue. We also did a copy editing pass. Thank you for all your help and comments.

Benjamin Fuller

[a] I would have liked to see a slightly longer discussion connecting the proposed lower bounds with existing constructions. For example, are the bounds tight in the sense that they match the complexity of existing constructions of information-theoretic fuzzy extractors in the distribution-sensitive setting?

Rewrote start of discussion to say that one can compress current constructions. Added new heading “Avoiding the result”  
  
The two natural directions stemming from this research are 1) can one use natural statistical properties to provide information-theoretic security and 2) can one \emph{compress} inefficient information-theoretic constructions to not require the whole probability distribution of $W\_z$.   
  
[b] Also, the existing lower bound only rules out information-theoretic fuzzy extractors in the distribution-sensitive setting for a constant fraction (concretely, a quarter) of distributions with super-logarithmic fuzzy min-entropy. Are there any implications of this restriction? Are there potentially interesting/useful distributions encountered in practical applications that are not captured by this lower bound? Alternatively, is there an intuitive explanation for why most useful distributions with with super-logarithmic fuzzy min-entropy are already covered by this result?   
  
Edited the first paragraph of the discussion to be the following:   
  
Lemma~\ref{lem:distributional advice suffices} shows the impossibility of efficient constructions for a constant fraction of the family. This means it may be possible to secure all low-entropy distributions of practical interest. However, new designs or analyses are required. One must use statistical properties beyond fuzzy min-entropy. Demarest, Fuller, and Russell~\cite{demarest2021code} provide a summary of statistical properties in addition to fuzzy min-entropy used in low-entropy computationally secure constructions, such as small, random subsets of bits having high entropy. Simhadri et al. provide a discussion on the current state of biometric cryptosystems and their limited security~\cite{simhadri2019cryptographic}. A natural question out of this research is whether one can use similar properties to provide information-theoretic security.   
  
[c] Is there an intuition for why distributions with larger min-entropy could potentially lead to more efficient constructions of information-theoretic fuzzy extractors? While a full-fledged feasibility result is clearly outside the scope of this paper, some more discussion in this regard would be valuable for designing new fuzzy extractors.

Added a sentence on first page of Intro saying:  
  
“This is achieved by writing down the coset of $w$ with respect to an error-correcting code with distance $t$~\cite{dodis2008fuzzy}.”

And paragraph in discussion saying:  
  
We provide some intuition for why high entropy distributions are easier to secure. First, from the construction perspective if the distribution has at $\log{|B\_t|}+\omega(\log \lambda)$ bits of entropy, one can write down enough bits to uniquely determine the original $w$ from a nearby $w'$ without removing all entropy of $w$ (assuming a perfect error correcting code). Second, from an impossibility perspective, impossibility results (both ours and prior results) require the construction to choose $\viable$ points in the construction and have some side information about the distribution to reduce the size of this set. The larger the support of the distribution the harder it is for this side information to reduce the entropy of this set. For example, Fuller, Reyzin, and Smith~\cite{fuller2020fuzzy} distributions, $W\in\mathcal{W}^{FRS}$, were lines that overlapped at one point, upper bounding their size.  
  
[d] Finally, from a more technical point of view, I did not gain a lot of insight into why the lower bounds for fuzzy extractors cannot tolerate errors while those for secure sketches can. A brief discussion would be helpful.

Added a paragraph in discussion called “Perfect Correctness”:  
  
Our result for fuzzy extractors considers perfect correctness. We do not think this is a fundamental limitation but we briefly explain the issue. As mentioned above, in the case of perfect correctness, one includes a point $w$ in $\viable\_{r,p}$ if it is distance $t$ from any point that produces a different $r'$. Once one allows imperfect correctness, there is no immediate test for whether a point $w$ should be considered viable. It seems possible that one could argue for a point to be viable when most points around $w$ produce the same key. We were not able to apply the isoperimetric inequality in this setting. If one finds a clean argument for viable points with imperfect correctness, it directly replaces Lemma~\ref{lem:smallgeneralviable}. The rest of our argument then applies. On the other hand, for a secure sketch, one can easily bound the size of the set of points \[ \left\{w \middle | \frac{\{w' |\rec(w', p) = w \wedge \dis(w, w')\}}{\{w' | \dis(w, w')\}}\ge 1-\delta \right\},\] this set forms a Shannon error correcting code. This is the viable set in the secure sketch case.  
  
  
Some typos (this is a non-exhaustive list; please proof-edit to fix similar issues):  
  
1. Pg-12: it suffices to show ... (Definition 8) for the family W\_{n,k,t,\gamma} -->  for the family W\_{n,k} (should refer to the family of uniform distributions)

This is correct as written. We show impossibility for a constant fraction of the family based on impossibility of securing the family with distributional advice.   
  
2. Pg-12: few elements in Z\_{n,k} that are not in Z\_{n,k,t,\gamma} --> few elements in Z\_{n,k} are not in Z\_{n,k,t,\gamma}  
  
Corrected.

Reviewer #2: This paper presents theoretical foundings about information-theoretic fuzzy extractors, which is, any distribution-sensitive information-theoretic fuzzy extractor requires an exponential amount of information about the distribution. Generally, it makes sense and the proof is correct.  
Besides, there are some mistakes in the paper:  
1, in page 5, line 44, it says: "with three properties". But below there are only two properties.  
2, in page 30, there are errors in reference [32].

Both corrected.