Harvard Privacy Tools Project

Randomness and Noise

Christian Covington

April 2, 2020

1 Overview

This document describes the strategies the library uses for generation of randomness and noise. I believe there will need to be ongoing discussions about how best to perform randomized computations in the library, as properly doing so is more complicated in practice than in theory.

2 Source of Randomness

All of our random number generation involves uniform random sampling of bits via OpenSSL. We will take as given that OpenSSL is cryptographically secure.

3 Preliminaries

Definition 1. *Differential Privacy [DMNS06]*
For $\epsilon, \delta \geq 0$, a randomized mechanism $\mathcal{M} : \mathcal{X}^n \times \mathcal{Q} \to \mathcal{Y}$ is (ϵ, δ)-DP if, for every pair of neighboring data sets $X, X' \in \mathcal{X}^n$ and every query $q \in \mathcal{Q}$ we have

$$\forall \mathcal{T} \subseteq \mathcal{Y} : \Pr[\mathcal{M}(X, \epsilon, \delta, q) \in \mathcal{T}] \leq e^{\epsilon} \Pr[\mathcal{M}(X', \epsilon, \delta, q) \in \mathcal{T}] + \delta.$$

If $\delta = 0$, we call this *Pure DP*. If $\delta > 0$, we call this *Approximate DP*. Note that, in practice, differential privacy could be thought of a bit more broadly – as a bounded distance between joint distributions over the mechanism output and runtime.[1] We will focus mostly on the distribution over mechanism output, as this is really the core idea of DP, but will touch on runtime when it seems appropriate.

[1] Conceivably, this idea could be extended further to talk about distributions over all quantities related in any way to the underlying data. For example, imagine that the US government uses $\epsilon = 1$ if the President is in the data and $\epsilon = 10$ if not – if anyone knew about this rule, the choice of epsilon would leak information not accounted for in the traditional definition of DP. We will focus only on mechanism output and runtime, as they seem to be by far the most plausible channels of information leakage.

Theorem 1. *Post-Processing*
Let $f : \mathcal{Y} \to \mathcal{Y}'$ be an arbitrary mapping independent of the data set X and $\mathcal{M}$ be an (ϵ, δ)-DP mechanism. Then $f \circ \mathcal{M}$ is also (ϵ, δ)-DP.

Proof. This is a well-known result – see Proposition 2.1 on pg. 19 of [DR+14] for a proof. □

Definition 2. *Exact Rounding*
Let $S \subset \mathbb{R}$ be some set. Let $\phi : \mathbb{R}^n \to \mathbb{R}$ be a function on the reals and $\phi' : S^n \to S$ be its implementation over S. Then, ϕ' respects exact rounding *for (ϕ, S) if*

$$\forall s \in S : \phi'(s) = round_S[\phi(s)],$$

where $round_S(\cdot)$ rounds a real number to a member of S according to some rounding rule.

For our purposes, we will care only about the case where $S = \mathbb{F}$, the set of IEEE-754 floating-point numbers. We may occasionally use a different definition of S for ease of reasoning about a proof, or refer to $\mathbb{F}$ specifically to more clearly contextualize what we are trying to do. Additionally, our rounding rule will typically be that we want to round our real number r to the $s \in S$ that minimizes $|r - s|$.

Corollary 1. *Exact Rounding as Post-Processing*
Let $\mathcal{M} : \mathbb{R}^n \times \mathcal{Q} \to \mathbb{R}$ be (ϵ, δ)-DP and $\mathcal{M}' : S^n \times \mathcal{Q} \to S$ be an implementation over S. If $\mathcal{M}'$ respects exact rounding for $(\mathcal{M}, S)$, then $\mathcal{M}'$ is (ϵ, δ)-DP.

Proof. $\mathcal{M}'$ can be viewed as a function that takes real-valued outputs from $\mathcal{M}$ and rounds them to an element of S according to a rounding rule. This is post-processing independent of the data X, and so the corollary follows directly from Theorem 1. □

Theorem 2. *Non-composability of Exact Rounding*
Let ϕ, η be functions on $\mathbb{R}$ and ϕ', η' be versions of ϕ, η that respect exact rounding with respect to some $S \subset \mathbb{R}$. Then, $\phi' \circ \eta'$ does not necessarily respect exact rounding with respect to S.

Proof. For ease of proof, we assume WLOG that $S = \mathbb{Z}$. Now, let $\phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be such that $\phi(a, b) = a + b$ and $\eta : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be such that $\eta(a, b) = a/b$. Let's examine the behavior of $\phi \circ \eta$ on a certain set of inputs:

$$\begin{aligned} \phi\left(\eta(3,2), \eta(6,5)\right) &= \phi\left(3/2, 6/5\right) \\ &= 27/10. \end{aligned}$$

Note that, for these inputs, exact rounding of $\phi \circ \eta$ with respect to $\mathbb{Z}$ would yield an output of 3.

We now consider $\phi' \circ \eta'$, where $\phi' : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ and $\eta' : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ each respects exact rounding with respect to $\mathbb{Z}$.

$$\begin{aligned} \phi'\left(\eta'(3,2), \eta'(6,5)\right) &= \phi'\left(1, 1\right) \\ &= 2. \end{aligned}$$

$2 \neq 3$, so we have our proof. □

The non-composability of exact rounding means that translating DP algorithms from $\mathbb{R}$ to $\mathbb{F}$ is not as easy as combining individual steps that respect exact rounding, as doing so does not imply that the mechanism as a whole respects exact rounding. In the next section, we will propose a weaker sufficient condition for DP on $\mathbb{F}$.

Definition 3. *Additive Noise Mechanism*
A differentially private mechanism $\mathcal{M}$ is an additive noise mechanism *if it is of the form*

$$\mathcal{M}(X, \phi) = \phi(X) + n,$$

where n is a draw from a noise distribution N.

Definition 4. *Truncation and Censoring*
Throughout our noise functions, we use the terms "truncated" and "censored". Both are means of bounding the support of the noise distribution, but they are distinct.

Truncating a distribution simply ignores events outside of the given bounds, so all probabilities within the given bounds are scaled up by a constant factor. One way to generate a truncated distribution is via rejection sampling. You can generate samples from a probability distribution as you normally would (without any bounding), and reject any sample that falls outside of your bounds.

Censoring a distribution, rather than ignoring events outside of the given bounds, pushes the probabilities of said events to the closest event within the given bounds. One way to generate a censored distribution would be to generate samples from a probability distribution as you typically would, and then clamp samples that fall outside of your bounds to the closest element inside your bounds.

4 Current Random Number Generation

We have a set of fairly standard procedures for generating draws from various noise distributions.

4.0.1 $sample\_uniform(min : f64, max : f64)$

Update

We have moved to uniform sampling from MPFR – updated notes for this section are on the develop branch.

In this method, we start by generating a floating-point number in $[0, 1)$, where each is generated with probability relative to its unit of least precision (ULP).[2] That is, we generate $x \in [2^{-i}, 2^{-i+1})$ with probability $\frac{1}{2^i}$ for all $i \in \{1, 2, \ldots, 1022\}$ and $x \in [0, 2^{-1022})$ for $i = 1023$.
Within each precision band (the set of numbers with the same unit of least precision), numbers are sampled uniformly. We achieve this sample our exponent from a geometric distribution with parameter $p = 0.5$ and a mantissa uniformly from $\{0, 1\}^{52}$. Let e be a draw from $Geom(0.5)$ (truncated such that $e \in \{1, 2, \ldots, 1023\}$) and $m_1, m_2 \ldots, m_{52}$ be the bits of our mantissa. At the end, we will scale our output from $[0, 1)$ to be instead in $[min, max)$. Then our function outputs u, where

$$u = (1.m_1 m_2 \ldots m_{52})_2 * 2^{-e} * (max - min) + min.$$

This method was proposed in [Mir12] as a component of a larger attempt to create a version of the Laplace mechanism that is not susceptible to floating-point attacks.[3] There is

[2] The ULP is the value represented by the least significant bit of the mantissa if that bit is a 1.
[3] Note that the original method generates values $\in [0, 1)$ rather than arbitrary $[min, max)$.

no universally agreed upon method for generating uniform random numbers (for privacy applications or otherwise), but this method seems to approximate the real numbers better than many other common methods because of the sampling relative to the ULP.

Known Privacy Issues

When $i = 1023$ we are sampling from subnormal floating-point numbers. Because processors do not typically support subnormals natively, they take much longer to sample and open us up to an easier timing attack, as seen in [AKM+15]. Protecting against timing attacks is mostly seen as out of scope for now, but I wanted to bring this up anyway.

We are incurring some floating-point error when converting from $[0, 1)$ to $[min, max)$ which could jeopardize privacy guarantees in ways that are difficult to reason about.[Mir12] [Ilv19]

4.1 Biased Bit Sampling

Recall that we are taking as given that we are able to sample uniform bits from OpenSSL. For many applications, however, we want to be able to sample bits non-uniformly, i.e. where $\Pr(bit = 1) \neq \frac{1}{2}$. To do so, we use the $sample\_bit$ function.

4.1.1 $sample\_bit(prob : f64)$

This function uses the unbiased bit generation from OpenSSL to return a single bit, where $\Pr(bit = 1) = prob$. I was introduced to the method for biasing an unbiased coin from a homework assignment given by Michael Mitzenmacher, and I later found a write-up online here. We will give a general form of the algorithm, and then talk about implementation details.

Algorithm 1 Biasing an unbiased coin

1: $p \leftarrow \Pr(bit = 1)$
2: Find the infinite binary expansion of p, which we call $b = (b_1, b_2, \ldots,)_2$. Note that $p = \sum_{i=1}^{\infty} \frac{b_i}{2^i}$.
3: Toss an unbiased coin until the first instance of "heads". Call the (1-based) index where this occurred k.
4: return b_k

Let's first show that this procedure gives the correct expectation:

$$\begin{aligned} p &= \Pr(bit = 1) \\ &= \sum_{i=1}^{\infty} \Pr(bit = 1 | k = i) \Pr(k = i) \\ &= \sum_{i=1}^{\infty} b_i \cdot \frac{1}{2^i} \\ &= \sum_{i=1}^{\infty} \frac{b_i}{2^i}. \end{aligned}$$

This is consistent with the statement in Algorithm 1, so we know that the process returns bits with the correct bias. In terms of efficiency, we know that we can stop coin flipping once we get a heads, so that part of the algorithm has $\mathbb{E}(\#flips) = 2$.

The part that is a bit more difficult is constructing the infinite binary expansion of p. We start by noting that, for our purposes, we do not actually need an infinite binary expansion. Because p will always be a 64-bit floating-point number, we need only get a binary expansion that covers all representable numbers in our floating-point standard that are also valid probabilities. Luckily, the underlying structure of floating-point numbers makes this quite easy.

In the 64-bit standard, floating-point numbers are represented as

$$(-1)^s(1.m_1m_2\dots m_{52})_2 * 2^{(e_1e_2\dots e_{11})_2-1023},$$

where s is a sign bit we ignore for our purposes. Our binary expansion is just the mantissa $(1.m_1m_2\dots m_{52})_2$, with the radix point shifted based on the value of the exponent. We can then index into the properly shifted mantissa and check the value of the kth element.

4.2 Other Continuous Distributions

In general, we can generate draws from non-uniform continuous distributions (e.g. Gaussian and Laplace) by using inverse transform sampling. To draw from a distribution f with CDF F, we sample u from $Unif[0, 1)$ and return $F^{-1}(u)$.

Known Privacy Issues

Carrying out the inverse probability transform employs floating-point arithmetic, so we run into the same problems as were described in the uniform sampling section. This is potentially a very significant problem, and one for which we do not currently have a good solution.

Because of the vulnerabilities inherent in using floating-point arithmetic, we would like to avoid using inverse transform sampling when possible.

4.3 Geometric Distribution

The Geometric is one such case where we can generate a distribution without inverse transform sampling. To generate a $Geom(p)$, we can use our *sample_bit* function to repeatedly sample random bits where $\Pr(bit = 1) = p$. We then return the number of samples it takes to get our first 1. This method is not susceptible to attacks based on floating-point vulnerabilities, as it operates only over the integers.

5 Sufficient Conditions for DP in Practice

Given the existence of the aforementioned floating-point vulnerabilities in standard mechanism implementations, we would like to explore ways to potentially ensure that implementations actually respect DP in practice. This section is very experimental/preliminary.

Disclaimer

I think at least one of the statements below is wrong – going to think about it more later.

5.1 Introduction to MPFR

The GNU MPFR Library[FHL+07] is a C library with methods for carrying out a number of floating-point operations with *exact rounding*. MPFR has methods for, among other things, performing basic arithmetic operations and generating samples from basic noise distributions.

5.2 Additive Noise Mechanisms

Let ϕ be a function we would like to privatize at the (ϵ, δ) level, with sensitivity Δ_ϕ.[4]

Let's start by considering the generation of noise according to some distribution $N_{\epsilon,\delta,\Delta_\phi}$, which for ease of notation we will call N. For our theoretical proofs of many common mechanisms we assume that $supp(N) = \mathbb{R}$, but in practice $supp(N) = \mathbb{F}$. It is well-established that privacy properties of noise distributions defined on $\mathbb{R}$ do not necessarily hold on $\mathbb{F}$. See [Mir12] and [Ilv19] for vulnerabilities of the Laplace and Exponential mechanisms, respectively, and [GMP16] for a more general treatment.

Theorem 3. *Valid Noise for Additive Noise Mechanisms on* $\mathbb{R}$
A noise distribution N *with* $supp(N) = \mathbb{R}$ *can be used as the noising portion of an additive noise mechanism to privatize* ϕ *if* $\forall \mathcal{T} \subseteq supp(N)$

$$\frac{\Pr(N \in \mathcal{T})}{\Pr(N \in \mathcal{T} - \Delta_\phi)} \leq e^\epsilon + \delta$$

and

$$\frac{\Pr(N \in \mathcal{T})}{\Pr(N \in \mathcal{T} + \Delta_\phi)} \leq e^\epsilon + \delta,$$

where $\mathcal{T} \pm \Delta_\phi = \{t \pm \Delta_\phi | t \in \mathcal{T}\}$.

Proof. This follows directly from Theorem 1. $\mathcal{M}(X, \epsilon, \delta, q) = \phi(X) + N$ (and likewise for X'), and we can just ignore the $\phi(X), \phi(X')$ terms because the relationship between $\mathcal{M}(X, \epsilon, \delta, q)$ and $\mathcal{M}(X', \epsilon, \delta, q)$ does not change if you shift both by the same factor. The $\pm\Delta_\phi$ terms are standing in for the notion of neighboring data sets. □

Corollary 2. *Valid Noise for Additive Noise Mechanisms on* $\mathbb{F}$
Let N *be a valid noise distribution with* $supp(N) = \mathbb{R}$ *as described in Theorem 3 and* N' *be an implementation of* N *that respects exact rounding with respect to* $\mathbb{F}$. *Then* N' *is valid to be used in an additive noise mechanism on* $\mathbb{F}$.

Proof. First, notice that in Theorem 3, we have effectively made the claim that if some property holds for an additive noise mechanism, it holds for the distribution of noise. Now, our result follows from Corollary 1. □

[4] This is the maximum the output of the function can differ, in terms of some distance metric, when evaluated on neighboring data sets.

Theorem 4. *Additive Noise Mechanisms on* $\mathbb{F}$
Let $\mathcal{M}(X, \epsilon, \delta, q) = \phi(X) + N$ *be an* (ϵ, δ)*-DP additive noise mechanism defined on* $\mathbb{R}$*. Let* ϕ' *be the floating-point implementation of* ϕ*,* N' *be a valid (in the sense of Corollary 2) implementation of* N *on* $\mathbb{F}$*, and* $\mathcal{M}'(X, \epsilon, \delta, q) = \phi'(X) + N'$ *respect exact rounding for* $(\phi'(X) + N', \mathbb{F})$*. Then,* $\mathcal{M}'(X, \epsilon, \delta, q)$ *respects* (ϵ, δ)*-DP.*

Proof. We know that N' is a valid noise distribution, i.e. that it has the property (bounded distance at intervals of Δ_ϕ) we need for an additive noise mechanism. So if we imagine an idealized notion of a function $\phi'(X) + N'$ with outputs in $\mathbb{R}$, this function would be (ϵ, δ)-DP because we know that $\phi(X) + N$ is (ϵ, δ)-DP. Our mechanism $\mathcal{M}'(\cdot)$ respects exact rounding for $(\phi'(X) + N', \mathbb{F})$, and so $\mathcal{M}'(\cdot)$ is (ϵ, δ)-DP by Corollary 1. □

The upshot of Theorem 4 is that the floating-point implementation of an additive noise mechanism is DP if both the noise generation and addition steps can be performed with exact rounding relative to $\mathbb{F}$.

References

[AKM+15] Marc Andrysco, David Kohlbrenner, Keaton Mowery, Ranjit Jhala, Sorin Lerner, and Hovav Shacham. On subnormal floating point and abnormal timing. In *2015 IEEE Symposium on Security and Privacy*, pages 623–639. IEEE, 2015.

[DMNS06] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pages 265–284. Springer, 2006.

[DR+14] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.

[FHL+07] Laurent Fousse, Guillaume Hanrot, Vincent Lefèvre, Patrick Pélissier, and Paul Zimmermann. Mpfr: A multiple-precision binary floating-point library with correct rounding. *ACM Trans. Math. Softw.*, 33(2):13–es, June 2007.

[GMP16] Ivan Gazeau, Dale Miller, and Catuscia Palamidessi. Preserving differential privacy under finite-precision semantics. *Theor. Comput. Sci.*, 655:92–108, 2016.

[Ilv19] Christina Ilvento. Implementing the exponential mechanism with base-2 differential privacy, 2019.

[Mir12] Ilya Mironov. On significance of the least significant bits for differential privacy. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 650–661, 2012.