Verifying Snapping Mechanism - Floating Point Implementation Version

Jiawen Liu

February 21, 2020

In order to verify the differential privacy property of an implementation of the snapping mechanism [5], we follow the logic rules designed from [1] and the floating point error semantics from [7, 4, 2, 6].

1 Preliminary Definitions

Definition 1 (Laplace mechanism [3])
Let $\epsilon > 0$. The Laplace mechanism $\mathcal{L}_\epsilon$: $\mathbb{R} \to \mathsf{Distr}(\mathbb{R})$ is defined by $\mathcal{L}(t) = t + v$, where $v \in \mathbb{R}$ is drawn from the Laplace distribution $\mathsf{laplce}(\frac{1}{\epsilon})$.

2 Syntax

Following are the syntax of the system. The circled operators are rounded operation in floating point computation.

$$
\begin{array}{llcl}
\text{Floating Point Expr.} & e_{\mathbb{F}} & ::= & c \mid x \mid f(x) \mid e_{\mathbb{F}} \circledast e_{\mathbb{F}} \mid \textcircled{\ln}(e_{\mathbb{F}}) \mid x \xleftarrow{\$} \mu \\
\text{Real Expr.} & e_{\mathbb{R}} & ::= & r \mid X \mid F(X) \mid e_{\mathbb{R}} * e_{\mathbb{R}} \mid \ln(e_{\mathbb{R}}) \mid X \xleftarrow{\$} \mu \\
\text{Arithmetic Operation} & * & ::= & + \mid - \mid \times \mid \div \\
\text{Value} & v & ::= & r \mid c \\
\text{Distribution} & \mu & ::= & \mathsf{laplce} \mid \mathsf{unif} \mid \mathtt{bernoulli} \\
\text{Error} & err & ::= & (e_{\mathbb{R}}, e_{\mathbb{R}})
\end{array}
$$

We use upper case for variables in real computation and lower case for variables in floating point computation. $\circledast$ represents the operation in floating point machine.

$F(X)$ denotes function F evaluates to value $F(X)$ given input X in real computation, and $f(x)$ denotes the same function F evaluates to value $f(x)$ given the same input x in floating point computation.

3 Semantics

The big step semantics with relative floating point computation error are shown in Figure. 1. The semantics are $e_{\mathbb{R}} \Downarrow e_{\mathbb{F}}, err$, which means a real world expression $e_{\mathbb{R}}$ can be represented in floating point computation $e_{\mathbb{F}}$ with error bound err. The η is the machine epsilon.

$$\frac{c = \mathtt{fl}(r)}{r \Downarrow c, \big(\frac{r}{(1+\eta)}, r(1+\eta)\big)}\ \textsc{const} \qquad \frac{e^1_{\mathbb{R}} \Downarrow e^1_{\mathbb{F}}, (\underline{e}^1_{\mathbb{R}}, \bar{e}^1_{\mathbb{R}}) \qquad e^2_{\mathbb{R}} \Downarrow e^2_{\mathbb{F}}, (\underline{e}^2_{\mathbb{R}}, \bar{e}^2_{\mathbb{R}})}{e^1_{\mathbb{R}} * e^2_{\mathbb{R}} \Downarrow \mathtt{fl}(e^1_{\mathbb{F}} \circledast e^2_{\mathbb{F}}), \big((\frac{\underline{e}^1_{\mathbb{R}} * \underline{e}^2_{\mathbb{R}})}{(1+\eta)}, (\bar{e}^1_{\mathbb{R}} * \bar{e}^2_{\mathbb{R}})(1+\eta)\big)}\ \textsc{op}$$

$$\frac{e_{\mathbb{R}} \Downarrow e_{\mathbb{F}}, (\underline{e}_{\mathbb{R}}, \bar{e}_{\mathbb{R}}) \qquad e_{\mathbb{R}} \geq 1}{\ln(e_{\mathbb{R}}) \Downarrow \textcircled{ln}(e_{\mathbb{F}}), \big((\frac{\textcircled{ln}(\underline{e}_{\mathbb{R}})}{(1+\eta)}, (\ln(\bar{e}_{\mathbb{R}}))(1+\eta)\big)}\ \textsc{ln} \qquad \frac{e_{\mathbb{R}} \Downarrow e_{\mathbb{F}}, (\underline{e}_{\mathbb{R}}, \bar{e}_{\mathbb{R}}) \qquad e_{\mathbb{R}} < 1}{\ln(e_{\mathbb{R}}) \Downarrow \textcircled{ln}(e_{\mathbb{F}}), \big((\ln(\underline{e}_{\mathbb{R}}))(1+\eta), \frac{\textcircled{ln}(\bar{e}_{\mathbb{R}})}{(1+\eta)}\big)}\ \textsc{ln-op}$$

Figure 1: Semantics with Relative Floating Point Error

Theorem 1 (Soundness Theorem)
Given $e_{\mathbb{R}}$ and $e_{\mathbb{F}}$ where $e_{\mathbb{R}} \Downarrow e_{\mathbb{F}}, err$, when evaluating the $e_{\mathbb{F}}$ in floating point computation and get the value c, we have $c \in err$.

4 Snapping Mechanism

Definition 2 ($\mathsf{Snap}_{\mathbb{R}}(a) : A \to \mathsf{Distr}(\mathbb{R})$)
Given privacy parameter ϵ, the ideal Snapping mechanism $\mathsf{Snap}_{\mathbb{R}}(a)$ is defined as:

$$U \xleftarrow{\$} \mu; S \xleftarrow{\$} \{-1, 1\}; Y = \ln(U) \div \epsilon; Z = S \times Y; X = F(a); W = X + Z; W' = \lfloor W \rceil_{\Lambda}; R = \mathsf{clamp}_B(W')$$

where f is the query function over input $a \in A$, ϵ is the privacy budget, B is the clamping bound and Λ is the rounding argument satisfying $\lambda = 2^k$ where 2^k is the smallest power of 2 greater or equal to the $\frac{1}{\epsilon}$.

Let $\mathsf{Snap}'_{\mathbb{R}}(a, U, S)$ be the same as $\mathsf{Snap}_{\mathbb{F}}(a)$ given U, S without rounding and clamping steps.

Definition 3 ($\mathsf{Snap}_{\mathbb{F}}(a) : A \to \mathsf{Distr}(\mathbb{R})$)
Given privacy parameter ϵ, the floating point implemented Snapping mechanism $\mathsf{Snap}_{\mathbb{F}}(a)$ is defined as (where all parameters are defined the same as above):

$$u_{\mathbb{F}} \xleftarrow{\$} \mu; s_{\mathbb{F}} \xleftarrow{\$} \{-1, 1\}; y = \textcircled{ln}(u) \oslash \epsilon; z = s \otimes y; x = f(a); w = x \oplus z; w' = \lfloor w \rceil_{\Lambda}; r = \mathsf{clamp}_B(w')$$

Let $\mathsf{Snap}'_{\mathbb{F}}(a, u, s)$ be the same as $\mathsf{Snap}_{\mathbb{F}}(a)$ without rounding and clamping precesses given u, s.

5 Main Theorem

Theorem 2 (The Snap mechanism is $\epsilon-$differentially private)
Consider $\mathsf{Snap}(a)$ defined as before, if $\mathsf{Snap}(a) = x$ given database a and privacy parameter ϵ, then its actual privacy loss is bounded by $\epsilon + 12x\epsilon\eta + 2\eta$

Proof. Given $\mathsf{Snap}_{\mathbb{F}}(a) = x$ and parameter ϵ, we consider a' be the adjacent database of a satisfying $|f(a) - f(a')| \leq 1$. Without loss of generalization, we assume $f(a) + 1 = f(a')$ ($\diamond$). The proof is developed by cases of the output of $\mathsf{Snap}_{\mathbb{F}}(a)$ mechanism.

Consider the $\mathsf{Snap}_{\mathbb{R}}(a)$ outputting the same result x, let (L, R) be the range where $\forall\, u \in (L, R)$ and some s, $\mathsf{Snap}'_{\mathbb{R}}(a, u, s) = x$, we have $\Pr[\mathsf{Snap}_{\mathbb{R}}(a)] = R - L$. Given the $\mathsf{Snap}_{\mathbb{R}}$ is $\epsilon-$dp, we have:

$$e^{-\epsilon} \leq \frac{\Pr[\mathsf{Snap}_{\mathbb{R}}(a)]}{\Pr[\mathsf{Snap}_{\mathbb{R}}(a)]} = \frac{R - L}{R' - L'} \leq e^{\epsilon}$$

Let (l, r) be the range where $\forall\, u \in (l, r)$ and some s, $\mathsf{Snap}'_{\mathbb{F}}(a, u, s) = x$, we estimated the $|r - l|$ in terms of floating point relative error and $|R - L|$ through our semantics in order to verify the privacy loss of $\mathsf{Snap}_{\mathbb{F}}$.

case $\boldsymbol{x = -B}$

Let b be the largest number rounded by Λ that is smaller than B. We know $s = 1$, $L = l = 0$ and $R = -b$, so we only need to estimate the right side range r in this case. The derivation of this case given $\mathsf{Snap}'_{\mathbb{F}}(a, R, 1) = \mathsf{Snap}'_{\mathbb{F}}(a', R, 1) = x$ is shown as following:

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{R \Downarrow r, (\underline{R}, \bar{R})}\;\text{LN}}{\ln(R) \Downarrow \textcircled{\scriptsize ln}(r), (\ln(\underline{R})(1+\eta), \dfrac{\ln(\bar{R})}{(1+\eta)})}\;\text{OP}}{\dfrac{1}{\epsilon} \times \ln(R) \Downarrow \dfrac{1}{\epsilon} \otimes \textcircled{\scriptsize ln}(r), ((\dfrac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2, \dfrac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})}\;\text{OP}}{f(a) + \dfrac{1}{\epsilon} \times \ln(R) \Downarrow f(a) \oplus \dfrac{1}{\epsilon} \otimes \textcircled{\scriptsize ln}(r), \Big(\big(f(a) + (\dfrac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2\big)(1+\eta), \dfrac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})}{(1+\eta)}\Big)}\;\text{ID}}{\mathsf{Snap}'_{\mathbb{R}}(a, R, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, r, 1), \Big(\big(f(a) + (\dfrac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2\big)(1+\eta), \dfrac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})}{(1+\eta)}\Big)}$$

In the same way, we have the derivation for $\mathsf{Snap}'_{\mathbb{F}}(a', r, 1)$:

$$\dfrac{\cdots}{\mathsf{Snap}'_{\mathbb{R}}(a', R', 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a', r, 1), \Big(\big(f(a') + (\dfrac{1}{\epsilon} \times \ln(\underline{R}'))(1+\eta)^2\big)(1+\eta), \dfrac{(f(a') + \frac{\frac{1}{\epsilon} \times \ln(\bar{R}')}{(1+\eta)^2})}{(1+\eta)}\Big)}$$

Given $\mathsf{Snap}_{\mathbb{F}}(a) = \mathsf{Snap}_{\mathbb{F}}(a') = x = -b$, we have following values for $\underline{R}, \bar{R}, \underline{R}'$ and $\bar{R}'$:

$$\underline{R} = e^{\epsilon\left((x(1+\eta) - f(a))(1+\eta)^2)\right)}, \bar{R} = e^{\epsilon \frac{(\frac{x}{1+\eta} - f(a))}{(1+\eta)^2}}$$
$$\underline{R}' = e^{\epsilon\left((x(1+\eta) - f(a'))(1+\eta)^2\right)}, \bar{R}' = e^{\epsilon(\frac{(\frac{x}{1+\eta} - f(a'))}{(1+\eta)^2})}$$

The privacy loss of $\mathsf{Snap}_{\mathbb{F}}(a)$ in this case is bounded by:

$$\begin{aligned} \frac{\frac{1}{2}(\bar{R} - 0)}{\frac{1}{2}(\underline{R}' - 0)} \quad &= e^{\epsilon\left(\frac{(\frac{x}{1+\eta} - f(a))}{(1+\eta)^2} - \left((x(1+\eta) - f(a'))(1+\eta)^2\right)\right)} \\ &= e^{\epsilon\left(\frac{x}{(1+\eta)^3} - \frac{f(a)}{(1+\eta)^2} - x(1+\eta)^3 + f(a')(1+\eta)^2\right)} \quad (\star) \end{aligned}$$

Since $(1+\eta)^3 > 1+3\eta$, $\frac{1}{(1+\eta)^3} < \frac{1}{1+3\eta}$, $(1+\eta)^2 < 1+2.1\eta$ and $\frac{1}{(1+\eta)^2} > 1-2\eta$, we have:

$$\begin{aligned}(\star) \quad &< e^{\epsilon\left(-\frac{9\eta+6}{1+3\eta}x+4.1\eta f(a)+(1+2.1\eta)\right)}\\ &< e^{\epsilon(10.1\eta B+1+2.1\eta)}\end{aligned}$$

case $\boldsymbol{x \in (-B, \lfloor f(a) \rceil_\Lambda)}$

subcase $\boldsymbol{\lfloor f(a) \rceil_\Lambda \le 0 \lor \left(\lfloor f(a) \rceil_\Lambda > 0 \land x \in (-B, 0)\right)}$

Let $y_1 = x - (\frac{\Lambda}{2})$, $y_2 = x + (\frac{\Lambda}{2})$, we know $y_1 < 0$, $y_2 < 0$, $S = s = 1$, $L = e^{\epsilon(y_1 - f(a))}$ and $R = e^{\epsilon(y_2 - f(a))}$ in this case. The derivations of estimating l and r are shown as following:

$$\dfrac{\dfrac{\dfrac{\dfrac{R \Downarrow r, (\underline{R}, \bar{R})}{\ln(R) \Downarrow ⓛⓝ(r), (\ln(\underline{R})(1+\eta), \dfrac{\ln(\bar{R})}{(1+\eta)})}\ \text{LN}}{\dfrac{1}{\epsilon} \times \ln(R) \Downarrow \dfrac{1}{\epsilon} \otimes ⓛⓝ(r), ((\dfrac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2, \dfrac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})}\ \text{OP}}{f(a) + \dfrac{1}{\epsilon} \times \ln(R) \Downarrow f(a) \oplus \dfrac{1}{\epsilon} \otimes ⓛⓝ(r), \left(\left(f(a) + (\dfrac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2\right)(1+\eta), \dfrac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})}{(1+\eta)}\right)}\ \text{OP}}{\mathsf{Snap}'_{\mathbb{R}}(a, R, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, r, 1), (err_1, err_2)}\ \text{ID}$$

From soundness theorem, we have $err_1 \le y_2 \le err_2$.
Taking the lower bound, we have: $\underline{R} = e^{\epsilon\left((y_1(1+\eta) - f(a))(1+\eta)^2)\right)}$.
Taking the upper bound, we have: $\bar{R} = e^{\epsilon \frac{(\frac{y_1}{1+\eta} - f(a))}{(1+\eta)^2}}$.

$$\dfrac{\dfrac{\cdots}{\mathsf{Snap}'_{\mathbb{R}}(a, L, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, l, 1), (\dfrac{f(a) + (\frac{1}{\epsilon} \times \ln(\underline{L}))(1+\eta)^2}{1+\eta}, (f(a) + \dfrac{\frac{1}{\epsilon} \times \ln(\bar{L})}{(1+\eta)^2})(1+\eta))}}{\mathsf{Snap}'_{\mathbb{R}}(a, L, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, l, 1), (err_1, err_2)}$$

From soundness theorem, we have $err_1 \le y_2 \le err_2$.
Taking the lower bound , we have: $\underline{L} = e^{\epsilon\left((y_2(1+\eta) - f(a))(1+\eta)^2)\right)}$.
Taking the upper bound, we have: $\bar{L} = e^{\epsilon \frac{(\frac{y_2}{1+\eta} - f(a))}{(1+\eta)^2}}$.
In the same way, we have the bound of l, r for adjacent data set a':

$$\underline{R}' = e^{\epsilon\left((y_1(1+\eta) - f(a'))(1+\eta)^2)\right)},\ \bar{R}' = e^{\epsilon \frac{(\frac{y_1}{1+\eta} - f(a'))}{(1+\eta)^2}}.$$

$$\underline{L}' = e^{\epsilon\left((y_2(1+\eta) - f(a'))(1+\eta)^2)\right)},\ \bar{L}' = e^{\epsilon \frac{(\frac{y_2}{1+\eta} - f(a'))}{(1+\eta)^2}}$$

Then, we have the privacy loss is bounded by:

$$\frac{|\bar{R}-\underline{L}|}{|\underline{R}'-\bar{L}'|}.$$

We also have:

$$\begin{array}{ll} \frac{\bar{R}}{R} & = e^{\epsilon\left(\frac{y_1}{(1+\eta)^3}-\frac{f(a)}{(1+\eta)^2}-y_1+f(a)\right)} \leq e^{\epsilon\left(-\frac{3\eta}{1+3\eta}y_1+2\eta f(a)\right)} \leq e^{\epsilon\left(\frac{3\eta}{1+3\eta}B+2\eta B\right)} \leq e^{5\epsilon B\eta} \\ \frac{\underline{L}}{L} & = e^{\epsilon\left(y_2(1+\eta)^3-f(a)(1+\eta)^2-y_2+f(a)\right)} \geq e^{\epsilon\left(3\eta y_1-2\eta f(a)\right)} \geq e^{-5\epsilon B\eta} \end{array}$$

Then, we can derive:

$$\begin{array}{ll} |\bar{R}-\underline{L}| & \leq e^{5\epsilon B\eta}R-e^{-5\epsilon B\eta}L \\ & = L\left(e^{\Lambda\epsilon+5\epsilon B\eta}-e^{-5\epsilon B\eta}\right) \\ & = L\left(e^{\Lambda\epsilon}e^{5\epsilon B\eta}-e^{5\epsilon B\eta}+e^{5\epsilon B\eta}-e^{-5\epsilon B\eta}\right) \\ & = L\left(e^{\Lambda\epsilon}e^{5\epsilon B\eta}-e^{5\epsilon B\eta}+\frac{1}{(e^{\Lambda\epsilon}-1)}(e^{\Lambda\epsilon}-1)e^{5\epsilon B\eta}-e^{-5\epsilon B\eta}\right) \\ & \leq L\left(e^{\Lambda\epsilon}e^{5\epsilon B\eta}-e^{5\epsilon B\eta}+\frac{1}{(e-1)}(e^{\Lambda\epsilon}-1)e^{5\epsilon B\eta}-e^{-5\epsilon B\eta}\right)\ (by 1\leq\Lambda\epsilon<2) \\ & = L\frac{e}{(e-1)}\left(e^{\Lambda\epsilon}e^{5\epsilon B\eta}-e^{5\epsilon B\eta}-e^{-5\epsilon B\eta}\right) \\ & < L\frac{e}{(e-1)}\left(e^{\Lambda\epsilon}e^{5\epsilon B\eta}-e^{5\epsilon B\eta}\right) \\ & = L(e^{\Lambda\epsilon}-1)e^{\ln(\frac{e}{(e-1)})+5\epsilon B\eta} \\ & < L(e^{\Lambda\epsilon}-1)e^{11\epsilon B\eta}\ (by\ (\frac{1}{\epsilon}<B<2^{42}\frac{1}{\epsilon})) \\ & = (R-L)e^{11\epsilon B\eta} \end{array}$$

In the same way, we can derive:

$$|\underline{R}-\bar{L}| > e^{-5\epsilon B\eta}R-e^{5\epsilon B\eta}L > (R-L)e^{-12\epsilon B\eta}$$

Then we have:

$$\frac{|\bar{R}-\underline{L}|}{|\underline{R}'-\bar{L}'|} < e^{(23\epsilon B\eta+\epsilon)}.$$

subcase $\lfloor f(a)\rceil_\Lambda > 0 \wedge x \in (0, \lfloor f(a)\rceil_\Lambda)$

Let $y_1 = x-(\frac{\Lambda}{2})$, $y_2 = x+(\frac{\Lambda}{2})$, we know $y_1 > 0$, $y_2 > 0$, $S = s = 1$, $L = e^{\epsilon(y_1-f(a))}$ and $R = e^{\epsilon(y_2-f(a))}$ in this case. The derivations of estimating l and r are shown as following:

$$\dfrac{\dfrac{\dfrac{\dfrac{L \Downarrow l, (\underline{L}, \bar{L})}{\ln(L) \Downarrow \text{ⓛⓝ}(l), (\ln(\underline{L})(1+\eta), \dfrac{\ln(\bar{L})}{(1+\eta)})}}{\dfrac{1}{\epsilon}\times\ln(L) \Downarrow \dfrac{1}{\epsilon}\otimes\text{ⓛⓝ}(l), ((\dfrac{1}{\epsilon}\times\ln(\underline{L}))(1+\eta)^2, \dfrac{\frac{1}{\epsilon}\times\ln(\bar{L})}{(1+\eta)^2})}}{f(a)+\dfrac{1}{\epsilon}\times\ln(L) \Downarrow f(a)\oplus\dfrac{1}{\epsilon}\otimes\text{ⓛⓝ}(l), (\dfrac{f(a)+(\frac{1}{\epsilon}\times\ln(\underline{L}))(1+\eta)^2}{1+\eta}, (f(a)+\dfrac{\frac{1}{\epsilon}\times\ln(\bar{L})}{(1+\eta)^2})(1+\eta))}}{\mathsf{Snap}'_{\mathbb{R}}(a, L, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, l, 1), (err_1, err_2)}$$

From soundness theorem, we have $err_1 \leq y_1 \leq err_2$.

Taking the lower bound (i.e. $err_1 = y_1$), we get: $\underline{L} = e^{(y_1/(1+\eta)-f(a))(1+\eta)^2\epsilon}$. Taking the upper bound (i.e. $err_2 = y_1$), we get: $\bar{L} = e^{(y_1(1+\eta)-f(a))\epsilon/(1+\eta)^2}$.

$$\frac{\dfrac{\cdots}{\mathsf{Snap}'_{\mathbb{R}}(a,R,1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a,r,1), (\frac{f(a)+(\frac{1}{\epsilon}\times\ln(\underline{R}))(1+\eta)^2}{1+\eta}, (f(a)+\frac{\frac{1}{\epsilon}\times\ln(\bar{R})}{(1+\eta)^2})(1+\eta))}}{\mathsf{Snap}'_{\mathbb{R}}(a,R,1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a,r,1), (err_1, err_2)}$$

From soundness theorem, we have $err_1 \le y_2 \le err_2$.

Taking the lower bound (i.e. $err_1 = y_2$), we have: $\underline{R} = e^{(y_2/(1+\eta)-f(a))(1+\eta)^2\epsilon}$. Taking the upper bound (i.e. $err_2 = y_1$), we have: $\bar{R} = e^{(y_2(1+\eta)-f(a))\epsilon/(1+\eta)^2}$.

In the same way, we have the derivation for $\mathsf{Snap}'_{\mathbb{F}}(a',l,1)$ and $\mathsf{Snap}'_{\mathbb{F}}(a',r,1)$:

$$\frac{\cdots}{\mathsf{Snap}'_{\mathbb{R}}(a',L',1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a',l',1), (\frac{f(a')+(\frac{1}{\epsilon}\times\ln(\underline{L}'))(1+\eta)^2}{1+\eta}, (f(a')+\frac{\frac{1}{\epsilon}\times\ln(\bar{L}')}{(1+\eta)^2})(1+\eta))}$$

From soundness theorem, we have $err_1 \le y_2 \le err_2$.

Taking the lower bound (i.e. $err_1 = y_1$), we get: $\underline{L} = e^{(y_1/(1+\eta)-f(a'))(1+\eta)^2\epsilon}$. Taking the upper bound (i.e. $err_2 = y_1$), we get: $\bar{L} = e^{(y_1(1+\eta)-f(a'))\epsilon/(1+\eta)^2}$.

$$\frac{\cdots}{\mathsf{Snap}'_{\mathbb{R}}(a',R',1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a',r',1), (\frac{f(a')+(\frac{1}{\epsilon}\times\ln(\underline{R}'))(1+\eta)^2}{1+\eta}, (f(a')+\frac{\frac{1}{\epsilon}\times\ln(\bar{R}')}{(1+\eta)^2})(1+\eta))}$$

From soundness theorem, we have $err_1 \le y_2 \le err_2$.

Taking the lower bound (i.e. $err_1 = y_2$), we have: $\underline{R} = e^{(y_2/(1+\eta)-f(a'))(1+\eta)^2\epsilon}$. Taking the upper bound (i.e. $err_2 = y_1$), we have: $\bar{R} = e^{(y_2(1+\eta)-f(a'))\epsilon/(1+\eta)^2}$.

The privacy loss is bounded by:

$$\frac{|\bar{R}-\underline{L}|}{|\underline{R}'-\bar{L}'|}$$

Since the following bound can be proved by using $1-2\eta < (1+\eta)^2 < 1+2.1\eta, y_1 > -B, y_2 > -B$ and simple approximation:

$$\bar{R}-\underline{L} < (R-L)e^{(5B\eta\epsilon)}, \underline{R}'-\bar{L}' > (R'-L')e^{-7B\eta\epsilon}$$

We also have the $\mathsf{Snap}_{\mathbb{R}}(a)$ is ϵ-dp:

$$\frac{|R-L|}{|R'-L'|} = e^{\epsilon}$$

So we can get:

$$\frac{|\bar{R}-\underline{L}|}{|\underline{R}'-\bar{L}'|} < \frac{|R-L|}{|R'-L'|}e^{(12B\eta\epsilon)} = e^{(1+12B\eta)\epsilon}$$

subcase $\lfloor f(a) \rceil_{\Lambda} > 0 \wedge x = 0$

Let $y_1 = x - (\frac{\Lambda}{2})$, $y_2 = x + (\frac{\Lambda}{2})$, we know $y_1 < 0$, $y_2 > 0$, $S = s = 1$, $L = e^{\epsilon(y_1 - f(a))}$ and $R = e^{\epsilon(y_2 - f(a))}$ in this case. We have the derivation as:

$$\dfrac{\dfrac{\cdots}{\mathsf{Snap}'_{\mathbb{R}}(a, L, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, l, 1), (\dfrac{f(a) + (\frac{1}{\epsilon} \times \ln(\underline{L}))(1+\eta)^2}{1+\eta}, (f(a) + \dfrac{\frac{1}{\epsilon} \times \ln(\bar{L})}{(1+\eta)^2})(1+\eta))}}{\mathsf{Snap}'_{\mathbb{R}}(a, L, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, l, 1), (err_1, err_2)}$$

From soundness theorem, we have $err_1 \leq y_2 \leq err_2$.
Taking the lower bound , we have: $\underline{L} = e^{\epsilon\left((y_2(1+\eta) - f(a))(1+\eta)^2)\right)}$.
Taking the upper bound, we have: $\bar{L} = e^{\epsilon \frac{(\frac{y_2}{1+\eta} - f(a))}{(1+\eta)^2}}$.

$$\dfrac{\dfrac{\cdots}{\mathsf{Snap}'_{\mathbb{R}}(a, R, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, r, 1), (\dfrac{f(a) + (\frac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2}{1+\eta}, (f(a) + \dfrac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})(1+\eta))}}{\mathsf{Snap}'_{\mathbb{R}}(a, R, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, r, 1), (err_1, err_2)}$$

From soundness theorem, we have $err_1 \leq y_2 \leq err_2$. Taking the lower bound (i.e. $err_1 = y_2$), we have: $\underline{R} = e^{(y_2/(1+\eta) - f(a))(1+\eta)^2 \epsilon}$. Taking the upper bound (i.e. $err_2 = y_1$), we have: $\bar{R} = e^{(y_2(1+\eta) - f(a))\epsilon/(1+\eta)^2}$. Using the bound we proved before, we have the folloing bound on $|\bar{R} - \underline{L}|$ and $|\underline{R} - \bar{L}|$:

$$\begin{aligned} \bar{R} - \underline{L} &< e^{(2B\eta\epsilon)} R - e^{-5B\eta\epsilon} L < (R - L) e^{6B\eta\epsilon} \\ \underline{R} - \bar{L} &> e^{(-3B\eta\epsilon)} R - e^{5B\eta\epsilon} L > (R - L) e^{-8B\eta\epsilon}, \end{aligned}$$

and privacy loss is bounded by:

$$\frac{|\bar{R} - \underline{L}|}{|\underline{R}' - \bar{L}'|} < e^{14B\eta\epsilon + \epsilon}$$

case $x = \lfloor f(a) \rceil_{\Lambda}$

This case can also be split into 3 subcases by: $\lfloor f(a) \rceil_{\Lambda} < 0$, $\lfloor f(a) \rceil_{\Lambda} = 0$ and $\lfloor f(a) \rceil_{\Lambda} > 0$. Without loss of generalization, we consider the worst case where the error propagate in the same direction, i.e. $\lfloor f(a) \rceil_{\Lambda} < 0$.
From this assumption, let $y_1 = x - (\frac{\Lambda}{2})$, $y_2 = x + (\frac{\Lambda}{2})$, we know $y_1 < 0$, $y_2 < 0$. Since $f(a) + 1 = f(a')$, we also have $\lfloor f(a) \rceil < \lfloor f(a') \rceil$. So, we know s can only be 1 for input a' but s can be 1 or -1 for input a.
For input a, when $s = 1$, we have following derivations:

$$\dfrac{\dfrac{\dfrac{\dfrac{R \Downarrow r, (R, R)}{\ln(R) \Downarrow ⓛⓝ(r), (\ln(R)(1+\eta), \dfrac{\ln(R)}{1+\eta})}}{\dfrac{1}{\epsilon}\ln(R) \Downarrow \dfrac{1}{\epsilon} \otimes ⓛⓝ(r), \left(\dfrac{1}{\epsilon}\ln(R)(1+\eta)^2, \dfrac{1}{\epsilon}\dfrac{\ln(R)}{(1+\eta)^2}\right)}}{f(a) + \dfrac{1}{\epsilon}\ln(R) \Downarrow f(a) \oplus \dfrac{1}{\epsilon} \otimes ⓛⓝ(r), \Big((f(a) + \dfrac{1}{\epsilon}\ln(R)(1+\eta)^2)(1+\eta), (f(a) + \dfrac{1}{\epsilon}\dfrac{\ln(R)}{(1+\eta)^2})/(1+\eta)\Big)}}{\mathsf{Snap}'_{\mathbb{R}}(a, 1, R) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, 1, r), (err_1, err_2)}$$

From soundness theorem, we have $err_1 \le y_2 \le err_2$. Then we can get following bounds for r:
$\underline{R}_+ = e^{\epsilon\left((y_2(1+\eta)-f(a))(1+\eta)^2)\right)}$, $\bar{R}_+ = e^{\epsilon\frac{(\frac{y_2}{1+\eta}-f(a))}{(1+\eta)^2}}$.
Since $y_2 = \lfloor f(a) \rceil + \frac{\Lambda}{2}$, we have $e^{\epsilon\left((y_2-f(a)))\right)} > 1$, so actually we know $R = r = 1$.
We can also derive the bound for l in the same way as:
$\underline{L}_+ = e^{\epsilon\left((y_1(1+\eta)-f(a))(1+\eta)^2)\right)}$, $\bar{L}_+ = e^{\epsilon\frac{(\frac{y_1}{1+\eta}-f(a))}{(1+\eta)^2}}$.
When $s = -1$, we can derive following bounds in the same way for l and r:
$\underline{L}_- = e^{\epsilon\left((f(a)-y_2(1+\eta))(1+\eta)^2)\right)}$, $\bar{L}_- = e^{\epsilon\frac{(f(a)-\frac{y_2}{1+\eta})}{(1+\eta)^2}}$.
$\underline{R}_2 = e^{\epsilon\left((f(a)-y_1(1+\eta))(1+\eta)^2)\right)}$, $\bar{R}_2 = e^{\epsilon\frac{(f(a)-\frac{y_1}{1+\eta})}{(1+\eta)^2}}$.
Since $y_1 = \lfloor f(a) \rceil - \frac{\Lambda}{2}$, we have $e^{\epsilon\left((f(a)-y_1))\right)} > 1$, so actually we know $R' = r' = 1$.
For input a', we have only one case where $s = 1$, the following bound can be derived:
$\underline{R}' = e^{\epsilon\left((y_2(1+\eta)-f(a'))(1+\eta)^2)\right)}$, $\bar{R}' = e^{\epsilon\frac{(\frac{y_2}{1+\eta}-f(a'))}{(1+\eta)^2}}$.
$\underline{L}' = e^{\epsilon\left((y_1(1+\eta)-f(a'))(1+\eta)^2)\right)}$, $\bar{L}' = e^{\epsilon\frac{(\frac{y_1}{1+\eta}-f(a'))}{(1+\eta)^2}}$.
We have following bounds on their ratios:

$$\frac{\underline{R}_+}{R_+} = e^{\epsilon\left((1+\eta)^3 y_2-(1+\eta)^2 f(a)-y_2+f(a)\right)} > e^{-3\epsilon B\eta}, \frac{\bar{R}_+}{R_+} = e^{\epsilon\left(fracy_2(1+\eta)^3-\frac{f(a)}{(1+\eta)^2}-y_2+f(a)\right)} < e^{3\epsilon B\eta},$$

The same bound for L_+ by substituting y_2 with y_1, and similar bound for L', R'.

$$\frac{\underline{R}'}{R} = e^{\epsilon\left((1+\eta)^2 f(a)-(1+\eta)^3 y_2-f(a)+y_2\right)} > e^{-2\epsilon B\eta}, \frac{\bar{R}'}{R'} = e^{\epsilon\left(\frac{f(a)}{(1+\eta)^2}-fracy_2(1+\eta)^3-f(a)+y_2\right)} < e^{2\epsilon B\eta},$$

Using the bound on their ratios, we can get following bounds on $|\bar{R}_+ - \underline{L}_+|$ and $|\underline{R}' - \bar{L}'|$:

$$|\bar{R}_+ - \underline{L}_+| < e^{3\epsilon B\eta}R - e^{-3\epsilon B\eta}L < (R-L)e^{7\epsilon B\eta}, |\underline{R}' - \bar{L}'| > e^{-2\epsilon B\eta}R - e^{2\epsilon B\eta}L > (R'-L')e^{-5\epsilon B\eta}$$

Then we have the following bounds on privacy loss:

$$\frac{2-(\underline{L}_+ + \underline{L}_-)}{\underline{R}' - \bar{L}'} < \frac{\bar{R}_+ - \underline{L}_+}{\underline{R}' - \bar{L}'} < \frac{e^{7\epsilon B\eta}(R_+ - L_+)}{e^{-5\epsilon B\eta}(R'-L')} = e^{12\epsilon B\eta+\epsilon}$$

case $x \in (\lfloor f(a) \rceil_\Lambda, \lfloor f(a') \rceil_\Lambda)$

case $x = \lfloor f(a') \rceil_\Lambda$

This case is symmetric with the case where $\boldsymbol{x = \lfloor f(a') \rceil_\Lambda}$. It can also be split into 3 subcases by: $\lfloor f(a') \rceil_\Lambda < 0$, $\lfloor f(a') \rceil_\Lambda = 0$ and $\lfloor f(a') \rceil_\Lambda > 0$. Without loss of generalization, we consider the worst case where the error propagate in the same direction, i.e. $\lfloor f(a') \rceil_\Lambda < 0$.
From this assumption, let $y_1 = x - (\frac{\Lambda}{2})$, $y_2 = x + (\frac{\Lambda}{2})$, we know $y_1 < 0$, $y_2 < 0$. Since $f(a) + 1 = f(a')$, we also have $\lfloor f(a) \rceil < \lfloor f(a') \rceil < 0$. So, we know s can only be -1 for input a but s can be 1 or -1 for input a'.

For input a', when $s=1$, we have following derivations:

$$\dfrac{\dfrac{\dfrac{\dfrac{R'_+ \Downarrow r_+, (R'_+, R'_+)}{\ln(R'_+) \Downarrow \text{ⓛⓝ}(r_+), (\ln(R'_+)(1+\eta), \frac{\ln(R'_+)}{1+\eta})}}{\frac{1}{\epsilon}\ln(R) \Downarrow \frac{1}{\epsilon} \otimes \text{ⓛⓝ}(r_+), (\frac{1}{\epsilon}\ln(R'_+)(1+\eta)^2, \frac{1}{\epsilon}\frac{\ln(R'_+)}{(1+\eta)^2})}}{f(a)+\frac{1}{\epsilon}\ln(R'_+) \Downarrow f(a) \oplus \frac{1}{\epsilon} \otimes \text{ⓛⓝ}(r_+), \Big((f(a)+\frac{1}{\epsilon}\ln(R'_+)(1+\eta)^2)(1+\eta), (f(a)+\frac{1}{\epsilon}\frac{\ln(R'_+)}{(1+\eta)^2})/(1+\eta)\Big)}}{\mathsf{Snap}'_{\mathbb{R}}(a,1,R'_+) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a,1,r_+), (err_1, err_2)}$$

From soundness theorem, we have $err_1 \le y_2 \le err_2$. Then we can get following bounds for r:
$\underline{R'_+} = e^{\epsilon\big((y_2(1+\eta)-f(a'))(1+\eta)^2\big)}$, $\bar{R'_+} = e^{\epsilon\frac{(\frac{y_2}{1+\eta}-f(a'))}{(1+\eta)^2}}$.
Since $y_2 = \lfloor f(a) \rceil + \frac{\Lambda}{2}$, we have $e^{\epsilon\big((y_2-f(a))\big)} > 1$, so actually we know $R'_+ = r'_+ = 1$.
We can also derive the bound for l in the same way as:
$\underline{L'_+} = e^{\epsilon\big((y_1(1+\eta)-f(a'))(1+\eta)^2\big)}$, $\bar{L'_+} = e^{\epsilon\frac{(\frac{y_1}{1+\eta}-f(a'))}{(1+\eta)^2}}$.
When $s=-1$, we can derive following bounds in the same way for l and r:
$\underline{L'_-} = e^{\epsilon\big((f(a')-y_2(1+\eta))(1+\eta)^2\big)}$, $\bar{L'_-} = e^{\epsilon\frac{(f(a')-\frac{y_2}{1+\eta})}{(1+\eta)^2}}$.
$\underline{R'_-} = e^{\epsilon\big((f(a')-y_1(1+\eta))(1+\eta)^2\big)}$, $\bar{R'_-} = e^{\epsilon\frac{(f(a')-\frac{y_1}{1+\eta})}{(1+\eta)^2}}$.
Since $y_1 = \lfloor f(a') \rceil - \frac{\Lambda}{2}$, we have $e^{\epsilon\big((f(a')-y_1)\big)} > 1$, so actually we know $R'_- = r'_- = 1$.
For input a, we have only one case where $s=-1$, the following bound can be derived:
$\underline{R} = e^{\epsilon\big(f(a)-(y_2(1+\eta))(1+\eta)^2\big)}$, $\bar{R} = e^{\epsilon\frac{(f(a)-\frac{y_2}{1+\eta})}{(1+\eta)^2}}$.
$\underline{L} = e^{\epsilon\big((f(a)-y_1(1+\eta))(1+\eta)^2\big)}$, $\bar{L} = e^{\epsilon\frac{f(a)-\frac{y_1}{1+\eta}}{(1+\eta)^2}}$.
We have following bounds on their ratios:

$$\frac{\underline{R_+}}{R_+} = e^{\epsilon\big((1+\eta)^3 y_2-(1+\eta)^2 f(a)-y_2+f(a)\big)} > e^{-3\epsilon B\eta}, \frac{\bar{R_+}}{R_+} = e^{\epsilon\big(fracy_2(1+\eta)^3-\frac{f(a)}{(1+\eta)^2}-y_2+f(a)\big)} < e^{3\epsilon B\eta},$$

The same bound for L_+ by substituting y_2 with y_1, and similar bound for L', R'.

$$\frac{\underline{R'}}{R} = e^{\epsilon\big((1+\eta)^2 f(a)-(1+\eta)^3 y_2-f(a)+y_2\big)} > e^{-2\epsilon B\eta}, \frac{\bar{R'}}{R'} = e^{\epsilon\big(\frac{f(a)}{(1+\eta)^2}-fracy_2(1+\eta)^3-f(a)+y_2\big)} < e^{2\epsilon B\eta},$$

Using the bound on their ratios, we can get following bounds on $|\bar{R_+} - \underline{L_+}|$ and $|\underline{R'} - \bar{L'}|$:

$$|\bar{R'_-} - \underline{L'_-}| < e^{3\epsilon B\eta}R - e^{-3\epsilon B\eta}L < (R'_- - L'_-)e^{7\epsilon B\eta}, |\underline{R} - \bar{L}| > e^{-2\epsilon B\eta}R - e^{2\epsilon B\eta}L > (R-L)e^{-5\epsilon B\eta}$$

Then we have the following bounds on privacy loss:

$$\frac{\underline{R}-\bar{L}}{2-(\underline{L'_+}+\underline{L'_-})} > \frac{\underline{R}-\bar{L}}{\bar{R'_-}-\underline{L'_-}} > \frac{e^{-5\epsilon B\eta}(R-L)}{e^{7\epsilon B\eta}(R'_- - L'_-)} = e^{-12\epsilon B\eta - \epsilon}$$

case $\boldsymbol{x \in (\lfloor f(a') \rceil_\Lambda, B)}$
This case can also be split into 3 subcases symmetric with the case where $\boldsymbol{x \in (-B, \lfloor f(a) \rceil_\Lambda)}$:

subcase $\lfloor f(a')\rceil_\Lambda > 0 \vee \lfloor f(a')\rceil_\Lambda < 0 \wedge x \in (0, B)$

let $y_1 = x - \frac{\Lambda}{2}$, $y_2 = x - \frac{\Lambda}{2}$, we have $y_1, y_2 > 0$. The bounds derived for l, r in this case are as follows:

subcase $\lfloor f(a')\rceil_\Lambda < 0 \wedge x \in (\lfloor f(a')\rceil_\Lambda, 0)$

let $y_1 = x - \frac{\Lambda}{2}$, $y_2 = x - \frac{\Lambda}{2}$, we have $y_1, y_2 < 0$. The bounds derived for l, r in this case are as follows:

subcase $\lfloor f(a')\rceil_\Lambda < 0 \wedge x = 0$

let $y_1 = x - \frac{\Lambda}{2}$, $y_2 = x - \frac{\Lambda}{2}$, we have $y_1 < 0$ and $y_2 > 0$. The bounds derived for l, r in this case are as follows:

case $x = B$

We know $s = -1$, $L = l = 0$ and $R = b$, so we only need to estimate the right side range r in this case. The bounds derived for r, r' are as following:

$$\underline{R} = e^{\epsilon\left((f(a) - \frac{x}{1+\eta})(1+\eta)^2\right)}, \bar{R} = e^{\epsilon\frac{(f(a)-x(1+\eta))}{(1+\eta)^2}}$$
$$\underline{R}' = e^{\epsilon\left((f(a') - \frac{x}{1+\eta})(1+\eta)^2\right)}, \bar{R}' = e^{\epsilon\frac{(f(a')-x(1+\eta))}{(1+\eta)^2}}$$

The privacy loss of $\mathsf{Snap}_{\mathbb{F}}(a)$ in this case is bounded by:

$$\begin{aligned}\frac{\frac{1}{2}(\underline{R}-0)}{\frac{1}{2}(\bar{R}'-0)} &= e^{\epsilon\left(\left((f(a)-\frac{x}{1+\eta})(1+\eta)^2\right) - \frac{(f(a')-x(1+\eta))}{(1+\eta)^2}\right)} \\ &= e^{\epsilon\left(f(a)(1+\eta)^2 - x(1+\eta) - \frac{f(a)}{(1+\eta)^2} + \frac{x}{(1+\eta)}\right)} \quad (\star)\end{aligned}$$

Since $1 + 2.1\eta > (1+\eta)^2 > 1 + 2\eta$ and $\frac{1}{(1+\eta)^2} > 1 - 2\eta$, we have:

$$\begin{aligned}(\star) \quad &> e^{\epsilon\left((1+2\eta)f(a) - \frac{\eta(\eta+2)}{1+\eta}x - \frac{1}{1+2\eta}(f(a)+1)\right)} \\ &= e^{\epsilon\left(\frac{4\eta(\eta+1)}{1+2\eta}f(a) - \frac{\eta(\eta+2)}{1+\eta}x - \frac{1}{1+2\eta}\right)} \\ &> e^{\epsilon\left(-B\eta\frac{4(\eta+1)}{1+2\eta} + \frac{(\eta+2)}{1+\eta}x - 1\right)} \\ &> e^{\epsilon(-6\eta B - 1)}\end{aligned}$$

□

References

[1] Gilles Barthe, Marco Gaboardi, Benjamin Grégoire, Justin Hsu, and Pierre-Yves Strub. Proving differential privacy via probabilistic couplings. In *LICS 2016*.

[2] H. Becker, N. Zyuzin, R. Monat, E. Darulova, M. O. Myreen, and A. Fox. A verified certificate checker for finite-precision error bounds in coq and hol4. In *2018 Formal Methods in Computer Aided Design (FMCAD)*, 2018.

[3] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating Noise to Sensitivity in Private Data Analysis. In *TCC*, 2016.

[4] Matthieu Martel. Semantics of roundoff error propagation in finite precision calculations. *Higher-Order and Symbolic Computation*, 2006.

[5] Ilya Mironov. On significance of the least significant bits for differential privacy. In *CCS 2012*, 2012.

[6] Mariano Moscato, Laura Titolo, Aaron Dutle, and César A. Muñoz. Automatic estimation of verified floating-point round-off errors via static analysis. In Stefano Tonetta, Erwin Schoitsch, and Friedemann Bitsch, editors, *Computer Safety, Reliability, and Security*, 2017.

[7] Tahina Ramananandro, Paul Mountcastle, Benoundefinedt Meister, and Richard Lethin. A unified coq framework for verifying c programs with floating-point computations. In *Proceedings of the 5th ACM SIGPLAN Conference on Certified Programs and Proofs (CPP)*. Association for Computing Machinery, 2016.