

Verifying Snapping Mechanism - Floating Point Implementation Version

Jiawen Liu

March 9, 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 $\mathcal{L}_\epsilon: \mathbb{R} \rightarrow \text{Distr}(\mathbb{R})$ is defined by $\mathcal{L}(t) = t + v$, where $v \in \mathbb{R}$ is drawn from the Laplace distribution $\text{laplce}(\frac{1}{\epsilon})$.

2 Syntax - IMP

Programs	p	$::=$	$x = e \mid x \stackrel{\$}{\leftarrow} \mu \mid p; p$
Expr.	e	$::=$	$r \mid c \mid x \mid f(D) \mid e * e \mid \circ(e)$
Binary Operation	$*$	$::=$	$+ \mid - \mid \times \mid \div$
Unary Operation	\circ	$::=$	$\ln \mid - \mid \lfloor \cdot \rfloor \mid \text{clamp}_B(\cdot)$
Value	v	$::=$	$r \mid c$
Distribution	μ	$::=$	$\text{laplce} \mid \text{unif} \mid \text{bernoulli}$
Error	err	$::=$	(e, e)
Transaction Env.	Θ	$::=$	$\cdot \mid \Theta[x \mapsto (e, err)]$

3 Semantics - IMP

The transition semantics with relative floating point computation error are shown in Figure. 5 for programs. The semantics are $\Theta, p \Rightarrow \Theta'$, which means a real computation programs p with environment Θ can be transited in floating point computation with error bound for all variables in Θ' , η is the machine epsilon.

$$\begin{array}{c}
\frac{\Theta(x) = (e, (\underline{e}, \bar{e}))}{\Theta, x \Rightarrow (e, (\underline{e}, \bar{e}))} \text{VAR} \qquad \frac{x \notin \text{dom}(\Theta)}{\Theta, x \Rightarrow (x, (x, x))} \text{VAR-NON} \qquad \frac{r \geq 0}{\Theta, r \Rightarrow (\frac{r}{(1+\eta)}, r(1+\eta))} \text{VAL} \\
\\
\frac{c = \text{fl}(r) \quad r < 0}{\Theta, r \Rightarrow (r(1+\eta), \frac{r}{(1+\eta)})} \text{VAL-NEG} \qquad \frac{r = \text{fl}(r)}{\Theta, r \Rightarrow (r, r)} \text{VAL-EQ} \qquad \frac{}{\Theta, f(D) \Rightarrow (f(D), (f(D), f(D)))} \text{F(D)} \\
\\
\frac{\Theta, e^1 \Rightarrow (e^1, \bar{e}^1) \quad \Theta, e^2 \Rightarrow (e^2, \bar{e}^2) \quad e^1 * e^2 \geq 0}{\Theta, e^1 * e^2 \Rightarrow (e^1 * e^2, (\frac{e^1 * e^2}{(1+\eta)}, (\bar{e}^1 * \bar{e}^2)(1+\eta)))} \text{BOP} \quad \frac{\Theta, e^1 \Rightarrow (e^1, \bar{e}^1) \quad \Theta, e^2 \Rightarrow (e^2, \bar{e}^2) \quad e^1 * e^2 < 0}{\Theta, e^1 * e^2 \Rightarrow (e^1 * e^2, (\bar{e}^1 * \bar{e}^2)(1+\eta), \frac{e^1 * e^2}{(1+\eta)})} \text{BOP-NEG} \\
\\
\frac{\Theta, e \Rightarrow (\underline{e}, \bar{e}) \quad \circ(e) \geq 0}{\Theta, \circ(e) \Rightarrow (\circ(e), (\frac{\circ(\underline{e})}{(1+\eta)}, (\circ(\bar{e}))(1+\eta))} \text{UOP} \quad \frac{\Theta, e \Rightarrow (\underline{e}, \bar{e}) \quad \circ(e) < 0}{\Theta, \circ(e) \Rightarrow (\circ(e), (\circ(\underline{e}))(1+\eta), \frac{\circ(\bar{e})}{(1+\eta)})} \text{UOP-NEG}
\end{array}$$

Figure 1: Semantics of Transition for Expressions with Relative Floating Point Error

$$\frac{\Theta, e \Rightarrow (e, \text{err})}{\Theta, x = e \Rightarrow \Theta[x \mapsto (e, \text{err})]} \text{ASG} \quad \frac{\Theta, p_1 \Rightarrow \Theta_1 \quad \Theta_2, p_2 \Rightarrow \Theta_2}{\Theta, p_1; p_2 \Downarrow \Theta_2} \text{CONSQ} \quad \frac{c \leftarrow \mu^\diamond}{\Theta, x \xleftarrow{\$} \mu \Downarrow \Theta[x \mapsto (c, (c, c))]} \text{SAMPLE}$$

Figure 2: Semantics of Transition with Relative Floating Point Error Propagation for Programs

$$\begin{array}{c}
\frac{\text{fl}(r) = c}{r \Downarrow c} \text{RVAL} \qquad \frac{}{c \Downarrow c} \text{FVAL} \qquad \frac{e^1 \Downarrow c^1 \quad e^2 \Downarrow c^2 \quad \text{fl}(c^1 * c^2) = c}{e^1 * e^2 \Downarrow c} \text{FBOP} \\
\\
\frac{e \Downarrow c', \quad \text{fl}(\circ(c')) = c}{\circ(e) \Downarrow c} \text{FUOP}
\end{array}$$

Figure 3: Semantics of Evaluation in Floating Point Computation

$$\begin{array}{c}
\frac{}{r \Downarrow r} \text{RVAL} \qquad \frac{}{c \Downarrow c} \text{RVAL} \qquad \frac{e^1 \Downarrow r^1 \quad e^2 \Downarrow r^2 \quad r^1 * r^2 = r}{e^1 * e^2 \Downarrow r} \text{RBOP} \\
\\
\frac{e \Downarrow r', \quad \circ(r') = r}{\circ(e) \Downarrow r} \text{RUOP} \qquad \frac{f(D) = c}{f(D) \Downarrow c} \text{F(D)}
\end{array}$$

Figure 4: Semantics of Evaluation in Real Computation

Theorem 1 (Soundness Theorem)

For any p , if the transition $\Theta, p \Rightarrow \Theta'$ holds and Θ is a safe transaction environment, then $\forall x \in \text{dom}(\Theta')$ s.t. $\Theta'(x) = (e, (\underline{e}, \bar{e}))$, we have if e evaluates to c in floating point computation and \underline{e} and \bar{e} evaluates to \underline{r} and \bar{r} in real computation, then:

$$\underline{r} \leq c \leq \bar{r}$$

Proof. Induction on p , we have following cases:

case $p_1; p_2$

case $x = e$

case $x \xleftarrow{\$} \mu$

□

4 Snapping Mechanism

Definition 2 ($\text{Snap}_{\mathbb{R}}(a) : A \rightarrow \text{Distr}(\mathbb{R})$)

Given privacy parameter ϵ , the Snapping mechanism $\text{Snap}_{\mathbb{R}}(a)$ is defined as:

$$U \xleftarrow{\$} \mu; S \xleftarrow{\$} \{-1, 1\}; y = f(a) + S \times \ln(U) \div \epsilon; z = \text{clamp}_B(\lfloor y \rfloor \Lambda)$$

where F is a primitive query function over input database $a \in A$, 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 $\text{Snap}'_{\mathbb{R}}(a, U, S)$ be the same as $\text{Snap}_{\mathbb{R}}(a)$ given U, S without rounding and clamping steps.

5 Main Theorem

Theorem 2 (The Snap mechanism is ϵ -differentially private)

Consider $\text{Snap}(a)$ defined as before, if $\text{Snap}(a) = x$ given database a and privacy parameter ϵ , then its actual privacy loss is bounded by $\epsilon + 23B\epsilon\eta$

Proof. Given $\text{Snap}_{\mathbb{F}}(a) = x$ 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 $\text{Snap}_{\mathbb{F}}(a)$ mechanism.

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

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

Let (l, r) be the range where $\forall u \in (l, r)$ and some s , $\text{Snap}'_{\mathbb{F}}(a, u, s) = x$, 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 $\text{Snap}_{\mathbb{F}}$.

case $x = -B$

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 $\text{Snap}'_{\mathbb{F}}(a, R, 1) = \text{Snap}'_{\mathbb{F}}(a', R, 1) = x$ is shown as following:

LN

$$\begin{array}{c}
 \frac{\text{VAL-EQ}}{R \Downarrow r, (R, R)} \\
 \hline
 \text{OP} \\
 \frac{\ln(R) \Downarrow \text{ID}(r), (\ln(R)(1 + \eta), \frac{\ln(R)}{(1 + \eta)})}{\text{OP}} \\
 \hline
 \frac{\frac{1}{\epsilon} \times \ln(R) \Downarrow \frac{1}{\epsilon} \otimes \text{ID}(r), ((\frac{1}{\epsilon} \times \ln(R))(1 + \eta)^2, \frac{\frac{1}{\epsilon} \times \ln(R)}{(1 + \eta)^2})}{\text{ID}} \\
 \hline
 \frac{f(a) + \frac{1}{\epsilon} \times \ln(R) \Downarrow f(a) \oplus \frac{1}{\epsilon} \otimes \text{ID}(r), \left((f(a) + (\frac{1}{\epsilon} \times \ln(R))(1 + \eta)^2)(1 + \eta), \frac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(R)}{(1 + \eta)^2})}{(1 + \eta)} \right)}{\text{ID}} \\
 \hline
 \text{Snap}'_{\mathbb{R}}(a, R, 1) \Downarrow \text{Snap}'_{\mathbb{F}}(a, r, 1), \left((f(a) + (\frac{1}{\epsilon} \times \ln(R))(1 + \eta)^2)(1 + \eta), \frac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(R)}{(1 + \eta)^2})}{(1 + \eta)} \right)
 \end{array}$$

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

$$\begin{array}{c}
 \dots \\
 \hline
 \text{Snap}'_{\mathbb{R}}(a', R', 1) \Downarrow \text{Snap}'_{\mathbb{F}}(a', r, 1), \left((f(a') + (\frac{1}{\epsilon} \times \ln(R'))(1 + \eta)^2)(1 + \eta), \frac{(f(a') + \frac{\frac{1}{\epsilon} \times \ln(R')}{(1 + \eta)^2})}{(1 + \eta)} \right)
 \end{array}$$

Given $\text{Snap}_{\mathbb{F}}(a) = \text{Snap}_{\mathbb{F}}(a') = x = -b$, we have the lower and upper bounds for R and R' , which are $\underline{R}, \bar{R}, \underline{R}'$ and \bar{R}' :

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

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

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

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:

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

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

subcase $\lfloor f(a) \rfloor_{\Lambda} \leq 0 \vee (\lfloor f(a) \rfloor_{\Lambda} > 0 \wedge x \in (-B, 0))$

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. The derivations of estimating l and r are shown as following:

LN

$$\begin{array}{c} \frac{\text{VAL-EQ}}{R \Downarrow r, (R, R)} \\ \hline \text{OP} \\ \ln(R) \Downarrow \mathbb{D}(r), (\ln(R)(1+\eta), \frac{\ln(R)}{(1+\eta)}) \\ \hline \text{OP} \\ \frac{1}{\epsilon} \times \ln(R) \Downarrow \frac{1}{\epsilon} \otimes \mathbb{D}(r), ((\frac{1}{\epsilon} \times \ln(R))(1+\eta)^2, \frac{\frac{1}{\epsilon} \times \ln(R)}{(1+\eta)^2}) \\ \hline \text{ID} \\ f(a) + \frac{1}{\epsilon} \times \ln(R) \Downarrow f(a) \oplus \frac{1}{\epsilon} \otimes \mathbb{D}(r), \left((f(a) + (\frac{1}{\epsilon} \times \ln(R))(1+\eta)^2)(1+\eta), \frac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(R)}{(1+\eta)^2})}{(1+\eta)} \right) \\ \hline \text{Snap}'_{\mathbb{R}}(a, R, 1) \Downarrow \text{Snap}'_{\mathbb{F}}(a, r, 1), (e^1, e^2) \end{array}$$

From soundness theorem, we have $e^1 \leq y_2 \leq e^2$, where we can get $\underline{R} \leq r \leq \bar{R}$.

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

Taking the upper bound, we have: $\bar{R} = e^{\epsilon(\frac{y_2}{1+\eta}-f(a))}$.

$$\begin{array}{c} \dots \\ \hline \text{Snap}'_{\mathbb{R}}(a, L, 1) \Downarrow \text{Snap}'_{\mathbb{F}}(a, l, 1), \left(\frac{f(a) + (\frac{1}{\epsilon} \times \ln(\underline{L}))(1+\eta)^2}{1+\eta}, (f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{L})}{(1+\eta)^2})(1+\eta) \right) \\ \hline \text{Snap}'_{\mathbb{R}}(a, L, 1) \Downarrow \text{Snap}'_{\mathbb{F}}(a, l, 1), (err_1, err_2) \end{array}$$

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

Taking the lower bound, we have: $\underline{L} = e^{\epsilon((y_2(1+\eta)-f(a))(1+\eta)^2)}$.

Taking the upper bound, we have: $\bar{L} = e^{\epsilon(\frac{y_2}{1+\eta}-f(a))}$.

In the same way, we have the bound of l, r for adjacent data set a' :

$$\begin{aligned} \underline{R}' &= e^{\epsilon((y_1(1+\eta)-f(a'))(1+\eta)^2)}, \quad \bar{R}' = e^{\epsilon \frac{(\frac{y_1}{1+\eta}-f(a'))}{(1+\eta)^2}}. \\ \underline{L}' &= e^{\epsilon((y_2(1+\eta)-f(a'))(1+\eta)^2)}, \quad \bar{L}' = e^{\epsilon \frac{(\frac{y_2}{1+\eta}-f(a'))}{(1+\eta)^2}} \end{aligned}$$

Then, we have the privacy loss is bounded by:

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

We also have:

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

Then, we can derive:

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

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 $\lfloor f(a) \rfloor_{\Lambda} > 0 \wedge x \in (0, \lfloor f(a) \rfloor_{\Lambda})$

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:

$$\begin{array}{c} L \Downarrow l, (\bar{L}, \bar{L}) \\ \hline \ln(L) \Downarrow \textcircled{\cap}(l), (\ln(L)(1+\eta), \frac{\ln(\bar{L})}{(1+\eta)}) \\ \hline \frac{1}{\epsilon} \times \ln(L) \Downarrow \frac{1}{\epsilon} \otimes \textcircled{\cap}(l), ((\frac{1}{\epsilon} \times \ln(L))(1+\eta)^2, \frac{\frac{1}{\epsilon} \times \ln(\bar{L})}{(1+\eta)^2}) \\ \hline f(a) + \frac{1}{\epsilon} \times \ln(L) \Downarrow f(a) \oplus \frac{1}{\epsilon} \otimes \textcircled{\cap}(l), (\frac{f(a) + (\frac{1}{\epsilon} \times \ln(L))(1+\eta)^2}{1+\eta}, (f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{L})}{(1+\eta)^2})(1+\eta)) \\ \hline \text{Snap}'_{\mathbb{R}}(a, L, 1) \Downarrow \text{Snap}'_{\mathbb{F}}(a, l, 1), (err_1, err_2) \end{array}$$

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: $\bar{L} = e^{(y_1(1+\eta)-f(a))\epsilon/(1+\eta)^2}$.

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

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: $\bar{R} = e^{(y_2(1+\eta)-f(a))\epsilon/(1+\eta)^2}$.

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

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

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

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: $\bar{L} = e^{(y_1(1+\eta)-f(a'))\epsilon/(1+\eta)^2}$.

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

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: $\bar{R} = e^{(y_2(1+\eta)-f(a'))\epsilon/(1+\eta)^2}$.

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 $\text{Snap}_{\mathbb{R}}(a)$ 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 $\lfloor f(a) \rfloor_{\Lambda} > 0 \wedge x = 0$

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:

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

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

Taking the lower bound, we have: $\underline{L} = e^{\epsilon((y_2(1 + \eta) - f(a))(1 + \eta)^2)}$.

Taking the upper bound, we have: $\bar{L} = e^{\epsilon \frac{(\frac{y_2}{1 + \eta} - f(a))}{(1 + \eta)^2}}$.

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

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

This case can also be split into 3 subcases by: $\lfloor f(a) \rfloor_{\Lambda} < 0$, $\lfloor f(a) \rfloor_{\Lambda} = 0$ and $\lfloor f(a) \rfloor_{\Lambda} > 0$. Without loss of generalization, we consider the worst case where the error propagate in the same direction, i.e. $\lfloor f(a) \rfloor_{\Lambda} < 0$.

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 $\lfloor f(a) \rfloor < \lfloor f(a') \rfloor$. 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:

$$\frac{R \Downarrow r, (R, R)}{\frac{\ln(R) \Downarrow \textcircled{\cap}(r), (\ln(R)(1 + \eta), \frac{\ln(R)}{1 + \eta})}{\frac{\frac{1}{\epsilon} \ln(R) \Downarrow \frac{1}{\epsilon} \otimes \textcircled{\cap}(r), \left(\frac{1}{\epsilon} \ln(R)(1 + \eta)^2, \frac{1}{\epsilon} \frac{\ln(R)}{(1 + \eta)^2} \right)} \\ \frac{f(a) + \frac{1}{\epsilon} \ln(R) \Downarrow f(a) \oplus \frac{1}{\epsilon} \otimes \textcircled{\cap}(r), \left((f(a) + \frac{1}{\epsilon} \ln(R)(1 + \eta)^2)(1 + \eta), (f(a) + \frac{1}{\epsilon} \frac{\ln(R)}{(1 + \eta)^2})/(1 + \eta) \right)} \\ \text{Snap}'_{\mathbb{R}}(a, 1, R) \Downarrow \text{Snap}'_{\mathbb{F}}(a, 1, r), (err_1, err_2)}$$

From soundness theorem, we have $err_1 \leq y_2 \leq err_2$. Then we can get following bounds for r :

$$\underline{R}_+ = e^{\epsilon((y_2(1+\eta)-f(a))(1+\eta)^2)}, \bar{R}_+ = e^{\epsilon \frac{(\frac{y_2}{1+\eta}-f(a))}{(1+\eta)^2}}.$$

Since $y_2 = \lfloor f(a) \rfloor + \frac{\Lambda}{2}$, we have $e^{\epsilon((y_2-f(a)))} > 1$, so actually we know $R = r = 1$.

We can also derive the bound for l in the same way as:

$$\underline{L}_+ = e^{\epsilon((y_1(1+\eta)-f(a))(1+\eta)^2)}, \bar{L}_+ = e^{\epsilon \frac{(\frac{y_1}{1+\eta}-f(a))}{(1+\eta)^2}}.$$

When $s = -1$, we can derive following bounds in the same way for l and r :

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

$$\underline{R}_2 = e^{\epsilon((f(a)-y_1(1+\eta))(1+\eta)^2)}, \bar{R}_2 = e^{\epsilon \frac{(f(a)-\frac{y_1}{1+\eta})}{(1+\eta)^2}}.$$

Since $y_1 = \lfloor f(a) \rfloor - \frac{\Lambda}{2}$, we have $e^{\epsilon((f(a)-y_1))} > 1$, so actually we know $R' = r' = 1$.

For input a' , we have only one case where $s = 1$, the following bound can be derived:

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

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

We have following bounds on their ratios:

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

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

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

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

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

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

Since the output set $(\lfloor f(a) \rfloor_\Lambda, \lfloor f(a') \rfloor_\Lambda)$ is empty when $\Lambda \geq 1$, so we consider the situation where $\Lambda < 1$. There are two subcases in this case : $x > 0$ and $x < 0$. Without loss of generalization, we consider the worst case where error propagate in the same direction, i.e., $\lfloor f(a') \rfloor_\Lambda < 0$. The bounds derived for l, r and l', r' under input a and a' are as follows:

For input a :

$$\underline{R} = e^{\epsilon((f(a)-y_2(1+\eta))(1+\eta)^2)}, \bar{R} = e^{\epsilon \frac{(f(a)-\frac{y_2}{1+\eta})}{(1+\eta)^2}}.$$

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

For input a' :

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

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

The bounds on their ratio are as follows:

$$\frac{R}{R'} > e^{-5B\eta\epsilon}, \frac{\bar{R}}{R'} < e^{5B\eta\epsilon}; \quad \frac{R'}{R} > e^{-5B\eta\epsilon}, \frac{\bar{R}'}{R'} < e^{5B\eta\epsilon}.$$

And the bounds on $|\underline{R} - \bar{L}|$ and $|\bar{R}' - \underline{L}'|$ are as follows:

$$|\underline{R} - \bar{L}| > e^{-12B\eta\epsilon} |R - L|, |\bar{R}' - \underline{L}'| < e^{11B\eta\epsilon} |R' - L'|$$

So we have the privacy loss is bounded by:

$$\frac{|\underline{R} - \bar{L}|}{|\bar{R}' - \underline{L}'|} > \frac{e^{-12B\eta\epsilon} |R - L|}{e^{11B\eta\epsilon} |R' - L'|} = e^{-23B\eta\epsilon - \epsilon}$$

case $\mathbf{x} = \lfloor f(a') \rfloor_{\Lambda}$

This case is symmetric with the case where $\mathbf{x} = \lfloor f(a') \rfloor_{\Lambda}$. It can also be split into 3 subcases by: $\lfloor f(a') \rfloor_{\Lambda} < 0$, $\lfloor f(a') \rfloor_{\Lambda} = 0$ and $\lfloor f(a') \rfloor_{\Lambda} > 0$. Without loss of generalization, we consider the worst case where the error propagate in the same direction, i.e. $\lfloor f(a') \rfloor_{\Lambda} < 0$.

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 $\lfloor f(a) \rfloor < \lfloor f(a') \rfloor < 0$. 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:

$$\begin{array}{c} R'_+ \Downarrow r_+, (R'_+, R'_+) \\ \hline \ln(R'_+) \Downarrow \textcircled{\cap}(r_+), (\ln(R'_+)(1+\eta), \frac{\ln(R'_+)}{1+\eta}) \\ \hline \frac{1}{\epsilon} \ln(R) \Downarrow \frac{1}{\epsilon} \otimes \textcircled{\cap}(r_+), \left(\frac{1}{\epsilon} \ln(R'_+)(1+\eta)^2, \frac{1}{\epsilon} \frac{\ln(R'_+)}{(1+\eta)^2} \right) \\ \hline f(a) + \frac{1}{\epsilon} \ln(R'_+) \Downarrow f(a) \oplus \frac{1}{\epsilon} \otimes \textcircled{\cap}(r_+), \left((f(a) + \frac{1}{\epsilon} \ln(R'_+)(1+\eta)^2)(1+\eta), (f(a) + \frac{1}{\epsilon} \frac{\ln(R'_+)}{(1+\eta)^2})/(1+\eta) \right) \\ \hline \text{Snap}'_{\mathbb{R}}(a, 1, R'_+) \Downarrow \text{Snap}'_{\mathbb{F}}(a, 1, r_+), (err_1, err_2) \end{array}$$

From soundness theorem, we have $err_1 \leq y_2 \leq err_2$. Then we can get following bounds for r :

$$R'_+ = e^{\epsilon((y_2(1+\eta)-f(a'))(1+\eta)^2)}, \bar{R}'_+ = e^{\epsilon \frac{y_2}{1+\eta} - f(a') \frac{1}{(1+\eta)^2}}.$$

Since $y_2 = \lfloor f(a) \rfloor + \frac{\Lambda}{2}$, we have $e^{\epsilon((y_2-f(a'))(1+\eta)^2)} > 1$, so actually we know $R'_+ = r'_+ = 1$.

We can also derive the bound for l in the same way as:

$$L'_+ = e^{\epsilon((y_1(1+\eta)-f(a'))(1+\eta)^2)}, \bar{L}'_+ = e^{\epsilon \frac{y_1}{1+\eta} - f(a') \frac{1}{(1+\eta)^2}}.$$

When $s = -1$, we can derive following bounds in the same way for l and r :

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

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

Since $y_1 = \lfloor f(a') \rfloor - \frac{\Lambda}{2}$, we have $e^{\epsilon((f(a')-y_1)(1+\eta)^2)} > 1$, so actually we know $R'_- = r'_- = 1$.

For input a , we have only one case where $s = -1$, the following bound can be derived:

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

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

We have following bounds on their ratios:

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

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

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

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

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

Then we have the following bounds on privacy loss:

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

case $\mathbf{x} \in (\lfloor f(a') \rfloor_\Lambda, B)$

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

subcase $\lfloor f(a') \rfloor_\Lambda > 0 \vee \lfloor f(a') \rfloor_\Lambda < 0 \wedge \mathbf{x} \in (0, B)$

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 and l', r' under input a and a' in this case are as follows:

For input a' :

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

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

For input a :

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

$$\underline{L} = e^{\epsilon \left((f(a) - \frac{y_1}{1+\eta})(1+\eta)^2 \right)}, \bar{L} = e^{\epsilon \frac{(f(a) - \frac{y_1}{1+\eta})}{(1+\eta)^2}}. \text{ The bounds on their ratio are as follows:}$$

$$\frac{\underline{R}}{R} > e^{-3B\eta\epsilon}, \frac{\bar{R}}{R} < e^{3B\eta\epsilon}$$

And the bounds on $|\underline{R} - \bar{L}|$ and $|\bar{R}' - L'_-|$ are as follows:

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

So we have the privacy loss is bounded by:

$$\frac{|\underline{R} - \bar{L}|}{|\bar{R}' - L'_-|} > \frac{e^{-7B\eta\epsilon} |R - L|}{e^{7B\eta\epsilon} |R' - L'|} = e^{-14B\eta\epsilon - \epsilon}$$

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

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:

For input a' :

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

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

For input a :

$$\underline{R} = e^{\epsilon((f(a) - y_2(1+\eta))(1+\eta)^2)}, \bar{R} = e^{\epsilon \frac{(f(a) - \frac{y_2}{1+\eta})}{(1+\eta)^2}}.$$

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

The bounds on their ratio are as follows:

$$\frac{\underline{R}}{\underline{L}} > e^{-5B\eta\epsilon}, \frac{\bar{R}}{\bar{L}} < e^{5B\eta\epsilon}$$

And the bounds on $|\underline{R} - \bar{L}|$ and $|\bar{R}' - \underline{L}'|$ are as follows:

$$|\underline{R} - \bar{L}| > e^{-12B\eta\epsilon} |R - L|, |\bar{R}' - \underline{L}'| < e^{11B\eta\epsilon} |R' - L'|$$

So we have the privacy loss is bounded by:

$$\frac{|\underline{R} - \bar{L}|}{|\bar{R}' - \underline{L}'|} > \frac{e^{-12B\eta\epsilon} |R - L|}{e^{11B\eta\epsilon} |R' - L'|} = e^{-23B\eta\epsilon - \epsilon}$$

subcase $\lfloor f(a') \rfloor_{\Lambda} < 0 \wedge x = 0$

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:

For input a' :

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

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

For input a :

$$\underline{R} = e^{\epsilon((f(a) - \frac{y_2}{1+\eta})(1+\eta)^2)}, \bar{R} = e^{\epsilon \frac{(f(a) - y_2(1+\eta))}{(1+\eta)^2}}.$$

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

The bounds on their ratio are as follows:

$$\frac{\underline{R}}{\underline{L}} > e^{-3B\eta\epsilon}, \frac{\bar{R}}{\bar{L}} < e^{3B\eta\epsilon} \frac{\underline{L}}{\underline{L}} > e^{-5B\eta\epsilon}, \frac{\bar{L}}{\bar{L}} < e^{5B\eta\epsilon}$$

And the bounds on $|\underline{R} - \bar{L}|$ and $|\bar{R}' - \underline{L}'|$ are as follows:

$$|\underline{R} - \bar{L}| > e^{-8B\eta\epsilon} |R - L|, |\bar{R}' - \underline{L}'| < e^{8B\eta\epsilon} |R' - L'|$$

So we have the privacy loss is bounded by:

$$\frac{|\underline{R} - \bar{L}|}{|\bar{R}' - \underline{L}'|} > \frac{e^{-8B\eta\epsilon} |R - L|}{e^{8B\eta\epsilon} |R' - L'|} = e^{-16B\eta\epsilon - \epsilon}$$

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:

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

The privacy loss of $\text{Snap}_{\mathbb{F}}(a)$ 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:

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

□

6 Syntax - V1

Following are the syntax of our system:

Expr.	e	$::=$	$x \mid r \mid c \mid F(D) \mid e * e \mid \circ(e) \mid \text{let } x \stackrel{\$}{\leftarrow} \mu \text{ in } e \mid \text{let } x = e_1 \text{ in } e_2$
Binary Operation	$*$	$::=$	$+ \mid - \mid \times \mid \div$
Unary Operation	\circ	$::=$	$\ln \mid - \mid [\cdot] \mid \text{clamp}_B(\cdot)$
Value	v	$::=$	$r \mid c$
Distribution	μ	$::=$	$\text{unif} \mid \text{bernoulli}$
Error	err	$::=$	(e, e)

$$\begin{array}{c}
\frac{r \geq 0}{r \Rightarrow (\frac{r}{(1+\eta)}, r(1+\eta))} \text{VAL} \qquad \frac{r < 0}{r \Rightarrow (r(1+\eta), \frac{r}{(1+\eta)})} \text{VAL-NEG} \qquad \frac{r = \text{fl}(r)}{r \Rightarrow (r, r)} \text{VAL-EQ} \\
\\
\frac{}{f(D) \Rightarrow (f(D), f(D))} \text{F(D)} \qquad \frac{}{\leftarrow^{\$} \mu \Rightarrow (\leftarrow^{\$} \mu, \leftarrow^{\$} \mu)} \text{SAMPLE} \\
\\
\frac{e^1 \Rightarrow (\underline{e}^1, \bar{e}^1) \quad e^2 \Rightarrow (\underline{e}^2, \bar{e}^2) \quad e^1 * e^2 \geq 0}{e^1 * e^2 \Rightarrow (\frac{\underline{e}^1 * \underline{e}^2}{(1+\eta)}, (\bar{e}^1 * \bar{e}^2)(1+\eta))} \text{BOP} \quad \frac{e^1 \Rightarrow (\underline{e}^1, \bar{e}^1) \quad e^2 \Rightarrow (\underline{e}^2, \bar{e}^2) \quad e^1 * e^2 < 0}{e^1 * e^2 \Rightarrow ((\bar{e}^1 * \bar{e}^2)(1+\eta), \frac{\underline{e}^1 * \underline{e}^2}{(1+\eta)})} \text{BOP-NEG} \\
\\
\frac{e \Rightarrow (\underline{e}, \bar{e}) \quad \circ(e) \geq 0}{\circ(e) \Rightarrow (\frac{\circ(\underline{e})}{(1+\eta)}, (\circ(\bar{e}))(1+\eta))} \text{UOP} \quad \frac{e \Rightarrow (\underline{e}, \bar{e}) \quad \circ(e) < 0}{\circ(e) \Rightarrow ((\circ(\underline{e}))(1+\eta), \frac{\circ(\bar{e})}{(1+\eta)})} \text{UOP-NEG}
\end{array}$$

Figure 5: Semantics of Transition for Expressions with Relative Floating Point Error

$$\frac{\text{fl}(r) = c}{r \Downarrow c} \text{FVAL} \qquad \frac{e^1 \Downarrow c^1 \quad e^2 \Downarrow c^2 \quad \text{fl}(c^1 * c^2) = c}{e^1 * e^2 \Downarrow c} \text{FBOP} \qquad \frac{e \Downarrow c', \quad \text{fl}(\circ(c')) = c}{\circ(e) \Downarrow c} \text{FUOP}$$

Figure 6: Semantics of Evaluation in Floating Point Computation

7 Semantics - V1

The transition semantics with relative floating point computation error are shown in Figure. 5. The semantics are $e \Rightarrow (err)$, which means a real expression e can be transited in floating point computation with error bound err , η is the machine epsilon.

We assume the SAMPLE and F(D) semantics for floating point and real computation are the same. $\mu \Downarrow_{\$} v$ represents v is sampled from the distribution μ .

Theorem 3 (Soundness Theorem)

Given e where the transition $e \Rightarrow (\underline{e}, \bar{e})$ holds, then if e evaluates to c in floating point computation and

$$\begin{array}{c}
\frac{}{r \Downarrow r} \text{RVAL} \qquad \frac{e^1 \Downarrow r^1 \quad e^2 \Downarrow r^2 \quad r^1 * r^2 = r}{e^1 * e^2 \Downarrow r} \text{RBOP} \qquad \frac{e \Downarrow r', \quad \circ(r') = r}{\circ(e) \Downarrow r} \text{RUOP} \\
\\
\frac{c \leftarrow \mu^{\diamond}}{\leftarrow^{\$} \mu \Downarrow c} \text{SAMPLE} \qquad \frac{f(D) = c}{f(D) \Downarrow c} \text{F(D)}
\end{array}$$

Figure 7: Semantics of Evaluation in Real Computation

\underline{e} and \bar{e} evaluates to \underline{r} and \bar{r} in real computation, we have:

$$\underline{r} \leq c \leq \bar{r}$$

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.