Verifying Snapping Mechanism - Floating Point Implementation Version

Jiawen Liu

March 22, 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 $\mathcal{L}_\epsilon \colon \mathbb{R} \to \mathsf{Distr}(\mathbb{R})$ 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 - IMP

Programs	p	::=	$x = e \mid x \xleftarrow{\$} \mu \mid p; p$
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	$\circ$	::=	$\ln \mid - \mid \lfloor \cdot \rceil \mid \mathsf{clamp}_B(\cdot)$
Value	v	::=	$r \mid c$
Distribution	μ	::=	$\mathsf{laplce} \mid \mathsf{unif} \mid \mathtt{bernoulli}$
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. 1 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.

$$\frac{\Theta(x) = (e, (\underline{e}, \bar{e}))}{\Theta, x \Rightarrow (e, (\underline{e}, \bar{e}))}\ \textsc{Var} \qquad \frac{r \geq 0}{\Theta, r \Rightarrow \big(r, (\frac{r}{(1+\eta)}, r(1+\eta))\big)}\ \textsc{Val} \qquad \frac{c = \texttt{fl}(r) \qquad r < 0}{\Theta, r \Rightarrow \big(r, (r(1+\eta), \frac{r}{(1+\eta)})\big)}\ \textsc{Val-Neg}$$

$$\frac{r = \texttt{fl}(r)}{\Theta, r \Rightarrow (r, (r, r))}\ \textsc{Val-Eq} \qquad \frac{}{\Theta, f(D) \Rightarrow (f(D), (f(D), f(D)))}\ \textsc{F(D)}$$

$$\frac{\Theta, e^1 \Rightarrow (e, (\underline{e^1}, \bar{e^1})) \quad \Theta, e^2 \Rightarrow (e, (\underline{e^2}, \bar{e^2})) \quad \bar{e}, \underline{e} = \max, \min(\underline{e^1} * \underline{e^2}, \bar{e^1} * \underline{e^2}, \underline{e^1} * \bar{e^2}, \bar{e^1} * \bar{e^2}) \quad e^1 * e^2 \geq 0}{\Theta, e^1 * e^2 \Rightarrow \big(e^1 * e^2, (\frac{\bar{e}}{(1+\eta)}, (\underline{e})(1+\eta))\big)}\ \textsc{Bop}$$

$$\frac{\Theta, e^1 \Rightarrow (e, (\underline{e^1}, \bar{e^1})) \quad \Theta, e^2 \Rightarrow (e, (\underline{e^2}, \bar{e^2})) \quad \bar{e}, \underline{e} = \max, \min(\underline{e^1} * \underline{e^2}, \bar{e^1} * \underline{e^2}, \underline{e^1} * \bar{e^2}, \bar{e^1} * \bar{e^2}) \quad e^1 * e^2 < 0}{\Theta, e^1 * e^2 \Rightarrow \big(e^1 * e^2, (\bar{e})(1+\eta), \frac{\underline{e}}{(1+\eta)}\big)}\ \textsc{Bop-Neg}$$

$$\frac{\Theta, e \Rightarrow (e, (\underline{e}, \bar{e})) \qquad \circ(e) \geq 0}{\Theta, \circ(e) \Rightarrow \Big(\circ(e), \big(\frac{\circ(\underline{e})}{(1+\eta)}, (\circ(\bar{e}))(1+\eta)\big)\Big)}\ \textsc{Uop} \qquad \frac{\Theta, e \Rightarrow (e, (\underline{e}, \bar{e})) \qquad \circ(e) < 0}{\Theta, \circ(e) \Rightarrow \Big(\circ(e), \big(\circ(\underline{e})(1+\eta), \frac{\circ(\bar{e})}{(1+\eta)}\big)\Big)}\ \textsc{Uop-Neg}$$

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

$$\frac{\Theta, e \Rightarrow (e, err)}{\Theta, x = e \Rightarrow \Theta[x \mapsto (e, err)]}\ \textsc{Asg} \qquad \frac{\Theta, p_1 \Rightarrow \Theta_1 \qquad \Theta_2, p_2 \Rightarrow \Theta_2}{\Theta, p_1; p_2 \Rightarrow \Theta_2}\ \textsc{Consq} \qquad \frac{c \leftarrow \mu^{\diamond}}{\Theta, x \xleftarrow{\$} \mu \Rightarrow \Theta[x \mapsto (c, (c, c))]}\ \textsc{Sample}$$

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

$$\frac{\texttt{fl}(r) = c}{r \Downarrow^{\mathbb{F}} c}\ \textsc{RVal} \qquad \frac{}{c \Downarrow^{\mathbb{F}} c}\ \textsc{FVal} \qquad \frac{e^1 \Downarrow^{\mathbb{F}} c^1 \quad e^2 \Downarrow^{\mathbb{F}} c^2 \quad \texttt{fl}(c^1 * c^2) = c}{e^1 * e^2 \Downarrow^{\mathbb{F}} c}\ \textsc{FBop} \qquad \frac{e \Downarrow^{\mathbb{F}} c', \quad \texttt{fl}(\circ(c')) = c}{\circ(e) \Downarrow^{\mathbb{F}} c}\ \textsc{FUop}$$

Figure 3: Semantics of Evaluation in Floating Point Computation

$$\frac{}{r \Downarrow^{\mathbb{R}} r}\ \textsc{RVal} \qquad \frac{}{c \Downarrow^{\mathbb{R}} c}\ \textsc{RVal} \qquad \frac{e^1 \Downarrow^{\mathbb{R}} r^1 \quad e^2 \Downarrow^{\mathbb{R}} r^2 \quad r^1 * r^2 = r}{e^1 * e^2 \Downarrow^{\mathbb{R}} r}\ \textsc{RBop} \qquad \frac{e \Downarrow^{\mathbb{R}} r', \quad \circ(r') = r}{\circ(e) \Downarrow^{\mathbb{R}} r}\ \textsc{RUop} \qquad \frac{f(D) = c}{f(D) \Downarrow c}\ \textsc{F(D)}$$

Figure 4: Semantics of Evaluation in Real Computation

Theorem 1 (Soundness Theorem)
For any p, if there exists a transition $\Theta, p \Rightarrow \Theta'$ and Θ is a bounded transaction environment (i.e., $\forall x \in dom(\Theta)$ s.t. $\Theta(x) = (e, (\underline{e}, \bar{e}))$, if $e \Downarrow^{\mathbb{F}} c$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r}$ and $\bar{e} \Downarrow^{\mathbb{R}} \bar{r}$, then $\underline{r} \leq c \leq \bar{r}$) , then $\forall x \in dom(\Theta')$ s.t. $\Theta'(x) = (e, (\underline{e}, \bar{e}))$, if $e \Downarrow^{\mathbb{F}} c$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r}$ and $\bar{e} \Downarrow^{\mathbb{R}} \bar{r}$, then:

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

Proof. Induction on transition rule of p, by assumption, we know Θ is a safe environment $(\star)$.

case

$$\frac{\Theta, p_1 \Rightarrow \Theta_1 \qquad \Theta_1, p_2 \Rightarrow \Theta_2}{\Theta, p_1; p_2 \Rightarrow \Theta_2}\ \textbf{CONSQ}$$

We need to show Θ_2 is a bounded environment.
Since we know Θ is a bounded environment by assumption $(\star)$, by induction hypothesis, we have:
Θ_1 and Θ_2 are all bounded environment. This case is proved.

case

$$\frac{c \leftarrow \mu^{\diamond}}{\Theta, x \xleftarrow{\$} \mu \Rightarrow \Theta[x \mapsto (c, (c, c))]}\ \textbf{SAMPLE}$$

We need to show $\Theta[x \mapsto (c, (c, c))]$ is a safe environment.
Since we know Θ is a safe environment by assumption $(\star)$. It is trivial that $c \leq c \leq c$. We can know $\Theta[x \mapsto (c, (c, c))]$ is also a safe environment.

case

$$\frac{\Theta, e \Rightarrow (e, err)}{\Theta, x = e \Rightarrow \Theta[x \mapsto (e, err)]}\ \textbf{ASG}$$

We need to show: $\Theta[x \mapsto (e, err)]$ is a safe environment.
By assumption $(\star)$ we know: Θ is already a safe environment. We still need to show:
Let $err = (\underline{e}, \bar{e})$, $e \Downarrow^{\mathbb{F}} c$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r}$ and $\bar{e} \Downarrow^{\mathbb{R}} \bar{r}$, $\underline{r} \leq c \leq \bar{r}$.
Induction on transition of e, we have:

subcase

$$\frac{\Theta(x) = (e, (\underline{e}, \bar{e}))}{\Theta, x \Rightarrow (e, (\underline{e}, \bar{e}))}\ \textbf{VAR}$$

By the assumption, we have $\forall x \in dom(\Theta)$ s.t. $\Theta(x) = (e, (\underline{e}, \bar{e}))$, $e \Downarrow^{\mathbb{F}} c$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r}$ and $\bar{e} \Downarrow^{\mathbb{R}} \bar{r}$, $\underline{r} \leq c \leq \bar{r}$. This case is proved.

subcase

$$\frac{r \geq 0}{\Theta, r \Rightarrow \left(r, \frac{r}{(1+\eta)}, r(1+\eta)\right)}\ \textbf{VAL}$$

By evaluation rule of floating point computation for r, we have:

$$\frac{\texttt{fl}(r) = c}{r \Downarrow^{\mathbb{F}} c} \text{ RVAL}$$

By the definition of floating point rounding error and $r \geq 0$, we have: $\frac{r}{(1+\eta)} \leq c \leq r(1+\eta)$

subcase

$$\frac{c = \texttt{fl}(r) \qquad r < 0}{\Theta, r \Rightarrow \left(r, r(1+\eta), \dfrac{r}{(1+\eta)}\right)} \textbf{ VAL-NEG}$$

By evaluation rule of floating point computation for r, we have:

$$\frac{\texttt{fl}(r) = c}{r \Downarrow^{\mathbb{F}} c} \text{ RVAL}$$

By the definition of floating point rounding error and $r < 0$, we have: $r(1+\eta) \leq c \leq \frac{r}{(1+\eta)}$

subcase

$$\frac{r = \texttt{fl}(r)}{\Theta, r \Rightarrow (r, r, r)} \textbf{ VAL-EQ}$$

Given $r \Downarrow^{\mathbb{F}} c$, it is trivial to show $r \leq c = \texttt{fl}(r) = r \leq r$

subcase

$$\frac{}{\Theta, f(D) \Rightarrow (f(D), (f(D), f(D)))} \textbf{ F(D)}$$

Given $f(D) \Downarrow c$ in both floating point and real computation, it is trivial to show $c \leq c \leq c$

subcase

$$\frac{\begin{array}{c}\Theta, e^1 \Rightarrow (e, (\underline{e}^1, \bar{e}^1))\ (\diamond) \qquad \Theta, e^2 \Rightarrow (e, (\underline{e}^2, \bar{e}^2))\ (\triangle) \\ \bar{e}, \underline{e} = \max, \min(\underline{e}^1 * \underline{e}^2, \bar{e}^1 * \underline{e}^2, \underline{e}^1 * \bar{e}^2, \bar{e}^1 * \bar{e}^2) \qquad e^1 * e^2 \geq 0\ (\square)\end{array}}{\Theta, e^1 * e^2 \Rightarrow \left(e^1 * e^2, (\dfrac{\underline{e}}{(1+\eta)}, (\bar{e})(1+\eta))\right)} \textbf{ BOP}$$

We need to show: for $e^1 * e^2 \Downarrow^{\mathbb{F}} c$, $\frac{\underline{e}}{(1+\eta)} \Downarrow^{\mathbb{R}} \underline{r}$ and $(\bar{e})(1+\eta) \Downarrow^{\mathbb{R}} \bar{r}$, the $\underline{r} \leq c \leq \bar{r}$ holds.
By induction hypothesis on $(\diamond)$ and $(\triangle)$, we have:
(1) for $e^1 \Downarrow^{\mathbb{F}} c_1$, $\underline{e}^1 \Downarrow^{\mathbb{R}} \underline{r_1}$ and $\bar{e}^1 \Downarrow^{\mathbb{R}} \bar{r}_1$, the $\underline{r_1} \leq c_1 \leq \bar{r}_1$ holds.
(2) for $e^2 \Downarrow^{\mathbb{F}} c_2$, $\underline{e}^2 \Downarrow^{\mathbb{R}} \underline{r_2}$ and $\bar{e}^2 \Downarrow^{\mathbb{R}} \bar{r}_2$, the $\underline{r_2} \leq c_2 \leq \bar{r}_2$ holds.
Let $\bar{r}' = \min(\bar{r}_2 * \bar{r}_1, \underline{r_2} * \bar{r}_1, \bar{r}_2 * \underline{r_1}, \underline{r_2} * \underline{r_1})$ and $\underline{r}' = \max(\bar{r}_2 * \bar{r}_1, \underline{r_2} * \bar{r}_1, \bar{r}_2 * \underline{r_1}, \underline{r_2} * \underline{r_1})$
By (1) and (2), we have: $\underline{r}' \leq c_2 * c_1 \leq \bar{r}'$.
By hypothesis $(\square)$ and relative error of floating point rounding, we have:
$\frac{\underline{r}'}{1+\eta} \leq \texttt{fl}(c_2 * c_1) \leq (\bar{r}')(1+\eta)$.
By evaluation rule FBOP and RBOP, we have:
$e^1 * e^2 \Downarrow^{\mathbb{F}} \texttt{fl}(c_2 * c_1)$, $\frac{\underline{e}}{(1+\eta)} \Downarrow^{\mathbb{R}} \frac{\underline{r}'}{1+\eta}$ and $(\bar{e})(1+\eta) \Downarrow^{\mathbb{R}} (\bar{r}')(1+\eta)$.
This case is proved.

subcase

$$\dfrac{\begin{array}{c}\Theta, e^1 \Rightarrow (e, (\underline{e^1}, \bar{e^1})) \qquad \Theta, e^2 \Rightarrow (e, (\underline{e^2}, \bar{e^2})) \\ \bar{e}, \underline{e} = \max, \min(\underline{e^1} * \underline{e^2}, \bar{e^1} * \underline{e^2}, \underline{e^1} * \bar{e^2}, \bar{e^1} * \bar{e^2}) \qquad e^1 * e^2 < 0\end{array}}{\Theta, e^1 * e^2 \Rightarrow \left(e^1 * e^2, (\bar{e})(1+\eta), \dfrac{\underline{e}}{(1+\eta)}\right)} \textbf{ BOP-NEG}$$

We need to show: for $e^1 * e^2 \Downarrow^{\mathbb{F}} c$, $(\underline{e})(1+\eta) \Downarrow^{\mathbb{R}} \underline{r}$ and $\frac{\bar{e}}{(1+\eta)} \Downarrow^{\mathbb{R}} \bar{r}$, the $\underline{r} \leq c \leq \bar{r}$ holds.
By induction hypothesis on $(\diamond)$ and $(\triangle)$, we have:
(1) for $e^1 \Downarrow^{\mathbb{F}} c_1$, $\underline{e^1} \Downarrow^{\mathbb{R}} \underline{r_1}$ and $\bar{e^1} \Downarrow^{\mathbb{R}} \bar{r}_1$, the $\underline{r_1} \leq c_1 \leq \bar{r}_1$ holds.
(2) for $e^2 \Downarrow^{\mathbb{F}} c_2$, $\underline{e^2} \Downarrow^{\mathbb{R}} \underline{r_2}$ and $\bar{e^2} \Downarrow^{\mathbb{R}} \bar{r}_2$, the $\underline{r_2} \leq c_2 \leq \bar{r}_2$ holds.
Let $\bar{r'} = \min(\bar{r}_2 * \bar{r}_1, \underline{r_2} * \bar{r}_1, \bar{r}_2 * \underline{r_1}, \underline{r_2} * \underline{r_1})$ and $\underline{r'} = \max(\bar{r}_2 * \bar{r}_1, \underline{r_2} * \bar{r}_1, \bar{r}_2 * \underline{r_1}, \underline{r_2} * \underline{r_1})$
By (1) and (2), we have: $\underline{r'} \leq c_2 * c_1 \leq \bar{r'}$.
By hypothesis $(\square)$ and relative error of floating point rounding, we have:
$\underline{r'}(1+\eta) \leq \mathtt{fl}(c_2 * c_1) \leq \frac{\bar{r'}}{1+\eta}$.
By evaluation rule FBOP and RBOP, we have:
$e^1 * e^2 \Downarrow^{\mathbb{F}} \mathtt{fl}(c_2 * c_1)$, $\underline{e}(1+\eta) \Downarrow^{\mathbb{R}} \underline{r'}(1+\eta)$ and $\frac{\bar{e}}{(1+\eta)} \Downarrow^{\mathbb{R}} \frac{\bar{r'}}{1+\eta}$.
This case is proved.

subcase

$$\dfrac{\Theta, e \Rightarrow (e, \underline{e}, \bar{e}) \ (\diamond) \qquad \circ(e) \geq 0 \ (\square)}{\Theta, \circ(e) \Rightarrow \left(\circ(e), \dfrac{\circ(\underline{e})}{(1+\eta)}, (\circ(\bar{e}))(1+\eta)\right)} \textbf{ UOP}$$

We need to show: for $\circ(e) \Downarrow^{\mathbb{F}} c$, $\frac{\circ(\underline{e})}{(1+\eta)} \Downarrow^{\mathbb{R}} \underline{r}$ and $\circ(\bar{e})(1+\eta) \Downarrow^{\mathbb{R}} \bar{r}$, the $\underline{r} \leq c \leq \bar{r}$ holds.
By induction hypothesis on $(\diamond)$, we have:
(1) for $e \Downarrow^{\mathbb{F}} c'$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r'}$ and $\bar{e} \Downarrow^{\mathbb{R}} \bar{r'}$, the $\underline{r'} \leq c \leq \bar{r'}$ holds.
By (1) and monotone of unary operations, we have: $\circ(\underline{r'}) \leq \circ(c') \leq \circ(\bar{r'})$.
By hypothesis $(\square)$ and relative error of floating point rounding, we have:
$\frac{\circ(\underline{r'})}{1+\eta} \leq \mathtt{fl}(\circ(c')) \leq \circ(\bar{r'})(1+\eta)$.
By evaluation rule FBOP and RBOP, we have:
$\circ(c') \Downarrow^{\mathbb{F}} \mathtt{fl}(\circ(c'))$, $\frac{\circ(\underline{e})}{1+\eta} \Downarrow^{\mathbb{R}} \frac{\circ(\underline{r'})}{1+\eta}$ and $\circ(\bar{e})(1+\eta) \Downarrow^{\mathbb{R}} \circ(\bar{r'})(1+\eta)$.
This case is proved.

subcase

$$\dfrac{\Theta, e \Rightarrow (e, \underline{e}, \bar{e}) \qquad \circ(e) < 0}{\Theta, \circ(e) \Rightarrow \left(\circ(e), (\circ(\underline{e}))(1+\eta), \dfrac{\circ(\bar{e})}{(1+\eta)}\right)} \textbf{ UOP-NEG}$$

We need to show: for $\circ(e) \Downarrow^{\mathbb{F}} c$, $\circ(\underline{e})(1+\eta) \Downarrow^{\mathbb{R}} \underline{r}$ and $\frac{\circ(\bar{e})}{(1+\eta)} \Downarrow^{\mathbb{R}} \bar{r}$, the $\underline{r} \leq c \leq \bar{r}$ holds.
By induction hypothesis on $(\diamond)$, we have:
(1) for $e \Downarrow^{\mathbb{F}} c'$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r'}$ and $\bar{e} \Downarrow^{\mathbb{R}} \bar{r'}$, the $\underline{r'} \leq c \leq \bar{r'}$ holds.
By (1) and monotone of unary operations, we have: $\circ(\underline{r'}) \leq \circ(c') \leq \circ(\bar{r'})$.
By hypothesis $(\square)$ and relative error of floating point rounding, we have:
$\circ(\underline{r'})(1+\eta) \leq \mathtt{fl}(\circ(c')) \leq \frac{\circ(\bar{r'})}{1+\eta}$.
By evaluation rule FBOP and RBOP, we have:
$\circ(c') \Downarrow^{\mathbb{F}} \mathtt{fl}(\circ(c'))$, $\circ(\underline{e})(1+\eta) \Downarrow^{\mathbb{R}} \circ(\underline{r'})(1+\eta)$ and $\frac{\circ(\bar{e})}{1+\eta} \Downarrow^{\mathbb{R}} \frac{\circ(\bar{r'})}{1+\eta}$.
Let $c = \mathtt{fl}(\circ(c'))$, $\underline{r} = \circ(\underline{r'})(1+\eta)$ and $\bar{r} = \frac{\circ(\bar{r'})}{1+\eta}$, this case is proved.

□

4 Snapping Mechanism

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

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

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 $\mathsf{Snap}'(a)$ be the same as $\mathsf{Snap}(a)$ given U, S without rounding and clamping steps, i.e., $\mathsf{Snap}'(a)$: $y = f(a) + S \times \ln(U) \div \epsilon$.
Let $\mathsf{Snap}''(a)$ be the same as $\mathsf{Snap}(a)$ given U, S, i.e., $\mathsf{Snap}''(a) : \mathsf{Snap}'(a); z = \mathsf{clamp}_B\big(\lfloor y \rceil_\Lambda\big)$.

5 Main Theorem

Theorem 2 (The Snap mechanism is ϵ−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 $\epsilon + 23B\epsilon\eta$

Proof. Given $\mathsf{Snap}(a) = x$ 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 $\mathsf{Snap}(a)$ mechanism.

Consider the $\mathsf{Snap}(a)$ outputting the same result x under floating point and real computaion, let (L, R) be the range where $\forall u \in (L, R)$ and some s s.t. $[U \mapsto u, S \mapsto s], \mathsf{Snap}''(a) \Downarrow^{\mathbb{R}} [z \mapsto x]$, we have $\Pr[\mathsf{Snap}(a) = x] = R - L$. Sice the $\mathsf{Snap}(a)$ is ϵ−DP, we have:

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

Let (l, r) be the range where $\forall u \in (l, r)$ and some s s.t.:

$$[U \mapsto u, S \mapsto s], \mathsf{Snap}''(a) \Downarrow^{\mathbb{F}} [z \mapsto x].$$

We estimate the worst case $|r - l|$ in terms of floating point relative error and $|R - L|$ through our semantics in order to verify the privacy loss of Snap.

case $x = -B$

Let b be the largest number rounded by Λ that is smaller than B, $b' = b - \Lambda/2$.
Let L and R be the range where $\forall u \in (L, R)$, $[U \mapsto u, S \mapsto s], \mathsf{Snap}''(a) \Downarrow^{\mathbb{F}} [z \mapsto x]$ and $[U \mapsto u, S \mapsto s], \mathsf{Snap}''(a) \Downarrow^{\mathbb{R}} [z \mapsto x]$.
So we know $s = 1$, $L = 0$, $[U \mapsto R, S \mapsto 1], \mathsf{Snap}'(a) \Downarrow^{\mathbb{F}} [y \mapsto -b']$ and $[U \mapsto R, S \mapsto 1], \mathsf{Snap}'(a) \Downarrow^{\mathbb{R}} [y \mapsto -b']$.
We need to estimate the worst case range of R in this case. The derivation of this case given $\Theta = [U \mapsto (R, (R, R)), S \mapsto (1, (1, 1))]$ is shown as following:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Theta, U \Rightarrow (R, (\underline{R}, \bar{R}))}\ \textsc{val-eq}}{\Theta, \ln(U) \Rightarrow (\ln(R), \ln(\underline{R})(1+\eta), \dfrac{\ln(\bar{R})}{(1+\eta)})}\ \textsc{uop}}{\Theta, \frac{1}{\epsilon} \times \ln(U) \Rightarrow (\frac{1}{\epsilon} \times \ln(R), ((\frac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2, \dfrac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2}))}\ \textsc{bop}}{\Theta, f(a) + \frac{1}{\epsilon} \times \ln(U) \Rightarrow \Big(f(a) + \frac{1}{\epsilon} \times \ln(R), \big((f(a) + (\frac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2)(1+\eta), \dfrac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})}{(1+\eta)}\big)\Big)}\ \textsc{bop}}{\Theta, \mathsf{Snap}'(a) \Rightarrow \Theta[y \mapsto \Big(f(a) + \frac{1}{\epsilon} \times \ln(R), \big((f(a) + (\frac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2)(1+\eta), \dfrac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})}{(1+\eta)}\big)\Big)]}\ \textsc{id}$$

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

$$\dfrac{\cdots}{\Theta, \mathsf{Snap}'(a'); \mathsf{Snap}'' \Rightarrow \Theta[y \mapsto \Big(\mathsf{Snap}'(a'), \big((f(a') + (\frac{1}{\epsilon} \times \ln(\underline{R}'))(1+\eta)^2)(1+\eta), \dfrac{(f(a') + \frac{\frac{1}{\epsilon}\times\ln(\bar{R}')}{(1+\eta)^2})}{(1+\eta)}\big)\Big)]}$$

Given $\mathsf{Snap}(a') \Downarrow^{\mathbb{F}} -b'$, $\mathsf{Snap}(a) \Downarrow^{\mathbb{F}} -b'$, we have the worst case lower and upper bounds for R and R', which are $\underline{R}, \bar{R}, \underline{R}'$ and $\bar{R}'$:

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

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

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

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:

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

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

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

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

$$\dfrac{\text{ID}\ \dfrac{\text{OP}\ \dfrac{\text{OP}\ \dfrac{\dfrac{}{R \Rightarrow (R,(R,R))}\ \text{VAL-EQ}}{\ln(R) \Rightarrow (\ln(R), (\ln(R)(1+\eta), \dfrac{\ln(R)}{(1+\eta)}))}}{\dfrac{1}{\epsilon}\times\ln(R) \Rightarrow \big(\dfrac{1}{\epsilon}\times\ln(R), ((\dfrac{1}{\epsilon}\times\ln(R))(1+\eta)^2, \dfrac{\frac{1}{\epsilon}\times\ln(R)}{(1+\eta)^2})\big)}}{f(a)+\dfrac{1}{\epsilon}\times\ln(R) \Rightarrow \Big(f(a)+\dfrac{1}{\epsilon}\times\ln(R), \Big(\big(f(a)+(\dfrac{1}{\epsilon}\times\ln(R))(1+\eta)^2\big)(1+\eta), \dfrac{(f(a)+\frac{\frac{1}{\epsilon}\times\ln(R)}{(1+\eta)^2})}{(1+\eta)}\Big)\Big)}}{\mathsf{Snap}'(a) \Rightarrow (\mathsf{Snap}'(a), (e^1, e^2))}$$

From soundness theorem, we have $e^1 \le y_2 \le e^2$, where we can get $\underline{R} \le r \le \bar{R}$.
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: $\bar{R} = e^{\epsilon\frac{(\frac{y_1}{1+\eta}-f(a))}{(1+\eta)^2}}$.

$$\frac{\dfrac{\dots}{\mathsf{Snap}'(a) \Rightarrow (\mathsf{Snap}'(a), \Big(\dfrac{f(a)+(\frac{1}{\epsilon}\times\ln(\underline{L}))(1+\eta)^2}{1+\eta}, (f(a)+\dfrac{\frac{1}{\epsilon}\times\ln(\bar{L})}{(1+\eta)^2})(1+\eta))\Big)}}{\mathsf{Snap}'(a) \Rightarrow (\mathsf{Snap}'(a), (err_1, err_2))}$$

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:

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

Then, we can derive:

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

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:

$$\cfrac{\cfrac{\cfrac{\cfrac{L \Rightarrow (L, (\underline{L}, \bar{L}))}{\ln(L) \Rightarrow (\ln(L), (\ln(\underline{L})(1+\eta), \frac{\ln(\bar{L})}{(1+\eta)}))}}{\frac{1}{\epsilon} \times \ln(L) \Rightarrow \left(\frac{1}{\epsilon} \times \ln(L), ((\frac{1}{\epsilon} \times \ln(\underline{L}))(1+\eta)^2, \frac{\frac{1}{\epsilon} \times \ln(\bar{L})}{(1+\eta)^2})\right)}}{f(a) + \frac{1}{\epsilon} \times \ln(L) \Rightarrow \left(f(a) \oplus \frac{1}{\epsilon} \otimes \text{ⓛⓝ}(l), (\frac{f(a) + (\frac{1}{\epsilon} \times \ln(\underline{L}))(1+\eta)^2}{1+\eta}, (f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{L})}{(1+\eta)^2})(1+\eta))\right)}}{\mathsf{Snap}'(a) \Rightarrow (\mathsf{Snap}'(a), (err_1, err_2))}$$

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

$$\cfrac{\cfrac{\cdots}{\mathsf{Snap}'(a) \Rightarrow \mathsf{Snap}'(a), (\frac{f(a) + (\frac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2}{1+\eta}, (f(a) + \frac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})(1+\eta))}}{\mathsf{Snap}'(a) \Rightarrow \mathsf{Snap}'(a), (err_1, err_2)}$$

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 $\mathsf{Snap}'(a', l, 1)$ and $\mathsf{Snap}'(a', r, 1)$:

$$\cfrac{\cdots}{\mathsf{Snap}'(a', L', 1) \Rightarrow \mathsf{Snap}'(a', l', 1), (\frac{f(a') + (\frac{1}{\epsilon} \times \ln(\underline{L}'))(1+\eta)^2}{1+\eta}, (f(a') + \frac{\frac{1}{\epsilon} \times \ln(\bar{L}')}{(1+\eta)^2})(1+\eta))}$$

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

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

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

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

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 $\mathsf{Snap}(a)$ 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:

$$\frac{\dots}{\dfrac{\mathsf{Snap}'(a) \Rightarrow \mathsf{Snap}'(a), (\dfrac{f(a) + (\frac{1}{\epsilon} \times \ln(\underline{L}))(1+\eta)^2}{1+\eta}, (f(a) + \dfrac{\frac{1}{\epsilon} \times \ln(\bar{L})}{(1+\eta)^2})(1+\eta))}{\mathsf{Snap}'(a) \Rightarrow \mathsf{Snap}'(a), (err_1, err_2)}}$$

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

$$\frac{\dots}{\dfrac{\mathsf{Snap}'(a) \Rightarrow \mathsf{Snap}'(a), (\dfrac{f(a) + (\frac{1}{\epsilon} \times \ln(\underline{R}))(1+\eta)^2}{1+\eta}, (f(a) + \dfrac{\frac{1}{\epsilon} \times \ln(\bar{R})}{(1+\eta)^2})(1+\eta))}{\mathsf{Snap}'(a) \Rightarrow (\mathsf{Snap}'(a), (err_1, err_2))}}$$

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

$$
\begin{array}{c}
R \Rightarrow r, (R, R) \\
\hline
\ln(R) \Rightarrow ⓛ(r), (\ln(R)(1+\eta), \dfrac{\ln(R)}{1+\eta}) \\
\hline
\dfrac{1}{\epsilon}\ln(R) \Rightarrow \dfrac{1}{\epsilon} \otimes ⓛ(r), (\dfrac{1}{\epsilon}\ln(R)(1+\eta)^2, \dfrac{1}{\epsilon}\dfrac{\ln(R)}{(1+\eta)^2}) \\
\hline
f(a) + \dfrac{1}{\epsilon}\ln(R) \Rightarrow f(a) \oplus \dfrac{1}{\epsilon} \otimes ⓛ(r), \Big((f(a) + \dfrac{1}{\epsilon}\ln(R)(1+\eta)^2)(1+\eta), (f(a) + \dfrac{1}{\epsilon}\dfrac{\ln(R)}{(1+\eta)^2})/(1+\eta)\Big) \\
\hline
\mathsf{Snap}'(a) \Rightarrow \mathsf{Snap}'(a), (err_1, err_2)
\end{array}
$$

From soundness theorem, we have $err_1 \leq y_2 \leq err_2$. Then we can get following bounds for r:
$\underline{R}_+ = e^{\epsilon\left((y_2(1+\eta) - f(a))(1+\eta)^2\right)}$, $\bar{R}_+ = e^{\epsilon\frac{(\frac{y_2}{1+\eta} - f(a))}{(1+\eta)^2}}$.
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 $\boldsymbol{x \in (\lfloor f(a) \rceil_\Lambda, \lfloor f(a') \rceil_\Lambda)}$

Since the output set $(\lfloor f(a) \rceil_\Lambda, \lfloor f(a') \rceil_\Lambda)$ 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., $\lfloor f(a') \rceil_\Lambda) < 0$. The bounds derived for l, r and l', r' under input a and a' are as follows:

For input a:

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

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

For input a':

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

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

The bounds on their ratio are as follows:

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

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

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:

$$\dfrac{\dfrac{\dfrac{\dfrac{R'_+ \Rightarrow r_+, (R'_+, R'_+)}{\ln(R'_+) \Rightarrow ⓛⓝ(r_+), (\ln(R'_+)(1+\eta), \frac{\ln(R'_+)}{1+\eta})}}{\frac{1}{\epsilon}\ln(R) \Rightarrow \frac{1}{\epsilon} \otimes ⓛⓝ(r_+), \left(\frac{1}{\epsilon}\ln(R'_+)(1+\eta)^2, \frac{1}{\epsilon}\frac{\ln(R'_+)}{(1+\eta)^2}\right)}}{f(a) + \frac{1}{\epsilon}\ln(R'_+) \Rightarrow f(a) \oplus \frac{1}{\epsilon} \otimes ⓛⓝ(r_+), \left((f(a) + \frac{1}{\epsilon}\ln(R'_+)(1+\eta)^2)(1+\eta), (f(a) + \frac{1}{\epsilon}\frac{\ln(R'_+)}{(1+\eta)^2})/(1+\eta)\right)}}{\mathsf{Snap}'(a) \Rightarrow (\mathsf{Snap}'(a), (err_1, err_2))}$$

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

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

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:
$\underline{L'_-} = e^{\epsilon\left((f(a') - y_2(1+\eta))(1+\eta)^2)\right)}$, $\bar{L'_-} = e^{\epsilon \frac{(f(a') - \frac{y_2}{1+\eta})}{(1+\eta)^2}}$.
$\underline{R'_-} = e^{\epsilon\left((f(a') - y_1(1+\eta))(1+\eta)^2)\right)}$, $\bar{R'_-} = e^{\epsilon \frac{(f(a') - \frac{y_1}{1+\eta})}{(1+\eta)^2}}$.
Since $y_1 = \lfloor f(a') \rceil - \frac{\Lambda}{2}$, we have $e^{\epsilon\left((f(a') - y_1))\right)} > 1$, so actually we know $R'_- = r'_- = 1$.
For input a, we have only one case where $s = -1$, the following bound can be derived:
$\underline{R} = e^{\epsilon\left(f(a) - (y_2(1+\eta))(1+\eta)^2)\right)}$, $\bar{R} = e^{\epsilon \frac{(f(a) - \frac{y_2}{1+\eta})}{(1+\eta)^2}}$.
$\underline{L} = e^{\epsilon\left((f(a) - y_1(1+\eta))(1+\eta)^2)\right)}$, $\bar{L} = e^{\epsilon \frac{f(a) - \frac{y_1}{1+\eta}}{(1+\eta)^2}}$.
We have following bounds on their ratios:

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

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:

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

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 $\boldsymbol{\lfloor f(a') \rceil_\Lambda > 0 \lor \lfloor f(a') \rceil_\Lambda < 0 \land x \in (0, B)}$
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':
$\underline{R'} = e^{\epsilon\left((f(a') - \frac{y_2}{1+\eta})(1+\eta)^2)\right)}$, $\bar{R'} = e^{\epsilon \frac{(f(a') - y_2(1+\eta))}{(1+\eta)^2}}$.
$\underline{L'} = e^{\epsilon\left((f(a') - \frac{y_1}{1+\eta}))(1+\eta)^2)\right)}$, $\bar{L'} = e^{\epsilon \frac{(f(a') - y_1(1+\eta)}{(1+\eta)^2}}$.
For input a:
$\underline{R} = e^{\epsilon\left((f(a) - \frac{y_2}{1+\eta})(1+\eta)^2)\right)}$, $\bar{R} = e^{\epsilon \frac{(f(a) - y_2(1+\eta))}{(1+\eta)^2}}$.
$\underline{L} = e^{\epsilon\left((f(a) - \frac{y_1}{1+\eta})(1+\eta)^2)\right)}$, $\bar{L} = e^{\epsilon \frac{f(a) - y_1(1+\eta)}{(1+\eta)^2}}$. 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 $|\bar{R}' - \underline{L}'|$ are as follows:

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

So we have the privacy loss is bounded by:

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

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:

For input a':

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

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

For input a:

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

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

The bounds on their ratio are as follows:

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

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:

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

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:

For input a':

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

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

For input a:

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

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

The bounds on their ratio are as follows:

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

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 $\boldsymbol{x = B}$

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 $\mathsf{Snap}(a)$ 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:

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

□

6 Syntax - Functional

Following are the syntax of our system:

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

$$\frac{r \geq 0}{r \Rightarrow \left(\frac{r}{(1+\eta)}, r(1+\eta)\right)}\ \text{VAL} \qquad \frac{r < 0}{r \Rightarrow \left(r(1+\eta), \frac{r}{(1+\eta)}\right)}\ \text{VAL-NEG} \qquad \frac{r = \mathtt{fl}(r)}{r \Rightarrow (r, r)}\ \text{VAL-EQ}$$

$$\frac{}{f(D) \Rightarrow (f(D), f(D))}\ \text{F(D)} \qquad \frac{}{\overset{\$}{\leftarrow} \mu \Rightarrow (\overset{\$}{\leftarrow} \mu, \overset{\$}{\leftarrow} \mu)}\ \text{SAMPLE}$$

$$\frac{e^1 \Rightarrow (\underline{e}^1, \bar{e}^1) \qquad e^2 \Rightarrow (\underline{e}^2, \bar{e}^2) \qquad e^1 * e^2 \geq 0}{e^1 * e^2 \Rightarrow \left(\frac{\underline{e}^1 * \underline{e}^2}{(1+\eta)}, (\bar{e}^1 * \bar{e}^2)(1+\eta)\right)}\ \text{BOP} \qquad \frac{e^1 \Rightarrow (\underline{e}^1, \bar{e}^1) \qquad e^2 \Rightarrow (\underline{e}^2, \bar{e}^2) \qquad e^1 * e^2 < 0}{e^1 * e^2 \Rightarrow \left((\bar{e}^1 * \bar{e}^2)(1+\eta), \frac{\underline{e}^1 * \underline{e}^2}{(1+\eta)}\right)}\ \text{BOP-NEG}$$

$$\frac{e \Rightarrow (\underline{e}, \bar{e}) \qquad \circ(e) \geq 0}{\circ(e) \Rightarrow \left(\frac{\circ(\underline{e})}{(1+\eta)}, (\circ(\bar{e}))(1+\eta)\right)}\ \text{UOP} \qquad \frac{e \Rightarrow (\underline{e}, \bar{e}) \qquad \circ(e) < 0}{\circ(e) \Rightarrow \left((\circ(\underline{e}))(1+\eta), \frac{\circ(\bar{e})}{(1+\eta)}\right)}\ \text{UOP-NEG}$$

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

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

Figure 6: Semantics of Evaluation in Floating Point Computation

7 Semantics - Functional

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

$$\frac{}{r \Downarrow r}\ \text{RVAL} \qquad \frac{e^1 \Downarrow r^1 \qquad e^2 \Downarrow r^2 \qquad r^1 * r^2 = r}{e^1 * e^2 \Downarrow r}\ \text{RBOP} \qquad \frac{e \Downarrow r', \qquad \circ(r') = r}{\circ(e) \Downarrow r}\ \text{RUOP}$$

$$\frac{c \leftarrow \mu^{\diamond}}{\overset{\$}{\leftarrow} \mu \Downarrow c}\ \text{SAMPLE} \qquad \frac{f(D) = c}{f(D) \Downarrow c}\ \text{F(D)}$$

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.