athm.8em1 2 (3)

athm
Transaction Env. $::= \cdot \mid [x \mapsto (,)]$

undefined
kslashchar $symbols110largesymbols178$
@bb
@bb ifpackageloadedamsmath ifpackageloadedamsfonts

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

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

2 Syntax - IMP

Programs	p	$::=$	$x = e \mid x \leftarrow \mu \mid p\, p$
Expr.	e	$::=$	$r \mid c \mid x \mid f\mathrm{D} \mid e * e \mid \circ e$
Binary Operation	$*$	$::=$	$+ \mid - \mid \times \mid \div$
Unary Operation	$\circ$	$::=$	$\mid - \mid \lfloor \cdot \rceil \mid \mathsf{clamp}_{\mathrm{B}} \cdot$
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.

$$\frac{\Theta x = e, \underline{e}, e}{\Theta, x \Rightarrow e, \underline{e}, e}\ \textsc{VAR} \qquad \frac{r \geq}{\Theta, r \Rightarrow \left(r, \frac{r}{+\eta}, r+\eta\right)}\ \textsc{VAL} \qquad \frac{c = \texttt{fl}\, r \qquad r <}{\Theta, r \Rightarrow \left(r, r+\eta, \frac{r}{+\eta}\right)}\ \textsc{VAL-NEG}$$

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

$$\frac{\Theta, e \Rightarrow e, \underline{e}, e \quad \Theta, e \Rightarrow e, \underline{e}, e \quad e, \underline{e} = , \underline{e} * \underline{e}, e * \underline{e}, \underline{e} * e, e * e \quad e * e \geq}{\Theta, e * e \Rightarrow \left(e * e, \frac{e}{+\eta}, \underline{e} + \eta\right)}\ \textsc{BOP}$$

$$\frac{\Theta, e \Rightarrow e, \underline{e}, e \quad \Theta, e \Rightarrow e, \underline{e}, e \quad e, \underline{e} = , \underline{e} * \underline{e}, e * \underline{e}, \underline{e} * e, e * e \quad e * e <}{\Theta, e * e \Rightarrow \left(e * e, e + \eta, \frac{\underline{e}}{+\eta}\right)}\ \textsc{BOP-NEG}$$

$$\frac{\Theta, e \Rightarrow e, \underline{e}, e \qquad \circ e \geq}{\Theta, \circ e \Rightarrow \left(\circ e, \left(\frac{\circ \underline{e}}{+\eta}, \circ e + \eta\right)\right)}\ \textsc{UOP} \qquad \frac{\Theta, e \Rightarrow e, \underline{e}, e \qquad \circ e <}{\Theta, \circ e \Rightarrow \left(\circ e, \left(\circ \underline{e} + \eta, \frac{\circ e}{+\eta}\right)\right)}\ \textsc{UOP-NEG}$$

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

$$\frac{\Theta, e \Rightarrow e, err}{\Theta, x = e \Rightarrow \Theta x \mapsto e, err}\ \textsc{ASG} \qquad \frac{\Theta, p \Rightarrow \Theta \qquad \Theta, p \Rightarrow \Theta}{\Theta, p\, p \Rightarrow \Theta}\ \textsc{CONSQ} \qquad \frac{c \leftarrow \mu^{\diamond}}{\Theta, x \leftarrow \mu \Rightarrow \Theta x \mapsto c, c, c}\ \textsc{SAMPLE}$$

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

$$\frac{\texttt{fl}\, r = c}{r \Downarrow^{\mathbb{F}} c}\ \textsc{RVAL} \qquad \frac{}{c \Downarrow^{\mathbb{F}} c}\ \textsc{FVAL} \qquad \frac{e \Downarrow^{\mathbb{F}} c \quad e \Downarrow^{\mathbb{F}} c \quad \texttt{fl}\, c * c = c}{e * e \Downarrow^{\mathbb{F}} c}\ \textsc{FBOP} \qquad \frac{e \Downarrow^{\mathbb{F}} c', \quad \texttt{fl} \circ c' = c}{\circ e \Downarrow^{\mathbb{F}} c}\ \textsc{FUOP}$$

Figure 3: Semantics of Evaluation in Floating Point Computation

$$\frac{}{r \Downarrow^{\mathbb{R}} r}\ \textsc{RVAL} \qquad \frac{}{c \Downarrow^{\mathbb{R}} c}\ \textsc{RVAL} \qquad \frac{e \Downarrow^{\mathbb{R}} r \quad e \Downarrow^{\mathbb{R}} r \quad r * r = r}{e * e \Downarrow^{\mathbb{R}} r}\ \textsc{RBOP} \qquad \frac{e \Downarrow^{\mathbb{R}} r', \quad \circ r' = r}{\circ e \Downarrow^{\mathbb{R}} r}\ \textsc{RUOP} \qquad \frac{f\mathrm{D} = c}{f\mathrm{D} \Downarrow c}\ \textsc{F(D)}$$

Figure 4: Semantics of Evaluation in Real Computation

thmSoundness 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. $\Theta x = e, \underline{e}, e$, if $e \Downarrow^{\mathbb{F}} c$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r}$ and $e \Downarrow^{\mathbb{R}} r$, then $\underline{r} \leq c \leq r$) , then $\forall x \in dom\Theta'$ s.t. $\Theta' x = e, \underline{e}, e$, if $e \Downarrow^{\mathbb{F}} c$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r}$ and $e \Downarrow^{\mathbb{R}} r$, then:

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

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

case

$$\frac{\Theta, p \Rightarrow \Theta \qquad \Theta, p \Rightarrow \Theta}{\Theta, p\, p \Rightarrow \Theta}\ \textbf{CONSQ}$$

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

case

$$\frac{c \leftarrow \mu^{\diamond}}{\Theta, x \leftarrow \mu \Rightarrow \Theta x \mapsto c, c, c}\ \textbf{SAMPLE}$$

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 $err = \underline{e}, e$, $e \Downarrow^{\mathbb{F}} c$, $\underline{e} \Downarrow^{\mathbb{R}} \underline{r}$ and $e \Downarrow^{\mathbb{R}} r$, $\underline{r} \leq c \leq r$.
Induction on transition of e, we have:

subcase

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

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

subcase

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

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

$$\frac{\mathtt{fl}\, r = c}{r \Downarrow^{\mathbb{F}} c}\ \text{RVAL}$$

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

subcase

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

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

$$\frac{\mathtt{fl}\, r = c}{r \Downarrow^{\mathbb{F}} c}\ \text{RVAL}$$

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

subcase

$$\frac{r = \mathtt{fl}\, r}{\Theta, r \Rightarrow r, r, r}\ \textbf{VAL-EQ}$$

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

subcase

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

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

subcase

$$\frac{\Theta, e \Rightarrow e, \underline{e}, e \diamond \qquad \Theta, e \Rightarrow e, \underline{e}, e\ \triangle \qquad e, \underline{e} = , \underline{e} * \underline{e}, e * \underline{e}, \underline{e} * e, e * e \qquad e * e \geq\ \Box}{\Theta, e * e \Rightarrow \left(e * e, \dfrac{\underline{e}}{+\eta}, e + \eta\right)}\ \textbf{BOP}$$

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

subcase

$$\frac{\Theta, e \Rightarrow e, \underline{e}, e \qquad \Theta, e \Rightarrow e, \underline{e}, e \qquad e, \underline{e} = , \underline{e} * \underline{e}, e * \underline{e}, \underline{e} * e, e * e \qquad e * e <}{\Theta, e * e \Rightarrow \left(e * e, \underline{e} + \eta, \frac{e}{+\eta}\right)} \text{ BOP-NEG}$$

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

subcase

$$\frac{\Theta, e \Rightarrow e, \underline{e}, e \diamond \qquad \circ e \ge \square}{\Theta, \circ e \Rightarrow \left(\circ e, \frac{\circ \underline{e}}{+\eta}, \circ e + \eta\right)} \text{ UOP}$$

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

subcase

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

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

□

4 Snapping Mechanism

defn$\mathsf{Snap} a : \mathrm{A} \to \mathsf{Distr}\mathbb{R}]$ Given privacy parameter ϵ, the Snapping mechanism $\mathsf{Snap} a$ is defined as:

$$\mathrm{U} \leftarrow \mu \, \mathrm{S} \leftarrow \{-,\} \; y = f\, a + \mathrm{S} \times \mathrm{U} \div \epsilon \; z = \mathsf{clamp}_{\mathrm{B}}(\lfloor y \rceil_{\Lambda})$$

where F is a primitive query function over input database $a \in \mathrm{A}$, ϵ is the privacy budget, B is the clamping bound and Λ is the rounding argument satisfying $\lambda = {}^{k}$ where ^{k} is the smallest power of 2 greater or equal to the $\frac{}{\epsilon}$.
Let $\mathsf{Snap}' a$ be the same as $\mathsf{Snap} a$ given U, S without rounding and clamping steps, i.e., $\mathsf{Snap}' a : y = f\, a + \mathrm{S} \times \mathrm{U} \div \epsilon$.
Let $\mathsf{Snap}'' a$ be the same as $\mathsf{Snap} a$ given U, S, i.e., $\mathsf{Snap}'' a : \mathsf{Snap}' a \, z = \mathsf{clamp}_{\mathrm{B}}(\lfloor y \rceil_{\Lambda})$.

5 Main Theorem

thmThe Snap mechanism is $\epsilon-$differentially private] Consider $\mathsf{Snap}a$ defined as before, if $\mathsf{Snap}a = x$ given database a and privacy parameter ϵ, then its actual privacy loss is bounded by $\epsilon + \mathrm{B}\epsilon\eta$.

Proof. Given $\mathsf{Snap}a = x$ and parameter ϵ, we consider a' be the adjacent database of a satisfying $|fa - fa'| \leq$. Without loss of generalization, we assume $fa + = fa'$ $\diamond$.

Consider the $\mathsf{Snap}a$ outputting the same result x under floating point and real computaion, let L, R be the range where $\forall u \in \mathrm{L}, \mathrm{R}$ and some s s.t.:

$$\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}''a \Downarrow^{\mathbb{R}} z \mapsto x.$$

We have $\ltimes\mathsf{Snap}a = x = \mathrm{R} - \mathrm{L}$. Sice the $\mathsf{Snap}a$ is $\epsilon-$DP, we can get:

$$e^{-\epsilon} \leq \frac{\ltimes\mathsf{Snap}a}{\ltimes\mathsf{Snap}a'} = \frac{\mathrm{R}-\mathrm{L}}{\mathrm{R}'-\mathrm{L}'} \leq e^{\epsilon}$$

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

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

To show the privacy loss of Snap mechanism in floating point computation is bounded by $\epsilon + \mathrm{B}\epsilon\eta$, it's sufficent to show: $|r - l|$ is bounded $f|\mathrm{R}-\mathrm{L}|$ and $g|\mathrm{R}-\mathrm{L}|$ s.t.:

$$-\epsilon + \mathrm{B}\epsilon\eta \leq \frac{f|\mathrm{R}-\mathrm{L}|}{g|\mathrm{R}-\mathrm{L}|} \leq \epsilon + \mathrm{B}\epsilon\eta.$$

Induction on the outputspace of $\mathsf{Snap}a$ mechanism, we have following cases:

case $x = -\mathrm{B}$

Let b be the largest number rounded by Λ that is smaller than B, $b' = b - \Lambda$.
Let L and R be the range where $\forall u \in \mathrm{L}, \mathrm{R}$ and $s =$, s.t. $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}''a \Downarrow^{\mathbb{R}} z \mapsto x$.
Let l and r be the range where $\forall u \in l, r$ and $s =$, s.t. $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}''a \Downarrow^{\mathbb{F}} z \mapsto x$.
So we know $s =$, $l = \mathrm{L} =$, $\underline{\mathrm{R}} < r < \mathrm{R}$ s.t.:

$$\mathrm{U} \mapsto r, \mathrm{S} \mapsto , \mathsf{Snap}'a \Downarrow^{\mathbb{F}} y \mapsto -b' \wedge \mathrm{U} \mapsto \mathrm{R}, \mathrm{S} \mapsto , \mathsf{Snap}'a \Downarrow^{\mathbb{R}} y \mapsto -b'.$$

The derivation of this case given $\Theta = \mathrm{U} \mapsto \mathrm{R}, \underline{\mathrm{R}}, \mathrm{R}, \mathrm{S} \mapsto , ,$ is shown as following:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{\Theta, \mathrm{U} \Rightarrow \mathrm{R}, \underline{\mathrm{R}}, \mathrm{R}}\ \textsc{val-eq}}{\Theta, \mathrm{U} \Rightarrow \mathrm{R}, \underline{\mathrm{R}} + \eta, \frac{\mathrm{R}}{+\eta}}\ \textsc{uop}}{\Theta, \frac{}{\epsilon} \times \mathrm{U} \Rightarrow \frac{}{\epsilon} \times \mathrm{R}, \frac{}{\epsilon} \times \underline{\mathrm{R}} + \eta, \frac{\frac{}{\epsilon} \times \mathrm{R}}{+\eta}}\ \textsc{bop}}{\Theta, fa + \frac{}{\epsilon} \times \mathrm{U} \Rightarrow \left(fa + \frac{}{\epsilon} \times \mathrm{R}, \left(fa + \frac{}{\epsilon} \times \underline{\mathrm{R}} + \eta + \eta, \frac{fa + \frac{\frac{}{\epsilon} \times \mathrm{R}}{+\eta}}{+\eta}\right)\right)}\ \textsc{bop}}{\Theta, \mathsf{Snap}'a \Rightarrow \Theta y \mapsto \left(fa + \frac{}{\epsilon} \times \mathrm{R}, \left(fa + \frac{}{\epsilon} \times \underline{\mathrm{R}} + \eta + \eta, \frac{fa + \frac{\frac{}{\epsilon} \times \mathrm{R}}{+\eta}}{+\eta}\right)\right)}\ \textsc{id}$$

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

$$\frac{\cdots}{\Theta, \mathsf{Snap}'a'\mathsf{Snap}'' \Rightarrow \Theta y \mapsto \left(\mathsf{Snap}'a', \left(fa' + \frac{}{\epsilon} \times \underline{\mathrm{R}}' + \eta + \eta, \frac{fa' + \frac{\frac{}{\epsilon} \times \mathrm{R}'}{+\eta}}{+\eta}\right)\right)}$$

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 $\underline{\mathrm{R}}, \mathrm{R}, \underline{\mathrm{R}}'$ and R':

$$\underline{\mathrm{R}} = e^{\epsilon\left(-b'+\eta-fa+\eta\right)}, \mathrm{R} = e^{\epsilon \frac{\frac{-b'}{+\eta} - fa}{+\eta}}$$
$$\underline{\mathrm{R}}' = e^{\epsilon\left(-b'+\eta-fa'+\eta\right)}, \mathrm{R}' = e^{\epsilon \frac{\frac{-b'}{+\eta} - fa'}{+\eta}}$$

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

$$\begin{aligned} \frac{\mathrm{R}-}{\underline{\mathrm{R}}'-} &= e^{\epsilon\left(\frac{\frac{-b'}{+\eta} - fa}{+\eta} - \left(-b'+\eta-fa'+\eta\right)\right)} \\ &= e^{\epsilon\left(\frac{-b'}{+\eta} - \frac{fa}{+\eta} - x + \eta + fa' + \eta\right)} \quad \star \end{aligned}$$

Since $+\eta > +\eta$, $\frac{}{+\eta} < \frac{}{+\eta}$, $+\eta < +.\eta$ and $\frac{}{+\eta} > -\eta$, we have:

$$\begin{aligned} \star \quad &< e^{\epsilon\left(\frac{\eta+}{+\eta} b' + .\eta fa + + .\eta\right)} \\ &< e^{\epsilon.\eta \mathrm{B} + + .\eta} \end{aligned}$$

case $\boldsymbol{x \in -\mathrm{B}, \lfloor fa \rceil_{\Lambda}}$

subcase $\boldsymbol{\lfloor fa \rceil_{\Lambda} \leq \vee \left(\lfloor fa \rceil_{\Lambda} > \wedge x \in -\mathrm{B}, \right)}$

Let $y = x - \frac{\Lambda}{}$, $y = x + \frac{\Lambda}{}$, we know $y <$, $y <$.
Let $\mathrm{L} = e^{\epsilon y - fa}$ and $\mathrm{R} = e^{\epsilon y - fa}$, we have: $\forall u \in \mathrm{L}, \mathrm{R}$: $\mathrm{U} \mapsto u, \mathrm{S} \mapsto , \mathsf{Snap}''a \Downarrow^{\mathbb{R}} z \mapsto x$.
Let l and r be the range where $\forall u \in l, r$ and $s =$, s.t. $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}''a \Downarrow^{\mathbb{F}} z \mapsto x$.
So we know: $\underline{\mathrm{L}} < l < \mathrm{L}$, $\underline{\mathrm{R}} < r < \mathrm{R}$ s.t.:

$$\mathrm{U} \mapsto l, \mathrm{S} \mapsto , \mathsf{Snap}'a \Downarrow^{\mathbb{F}} y \mapsto y \wedge \mathrm{U} \mapsto r, \mathrm{S} \mapsto , \mathsf{Snap}'a \Downarrow^{\mathbb{F}} y \mapsto y.$$

The transition from R to r given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{R}, \underline{\mathrm{R}}, \mathrm{R}, \mathrm{S} \mapsto , ,$ is shown as following:

LN

$$\cfrac{\cfrac{\cfrac{\cfrac{}{\Theta, \mathrm{R} \Rightarrow \mathrm{R}, \underline{\mathrm{R}}, \mathrm{R}}\ \text{VAL-EQ}}{\Theta, \mathrm{U} \Rightarrow \mathrm{R}, \underline{\mathrm{R}} + \eta, \frac{\mathrm{R}}{+\eta}}\ \text{OP}}{\Theta, \frac{}{\epsilon} \times \mathrm{U} \Rightarrow \left(\frac{}{\epsilon} \times \mathrm{R}, \frac{}{\epsilon} \times \underline{\mathrm{R}} + \eta, \frac{\frac{}{\epsilon} \times \mathrm{R}}{+\eta}\right)}\ \text{OP}}{\cfrac{\Theta, fa + \frac{}{\epsilon} \times \mathrm{U} \Rightarrow \left(fa + \frac{}{\epsilon} \times \mathrm{R}, \left(\left(fa + \frac{}{\epsilon} \times \underline{\mathrm{R}} + \eta\right) + \eta, \frac{fa + \frac{\frac{}{\epsilon} \times \mathrm{R}}{+\eta}}{+\eta}\right)\right)}{\Theta, \mathsf{Snap}'a \Rightarrow \Theta y \mapsto fa + \frac{}{\epsilon} \times \mathrm{R}, e, e}}\ \text{ID}$$

From soundness theorem, we have $e \leq y \leq e$, where we can get:
$\underline{R} = e^{\epsilon\left(y+\eta-fa+\eta\right)}$ and $R = e^{\epsilon\frac{\frac{y}{+\eta}-fa}{+\eta}}$. The transition from L to l given the transition environment $\Theta = U \mapsto L, \underline{L}, L, S \mapsto ,,$ is shown as following:

$$\frac{\cdots}{\Theta, \mathsf{Snap}'a \Rightarrow \Theta z \mapsto fa + \frac{}{\epsilon} \times \underline{L}, \left(\frac{fa + \frac{}{\epsilon} \times \underline{L} + \eta}{+\eta}, fa + \frac{\frac{}{\epsilon} \times L}{+\eta} + \eta\right)}$$

From soundness theorem, we have $err \leq y \leq err$.
Taking the lower bound , we have: $\underline{L} = e^{\epsilon\left(y+\eta-fa+\eta\right)}$.
Taking the upper bound, we have: $L = e^{\epsilon\frac{\frac{y}{+\eta}-fa}{+\eta}}$.
In the same way, we have the bound of l, r for adjacent data set a':

$$\underline{R}' = e^{\epsilon\left(y+\eta-fa'+\eta\right)},\ R' = e^{\epsilon\frac{\frac{y}{+\eta}-fa'}{+\eta}}.$$

$$\underline{L}' = e^{\epsilon\left(y+\eta-fa'+\eta\right)},\ L' = e^{\epsilon\frac{\frac{y}{+\eta}-fa'}{+\eta}}$$

Then, we have the privacy loss is bounded by:

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

We also have:

$$\begin{array}{ll} \frac{\underline{R}}{R} & = e^{\epsilon\left(\frac{y}{+\eta} - \frac{fa}{+\eta} - y + fa\right)} \leq e^{\epsilon\left(-\frac{\eta}{+\eta}y + \eta fa\right)} \leq e^{\epsilon\left(\frac{\eta}{+\eta}B + \eta B\right)} \leq e^{\epsilon B\eta} \\ \frac{\underline{L}}{\overline{L}} & = e^{\epsilon\left(y+\eta-fa+\eta-y+fa\right)} \geq e^{\epsilon\left(\eta y - \eta fa\right)} \geq e^{-\epsilon B\eta} \end{array}$$

Then, we can derive:

$$\begin{array}{ll} |R - \underline{L}| & \leq e^{\epsilon B\eta}R - e^{-\epsilon B\eta}L \\ & = L\left(e^{\Lambda\epsilon+\epsilon B\eta} - e^{-\epsilon B\eta}\right) \\ & = L\left(e^{\Lambda\epsilon}e^{\epsilon B\eta} - e^{\epsilon B\eta} + e^{\epsilon B\eta} - e^{-\epsilon B\eta}\right) \\ & = L\left(e^{\Lambda\epsilon}e^{\epsilon B\eta} - e^{\epsilon B\eta} + \frac{}{e^{\Lambda\epsilon}-}e^{\Lambda\epsilon} - e^{\epsilon B\eta} - e^{-\epsilon B\eta}\right) \\ & \leq L\left(e^{\Lambda\epsilon}e^{\epsilon B\eta} - e^{\epsilon B\eta} + \frac{}{e-}e^{\Lambda\epsilon} - e^{\epsilon B\eta} - e^{-\epsilon B\eta}\right)\ by \leq \Lambda\epsilon < \\ & = L\frac{e}{e-}\left(e^{\Lambda\epsilon}e^{\epsilon B\eta} - e^{\epsilon B\eta} - e^{-\epsilon B\eta}\right) \\ & < L\frac{e}{e-}\left(e^{\Lambda\epsilon}e^{\epsilon B\eta} - e^{\epsilon B\eta}\right) \\ & = Le^{\Lambda\epsilon} - e^{\frac{e}{e-}+\epsilon B\eta} \\ & < Le^{\Lambda\epsilon} - e^{\epsilon B\eta}\ by\ \frac{}{\epsilon} < B < \frac{}{\epsilon} \\ & = R - Le^{\epsilon B\eta} \end{array}$$

In the same way, we can derive:

$$|\underline{R} - L| > e^{-\epsilon B\eta}R - e^{\epsilon B\eta}L > R - Le^{-\epsilon B\eta}$$

Then we have:

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

subcase $\lfloor fa \rceil_{\Lambda} > \wedge x \in , \lfloor fa \rceil_{\Lambda}$

Let $y = x - \frac{\Delta}{}$, $y = x + \frac{\Delta}{}$, we know $y >$, $y >$.
Let S = , $\mathrm{L} = e^{\epsilon y - fa}$ and $\mathrm{R} = e^{\epsilon y - fa}$, we have $\forall u \in \mathrm{L}, \mathrm{R}$: $\mathrm{U} \mapsto u, \mathrm{S} \mapsto , \mathsf{Snap}'' a \Downarrow^{\mathbb{R}} z \mapsto x$.
Let l and r be the range where $\forall u \in l, r$ and $s =$, s.t. $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}'' a \Downarrow^{\mathbb{F}} z \mapsto x$.
We know: $\underline{\mathrm{L}} < l < \mathrm{L}$, $\underline{\mathrm{R}} < r < \mathrm{R}$ s.t.:

$$\mathrm{U} \mapsto l, \mathrm{S} \mapsto , \mathsf{Snap}' a \Downarrow^{\mathbb{F}} y \mapsto y \wedge \mathrm{U} \mapsto r, \mathrm{S} \mapsto , \mathsf{Snap}' a \Downarrow^{\mathbb{F}} y \mapsto y.$$

The transition from L to l given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{L}, \underline{\mathrm{L}}, \mathrm{L}, \mathrm{S} \mapsto , ,$ is shown as following:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Theta, \mathrm{U} \Rightarrow \mathrm{L}, \underline{\mathrm{L}}, \mathrm{L}}{\Theta, \mathrm{U} \Rightarrow \mathrm{L}, \underline{\mathrm{L}} + \eta, \frac{\mathrm{L}}{+\eta}}}{\Theta, \frac{-}{\epsilon} \times \mathrm{U} \Rightarrow \left(\frac{-}{\epsilon} \times \mathrm{L}, \frac{-}{\epsilon} \times \underline{\mathrm{L}} + \eta, \frac{\frac{-}{\epsilon} \times \mathrm{L}}{+\eta}\right)}}{\Theta, fa + \frac{-}{\epsilon} \times \mathrm{U} \Rightarrow \left(fa + \frac{-}{\epsilon} \times l, \frac{fa + \frac{-}{\epsilon} \times \underline{\mathrm{L}} + \eta}{+\eta}, fa + \frac{\frac{-}{\epsilon} \times \mathrm{L}}{+\eta} + \eta\right)}}{\Theta, \mathsf{Snap}' a \Rightarrow \Theta y \mapsto fa + \frac{-}{\epsilon} \times \mathrm{L}, err, err}$$

From soundness theorem, we have $err \le y \le err$, then we can get:
$\underline{\mathrm{L}} = e^{y + \eta - fa + \eta\epsilon}$ and $\mathrm{L} = e^{y + \eta - fa\epsilon + \eta}$. The transition from R to r given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{R}, \underline{\mathrm{R}}, \mathrm{R}, \mathrm{S} \mapsto , ,$ is shown as following:

$$\dfrac{\cdots}{\Theta, \mathsf{Snap}' a \Rightarrow \Theta y \mapsto \left(fa + \frac{-}{\epsilon} \times \mathrm{R}, \frac{fa + \frac{-}{\epsilon} \times \underline{\mathrm{R}} + \eta}{+\eta}, fa + \frac{\frac{-}{\epsilon} \times \mathrm{R}}{+\eta} + \eta\right)}$$

From soundness theorem, we have $err \le y \le err$.
Taking the lower bound (i.e. $err = y$), we have: $\underline{\mathrm{R}} = e^{y + \eta - fa + \eta\epsilon}$. Taking the upper bound (i.e. $err = y$), we have: $\mathrm{R} = e^{y + \eta - fa\epsilon + \eta}$.

For the adjacent input a, we first have the same setting as input a for R' and L'. Then the transition from L' to l' given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{L}', \underline{\mathrm{L}}', \mathrm{L}', \mathrm{S} \mapsto , ,$ is shown as following:

$$\dfrac{\cdots}{\Theta, \mathsf{Snap}' a' \Rightarrow \Theta y \mapsto \left(fa + \frac{-}{\epsilon} \times \mathrm{L}', \frac{fa' + \frac{-}{\epsilon} \times \underline{\mathrm{L}}' + \eta}{+\eta}, fa' + \frac{\frac{-}{\epsilon} \times \mathrm{L}'}{+\eta} + \eta\right)}$$

From soundness theorem, we have $err \le y \le err$.

Taking the lower bound (i.e. $err = y$), we get: $\underline{\mathrm{L}}' = e^{y + \eta - fa' + \eta\epsilon}$. Taking the upper bound (i.e. $err = y$), we get: $\mathrm{L}' = e^{y + \eta - fa'\epsilon + \eta}$. The transition from R' to r' given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{R}', \underline{\mathrm{R}}', \mathrm{R}', \mathrm{S} \mapsto , ,$ is shown as following:

$$\dfrac{\cdots}{\Theta, \mathsf{Snap}' a' \Rightarrow \Theta y \mapsto \left(fa + \frac{-}{\epsilon} \times \mathrm{R}', \frac{fa' + \frac{-}{\epsilon} \times \underline{\mathrm{R}}' + \eta}{+\eta}, fa' + \frac{\frac{-}{\epsilon} \times \mathrm{R}'}{+\eta} + \eta\right)}$$

From soundness theorem, we have $err \le y \le err$.

Taking the lower bound (i.e. $err = y$), we have: $\underline{\mathrm{R}}' = e^{y+\eta-fa'+\eta\epsilon}$. Taking the upper bound (i.e. $err = y$), we have: $\mathrm{R}' = e^{y+\eta-fa'\epsilon+\eta}$.
We have the privacy loss is bounded by:

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

Since the following bound can be proved by using $-\eta < +\eta < +.\eta, y > -\mathrm{B}, y > -\mathrm{B}$ and simple approximation:

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

We also have the $\mathsf{Snap}a$ is ϵ-dp:

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

So we can get:

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

subcase $\lfloor \boldsymbol{fa} \rceil_{\Lambda} > \wedge\, \boldsymbol{x} =$

Let $y = x - \frac{\Lambda}{}$, $y = x + \frac{\Lambda}{}$, we know $y <$, $y >$.
Let $\mathrm{S} =$, $\mathrm{L} = e^{\epsilon y - fa}$ and $\mathrm{R} = e^{\epsilon y - fa}$, we have $\forall u \in \mathrm{L}, \mathrm{R}$: $\mathrm{U} \mapsto u, \mathrm{S} \mapsto , \mathsf{Snap}''a \Downarrow^{\mathbb{R}} z \mapsto x$.
Let l and r be the range where $\forall u \in l, r$ and $s =$, s.t. $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}''a \Downarrow^{\mathbb{F}} z \mapsto x$.
We know: $\underline{\mathrm{L}} < l < \mathrm{L}$, $\underline{\mathrm{R}} < r < \mathrm{R}$ s.t.:

$$\mathrm{U} \mapsto l, \mathrm{S} \mapsto , \mathsf{Snap}'a \Downarrow^{\mathbb{F}} y \mapsto y \wedge \mathrm{U} \mapsto r, \mathrm{S} \mapsto , \mathsf{Snap}'a \Downarrow^{\mathbb{F}} y \mapsto y.$$

The transition from L to l given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{L}, \underline{\mathrm{L}}, \mathrm{L}, \mathrm{S} \mapsto , ,$ is shown as following:

$$\frac{\cdots}{\Theta, \mathsf{Snap}'a \Rightarrow \Theta y \mapsto \left(fa + \frac{}{\epsilon} \times \underline{\mathrm{L}}, \frac{fa + \frac{}{\epsilon} \times \underline{\mathrm{L}} + \eta}{+\eta}, fa + \frac{\frac{}{\epsilon} \times \mathrm{L}}{+\eta} + \eta\right)}$$

From soundness theorem, we have $err \le y \le err$.
Taking the lower bound , we have: $\underline{\mathrm{L}} = e^{\epsilon\left(y+\eta-fa+\eta\right)}$.

Taking the upper bound, we have: $\mathrm{L} = e^{\epsilon\frac{\frac{y}{+\eta}-fa}{+\eta}}$. The transition from R to r given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{R}, \underline{\mathrm{R}}, \mathrm{R}, \mathrm{S} \mapsto , ,$ is shown as following:

$$\frac{\cdots}{\Theta, \mathsf{Snap}'a \Rightarrow \Theta y \mapsto \left(fa + \frac{}{\epsilon} \times \underline{\mathrm{R}}, \frac{fa + \frac{}{\epsilon} \times \underline{\mathrm{R}} + \eta}{+\eta}, fa + \frac{\frac{}{\epsilon} \times \mathrm{R}}{+\eta} + \eta\right)}$$

From soundness theorem, we have $err \le y \le err$. Taking the lower bound (i.e. $err = y$), we have: $\underline{\mathrm{R}} = e^{y+\eta-fa+\eta\epsilon}$. Taking the upper bound (i.e. $err = y$), we have: $\mathrm{R} = e^{y+\eta-fa\epsilon+\eta}$. Using the bound we proved before, we have the folloing bound on $|\mathrm{R}-\underline{\mathrm{L}}|$ and $|\underline{\mathrm{R}}-\mathrm{L}|$:

$$\begin{aligned} \mathrm{R}-\underline{\mathrm{L}} &< e^{\mathrm{B}\eta\epsilon}\mathrm{R} - e^{-\mathrm{B}\eta\epsilon}\mathrm{L} < \mathrm{R}-\mathrm{L}e^{\mathrm{B}\eta\epsilon} \\ \underline{\mathrm{R}}-\mathrm{L} &> e^{-\mathrm{B}\eta\epsilon}\mathrm{R} - e^{\mathrm{B}\eta\epsilon}\mathrm{L} > \mathrm{R}-\mathrm{L}e^{-\mathrm{B}\eta\epsilon}, \end{aligned}$$

and privacy loss is bounded by:

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

case $x = \lfloor fa \rceil_\Lambda$

This case can also be split into 3 subcases by: $\lfloor fa \rceil_\Lambda <$, $\lfloor fa \rceil_\Lambda =$ and $\lfloor fa \rceil_\Lambda >$. Without loss of generalization, we consider the worst case where the error propagate in the same direction, i.e. $\lfloor fa \rceil_\Lambda <$.

From this assumption, let $y = x - \frac{\Lambda}{}$, $y = x + \frac{\Lambda}{}$, we know $y <$, $y <$. Since $fa + = fa'$, we also have $\lfloor fa \rceil < \lfloor fa' \rceil$. So, we know s can only be for input a' but s can be or $-$ for input a.

For input a, let $\mathrm{S} = s$, $\mathrm{L} = e^{\epsilon y - fa}$ and $\mathrm{R} = e^{\epsilon y - fa}$, we have $\forall u \in \mathrm{L}, \mathrm{R}$: $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}'' a \Downarrow^{\mathbb{R}} z \mapsto x$.

Let l and r be the range where $\forall u \in l, r$ and $\mathrm{S} = s$, s.t. $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}'' a \Downarrow^{\mathbb{F}} z \mapsto x$.

We know: $\underline{\mathrm{L}} < l < \mathrm{L}$, $\underline{\mathrm{R}} < r < \mathrm{R}$ s.t.:

$$\mathrm{U} \mapsto l, \mathrm{S} \mapsto s, \mathsf{Snap}' a \Downarrow^{\mathbb{F}} y \mapsto y \wedge \mathrm{U} \mapsto r, \mathrm{S} \mapsto s, \mathsf{Snap}' a \Downarrow^{\mathbb{F}} y \mapsto y.$$

Induction on s, we have when $s =$:

The transition from R to r given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{R}_+, \underline{\mathrm{R}}_+, \mathrm{R}_+, \mathrm{S} \mapsto , ,$ is shown as following:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Theta, \mathrm{U} \Rightarrow \mathrm{R}_+, \underline{\mathrm{R}}_+, \mathrm{R}_+}{\Theta, \mathrm{U} \Rightarrow \left(\mathrm{R}_+, \underline{\mathrm{R}}_+ + \eta, \frac{\mathrm{R}_+}{+\eta}\right)}}{\Theta, \frac{}{\epsilon}\mathrm{U} \Rightarrow \left(\frac{}{\epsilon} \times \mathrm{R}_+, \left(\frac{}{\epsilon}\underline{\mathrm{R}}_+ + \eta, \frac{}{\epsilon}\frac{\mathrm{R}_+}{+\eta}\right)\right)}}{\Theta, fa + \frac{}{\epsilon}\mathrm{U} \Rightarrow \left(fa + \frac{}{\epsilon} \times \mathrm{R}_+, \left(fa + \frac{}{\epsilon}\underline{\mathrm{R}}_+ + \eta + \eta, fa + \frac{}{\epsilon}\frac{\mathrm{R}_+}{+\eta} + \eta\right)\right)}}{\Theta, \mathsf{Snap}' a \Rightarrow \Theta y \mapsto fa + \frac{}{\epsilon} \times \mathrm{R}_+, err, err}$$

From soundness theorem, we have $err \le y \le err$. Then we can get following bounds for r:

$\underline{\mathrm{R}}_+ = e^{\epsilon\left(y+\eta-fa+\eta\right)}$, $\mathrm{R}_+ = e^{\epsilon\frac{\frac{y}{+\eta}-fa}{+\eta}}$.

Since $y = \lfloor fa \rceil + \frac{\Lambda}{}$, we have $e^{\epsilon\left(y-fa\right)} >$, so actually we know $\mathrm{R} = r =$.

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

$\underline{\mathrm{L}}_+ = e^{\epsilon\left(y+\eta-fa+\eta\right)}$, $\mathrm{L}_+ = e^{\epsilon\frac{\frac{y}{+\eta}-fa}{+\eta}}$.

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

$\underline{\mathrm{L}}_- = e^{\epsilon\left(fa-y+\eta+\eta\right)}$, $\mathrm{L}_- = e^{\epsilon\frac{fa-\frac{y}{+\eta}}{+\eta}}$.

$\underline{\mathrm{R}} = e^{\epsilon\left(fa-y+\eta+\eta\right)}$, $\mathrm{R} = e^{\epsilon\frac{fa-\frac{y}{+\eta}}{+\eta}}$.

Since $y = \lfloor fa \rceil - \frac{\Lambda}{}$, we have $e^{\epsilon\left(fa-y\right)} >$, so actually we know $\mathrm{R}' = r' =$.

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

$\underline{\mathrm{R}}' = e^{\epsilon\left(y+\eta-fa'+\eta\right)}$, $\mathrm{R}' = e^{\epsilon\frac{\frac{y}{+\eta}-fa'}{+\eta}}$.

$\underline{\mathrm{L}}' = e^{\epsilon\left(y+\eta-fa'+\eta\right)}$, $\mathrm{L}' = e^{\epsilon\frac{\frac{y}{+\eta}-fa'}{+\eta}}$.

We have following bounds on their ratios:

$$\frac{\underline{\mathrm{R}}_+}{\mathrm{R}_+} = e^{\epsilon\left(+\eta y - +\eta fa - y + fa\right)} > e^{-\epsilon B\eta}, \frac{\mathrm{R}_+}{\mathrm{R}_+} = e^{\epsilon\left(fracy + \eta - \frac{fa}{+\eta} - y + fa\right)} < e^{\epsilon B\eta},$$

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

$$\frac{\underline{\mathrm{R}}'}{\mathrm{R}} = e^{\epsilon\left(+\eta fa - +\eta y - fa + y\right)} > e^{-\epsilon B\eta}, \frac{\mathrm{R}'}{\mathrm{R}'} = e^{\epsilon\left(\frac{fa}{+\eta} - fracy + \eta - fa + y\right)} < e^{\epsilon B\eta},$$

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

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

Then we have the following bounds on privacy loss:

$$\frac{-\underline{\mathrm{L}}_+ + \underline{\mathrm{L}}_-}{\underline{\mathrm{R}}' - \mathrm{L}'} < \frac{\mathrm{R}_+ - \underline{\mathrm{L}}_+}{\underline{\mathrm{R}}' - \mathrm{L}'} < \frac{e^{\epsilon B\eta}\mathrm{R}_+ - \mathrm{L}_+}{e^{-\epsilon B\eta}\mathrm{R}' - \mathrm{L}'} = e^{\epsilon B\eta + \epsilon}$$

case $\boldsymbol{x \in \lfloor fa \rceil_\Lambda, \lfloor fa' \rceil_\Lambda}$

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

For input a:

$\underline{\mathrm{R}} = e^{\epsilon\left(fa - y + \eta + \eta\right)}$, $\mathrm{R} = e^{\epsilon \frac{fa - \frac{y}{+\eta}}{+\eta}}$.

$\underline{\mathrm{L}} = e^{\epsilon\left(fa - y + \eta + \eta\right)}$, $\mathrm{L} = e^{\epsilon \frac{fa - \frac{y}{+\eta}}{+\eta}}$.

For input a':

$\underline{\mathrm{R}}' = e^{\epsilon\left(y + \eta - fa' + \eta\right)}$, $\mathrm{R}' = e^{\epsilon \frac{\frac{y}{+\eta} - fa'}{+\eta}}$.

$\underline{\mathrm{L}}' = e^{\epsilon\left(y + \eta - fa' + \eta\right)}$, $\mathrm{L}' = e^{\epsilon \frac{\frac{y}{+\eta} - fa'}{+\eta}}$.

The bounds on their ratio are as follows:

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

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

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

So we have the privacy loss is bounded by:

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

case $\boldsymbol{x = \lfloor fa' \rceil_\Lambda}$

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

From this assumption, let $y = x - \frac{\Lambda}{}$, $y = x + \frac{\Lambda}{}$, we know $y <$, $y <$. Since $fa + = fa'$, we also

have $\lfloor fa \rceil < \lfloor fa' \rceil <$. So, we know s can only be $-$ for input a but s can be or $-$ for input a'.
For input a', Let $\mathrm{S} = s$, $\mathrm{L}' = e^{\epsilon y - fa'}$ and $\mathrm{R}' = e^{\epsilon y - fa}$, we have $\forall u \in \mathrm{L}', \mathrm{R}'$: $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}'' a' \Downarrow^{\mathbb{R}} z \mapsto x$.
Let l' and r' be the range where $\forall u \in l', r'$ and $\mathrm{S} = s$, s.t. $\mathrm{U} \mapsto u, \mathrm{S} \mapsto s, \mathsf{Snap}'' a \Downarrow^{\mathbb{F}} z \mapsto x$.
We know: $\underline{\mathrm{L}}' < l' < \mathrm{L}'$, $\underline{\mathrm{R}}' < r < \mathrm{R}'$ s.t.:

$$\mathrm{U} \mapsto l', \mathrm{S} \mapsto s, \mathsf{Snap}' a \Downarrow^{\mathbb{F}} y \mapsto y \wedge \mathrm{U} \mapsto r', \mathrm{S} \mapsto s, \mathsf{Snap}' a \Downarrow^{\mathbb{F}} y \mapsto y.$$

Induction on s, we have: When $s =$.
The transition from R' to r' given the transition environment $\Theta = \mathrm{U} \mapsto \mathrm{R}'_{+}, \underline{\mathrm{R}}'_{+}, \mathrm{R}'_{+}, \mathrm{S} \mapsto , ,$ is shown as following:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Theta, \mathrm{U} \Rightarrow \mathrm{R}_{+}, \mathrm{R}'_{+}, \mathrm{R}'_{+}}{\Theta, \mathrm{U} \Rightarrow \left(\mathrm{R}_{+}, \mathrm{R}'_{+} + \eta, \dfrac{\mathrm{R}'_{+}}{+\eta}\right)}}{\Theta, \dfrac{}{\epsilon}\mathrm{U} \Rightarrow \dfrac{}{\epsilon} \times \mathrm{R}_{+}, \left(\dfrac{}{\epsilon}\mathrm{R}'_{+} + \eta, \dfrac{}{\epsilon}\dfrac{\mathrm{R}'_{+}}{+\eta}\right)}}{\Theta, fa + \dfrac{}{\epsilon}\mathrm{U} \Rightarrow \left(fa + \dfrac{}{\epsilon} \times \mathrm{R}_{+}, \left(fa + \dfrac{}{\epsilon}\mathrm{R}'_{+} + \eta + \eta, fa + \dfrac{}{\epsilon}\dfrac{\mathrm{R}'_{+}}{+\eta} + \eta\right)\right)}}{\Theta, \mathsf{Snap}' a \Rightarrow \Theta y \mapsto fa + \dfrac{}{\epsilon} \times \mathrm{R}_{+}, err, err}$$

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

$$\frac{\underline{\mathrm{R}}'_{+}}{\underline{\mathrm{R}}'_{+}} = e^{\epsilon\left(+\eta y - +\eta fa - y + fa\right)} > e^{-\epsilon \mathrm{B}\eta}, \frac{\mathrm{R}'_{+}}{\mathrm{R}'_{+}} = e^{\epsilon\left(fracy + \eta - \frac{fa}{+\eta} - y + fa\right)} < e^{\epsilon \mathrm{B}\eta},$$

The same bound for L'_{+} by substituting y with y, and similar bound for L, R.

$$\frac{\underline{\mathrm{R}}}{\mathrm{R}} = e^{\epsilon\left(+\eta fa - +\eta y - fa + y\right)} > e^{-\epsilon \mathrm{B}\eta}, \frac{\mathrm{R}}{\mathrm{R}} = e^{\epsilon\left(\frac{fa}{+\eta} - fracy + \eta - fa + y\right)} < e^{\epsilon \mathrm{B}\eta},$$

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

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

Then we have the following bounds on privacy loss:

$$\frac{\underline{R} - L}{-\underline{L}'_+ + \underline{L}'_-} > \frac{\underline{R} - L}{R'_- - \underline{L}'_-} > \frac{e^{-\epsilon B\eta}R - L}{e^{\epsilon B\eta}R'_- - L'_-} = e^{-\epsilon B\eta - \epsilon}$$

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 $\boldsymbol{\lfloor f a' \rceil_\Lambda > \vee \lfloor f a' \rceil_\Lambda < \wedge x \in , B}$

let $y = x - \frac{\Lambda}{}$, $y = x + \frac{\Lambda}{}$, we have $y, y >$. The bounds derived for l, r and l', r' under input a and a' in this case are as follows:

For input a':

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

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

For input a:

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

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

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

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

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

So we have the privacy loss is bounded by:

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

subcase $\boldsymbol{\lfloor f a' \rceil_\Lambda < \wedge x \in \lfloor f a' \rceil_\Lambda ,}$

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

For input a':

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

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

For input a:

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

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

The bounds on their ratio are as follows:

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

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

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

So we have the privacy loss is bounded by:

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

subcase $\lfloor fa' \rceil_{\Lambda} < \wedge x =$

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

For input a':

$\underline{R}' = e^{\epsilon\left(fa' - \frac{y}{+\eta} + \eta\right)}$, $R' = e^{\epsilon\frac{fa'-y+\eta}{+\eta}}$.

$\underline{L}' = e^{\epsilon\left(fa' - y + \eta + \eta\right)}$, $L' = e^{\epsilon\frac{fa' - \frac{y}{+\eta}}{+\eta}}$.

For input a:

$\underline{R} = e^{\epsilon\left(fa - \frac{y}{+\eta} + \eta\right)}$, $R = e^{\epsilon\frac{fa-y+\eta}{+\eta}}$.

$\underline{L} = e^{\epsilon\left(fa - y + \eta + \eta\right)}$, $L = e^{\epsilon\frac{fa - \frac{y}{+\eta}}{+\eta}}$.

The bounds on their ratio are as follows:

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

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

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

So we have the privacy loss is bounded by:

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

case $x = B$

We know $s = -$, $L = l =$ 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:

$$\underline{R} = e^{\epsilon\left(fa - \frac{x}{+\eta} + \eta\right)}, R = e^{\epsilon\frac{fa-x+\eta}{+\eta}}$$
$$\underline{R}' = e^{\epsilon\left(fa' - \frac{x}{+\eta} + \eta\right)}, R' = e^{\epsilon\frac{fa'-x+\eta}{+\eta}}$$

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

$$\begin{aligned} \frac{\underline{R}-}{R'-} &= e^{\epsilon\left(\left(fa - \frac{x}{+\eta} + \eta\right) - \frac{fa'-x+\eta}{+\eta}\right)} \\ &= e^{\epsilon\left(fa + \eta - x + \eta - \frac{fa}{+\eta} + \frac{x}{+\eta}\right)} \quad \star \end{aligned}$$

Since $+ .\eta > + \eta > + \eta$ and $\frac{}{+\eta} > -\eta$, we have:

$$\begin{aligned} \star \quad &> e^{\epsilon\left(+\eta fa - \frac{\eta\eta+}{+\eta}x - \frac{}{+\eta}fa +\right)} \\ &= e^{\epsilon\left(\frac{\eta\eta+}{+\eta}fa - \frac{\eta\eta+}{+\eta}x - \frac{}{+\eta}\right)} \\ &> e^{\epsilon\left(-B\eta\frac{\eta+}{+\eta} + \frac{\eta+}{+\eta}x -\right)} \\ &> e^{\epsilon-\eta B-} \end{aligned}$$

□

6 Syntax - Functional

Following are the syntax of our system:

Expr.	e	$::=$	$x \mid r \mid c \mid \mathrm{FD} \mid e * e \mid \circ e \mid \texttt{let}\ x \leftarrow \mu\ \texttt{in}\ e \mid \texttt{let}\ x = e\ \texttt{in}\ e$
Binary Operation	$*$	$::=$	$+ \mid - \mid \times \mid \div$
Unary Operation	$\circ$	$::=$	$\mid - \mid \lfloor \cdot \rceil \mid \mathsf{clamp}_{\mathrm{B}} \cdot$
Value	v	$::=$	$r \mid c$
Distribution	μ	$::=$	$\mathsf{unif} \mid \texttt{bernoulli}$
Error	err	$::=$	e, e

$$\frac{r \geq}{r \Rightarrow \left(\frac{r}{+\eta}, r+\eta\right)}\ \textsc{val} \qquad \frac{r <}{r \Rightarrow \left(r+\eta, \frac{r}{+\eta}\right)}\ \textsc{val-neg} \qquad \frac{r = \mathtt{fl}\, r}{r \Rightarrow r, r}\ \textsc{val-eq} \qquad \frac{}{f\mathrm{D} \Rightarrow f\mathrm{D}, f\mathrm{D}}\ \textsc{f(d)}$$

$$\frac{}{\leftarrow \mu \Rightarrow \leftarrow \mu, \leftarrow \mu}\ \textsc{sample}$$

$$\frac{e \Rightarrow \underline{e}, e \qquad e \Rightarrow \underline{e}, e \qquad e * e \geq}{e * e \Rightarrow \left(\frac{\underline{e} * \underline{e}}{+\eta}, e * e + \eta\right)}\ \textsc{bop} \qquad \frac{e \Rightarrow \underline{e}, e \qquad e \Rightarrow \underline{e}, e \qquad e * e <}{e * e \Rightarrow \left(e * e + \eta, \frac{\underline{e} * \underline{e}}{+\eta}\right)}\ \textsc{bop-neg}$$

$$\frac{e \Rightarrow \underline{e}, e \qquad \circ e \geq}{\circ e \Rightarrow \left(\frac{\circ \underline{e}}{+\eta}, \circ e + \eta\right)}\ \textsc{uop} \qquad \frac{e \Rightarrow \underline{e}, e \qquad \circ e <}{\circ e \Rightarrow \left(\circ \underline{e} + \eta, \frac{\circ e}{+\eta}\right)}\ \textsc{uop-neg}$$

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

$$\frac{\mathtt{fl}\, r = c}{r \Downarrow c}\ \textsc{fval} \qquad \frac{e \Downarrow c \qquad e \Downarrow c \qquad \mathtt{fl}\, c * c = c}{e * e \Downarrow c}\ \textsc{fbop} \qquad \frac{e \Downarrow c', \qquad \mathtt{fl} \circ c' = c}{\circ e \Downarrow c}\ \textsc{fuop}$$

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.

thmSoundness Theorem] Given e where the transition $e \Rightarrow \underline{e}, e$ holds, then if e evaluates to c in floating point computation and $\underline{e}$ and e evaluates to $\underline{r}$ and r in real computation, we have:

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

$$\frac{}{r \Downarrow r}\ \textsc{rval} \qquad \frac{e \Downarrow r \qquad e \Downarrow r \qquad r * r = r}{e * e \Downarrow r}\ \textsc{rbop} \qquad \frac{e \Downarrow r', \qquad \circ r' = r}{\circ e \Downarrow r}\ \textsc{ruop}$$

$$\frac{c \leftarrow \mu^{\diamond}}{\leftarrow \mu \Downarrow c}\ \textsc{sample} \qquad \frac{f\mathrm{D} = c}{f\mathrm{D} \Downarrow c}\ \textsc{f(d)}$$

Figure 7: Semantics of Evaluation in Real Computation

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.