Verifying Snapping Mechanism - Floating Point Implementation Version

Jiawen Liu

March 3, 2020

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

1 Preliminary Definitions

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

2 Syntax

Following are the syntax of our system:

Programs	p	::=	$x = e \mid x \xleftarrow{\$} \mu \mid p; p$
Real Expr.	$e_{\mathbb{R}}$	::=	$X \mid r \mid F(D) \mid e_{\mathbb{R}} * e_{\mathbb{R}} \mid \circ(e_{\mathbb{R}})$
Floating Point Expr.	$e_{\mathbb{F}}$	::=	$x \mid c \mid f(D) \mid e_{\mathbb{F}} \circledast e_{\mathbb{F}} \mid \circledcirc(e_{\mathbb{F}})$
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	::=	$(e_{\mathbb{R}}, e_{\mathbb{R}})$
Transaction Env.	Θ	::=	$\cdot \mid \Theta[x \mapsto (e, err)]$
Evaluation Env.	Γ	::=	$\cdot \mid \Gamma[x \mapsto v]$

$\circledast$ and $\circledcirc$ represent the binary and unary operations in floating point computation. $F(D)$ and $f(D)$ denotes primitive query F evaluates to value $F(D)$ and $f(D)$ given input database D in real computation and floating point computation separately. We assume the query to be primitive, where the computation of the query results introduce no floating point error. We also assume the sample process, negation, rounding ($\lfloor\rceil$) and clamping ($\mathsf{clamp}_B()$) are perfect, i.e., introducing no error in floating point computation.

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

$$\frac{e^1_{\mathbb{R}} \Rightarrow e^1_{\mathbb{F}}, (e^1_{\underline{\mathbb{R}}}, e^1_{\bar{\mathbb{R}}}) \qquad e^2_{\mathbb{R}} \Rightarrow e^2_{\mathbb{F}}, (e^2_{\underline{\mathbb{R}}}, e^2_{\bar{\mathbb{R}}}) \qquad e^1_{\mathbb{R}} * e^2_{\mathbb{R}} \geq 0}{e^1_{\mathbb{R}} * e^2_{\mathbb{R}} \Rightarrow e^1_{\mathbb{F}} \circledast e^2_{\mathbb{F}}, \big(\frac{e^1_{\underline{\mathbb{R}}} * e^2_{\underline{\mathbb{R}}}}{(1+\eta)}, (e^1_{\bar{\mathbb{R}}} * e^2_{\bar{\mathbb{R}}})(1+\eta)\big)}\ \text{BOP}$$

$$\frac{e^1_{\mathbb{R}} \Rightarrow e^1_{\mathbb{F}}, (e^1_{\underline{\mathbb{R}}}, e^1_{\bar{\mathbb{R}}}) \qquad e^2_{\mathbb{R}} \Rightarrow e^2_{\mathbb{F}}, (e^2_{\underline{\mathbb{R}}}, e^2_{\bar{\mathbb{R}}}) \qquad e^1_{\mathbb{R}} * e^2_{\mathbb{R}} < 0}{e^1_{\mathbb{R}} * e^2_{\mathbb{R}} \Rightarrow e^1_{\mathbb{F}} \circledast e^2_{\mathbb{F}}, \big((e^1_{\bar{\mathbb{R}}} * e^2_{\bar{\mathbb{R}}})(1+\eta), \frac{e^1_{\underline{\mathbb{R}}} * e^2_{\underline{\mathbb{R}}}}{(1+\eta)}\big)}\ \text{BOP-N}$$

$$\frac{e_{\mathbb{R}} \Rightarrow e_{\mathbb{F}}, (e_{\underline{\mathbb{R}}}, e_{\bar{\mathbb{R}}}) \qquad \circ(e_{\mathbb{R}}) \geq 0}{\circ(e_{\mathbb{R}}) \Rightarrow \circledcirc(e_{\mathbb{F}}), \big(\frac{\circ(e_{\underline{\mathbb{R}}})}{(1+\eta)}, (\circ(e_{\bar{\mathbb{R}}}))(1+\eta)\big)}\ \text{UOP} \qquad \frac{e_{\mathbb{R}} \Rightarrow e_{\mathbb{F}}, (e_{\underline{\mathbb{R}}}, e_{\bar{\mathbb{R}}}) \qquad \circ(e_{\mathbb{R}}) < 0}{\circ(e_{\mathbb{R}}) \Rightarrow \circledcirc(e_{\mathbb{F}}), \big((\circ(e_{\underline{\mathbb{R}}}))(1+\eta), \frac{\circ(e_{\bar{\mathbb{R}}})}{(1+\eta)}\big)}\ \text{UOP-NEG}$$

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

$$\frac{}{c \Downarrow c}\ \text{FVAL} \qquad \frac{e^1_{\mathbb{F}} \Downarrow c^1 \qquad e^2_{\mathbb{F}} \Downarrow c^2 \qquad c^1 \circledast c^2 = c}{e^1_{\mathbb{F}} \circledast e^2_{\mathbb{F}} \Downarrow c}\ \text{FBOP} \qquad \frac{e_{\mathbb{F}} \Downarrow c', \qquad \circledcirc(c') = c}{\circledcirc(e_{\mathbb{F}}) \Downarrow c}\ \text{FUOP}$$

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

Figure 2: Semantics of Evaluation for Floating Point and Real Expressions

3 Semantics

The transition semantics with relative floating point computation error are shown in Figure. 3. The semantics are $e_{\mathbb{R}} \Downarrow e_{\mathbb{F}}, err$, which means a real expression $e_{\mathbb{R}}$ can be transited in floating point computation expression $e_{\mathbb{F}}$ with error bound err, η is the machine epsilon.

Theorem 1 (Soundness Theorem)
Given $e_{\mathbb{R}}$ and $e_{\mathbb{F}}$ where the transition $e_{\mathbb{R}} \Downarrow e_{\mathbb{F}}, (e^1_{\mathbb{R}}, e^2_{\mathbb{R}})$ holds, if $e_{\mathbb{F}}$ evaluates to c in floating point computation and $e_{\mathbb{R}}$, $e^1_{\mathbb{R}}$ and $e^2_{\mathbb{R}}$ evaluates to r, r^1 and r^2 in real computation, then:

$$r^1 \leq c \leq r^2$$

Proof. Induction on $e_{\mathbb{R}}$, we have following cases:

□

$$\frac{\Theta(X) = (e_{\underline{\mathbb{R}}}, e_{\bar{\mathbb{R}}})}{\Theta, X \Rightarrow (e_{\underline{\mathbb{R}}}, e_{\bar{\mathbb{R}}})}\ \text{VAR} \qquad \frac{X \notin dom(\Theta)}{\Theta, X \Rightarrow (X, X)}\ \text{VAR-NON} \qquad \frac{r \geq 0}{\Theta, r \Rightarrow \left(\frac{r}{(1+\eta)}, r(1+\eta)\right)}\ \text{VAL}$$

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

$$\frac{\Theta, e^1_{\mathbb{R}} \Rightarrow (e^1_{\underline{\mathbb{R}}}, e^1_{\bar{\mathbb{R}}}) \qquad \Theta, e^2_{\mathbb{R}} \Rightarrow (e^2_{\underline{\mathbb{R}}}, e^2_{\bar{\mathbb{R}}}) \qquad e^1_{\mathbb{R}} * e^2_{\mathbb{R}} \geq 0}{\Theta, e^1_{\mathbb{R}} * e^2_{\mathbb{R}} \Rightarrow \left(\frac{e^1_{\underline{\mathbb{R}}} * e^2_{\underline{\mathbb{R}}}}{(1+\eta)}, (e^1_{\bar{\mathbb{R}}} * e^2_{\bar{\mathbb{R}}})(1+\eta)\right)}\ \text{BOP}$$

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

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

Figure 3: Semantics of Transition for Expressions with Relative Floating Point Error

$$\frac{\Theta, e_{\mathbb{R}} \Rightarrow err}{\Theta, X = e_{\mathbb{R}} \Rightarrow \Theta[X \mapsto err]}\ \text{ASG} \qquad \frac{\Theta, p_1 \Rightarrow \Theta_1 \qquad \Theta_2, p_2 \Rightarrow \Theta_2}{\Theta, p_1; p_2 \Downarrow \Theta_2}\ \text{CONSQ} \qquad \frac{}{\Theta, x \overset{\$}{\leftarrow} \mu \Downarrow \Theta[x \mapsto \overset{\$}{\leftarrow} \mu]}\ \text{SAMPLE}$$

Figure 4: Semantics of Transition with Relative Floating Point Error Propagation for Programs

4 Semantics For Programs

The transition semantics with relative floating point computation error are shown in Figure. 3 for programs. The semantics are $\Theta, p_{\mathbb{R}} \Downarrow p_{\mathbb{F}}, \Theta$, which means a real programs $p_{\mathbb{R}}$ can be transited in floating point computation program $p_{\mathbb{F}}$ with error bound for all variables in Θ, η is the machine epsilon.

Theorem 2 (Soundness Theorem)
For any p, if the transition $\cdot, p \Rightarrow \Theta$ holds, then $\forall x \in dom(\Theta)$ s.t. $\Theta(x) = (e, (e_{\underline{\mathbb{R}}}, e_{\bar{\mathbb{R}}}))$, we have if e evaluates to c in floating point computation and $e_{\underline{\mathbb{R}}}$ and $e_{\bar{\mathbb{R}}}$ evaluates to $\underline{r}$ and $\bar{r}$ in real computation, then:

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

Proof. Induction on $e_{\mathbb{R}}$, we have following cases:

□

$$\frac{}{c \Downarrow c}\ \text{FVAL} \qquad \frac{e^1_{\mathbb{F}} \Downarrow c^1 \qquad e^2_{\mathbb{F}} \Downarrow c^2 \qquad c^1 \circledast c^2 = c}{e^1_{\mathbb{F}} \circledast e^2_{\mathbb{F}} \Downarrow c}\ \text{FBOP} \qquad \frac{e_{\mathbb{F}} \Downarrow c', \qquad \circledcirc(c') = c}{\circledcirc(e_{\mathbb{F}}) \Downarrow c}\ \text{FUOP}$$

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

Figure 5: Semantics of Evaluation for Floating Point and Real Expressions

5 Snapping Mechanism

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

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

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

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

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

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

6 Main Theorem

Theorem 3 (**The** Snap **mechanism is** $\epsilon-$**differentially private**)
Consider $\mathsf{Snap}(a)$ defined as before, if $\mathsf{Snap}(a) = x$ given database a and privacy parameter ϵ, then its actual privacy loss is bounded by $\epsilon + 12x\epsilon\eta + 2\eta$

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

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

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

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

case $x = -B$

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

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

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

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

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

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

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

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

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

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

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

subcase $\lfloor f(a)\rceil_\Lambda \le 0 \vee \left(\lfloor f(a)\rceil_\Lambda > 0 \wedge x \in (-B, 0)\right)$

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{R \Downarrow r, (R, R)}\ \text{VAL-EQ}}{\ln(R) \Downarrow \textcircled{n}(r), (\ln(R)(1+\eta), \dfrac{\ln(R)}{(1+\eta)})}\ \text{OP}}{\dfrac{1}{\epsilon} \times \ln(R) \Downarrow \dfrac{1}{\epsilon} \otimes \textcircled{n}(r), ((\dfrac{1}{\epsilon} \times \ln(R))(1+\eta)^2, \dfrac{\frac{1}{\epsilon} \times \ln(R)}{(1+\eta)^2})}\ \text{OP}}{f(a) + \dfrac{1}{\epsilon} \times \ln(R) \Downarrow f(a) \oplus \dfrac{1}{\epsilon} \otimes \textcircled{n}(r), \left(\left(f(a) + (\dfrac{1}{\epsilon} \times \ln(R))(1+\eta)^2\right)(1+\eta), \dfrac{(f(a) + \frac{\frac{1}{\epsilon} \times \ln(R)}{(1+\eta)^2})}{(1+\eta)}\right)}\ \text{ID}$$

$$\overline{\mathsf{Snap}'_{\mathbb{R}}(a, R, 1) \Downarrow \mathsf{Snap}'_{\mathbb{F}}(a, r, 1), (e^1_{\mathbb{R}}, e^2_{\mathbb{R}})}$$

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

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

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

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

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

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

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

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

Then, we have the privacy loss is bounded by:

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

We also have:

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

Then, we can derive:

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

In the same way, we can derive:

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

Then we have:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

So we can get:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$\underline{R_2} = e^{\epsilon\left((f(a) - y_1(1+\eta))(1+\eta)^2\right)}$, $\bar{R_2} = e^{\epsilon \frac{(f(a) - \frac{y_1}{1+\eta})}{(1+\eta)^2}}$.

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

We have following bounds on their ratios:

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

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

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

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

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

Then we have the following bounds on privacy loss:

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

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

This case is symmetric with the case where $x = \lfloor f(a') \rceil_\Lambda$. 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:

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

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

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

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:

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

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

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

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

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

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

let $y_1 = x - \frac{\Lambda}{2}$, $y_2 = x + \frac{\Lambda}{2}$, we have $y_1, y_2 > 0$. The bounds derived for l, r 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 $x = B$

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

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

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

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

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

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

□

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.