Verifying Snapping Mechanism - Floating Point Implementation Version

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

1 Preliminary Definitions

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

2 Syntax

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

$$
\begin{array}{llll}
\text{Expr.} & e & ::= & r \mid c \mid x \mid f(x) \mid e_1 \oplus e_2 \mid e_1 \otimes e_2 \mid e_1 \ominus e_2 \mid e_1 \oslash e_2 \mid \text{ⓛⓝ}(e) \mid x \xleftarrow{\$} \mu \\
\text{Value} & v & ::= & r \mid c \\
\text{Distribution} & \mu & ::= & \mathsf{laplce} \mid \mathsf{unif} \mid \mathtt{bernoulli} \\
\text{Error} & err & ::= & (e_1, e_2) \\
\text{Condition} & \Phi & ::= & \mathtt{true} \mid \mathtt{false} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2
\end{array}
$$

Definition 2 ($\mathsf{Snap}(a) : A \to \mathsf{Distr}(B)$)
The ideal Snapping mechanism $\mathsf{Snap}(a)$ is defined as:

$$u \xleftarrow{\$} \mu; y = \text{ⓛⓝ}(u) \oslash \epsilon; s \xleftarrow{\$} \{-1, 1\}; z = s \otimes y; x = f(a); w = x \oplus z; w' = \lfloor w \rceil_\Lambda; r = \mathsf{clamp}_B(w')$$

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

3 Semantics

The big step semantics with floating point computation error are shown in Figure. 1.

The big step semantics with relative floating point computation error are shown in Figure. 2.

$$\frac{(e_1, err, \Phi) \Downarrow (r_1, err_1) \qquad (e_2, err, \Phi) \Downarrow (r_2, err_2)}{(e_1 \oplus e_2, err, \Phi) \Downarrow (r_1 + r_2, err_1 \uplus err_2 \uplus err, \Phi_1 \wedge \Phi_2 \wedge \Phi)} \text{ PLUS} \qquad \cdots$$

Figure 1: Semantics with Absolutes Floating Point Error [2]

$$\frac{c = \texttt{fl}(r)}{r \Downarrow c, \big(r(1-\eta), r(1+\eta)\big)} \text{ CONST} \qquad \frac{e_1 \Downarrow c_1, (\underline{r_1}, \bar{r_1}) \qquad e_2 \Downarrow c_2, (\underline{r_2}, \bar{r_2})}{e_1 \oplus e_2 \Downarrow \texttt{fl}(c_1 + c_2), \big((\underline{r_1} + \underline{r_2})(1-\eta), (\bar{r_1} + \bar{r_2})(1+\eta)\big)} \text{ PLUS}$$

$$\frac{e_1 \Downarrow c_1, (\underline{r_1}, \bar{r_1}) \qquad e_2 \Downarrow c_2, (\underline{r_2}, \bar{r_2})}{e_1 \otimes e_2 \Downarrow \texttt{fl}(c_1 \times c_2), \big((\underline{r_1} \times \underline{r_2})(1-\eta), (\bar{r_1} \times \bar{r_2})(1+\eta)\big)} \text{ TIMES}$$

$$\frac{e_1 \Downarrow c_1, (\underline{r_1}, \bar{r_1}) \qquad e_2 \Downarrow c_2, (\underline{r_2}, \bar{r_2})}{e_1 \ominus e_2 \Downarrow \texttt{fl}(c_1 - c_2), \big((\underline{r_1} - \underline{r_2})(1-\eta), (\bar{r_1} - \bar{r_2})(1+\eta)\big)} \text{ SUB}$$

Figure 2: Semantics with Relative Floating Point Error (By Jiawen)

4 Main Theorem

Theorem 1 (The Snap mechanism is ϵ−differentially private)
Consider $\mathsf{Snap}(a)$ defined as before, if $\mathsf{Snap}(a) = x$ given database a and privacy parameter ϵ, then its actual privacy loss is bounded by $\epsilon + 12x\epsilon\eta + 2\eta$

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

case $x = -B$

Let b be the largest number rounded by Λ that is smaller than B. Based on the proof of the ideal version, the derivation of this case given $\mathsf{Snap}(a) = \mathsf{Snap}(a') = x$ is shown as following:

$$\frac{\dfrac{u \in \big(0, ⓔ^{\epsilon \otimes (-b \ominus \frac{\Lambda}{2} \ominus f(a))}\big) \sim u' \in \big(0, ⓔ^{\epsilon \otimes (-b \ominus \frac{\Lambda}{2} \ominus f(a'))}\big)}{\cdots}}{\mathsf{Snap}(a) = -B \sim \mathsf{Snap}(a') = -B}$$

Following the semantics in Figure 2, we have following evaluation results:

$$u \in \big(0, (\underline{r}, \bar{r})\big) \wedge (s = -1) \sim u' \in \big(0, (\underline{r}', \bar{r}')\big) \wedge (s = -1)$$

[[where $\underline{r}, \bar{r}, \underline{r}'$ and $\bar{r}'$ have following values:

$$u \in \Big(0, (e^{\epsilon(\frac{-b-\frac{\Lambda}{2}}{1+\eta} - f(a))(1+\eta)^2)}, e^{\epsilon \frac{(-b-\frac{\Lambda}{2})(1+\eta) - f(a)}{(1+\eta)^2}})\Big) \wedge (s = -1)$$
$$\sim u' \in \Big(0, (e^{\epsilon(\frac{-b-\frac{\Lambda}{2}}{1+\eta} - f(a'))(1+\eta)^2)}, e^{\epsilon \frac{(-b-\frac{\Lambda}{2})(1+\eta) - f(a')}{(1+\eta)^2}})\Big) \wedge (s = -1)$$

Given that the probability is equivalent to the length of the range, we have the ratio between u and u' is bounded by:

$$\frac{u}{u'} \le \frac{\frac{1}{2}\bar{r}}{\frac{1}{2}\underline{r}'} = e^{\epsilon((-b-\frac{\Lambda}{2})(1+\eta-\frac{1}{1+\eta})+f(a)((1+\eta)^2-\frac{1}{(1+\eta)^2})+(1+\eta)^2)} \le e^{\epsilon(1+\eta)^2 2B} ? \le e^{\epsilon+12B\epsilon\eta+2\eta}$$

By the AxUnif rule, we have the actual privacy loss is bounded by the same value.]]

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

The derivation of this case is shown as following:

$$\dfrac{\dfrac{\dfrac{\dfrac{u \in \left[ⓔ^{\epsilon \otimes (x \ominus \frac{\Lambda}{2} \ominus f(a))}, ⓔ^{\epsilon \otimes (x \oplus \frac{\Lambda}{2} \ominus f(a))} \right) \sim u' \in \left[ⓔ^{\epsilon \otimes (x \ominus \frac{\Lambda}{2} \ominus f(a'))}, ⓔ^{\epsilon \otimes (x \oplus \frac{\Lambda}{2} \ominus f(a'))} \right)}{\cdots}}{\mathsf{Snap}''(a) \in [x \ominus \frac{\Lambda}{2} \ominus f(a), x \oplus \frac{\Lambda}{2} \ominus f(a)) \sim_{\_} \mathsf{Snap}''(a') \in [x \ominus \frac{\Lambda}{2} \ominus f(a'), x \oplus \frac{\Lambda}{2} \ominus f(a'))}}{\mathsf{Snap}'(a) \in [x \ominus \frac{\Lambda}{2}, x \oplus \frac{\Lambda}{2}) \sim_{\_} \mathsf{Snap}'(a') \in [x \ominus \frac{\Lambda}{2}, x \oplus \frac{\Lambda}{2})}}{\mathsf{Snap}(a) = x \sim \mathsf{Snap}(a') = x}$$

Following the semantics in Figure 2, we have following evaluation results:

$$u \in \left[(\underline{r}_1, \bar{r}_1), (\underline{r}_2, \bar{r}_2) \right) \land (s = -1) \sim u' \in \left[(\underline{r}'_1, \bar{r}'_1), (\underline{r}'_2, \bar{r}'_2) \right) \land (s = -1)$$

[[where $\underline{r}_1, \bar{r}_1, \underline{r}_2, \bar{r}_2, \underline{r}'_1, \bar{r}'_1, \underline{r}'_2 and \bar{r}'_2$ **have following values:**

$$u \in \left[((1-\eta)e^{\epsilon(x-\frac{\Lambda}{2}-f(a))(1-\eta)^2}, (1+\eta)e^{\epsilon(x-\frac{\Lambda}{2}-f(a))(1+\eta)^2}), ((1-\eta)e^{\epsilon(x+\frac{\Lambda}{2}-f(a))(1-\eta)^2}, (1+\eta)e^{\epsilon(x+\frac{\Lambda}{2}-f(a))(1+\eta)^2}) \right)$$
$$\sim u' \in \left[((1-\eta)e^{\epsilon(x-\frac{\Lambda}{2}-f(a'))(1-\eta)^2}, (1+\eta)e^{\epsilon(x-\frac{\Lambda}{2}-f(a'))(1+\eta)^2}), ((1-\eta)e^{\epsilon(x+\frac{\Lambda}{2}-f(a'))(1-\eta)^2}, (1+\eta)e^{\epsilon(x+\frac{\Lambda}{2}-f(a'))(1+\eta)^2}) \right)$$

Given that the probability is equivalent to the length of the range, we have the ratio between u and u' is bounded by:

$$\frac{u}{u'} \le \frac{\bar{r}_2 - \underline{r}_1}{\underline{r}'_2 - \bar{r}'_1} \le \epsilon + 12x\epsilon\eta + 2\eta$$

By the AxUnif rule, we have the actual privacy loss is bounded by the same value.]]

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

$$\dfrac{\dfrac{u \in \left(ⓔ^{\epsilon \otimes (\lfloor f(a) \rceil_\Lambda \ominus \frac{\Lambda}{2} \ominus f(a))}, 1 \right] \lor \left(ⓔ^{\epsilon \otimes (f(a) \ominus \lfloor f(a) \rceil_\Lambda \ominus \frac{\Lambda}{2})}, 1 \right] \sim u' \in \left(ⓔ^{\epsilon \otimes (\lfloor f(a) \rceil_\Lambda \ominus f(a') \ominus \frac{\Lambda}{2})}, ⓔ^{\epsilon \otimes (\lfloor f(a) \rceil_\Lambda \ominus f(a') \oplus \frac{\Lambda}{2})} \right)}{\cdots}}{\mathsf{Snap}(a) = x \sim \mathsf{Snap}(a') = x}$$

Following the semantics in Figure 2, we have following evaluation results:

$$u \in \left[(\underline{r}_1, \bar{r}_1), 1 \right] \land (s = -1) \lor u \in \left[(\underline{r}_2, \bar{r}_2), 1 \right] \land (s = 1) \sim u' \in \left[(\underline{r}'_1, \bar{r}'_1), (\underline{r}'_2, \bar{r}'_2) \right) \land (s = -1),$$

[[where $\underline{r}_1, \bar{r}_1, \underline{r}_2, \bar{r}_2, \underline{r}'_1, \bar{r}'_1, \underline{r}'_2 and \bar{r}'_2$ **have following values: Given that the probability is equivalent to the length of the range, we have the ratio between u and u' is bounded by:**

$$\frac{u}{u'} \le \frac{1 - \frac{1}{2}(\underline{r}_2 + \underline{r}_1)}{\frac{1}{2}(\underline{r}'_2 - \bar{r}'_1)} \le \epsilon + 12x\epsilon\eta + 2\eta$$

By the AxUnif rule, we have the actual privacy loss is bounded by the same value.]]

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

$$\frac{\dfrac{u \in \left(ⓔ^{\epsilon \otimes (f(a) \oplus \frac{\Lambda}{2} \ominus \lfloor f(a) \rceil_\Lambda)}, ⓔ^{\epsilon \otimes (f(a) \ominus \frac{\Lambda}{2} \ominus \lfloor f(a) \rceil_\Lambda)}\right] \sim u' \in \left(ⓔ^{\epsilon \otimes (\lfloor f(a) \rceil_\Lambda \ominus f(a') \oplus \frac{\Lambda}{2})}, ⓔ^{\epsilon \otimes (\lfloor f(a) \rceil_\Lambda \ominus f(a') \ominus \frac{\Lambda}{2})}\right)}{\cdots}}{\mathsf{Snap}(a) = x \sim \mathsf{Snap}(a') = x}$$

Following the semantics in Figure 2, we have following evaluation results:

$$u \in \left((\underline{r_1}, \bar{r_1}), (\underline{r_2}, \bar{r_2})\right] \wedge (s = 1) \sim u' \in \left[(\underline{r'_1}, \bar{r'_1}), (\underline{r'_2}, \bar{r'_2})\right) \wedge (s = -1),$$

[[where $\underline{r_1}, \bar{r_1}, \underline{r_2}, \bar{r_2}, \underline{r'_1}, \bar{r'_1}, \underline{r'_2} and \bar{r'_2}$ have following values: Given that the probability is equivalent to the length of the range, we have the ratio between u and u' is bounded by:

$$\frac{u}{u'} \leq \frac{\frac{1}{2}(\bar{r_2} - \underline{r_1})}{\frac{1}{2}(\underline{r'_2} - \bar{r'_1})} \leq \epsilon + 12x\epsilon\eta + 2\eta$$

By the AxUnif rule, we have the actual privacy loss is bounded by the same value.]]

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

$$\frac{\dfrac{u \in \left(ⓔ^{\epsilon \otimes (f(a) \ominus \frac{\Lambda}{2} \ominus \lfloor f(a') \rceil_\Lambda)}, ⓔ^{\epsilon \otimes (f(a) \oplus \frac{\Lambda}{2} \ominus \lfloor f(a') \rceil_\Lambda)}\right] \sim u' \in \left(ⓔ^{\epsilon \otimes (\lfloor f(a) \rceil_\Lambda \ominus f(a') \ominus \frac{\Lambda}{2})}, 1\right] \vee u' \in \left(ⓔ^{\epsilon \otimes (f(a) \ominus \lfloor f(a') \rceil_\Lambda \ominus \frac{\Lambda}{2})} 1, \right]}{\cdots}}{\mathsf{Snap}(a) = x \sim \mathsf{Snap}(a') = x}$$

Following the semantics in Figure 2, we have following evaluation results:

$$u \in \left((\underline{r_1}, \bar{r_1}), (\underline{r_2}, \bar{r_2})\right] \wedge (s = 1) \sim u' \in \left[(\underline{r'_1}, \bar{r'_1}), 1\right] \wedge (s = -1) \vee \left[(\underline{r'_2}, \bar{r'_2}), 1\right] \wedge (s = 1),$$

[[where $\underline{r_1}, \bar{r_1}, \underline{r_2}, \bar{r_2}, \underline{r'_1}, \bar{r'_1}, \underline{r'_2} and \bar{r'_2}$ have following values: Given that the probability is equivalent to the length of the range, we have the ratio between u and u' is bounded by:

$$\frac{u}{u'} \leq \frac{\frac{1}{2}(\bar{r_2} - \underline{r_1})}{1 - \frac{1}{2}(\underline{r'_2} + \bar{r'_1})} \leq \epsilon + 12x\epsilon\eta + 2\eta$$

By the AxUnif rule, we have the actual privacy loss is bounded by the same value.]]

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

$$\frac{\dfrac{u \in \left(ⓔ^{\epsilon \otimes (f(a) \oplus \frac{\Lambda}{2} \ominus x)}, ⓔ^{\epsilon \otimes (f(a) \ominus \frac{\Lambda}{2} \ominus x)}\right] \sim u' \in \left(ⓔ^{\epsilon \otimes (f(a') \oplus \frac{\Lambda}{2} \ominus x)}, ⓔ^{\epsilon \otimes (f(a') \ominus \frac{\Lambda}{2} \ominus x)}\right)}{\cdots}}{\mathsf{Snap}(a) = x \sim \mathsf{Snap}(a') = x}$$

Following the semantics in Figure 2, we have following evaluation results:

$$u \in \left((\underline{r_1}, \bar{r_1}), (\underline{r_2}, \bar{r_2})\right] \wedge (s = 1) \sim u' \in \left((\underline{r'_1}, \bar{r'_1}), (\underline{r'_2}, \bar{r'_2})\right] \wedge (s = 1),$$

[[where $\underline{r_1}, \bar{r_1}, \underline{r_2}, \bar{r_2}, \underline{r'_1}, \bar{r'_1}, \underline{r'_2} and \bar{r'_2}$ have following values: Given that the probability is equivalent to the length of the range, we have the ratio between u and u' is bounded by:

$$\frac{u}{u'} \leq \frac{\frac{1}{2}(\bar{r_2} - \underline{r_1})}{\frac{1}{2}(\underline{r'_2} - \bar{r'_1})} \leq \epsilon + 12x\epsilon\eta + 2\eta$$

By the AxUnif rule, we have the actual privacy loss is bounded by the same value.]]

case $\boldsymbol{x = B}$

$$\frac{\dfrac{u \in \left(0, ⓔ^{\epsilon \otimes (-b \ominus \frac{\Lambda}{2} \oplus f(a))}\right) \sim u' \in \left(0, ⓔ^{\epsilon \otimes (-b \ominus \frac{\Lambda}{2} \oplus f(a'))}\right)}{\cdots}}{\mathsf{Snap}(a) = B \sim \mathsf{Snap}(a') = B}$$

Following the semantics in Figure 2, we have following evaluation results:

$$u \in \left(0, (\underline{r}, \bar{r})\right) \sim u' \in \left(0, (\underline{r}', \bar{r}')\right),$$

[[where $\underline{r}, \bar{r}, \underline{r}'$ and $\bar{r}'$ have following values: Given that the probability is equivalent to the length of the range, we have the ratio between u and u' is bounded by:

$$\frac{u}{u'} \leq \frac{\frac{1}{2}\bar{r}}{\frac{1}{2}\underline{r}'} \leq \epsilon + 12x\epsilon\eta + 2\eta$$

By the AxUnif rule, we have the actual privacy loss is bounded by the same value.]]

$\square$

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.