

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

2 Syntax

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

Expr.	e	$::=$	$r \mid c \mid x \mid f(x) \mid e_1 \oplus e_2 \mid e_1 \otimes e_2 \mid e_1 \ominus e_2 \mid e_1 \oslash e_2 \mid \textcircled{\cap}(e) \mid x \stackrel{\$}{\leftarrow} \mu$
Value	v	$::=$	$r \mid c$
Distribution	μ	$::=$	$\text{laplce} \mid \text{unif} \mid \text{bernoulli}$
Error	err	$::=$	(e_1, e_2)
Condition	Φ	$::=$	$\text{true} \mid \text{false} \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2$

Definition 2 ($\text{Snap}(a) : A \rightarrow \text{Distr}(B)$)

The ideal Snapping mechanism $\text{Snap}(a)$ is defined as:

$$u \stackrel{\$}{\leftarrow} \mu; y = \textcircled{\cap}(u) \oslash \epsilon; s \stackrel{\$}{\leftarrow} \{-1, 1\}; z = s \otimes y; x = f(a); w = x \oplus z; w' = \lfloor w \rfloor_\Lambda; r = \text{clamp}_B(w')$$

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.

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

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

$$\begin{aligned} & \frac{c = \text{fl}(r)}{r \Downarrow c, (r(1-\eta), r(1+\eta))} \text{ CONST} \quad \frac{e_1 \Downarrow c_1, (r_1, \bar{r}_1) \quad e_2 \Downarrow c_2, (r_2, \bar{r}_2)}{e_1 \oplus e_2 \Downarrow \text{fl}(c_1 + c_2), ((r_1 + r_2)(1-\eta), (\bar{r}_1 + \bar{r}_2)(1+\eta))} \text{ PLUS} \\ & \frac{e_1 \Downarrow c_1, (r_1, \bar{r}_1) \quad e_2 \Downarrow c_2, (r_2, \bar{r}_2)}{e_1 \otimes e_2 \Downarrow \text{fl}(c_1 \times c_2), ((r_1 \times r_2)(1-\eta), (\bar{r}_1 \times \bar{r}_2)(1+\eta))} \text{ TIMES} \\ & \frac{e_1 \Downarrow c_1, (r_1, \bar{r}_1) \quad e_2 \Downarrow c_2, (r_2, \bar{r}_2)}{e_1 \ominus e_2 \Downarrow \text{fl}(c_1 - c_2), ((r_1 - r_2)(1-\eta), (\bar{r}_1 - \bar{r}_2)(1+\eta))} \text{ SUB} \end{aligned}$$

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

4 Soundness Theorems

Theorem 1 (The Snap mechanism is ϵ -differentially private)

Consider $\text{Snap}(a)$ defined as before, if $\text{Snap}(a) = x$ given database a and privacy parameter ϵ , then its actual privacy loss is bounded by $\epsilon + 12x\epsilon\eta + 2\eta$

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

$$\frac{u \in (0, \ominus^{\epsilon \otimes (-b \ominus \frac{\Lambda}{2} \ominus f(a))}) \sim u' \in (0, \ominus^{\epsilon \otimes (-b \ominus \frac{\Lambda}{2} \ominus f(a'))})}{\dots} \quad \frac{\dots}{\text{Snap}(a) = -B \sim \text{Snap}(a') = -B}$$

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

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

[[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.]]

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

The derivation of this case is shown as following:

$$\begin{array}{c}
 \frac{u \in [\ominus^{\epsilon \otimes (x \ominus \frac{\Lambda}{2} \ominus f(a))}, \ominus^{\epsilon \otimes (x \oplus \frac{\Lambda}{2} \ominus f(a))}] \sim u' \in [\ominus^{\epsilon \otimes (x \ominus \frac{\Lambda}{2} \ominus f(a'))}, \ominus^{\epsilon \otimes (x \oplus \frac{\Lambda}{2} \ominus f(a'))}]}{\dots} \\
 \frac{\text{Snap}''(a) \in [x \ominus \frac{\Lambda}{2} \ominus f(a), x \oplus \frac{\Lambda}{2} \ominus f(a)] \sim \text{Snap}''(a') \in [x \ominus \frac{\Lambda}{2} \ominus f(a'), x \oplus \frac{\Lambda}{2} \ominus f(a')]}{\text{Snap}'(a) \in [x \ominus \frac{\Lambda}{2}, x \oplus \frac{\Lambda}{2}] \sim \text{Snap}'(a') \in [x \ominus \frac{\Lambda}{2}, x \oplus \frac{\Lambda}{2}]} \\
 \text{Snap}(a) = x \sim \text{Snap}(a') = x
 \end{array}$$

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

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

[[where $r_1, \bar{r}_1, r_2, \bar{r}_2, r'_1, \bar{r}'_1, r'_2, \bar{r}'_2$ have following values:

$$\begin{aligned}
 u &\in [((1-\eta)e^{\epsilon(x-\frac{\Lambda}{2}-f(a))(1-\eta)^2}, (1+\eta)e^{\epsilon(x-\frac{\Lambda}{2}-f(a))(1+\eta)^2}), ((1-\eta)e^{\epsilon(x+\frac{\Lambda}{2}-f(a))(1-\eta)^2}, (1+\eta)e^{\epsilon(x+\frac{\Lambda}{2}-f(a))(1+\eta)^2})] \\
 &\sim u' \in [((1-\eta)e^{\epsilon(x-\frac{\Lambda}{2}-f(a'))(1-\eta)^2}, (1+\eta)e^{\epsilon(x-\frac{\Lambda}{2}-f(a'))(1+\eta)^2}), ((1-\eta)e^{\epsilon(x+\frac{\Lambda}{2}-f(a'))(1-\eta)^2}, (1+\eta)e^{\epsilon(x+\frac{\Lambda}{2}-f(a'))(1+\eta)^2})]
 \end{aligned}$$

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

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

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

case $x = \lfloor f(a) \rfloor_\Lambda$

$$\begin{array}{c}
 \frac{u \in (\ominus^{\epsilon \otimes (\lfloor f(a) \rfloor_\Lambda \ominus \frac{\Lambda}{2} \ominus f(a))}, 1] \vee (\ominus^{\epsilon \otimes (f(a) \ominus \lfloor f(a) \rfloor_\Lambda \ominus \frac{\Lambda}{2})}, 1] \sim u' \in (\ominus^{\epsilon \otimes (\lfloor f(a) \rfloor_\Lambda \ominus f(a') \ominus \frac{\Lambda}{2})}, \ominus^{\epsilon \otimes (\lfloor f(a) \rfloor_\Lambda \ominus f(a') \oplus \frac{\Lambda}{2})})}{\dots} \\
 \text{Snap}(a) = x \sim \text{Snap}(a') = x
 \end{array}$$

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

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

[[where $r_1, \bar{r}_1, r_2, \bar{r}_2, r'_1, \bar{r}'_1, r'_2, \bar{r}'_2$ 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:

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

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

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

$$\begin{array}{c}
 \frac{u \in (\ominus^{\epsilon \otimes (f(a) \ominus \frac{\Lambda}{2} \ominus \lfloor f(a) \rfloor_\Lambda)}, \ominus^{\epsilon \otimes (f(a) \ominus \frac{\Lambda}{2} \ominus \lfloor f(a) \rfloor_\Lambda)}) \sim u' \in (\ominus^{\epsilon \otimes (\lfloor f(a) \rfloor_\Lambda \ominus f(a') \oplus \frac{\Lambda}{2})}, \ominus^{\epsilon \otimes (\lfloor f(a) \rfloor_\Lambda \ominus f(a') \ominus \frac{\Lambda}{2})})}{\dots} \\
 \text{Snap}(a) = x \sim \text{Snap}(a') = x
 \end{array}$$

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

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

[[where $r_1, \bar{r}_1, r_2, \bar{r}_2, r'_1, \bar{r}'_1, r'_2, \bar{r}'_2$ 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:

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

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

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

$$\frac{u \in (\ominus^{\epsilon \otimes (f(a) \ominus \frac{\Lambda}{2} \ominus \lfloor f(a') \rfloor_\Lambda)}, \ominus^{\epsilon \otimes (f(a) \oplus \frac{\Lambda}{2} \ominus \lfloor f(a') \rfloor_\Lambda)}) \sim u' \in (\ominus^{\epsilon \otimes (\lfloor f(a) \rfloor_\Lambda \ominus f(a') \ominus \frac{\Lambda}{2})}, 1] \vee u' \in (\ominus^{\epsilon \otimes (f(a) \ominus \lfloor f(a') \rfloor_\Lambda \ominus \frac{\Lambda}{2})}, 1],}{\dots} \text{Snap}(a) = x \sim \text{Snap}(a') = x$$

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

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

[[where $r_1, \bar{r}_1, r_2, \bar{r}_2, r'_1, \bar{r}'_1, r'_2, \bar{r}'_2$ 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:

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

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

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

$$\frac{u \in (\ominus^{\epsilon \otimes (f(a) \oplus \frac{\Lambda}{2} \ominus x)}, \ominus^{\epsilon \otimes (f(a) \ominus \frac{\Lambda}{2} \ominus x)}) \sim u' \in (\ominus^{\epsilon \otimes (f(a') \oplus \frac{\Lambda}{2} \ominus x)}, \ominus^{\epsilon \otimes (f(a') \ominus \frac{\Lambda}{2} \ominus x)})}{\dots} \text{Snap}(a) = x \sim \text{Snap}(a') = x$$

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

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

[[where $r_1, \bar{r}_1, r_2, \bar{r}_2, r'_1, \bar{r}'_1, r'_2, \bar{r}'_2$ 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:

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

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

case $x = B$

$$\frac{u \in (0, \ominus^{\epsilon \otimes (-b \ominus \frac{\Lambda}{2} \oplus f(a))}) \sim u' \in (0, \ominus^{\epsilon \otimes (-b \ominus \frac{\Lambda}{2} \oplus f(a'))})}{\dots} \text{Snap}(a) = B \sim \text{Snap}(a') = B$$

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

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

[[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.]]

□

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.