A Noise Parameter Configuration Technique to Prevent Correlated Inference Attack using Differential Privacy

Taebo Jeong[1] inthewinter11@gmail.com

Sehwa Park[1] sehwapark@sogang.ac.kr

Kangsoo Jung[1] azure84@sogang.ac.kr

Seog Park[1] spark@sogang.ac.kr

[1]Sogang University, Korea

Introduction

Differential Privacy

Differential privacy ensures that the removal or addition of a single database item does not affect the outcome of any analysis.

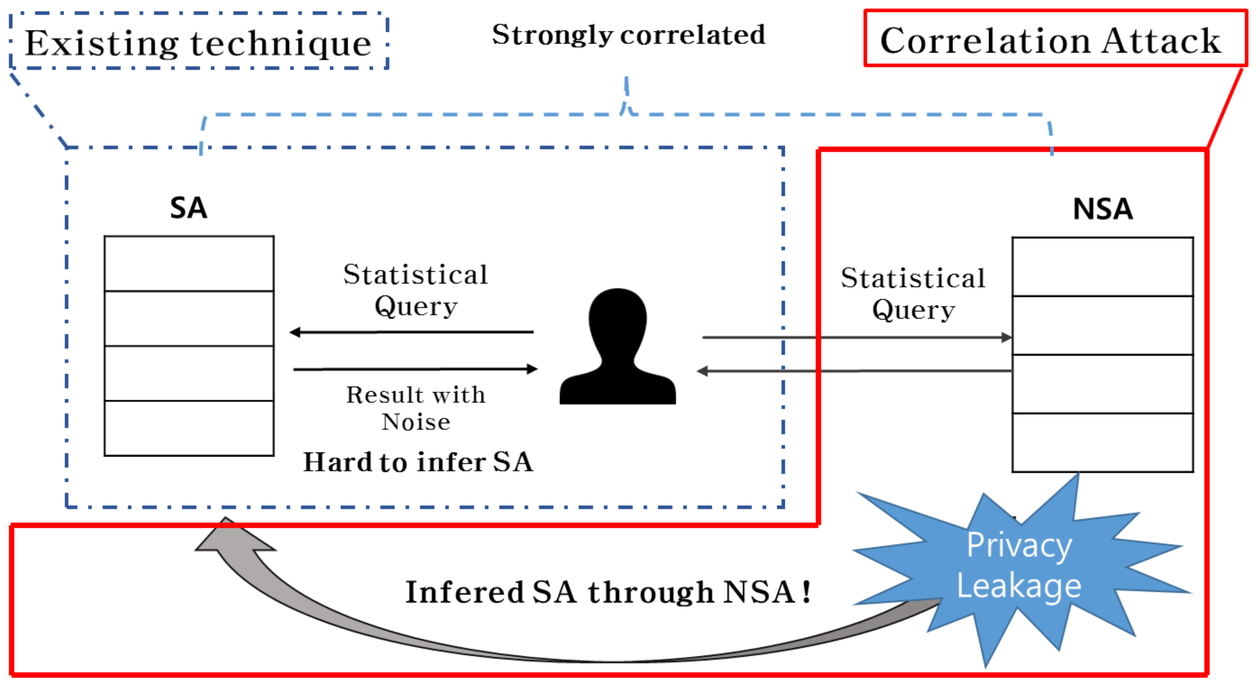
- A randomized function f gives ε-differential privacy if all data sets D and D' differing on at most element, and all $S \subseteq Range(f)$,

$$Prob[f(D) = S] \leq e^{\varepsilon} \cdot Prob[f(D') = S]$$

Problems

Existing studies do not consider correlation attack.

- Correlation between sensitive and non-sensitive attributes(NSA)
- Malicious users can get sensitive attribute(SA) through linear regression.



Proposed Technique

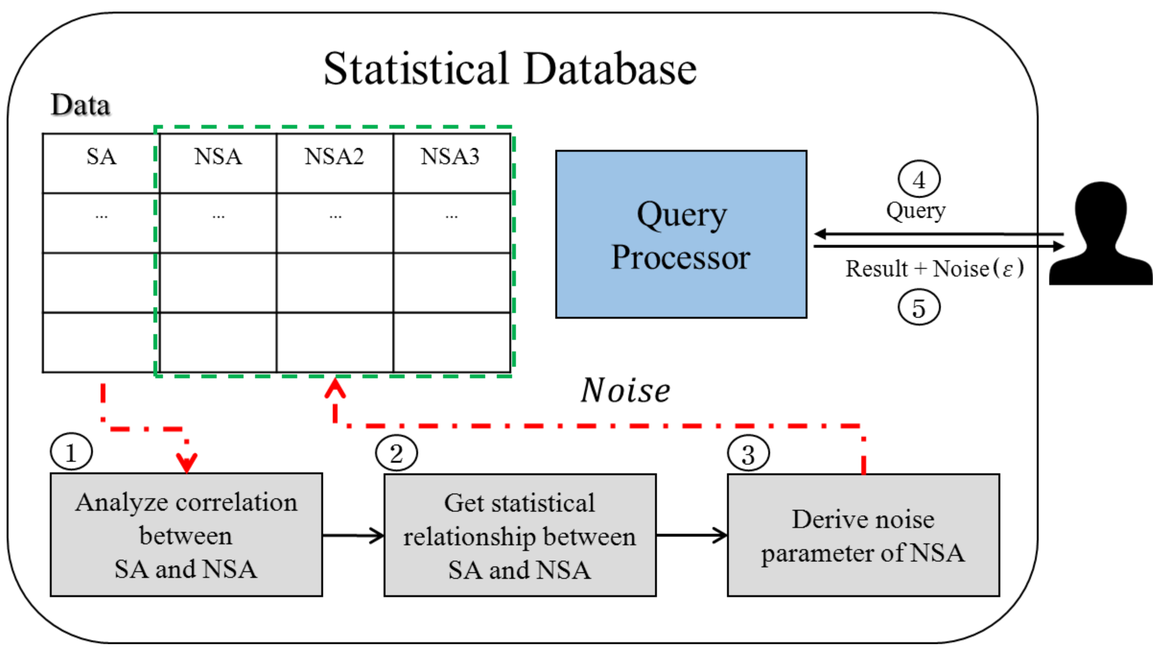
Goals

Preventing correlation attack.

- Disturb linear regression analysis.
- Do not increase noise of SA.
- Minimize performance degradation of NSA's data utility.

Overall Framework

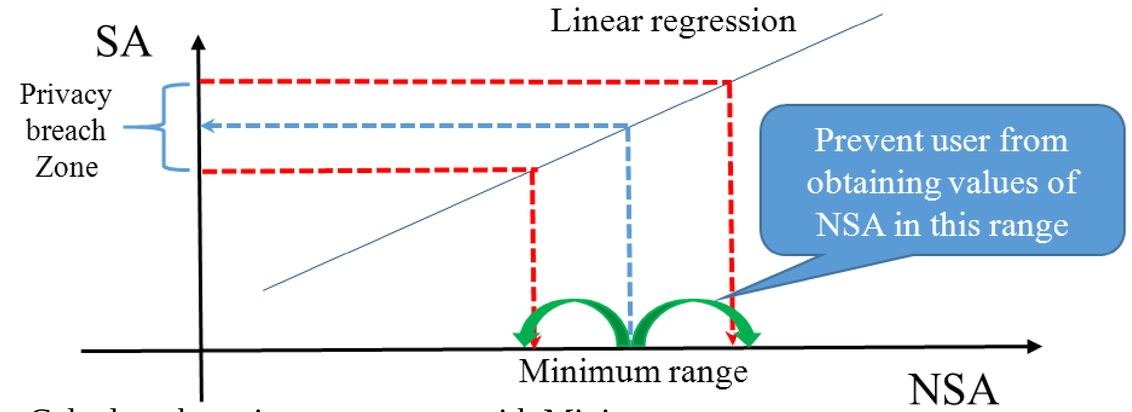
Our solution injects noise to NSA with minor overheads



Noise Parameter Setting

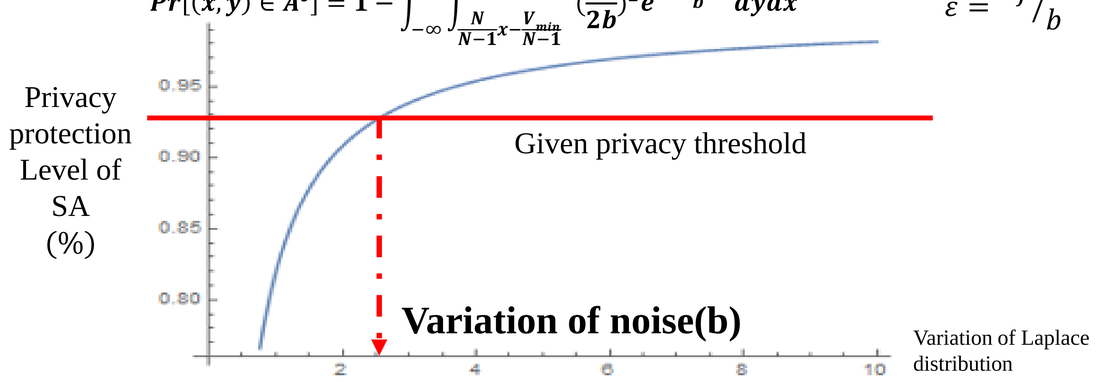
How much noise should be inserted?

1. Get range of NSA which can infer the exact value of SA with high probability.
   - ✓ Linear regression and given privacy threshold of SA



2. Calculate the noise parameter ε with Minimum range.
   - ✓ Apply differential privacy with derived ε to NSA.

$$Pr[(x, y) \in A^c] = 1 - \int_{-\infty}^{\infty} \int_{\frac{N}{N-1}x - \frac{V_{min}}{N-1}}^{\frac{N}{N-1}x + \frac{V_{min}}{N-1}} \left(\frac{1}{2b}\right)^2 e^{-\frac{|x|+|y|}{b}} dydx \qquad \varepsilon = \Delta f / b$$



Variation of Laplace distribution

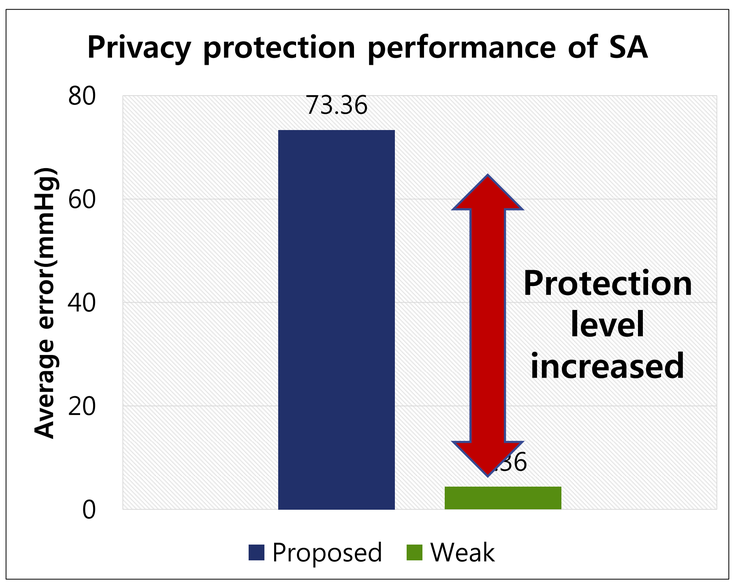
Experimental Results

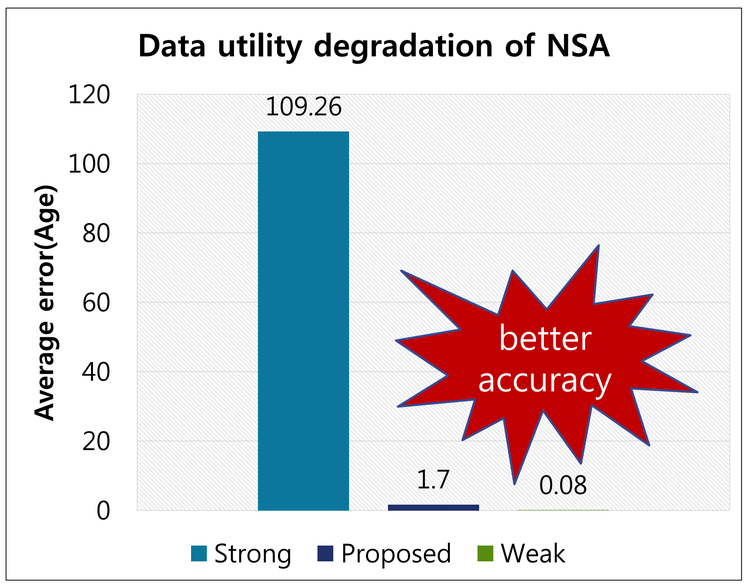
Dataset

- Correlation between age and blood pressure
- Privacy requirement
  - ✓ Safe boundary of SA: 10, Probability threshold: 90%
- Sensitive attribute: Blood Pressure
- Non-sensitive attribute: Age

Age	Blood pressure
39	144
45	138
47	145
65	162
…	…

- **Noise Parameters**
  - Proposed: 0.45
  - Strong: 0.01
  - Weak: 10
- **Correlation Attacks 50 times**
  - using average query





Acknowledgement. This research work is supported by DGIST Global CPS Center