Fuzzi: A Three Level Logic for Differential Privacy

Hengchu Zhang, Edo Roth, Andreas Haeberlen,
Benjamin C. Pierce, Aaron Roth

University of Pennsylvania

Differential Privacy is Useful

Census Bureau Adopts Cutting Edge Privacy Protections for 2020 Census

Fri Feb 15 2019

WRITTEN BY: DR. RON JARMIN. DEPUTY DIRECTOR AND COO

RESEARCH › PUBLICATIONS ›

RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response

Learning with Privacy at Scale

Vol. 1, Issue 8 • December 2017
by Differential Privacy Team

Differential Privacy is Useful

RESEARCH › PUBLICATIONS ›

RAPPOR: Randomized

$\forall \; \sim$

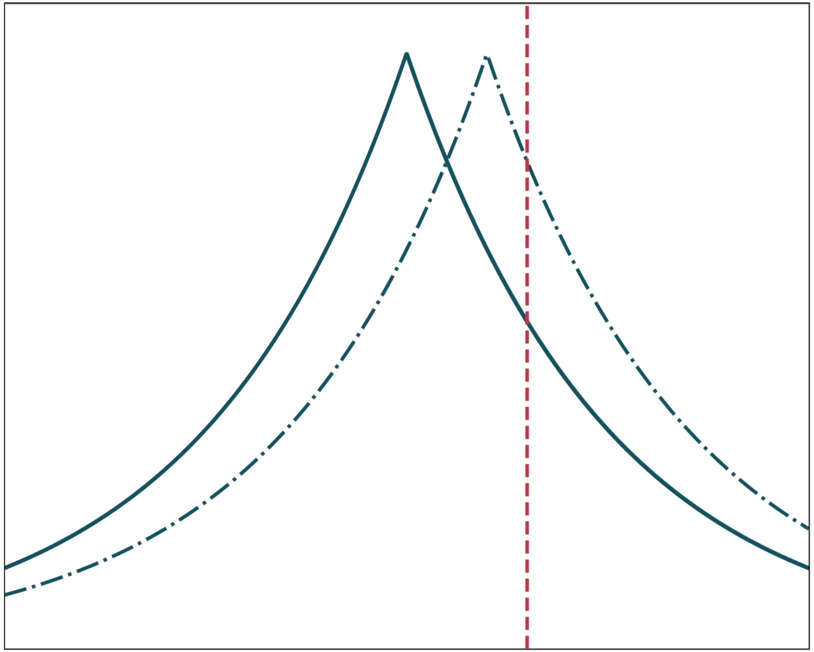
$f(\;)$ is (ϵ, δ) close to $f(\;)$

Census Bureau Adopts Cutting Edge Privacy Protections for 2020 Census

Fri Feb 15 2019

WRITTEN BY: DR. RON JARMIN, DEPUTY DIRECTOR AND COO

Privacy Parameters



Parameter ε bounds the multiplicative difference in probability

Differential Privacy in an imperative programming language?

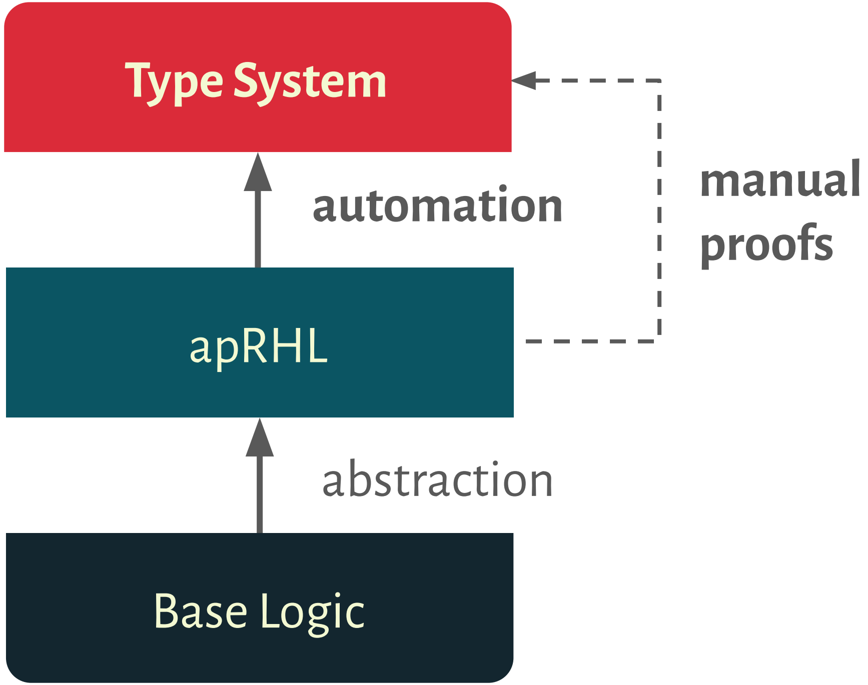
```
c := c1; c2
   | if e then c1 else c2
   | while e do c end
   | x = e
   | x[e1] = e2
   | x $= laplace(e, width)
```

Fuzzi and its Three Levels

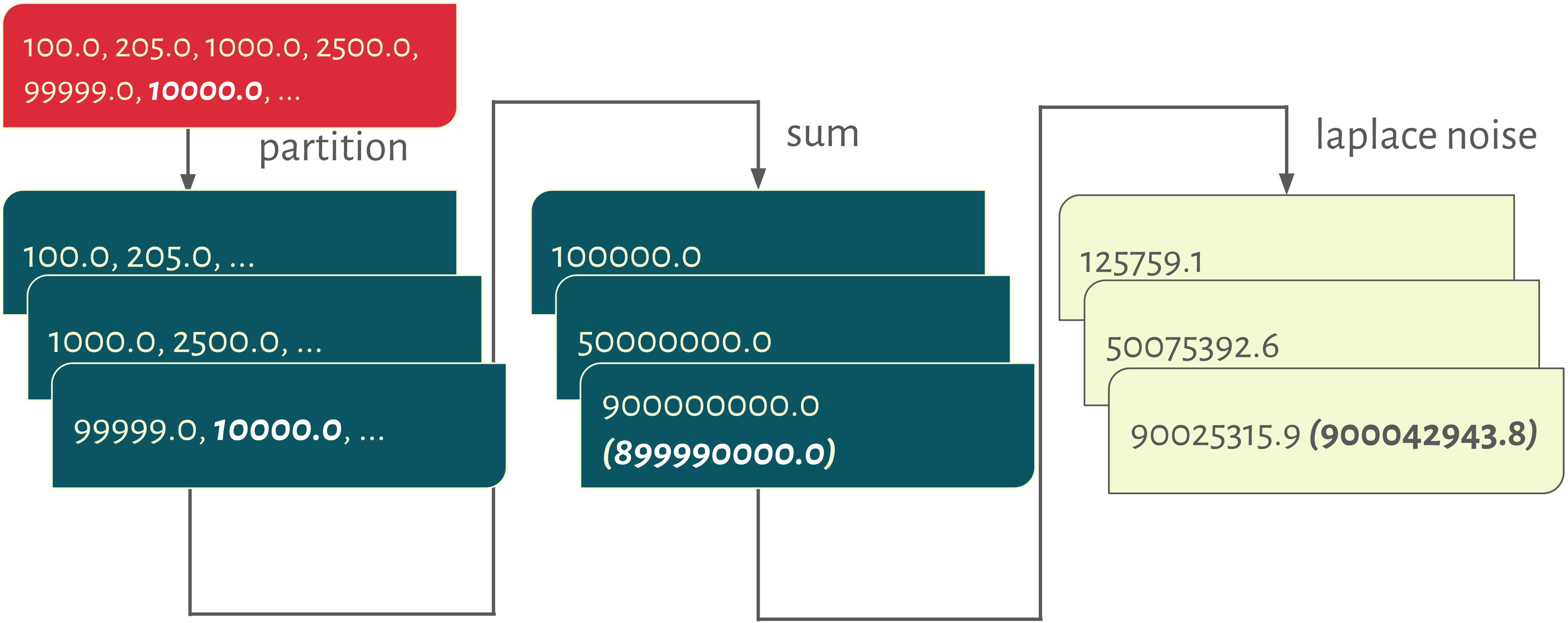
Type System for differentially private, imperative programs

Advanced Probabilistic Couplings for Differential Privacy
Barthe et al. 2016.

Language Semantics

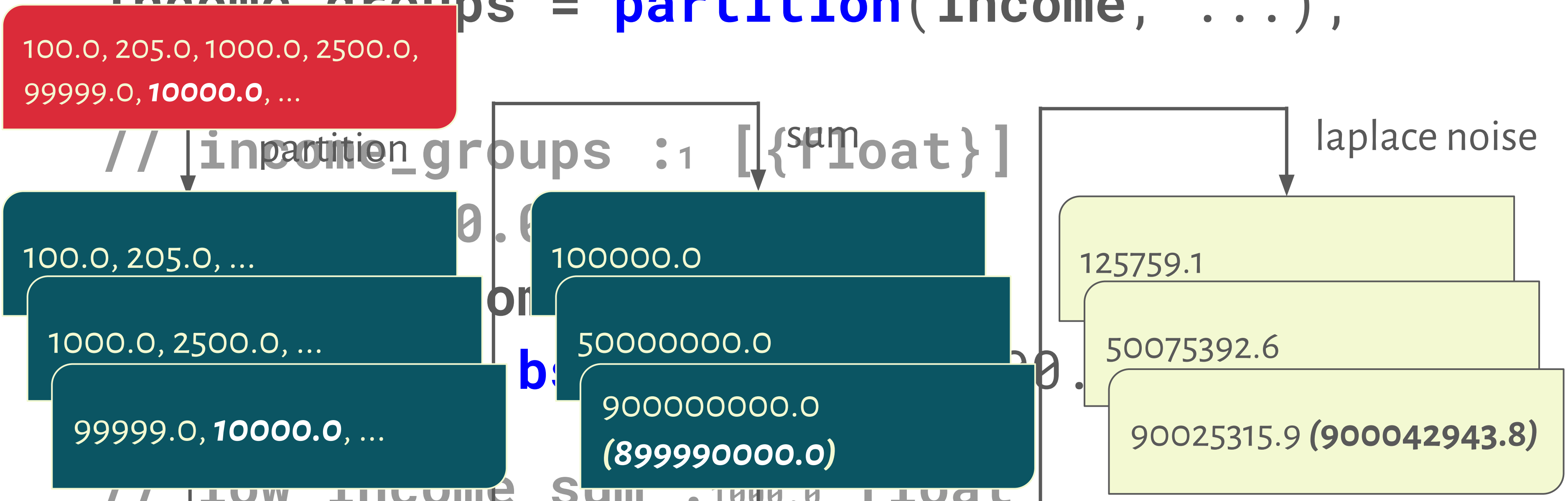


An Example Fuzzi Program



An Example Fuzzi Program

```
// income :1 {float}
// epsilon=0.0, delta=0.0
income_groups = partition(income, ...);
// income_groups :1 [{float}]
...
// low_income_sum :1000.0 float
// epsilon=1.0, delta=0.0
income_sum = laplace(income_sum, 1000.0);
```

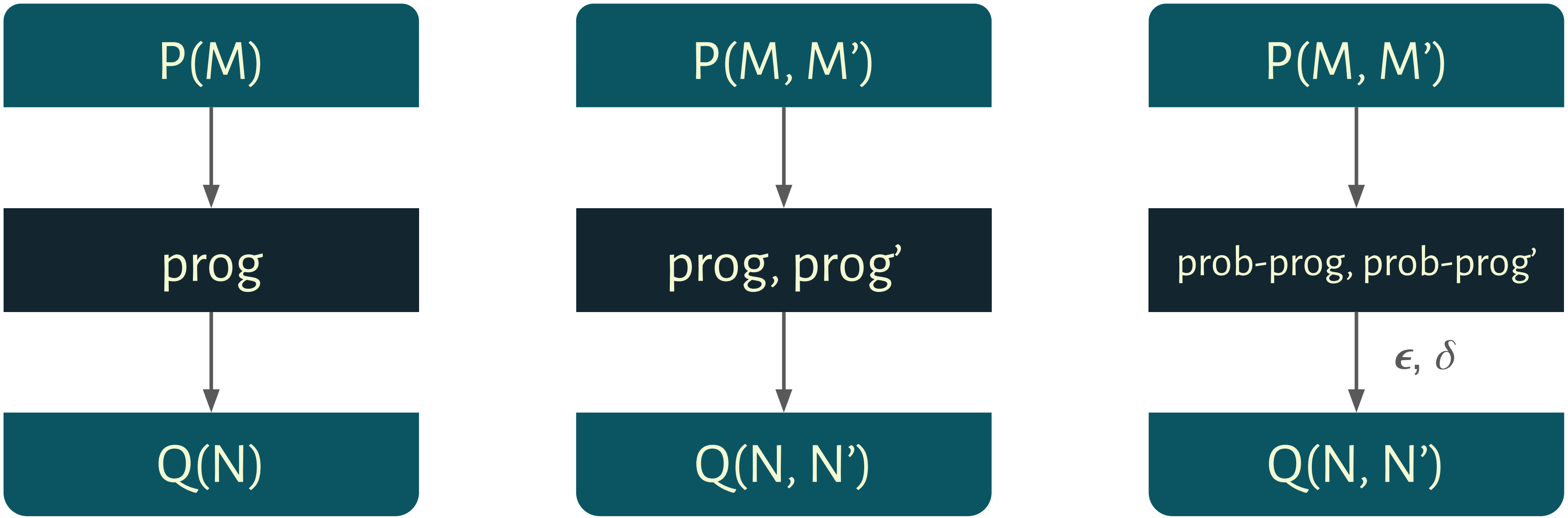


Fuzzi Type System

$$\frac{\{\Gamma_1\}\, c\, \{\Gamma_2, (\epsilon, \delta)\} \qquad \{\Gamma_2\}\, c'\, \{\Gamma_3, (\epsilon', \delta')\}}{\{\Gamma_1\}\, c\, ;\, c'\, \{\Gamma_3, (\epsilon+\epsilon', \delta+\delta')\}}$$

Type System as an Interface to apRHL

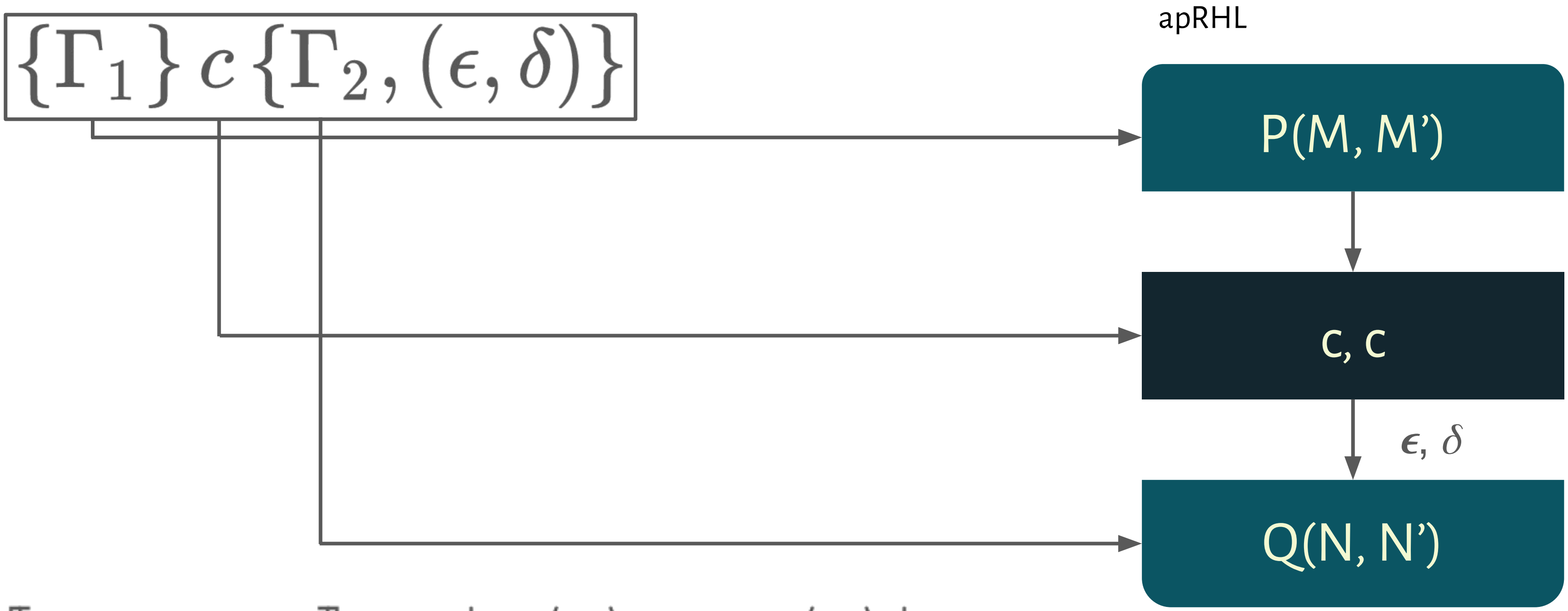
Hoare Logic | Relational | Approximate Relational Hoare Logic



$$P, Q := x\langle 1\rangle = x\langle 2\rangle \wedge y\langle 1\rangle = 5$$

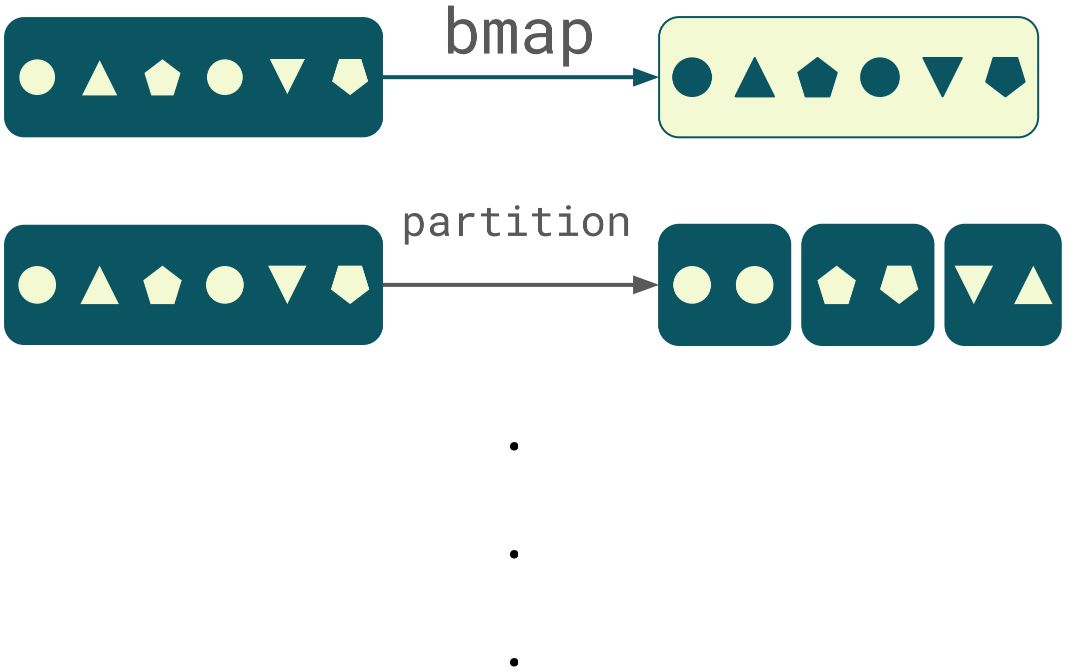
Type System as an Interface to apRHL

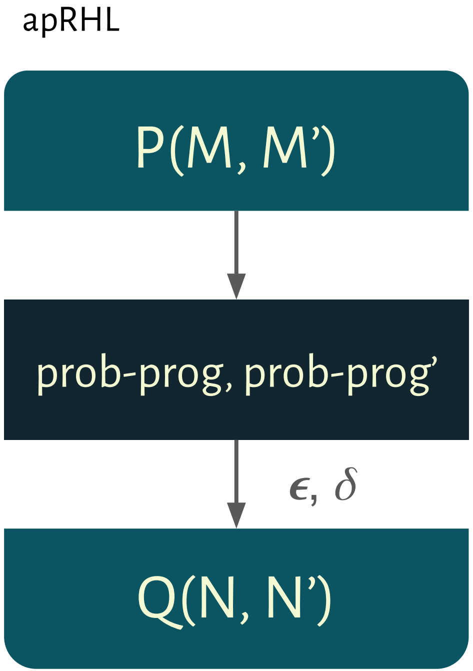
$$\{\Gamma_1\}\, c\, \{\Gamma_2, (\epsilon, \delta)\}$$



$$[\![x :_s \mathtt{int}]\!] = |x\langle 1\rangle - x\langle 2\rangle| \leq s$$

Packaging Manual Proofs for Mechanisms





Evaluation

	Differentially Private	Dataset
Logistic Regression	0.84 (11.02, 10e-6)	MNIST
Ensemble of Logistic Regression	0.82 (20.0, 0.0)	MNIST (partitioned)
Naive Bayes	0.69 (7.70, 0.0)	Spambase
K-Means	0.55 - 0.9, median 0.69 (21.0, 0.0)	Iris

Linear Dependent Types for Differential Privacy.
Gaboardi et al. 2013.

Distance Makes the Types Grow Stronger: A Calculus for Differential Privacy.
Reed and Pierce. 2010.

A Framework for Adaptive Differential Privacy.
Winograd-Cort et al. 2017.

Linear Dependent Types for Differential Privacy.
Gaboardi et al. 2013.

A Framework for Adaptive Differential Privacy.
Winograd-Cort et al. 2017.

Fuzzi: A Three Level Logic for Differential Privacy.
Zhang et al. 2019.

Semantics of Types for Mutable State.
Ahmed. 2004.

A very modal model of a modern, major, general type system.
Appel et al. 2007.

Foundational Proof-Carrying Code.
Appel. 2001.

RustBelt: Securing the Foundations of the Rust Programming Language.
Jung et al. 2017.

Semantics of Types for Mutable State.
Ahmed. 2004.

A very modal model of a modern, major, general type system.
Appel et al. 2007.

RustBelt: Securing the Foundations of the Rust Programming Language.
Jung et al. 2017.

Conclusion

1. We propose a high-level sensitivity type system for tracking differential privacy
   a. We establish soundness through straightforward embedding into apRHL;
   b. The type system is expressive enough for verification conditions of manual differential privacy proofs in apRHL.
2. We show how to push manual proof results of DP back into sensitivity type system
   a. We develop manual proofs of bag-map, bag-sum, partition, advanced composition.
3. We evaluate Fuzzi by implementing 4 textbook machine learning algorithms
   a. We build a prototype of Fuzzi in Haskell
   b. We translate Fuzzi program into Python3 for execution

Fuzzi: A Three Level Logic for Differential Privacy

Hengchu Zhang, Edo Roth, Andreas Haeberlen, Benjamin C. Pierce, Aaron Roth

University of Pennsylvania

A Privacy Type System for Simple While Programs

$$\Gamma := \emptyset \mid \Gamma, x :_s \tau$$

Plus

$$\frac{\Gamma \vdash e_l :_s \texttt{int} \qquad \Gamma \vdash e_r :_t \texttt{int}}{\Gamma \vdash e_l + e_r :_{s+t} \texttt{int}}$$

A Privacy Type System for Simple While Programs

Plus

$$\frac{\Gamma \vdash e_l :_s \mathtt{int} \qquad \Gamma \vdash e_r :_t \mathtt{int}}{\Gamma \vdash e_l + e_r :_{s+t} \mathtt{int}}$$

Laplace

$$\frac{\Gamma \vdash e :_s \mathtt{float}}{\{\Gamma\}\, x = laplace(e, w)\, \{\Gamma[x \mapsto 0], (s/w, 0)\}}$$

Properties of Differential Privacy

1. Compositional
   - ✓ Given **f1** (ϵ_1, δ_1) -DP, and **f2** (ϵ_2, δ_2) -DP
   - ✓ Running **f1** followed by **f2** is $(\epsilon_1 + \epsilon_2, \delta_1 + \delta_2)$ -DP
2. Robust to post-processing
   - ✓ Further analysis on the results of **f** does not weaken its DP guarantees

Differential Privacy is Subtle

Understanding the Sparse Vector Technique for Differential Privacy

Min et al. 2016.

On the Privacy Properties of Variants on the Sparse Vector Technique

Chen and Machanavajjhala. 2015.