

Differentially Private Runtime Monitoring

Bernd Finkbeiner and **Frederik Scheerer** | CAV 2026 | July 27, 2026



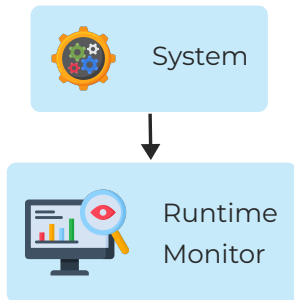
Stream-Based Runtime Monitoring



System

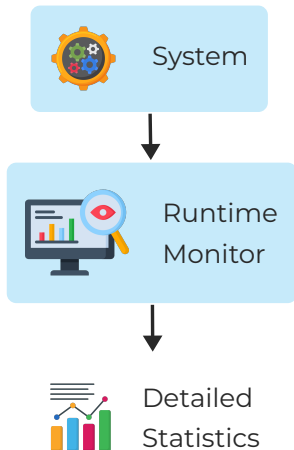


Stream-Based Runtime Monitoring



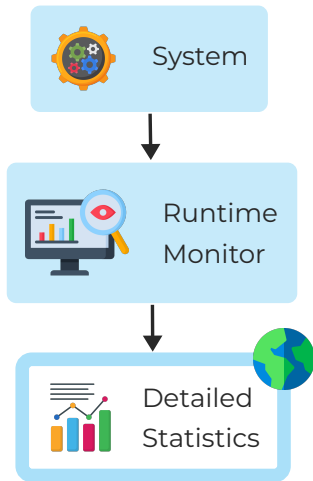


Stream-Based Runtime Monitoring



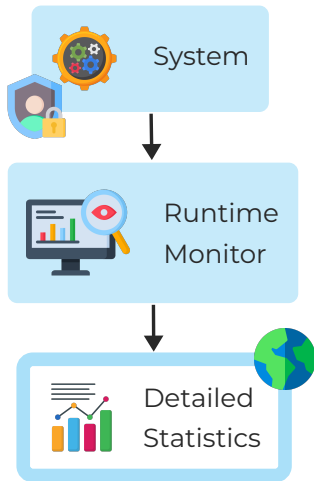


Stream-Based Runtime Monitoring



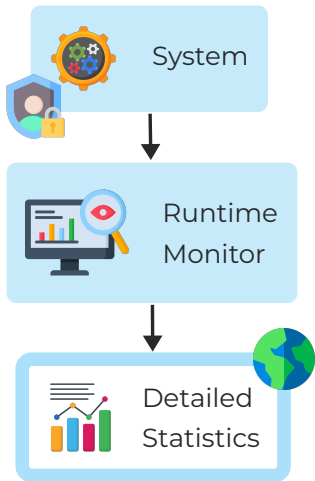


Stream-Based Runtime Monitoring



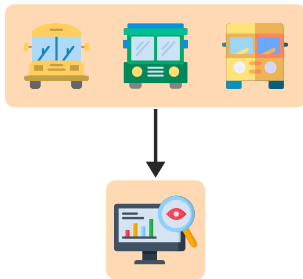
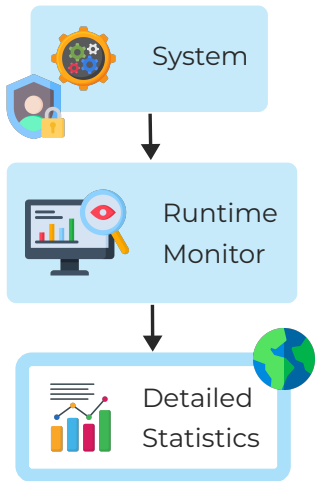


Stream-Based Runtime Monitoring



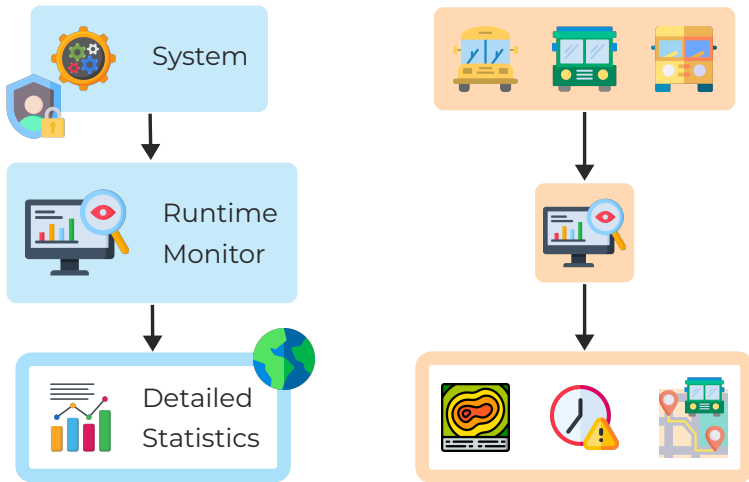


Stream-Based Runtime Monitoring



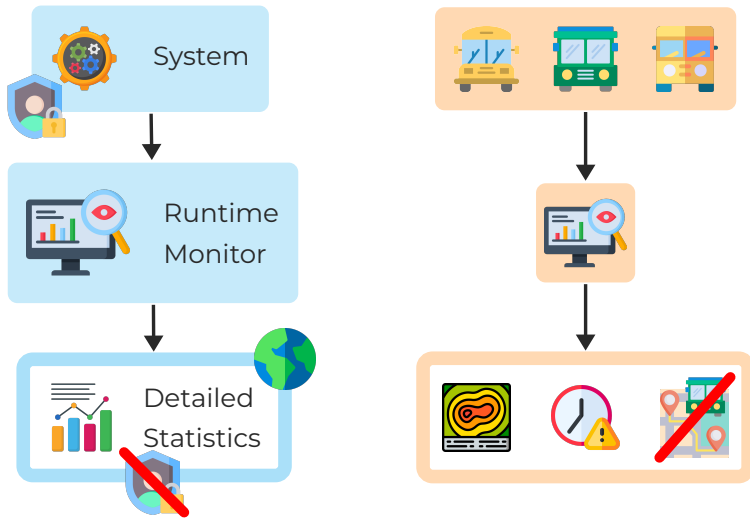


Stream-Based Runtime Monitoring





Stream-Based Runtime Monitoring





Stream-Based Monitoring in Practice



Unmanned Aircraft
Baumeister et. al., CAV 2024



Stream-Based Monitoring in Practice



Unmanned Aircraft

Baumeister et. al., CAV 2024



Algorithmic Fairness

Baumeister et.al., TACAS 2025



Stream-Based Monitoring in Practice



Image Source: DLR, CC BY-NC-ND 3.0



Unmanned Aircraft

Baumeister et. al., CAV 2024



Algorithmic Fairness

Baumeister et.al., TACAS 2025



Car Exhaust Emission

Biewer et al., TACAS 2021



Stream-Based Monitoring in Practice



Unmanned Aircraft

Baumeister et. al., CAV 2024



Algorithmic Fairness

Baumeister et.al., TACAS 2025



Car Exhaust Emission

Biewer et al., TACAS 2021



Differential Privacy¹



¹Dwork et al., Calibrating noise to sensitivity in private data analysis, 2006



Differential Privacy¹



¹Dwork et al., Calibrating noise to sensitivity in private data analysis, 2006



Differential Privacy¹



Databases differ
by a single row

¹Dwork et al., Calibrating noise to sensitivity in private data analysis, 2006



Differential Privacy¹

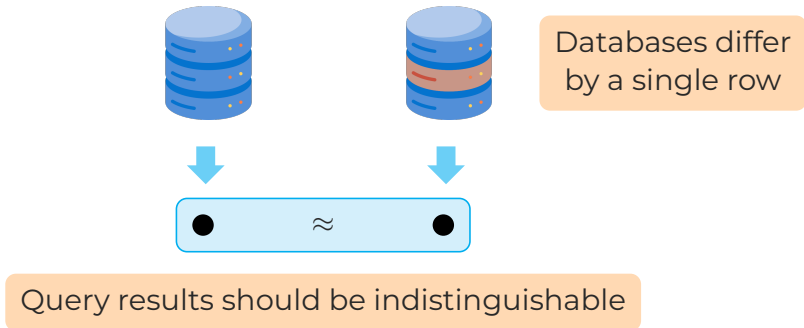


Databases differ
by a single row

¹Dwork et al., Calibrating noise to sensitivity in private data analysis, 2006



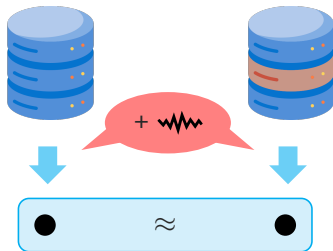
Differential Privacy¹



¹Dwork et al., Calibrating noise to sensitivity in private data analysis, 2006



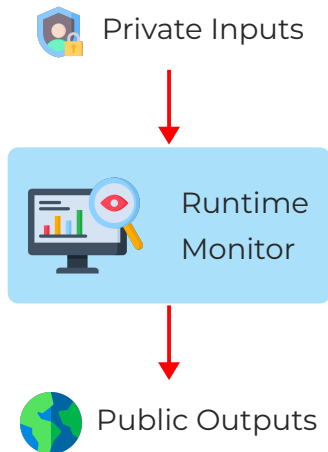
Differential Privacy¹



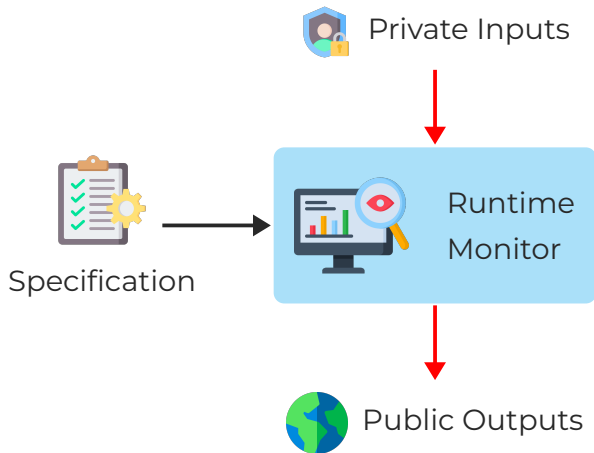
Databases differ
by a single row

Query results should be indistinguishable

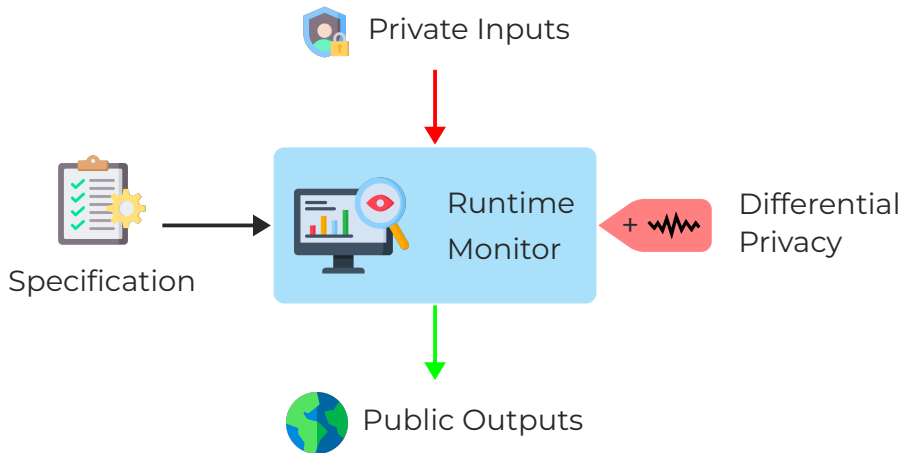
¹Dwork et al., Calibrating noise to sensitivity in private data analysis, 2006



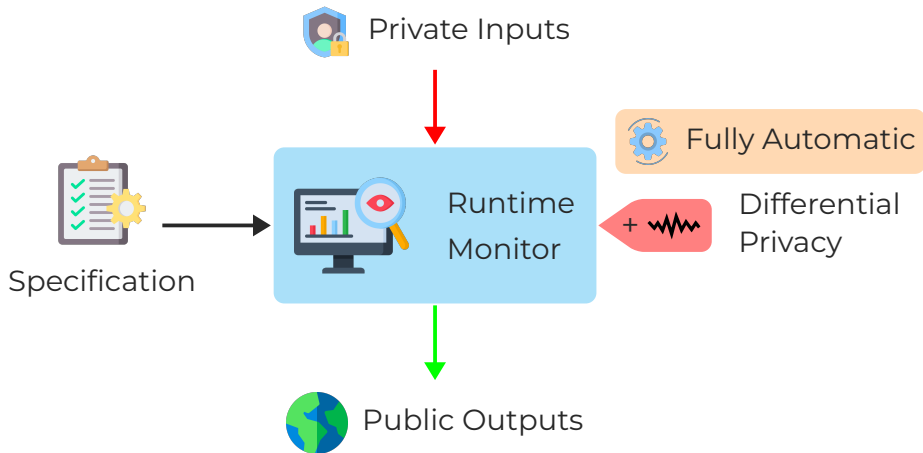
Overview



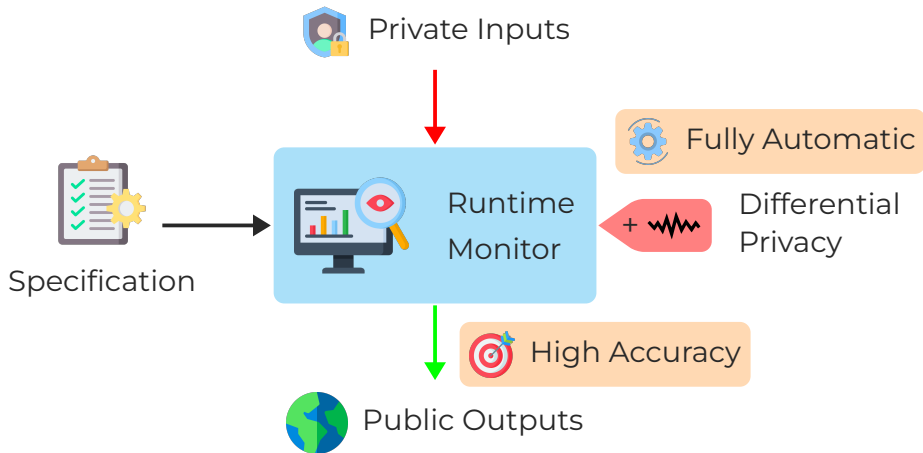
Overview



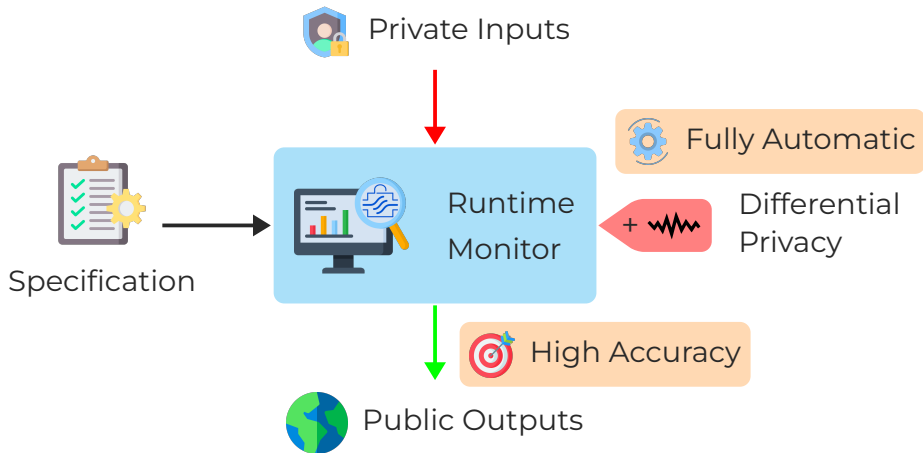
Overview



Overview

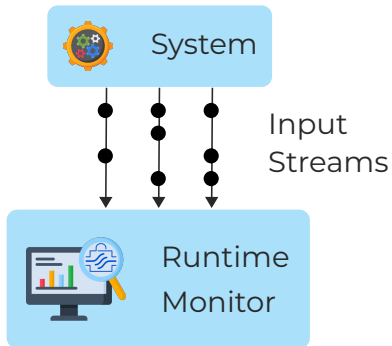


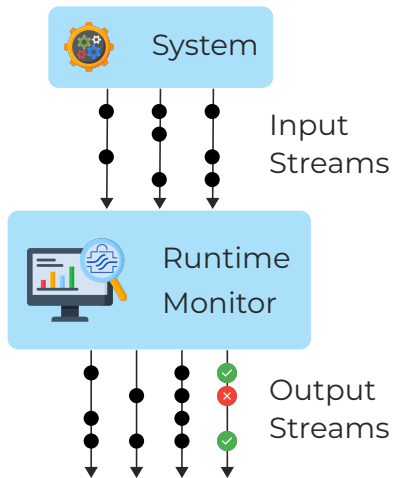
Overview

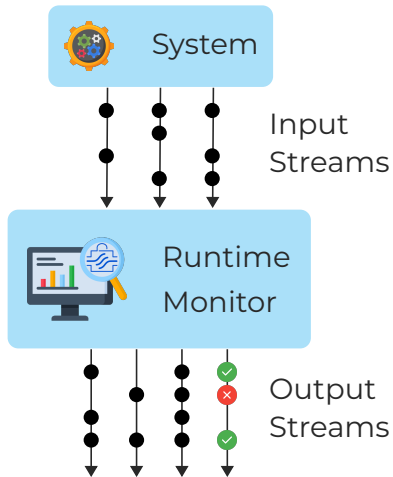




Runtime
Monitor

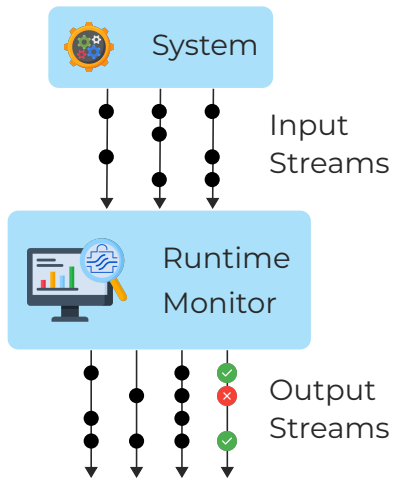




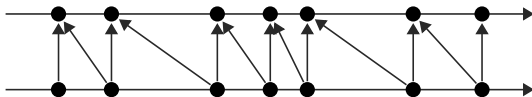


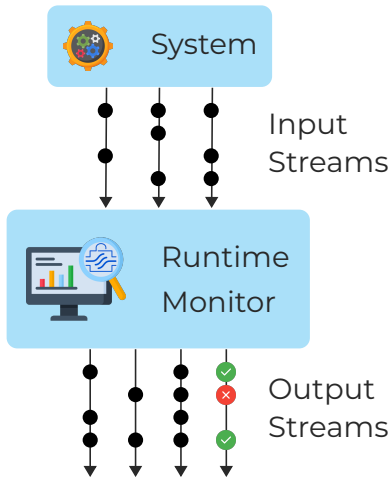
`input a : UInt64`



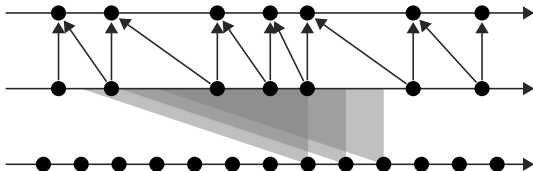


```
input a : UInt64
output b := a + a.offset(by: -1, or: 0)
```





```
input a : UInt64
output b := a + a.offset(by: -1, or: 0)
output c @1s := b.aggregate(over: 6s, using: Σ)
```





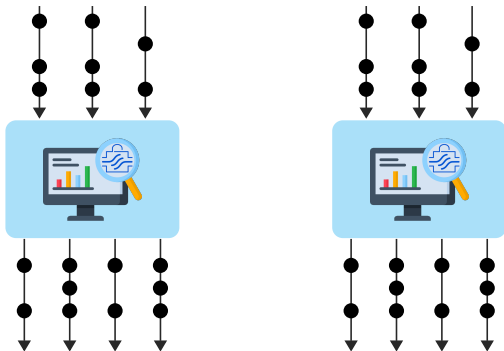
Event-Based Privacy²



²Dwork et al., Differential privacy under continual observation, 2010



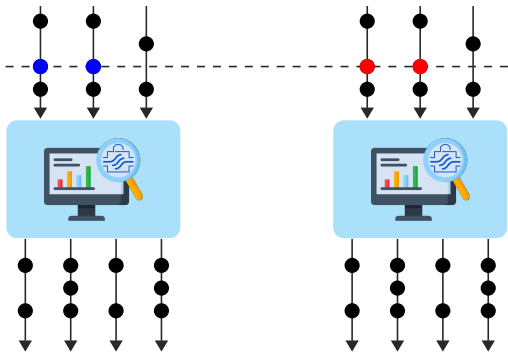
Event-Based Privacy²



²Dwork et al., Differential privacy under continual observation, 2010



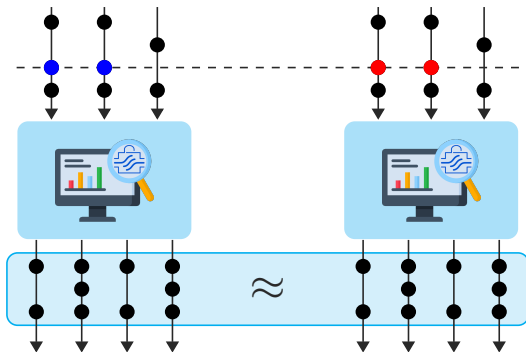
Event-Based Privacy²



²Dwork et al., Differential privacy under continual observation, 2010



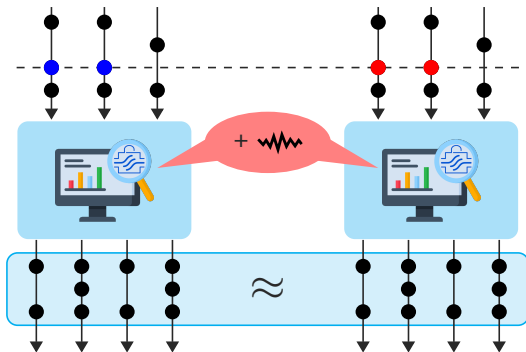
Event-Based Privacy²



²Dwork et al., Differential privacy under continual observation, 2010



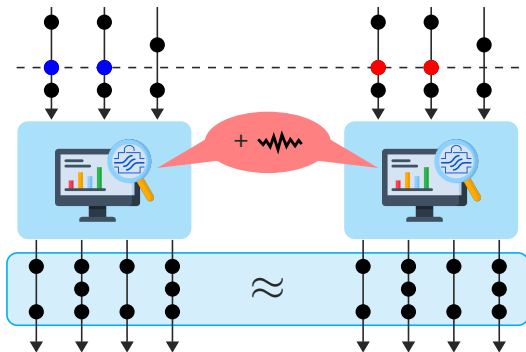
Event-Based Privacy²



²Dwork et al., Differential privacy under continual observation, 2010



Event-Based Privacy²



Noise calibrated to
monitor's
sensitivity:

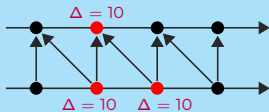
The maximum
change in outputs
caused by a single
changed input event

²Dwork et al., Differential privacy under continual observation, 2010

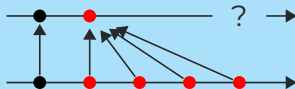


Challenges

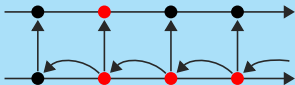
Temporal Operators



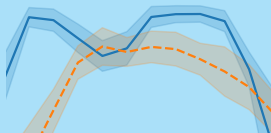
Asynchronous



Dependency Cycles



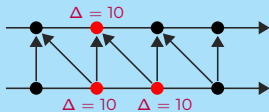
Accuracy





Challenges

Temporal Operators



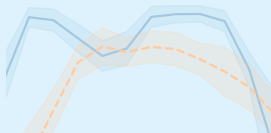
Asynchronous



Dependency Cycles



Accuracy





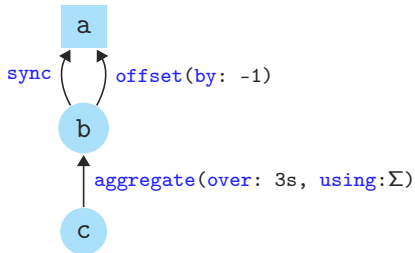
Sensitivity Analysis

```
input a : UInt64
output b := a + a.offset(by: -1, or: 0)
output c @1s := b.aggregate(over: 3s, using:  $\Sigma$ )
```



Sensitivity Analysis

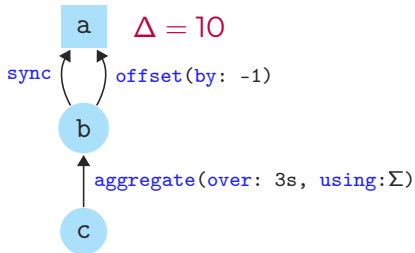
```
input a : UInt64  
output b := a + a.offset(by: -1, or: 0)  
output c @1s := b.aggregate(over: 3s, using:  $\Sigma$ )
```





Sensitivity Analysis

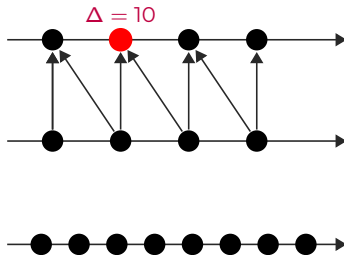
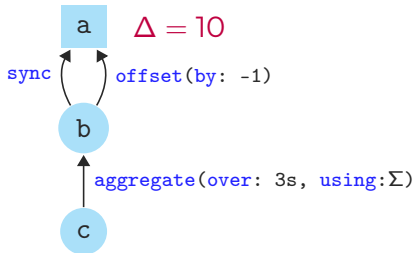
```
#[ $\Delta = 10$ ]  
input a : UInt64  
output b := a + a.offset(by: -1, or: 0)  
output c @1s := b.aggregate(over: 3s, using:  $\Sigma$ )
```





Sensitivity Analysis

```
#[ $\Delta = 10$ ]  
input a : UInt64  
output b := a + a.offset(by: -1, or: 0)  
output c @1s := b.aggregate(over: 3s, using:  $\Sigma$ )
```





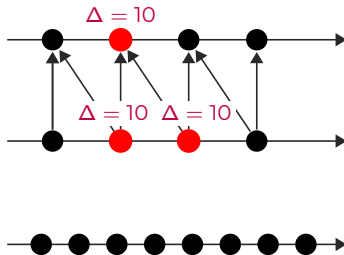
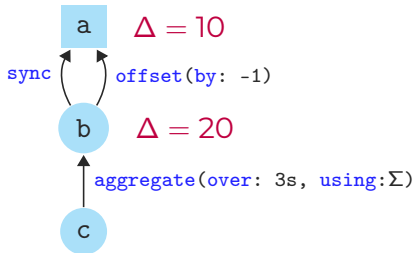
Sensitivity Analysis

$\#[\Delta = 10]$

input a : UInt64

output b := a + a.offset(by: -1, or: 0)

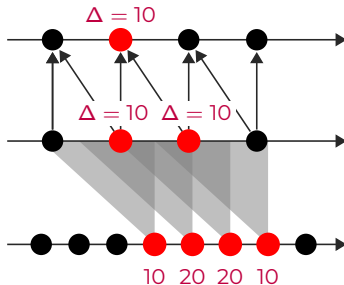
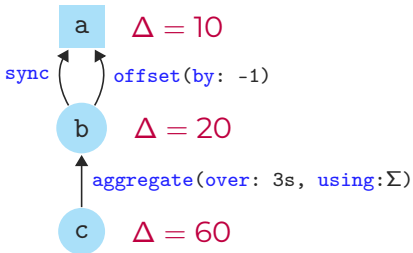
output c @1s := b.aggregate(over: 3s, using: Σ)





Sensitivity Analysis

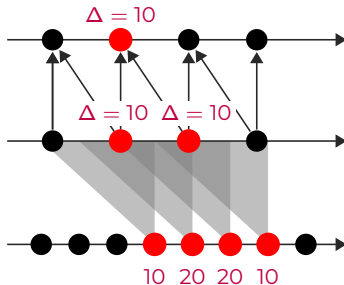
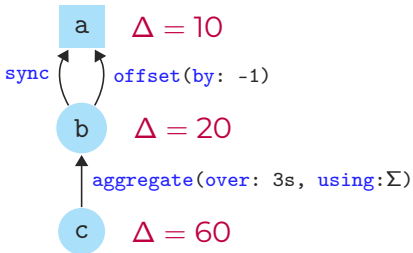
```
#[ $\Delta = 10$ ]  
input a : UInt64  
output b := a + a.offset(by: -1, or: 0)  
output c @1s := b.aggregate(over: 3s, using:  $\Sigma$ )
```





Sensitivity Analysis

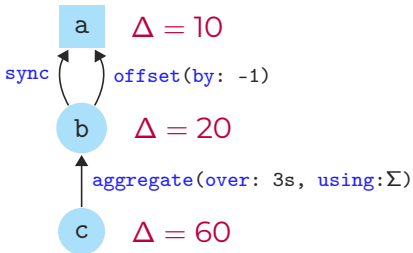
```
#[ $\Delta = 10$ ]  
input a : UInt64  
output b := a + a.offset(by: -1, or: 0)  
output c @1s := b.aggregate(over: 3s, using:  $\Sigma$ )  
+ laplace(60 /  $\epsilon$ )
```



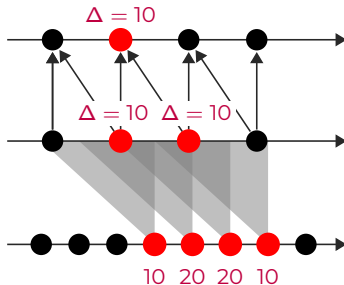


Sensitivity Analysis

```
#[ $\Delta = 10$ ]  
input a : UInt64  
output b := a + a.offset(by: -1, or: 0)  
output c @1s := b.aggregate(over: 3s, using:  $\Sigma$ )  
               + laplace(60 /  $\epsilon$ )
```



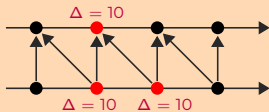
Sensitivity Bound enables
calibration of DP noise
at compile time.





Challenges

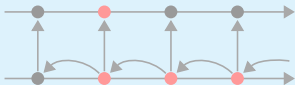
Temporal Operators



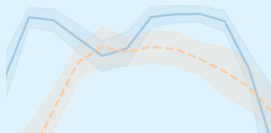
Asynchronous



Dependency Cycles



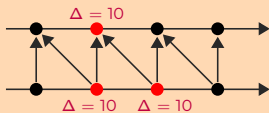
Accuracy



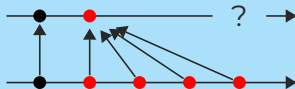


Challenges

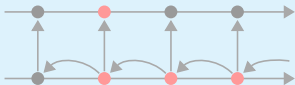
Temporal Operators



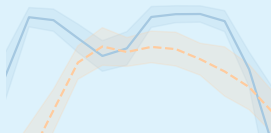
Asynchronous



Dependency Cycles



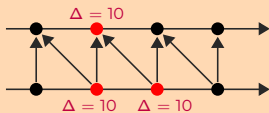
Accuracy



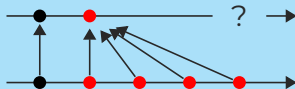


Challenges

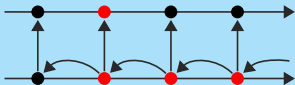
Temporal Operators



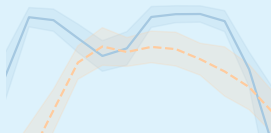
Asynchronous



Dependency Cycles



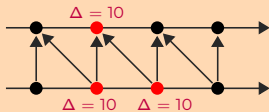
Accuracy



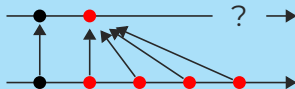


Challenges

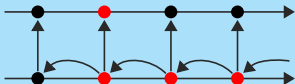
Temporal Operators



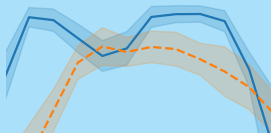
Asynchronous

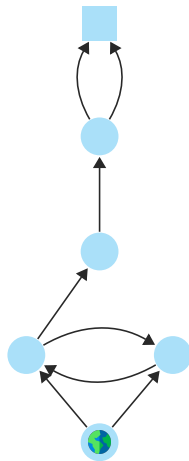


Dependency Cycles



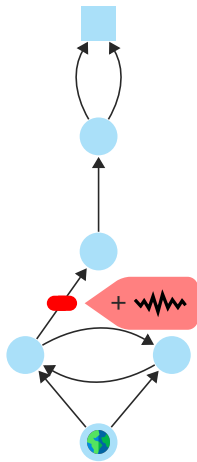
Accuracy







Privacy Barriers





Privacy Barriers



Private Inputs



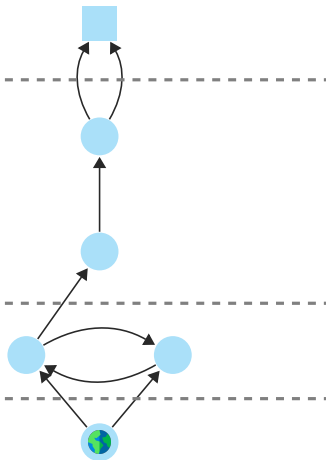
Private
Segment



Post-Processed
Segment



Public Outputs





Privacy Barriers



Private Inputs



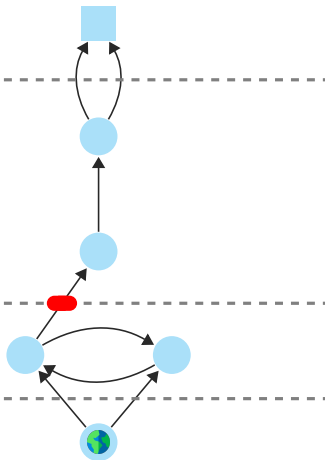
Private
Segment



Post-Processed
Segment



Public Outputs





Privacy Barriers



Private Inputs



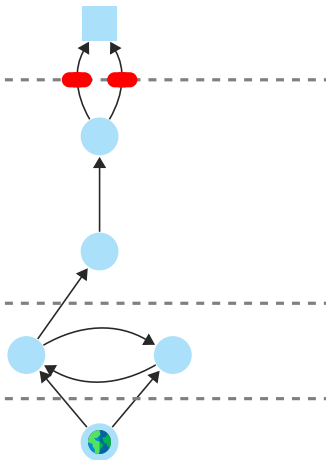
Private
Segment



Post-Processed
Segment



Public Outputs





Privacy Barriers



Private Inputs



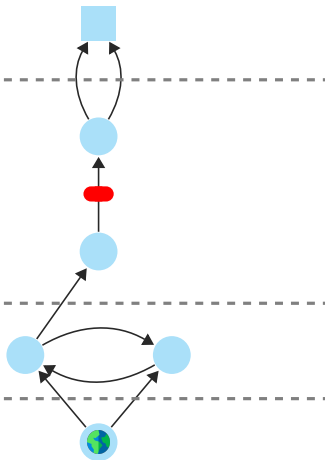
Private
Segment



Post-Processed
Segment



Public Outputs





Tree-Based Aggregation^{3,4}

```
output b @1s := a.aggregate(over: 4s, using:  $\Sigma$ )
```



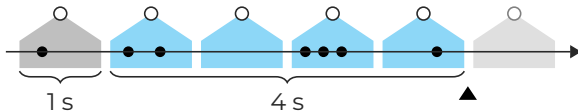
³Dwork et al., Differential privacy under continual observation, 2010

⁴Chan et al., Private and continual release of statistics, 2011



Tree-Based Aggregation^{3,4}

```
output b @1s := a.aggregate(over: 4s, using:  $\Sigma$ )
```



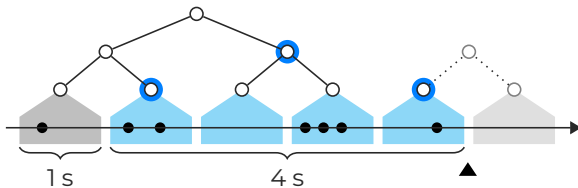
³Dwork et al., Differential privacy under continual observation, 2010

⁴Chan et al., Private and continual release of statistics, 2011



Tree-Based Aggregation^{3,4}

```
output b @1s := a.aggregate(over: 4s, using:  $\Sigma$ )
```

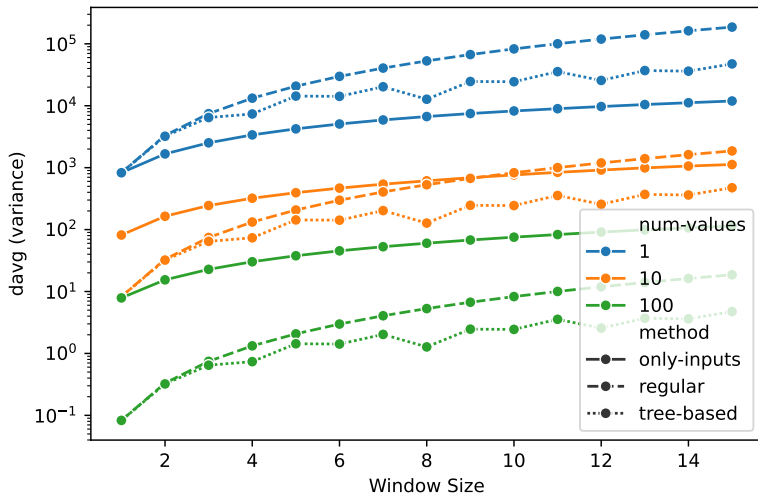


³Dwork et al., Differential privacy under continual observation, 2010

⁴Chan et al., Private and continual release of statistics, 2011

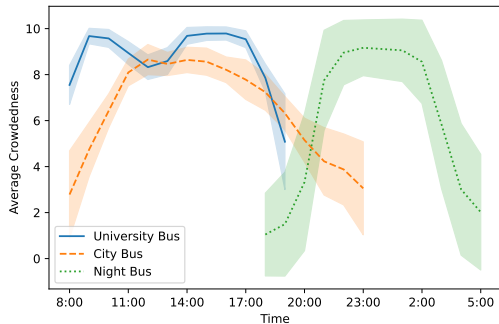
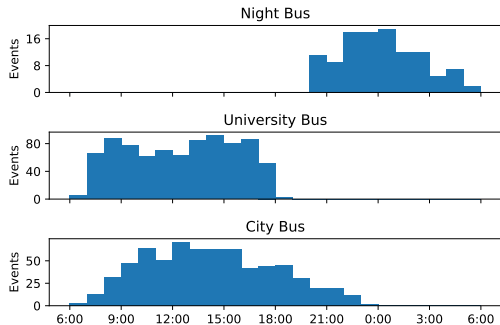


Aggregation Method Comparison

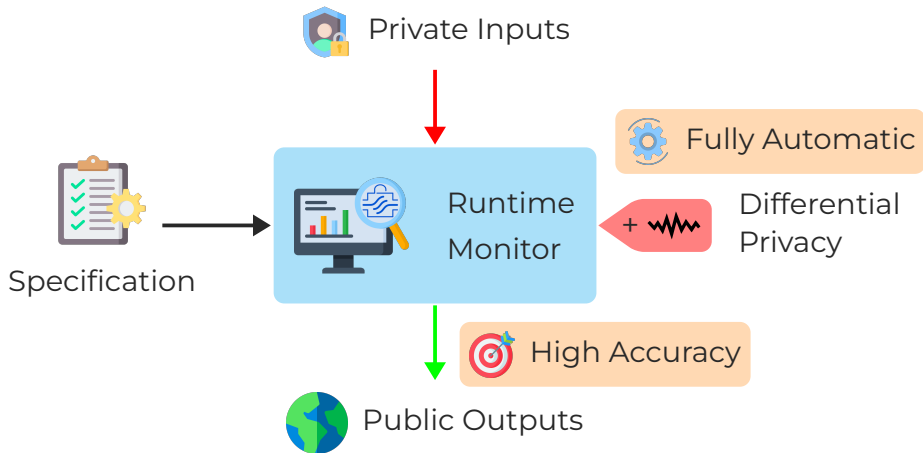




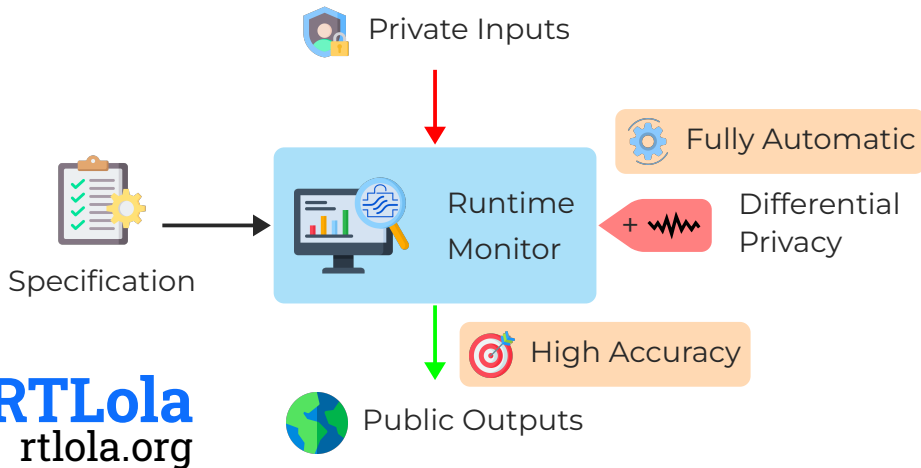
Case Study: Public Transportation



Summary



Summary



The icons used in this presentation are designed by Magnific:
www.magnific.com.