Opaque

An Oblivious and Encrypted Distributed Analytics Platform

Wenting Zheng, Ankur Dave, Jethro G. Beekman, Raluca Ada Popa, Joseph E. Gonzalez, Ion Stoica

UC Berkeley
Complex analytics run on sensitive data
Complex analytics run on sensitive data

- Spark SQL
- MLLib
- GraphX
- Spark Streaming

client

cloud provider

sensitive data
Complex analytics run on sensitive data
Cloud attackers

client

cloud provider

sensitive data
Cloud attackers

- client
- cloud provider
- sensitive data
Cloud attackers

client

cloud provider

sensitive data

Diagram showing a client connecting to a cloud provider, with an indication of sensitive data being transmitted.
Cloud attackers
Cloud attackers
Cloud attackers

client

cloud provider

sensitive data
Cloud attackers

client

cloud provider

sensitive data
Cloud attackers

client

cloud provider

sensitive data
How to protect data while preserving functionality?
Cryptographic approach?
Cryptographic approach?

- Fully homomorphic encryption [Gentry ’09]
Cryptographic approach?

- Fully homomorphic encryption [Gentry ’09]
  - fully functional
Cryptographic approach?

- Fully homomorphic encryption [Gentry ’09]
  - fully functional
  - too slow
Cryptographic approach?

- Fully homomorphic encryption [Gentry '09]
  - fully functional
  - too slow
- CryptDB [PRZB '11]
Cryptographic approach?

- Fully homomorphic encryption [Gentry ’09]
  - **fully functional**
  - **too slow**
- CryptDB [PRZB ’11]
  - more practical performance
Cryptographic approach?

- Fully homomorphic encryption [Gentry ’09]
  - fully functional
  - too slow
- CryptDB [PRZB ’11]
  - more practical performance
  - limited functionality
Cryptographic approach?

- Fully homomorphic encryption [Gentry '09]
  - fully functional
  - too slow
- CryptDB [PRZB '11]
  - more practical performance
  - limited functionality

Alternative: hardware enclaves
Hardware enclaves
(e.g., Intel SGX, AMD memory encryption)
Hardware enclaves
(e.g., Intel SGX, AMD memory encryption)

- Hardware-enforced secure execution environment
Hardware enclaves
(e.g., Intel SGX, AMD memory encryption)

- Hardware-enforced secure execution environment
Hardware enclaves
(e.g., Intel SGX, AMD memory encryption)

- Hardware-enforced secure execution environment
- Encrypted enclave memory (accessible only from the enclave)
Hardware enclaves
(e.g., Intel SGX, AMD memory encryption)

- Hardware-enforced secure execution environment
- Encrypted enclave memory (accessible only from the enclave)
Hardware enclaves
(e.g., Intel SGX, AMD memory encryption)

- Hardware-enforced secure execution environment
- Encrypted enclave memory (accessible only from the enclave)
- Protect against an attacker who has root access
Enclave-based systems
Enclave-based systems

• Prior work: Haven [BMG '14], VC3 [SCFGPMR '15]:
Enclave-based systems

- Prior work: Haven [BMG '14], VC3 [SCFGPMR '15]:
  - full functionality
Enclave-based systems

- Prior work: Haven [BMG ’14], VC3 [SCFGPMR ‘15]:
  - full functionality
  - great performance
Enclave-based systems

- Prior work: Haven [BMG ’14], VC3 [SCFGPMR ’15]:
  - full functionality
  - great performance
  - data access pattern leakage [XCP ’15, OCFGKS ’15]
Problem: access pattern leakage [XCP ’15, OCFGKS ’15]
Problem: access pattern leakage [XCP '15, OCFGKS '15]

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
</tr>
</tbody>
</table>
**Problem: access pattern leakage**

[XCP '15, OCFGKS '15]

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
</tr>
</tbody>
</table>

```
SELECT count(*) FROM medical
GROUP BY disease
```
<table>
<thead>
<tr>
<th></th>
<th>Diabetes</th>
<th>Cancer</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29489</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13744</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18740</td>
<td></td>
<td></td>
</tr>
<tr>
<td>98329</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32591</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Problem: access pattern leakage [XCP ‘15, OCFGKS ‘15]
Problem: access pattern leakage [XCP '15, OCFGKS '15]
Problem: access pattern leakage

[XCP '15, OCFGKS '15]
Problem: access pattern leakage [XCP ‘15, OCFGKS ‘15]

12809 ... Diabetes
129489 ... Diabetes
13744 ... Cancer

18740 ... Diabetes
198329 ... Cancer
32591 ... Diabetes
Problem: access pattern leakage [XCP '15, OCFGKS '15]
Problem: access pattern leakage [XCP '15, OCFGKS '15]
Problem: access pattern leakage  
[XCP ‘15, OCFGKS ‘15]

Public information:
Diabetes twice as common as cancer
Problem: access pattern leakage [XCP ‘15, OCFGKS ‘15]

Public information: Diabetes twice as common as cancer
Problem: access pattern leakage [XCP ‘15, OCFGKS ‘15]

Public information: Diabetes twice as common as cancer
Problem: access pattern leakage [XCP ‘15, OCFGKS ‘15]

Public information: Diabetes twice as common as cancer
Problem: access pattern leakage [XCP '15, OCFGKS '15]
Problem: access pattern leakage [XCP ’15, OCFGKS ’15]
Problem: access pattern leakage [XCP ‘15, OCFGKS ‘15]
Problem: access pattern leakage [XCP ‘15, OCFGKS ‘15]
Problem: access pattern leakage \[XCP \, '15, \, OCFGKS \, '15\]
Problem: access pattern leakage [XCP ‘15, OCFGKS ‘15]

![Diagram showing access pattern leakage with examples of diabetes and cancer data]

- 12809 ... Diabetes
- 29489 ... Diabetes
- 13744 ... Cancer
- 18740 ... Diabetes
- 32591 ... Diabetes
- 98329 ... Cancer
Problem: access pattern leakage \[\text{XCP '15, OCFGKS '15}\]

<table>
<thead>
<tr>
<th></th>
<th>Diabetes</th>
<th>Cancer</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13744</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Diabetes</th>
</tr>
</thead>
<tbody>
<tr>
<td>29489</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Diabetes</th>
</tr>
</thead>
<tbody>
<tr>
<td>32591</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Diabetes</th>
</tr>
</thead>
<tbody>
<tr>
<td>18740</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Cancer</th>
</tr>
</thead>
<tbody>
<tr>
<td>98329</td>
<td></td>
</tr>
</tbody>
</table>

\[\text{Diabetes} \quad \text{Cancer}\]
Problem: access pattern leakage

[XCP ‘15, OCFGKS ‘15]

Learns that the patient has cancer
Problem: access pattern leakage [XCP ’15, OCFGKS ‘15]

Attack viable by observing both memory and network accesses!

Learns that the patient has cancer
Opaque*: secure distributed analytics

* Oblivious Platform for Analytic QUEries
Security guarantees
Security guarantees

- Data encryption and authentication
Security guarantees

- Data encryption and authentication
- Computation integrity: a check enforcing that the computation is executed correctly
Security guarantees

- Data encryption and authentication
- Computation integrity: a check enforcing that the computation is executed correctly
  - see paper for more!
Security guarantees

- Data encryption and authentication
- Computation integrity: a check enforcing that the computation is executed correctly
  - see paper for more!
- **Obliviousness = hiding access patterns**
Security guarantees

- Data encryption and authentication
- Computation integrity: a check enforcing that the computation is executed correctly
  - see paper for more!
- **Obliviousness** = hiding access patterns
  - *Informal statement*
Security guarantees

- Data encryption and authentication
- Computation integrity: a check enforcing that the computation is executed correctly
  - see paper for more!
- **Obliviousness = hiding access patterns**
  - *Informal statement*
    - *The memory and network accesses of the computation is the same for any input of the same size*
Challenge: obliviousness is expensive
Challenge: obliviousness is expensive

Two-part solution:
Challenge: obliviousness is expensive

Two-part solution:
Distributed oblivious SQL operators
Challenge: obliviousness is expensive

Two-part solution:
Distributed oblivious SQL operators
Novel query planning techniques
Two-part solution:

Distributed oblivious SQL operators

Novel query planning techniques
Two-part solution:

- Distributed oblivious SQL operators
- Novel query planning techniques

Oblivious filter
Two-part solution:

Distributed oblivious SQL operators

- Oblivious filter
- Oblivious sort

Novel query planning techniques
Two-part solution:

Distributed oblivious SQL operators

- Oblivious filter
- Oblivious sort
- Oblivious aggregation

Novel query planning techniques
Two-part solution:

Distributed oblivious SQL operators
- Oblivious filter
- Oblivious sort
- Oblivious aggregation
- Oblivious join

Novel query planning techniques
Two-part solution:

Distributed oblivious SQL operators
- Oblivious filter
- Oblivious sort
- Oblivious aggregation
- Oblivious join

Novel query planning techniques
- Rule-based optimization
Two-part solution:

Distributed oblivious SQL operators:
- Oblivious filter
- Oblivious sort
- Oblivious aggregation
- Oblivious join

Novel query planning techniques:
- Rule-based optimization
- Cost model
Two-part solution:

Distributed oblivious SQL operators
- Oblivious filter
- Oblivious sort
- Oblivious aggregation
- Oblivious join

Novel query planning techniques
- Rule-based optimization
- Cost model
- Cost-based optimization
Two-part solution:

Distributed oblivious SQL operators
- Oblivious filter
- Oblivious sort
- Oblivious aggregation
- Oblivious join

Novel query planning techniques
- Rule-based optimization
- Cost model
- Cost-based optimization
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

| 12809 | ... | Diabetes |
| 129489 | ... | Diabetes |
| 13744 | ... | Cancer |
| 18740 | ... | Diabetes |
| 98329 | ... | Cancer |
| 32591 | ... | Diabetes |
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12809</td>
<td>Diabetes</td>
</tr>
<tr>
<td></td>
<td>29489</td>
<td>Diabetes</td>
</tr>
<tr>
<td></td>
<td>13744</td>
<td>Cancer</td>
</tr>
<tr>
<td>2</td>
<td>18740</td>
<td>Diabetes</td>
</tr>
<tr>
<td></td>
<td>98329</td>
<td>Cancer</td>
</tr>
<tr>
<td></td>
<td>32591</td>
<td>Diabetes</td>
</tr>
</tbody>
</table>
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>...</td>
<td>Diabetes</td>
</tr>
<tr>
<td>29489</td>
<td>...</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>...</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>...</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>...</td>
<td>Cancer</td>
</tr>
<tr>
<td>32591</td>
<td>...</td>
<td>Diabetes</td>
</tr>
</tbody>
</table>
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Map

Sort

Oblivious sort
[CLRS, Leighton ‘85]
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Map

Sort

[CLRS, Leighton ‘85]
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Oblivious sort
[CLRS, Leighton ‘85]

Map

Sort

13744 ... Cancer
98329 ... Cancer
12809 ... Diabetes
29489 ... Diabetes
18740 ... Diabetes
32591 ... Diabetes
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Oblivious sort
[CLRS, Leighton ‘85]
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

The "Diabetes" group is split!
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13744</td>
<td>...</td>
<td>Cancer</td>
</tr>
<tr>
<td>98329</td>
<td>...</td>
<td>Cancer</td>
</tr>
<tr>
<td>12809</td>
<td>...</td>
<td>Diabetes</td>
</tr>
<tr>
<td>29489</td>
<td>...</td>
<td>Diabetes</td>
</tr>
<tr>
<td>18740</td>
<td>...</td>
<td>Diabetes</td>
</tr>
<tr>
<td>32591</td>
<td>...</td>
<td>Diabetes</td>
</tr>
</tbody>
</table>
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

How to aggregate obliviously and in parallel?
Oblivious aggregation

```
SELECT count(*) FROM medical GROUP BY disease
```
Oblivious aggregation

```
SELECT count(*) FROM medical GROUP BY disease
```
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Scan

Boundary processing
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Scan Boundary processing
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Scan Boundary processing
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Scan

Boundary processing
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Scan Boundary processing
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Scan Boundary processing
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
SELECT count(*) FROM medical GROUP BY disease

Scan  Boundary processing
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

`SELECT count(*) FROM medical GROUP BY disease`
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease
Oblivious aggregation

\[
\text{SELECT count(*) FROM medical GROUP BY disease}
\]
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Oblivious sort
[CLRS, Leighton ‘85]

Sort

Cancer: 2
Diabetes: 4
DUMMY
DUMMY
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Oblivious sort
[CLRS, Leighton ‘85]

Cancer: 2
Diabetes: 4
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Sort

Oblivious sort
[CLRS, Leighton ‘85]

Final result

Cancer: 2
Diabetes: 4
Oblivious aggregation

SELECT count(*) FROM medical GROUP BY disease

Aggregation has two sorts...

Oblivious sort
[CLRS, Leighton '85]
Oblivious aggregation

```
SELECT count(*) FROM medical GROUP BY disease
```

Aggregation has two sorts…

Can we do better?

Oblivious sort

[CLRS, Leighton ‘85]
Two-part solution:

Distributed oblivious SQL operators

- Oblivious filter
- Oblivious sort
- Oblivious aggregation
- Oblivious join

Novel query planning techniques

- Rule-based optimization
- Cost model
- Cost-based optimization
Two-part solution:

Distributed oblivious SQL operators

- Oblivious filter
- Oblivious sort
- Oblivious aggregation
- Oblivious join

Novel query planning techniques

Rule-based optimization

- Cost model
- Cost-based optimization
Rule-based optimization
SELECT count(*)
FROM medical
WHERE age > 30
GROUP BY disease
Rule-based optimization

```
SELECT count(*)
FROM medical
WHERE age > 30
GROUP BY disease
```
Insight 1
Insight 1

1. Split each logical operator into smaller Opaque operators
Insight 1

1. Split each logical operator into smaller Opaque operators

2. Take a global view across the plan to remove some Opaque operators
Rule-based optimization

Logical op.

Aggregation

Filter

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

Scan

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
</tr>
<tr>
<td>129489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

O-sort

Project

Scan

medical

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
</tr>
<tr>
<td>129489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

↑

Filter

↑

Project

↑

Scan

↑

medical

Filter

O-sort

medical

Amanda D. Edwards 40 Diabetes
Robert R. McGowan 56 Diabetes
Kimberly R. Seay 51 Cancer
Dennis G. Bates 32 Diabetes
Donna R. Bridges 26 Diabetes
Ronald S. Ogden 53 Cancer
## Rule-based optimization

### Logical op.

<table>
<thead>
<tr>
<th>Opaque op.</th>
<th>Logical op.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregation</td>
<td>Filter</td>
</tr>
<tr>
<td></td>
<td>O-sort</td>
</tr>
<tr>
<td></td>
<td>Project</td>
</tr>
<tr>
<td></td>
<td>Scan</td>
</tr>
</tbody>
</table>

### Medical

<table>
<thead>
<tr>
<th>Opaque op.</th>
<th>Logical op.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregation</td>
<td>Filter</td>
</tr>
<tr>
<td></td>
<td>O-sort</td>
</tr>
<tr>
<td></td>
<td>Project</td>
</tr>
<tr>
<td></td>
<td>Scan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

↑

Filter

↑

medical

Filter

O-sort

Project

Scan

↑

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
</tr>
<tr>
<td>12949</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

O-sort

Project

Scan

medical

medical

Filter

O-sorted

Project

Scan

medical

Rule-based optimization

Amanda D. Edwards 40 Diabetes
Robert R. McGowan 56 Diabetes
Kimberly R. Seay 51 Cancer
Dennis G. Bates 32 Diabetes
Donna R. Bridges 26 Diabetes
Ronald S. Ogden 53 Cancer
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

O-sort

Project

Scan

medical

medical

<table>
<thead>
<tr>
<th>Rule-based optimization</th>
<th>Filter</th>
<th>O-sort</th>
<th>Project</th>
<th>Scan</th>
<th>medical</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>129489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

Filter

O-sort

Project

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Diagnosis</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>129489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>
## Rule-based optimization

### Logical op.

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Age</th>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>129489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>

### Opaque op.
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

Project

Scan

Filter

O-sort

medical

medical

12809 Amanda D. Edwards 40 Diabetes 0
129489 Robert R. McGowan 56 Diabetes 0
13744 Kimberly R. Seay 51 Cancer 0
18740 Dennis G. Bates 32 Diabetes 0
32591 Donna R. Bridges 26 Diabetes 1
98329 Ronald S. Ogden 53 Cancer 0

0 0 0 0 1 0
Rule-based optimization

Opaque op.

Logical op.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

O-sort

Project

Scan

medical

Filter

medical

Amanda D. Edwards 40 Diabetes 0
Robert R. McGowan 56 Diabetes 0
Kimberly R. Seay 51 Cancer 0
Dennis G. Bates 32 Diabetes 0
Ronald S. Ogden 53 Cancer 0
Donna R. Bridges 26 Diabetes 1
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Project

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Age Group</th>
<th>Disease</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

O-sort

Project

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Diagnosis</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

O-sort

Project

Scan

medical

Rule-based optimization

12809 Amanda D. Edwards 40 Diabetes 0
129489 Robert R. McGowan 56 Diabetes 0
13744 Kimberly R. Seay 51 Cancer 0
18740 Dennis G. Bates 32 Diabetes 0
98329 Ronald S. Ogden 53 Cancer 0
32591 Donna R. Bridges 26 Diabetes 1
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

Filter

O-sort

Project

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>129489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

Filter

O-sort

Project

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

O-sort

Agg.

O-sort

Filter

O-sort

Project

Scan

medical

98329 Ronald S. Ogden 53 Cancer 0
18740 Dennis G. Bates 32 Diabetes 0
13744 Kimberly R. Seay 51 Cancer 0
29489 Robert R. McGowan 56 Diabetes 0
12809 Amanda D. Edwards 40 Diabetes 0

Rule-based optimization

Opaque op.

Logical op.

Aggregation

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Diagnosis</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Agg.

O-sort

Filter

Project

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>
Rule-based optimization

Can we remove any sort?
Rule-based optimization

Opaque op.

Logical op.

- O-sort
- Agg.
- Filter
- Project
- Scan

medical

medical

Aggregation

Filter

Rule-based optimization

Opaque op.

Logical op.

- Aggregation
- Filter
- medical

- O-sort
- Agg.
- O-sort
- Filter
- O-sort
- Project
- Scan
- medical

medical
Rule-based optimization

Opaque op.

Logical op.

1. O-sorted
2. Aggregation
3. Filter
4. Project
5. Scan

medical

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

Scan

Project

O-sort

O-sort

Agg.

Sort on 0/1 column

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

↑

Filter

↑

medical

O-sort

Agg.

O-sort

Filter

O-sort

Project

Scan

↑

medical

Sort on 0/1 column
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Agg.

Sort on Disease

O-sort

Filter

Sort on 0/1 column

O-sort

Project

Scan

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

Sort on Disease

Sort on 0/1 column

Scan

Project

O-sort

Agg.
Rule-based optimization

Opaque op.

Logical op.

```
Aggregation

↑

Filter

↑

medical

O-sort

↑

Agg.

↑

O-sort

↑

Filter

↑

O-sort

↑

Project

↑

Scan

↑

medical

Sort on Disease

+ 

Sort on 0/1 column

= 
```
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Agg.

O-sort

Filter

O-sort

Project

Scan

medical

Sort on Disease

+

Sort on 0/1 column

= 

Sort on (0/1, Disease)
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Agg.

Filter

O-sort

Project

Scan

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

↑

Filter

↑

medical

O-sort

Agg.

Filter

O-sort

Project

Scan

↑

medical
Rule-based optimization

Opaque op.

Logical op.

- Aggregation
  - Filter
    - medical

- O-sorted
  - Agg.
    - Filter
      - Project
        - Scan
          - medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

medical
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

medical

Scan

Project

O-sort

Filter

Agg.

O-sort
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

medical

12809  Amanda D. Edwards  40  Diabetes
129489 Robert R. McGowan  56  Diabetes
13744  Kimberly R. Seay  51  Cancer
18740  Dennis G. Bates  32  Diabetes
32591  Donna R. Bridges  26  Diabetes
98329  Ronald S. Ogden  53  Cancer
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

- Aggregation
- Filter
- Project
- Scan

- O-sort
- Agg.
- Filter

Table:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

Project

Scan

medical

O-sort

Agg.

Filter

O-sort

Opaque op.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
<th>Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>129489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Condition</th>
<th>Metastasis</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

↑

Filter

↑

medical

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

Filter

O-sort

Agg.

12809 Amanda D. Edwards 40 Diabetes 0
129489 Robert R. McGowan 56 Diabetes 0
13744 Kimberly R. Seay 51 Cancer 0
18740 Dennis G. Bates 32 Diabetes 0
32591 Donna R. Bridges 26 Diabetes 1
98329 Ronald S. Ogden 53 Cancer 0
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

medical

multi-column sort

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Diagnosis</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
</tbody>
</table>
Rule-based optimization

Logical op.

Opaque op.

multi-column sort

Filter

O-sort

Agg.

Project

Scan

medical

medical

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

Amanda D. Edwards 40 Diabetes 0
Robert R. McGowan 56 Diabetes 0
Kimberly R. Seay 51 Cancer 0
Dennis G. Bates 32 Diabetes 0
Donna R. Bridges 26 Diabetes 1
Ronald S. Ogden 53 Cancer 0
Rule-based optimization

- Logical op.
  - Aggregation
  - Filter
    - medical
  - O-sort
  - Agg.
  - Filter
    - O-sort
    - Project
      - Scan
        - medical
  - multi-column sort

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Condition</th>
<th>Discharge</th>
</tr>
</thead>
<tbody>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
</tbody>
</table>
Rule-based optimization

Opaque op.

Logical op.

Aggregation

Filter

medical

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

multi-column sort

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Diagnosis</th>
<th>Incidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
</tbody>
</table>
Rule-based optimization

Logical op.

Opaque op.

Filter

O-sort

Agg.

Aggregation

Filter

O-sort

Project

Scan

medical

medical

multi-column sort

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Diagnosis</th>
<th>Has Diabetes</th>
</tr>
</thead>
<tbody>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>32591</td>
<td>Donna R. Bridges</td>
<td>26</td>
<td>Diabetes</td>
<td>1</td>
</tr>
</tbody>
</table>
Rule-based optimization

Logical op.

Opaque op.

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

medical

multi-column sort

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
</tbody>
</table>
Rule-based optimization

Logical op.

Opaque op.

O-sort

Agg.

Filter

O-sort

Project

Scan

medical

medical

Filter

Aggregation

multi-column sort

13744 Kimberly R. Seay 51 Cancer 0
98329 Ronald S. Ogden 53 Cancer 0
12809 Amanda D. Edwards 40 Diabetes 0
18740 Dennis G. Bates 32 Diabetes 0
29489 Robert R. McGowan 56 Diabetes 0
Rule-based optimization

Logical op.

Opaque op.

Filter

O-sort

Agg.

Project

Scan

medical

Eliminated one oblivious sort!

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Age</th>
<th>Disease</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>13744</td>
<td>Kimberly R. Seay</td>
<td>51</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>98329</td>
<td>Ronald S. Ogden</td>
<td>53</td>
<td>Cancer</td>
<td>0</td>
</tr>
<tr>
<td>12809</td>
<td>Amanda D. Edwards</td>
<td>40</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>18740</td>
<td>Dennis G. Bates</td>
<td>32</td>
<td>Diabetes</td>
<td>0</td>
</tr>
<tr>
<td>29489</td>
<td>Robert R. McGowan</td>
<td>56</td>
<td>Diabetes</td>
<td>0</td>
</tr>
</tbody>
</table>
Two-part solution:

Distributed oblivious SQL operators

- Oblivious filter
- Oblivious sort
- Oblivious aggregation
- Oblivious join

Novel query planning techniques

- Rule-based optimization
- Cost model
- **Cost-based optimization**
Observation: not all tables are sensitive
Observation: not all tables are sensitive

**Hospitalized patients**
- P_ID
- D_ID
- Name
- Age

**Disease**
- D_ID
- Name
- G_ID

**Medication**
- M_ID
- D_ID
- Name
- Cost
Observation: not all tables are sensitive
Observation: not all tables are sensitive

Opaque can operate in *mixed sensitivity*: sensitive tables are run with oblivious operators
Observation: not all tables are sensitive
Observation: not all tables are sensitive
Observation: not all tables are sensitive

Not oblivious!
Observation: not all tables are sensitive
Observation: not all tables are sensitive

Sensitivity propagation: propagate obliviousness from leaf to root
Observation: not all tables are sensitive

Sensitivity propagation: propagate obliviousness from leaf to root
Observation: not all tables are sensitive

Sensitivity propagation: propagate obliviousness from leaf to root
Insight 2

Sensitivity propagation introduces a new dimension to query optimization
Cost-based optimization

Find the least costly medication for each patient
Find the least costly medication for each patient

Assumption: $|P| < |D| < |M|$
Cost-based optimization

Find the least costly medication for each patient

Assumption: |P| < |D| < |M|

```sql
SELECT p_name, d_name, med_cost
FROM patient, disease,
    (SELECT d_id, min(cost) AS med_cost
     FROM medication
     GROUP BY d_id) AS med
WHERE disease.d_id = patient.d_id
    AND disease.d_id = med.d_id
```
Cost-based optimization

Hospitalized patients

P_ID
D_ID
Name
Age

Disease

D_ID
Name
G_ID

Medication

M_ID
D_ID
Name
Cost

Find the least costly medication for each patient

Assumption: |P| < |D| < |M|

SELECT p_name, d_name, med_cost
FROM patient, disease,
    (SELECT d_id, min(cost) AS med_cost
     FROM medication
     GROUP BY d_id) AS med
WHERE disease.d_id = patient.d_id
AND disease.d_id = med.d_id
Cost-based optimization

Find the least costly medication for each patient

Assumption: |P| < |D| < |M|

```
SELECT p_name, d_name, med_cost
FROM patient, disease,
     (SELECT d_id, min(cost) AS med_cost
      FROM medication
      GROUP BY d_id) AS med
WHERE disease.d_id = patient.d_id
  AND disease.d_id = med.d_id
```
Cost-based optimization

SQL optimizer with new cost:
Cost-based optimization

SQL optimizer with new cost:

More selective non-oblivious join
Cost-based optimization

SQL optimizer with new cost:

More selective non-oblivious join
Cost-based optimization

SQL optimizer with new cost and sensitivity propagation:
Cost-based optimization

SQL optimizer with new cost and sensitivity propagation:

Fewer oblivious joins
Cost-based optimization

SQL optimizer with new cost and *sensitivity propagation*:

Fewer oblivious joins
Evaluation setup
Evaluation setup

- Single machine experiments:
  - Intel Xeon E3-1280 v5, 4 cores, 64 GB RAM
  - Intel SGX: 128 MB of enclave page cache (EPC)
Evaluation setup

• Single machine experiments:
  • Intel Xeon E3-1280 v5, 4 cores, 64 GB RAM
  • Intel SGX: 128 MB of enclave page cache (EPC)

• Distributed experiments
  • A cluster of 5 SGX machines
Evaluation
Evaluation

• How does Opaque compare to Spark SQL?
Evaluation

• How does Opaque compare to Spark SQL?
  • Big Data Benchmark (BDB); 4 queries total
Evaluation

• How does Opaque compare to Spark SQL?
  • Big Data Benchmark (BDB); 4 queries total
    • Queries 1, 2, 3: filter, aggregation, join
Evaluation

• How does Opaque compare to Spark SQL?
  • Big Data Benchmark (BDB); 4 queries total
    • Queries 1, 2, 3: filter, aggregation, join
    • 1 million records
Evaluation

• How does Opaque compare to Spark SQL?
  • Big Data Benchmark (BDB); 4 queries total
    • Queries 1, 2, 3: filter, aggregation, join
    • 1 million records

• How does Opaque compare to state-of-the-art oblivious systems?
Evaluation

• How does Opaque compare to Spark SQL?
  • Big Data Benchmark (BDB); 4 queries total
    • Queries 1, 2, 3: filter, aggregation, join
    • 1 million records

• How does Opaque compare to state-of-the-art oblivious systems?
  • GraphSC (oblivious graph analytics)
Evaluation

• How does Opaque compare to Spark SQL?
  • Big Data Benchmark (BDB); 4 queries total
    • Queries 1, 2, 3: filter, aggregation, join
    • 1 million records

• How does Opaque compare to state-of-the-art oblivious systems?
  • GraphSC (oblivious graph analytics)
    • PageRank
Big Data Benchmark (distributed)
Big Data Benchmark (distributed)

Data encryption, authentication, computation verification
Big Data Benchmark (distributed)

Data encryption, authentication, computation verification

<table>
<thead>
<tr>
<th>Runtime (s)</th>
<th>Spark SQL</th>
<th>Opaque</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.01</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Query number

Query 1  Query 2  Query 3
Big Data Benchmark (distributed)

Data encryption, authentication, computation verification

```
<table>
<thead>
<tr>
<th>Query number</th>
<th>Spark SQL</th>
<th>Opaque</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query 1</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>Query 2</td>
<td>1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>Query 3</td>
<td>10.0</td>
<td>10.0</td>
</tr>
</tbody>
</table>
```
Big Data Benchmark (distributed)

Data encryption, authentication, computation verification

Runtime (s)

- Spark SQL
- Opaque

Query number

Query 1 | Query 2 | Query 3
Big Data Benchmark (distributed)

Data encryption, authentication, computation verification

Overhead: 0.47x to 2.3x
Big Data Benchmark
(distributed)

Data encryption, authentication, computation verification
+ Obliviousness

Overhead: 0.47x to 2.3x
Big Data Benchmark (distributed)

Data encryption, authentication, computation verification

Overhead: 0.47x to 2.3x
Big Data Benchmark (distributed)

Data encryption, authentication, computation verification

+ Obliviousness

Overhead: 0.47x to 2.3x
## Big Data Benchmark (distributed)

<table>
<thead>
<tr>
<th>Query number</th>
<th>Spark SQL</th>
<th>Opaque</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query 1</td>
<td>0.01</td>
<td>0.01</td>
</tr>
<tr>
<td>Query 2</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>Query 3</td>
<td>1.0</td>
<td>1.0</td>
</tr>
</tbody>
</table>

**Data encryption, authentication, computation verification**

+ Obliviousness

**Overhead:** 0.47x to 2.3x
Big Data Benchmark (distributed)

Data encryption, authentication, computation verification

+ Obliviousness

Overhead: 0.47x to 2.3x

Overhead: 21x to 45x
PageRank: comparison with GraphSC (single machine)
Conclusion

Opaque is an oblivious and encrypted distributed analytics platform

Open source: github.com/ucbrise/opaque