IntegriDB: Verifiable SQL for Outsourced Databases
Yupeng Zhang, Jonathan Katz and Charalampos Papamanthou

Verifiable Database

Supported Queries
1. Multi-range.
2. Join: reduce to intersections.
3. Sum: modified accumulator. $\prod (x+s) acc(A) = g^{sx+A}$
5. Max/Min: reduce to range with unique answer.
6. Nested queries.
7. Updates.

Our System

Experimental Results

TPC benchmark:
TPC-H database: largest table with 6 million rows and 16 columns (2.8GB).
TPC-H query #19: 7-dimensional range on two tables + join + sum.

<table>
<thead>
<tr>
<th>Setup time</th>
<th>Prover time</th>
<th>Verification time</th>
<th>Proof size</th>
<th>Update time</th>
<th>Digest size</th>
</tr>
</thead>
<tbody>
<tr>
<td>25272.76s</td>
<td>6422.13s</td>
<td>232ms</td>
<td>184.16KB</td>
<td>150ms</td>
<td>256bits</td>
</tr>
</tbody>
</table>

IntegriDB supports 12 out of 22 queries in TPC-H benchmark, 94% of the queries in TPC-C benchmark.

Improvement upon prior work:
Table: 1000 rows and 10 columns. Query: 10-dimensional range + sum.

<table>
<thead>
<tr>
<th>Setup time</th>
<th>Libsnark (circuit-based)</th>
<th>SNARKs for C (RAM-based)</th>
<th>IntegriDB</th>
</tr>
</thead>
<tbody>
<tr>
<td>187.96s</td>
<td>2000s*</td>
<td>1000s*</td>
<td>10.420s</td>
</tr>
<tr>
<td>47.57s</td>
<td>8ms*</td>
<td>10ms*</td>
<td>112ms</td>
</tr>
<tr>
<td>288 Bytes</td>
<td>288 Bytes</td>
<td>84 KB</td>
<td></td>
</tr>
</tbody>
</table>