**Goal: Increase efficiency of cryptographic techniques**

**Existing Problem**
Cryptographic techniques are:

1. Not efficient
2. Prone to various attacks

**Partition Computation**
- Partition the data into sensitive and non-sensitive
- Sensitive data is cryptographically secure
- Non-sensitive data is in cleartext

<table>
<thead>
<tr>
<th>Technique</th>
<th>Time</th>
<th>Resilient to attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>DET Enc.</td>
<td>1.43x</td>
<td></td>
</tr>
<tr>
<td>Non-DET Enc.</td>
<td>2.1x</td>
<td></td>
</tr>
<tr>
<td>Distributed</td>
<td>3281x</td>
<td></td>
</tr>
<tr>
<td>Searchable Enc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SGX</td>
<td>6724x</td>
<td></td>
</tr>
<tr>
<td>Full-Retrieval</td>
<td>11235x</td>
<td></td>
</tr>
<tr>
<td>Homomorphic</td>
<td>&gt;11235x</td>
<td></td>
</tr>
<tr>
<td>+ ORAM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- The time to search a predicate in cleartext.
- A technique is resilient to a given attack.

**Query Binning**
- Distribute “values” into a matrix
- Rows become sensitive bins
- Columns become non-sensitive bins

**Idea of Query Binning**
- Distribute “values” into a matrix
- Rows become sensitive bins
- Columns become non-sensitive bins

**Performance**

\[
\eta = \frac{\text{Cost}_{\text{crypt}}(|SB|, S)}{\text{Cost}_{\text{Crypt}}(1, D)} + \frac{\text{Cost}_{\text{plain}}(|NSB|, NS)}{\text{Cost}_{\text{Crypt}}(1, D)}
\]

**Inference Attacks due to Data Partitioning**
Adversarial view what the adversary observes

- Works for any number of sensitive and non-sensitive values
- Improves an underlying cryptographic technique by preventing output-size and frequency-count attacks
- Supports conjunctive selection, join, and range queries

**Reference**