Goal: Highly secure aggregation queries with verification

1. Information-Theoretically Secure Computations
   - Secret-shared data
   - Secret-shared query
   - Database owner
   - Public cloud servers

   • Secure regardless of the computational power of the adversary
   • No need to involve the database owner in executing a query
   • Completely access-patterns hiding but not slow
   • Supported queries: Sum, Maximum, Minimum, Group-by with complex selection predicates

2. Data Outsourcing
   - Employee Relation
   - Fast answering to maximum finding queries

   Query: select count(*) from Employee where Name = ‘John’ and Salary = 1000

3. Additional Key Points
   - Handle one or more database owners
   - A tradeoff between the number of shares and the computation time
   - Can be used with a secret-sharing technique that supports multiplicative string-matching

4. Performance
   - Execution time over 6M rows
   - Verification time over 6M rows

5. Reference
   - OBSCURE: Information-Theoretically Secure, Oblivious, and Verifiable Aggregation Queries, PVLDB, 12(9), 2019.