

OBSCURE: Information-Theoretically Secure, Oblivious, and Verifiable Aggregation Queries

Shantanu Sharma¹

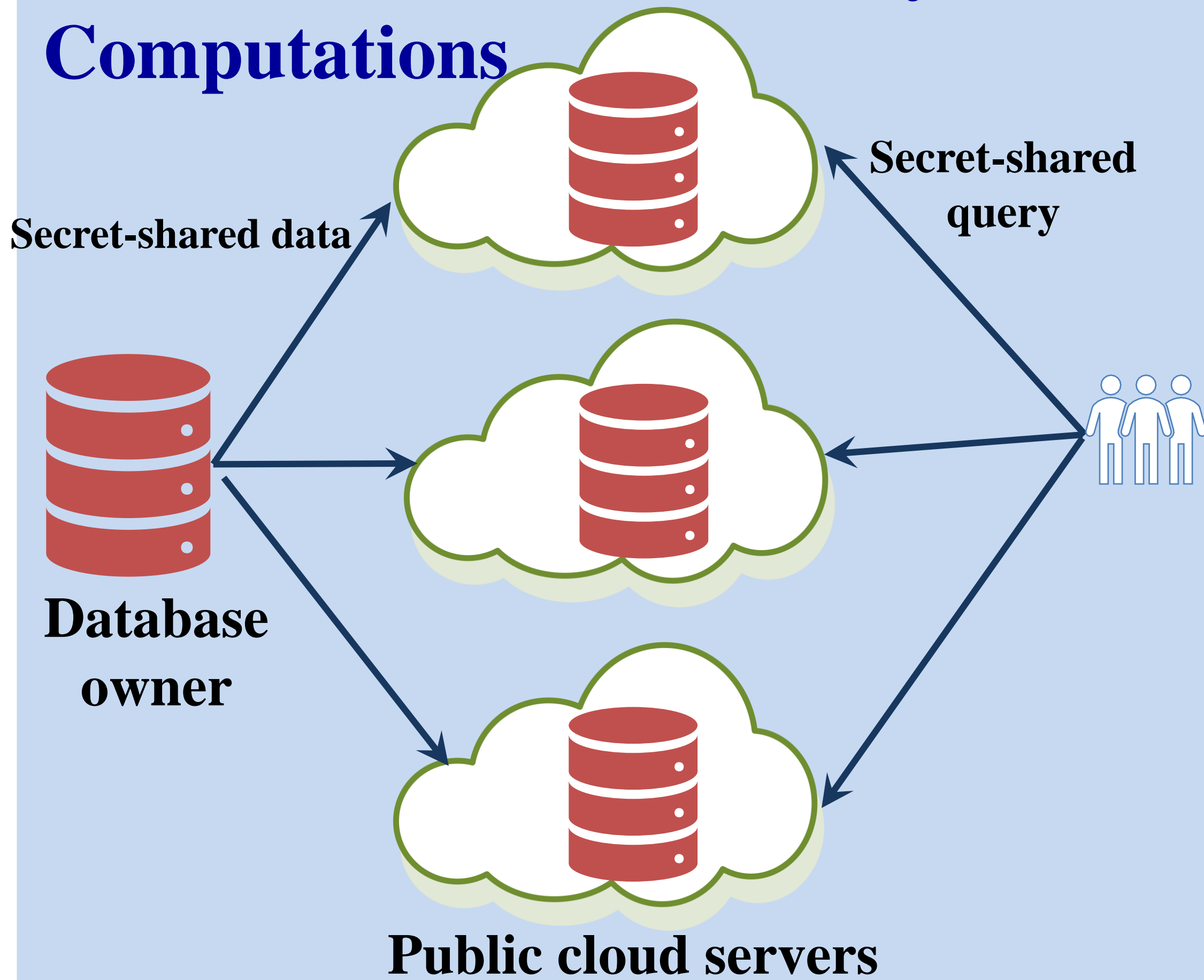
a joint work with

Peeyush Gupta¹, Yin Li², Sharad Mehrotra¹, and Nisha Panwar¹

¹University of California, Irvine, USA. ²Xinyang Normal University, China.

Goal: Highly secure aggregation queries with verification

1 Information-Theoretically Secure Computations

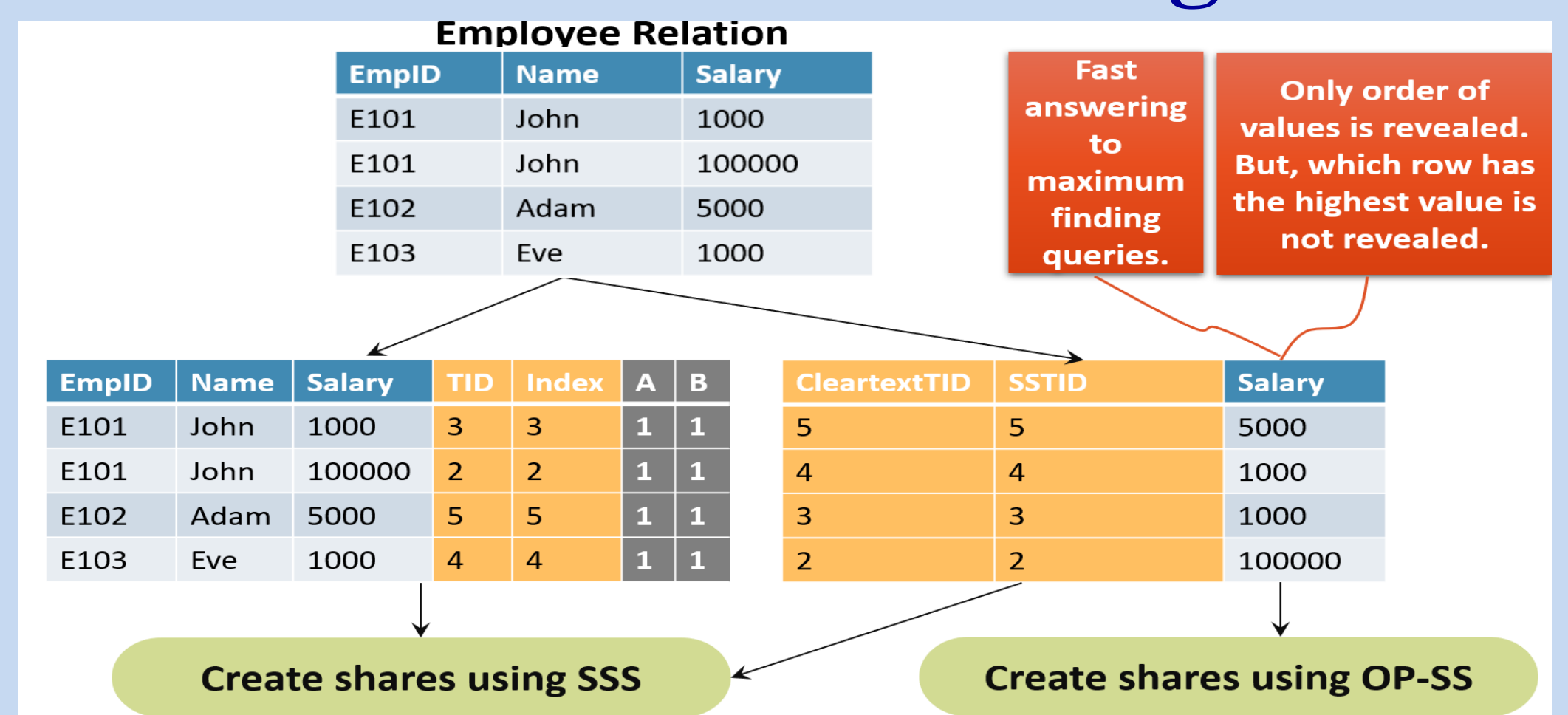


- Secure regardless of the computational power of the adversary
- No need to involve the database owner in executing a query
- **Completely access-patterns hiding but not slow**
- **Supported queries: Sum, Maximum, Minimum, Group-by with complex selection predicates**

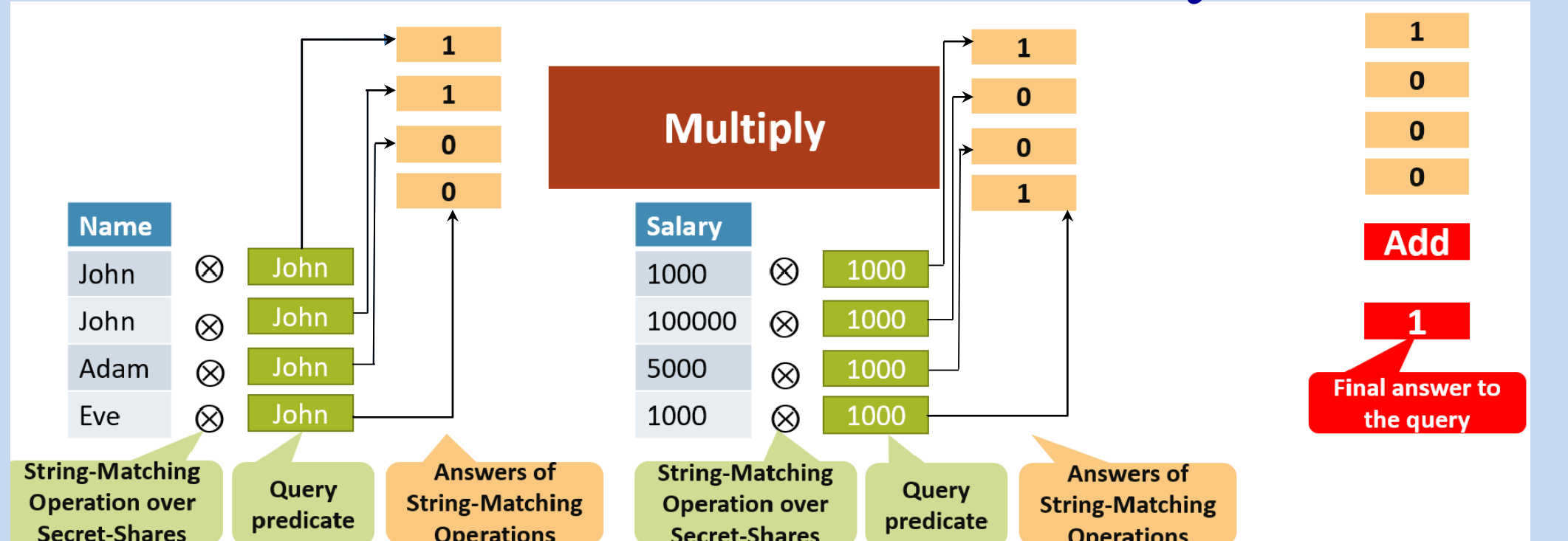
3 Additional Key Points

- 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

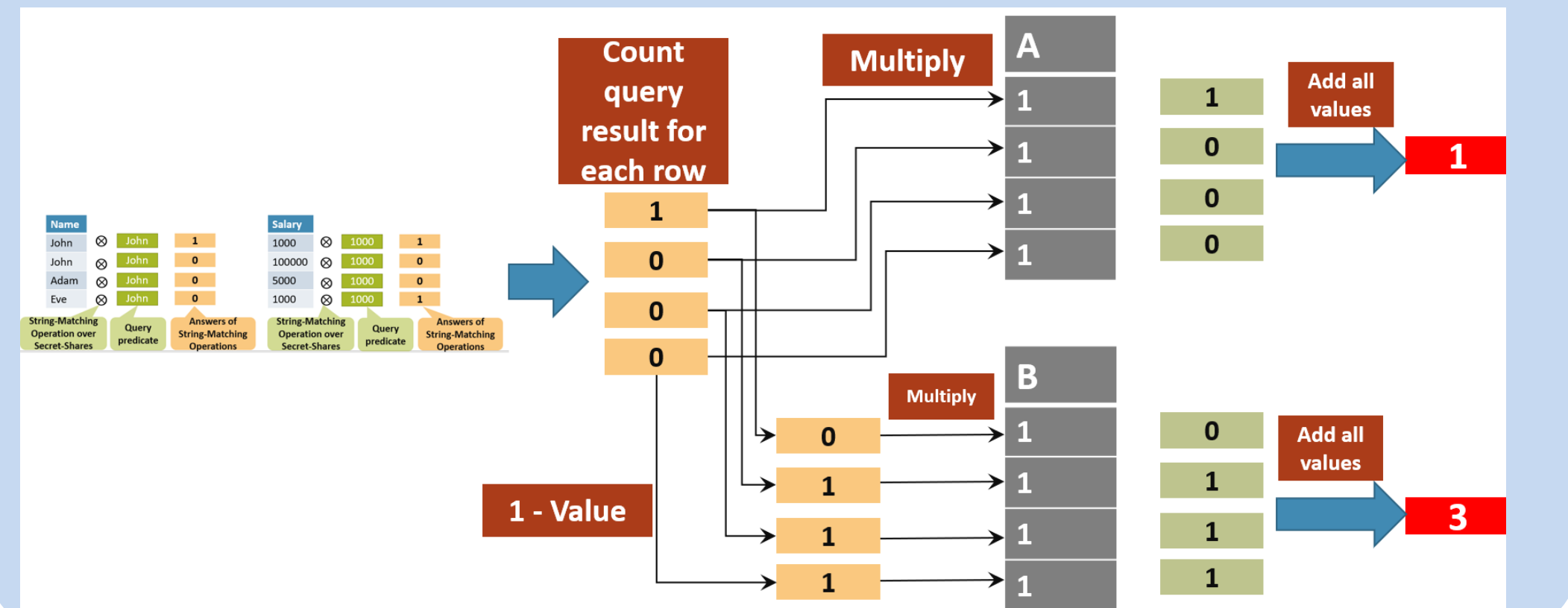
2 Data Outsourcing



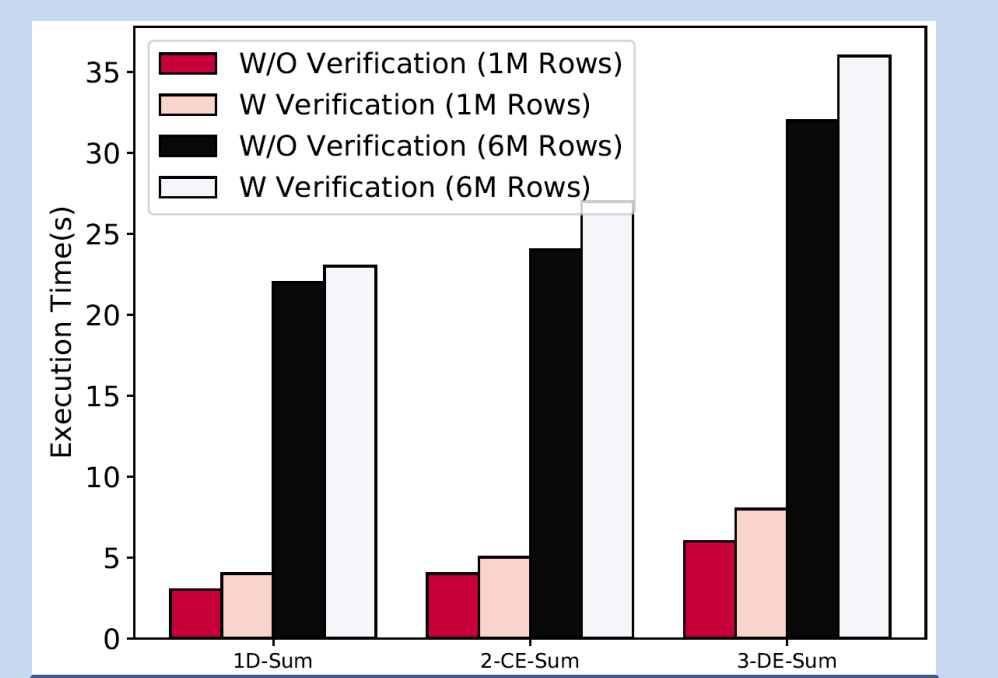
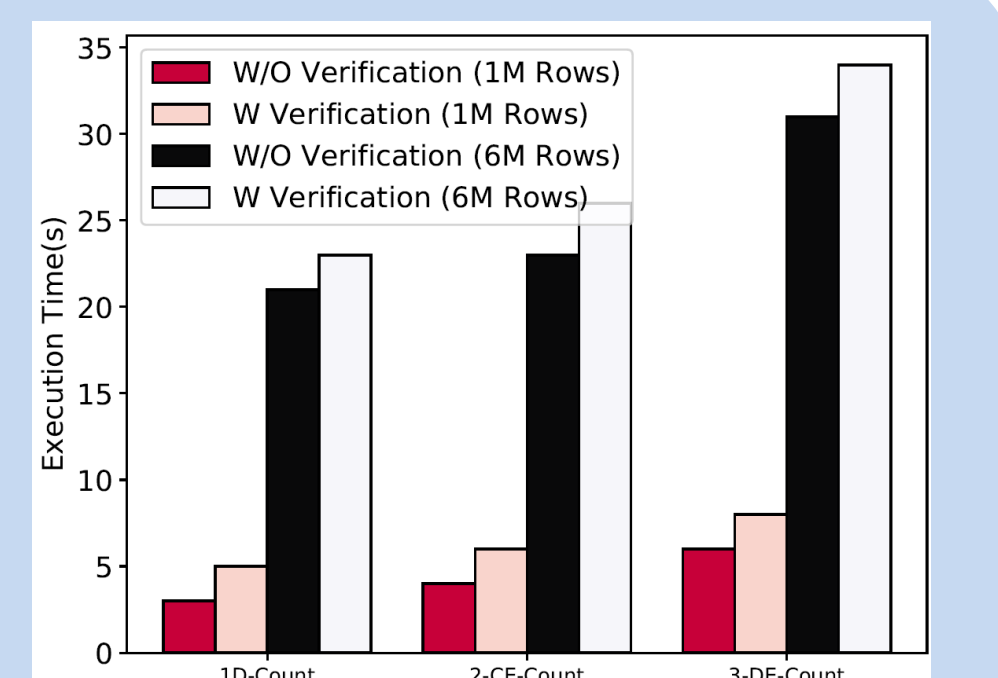
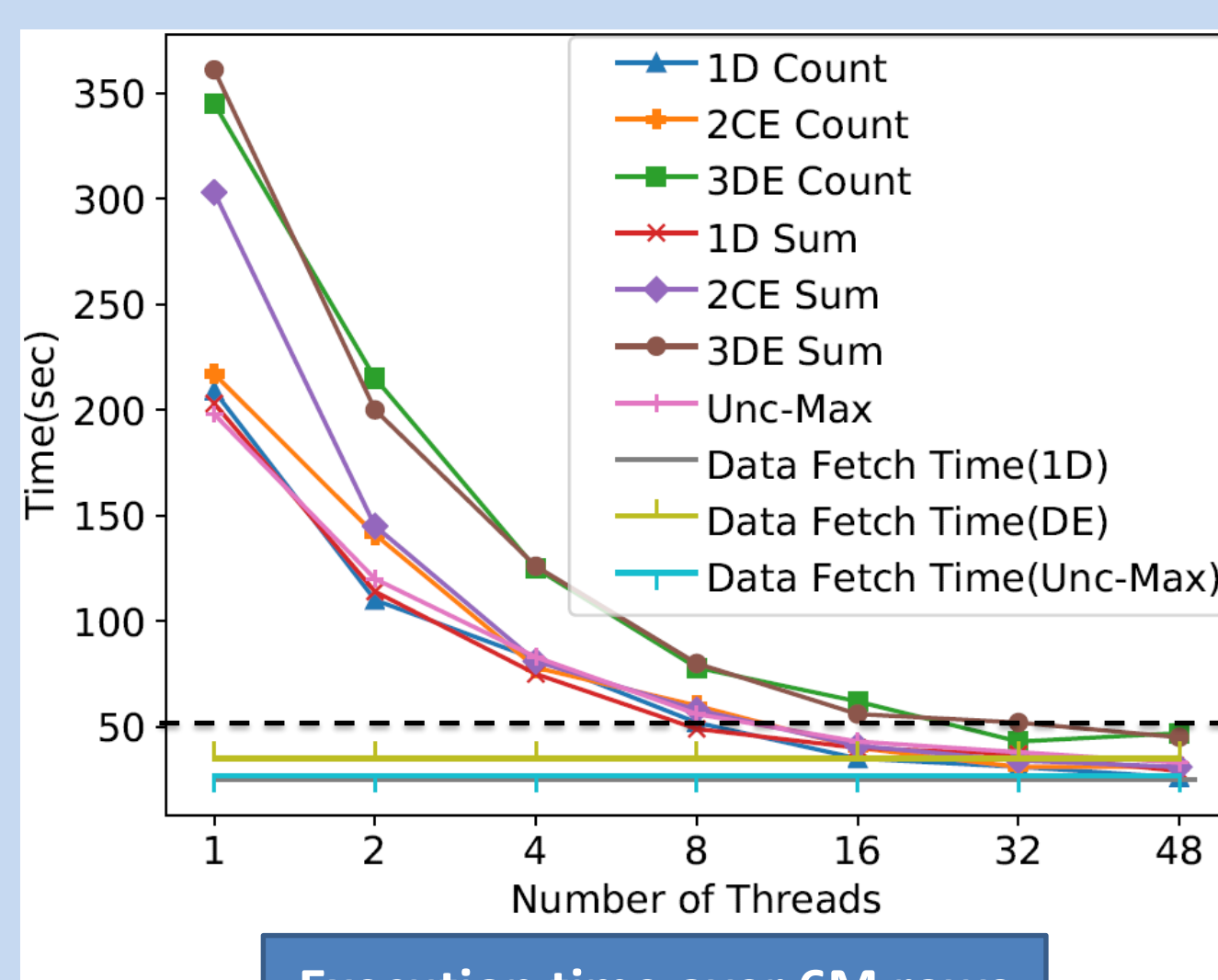
Query: select count(*) from Employee where Name = 'John' and Salary = 1000



Verification



4 Performance



5 Reference

- OBSCURE: Information-Theoretic Oblivious and Verifiable Aggregation Queries, *PVLDB*, 12(9), 2019.

