TWC: Small: General and Modular Secure Computation in the Offline-Online Paradigm

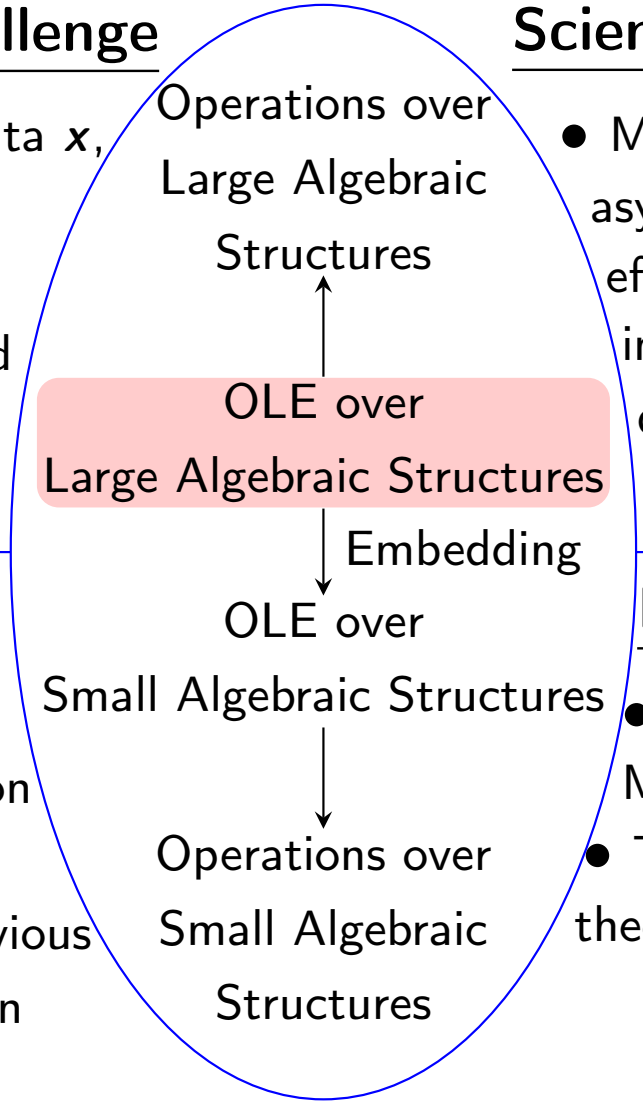
(Representative) Challenge

For distributed private data $\boldsymbol{x}$, compare MSBs of $A \cdot \boldsymbol{x}$ with a fixed vector $\boldsymbol{b}$

Computation Represented using operators over different fields

Solution

- Secure Computation indep. of the Computation Representation
- Generalize OT to Oblivious Linear-function Evaluation over Fields/Rings (OLE)



Scientific Impact

- MPC protocols with asymptotic and concrete efficiency, for example, in privacy-preserving data mining

Broader Impact

- Practical and scalable MPC
- Training in Information-theoretic MPC

Award: CNS 1618822, PI: Hemanta K . Maji