

CRII: SaTC: Computational Correlations: A New Tool for Cryptography



Challenge

Understanding the computational essence of securely realizing oblivious transfer (OT)

Solution

- Computational analog of “Information-theoretic Completeness,” a.k.a. Computational Correlations

Scientific Impact

- Theory of “Computational Correlations”
- Computational hardness Results

Broader Impact

- Efficient protocols for oblivious transfer
- Training in Information-theoretic Cryptography

