

From OT to OLE with Subquadratic Communication

Jack Doerner, Iftach Haitner, Yuval Ishai, Nikolaos Makriyannis

I enthusiastically nominate the paper "*From OT to OLE with Subquadratic Communication*" for its profound algorithmic breakthrough in secure multiparty computation (MPC). The paper tackles the longstanding efficiency gap between Oblivious Transfer (OT) and Oblivious Linear Evaluation (OLE). The authors creatively apply the Chinese Remainder Theorem (CRT) to Gilboa's classic 1999 protocol to drop the communication cost of reducing OLE to OT from $O(\ell^2)$ down to subquadratic $\tilde{O}(\ell)$ bits (where ℓ is the modulus bit length). To secure this against malicious receivers—a flaw in direct CRT applications—they ingeniously weave together number-theoretic and RSA-based techniques, maintaining low overhead while guaranteeing full malicious security. Oblivious Linear Evaluation is an incredibly powerful algebraic primitive, yet its practical utility has long been suppressed by massive communication bandwidth bottlenecks. By essentially aligning the communication overhead of OLE much closer to that of standard OT, this work unlocks a new tier of efficiency for applied cryptography. The significance of this optimization immediately translates into dramatic performance boosts for dependent downstream technologies, drastically accelerating modern digital asset operations, threshold/distributed signatures (like ECDSA), and post-quantum oblivious pseudorandom functions (OPRFs).