MyOPE: Malicious securitY for Oblivious Polynomial Evaluation

Talk by Paola de Perthuis

Work by: Malika Izabachène[1], Anca Nitulescu[2], Paola de Perthuis[1,3,4], and David Pointcheval[3,4]

[1] Cosmian
[2] Protocol Labs
[3] DIENS, École normale supérieure, CNRS, PSL University, Paris, France
[4] INRIA, Paris, France

Abstract. Oblivious Polynomial Evaluation (OPE) schemes are interactive protocols between a sender with a private polynomial and a receiver with a private evaluation point where the receiver learns the evaluation of the polynomial in their point and no additional information. They are used in Private Set Intersection (PSI) protocols, where two users with private sets want to compute their intersection without revealing any information about the other data.

We introduce a scheme for OPE in the presence of malicious senders that has sublinear communication thanks to the use of FHE ciphertexts, enforcing honest sender behavior and consistency by adding verifiability to the calculations. This scheme is also secure against honest-but-curious receivers. The FHE grants input privacy and succinct arguments of knowledge using a linear-only homomorphic encoding scheme give the verifiability property. MyOPE deploys sublinear communication costs in the sender's polynomial degree and one to five rounds of interaction.

In other words, it can be used as a verifiable computation scheme for polynomial evaluation over FHE ciphertexts. While classical techniques in pairing-based settings allow generic succinct proofs for such evaluations, they require large prime order subgroups which highly impact the communication complexity, and prevent the use of FHE with practical parameters. MyOPE builds on generic secure encodings techniques that allow composite integers and enable real-world FHE parameters and even RNS-based optimizations. It is best adapted for the unbalanced setting where the degree of the polynomial and the computing power of the sender are large.

MyOPE can be used as a building block in specialized two-party protocols such as PSI, oblivious keyword search, set membership and more using the OPE instantiation.

As another contribution, our techniques are generalized to applications other than OPE, such as Symmetric Private Information Retrieval (SPIR), to make them secure against a malicious sender.

We are currently working on making this protocol also secure against a malicious receiver when they initially send several intermediate ciphertexts to have the sender make calculations with less multiplicative depth on them, thus smaller FHE ciphertexts.