Multi-party Function Evaluation with Perfectly Private Audit Trail

Édouard Cuvelier and Olivier Pereira

Université catholique de Louvain – ICTEAM - Crypto Group
1348 Louvain-la-Neuve Belgium

We propose an efficient and simple protocol for the evaluation of functions getting their inputs from multiple parties in a way that guarantees the correctness of the computation to everyone and the perfect privacy of the inputs as long as the worker is honest. Our protocol finds applications in a Clients-Workers environment where we assume that the clients have a strong incentive to collaborate if they receive a high level guarantee about the result correctness. In conventional Secure Multi-Party Computation schemes, the complexity cost for the clients is at least the complexity of the algorithm that evaluates the function. In our proposal, this is only the maximum bound and in most cases, the complexity for the clients is considerably lower. Indeed, rather than having each client evaluate the whole algorithm to compute the solution, in our case, each client only verifies that the solution provided by the workers is correct. For example, many NP problems require costly computing algorithms but, once the solution is found, it is quickly verifiable. In addition to computational verifiability, our protocol offers perfect privacy towards the public in the sense of the theory of information. Moreover, it is universally composable.

Our construction relies on homomorphic *commitment consistent encryption*, a type of encryption scheme that enables the extraction of perfectly hiding commitments on encrypted messages. Encryption guarantees private communications with the worker, while commitments enable public verification with no impact on privacy. To enrich the possible operations between commitments such as multiplications and comparisons, we rely on non-interactive zero-Knowledge proofs of knowledge. As the building blocks are well-studied tools, our generic construction is user-friendly and efficiently implementable.

We present three unrelated applications of our technique : solving a linear system of equations, an auction scheme and the search of the shortest path in a shared graph. These examples illustrate the ease of use and the advantage in terms of complexity of our approach. We based a prototype implementation on Elliptic Curve, which gives us encouraging timing result.