Efficient Secure Two-Party Computation

Thomas Schneider and Michael Zohner

Engineering Cryptographic Protocols Group
European Center for Security and Privacy by Design (EC SPRIDE)
Technische Universität Darmstadt, Germany

Secure two-party computation allows two mutually distrusting parties to compute a function on their private inputs without revealing anything but the result to each other. This enables a variety of privacy-preserving applications, such as biometric identification, mobile social networks, or online market places. In the mid-eighties, two conceptually different generic approaches for constructing secure two-party protocols have been proposed: Yao's garbled circuit protocol [4] and the Goldreich-Micali-Widgerson (GMW) protocol [2]. Both protocols represent a function as (boolean) circuit and compute the output of the function by evaluating each gate in the circuit.

Since the introduction of both approaches, a lot of research was dedicated to improving the efficiency of Yao's garbled circuits. The GMW protocol, on the other hand, was believed to be too inefficient as it requires a huge number of oblivious transfer evaluations and an interaction step for each AND gate. A recent work [1] demonstrated that by precomputing oblivious transfers efficiently in a setup phase, the actual function can be evaluated very efficiently in a later online phase. However, the authors present benchmarks only for $n > 2$ parties and expected their implementation to be slower by a factor of two compared to the currently fastest Yao's garbled circuit framework of [3] in the two-party case with semi-honest adversaries.

In this talk we present several optimizations for the GMW protocol and show that in the two-party case with semi-honest adversaries, the GMW protocol is a noticable alternative to Yao's garbled circuits. Our optimizations include the use of load balancing and bytewise processing, which allow an efficient online phase and make the GMW protocol suited for the use in resource restricted devices such as mobile phones. In order to reduce the impact of the interaction step on the online time of the GMW protocol we summarize depth-optimized circuit constructions for various standard tasks. As an application scenario we consider privacy-preserving face recognition and compare the performance of our framework with the framework of [3]. Our experiments show that the online phase of our GMW implementation is faster than the framework of [3] by a factor of up to 150 on databases that contain tens of thousands of face images.

References

[1] Choi, S.G., Hwang, K.W., Katz, J., Malkin, T., Rubenstein, D.: Secure multi-party computation of Boolean circuits with applications to privacy in on-line market-places. In: Cryptographers Track at the RSA Conference (CT-RSA12). LNCS, vol. 7178, pp. 416-432. Springer (2012)

[2] Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game or a completeness theorem for protocols with honest majority. In: Symposium on Theory of Computing (STOC87). pp. 218-229. ACM (1987)

[3] Huang, Y., Evans, D., Katz, J., Malka, L.: Faster secure two-party computation using garbled circuits. In: Security Symposium. USENIX (2011)

[4] Yao, A.C.: How to generate and exchange secrets. In: Foundations of Computer Science (FOCS86). pp. 162-167. IEEE (1986)