Practical Secure Function Evaluation

Vladimir Kolesnikov†, Thomas Schneider* and Volker Strehl*

* Friedrich-Alexander Universität
Erlangen-Nürnberg
Germany

† Bell Laboratories
600 Mountain Ave. Murray Hill, NJ 07974
USA

Since the first publication of Yao [Yao86], Secure Function Evaluation (SFE) is a well-researched problem. Continuing advances in available computational power and communication have made secure computation of many useful functions affordable. Recent work like Fairplay [MNPS04] demonstrate practicability of general SFE. This thesis focuses on several practical aspects of SFE.

Our new improved SFE protocol allows free evaluation of XOR gates and is provably secure against semi-honest adversaries in the random oracle model - the same assumptions that Fairplay relies on. The protocol merges elements of the information-theoretic SFE protocol GESS [Kol05] with Fairplay. This results in substantial performance improvements of 50% for many important circuit structures like addition or number comparison.

SFE is extended to allow the evaluated function to be secret and only known by one party, called SFE of private functions (PF-SFE). These settings occur naturally in applications like no-fly-list-, credit report-, or medical history checking. It is known that PF-SFE can easily be reduced to SFE of universal circuits (UC). We give a practical UC construction [KS08] that is up to 50% smaller than the best UC of Valiant [Val76] when used in today's PF-SFE. FairplayPF was implemented as extension of Fairplay to demonstrate practicability of PF-SFE based on the new UC construction. Using the improved SFE protocol, UC-based PF-SFE can be improved by another factor of 4.

Besides these circuit-based approaches for SFE and PF-SFE new protocols for SFE and PF-SFE of functions represented as Ordered Binary Decision Diagrams (OBDDs) are given that are based on [KJGB06]. This SFE protocol for OBDDs is extended to the malicious model and shown how to obtain a PF-SFE protocol for OBDDs at the cost of a small overhead only.

The results of this thesis substantially improve general SFE for many practical functions and demonstrate practicability of general PF-SFE for "small" functions.

References

[Kol05] Vladimir Kolesnikov. Gate evaluation secret sharing and secure one-round two-party computation. In *Advances in Cryptology – ASIACRYPT05*, volume 3788 of *LNCS*, pages 136–155. Springer, 2005.

[KS08] Vladimir Kolesnikov and Thomas Schneider. A practical universal circuit construction and secure evaluation of private functions. In *Financial Cryptography and Data Security, FC08*, LNCS. Springer, 2008. `http://thomaschneider.de/FairplayPF`.

[KJGB06] Louis Kruger, Somesh Jha, Eu-Jin Goh, and Dan Boneh. Secure function evaluation with ordered binary decision diagrams. In *CCS*, pages 410–420. ACM Press, 2006.

[MNPS04] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay - a secure two-party computation system. In *USENIX*, 2004.
`http://www.cs.huji.ac.il/project/Fairplay/fp1.html`.

[Val76] Leslie G. Valiant. Universal circuits (preliminary report). In *Proc. 8th ACM Symp. on Theory of Computing*, pages 196–203, New York, NY, USA, 1976. ACM Press.

[Yao86] Andrew C. Yao. How to generate and exchange secrets. In *Proc. 27th IEEE Symp. on Foundations of Comp. Science*, pages 162–167, Toronto, 1986. IEEE.