Private Function Evaluation with Universal Circuits

Daniel Günther
Technische Universität Darmstadt
Darmstadt, Germany
guenther@rangar.de

Secure Function Evaluation (SFE) is a cryptographic primitive that allows two parties to jointly compute a public function without revealing their inputs, while *Private Function Evaluation* (PFE) additionally hides the computed function that one party provides. There exist many applications of PFE, e.g. analyzing and processing medical data for a privacy-friendly diagnostic service [BFK+09] or privacy-preserving intrusion detection [NSMS14]. [PKV+14, FVK+15] make use of PFE in order to hide queries in a database management system.

PFE can be efficiently reduced to SFE by using a Universal Circuit (UC) as public function. A UC is a special Boolean circuit that can be programmed to compute arbitrary functions up to a given size n by providing the corresponding programming bits. Beyond PFE, UC's have several applications such as *multi-hop homomorphic encryption* [GHV10], *Ciphertext-policy Attribute-Based Encryption* [Att14], and *Direct Program Obfuscation* [Zim15]. [Weg87] proved that the asymptotical lower bound of the size of UCs is $\Omega(n \log n)$. The first two theoretical UC constructions were provided by Valiant in [Val76] - today known as 2-way and 4-way split constructions due to their recursive structure built up of 2 or 4 substructures - with sizes $5n \log_2 n$ and $4.75n \log_2 n$, respectively. The 2-way split construction was implemented by [KS16] and [LMS16] in concurrent and independent works, while the implementation of the 4-way split construction was provided by [Gün17, GKS17].

In this talk, we present the modular design of our 4-way split implementation which can be generalized to any k-way split construction. We explain the single components of our UC compiler. [LMS16] introduced this idea and we have turned this approach into a modular design and implementation in [Gün17, GKS17]. The 2-way split construction leads in general to a better size for small functions while the 4-way split construction has smaller sizes for large functions. However, due to the recursive structure of Valiant's UC construction, in [GKS17] we present a hybrid UC construction that combines the 2-way and 4-way split UCs in order to use the best available substructure at each recursion step, and yields the best sizes for all functions. The implementation of our 4-way split UC is available at `https://github.com/encryptogroup/UC`.

The improvement of the 4-way construction over the 2-way construction is on average 3.12% and for our hybrid construction it is 3.65%. The hybrid construction is practical for many applications. Our hybrid UC construction is the best known to date and our implementation allows on a machine with 32 GB of memory to process circuits up to $n = 1{,}4$ million gates which results in a UC with around 120 million AND gates.

References

[Att14] Attrapadung, N. Fully secure and succinct attribute based encryption for circuits from multi-linear maps. Cryptology ePrint Archive, Report 2014/772 (2014).

[BFK+09] Barni, M., Failla, P., Kolesnikov, V., Lazzeretti, R., Sadeghi, A.-R., Schneider, T. Secure evaluation of private linear branching programs with medical applications. ESORICS 2009. Springer.

crypto day matters 29 (2018)
Beiträge vom 29. Krypto-Tag, 06.-07.09.2018, Bosch, Renningen.
doi:10.18420/cdm-2018-29-01

[FVK+15] Fisch, B., Vo, B., Krell, F., Kumarasubramanian, A., Kolesnikov, V., Malkin, T., Bellovin, S.M. Malicious-client security in Blind Seer: a scalable private DBMS. IEEE S&P 2015. IEEE (2015).

[GHV10] Gentry, C., Halevi, S., Vaikuntanathan, V.. i-hop homomorphic encryption and rerandomizable Yao circuits. Rabin, T. (ed.). CRYPTO 2010. Springer.

[GKS17] Günther, D., Kiss, A., Schneider, T. More efficient universal circuit constructions. ASIACRYPT 2017. Springer.

[Gün17] Günther, D. Valiant's universal circuit - towards a modular construction and implementation. Bachelor Thesis. March 2017. Publication: `https://www.encrypto.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_ENCRYPTO/theses/BSc_DGunther.pdf`.

[KS16] Kiss, A., Schneider, T. Valiant's universal circuit is practical. EUROCRYPT 2016. Springer.

[LMS16] Lipmaa, H., Mohassel, P., Sadeghian, S.S. Valiant's universal circuit: improvements, implementation, and applications. Cryptology ePrint Archive, Report 2016/017. (2016).

[NSMS14] Niksefat, S., Sadeghiyan, B., Mohassel, P., Sadeghian, S.S. ZIDS: a privacy-preserving intrusion detection system using secure two-party computation protocols. Computer Journal 57(4) (2014).

[PKV+14] Pappas, V., Krell, F., Vo, B., Kolesnikov, V., Malkin, T., Geol Choi, S., George, W., Keromytis, A.D., Bellovin, S. Blind Seer: a scalable private DBMS. IEEE S&P 2014. IEEE (2014).

[Val76] Valiant, L.G. Universal circuits (preliminary report). STOC-1976. ACM (1976).

[Weg87] Wegener, I. The complexity of Boolean functions. Wiley-Teubner (1987).

[Zim15] Zimmerman, J. How to obfuscate programs directly. EUROCRYPT 2015. Springer.