1. Samee Zahur, Mike Rosulek, and David Evans. “Two Halves Make a Whole - Reducing Data Transfer in Garbled Circuits Using Half Gates”. In: *EUROCRYPT 2015, Part II.* ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9057. LNCS. Springer, Heidelberg, Apr. 2015, pp. 220–250. DOI: 10.1007/978-3-662-46803-6_8

2. Xiao Wang, Samuel Ranellucci, and Jonathan Katz. “Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation”. In: *ACM CCS 2017.* Ed. by Bhavani M. Thuraisingham et al. ACM Press, Oct. 2017, pp. 21–37. DOI: 10.1145/3133956.3134053

3. Jonathan Katz et al. “Optimizing Authenticated Garbling for Faster Secure Two-Party Computation”. In: *CRYPTO 2018, Part III.* ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. LNCS. Springer, Heidelberg, Aug. 2018, pp. 365–391. DOI: 10.1007/978-3-319-96878-0_13

4. Samuel Dittmer et al. “Authenticated Garbling from Simple Correlations”. In: *CRYPTO 2022, Part IV.* ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13510. LNCS. Springer, Heidelberg, Aug. 2022, pp. 57–87. DOI: 10.1007/978-3-031-15985-5_3

5. Hongrui Cui et al. “Actively Secure Half-Gates with Minimum Overhead Under Duplex Networks”. In: *EUROCRYPT 2023, Part II.* ed. by Carmit Hazay and Martijn Stam. Vol. 14005. LNCS. Springer, Heidelberg, Apr. 2023, pp. 35–67. DOI: 10.1007/978-3-031-30617-4_2

References

[Cui+23] Hongrui Cui et al. “Actively Secure Half-Gates with Minimum Overhead Under Duplex Networks”. In: *EUROCRYPT 2023, Part II.* Ed. by Carmit Hazay and Martijn Stam. Vol. 14005. LNCS. Springer, Heidelberg, Apr. 2023, pp. 35–67. DOI: 10.1007/978-3-031-30617-4_2.

[Dit+22] Samuel Dittmer et al. “Authenticated Garbling from Simple Correlations”. In: *CRYPTO 2022, Part IV.* Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13510. LNCS. Springer, Heidelberg, Aug. 2022, pp. 57–87. DOI: 10.1007/978-3-031-15985-5_3.

[Kat+18] Jonathan Katz et al. “Optimizing Authenticated Garbling for Faster Secure Two-Party Computation”. In: *CRYPTO 2018, Part III.* Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. LNCS. Springer, Heidelberg, Aug. 2018, pp. 365–391. DOI: 10.1007/978-3-319-96878-0_13.

[WRK17] Xiao Wang, Samuel Ranellucci, and Jonathan Katz. “Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation”. In: *ACM CCS 2017.* Ed. by Bhavani M. Thuraisingham et al. ACM Press, Oct. 2017, pp. 21–37. DOI: 10.1145/3133956.3134053.

[ZRE15] Samee Zahur, Mike Rosulek, and David Evans. “Two Halves Make a Whole - Reducing Data Transfer in Garbled Circuits Using Half Gates”. In: *EUROCRYPT 2015, Part II.* Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9057. LNCS. Springer, Heidelberg, Apr. 2015, pp. 220–250. DOI: 10.1007/978-3-662-46803-6_8.