References

Afshar, A., Z. Hu, P. Mohassel, and M. Rosulek. 2015. "How to Efficiently Evaluate RAM Programs with Malicious Security". In: *Advances in Cryptology – EUROCRYPT 2015, Part I*. Ed. by E. Oswald and M. Fischlin. Vol. 9056. *Lecture Notes in Computer Science*. Springer, Heidelberg. 702–729. DOI: 10.1007/978-3-662-46800-5_27.

Aly, A., M. Keller, E. Orsini, D. Rotaru, P. Scholl, N. Smart, and T. Wood. 2018. "SCALE and MAMBA Documentation". https://homes.esat.kuleuven.be/~nsmart/SCALE/Documentation.pdf.

Ames, S., C. Hazay, Y. Ishai, and M. Venkitasubramaniam. 2017. "Ligero: Lightweight Sublinear Arguments Without a Trusted Setup". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 2087–2104.

Araki, T., A. Barak, J. Furukawa, T. Lichter, Y. Lindell, A. Nof, K. Ohara, A. Watzman, and O. Weinstein. 2017. "Optimized Honest-Majority MPC for Malicious Adversaries - Breaking the 1 Billion-Gate Per Second Barrier". In: *2017 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 843–862.

Araki, T., J. Furukawa, Y. Lindell, A. Nof, and K. Ohara. 2016. "High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority". In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 805–817.

Asharov, G., A. Beimel, N. Makriyannis, and E. Omri. 2015a. "Complete Characterization of Fairness in Secure Two-Party Computation of Boolean Functions". In: *TCC 2015: 12th Theory of Cryptography Conference, Part I*. Ed. by Y. Dodis and J. B. Nielsen. Vol. 9014. *Lecture Notes in Computer Science*. Springer, Heidelberg. 199–228. DOI: 10.1007/978-3-662-46494-6_10.

Asharov, G., A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs. 2012. "Multiparty computation with low communication, computation and interaction via threshold FHE". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt)*. Springer. 483–501.

Asharov, G., Y. Lindell, T. Schneider, and M. Zohner. 2015b. "More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries". In: *Advances in Cryptology – EUROCRYPT 2015, Part I*. Ed. by E. Oswald and M. Fischlin. Vol. 9056. *Lecture Notes in Computer Science*. Springer, Heidelberg. 673–701. DOI: 10.1007/978-3-662-46800-5_26.

Asharov, G. and C. Orlandi. 2012. "Calling Out Cheaters: Covert Security with Public Verifiability". In: *Advances in Cryptology – ASIACRYPT 2012*. Ed. by X. Wang and K. Sako. Vol. 7658. *Lecture Notes in Computer Science*. Springer, Heidelberg. 681–698. DOI: 10.1007/978-3-642-34961-4_41.

Aumann, Y. and Y. Lindell. 2007. "Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries". In: *TCC 2007: 4th Theory of Cryptography Conference*. Ed. by S. P. Vadhan. Vol. 4392. *Lecture Notes in Computer Science*. Springer, Heidelberg. 137–156.

Bahmani, R., M. Barbosa, F. Brasser, B. Portela, A.-R. Sadeghi, G. Scerri, and B. Warinschi. 2017. "Secure multiparty computation from SGX". In: *International Conference on Financial Cryptography and Data Security*. 477–497.

Ball, M., T. Malkin, and M. Rosulek. 2016. "Garbling Gadgets for Boolean and Arithmetic Circuits". In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 565–577.

Bar-Ilan Center for Research in Applied Cryptography and Cyber Security. 2014. "SCAPI: Secure Computation API". https://cyber.biu.ac.il/scapi/.

Beaver, D. 1992. "Efficient Multiparty Protocols Using Circuit Randomization". In: *Advances in Cryptology – CRYPTO'91*. Ed. by J. Feigenbaum. Vol. 576. *Lecture Notes in Computer Science*. Springer, Heidelberg. 420–432.

Beaver, D. 1995. "Precomputing Oblivious Transfer". In: *Advances in Cryptology – CRYPTO'95*. Ed. by D. Coppersmith. Vol. 963. *Lecture Notes in Computer Science*. Springer, Heidelberg. 97–109.

Beaver, D. 1996. "Correlated Pseudorandomness and the Complexity of Private Computations". In: *28th Annual ACM Symposium on Theory of Computing*. ACM Press. 479–488.

Beaver, D., S. Micali, and P. Rogaway. 1990. "The Round Complexity of Secure Protocols (Extended Abstract)". In: *22nd Annual ACM Symposium on Theory of Computing*. ACM Press. 503–513.

Beerliová-Trubíniová, Z. and M. Hirt. 2008. "Perfectly-Secure MPC with Linear Communication Complexity". In: *TCC 2008: 5th Theory of Cryptography Conference*. Ed. by R. Canetti. Vol. 4948. *Lecture Notes in Computer Science*. Springer, Heidelberg. 213–230.

Beimel, A. and B. Chor. 1993. "Universally Ideal Secret Sharing Schemes (Preliminary Version)". In: *Advances in Cryptology – CRYPTO'92*. Ed. by E. F. Brickell. Vol. 740. *Lecture Notes in Computer Science*. Springer, Heidelberg. 183–195.

Bellare, M., V. T. Hoang, S. Keelveedhi, and P. Rogaway. 2013. "Efficient Garbling from a Fixed-Key Blockcipher". In: *2013 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 478–492.

Bellare, M., V. T. Hoang, and P. Rogaway. 2012. "Foundations of garbled circuits". In: *ACM CCS 12: 19th Conference on Computer and Communications Security*. Ed. by T. Yu, G. Danezis, and V. D. Gligor. ACM Press. 784–796.

Bellare, M. and P. Rogaway. 1993. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols". In: *ACM CCS 93: 1st Conference on Computer and Communications Security*. Ed. by V. Ashby. ACM Press. 62–73.

Bendlin, R., I. Damgård, C. Orlandi, and S. Zakarias. 2011. "Semi-homomorphic Encryption and Multiparty Computation". In: *Advances in Cryptology – EUROCRYPT 2011*. Ed. by K. G. Paterson. Vol. 6632. *Lecture Notes in Computer Science*. Springer, Heidelberg. 169–188.

Ben-Or, M., S. Goldwasser, and A. Wigderson. 1988. "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract)". In: *20th Annual ACM Symposium on Theory of Computing*. ACM Press. 1–10.

Bestavros, A., A. Lapets, and M. Varia. 2017. "User-centric Distributed Solutions for Privacy-preserving Analytics". *Communications of the ACM*. 60(2): 37–39. ISSN: 0001-0782. DOI: 10.1145/3029603.

Biryukov, A., D. Khovratovich, and I. Nikolic. 2009. "Distinguisher and Related-Key Attack on the Full AES-256". In: *Advances in Cryptology – CRYPTO 2009*. Ed. by S. Halevi. Vol. 5677. *Lecture Notes in Computer Science*. Springer, Heidelberg. 231–249.

Bogdanov, D. 2015. "Smarter decisions with no privacy breaches - practical secure computation for governments and companies". https://rwc.iacr.org/2015/Slides/RWC-2015-Bogdanov-final.pdf, retrieved March 9, 2018.

Bogdanov, D., S. Laur, and J. Willemson. 2008a. "Sharemind: A Framework for Fast Privacy-Preserving Computations". In: *ESORICS 2008: 13th European Symposium on Research in Computer Security*. Ed. by S. Jajodia and J. López. Vol. 5283. *Lecture Notes in Computer Science*. Springer, Heidelberg. 192–206.

Bogdanov, D., S. Laur, and J. Willemson. 2008b. "Sharemind: A framework for fast privacy-preserving computations". In: *European Symposium on Research in Computer Security*. Springer. 192–206.

Bogetoft, P., D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. I. Schwartzbach, and T. Toft. 2009. "Secure Multiparty Computation Goes Live". In: *FC 2009: 13th International Conference on Financial Cryptography and Data Security*. Ed. by R. Dingledine and P. Golle. Vol. 5628. *Lecture Notes in Computer Science*. Springer, Heidelberg. 325–343.

Boneh, D., E.-J. Goh, and K. Nissim. 2005. "Evaluating 2-DNF formulas on ciphertexts". In: *Theory of Cryptography Conference*. Springer. 325–341.

Boyle, E., N. Gilboa, and Y. Ishai. 2016a. "Breaking the circuit size barrier for secure computation under DDH". In: *Annual Cryptology Conference*. Springer. 509–539.

Boyle, E., N. Gilboa, and Y. Ishai. 2016b. "Function Secret Sharing: Improvements and Extensions". In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 1292–1303.

Boyle, E., Y. Ishai, and A. Polychroniadou. 2018. "Limits of Practical Sublinear Secure Computation". In: *Annual Cryptology Conference*. Springer.

Brandão, L. T. A. N. 2013. "Secure Two-Party Computation with Reusable Bit-Commitments, via a Cut-and-Choose with Forge-and-Lose Technique - (Extended Abstract)". In: *Advances in Cryptology – ASIACRYPT 2013, Part II*. Ed. by K. Sako and P. Sarkar. Vol. 8270. *Lecture Notes in Computer Science*. Springer, Heidelberg. 441–463. DOI: 10.1007/978-3-642-42045-0_23.

Brickell, J., D. E. Porter, V. Shmatikov, and E. Witchel. 2007. "Privacy-preserving remote diagnostics". In: *ACM CCS 07: 14th Conference on Computer and Communications Security*. Ed. by P. Ning, S. D. C. di Vimercati, and P. F. Syverson. ACM Press. 498–507.

Buescher, N. and S. Katzenbeisser. 2015. "Faster Secure Computation through Automatic Parallelization." In: *USENIX Security Symposium*. 531–546.

Buescher, N., A. Weber, and S. Katzenbeisser. 2018. "Towards Practical RAM Based Secure Computation". In: *European Symposium on Research in Computer Security*. Springer. 416–437.

Bulck, J. V., M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx. 2018. "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution". In: *27th USENIX Security Symposium*. Baltimore, MD: USENIX Association. 991–1008.

Burkhart, M., M. Strasser, D. Many, and X. Dimitropoulos. 2010. "SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics". In: *Proceedings of the 19th USENIX Security Symposium*. Washington, DC, USA: USENIX Association.

Calctopia, Inc. 2017. "SECCOMP — The Secure Spreadsheet". https://www.calctopia.com/.

Canetti, R. 2001. "Universally Composable Security: A New Paradigm for Cryptographic Protocols". In: *42nd Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press. 136–145.

Canetti, R., A. Cohen, and Y. Lindell. 2015. "A Simpler Variant of Universally Composable Security for Standard Multiparty Computation". In: *Advances in Cryptology – CRYPTO 2015, Part II*. Ed. by R. Gennaro and M. J. B. Robshaw. Vol. 9216. *Lecture Notes in Computer Science*. Springer, Heidelberg. 3–22. DOI: 10.1007/978-3-662-48000-7_1.

Canetti, R., O. Goldreich, and S. Halevi. 1998. "The Random Oracle Methodology, Revisited (Preliminary Version)". In: *30th Annual ACM Symposium on Theory of Computing*. ACM Press. 209–218.

Canetti, R., A. Jain, and A. Scafuro. 2014. "Practical UC security with a Global Random Oracle". In: *ACM CCS 14: 21st Conference on Computer and Communications Security*. Ed. by G.-J. Ahn, M. Yung, and N. Li. ACM Press. 597–608.

Carter, H., B. Mood, P. Traynor, and K. Butler. 2013. "Secure outsourced Garbled Circuit Evaluation for Mobile Devices". In: *22nd USENIX Security Symposium*. USENIX Association.

Carter, H., B. Mood, P. Traynor, and K. Butler. 2016. "Secure outsourced garbled circuit evaluation for mobile devices". *Journal of Computer Security*. 24(2): 137–180.

Cash, D., P. Grubbs, J. Perry, and T. Ristenpart. 2015. "Leakage-Abuse Attacks Against Searchable Encryption". In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 668–679.

Chan, T.-H. H., K.-M. Chung, B. Maggs, and E. Shi. 2017. "Foundations of Differentially Oblivious Algorithms". Cryptology ePrint Archive, Report 2017/1033. https://eprint.iacr.org/2017/1033.

Chandran, N., J. A. Garay, P. Mohassel, and S. Vusirikala. 2017. "Efficient, Constant-Round and Actively Secure MPC: Beyond the Three-Party Case". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 277–294.

Chase, M., D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, and G. Zaverucha. 2017. "Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 1825–1842.

Chaum, D. 1983. "Blind Signature System". In: *Advances in Cryptology – CRYPTO'83*. Ed. by D. Chaum. Plenum Press, New York, USA. 153.

Chaum, D., C. Crépeau, and I. Damgård. 1988. "Multiparty Unconditionally Secure Protocols (Extended Abstract)". In: *20th Annual ACM Symposium on Theory of Computing*. ACM Press. 11–19.

Chillotti, I., N. Gama, M. Georgieva, and M. Izabachène. 2016. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *Advances in Cryptology – ASIACRYPT 2016, Part I*. Ed. by J. H. Cheon and T. Takagi. Vol. 10031. *Lecture Notes in Computer Science*. Springer, Heidelberg. 3–33. DOI: 10.1007/978-3-662-53887-6_1.

Chillotti, I., N. Gama, M. Georgieva, and M. Izabachène. 2017. "Faster Packed Homomorphic Operations and Efficient Circuit Bootstrapping for TFHE". In: *Advances in Cryptology – ASIACRYPT 2017, Part I*. Ed. by T. Takagi and T. Peyrin. Vol. 10624. *Lecture Notes in Computer Science*. Springer, Heidelberg. 377–408.

Choi, S. G., K.-W. Hwang, J. Katz, T. Malkin, and D. Rubenstein. 2012a. "Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces". In: *Topics in Cryptology – CT-RSA 2012*. Ed. by O. Dunkelman. Vol. 7178. *Lecture Notes in Computer Science*. Springer, Heidelberg. 416–432.

Choi, S. G., J. Katz, R. Kumaresan, and H.-S. Zhou. 2012b. "On the Security of the "Free-XOR" Technique". In: *TCC 2012: 9th Theory of Cryptography Conference*. Ed. by R. Cramer. Vol. 7194. *Lecture Notes in Computer Science*. Springer, Heidelberg. 39–53.

Chor, B., O. Goldreich, E. Kushilevitz, and M. Sudan. 1995. "Private Information Retrieval". In: *36th Symposium on Foundations of Computer Science*. IEEE. 41–50.

Clarke, E., D. Kroening, and F. Lerda. 2004. "A tool for checking ANSI-C programs". In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer. 168–176.

Cleve, R. 1986. "Limits on the Security of Coin Flips when Half the Processors Are Faulty (Extended Abstract)". In: *18th Annual ACM Symposium on Theory of Computing*. ACM Press. 364–369.

Cybernetica. 2015. "Track Big Data Between Government and Education". https://sharemind.cyber.ee/big-data-analytics-protection/, retrieved March 9, 2018.

Damgård, I. and M. Jurik. 2001. "A generalisation, a simpli. cation and some applications of Paillier's probabilistic public-key system". In: *International Workshop on Public Key Cryptography*. 119–136.

Damgård, I., M. Keller, E. Larraia, C. Miles, and N. P. Smart. 2012a. "Implementing AES via an actively/covertly secure dishonest-majority MPC protocol". In: *International Conference on Security and Cryptography for Networks*. Springer. 241–263.

Damgård, I., J. B. Nielsen, M. Nielsen, and S. Ranellucci. 2017. "The TinyTable Protocol for 2-Party Secure Computation, or: Gate-Scrambling Revisited". In: *Advances in Cryptology – CRYPTO 2017, Part I*. Ed. by J. Katz and H. Shacham. Vol. 10401. *Lecture Notes in Computer Science*. Springer, Heidelberg. 167–187.

Damgård, I., V. Pastro, N. P. Smart, and S. Zakarias. 2012b. "Multiparty Computation from Somewhat Homomorphic Encryption". In: *Advances in Cryptology – CRYPTO 2012*. Ed. by R. Safavi-Naini and R. Canetti. Vol. 7417. *Lecture Notes in Computer Science*. Springer, Heidelberg. 643–662.

Damgård, I. and S. Zakarias. 2013. "Constant-Overhead Secure Computation of Boolean Circuits using Preprocessing". In: *TCC 2013: 10th Theory of Cryptography Conference*. Ed. by A. Sahai. Vol. 7785. *Lecture Notes in Computer Science*. Springer, Heidelberg. 621–641. DOI: 10.1007/978-3-642-36594-2_35.

D'Arco, P. and R. De Prisco. 2014. "Secure Two-Party Computation: A Visual Way". In: *ICITS 13: 7th International Conference on Information Theoretic Security*. Ed. by C. Padró. Vol. 8317. *Lecture Notes in Computer Science*. Springer, Heidelberg. 18–38. DOI: 10.1007/978-3-319-04268-8_2.

D'Arco, P. and R. De Prisco. 2016. "Secure computation without computers". 651(Sept.).

De Cristofaro, E., M. Manulis, and B. Poettering. 2013. "Private Discovery of Common Social Contacts". *International Journal of Information Security*. 12(1): 49–65.

Demmler, D., T. Schneider, and M. Zohner. 2015. "ABY - A Framework for Efficient Mixed-Protocol Secure Two-Party Computation". In: *ISOC Network and Distributed System Security Symposium – NDSS 2015*. The Internet Society.

Dessouky, G., F. Koushanfar, A.-R. Sadeghi, T. Schneider, S. Zeitouni, and M. Zohner. 2017. "Pushing the communication barrier in secure computation using lookup tables". In: *Network and Distributed System Security Symposium*.

Doerner, J., D. Evans, and A. Shelat. 2016. "Secure Stable Matching at Scale". In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 1602–1613.

Doerner, J. and A. Shelat. 2017. "Scaling ORAM for Secure Computation". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 523–535.

Dwork, C. and A. Roth. 2014. "The algorithmic foundations of differential privacy". *Foundations and Trends in Theoretical Computer Science*. 9(3–4): 211–407.

Ejgenberg, Y., M. Farbstein, M. Levy, and Y. Lindell. 2012. "SCAPI: The Secure Computation Application Programming Interface". Cryptology ePrint Archive, Report 2012/629. https://eprint.iacr.org/2012/629.

Faber, S., S. Jarecki, S. Kentros, and B. Wei. 2015. "Three-party ORAM for secure computation". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 360–385.

Fan, X., C. Ganesh, and V. Kolesnikov. 2017. "Hashing Garbled Circuits for Free". In: *Advances in Cryptology – EUROCRYPT 2017, Part II*. Ed. by J. Coron and J. B. Nielsen. Vol. 10211. *Lecture Notes in Computer Science*. Springer, Heidelberg. 456–485.

Fisch, B. A., B. Vo, F. Krell, A. Kumarasubramanian, V. Kolesnikov, T. Malkin, and S. M. Bellovin. 2015. "Malicious-Client Security in Blind Seer: A Scalable Private DBMS". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 395–410. DOI: 10.1109/SP.2015.31.

Fraser, C. W. and D. R. Hanson. 1995. *A retargetable C compiler: design and implementation*. Addison-Wesley Longman Publishing Co., Inc.

Frederiksen, T. K., T. P. Jakobsen, J. B. Nielsen, and R. Trifiletti. 2015. "TinyLEGO: An Interactive Garbling Scheme for Maliciously Secure Two-Party Computation". Cryptology ePrint Archive, Report 2015/309. https://eprint.iacr.org/2015/309.

Frederiksen, T. K., T. P. Jakobsen, J. B. Nielsen, P. S. Nordholt, and C. Orlandi. 2013. "MiniLEGO: Efficient Secure Two-Party Computation from General Assumptions". In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by T. Johansson and P. Q. Nguyen. Vol. 7881. *Lecture Notes in Computer Science*. Springer, Heidelberg. 537–556. DOI: 10.1007/978-3-642-38348-9_32.

Furukawa, J., Y. Lindell, A. Nof, and O. Weinstein. 2017. "High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority". In: *Advances in Cryptology – EUROCRYPT 2017, Part II*. Ed. by J. Coron and J. B. Nielsen. Vol. 10211. *Lecture Notes in Computer Science*. Springer, Heidelberg. 225–255.

Gallagher, B., D. Lo, P. F. Frandsen, J. B. Nielsen, and K. Nielsen. 2017. "Insights Network – A Blockchain Data Exchange". https://s3.amazonaws.com/insightsnetwork/InsightsNetworkWhitepaperV0.5.pdf.

Gascón, A., P. Schoppmann, B. Balle, M. Raykova, J. Doerner, S. Zahur, and D. Evans. 2017. "Privacy-Preserving Distributed Linear Regression on High-Dimensional Data". *Proceedings on Privacy Enhancing Technologies*. 2017(4): 248–267.

Gentry, C. 2009. "Fully homomorphic encryption using ideal lattices". In: *41st ACM Symposium on Theory of Computing*.

Gentry, C. and S. Halevi. 2011. "Implementing Gentry's Fully-Homomorphic Encryption Scheme". In: *Advances in Cryptology – EUROCRYPT 2011*. Ed. by K. G. Paterson. Vol. 6632. *Lecture Notes in Computer Science*. Springer, Heidelberg. 129–148.

Giacomelli, I., J. Madsen, and C. Orlandi. 2016. "ZKBoo: Faster Zero-Knowledge for Boolean Circuits". In: *25th USENIX Security Symposium*. Austin, TX: USENIX Association. 1069–1083.

Gilboa, N. and Y. Ishai. 2014. "Distributed Point Functions and Their Applications". In: *Advances in Cryptology – EUROCRYPT 2014*. Ed. by P. Q. Nguyen and E. Oswald. Vol. 8441. *Lecture Notes in Computer Science*. Springer, Heidelberg. 640–658. DOI: 10.1007/978-3-642-55220-5_35.

Goldreich, O. 2004. *Foundations of Cryptography: Volume 2*. Cambridge University Press.

Goldreich, O., S. Micali, and A. Wigderson. 1987. "How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority". In: *19th Annual ACM Symposium on Theory of Computing*. Ed. by A. Aho. ACM Press. 218–229.

Goldreich, O. and R. Ostrovsky. 1996. "Software Protection and Simulation on Oblivious RAMs". *Journal of the ACM*. 43(3).

Goldwasser, S. and S. Micali. 1984. "Probabilistic Encryption". *Journal of Computer and System Sciences*. 28(2): 270–299.

Goldwasser, S., S. Micali, and C. Rackoff. 1985. "The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract)". In: *17th Annual ACM Symposium on Theory of Computing*. ACM Press. 291–304.

Gordon, S. D., C. Hazay, J. Katz, and Y. Lindell. 2008. "Complete fairness in secure two-party computation". In: *40th Annual ACM Symposium on Theory of Computing*. Ed. by R. E. Ladner and C. Dwork. ACM Press. 413–422.

Gordon, S. D., J. Katz, V. Kolesnikov, F. Krell, T. Malkin, M. Raykova, and Y. Vahlis. 2012. "Secure two-party computation in sublinear (amortized) time". In: *ACM CCS 12: 19th Conference on Computer and Communications Security*. Ed. by T. Yu, G. Danezis, and V. D. Gligor. ACM Press. 513–524.

Goyal, V., Y. Ishai, A. Sahai, R. Venkatesan, and A. Wadia. 2010. "Founding Cryptography on Tamper-Proof Hardware Tokens". In: *TCC 2010: 7th Theory of Cryptography Conference*. Ed. by D. Micciancio. Vol. 5978. *Lecture Notes in Computer Science*. Springer, Heidelberg. 308–326.

Goyal, V., P. Mohassel, and A. Smith. 2008. "Efficient Two Party and Multi Party Computation Against Covert Adversaries". In: *Advances in Cryptology – EUROCRYPT 2008*. Ed. by N. P. Smart. Vol. 4965. *Lecture Notes in Computer Science*. Springer, Heidelberg. 289–306.

Gueron, S., Y. Lindell, A. Nof, and B. Pinkas. 2015. "Fast Garbling of Circuits Under Standard Assumptions". In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 567–578.

Gupta, D., B. Mood, J. Feigenbaum, K. Butler, and P. Traynor. 2016. "Using Intel Software Guard Extensions for efficient two-party secure function evaluation". In: *International Conference on Financial Cryptography and Data Security*. Springer. 302–318.

Gupta, T., H. Fingler, L. Alvisi, and M. Walfish. 2017. "Pretzel: Email encryption and provider-supplied functions are compatible". In: *Proceedings of the Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)*. ACM. 169–182.

Halevi, S. and V. Shoup. 2014. "Bootstrapping for HElib". Cryptology ePrint Archive, Report 2014/873. https://eprint.iacr.org/2014/873.

Hazay, C. and Y. Lindell. 2008. "Constructions of truly practical secure protocols using standardsmartcards". In: *ACM CCS 08: 15th Conference on Computer and Communications Security*. Ed. by P. Ning, P. F. Syverson, and S. Jha. ACM Press. 491–500.

He, X., A. Machanavajjhala, C. J. Flynn, and D. Srivastava. 2017. "Composing Differential Privacy and Secure Computation: A Case Study on Scaling Private Record Linkage". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 1389–1406.

Henecka, W., S. Kögl, A.-R. Sadeghi, T. Schneider, and I. Wehrenberg. 2010. "TASTY: tool for automating secure two-party computations". In: *ACM CCS 10: 17th Conference on Computer and Communications Security*. Ed. by E. Al-Shaer, A. D. Keromytis, and V. Shmatikov. ACM Press. 451–462.

Hofheinz, D. and V. Shoup. 2011. "GNUC: A New Universal Composability Framework". Cryptology ePrint Archive, Report 2011/303. http://eprint.iacr.org/2011/303.

Holzer, A., M. Franz, S. Katzenbeisser, and H. Veith. 2012. "Secure two-party computations in ANSI C". In: *ACM CCS 12: 19th Conference on Computer and Communications Security*. Ed. by T. Yu, G. Danezis, and V. D. Gligor. ACM Press. 772–783.

Huang, Y., P. Chapman, and D. Evans. 2011a. "Privacy-Preserving Applications on Smartphones". In: *6th USENIX Workshop on Hot Topics in Security*.

Huang, Y., D. Evans, and J. Katz. 2012a. "Private Set Intersection: Are Garbled Circuits Better than Custom Protocols?" In: *ISOC Network and Distributed System Security Symposium – NDSS 2012*. The Internet Society.

Huang, Y., D. Evans, J. Katz, and L. Malka. 2011b. "Faster Secure Two-Party Computation Using Garbled Circuits". In: *20th USENIX Security Symposium*.

Huang, Y., J. Katz, and D. Evans. 2012b. "Quid-Pro-Quo-tocols: Strengthening Semi-honest Protocols with Dual Execution". In: *2012 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 272–284.

Huang, Y., J. Katz, V. Kolesnikov, R. Kumaresan, and A. J. Malozemoff. 2014. "Amortizing Garbled Circuits". In: *Advances in Cryptology – CRYPTO 2014, Part II*. Ed. by J. A. Garay and R. Gennaro. Vol. 8617. *Lecture Notes in Computer Science*. Springer, Heidelberg. 458–475. DOI: 10.1007/978-3-662-44381-1_26.

Huang, Y., L. Malka, D. Evans, and J. Katz. 2011c. "Efficient Privacy-Preserving Biometric Identification". In: *ISOC Network and Distributed System Security Symposium – NDSS 2011*. The Internet Society.

Husted, N., S. Myers, A. Shelat, and P. Grubbs. 2013. "GPU and CPU parallelization of honest-but-curious secure two-party computation". In: *Proceedings of the 29th Annual Computer Security Applications Conference*. ACM. 169–178.

Impagliazzo, R. and S. Rudich. 1989. "Limits on the Provable Consequences of One-Way Permutations". In: *21st Annual ACM Symposium on Theory of Computing*. ACM Press. 44–61.

Ishai, Y., J. Kilian, K. Nissim, and E. Petrank. 2003. "Extending Oblivious Transfers Efficiently". In: *Advances in Cryptology – CRYPTO 2003*. Ed. by D. Boneh. Vol. 2729. *Lecture Notes in Computer Science*. Springer, Heidelberg. 145–161.

Ishai, Y., E. Kushilevitz, R. Ostrovsky, and A. Sahai. 2007. "Zero-knowledge from secure multiparty computation". In: *39th Annual ACM Symposium on Theory of Computing*. Ed. by D. S. Johnson and U. Feige. ACM Press. 21–30.

Ishai, Y., M. Prabhakaran, and A. Sahai. 2008. "Founding Cryptography on Oblivious Transfer - Efficiently". In: *Advances in Cryptology – CRYPTO 2008*. Ed. by D. Wagner. Vol. 5157. *Lecture Notes in Computer Science*. Springer, Heidelberg. 572–591.

Islam, M. S., M. Kuzu, and M. Kantarcioglu. 2012. "Access Pattern disclosure on Searchable Encryption: Ramification, Attack and Mitigation". In: *ISOC Network and Distributed System Security Symposium – NDSS 2012*. The Internet Society.

Jagadeesh, K., D. Wu, J. Birgmeier, D. Boneh, and G. Bejerano. 2017. "Deriving Genomic Diagnoses Without Revealing Patient Genomes". *Science*. 357(6352): 692–695.

Jakobsen, T. P., J. B. Nielsen, and C. Orlandi. 2016. "A Framework for Outsourcing of Secure Computation". Cryptology ePrint Archive, Report 2016/037. https://eprint.iacr.org/2016/037 (subsumes earlier version published in 6th ACM Workshop on Cloud Computing Security).

Jarecki, S. and V. Shmatikov. 2007. "Efficient Two-Party Secure Computation on Committed Inputs". In: *Advances in Cryptology – EUROCRYPT 2007*. Ed. by M. Naor. Vol. 4515. *Lecture Notes in Computer Science*. Springer, Heidelberg. 97–114.

Jawurek, M., F. Kerschbaum, and C. Orlandi. 2013. "Zero-knowledge using garbled circuits: how to prove non-algebraic statements efficiently". In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 955–966.

Juma, A. and Y. Vahlis. 2010. "Protecting Cryptographic Keys against Continual Leakage". In: *Advances in Cryptology – CRYPTO 2010*. Ed. by T. Rabin. Vol. 6223. *Lecture Notes in Computer Science*. Springer, Heidelberg. 41–58.

Kairouz, P., S. Oh, and P. Viswanath. 2015. "Secure multi-party differential privacy". In: *Advances in Neural Information Processing Systems*. 2008–2016.

Kamara, S., P. Mohassel, M. Raykova, and S. S. Sadeghian. 2014. "Scaling Private Set Intersection to Billion-Element Sets". In: *FC 2014: 18th International Conference on Financial Cryptography and Data Security*. Ed. by N. Christin and R. Safavi-Naini. Vol. 8437. *Lecture Notes in Computer Science*. Springer, Heidelberg. 195–215. DOI: 10.1007/978-3-662-45472-5_13.

Kamara, S., P. Mohassel, and B. Riva. 2012. "Salus: a system for server-aided secure function evaluation". In: *ACM CCS 12: 19th Conference on Computer and Communications Security*. Ed. by T. Yu, G. Danezis, and V. D. Gligor. ACM Press. 797–808.

Katz, J. 2007. "Universally Composable Multi-party Computation Using Tamper-Proof Hardware". In: *Advances in Cryptology – EUROCRYPT 2007*. Ed. by M. Naor. Vol. 4515. *Lecture Notes in Computer Science*. Springer, Heidelberg. 115–128.

Katz, J., V. Kolesnikov, and X. Wang. 2018. "Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures". Cryptology ePrint Archive, Report 2018/475. https://eprint.iacr.org/2018/475.

Keller, M., E. Orsini, and P. Scholl. 2015. "Actively Secure OT Extension with Optimal Overhead". In: *Advances in Cryptology – CRYPTO 2015, Part I*. Ed. by R. Gennaro and M. J. B. Robshaw. Vol. 9215. *Lecture Notes in Computer Science*. Springer, Heidelberg. 724–741. DOI: 10.1007/978-3-662-47989-6_35.

Keller, M., E. Orsini, and P. Scholl. 2016. "MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer". In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 830–842.

Keller, M., V. Pastro, and D. Rotaru. 2018. "Overdrive: making SPDZ great again". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 158–189.

Keller, M. and P. Scholl. 2014. "Efficient, oblivious data structures for MPC". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 506–525.

Kempka, C., R. Kikuchi, and K. Suzuki. 2016. "How to circumvent the two-ciphertext lower bound for linear garbling schemes". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 967–997.

Kennedy, W. S., V. Kolesnikov, and G. T. Wilfong. 2017. "Overlaying Conditional Circuit Clauses for Secure Computation". In: *Advances in Cryptology – ASIACRYPT 2017, Part II*. Ed. by T. Takagi and T. Peyrin. Vol. 10625. *Lecture Notes in Computer Science*. Springer, Heidelberg. 499–528.

Kerschbaum, F., T. Schneider, and A. Schröpfer. 2014. "Automatic Protocol Selection in Secure Two-Party Computations". In: *ACNS 14: 12th International Conference on Applied Cryptography and Network Security*. Ed. by I. Boureanu, P. Owesarski, and S. Vaudenay. Vol. 8479. *Lecture Notes in Computer Science*. Springer, Heidelberg. 566–584. DOI: 10.1007/978-3-319-07536-5_33.

Kilian, J. 1988. "Founding Cryptography on Oblivious Transfer". In: *20th Annual ACM Symposium on Theory of Computing*. ACM Press. 20–31.

Kiraz, M. and B. Schoenmakers. 2006. "A protocol issue for the malicious case of Yao's garbled circuit construction". In: *27th Symposium on Information Theory in the Benelux*. 283–290.

Knudsen, L. R. and V. Rijmen. 2007. "Known-Key Distinguishers for Some Block Ciphers". In: *Advances in Cryptology – ASIACRYPT 2007*. Ed. by K. Kurosawa. Vol. 4833. *Lecture Notes in Computer Science*. Springer, Heidelberg. 315–324.

Kolesnikov, V. 2005. "Gate Evaluation Secret Sharing and Secure One-Round Two-Party Computation". In: *Advances in Cryptology – ASIACRYPT 2005*. Ed. by B. K. Roy. Vol. 3788. *Lecture Notes in Computer Science*. Springer, Heidelberg. 136–155.

Kolesnikov, V. 2006. "Secure Two-party Computation and Communication". University of Toronto Ph.D. Thesis.

Kolesnikov, V. 2010. "Truly Efficient String Oblivious Transfer Using Resettable Tamper-Proof Tokens". In: *TCC 2010: 7th Theory of Cryptography Conference*. Ed. by D. Micciancio. Vol. 5978. *Lecture Notes in Computer Science*. Springer, Heidelberg. 327–342.

Kolesnikov, V. and R. Kumaresan. 2013. "Improved OT Extension for Transferring Short Secrets". In: *Advances in Cryptology – CRYPTO 2013, Part II*. Ed. by R. Canetti and J. A. Garay. Vol. 8043. *Lecture Notes in Computer Science*. Springer, Heidelberg. 54–70. DOI: 10.1007/978-3-642-40084-1_4.

Kolesnikov, V., R. Kumaresan, M. Rosulek, and N. Trieu. 2016. "Efficient Batched Oblivious PRF with Applications to Private Set Intersection". In: *ACM CCS 16: 23rd Conference on Computer and Communications Security*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press. 818–829.

Kolesnikov, V. and A. J. Malozemoff. 2015. "Public Verifiability in the Covert Model (Almost) for Free". In: *Advances in Cryptology – ASIACRYPT 2015, Part II*. Ed. by T. Iwata and J. H. Cheon. Vol. 9453. *Lecture Notes in Computer Science*. Springer, Heidelberg. 210–235. DOI: 10.1007/978-3-662-48800-3_9.

Kolesnikov, V., N. Matania, B. Pinkas, M. Rosulek, and N. Trieu. 2017a. "Practical Multi-party Private Set Intersection from Symmetric-Key Techniques". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 1257–1272.

Kolesnikov, V., P. Mohassel, B. Riva, and M. Rosulek. 2015. "Richer Efficiency/Security Trade-offs in 2PC". In: *TCC 2015: 12th Theory of Cryptography Conference, Part I*. Ed. by Y. Dodis and J. B. Nielsen. Vol. 9014. *Lecture Notes in Computer Science*. Springer, Heidelberg. 229–259. DOI: 10.1007/978-3-662-46494-6_11.

Kolesnikov, V., P. Mohassel, and M. Rosulek. 2014. "FleXOR: Flexible Garbling for XOR Gates That Beats Free-XOR". In: *Advances in Cryptology – CRYPTO 2014, Part II*. Ed. by J. A. Garay and R. Gennaro. Vol. 8617. *Lecture Notes in Computer Science*. Springer, Heidelberg. 440–457. DOI: 10.1007/978-3-662-44381-1_25.

Kolesnikov, V., J. B. Nielsen, M. Rosulek, N. Trieu, and R. Trifiletti. 2017b. "DUPLO: Unifying Cut-and-Choose for Garbled Circuits". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 3–20.

Kolesnikov, V., A.-R. Sadeghi, and T. Schneider. 2009. "Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima". In: *CANS 09: 8th International Conference on Cryptology and Network Security*. Ed. by J. A. Garay, A. Miyaji, and A. Otsuka. Vol. 5888. *Lecture Notes in Computer Science*. Springer, Heidelberg. 1–20.

Kolesnikov, V., A.-R. Sadeghi, and T. Schneider. 2010. "From Dust to Dawn: Practically Efficient Two-Party Secure Function Evaluation Protocols and their Modular Design". https://eprint.iacr.org/2010/079.

Kolesnikov, V., A.-R. Sadeghi, and T. Schneider. 2013. "A Systematic Approach to Practically Efficient General Two-party Secure Function Evaluation Protocols and Their Modular Design". *J. Comput. Secur.* 21(2): 283–315. ISSN: 0926-227X. URL: http://dl.acm.org/citation.cfm?id=2590614.2590617.

Kolesnikov, V. and T. Schneider. 2008a. "A Practical Universal Circuit Construction and Secure Evaluation of Private Functions". In: *FC 2008: 12th International Conference on Financial Cryptography and Data Security*. Ed. by G. Tsudik. Vol. 5143. *Lecture Notes in Computer Science*. Springer, Heidelberg. 83–97.

Kolesnikov, V. and T. Schneider. 2008b. "Improved Garbled Circuit: Free XOR Gates and Applications". In: *ICALP 2008: 35th International Colloquium on Automata, Languages and Programming, Part II*. Ed. by L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz. Vol. 5126. *Lecture Notes in Computer Science*. Springer, Heidelberg. 486–498.

Kreuter, B. 2017. "Secure MPC at Google". Real World Crypto.

Kreuter, B., a. shelat abhi, B. Mood, and K. Butler. 2013. "PCF: A Portable Circuit Format for Scalable Two-Party Secure Computation." In: *USENIX Security Symposium*. 321–336.

Küsters, R., T. Truderung, and A. Vogt. 2012. "A game-based definition of coercion resistance and its applications". *Journal of Computer Security*. 20(6): 709–764.

Launchbury, J., I. S. Diatchki, T. DuBuisson, and A. Adams-Moran. 2012. "Efficient lookup-table protocol in secure multiparty computation". In: *ACM SIGPLAN Notices*. Vol. 47. No. 9. ACM. 189–200.

Lee, J., J. Jang, Y. Jang, N. Kwak, Y. Choi, C. Choi, T. Kim, M. Peinado, and B. B. Kang. 2017a. "Hacking in Darkness: Return-oriented Programming Against Secure Enclaves". In: *Proceedings of the 26th USENIX Conference on Security Symposium. SEC'17*. Vancouver, BC, Canada: USENIX Association. 523–539. ISBN: 978-1-931971-40-9. URL: http://dl.acm.org/citation.cfm?id=3241189.3241231.

Lee, S., M.-W. Shih, P. Gera, T. Kim, H. Kim, and M. Peinado. 2017b. "Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing". In: *Proceedings of the 26th USENIX Conference on Security Symposium. SEC'17*. Vancouver, BC, Canada: USENIX Association. 557–574. ISBN: 978-1-931971-40-9. URL: http://dl.acm.org/citation.cfm?id=3241189.3241233.

Li, M., S. Yu, N. Cao, and W. Lou. 2013. "Privacy-preserving distributed profile matching in proximity-based mobile social networks". *IEEE Transactions on Wireless Communications*. 12(5): 2024–2033.

Lindell, Y. 2013. "Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries". In: *Advances in Cryptology – CRYPTO 2013, Part II*. Ed. by R. Canetti and J. A. Garay. Vol. 8043. *Lecture Notes in Computer Science*. Springer, Heidelberg. 1–17. DOI: 10.1007/978-3-642-40084-1_1.

Lindell, Y. and B. Pinkas. 2007. "An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries". In: *Advances in Cryptology – EUROCRYPT 2007*. Ed. by M. Naor. Vol. 4515. *Lecture Notes in Computer Science*. Springer, Heidelberg. 52–78.

Lindell, Y. and B. Pinkas. 2009. "A Proof of Security of Yao's Protocol for Two-Party Computation". *Journal of Cryptology*. 22(2): 161–188.

Lindell, Y. and B. Pinkas. 2011. "Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer". In: *TCC 2011: 8th Theory of Cryptography Conference*. Ed. by Y. Ishai. Vol. 6597. *Lecture Notes in Computer Science*. Springer, Heidelberg. 329–346.

Lindell, Y., B. Pinkas, and N. P. Smart. 2008. "Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries". In: *SCN 08: 6th International Conference on Security in Communication Networks*. Ed. by R. Ostrovsky, R. D. Prisco, and I. Visconti. Vol. 5229. *Lecture Notes in Computer Science*. Springer, Heidelberg. 2–20.

Lindell, Y. and B. Riva. 2014. "Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings". In: *Advances in Cryptology – CRYPTO 2014, Part II*. Ed. by J. A. Garay and R. Gennaro. Vol. 8617. *Lecture Notes in Computer Science*. Springer, Heidelberg. 476–494. DOI: 10.1007/978-3-662-44381-1_27.

Lindell, Y. and B. Riva. 2015. "Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries". In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 579–590.

Liu, J., M. Juuti, Y. Lu, and N. Asokan. 2017. "Oblivious Neural Network Predictions via MiniONN Transformations". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 619–631.

López-Alt, A., E. Tromer, and V. Vaikuntanathan. 2012. "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption". In: *44th Annual ACM Symposium on Theory of Computing*. ACM. 1219–1234.

Lu, S. and R. Ostrovsky. 2013. "How to Garble RAM Programs". In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by T. Johansson and P. Q. Nguyen. Vol. 7881. *Lecture Notes in Computer Science*. Springer, Heidelberg. 719–734. DOI: 10.1007/978-3-642-38348-9_42.

Malkhi, D., N. Nisan, B. Pinkas, and Y. Sella. 2004. "Fairplay-Secure Two-Party Computation System". In: *USENIX Security Symposium*.

Marlinspike, M. 2017. "Technology preview: Private contact discovery for Signal". https://signal.org/blog/private-contact-discovery/.

Micali, S. and L. Reyzin. 2004. "Physically Observable Cryptography (Extended Abstract)". In: *TCC 2004: 1st Theory of Cryptography Conference*. Ed. by M. Naor. Vol. 2951. *Lecture Notes in Computer Science*. Springer, Heidelberg. 278–296.

Mishra, P., R. Poddar, J. Chen, A. Chiesa, and R. A. Popa. 2018. "Oblix: An Efficient Oblivious Search Index". In: *2018 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press.

Mohassel, P. and M. Franklin. 2006. "Efficiency Tradeoffs for Malicious Two-Party Computation". In: *PKC 2006: 9th International Conference on Theory and Practice of Public Key Cryptography*. Ed. by M. Yung, Y. Dodis, A. Kiayias, and T. Malkin. Vol. 3958. *Lecture Notes in Computer Science*. Springer, Heidelberg. 458–473.

Mohassel, P. and B. Riva. 2013. "Garbled Circuits Checking Garbled Circuits: More Efficient and Secure Two-Party Computation". In: *Advances in Cryptology – CRYPTO 2013, Part II*. Ed. by R. Canetti and J. A. Garay. Vol. 8043. *Lecture Notes in Computer Science*. Springer, Heidelberg. 36–53. DOI: 10.1007/978-3-642-40084-1_3.

Mohassel, P., M. Rosulek, and Y. Zhang. 2015. "Fast and Secure Three-party Computation: The Garbled Circuit Approach". In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 591–602.

Mohassel, P. and Y. Zhang. 2017. "SecureML: A System for Scalable Privacy-Preserving Machine Learning". In: *2017 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 19–38.

Mood, B., D. Gupta, H. Carter, K. Butler, and P. Traynor. 2016. "Frigate: A validated, extensible, and efficient compiler and interpreter for secure computation". In: *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. 112–127.

Mukherjee, P. and D. Wichs. 2016. "Two round multiparty computation via multi-key FHE". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EuroCrypt)*. Springer. 735–763.

Naccache, D. and J. Stern. 1998. "A New Public Key Cryptosystem Based on Higher Residues". In: *ACM CCS 98: 5th Conference on Computer and Communications Security*. ACM Press. 59–66.

Naor, M., B. Pinkas, and R. Sumner. 1999. "Privacy Preserving Auctions and Mechanism Design". In: *1st ACM Conference on Electronic Commerce*.

Naveed, M., S. Kamara, and C. V. Wright. 2015. "Inference Attacks on Property-Preserving Encrypted Databases". In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 644–655.

Nielsen, J. B., P. S. Nordholt, C. Orlandi, and S. S. Burra. 2012. "A New Approach to Practical Active-Secure Two-Party Computation". In: *Advances in Cryptology – CRYPTO 2012*. Ed. by R. Safavi-Naini and R. Canetti. Vol. 7417. *Lecture Notes in Computer Science*. Springer, Heidelberg. 681–700.

Nielsen, J. B. and C. Orlandi. 2009. "LEGO for Two-Party Secure Computation". In: *TCC 2009: 6th Theory of Cryptography Conference*. Ed. by O. Reingold. Vol. 5444. *Lecture Notes in Computer Science*. Springer, Heidelberg. 368–386.

Nikolaenko, V., S. Ioannidis, U. Weinsberg, M. Joye, N. Taft, and D. Boneh. 2013a. "Privacy-preserving matrix factorization". In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 801–812.

Nikolaenko, V., U. Weinsberg, S. Ioannidis, M. Joye, D. Boneh, and N. Taft. 2013b. "Privacy-Preserving Ridge Regression on Hundreds of Millions of Records". In: *2013 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 334–348.

Ohrimenko, O., F. Schuster, C. Fournet, A. Mehta, S. Nowozin, K. Vaswani, and M. Costa. 2016. "Oblivious Multi-Party Machine Learning on Trusted Processors." In: *USENIX Security Symposium*. 619–636.

Ostrovsky, R. and V. Shoup. 1997. "Private Information Storage". In: *ACM Symposium on Theory of Computing*.

Pagh, R. and F. F. Rodler. 2004. “Cuckoo hashing”. *J. Algorithms*. 51(2): 122–144. DOI: 10.1016/j.jalgor.2003.12.002.

Paillier, P. 1999. “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes”. In: *Advances in Cryptology – EUROCRYPT’99*. Ed. by J. Stern. Vol. 1592. *Lecture Notes in Computer Science*. Springer, Heidelberg. 223–238.

Pappas, V., F. Krell, B. Vo, V. Kolesnikov, T. Malkin, S. G. Choi, W. George, A. D. Keromytis, and S. Bellovin. 2014. “Blind Seer: A Scalable Private DBMS”. In: *2014 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 359–374. DOI: 10.1109/SP.2014.30.

Patra, A. and D. Ravi. 2018. “On the Exact Round Complexity of Secure Three-Party Computation”. In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference*. Ed. by H. Shacham and A. Boldyreva. Vol. 10992. *Lecture Notes in Computer Science*. Springer. 425–458. DOI: 10.1007/978-3-319-96881-0.

Peikert, C., V. Vaikuntanathan, and B. Waters. 2008. “A Framework for Efficient and Composable Oblivious Transfer”. In: *Advances in Cryptology – CRYPTO 2008*. Ed. by D. Wagner. Vol. 5157. *Lecture Notes in Computer Science*. Springer, Heidelberg. 554–571.

Pettai, M. and P. Laud. 2015. “Combining differential privacy and secure multiparty computation”. In: *31st Annual Computer Security Applications Conference*. ACM. 421–430.

Pfitzmann, B. and M. Waidner. 2000. “Composition and Integrity Preservation of Secure Reactive Systems”. In: *ACM CCS 00: 7th Conference on Computer and Communications Security*. Ed. by S. Jajodia and P. Samarati. ACM Press. 245–254.

Pinkas, B., T. Schneider, G. Segev, and M. Zohner. 2015. “Phasing: Private Set Intersection Using Permutation-based Hashing”. In: *24th USENIX Security Symposium*. Ed. by J. Jung and T. Holz. USENIX Association. 515–530. URL: https://www.usenix.org/conference/usenixsecurity15.

Pinkas, B., T. Schneider, N. P. Smart, and S. C. Williams. 2009. “Secure Two-Party Computation Is Practical”. In: *Advances in Cryptology – ASIACRYPT 2009*. Ed. by M. Matsui. Vol. 5912. *Lecture Notes in Computer Science*. Springer, Heidelberg. 250–267.

Pippenger, N. and M. J. Fischer. 1979. "Relations among Complexity Measures". *Journal of the ACM*. 26(2).

Poddar, R., T. Boelter, and R. A. Popa. 2016. "Arx: A strongly encrypted database system." *IACR Cryptology ePrint Archive*. 2016: 591.

Priebe, C., K. Vaswani, and M. Costa. 2018. "EnclaveDB: A Secure Database using SGX". In: *2018 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press.

Rastogi, A., M. A. Hammer, and M. Hicks. 2014. "Wysteria: A Programming Language for Generic, Mixed-Mode Multiparty Computations". In: *2014 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 655–670. DOI: 10.1109/SP.2014.48.

Rivest, R. L., L. Adleman, and M. L. Dertouzos. 1978. "On Data Banks and Privacy Homomorphisms". In: *Foundations of Secure Computation*.

Rogaway, P. 1991. "The Round Complexity of Secure Protocols". Massachusetts Institute of Technology Ph.D. Thesis.

Sadeghi, A.-R., T. Schneider, and I. Wehrenberg. 2010. "Efficient Privacy-Preserving Face Recognition". In: *ICISC 09: 12th International Conference on Information Security and Cryptology*. Ed. by D. Lee and S. Hong. Vol. 5984. *Lecture Notes in Computer Science*. Springer, Heidelberg. 229–244.

Schneider, T. and M. Zohner. 2013. "GMW vs. Yao? Efficient Secure Two-Party Computation with Low Depth Circuits". In: *FC 2013: 17th International Conference on Financial Cryptography and Data Security*. Ed. by A.-R. Sadeghi. Vol. 7859. *Lecture Notes in Computer Science*. Springer, Heidelberg. 275–292. DOI: 10.1007/978-3-642-39884-1_23.

Shamir, A. 1979. "How to share a secret". *Communications of the ACM*. 22(11): 612–613.

Shan, Z., K. Ren, M. Blanton, and C. Wang. 2017. "Practical Secure Computation Outsourcing: A Survey". *ACM Computing Surveys*.

Shannon, C. E. 1937. "A symbolic analysis of relay and switching circuits". Massachusetts Institute of Technology Master's Thesis.

Shaon, F., M. Kantarcioglu, Z. Lin, and L. Khan. 2017. "SGX-BigMatrix: A Practical Encrypted Data Analytic Framework With Trusted Processors". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 1211–1228.

shelat, a. and C.-H. Shen. 2011. "Two-Output Secure Computation with Malicious Adversaries". In: *Advances in Cryptology – EUROCRYPT 2011*. Ed. by K. G. Paterson. Vol. 6632. *Lecture Notes in Computer Science*. Springer, Heidelberg. 386–405.

shelat, a. and C.-H. Shen. 2013. "Fast two-party secure computation with minimal assumptions". In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 523–534.

Shi, E., T.-H. H. Chan, E. Stefanov, and M. Li. 2011. "Oblivious RAM with $O((\log N)^3)$ Worst-Case Cost". In: *Advances in Cryptology – ASIACRYPT 2011*. Ed. by D. H. Lee and X. Wang. Vol. 7073. *Lecture Notes in Computer Science*. Springer, Heidelberg. 197–214.

Songhori, E. M., S. U. Hussain, A.-R. Sadeghi, T. Schneider, and F. Koushanfar. 2015. "TinyGarble: Highly Compressed and Scalable Sequential Garbled Circuits". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 411–428. DOI: 10.1109/SP.2015.32.

Stefanov, E., M. van Dijk, E. Shi, C. W. Fletcher, L. Ren, X. Yu, and S. Devadas. 2013. "Path ORAM: an extremely simple oblivious RAM protocol". In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 299–310.

Unbound Tech. 2018. "How to Control Your Own Keys (CYOK) in the Cloud". White Paper available from https://www.unboundtech.com.

Wagh, S., P. Cuff, and P. Mittal. 2018. "Differentially Private Oblivious RAM". *Proceedings on Privacy Enhancing Technologies*. 2018(4): 64–84.

Waksman, A. 1968. "A Permutation Network". *Journal of the ACM*. 15(1).

Wang, X. S., Y. Huang, T.-H. H. Chan, A. Shelat, and E. Shi. 2014a. "SCORAM: Oblivious RAM for Secure Computation". In: *ACM CCS 14: 21st Conference on Computer and Communications Security*. Ed. by G.-J. Ahn, M. Yung, and N. Li. ACM Press. 191–202.

Wang, X. S., Y. Huang, Y. Zhao, H. Tang, X. Wang, and D. Bu. 2015a. "Efficient Genome-Wide, Privacy-Preserving Similar Patient Query based on Private Edit Distance". In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 492–503.

Wang, X. S., K. Nayak, C. Liu, T.-H. H. Chan, E. Shi, E. Stefanov, and Y. Huang. 2014b. "Oblivious Data Structures". In: *ACM CCS 14: 21st Conference on Computer and Communications Security*. Ed. by G.-J. Ahn, M. Yung, and N. Li. ACM Press. 215–226.

Wang, X., T.-H. H. Chan, and E. Shi. 2015b. "Circuit ORAM: On Tightness of the Goldreich-Ostrovsky Lower Bound". In: *ACM CCS 15: 22nd Conference on Computer and Communications Security*. Ed. by I. Ray, N. Li, and C. Kruegel: ACM Press. 850–861.

Wang, X., A. J. Malozemoff, and J. Katz. 2017a. "EMP-toolkit: Efficient MultiParty computation toolkit". https://github.com/emp-toolkit.

Wang, X., S. Ranellucci, and J. Katz. 2017b. "Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 21–37.

Wang, X., S. Ranellucci, and J. Katz. 2017c. "Global-Scale Secure Multiparty Computation". In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 39–56.

Winternitz, R. S. 1984. "A Secure One-Way Hash Function Built from DES". In: *IEEE Symposium on Security and Privacy*. 88–88.

Wyden, R. 2017. "S.2169 — Student Right to Know Before You Go Act of 2017". https://www.congress.gov/bill/115th-congress/senate-bill/2169/.

Xu, Y., W. Cui, and M. Peinado. 2015. "Controlled-Channel Attacks: Deterministic Side Channels for Untrusted Operating Systems". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 640–656. DOI: 10.1109/SP.2015.45.

Yao, A. C.-C. 1982. "Protocols for Secure Computations (Extended Abstract)". In: *23rd Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press. 160–164.

Zahur, S. and D. Evans. 2013. “Circuit Structures for Improving Efficiency of Security and Privacy Tools”. In: *2013 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 493–507.

Zahur, S. and D. Evans. 2015. “Obliv-C: A Lightweight Compiler for Data-Oblivious Computation”. Cryptology ePrint Archive, Report 2015/1153. http://oblivc.org.

Zahur, S., M. Rosulek, and D. Evans. 2015. “Two Halves Make a Whole - Reducing Data Transfer in Garbled Circuits Using Half Gates”. In: *Advances in Cryptology – EUROCRYPT 2015, Part II*. Ed. by E. Oswald and M. Fischlin. Vol. 9057. *Lecture Notes in Computer Science*. Springer, Heidelberg. 220–250. DOI: 10.1007/978-3-662-46803-6_8.

Zahur, S., X. S. Wang, M. Raykova, A. Gascón, J. Doerner, D. Evans, and J. Katz. 2016. “Revisiting Square-Root ORAM: Efficient Random Access in Multi-party Computation”. In: *2016 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press. 218–234. DOI: 10.1109/SP.2016.21.

Zhang, Y., A. Steele, and M. Blanton. 2013. “PICCO: a general-purpose compiler for private distributed computation”. In: *ACM CCS 13: 20th Conference on Computer and Communications Security*. Ed. by A.-R. Sadeghi, V. D. Gligor, and M. Yung. ACM Press. 813–826.

Zheng, W., A. Dave, J. G. Beekman, R. A. Popa, J. E. Gonzalez, and I. Stoica. 2017. “Opaque: An Oblivious and Encrypted Distributed Analytics Platform”. In: *NSDI*. 283–298.

Zhu, R. and Y. Huang. 2017. “JIMU: Faster LEGO-Based Secure Computation Using Additive Homomorphic Hashes”. In: *Advances in Cryptology – ASIACRYPT 2017, Part II*. Ed. by T. Takagi and T. Peyrin. Vol. 10625. *Lecture Notes in Computer Science*. Springer, Heidelberg. 529–572.

Zhu, R., Y. Huang, and D. Cassel. 2017. “Pool: Scalable On-Demand Secure Computation Service Against Malicious Adversaries”. In: *ACM CCS 17: 24th Conference on Computer and Communications Security*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press. 245–257.

Zhu, R., Y. Huang, J. Katz, and A. Shelat. 2016. “The Cut-and-Choose Game and Its Application to Cryptographic Protocols.” In: *USENIX Security Symposium*. 1085–1100.