# References


[1] Privacy on the blockchain — ethereum foundation blog, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/, (Accessed on 03/11/2022).

[2] R. Pass, A. Shelat, Impossibility of vbb obfuscation with ideal constant-degree graded encodings, in: Theory of Cryptography Conference, Springer, 2016, pp. 3–17.

[3] A. Jain, H. Lin, A. Sahai, Indistinguishability obfuscation from lpn over f_p, dlin, and prgs in nc^ 0, Cryptology ePrint Archive (2021).

[4] A. Jain, H. Lin, A. Sahai, Indistinguishability obfuscation from well-founded assumptions, in: Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing, 2021, pp. 60–73.

[5] L. Devadas, W. Quach, V. Vaikuntanathan, H. Wee, D. Wichs, Succinct lwe sampling, random polynomials, and obfuscation, in: Theory of Cryptography Conference, Springer, 2021, pp. 256–287.

[6] R. Gay, R. Pass, Indistinguishability obfuscation from circular security, in: Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing, 2021, pp. 736–749.

[7] H. Wee, D. Wichs, Candidate obfuscation via oblivious lwe sampling, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2021, pp. 127–156.

[8] S. Garg, C. Gentry, A. Sahai, B. Waters, Witness encryption and its applications, in: Proceedings of the forty-fifth annual ACM symposium on Theory of computing, 2013, pp. 467–476.

[9] S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, N. Zeldovich, How to run turing machines on encrypted data, in: Annual Cryptology Conference, Springer, 2013, pp. 536–553.

[10] C. Gentry, A. Lewko, B. Waters, Witness encryption from instance independent assumptions, in: Annual Cryptology Conference, Springer, 2014, pp. 426–443.

[11] H. Abusalah, G. Fuchsbauer, K. Pietrzak, Offline witness encryption, in: International Conference on Applied Cryptography and Network Security, Springer, 2016, pp. 285–303.

[12] D. Pan, B. Liang, H. Li, P. Ni, Witness encryption with (weak) unique decryption and message indistinguishability: constructions and applications, in: Australasian Conference on Information Security and Privacy, Springer, 2019, pp. 609–619.

[13] P. Chvojka, T. Jager, S. A. Kakvi, Offline witness encryption with semi-adaptive security, in: International Conference on Applied Cryptography and Network Security, Springer, 2020, pp. 231–250.

[14] P. Chvojka, Time reveals the truth-more efficient constructions of timed cryptographic primitives, Ph.D. thesis, Universität Wuppertal, Fakultät für Elektrotechnik, Informationstechnik und ⋯ (2021).

[15] J. Bartusek, Y. Ishai, A. Jain, F. Ma, A. Sahai, M. Zhandry, Affine determinant programs: a framework for obfuscation and witness encryption, in: 11th Innovations in Theoretical Computer Science Conference, 2020.

[16] K. Kluczniak, Witness encryption from garbled circuit and multikey fully homomorphic encryption techniques, IACR Cryptol. ePrint Arch. 2020 (2020) 1502.

[17] V. Vaikuntanathan, H. Wee, D. Wichs, Witness encryption and null-io from evasive lwe, IACR Cryptol. ePrint Arch. 2022 (2022) 1140.

[18] RANDAO, randao/randao: Randao: A dao working as rng of ethereum, `https://github.com/randao/randao/`, (Accessed on 11/16/2022) (2022).

[19] WBTC, Wrapped bitcoin ( wbtc ) an erc20 token backed 1:1 with bitcoin, `https://wbtc.network/`, (Accessed on 09/20/2022).

[20] R. P. Kyber Network, BitGo Inc, wrapped-tokens-whitepaper.pdf, `https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf`, (Accessed on 09/20/2022) (January 2019).

[21] leohio, Trustless bitcoin bridge creation with witness encryption - cryptography - ethereum research, `https://ethresear.ch/t/trustless-bitcoin-bridge-creation-with-witness-encryption/11953`, (Accessed on 09/19/2022) (February 2022).

[22] Script - bitcoin wiki, `https://en.bitcoin.it/wiki/Script`, (Accessed on 09/20/2022).

[23] A. Scafuro, B. Zhang, One-time traceable ring signatures, in: European Symposium on Research in Computer Security, Springer, 2021, pp. 481–500.

[24] E. Fujisaki, K. Suzuki, Traceable ring signature, in: International Workshop on Public Key Cryptography, Springer, 2007, pp. 181–200.

[25] M. Blum, S. Micali, How to generate cryptographically strong sequences of pseudo random bits, in: Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, 2019, pp. 227–240.

[26] A. C. Yao, Theory and application of trapdoor functions, in: 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), IEEE, 1982, pp. 80–91.

[27] O. Goldreich, H. Krawczyk, M. Luby, On the existence of pseudorandom generators, SIAM Journal on Computing 22 (6) (1993) 1163–1175.

[28] J. Håstad, R. Impagliazzo, L. A. Levin, M. Luby, A pseudorandom generator from any one-way function, SIAM Journal on Computing 28 (4) (1999) 1364–1396.

[29] A. Pertsev, R. Semenov, R. Storm, Tornado cash privacy solution version 1.4 (2019).

[30] U. D. of the Treasury, U.s. treasury sanctions notorious virtual currency mixer tornado cash — u.s. department of the treasury, `https://home.treasury.gov/news/press-releases/jy0916`, (Accessed on 09/20/2022) (August 2022).

[31] S. Goldwasser, Y. T. Kalai, G. N. Rothblum, One-time programs, in: Annual International Cryptology Conference, Springer, 2008, pp. 39–56.

[32] R. Goyal, V. Goyal, Overcoming cryptographic impossibility results using blockchains, in: Theory of Cryptography Conference, Springer, 2017, pp. 529–561.

[33] A. C.-C. Yao, How to generate and exchange secrets, in: 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), IEEE, 1986, pp. 162–167.

[34] S. Goldwasser, Y. Kalai, R. A. Popa, V. Vaikuntanathan, N. Zeldovich, Reusable garbled circuits and succinct functional encryption, in: Proceedings of the forty-fifth annual ACM symposium on Theory of computing, 2013, pp. 555–564.

[35] P. Ananth, Z. Brakerski, G. Segev, V. Vaikuntanathan, From selective to adaptive security in functional encryption, in: Annual Cryptology Conference, Springer, 2015, pp. 657–677.

[36] D. Boneh, A. Sahai, B. Waters, Functional encryption: Definitions and challenges, in: Theory of Cryptography Conference, Springer, 2011, pp. 253–273.

[37] Z. Brakerski, G. Segev, Function-private functional encryption in the private-key setting, Journal of Cryptology 31 (1) (2018) 202–225.

[38] S. Gorbunov, V. Vaikuntanathan, H. Wee, Functional encryption with bounded collusions via multi-party computation, in: Annual Cryptology Conference, Springer, 2012, pp. 162–179.

[39] P. Ananth, A. Jain, Z. Jin, G. Malavolta, Multi-key fully-homomorphic encryption in the plain model, in: Theory of Cryptography Conference, Springer, 2020, pp. 28–57.

[40] Z. Jafargholi, D. Wichs, Adaptive security of yao' s garbled circuits, in: Theory of Cryptography Conference, Springer, 2016, pp. 433–458.

[41] Z. Brakerski, C. Gentry, V. Vaikuntanathan, (leveled) fully homomorphic encryption without bootstrapping, ACM Transactions on Computation Theory (TOCT) 6 (3) (2014) 1–36.

[42] C. Gentry, A. Sahai, B. Waters, Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based, in: Annual Cryptology Conference, Springer, 2013, pp. 75–92.

[43] S. Gorbunov, V. Vaikuntanathan, H. Wee, Attribute-based encryption for circuits, Cryptology ePrint Archive, Paper 2013/337, `https://eprint.iacr.org/2013/337` (2013). URL `https://eprint.iacr.org/2013/337`

[44] X. Dai, W. Wu, Y. Feng, Key lifting: Multi-key fully homomorphic encryption in plain model, Cryptology ePrint Archive (2022).