REFERENCES

Abrera, J. (2023). *Data Privacy and Security in Cloud Computing: A Comprehensive Review*.

Akram, A., Akella, V., Peisert, S., & Lowe-Power, J. (2021). *Enabling Design Space Exploration for RISC-V Secure Compute Environments*.

Bellare, M., Canetti, R., & Krawczyk, H. (1996). Keying Hash Functions for Message Authentication. In N. Koblitz (Ed.), *Advances in Cryptology—CRYPTO '96* (Vol. 1109, pp. 1–15). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-68697-5_1

Bellare, M., Desai, A., Jokipii, E., & Rogaway, P. (1997). A concrete security treatment of symmetric encryption. Proceedings 38th Annual Symposium on Foundations of Computer Science, 394-403.

Binkert, N., Beckmann, B., Black, G., Reinhardt, S. K., Saidi, A., Basu, A., Hestness, J., Hower, D. R., Krishna, T., Sardashti, S., Sen, R., Sewell, K., Shoaib, M., Vaish, N., Hill, M. D., & Wood, D. A. (2011). The gem5 simulator. ACM SIGARCH Computer Architecture News, 39(2), 1-7. https://doi.org/10.1145/2024716.2024718

Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). *Fully Homomorphic Encryption without Bootstrapping*.

Brakerski, Z., & Vaikuntanathan, V. (2011). Efficient Fully Homomorphic Encryption from (Standard) LWE. *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, 97–106. https://doi.org/10.1109/FOCS.2011.12

Chatel, S., Knabenhans, C., Pyrgelis, A., Troncoso, C., & Hubaux, J.-P. (2024). *Verifiable Encodings for Secure Homomorphic Analytics* (No. arXiv:2207.14071). arXiv. https://doi.org/10.48550/arXiv.2207.14071

Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic Encryption for Arithmetic of

Approximate Numbers. In T. Takagi & T. Peyrin (Eds.), *Advances in Cryptology – ASIACRYPT 2017* (Vol. 10624, pp. 409–437). Springer International Publishing. https://doi.org/10.1007/978-3-319-70694-8_15

Costan, V., Lebedev, I., & Devadas, S. (2017). Secure Processors Part II: Intel SGX Security Analysis and MIT Sanctum Architecture. *Foundations and Trends® in Electronic Design Automation*, *11*(3), 249–361. https://doi.org/10.1561/1000000052

Dong, A. X., Gwinn, R. P., Warner, N. M., Caylor, L. M., & Doherty, M. J. (2016). Mitigating bit flips or single event upsets in epilepsy neurostimulators. *Epilepsy & Behavior Case Reports*, *5*, 72–74. https://doi.org/10.1016/j.ebcr.2016.04.002

Dworkin, Morris. (2001). Recommendation for Block Cipher Modes of Operation. Methods and Techniques. 67.

Fan, J., & Vercauteren, F. (2012). *Somewhat Practical Fully Homomorphic Encryption ?*

Fully Homomorphic Message Authenticators. (2013). In R. Gennaro & D. Wichs, *Lecture Notes in Computer Science* (pp. 301–320). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-42045-0_16

Gassend, B., Suh, G. E., Clarke, D., Van Dijk, M., & Devadas, S. (2003). Caches and hash trees for efficient memory integrity verification. *The Ninth International Symposium on High-Performance Computer Architecture, 2003. HPCA-9 2003. Proceedings.*, 295–306. https://doi.org/10.1109/HPCA.2003.1183547

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, 169–178. https://doi.org/10.1145/1536414.1536440

Gharpure, R., & Ghodke, D. M. (2021). *Effect of Cloud computing technology adoption on*

Reduction in Costs: A critical review from the perspective of business.

Gouert, C., Mouris, D., & Tsoutsos, N. (2023). SoK: New Insights into Fully Homomorphic Encryption Libraries via Standardized Benchmarks. *Proceedings on Privacy Enhancing Technologies*, *2023*(3), 154–172. https://doi.org/10.56553/popets-2023-0075

Gueron, S. (2016). *A Memory Encryption Engine Suitable for General Purpose Processors*.

Hennessy, J. L., & Patterson, D. A. (2011). Computer architecture: A quantitative approach (5th ed.). Morgan Kaufmann.

Hong, C. (2025). Recent advances of privacy-preserving machine learning based on (Fully) Homomorphic Encryption. *Security and Safety*, *4*, 2024012. https://doi.org/10.1051/sands/2024012

Jain, N., & Cherukuri, A. K. (2023). *Revisiting Fully Homomorphic Encryption Schemes*.

Jang, Y., Lee, J., Lee, S., & Kim, T. (2017). SGX-Bomb: Locking Down the Processor via Rowhammer Attack. *Proceedings of the 2nd Workshop on System Software for Trusted Execution*, 1–6. https://doi.org/10.1145/3152701.3152709

Jun Yang, Youtao Zhang, & Lan Gao. (2003). Fast secure processor for inhibiting software piracy and tampering. *22nd Digital Avionics Systems Conference. Proceedings (Cat. No.03CH37449)*, 351–360. https://doi.org/10.1109/MICRO.2003.1253209

Krawczyk, H., Bellare, M., & Canetti, R. (1997). *HMAC: Keyed-Hashing for Message Authentication* (No. RFC2104; p. RFC2104). RFC Editor. https://doi.org/10.17487/rfc2104

Lee, D., Kohlbrenner, D., Shinde, S., Song, D., & Asanović, K. (2019). *Keystone: An Open Framework for Architecting TEEs* (No. arXiv:1907.10119). arXiv. https://doi.org/10.48550/arXiv.1907.10119

Lee, R. B., Kwan, P. C. S., McGregor, J. P., Dwoskin, J., & Wang, Z. (2005). Architecture for protecting critical secrets in microprocessors. ACM SIGARCH Computer Architecture News, 33(2), 2-13. https://doi.org/10.1145/1080695.1069971

Lipmaa, Helger & Rogaway, Phillip & Wagner, David. (2000). Comments to NIST concerning AES-modes of operations: CTR-mode encryption.

Lowe-Power, J., Ahmad, A. M., Akram, A., Alian, M., Amslinger, R., Andreozzi, M., Armejach, A., Asmussen, N., Beckmann, B., Bharadwaj, S., Black, G., Bloom, G., Bruce, B. R., Carvalho, D. R., Castrillon, J., Chen, L., Derumigny, N., Diestelhorst, S., Elsasser, W., … Zulian, É. F. (2020). *The gem5 Simulator: Version 20.0+* (No. arXiv:2007.03152). arXiv. https://doi.org/10.48550/arXiv.2007.03152

Mordor Intelligence. (2021). Indonesia data center market: Growth, trends, COVID-19 impact, and forecasts (2021–2026). Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/indonesia-data-center-market

Mutlu, O., & Kim, J. S. (2019). *RowHammer: A Retrospective* (No. arXiv:1904.09724). arXiv. https://doi.org/10.48550/arXiv.1904.09724

Natarajan, D., Loveless, A., Dai, W., & Dreslinski, R. (2023). Chex-Mix: Combining Homomorphic Encryption with Trusted Execution Environments for Oblivious Inference in the Cloud. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, 73–91. https://doi.org/10.1109/EuroSP57164.2023.00014

Raj, S., & Paliwal, M. (2021). An Overview on the Study of Data Encryption and Decryption in Cloud Computing. *International Journal of Innovative Research in Computer Science & Technology*, 139–143. https://doi.org/10.55524/ijircst.2021.9.6.32

Sabt, M., Achemlal, M., & Bouabdallah, A. (2015). Trusted Execution Environment: What It is,

and What It is Not. *2015 IEEE Trustcom/BigDataSE/ISPA*, 57–64. https://doi.org/10.1109/Trustcom.2015.357

Santriaji, M. H., Xue, J., Lou, Q., & Solihin, Y. (2024). *DataSeal: Ensuring the Verifiability of Private Computation on Encrypted Data* (No. arXiv:2410.15215). arXiv. https://doi.org/10.48550/arXiv.2410.15215

Smart, N. P., & Vercauteren, F. (2014). Fully homomorphic SIMD operations. *Designs, Codes and Cryptography*, *71*(1), 57–81. https://doi.org/10.1007/s10623-012-9720-4

Stallings, W. (2014). Cryptography and Network Security: Principles and Practice (6th ed.). Pearson Education.

Suh, G. E., Clarke, D., Gassend, B., van Dijk, M., & Devadas, S. (2003). *AEGIS: Architecture for Tamper-Evident and Tamper-Resistant Processing*.

Talapkaliyev, D. (2019). *Hiding Decryption Latency in Intel SGX using Metadata Prediction*.

van Dijk, M., & Juels, A. (2010). *On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing*.

Viand, A., Knabenhans, C., & Hithnawi, A. (2023). *Verifiable Fully Homomorphic Encryption* (No. arXiv:2301.07041). arXiv. https://doi.org/10.48550/arXiv.2301.07041

Waterman, A., & Asanović, K. (2019). The RISC-V Instruction Set Manual, Volume I: User-Level ISA, Document Version 20191213. RISC-V Foundation.

Yan, C., Rogers, B., Englender, D., Solihin, Y., & Prvulovic, M. (2006). *Improving Cost, Performance, and Security of Memory Encryption and Authentication*.