REFERENCES

Badawi, A., Bates, J., Bergamaschi, F., Cousins, D.B., Erabelli, S., Genise, N., Halevi, S., Hunt, H., Kim, A., Lee, Y., Liu, Z., Micciancio, D., Quah, I., Polyakov, Y., R.v, S., Rohloff, K., Saylor, J., Suponitsky, D., Triplett, M. and Vaikuntanathan, V. (2022). OpenFHE: OpenSource Fully Homomorphic Encryption Library. In: *Proceedings of the 10th Workshop on Encrypted Computing & Applied*. [online] Association for Computing Machinery, p.5363. doi:https://doi.org/10.1145/3560827.3563379.

Bulck, V., Minkin, M., Weisse, O., Genkin, D., Kasikci, B., Piessens, F., Silberstein, M., Wenisch, T.F., Yarom, Y. and Strackx, R. (2018). Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient. In: *27th USENIX Security Symposium (USENIX Security 18)*. [online] USENIX Association, pp.991\textendash1008. Available at: https://www.usenix.org/conference/usenixsecurity18/presentation/bulck.

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

Dwork, C. and Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4), pp.211–407. doi:https://doi.org/10.1561/0400000042.

Ebel, A., Garimella, K. and Reagen, B. (2025). Orion: A Fully Homomorphic Encryption Framework for Deep Learning. In: *Proceedings of the 30th ACM International Conference on Architectural*. [online] Association for Computing Machinery, pp.734–749. doi:https://doi.org/10.1145/3676641.3716008.

Eldefrawy, K., Genise, N. and Manohar, N. (2023). On the Hardness of Scheme-Switching Between SIMD FHE Schemes. In: T. Johansson and D. SmithTone, eds., *Post-Quantum Cryptography*. Cham: Springer Nature Switzerland, pp.196–224.

Evans, D., Kolesnikov, V. and Rosulek, M. (2018). *A Pragmatic Introduction to Secure MultiParty Computation*. [online] now, pp.1-. doi:https://doi.org/10.1561/3300000019.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In: *Proceedings of the FortyFirst Annual ACM Symposium on Theory of Computing*. [online] Association for Computing Machinery, pp.169–178. doi:https://doi.org/10.1145/1536414.1536440.

Gharpure, R. and Ghodke, M. (2021). Effect of Cloud computing technology adoption on Reduction in Costs: A critical review from the perspective of business. *Turkish*

Journal of Computer and Mathematics Education (TURCOMAT), [online] 12(10), pp.4391–4399. Available at: https://turcomat.org/index.php/turkbilmat/article/view/5172.

Halevi, S. and Shoup, V. (2020). Design and implementation of HElib: a homomorphic encryption library. [online] Available at: https://eprint.iacr.org/2020/1481.

Hong, C. (2024). Recent advances of privacypreserving machine learning based on (Fully) Homomorphic Encryption. *Security and Safety*, 4. doi:https://doi.org/10.1051/sands/2024012.

Hornik, K., Stinchcombe, M. and White, H. (1989). Multilayer feedforward networks are universal approximators. *Neural Networks*, [online] 2(5), pp.359–366. doi:https://doi.org/10.1016/08936080(89)900208.

Jain, N., Cherukuri, A.K. and Kamalov, F. (2023). Revisiting Fully Homomorphic Encryption Schemes for PrivacyPreserving Computing. In: *Emerging Technologies and Security in Cloud Computing*. IGI Global, pp.276–294. doi:https://doi.org/10.4018/9798369320815.ch012.

Lee, S., Lee, G., Kim, J.W., Shin, J., Lee, M., Krause, A., Brunskill, E., Cho, K., Engelhardt, B., Sabato, S. and Scarlett, J. (2023). HETAL: Efficient Privacypreserving Transfer Learning with Homomorphic. In: *Proceedings of the 40th International Conference on Machine Learning*. [online] PMLR, p.1901019035. Available at: https://proceedings.mlr.press/v202/lee23m.html.

Li, T., Sahu, A.K., A. Talwalkar and Smith, V. (). Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal Processing Magazine*, 37(3), pp.50–60. doi:https://doi.org/10.1109/MSP.2020.2975749.

Lyubashevsky, V., Peikert, C. and Regev, O. (2010). On Ideal Lattices and Learning with Errors over Rings. In: H. Gilbert, ed., *Advances in Cryptology – EUROCRYPT 2010*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp.1–23.

Maas, A.L., Hannun, A.Y. and Ng, A.Y. (2013). Rectifier nonlinearities improve neural network acoustic models. In: *Proceedings of the 30th International Conference on Machine Learning*. [online] International Conference on Machine Learning. Atlanta, Georgia, p.3. Available at: https://ai.stanford.edu/~amaas/papers/relu_hybrid_icml2013_final.pdf.

Micciancio, D. and Regev, O. (2009). Lattice-based Cryptography. In: D.J. Bernstein, J. Buchmann and E. Dahmen, eds., *Post-Quantum Cryptography*. [online] Berlin, Heidelberg: Springer Berlin Heidelberg, pp.147–191. doi:https://doi.org/10.1007/9783540887027_5.

Microsoft (2023). *SEAL (release 4.1)*. [online] Available at: https://github.com/Microsoft/SEAL.

Mutlu, O. and Kim, J.S. (2020). RowHammer: A Retrospective. *Trans. Comp.Aided Des. Integ. Cir. Sys.*, [online] 39(8), pp.1555–1571. doi:https://doi.org/10.1109/TCAD.2019.2915318.

Raj, S. and 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*, 9(6), pp.139–143. doi:https://doi.org/10.55524/ijircst.2021.9.6.32.

Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. In: *Proceedings of the ThirtySeventh Annual ACM Symposium on Theory of*. [online] Association for Computing Machinery, pp.84–93. doi:https://doi.org/10.1145/1060590.1060603.

Rovida, L. and Leporati, A. (2024). Encrypted Image Classification with Low Memory Footprint Using Fully Homomorphic Encryption. *Int. J. Neur. Syst.*, [online] 34(05), p.2450025. doi:https://doi.org/10.1142/S0129065724500254.

Shanks, D. (1971). Class Number, a Theory of Factorization and Genera. *Proceedings of Symposium of Pure Mathematics*, 20, pp.415–440.