Ahmad Al Badawi, Ph.D.

Cryptography • Privacy-Enhancing Technologies • Hardware Acceleration

Hoboken, NJ, US • (+1) 862 600 4745

ahmad.albadawi.phd@gmail.com

www.ahmadalbadawi.com • linkedin.com/in/ahmad-al-badawi • Google Scholar

ORCID 0000-0001-7759-7368 • US Permanent Resident (EB-1A "Extraordinary Ability")

Summary

Cryptography research scientist with 20 years of professional experience, including more than 10 years in privacy-enhancing technologies (PETs). Ph.D. in Electrical and Computer Engineering from the National University of Singapore. Co-author and maintainer of OpenFHE, ranked the most used fully homomorphic encryption (FHE) library at 51% adoption in an independent 2026 industry survey. Technical Principal Investigator of the $15M DARPA DPRIVE program, which delivered a fully verified 12 nm FHE accelerator ASIC design with 1 GHz timing closure on a 176 mm^2 floorplan. Author or co-author of more than 50 peer-reviewed publications with more than 2,500 citations, an h-index of 20, and an i10-index of 28. Named inventor on 3 patents, 2 of them granted in the United States.

Expertise spans the full stack of encrypted computation: the underlying number theory and polynomial arithmetic, the software libraries that implement it, and the GPU, FPGA and ASIC hardware that accelerates it. Work has been applied to regulated data in healthcare, finance, genomics, aerospace and government, including a multiparty FHE study on real oncological data published in the *Proceedings of the National Academy of Sciences*.

Professional Experience

Senior Scientist & Principal Investigator, Cryptography, Duality Technologies Inc., Hoboken, NJ, US
Sep 2022 – Present

- **Program leadership.** Served as Technical Principal Investigator for DARPA's DPRIVE program, with responsibility for all technical aspects of a four-organization, four-team effort. Led the Applied Cryptography, Hardware, Software/ISA and Verification teams, and coordinated research, development and integration across the consortium to deliver program objectives.
- **Silicon delivery.** Directed the design and tape-out preparation of a 12 nm ASIC for accelerating FHE computation. Delivered a fully verified register-transfer-level implementation and top-level floorplan of 176 mm^2, achieving timing closure at 1 GHz for a node-array architecture.
- **Instruction set and validation.** Supervised development of a custom instruction set architecture and microcode scheduler, and validated hardware performance using high-complexity workloads, including encrypted convolutional neural network training and inference and AES transciphering.
- **Encrypted machine learning.** Architected encrypted inference pipelines for convolutional neural networks, logistic regression and transformer language models (BERT, GPT-2, LLaMA-3) on Duality's enterprise platform, across CPU and GPU. Proved that model-preserving encrypted transformer inference under CKKS is achievable with under 0.5% accuracy loss.
- **Secure protocol development.** Built secure protocols for CNN inference and training (healthcare, finance, government), logistic regression (marketing, fraud detection), personalized recommendation and private query systems.
- **Open-source engineering.** Co-authored and maintains OpenFHE. Wrote optimized C++ implemen-

tations of private information retrieval, private set intersection and threshold multi-party computation primitives, together with the Python bindings that expose FHE to data scientists. Co-authored OpenFHE-NumPy, a NumPy-like application programming interface for computation on encrypted data.

- **Performance ownership.** Owns the performance roadmap for privacy protocols, covering AVX-512 vectorization, multi-GPU acceleration and bottleneck refactoring. Builds analytical performance models (roofline and queueing) that guide accelerator architecture decisions across platforms and workloads.
- **Hardware-software integration.** Responsible for full-stack integration of FHE accelerators, and for accelerator development on multi-core CPUs, GPUs, FPGAs and ASICs.
- **Partnerships.** Leads Duality's partnerships with Intel, NVIDIA and several startups on OpenFHE hardware acceleration, converting research into customer prototypes and pilots.

Cryptography Consultant (part-time), Duality Technologies Inc., NJ, US **Jul 2021 – Aug 2022**

- Served as Co-Principal Investigator on DARPA DPRIVE, translating cryptographic constraints into low-level specifications for the 12 nm ASIC architecture, and developing the software library used to program it.
- Implemented bootstrapping for integer FHE schemes (BGV and BFV) in the PALISADE library in C++, enabling unbounded-depth computation on encrypted data and extending integer FHE to machine-learning and data-analytics workloads.
- Designed fixed-point packed encodings that allow floating-point models to run on integer-based schemes with negligible accuracy loss. Documented low-level homomorphic operations for hardware-acceleration engineers.

Assistant Professor, Cybersecurity & Data Analytics, Rabdan Academy, Abu Dhabi, UAESep 2021 – Aug 2022

- Taught Introduction to Cybersecurity, Cryptography, Network Security, Incident Response, Information Security Management, and Data Analytics for Cybersecurity.
- Led research on post-quantum cryptography, privacy-enhancing technologies, cryptographic engineering, and machine learning for cybersecurity, publishing in peer-reviewed journals and conferences.
- Mentored an undergraduate data-analytics team on intrusion detection systems; the team was selected for the academy's first student conference trip.

Privacy Consultant (part-time), Inferati Inc., Seattle, WA, US **Oct 2019 – Feb 2022**

- Designed homomorphic string-operation algorithms, including string matching, wildcard search and natural-language-processing primitives over encrypted text, and improved the performance of existing operations.
- Developed homomorphic algorithms and protocols for integer computation.
- Authored technical whitepapers and articles explaining homomorphic encryption and privacy-enhancing technologies for industry audiences, including guidance on applying these techniques to protect privacy and security.

Research Scientist II, Privacy Engineering Lead, A*STAR Institute for Infocomm Research, Singapore **Dec 2018 – Sep 2021**

- **Research leadership.** Led ten research and development projects with values from S$100K to S$3.3M each, managing lifecycles, resources and roadmaps. Oversaw a team of scientists, engineers and doctoral students developing FPGA-accelerated FHE.
- **Applied cryptographic systems.** Delivered HCNN (encrypted CNN inference on MNIST, CIFAR-10 and diabetic-retinopathy images), PrivFT (encrypted text classification with training and prediction), GI-FHE (genotype imputation on encrypted DNA sequences), AML-FHE (anti-money-laundering detection on encrypted transactions), and CASHE (spacecraft conjunction analysis on encrypted orbital data).
- **High-performance implementation.** Implemented AVX2, AVX-512, FPGA and GPU versions of post-quantum schemes (Kyber, NTTRU, LAC) and FHE schemes (BFV, BGV, CKKS, TFHE).
- **Technical advisory.** Served on the I2R Technical Expert Panel, advising cross-functional teams on privacy architecture and resolving cryptographic implementation issues.
- **Funding and intellectual property.** Authored research grants, project proposals and invention disclosures. Developed customer engagements through applied-research prototypes and pilots.

Research Scholar, HPC & Cryptography, A*STAR Data Storage Institute / National University of Singapore **Jan 2015 – Nov 2018**

- Engineered the first single-GPU and multi-GPU implementations of the BFV, BGV and CKKS schemes, achieving 10–100$\times$ speedups over CPU baselines and establishing the foundation for modern GPU-accelerated FHE libraries.
- Designed the BEHZ and HPS residue-number-system variants of BFV and contributed them to PALISADE; these are now standard building blocks in OpenFHE, Microsoft SEAL and HElib.
- Proposed a generalization of the Discrete Galois Transform multiplication algorithm for post-quantum and homomorphic cryptography, which became the basis of two United States patents.
- Designed and implemented three post-quantum cryptosystems (subset-sum, LWE and Ring-LWE public-key cryptosystems), accelerating them by one to two orders of magnitude at large parameter settings.
- Scaled the BFV GPU crypto-processor to multi-GPU clusters with near-linear speedup in the number of GPUs. Served as teaching assistant for undergraduate and graduate ECE modules.

Lecturer, Dept. of Computer Engineering, Taif University, Taif, Saudi Arabia Sep 2011 – Dec 2014

- Taught Introduction to Computer Science, Operating Systems and Matlab, Compilers, Algorithms and Data Structures, and Computer Programming in C++.
- Led ABET accreditation preparation: assembled assessment course files, analyzed programme data, and prepared reports for the accreditation committee.
- Developed multiprocessor task-scheduling algorithms using evolutionary optimization heuristics. Designed and maintained the college website. Trained and led the robotics team.

Senior Software Engineer, Globitel, Amman, Jordan **Jun 2008 – Sep 2011**

- Architected real-time, zero-downtime GSM and SS7 roaming systems in C++, Java and Pthreads on Unix and Linux, using CAMEL, SIP, Berkeley sockets, Perl and Oracle.
- Developed Intelligent Traffic Steering, a roaming traffic-redirection system, and Collect Call, a callee-pays service built on the Diameter charging protocol.

- Redesigned business logic for shared-memory and NUMA platforms and the data model for multi-platform support. Applied layered architecture, dependency injection and continuous integration, with unit and integration test coverage.

Teaching Assistant, Jordan University of Science and Technology, Jordan **Feb 2008 – Jun 2008**

- Co-taught undergraduate Computer Engineering courses.

Intern, Technical Support Engineer, Cairo Amman Bank, Jordan **Feb 2007 – May 2007**

- Resolved and documented customer technical issues and contributed to support procedures.

Education

National University of Singapore, Doctor of Philosophy **Singapore, Nov 2018**

- Major: Electrical & Computer Engineering.
- Thesis: Practical Post-Quantum Cryptography & Fully Homomorphic Encryption on Graphics Processors: Design & Performance Evaluation (7 chapters, 203 pages).
- Thesis Advisor: Prof. Bharadwaj Veeravalli. Singapore International Graduate Award (SINGA) Fellowship.

Jordan University of Science and Technology, Master of Science **Jordan, Mar 2010**

- Major: Computer Engineering. Thesis: Static Scheduling of Directed Acyclic Data Flow Graphs onto Multiprocessors Using Particle Swarm Optimization. Advisor: Prof. Ali M. Shatnawi.

Al-Balqa' Applied University, Bachelor of Science **Jordan, Jun 2007**

- Major: Computer Engineering. Capstone: Wireless Control System Using Speech Recognition and a Smartphone. Advisor: Prof. Abdelwadood Mesleh.

Honors and Recognitions

- Nov 2024. EB-1A "Extraordinary Ability" US Permanent Residency, awarded by USCIS in recognition of significant contributions to science, research and technology.
- Sep 2023. Honorary token from Sabancı University for instructing at the enCRYPTON Summer School.
- Feb 2022. O-1A "Extraordinary Ability" US visa, awarded by USCIS in recognition of significant contributions to privacy-enhancing technologies.
- Aug 2017. Outstanding Technical Oral Presentation, Electrical and Computer Engineering Graduate Student Symposium, National University of Singapore.
- Dec 2015. Student Travel Grant Award, Annual Computer Security Applications Conference (ACSAC).
- Jan 2015. Singapore International Graduate Award (SINGA) Ph.D. Scholarship, A*STAR.
- Dec 2014. Honorary Shield from Taif University for training and leading the robotics team.
- Feb 2009. M.Sc. Scholarship, Jordan University of Science and Technology.

Selected Publications

More than 50 peer-reviewed journal, conference and workshop papers; more than 2,500 citations; h-index 20; i10-index 28 (Google Scholar, September 2026). Citation counts below are from the same snapshot.

Complete list: Google Scholar.

- **Al Badawi, A.**, A. Alexandru, G. Arakelov, C. Gouert, S. Gomenyuk, et al. "Efficient Large-Integer Arithmetic for FHE." Cryptology ePrint Archive, 2026. *First author.*
- **Al Badawi, A.**, A. Alexandru, Y. Polyakov, and V. Vaikuntanathan. "SoK: Private LLM Inference using Approximate Homomorphic Encryption." Cryptology ePrint Archive 2026/935, 2026. *First author; manuscript under review. 5 citations.*
- Alexandru, A., **Al Badawi, A.**, D. Micciancio, and Y. Polyakov. "Application-Aware Approximate Homomorphic Encryption: Configuring FHE for Practical Use." *IACR Communications in Cryptology* 2(4), 2026. *46 citations.*
- Vig, S., **Al Badawi, A.**, and M. F. B. Yusof. "Hardware design for fast gate bootstrapping in fully homomorphic encryption over the Torus." *International Journal of Reconfigurable and Embedded Systems* 14(3):659–675, 2025.
- Adamek, J., et al. (incl. **Al Badawi, A.**). "FHERMA Cookbook: FHE Components for Privacy-Preserving Applications." 13th Workshop on Encrypted Computing & Applied Homomorphic Computing (WAHC), pp. 68–76, 2025.
- Mazzone, F., **Al Badawi, A.**, Y. Polyakov, M. Everts, F. Hahn, and A. Peter. "Encrypt What Matters: Selective Model Encryption for More Efficient Secure Federated Learning." IFIP DBSec, pp. 96–115, 2025.
- **Al Badawi, A.** "Private SVM Inference on Encrypted Data." In *Federated Learning: A Systematic Review*, p. 143. IntechOpen, 2025. *Sole author.*
- **Al Badawi, A.**, and M. F. B. Yusof. "Private pathological assessment via machine learning and homomorphic encryption." *BioData Mining* 17(1):33, 2024. *First author. 32 citations.*
- **Al Badawi, A.**, S. L. Yeo, and M. F. B. Yusof. "A generalized number-theoretic transform for efficient multiplication in lattice cryptography." *Contemporary Mathematics* 5(4):4200–4222, 2024. *First author; subject matter of US Patents 11,368,280 and US 2022/0085970 A1.*
- Geva, R., et al. (incl. **Al Badawi, A.**, D. Micciancio, V. Vaikuntanathan, S. Goldwasser). "Collaborative privacy-preserving analysis of oncological data using multiparty homomorphic encryption." *Proceedings of the National Academy of Sciences* 120(33):e2304415120, 2023. *40 citations.*
- Soni, D., et al. (incl. **Al Badawi, A.**). "RPU: The Ring Processing Unit." IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), pp. 272–282, 2023. *32 citations.*
- Cousins, D. B., Y. Polyakov, **Al Badawi, A.**, et al. "TREBUCHET: Fully Homomorphic Encryption Accelerator for Deep Computation." arXiv:2304.05237, 2023. *13 citations.*
- **Al Badawi, A.**, and Y. Polyakov. "Demystifying bootstrapping in fully homomorphic encryption." Cryptology ePrint Archive 2023/149, 2023. *First author. 88 citations.*
- **Al Badawi, A.**, et al. "OpenFHE: Open-Source Fully Homomorphic Encryption Library." 10th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC) at ACM CCS, pp. 53–63, 2022. *First author. 745 citations.*
- Zhang, N., et al. (incl. **Al Badawi, A.**). "Towards full-stack acceleration for fully homomorphic encryption." IEEE High Performance Extreme Computing Conference (HPEC), 2022.
- **Al Badawi, A.**, L. Chen, and S. Vig. "Fast homomorphic SVM inference on encrypted data." *Neural Computing and Applications* 34(18), 2022. *First author. 17 citations.*
- Abu Al-Haija, Q., and **Al Badawi, A.** "High-performance intrusion detection system for networked UAVs via deep learning." *Neural Computing and Applications* 34(13), 2022. *159 citations.*

- Paul, J., M. S. M. S. Annamalai, W. Ming, **Al Badawi, A.**, B. Veeravalli, and K. M. M. Aung. "Privacy-preserving collective learning with homomorphic encryption." *IEEE Access* 9:132084–132096, 2021. *58 citations.*
- Chan, F. M., **Al Badawi, A.**, J. J. Sim, B. H. M. Tan, F. C. Sheng, and K. M. M. Aung. "Genotype imputation with homomorphic encryption." 6th International Conference on Biomedical Signal and Image Processing (ICBIP), pp. 9–13, 2021. *11 citations.*
- **Al Badawi, A.**, L. Hoang, C. F. Mun, K. Laine, and K. M. M. Aung. "PrivFT: Private and Fast Text Classification with Homomorphic Encryption." *IEEE Access* 8:226544–226556, 2020. *First author. 174 citations.*
- **Al Badawi, A.**, et al. "Towards the AlexNet Moment for Homomorphic Encryption: HCNN, the First Homomorphic CNN on Encrypted Data with GPUs." *IEEE Transactions on Emerging Topics in Computing* 9(3):1330–1343, 2021. *First author. 325 citations.*
- **Al Badawi, A.**, B. Veeravalli, J. Lin, N. Xiao, M. Kazuaki, and K. M. M. Aung. "Multi-GPU design and performance evaluation of homomorphic encryption on GPU clusters." *IEEE Transactions on Parallel and Distributed Systems* 32(2):379–391, 2021. *First author. 80 citations.*
- Chung, H., M. Kim, **Al Badawi, A.**, K. M. M. Aung, and B. Veeravalli. "Homomorphic comparison for point numbers with user-controllable precision and its applications." *Symmetry* 12(5):788, 2020. *10 citations.*
- **Al Badawi, A.**, Y. Polyakov, K. M. M. Aung, B. Veeravalli, and K. Rohloff. "Implementation and performance evaluation of RNS variants of the BFV homomorphic encryption scheme." *IEEE Transactions on Emerging Topics in Computing* 9(2):941–956, 2021. *First author. 195 citations.*
- **Al Badawi, A.**, B. Veeravalli, and K. M. M. Aung. "Efficient polynomial multiplication via modified discrete Galois transform and negacyclic convolution." Future of Information and Communication Conference (FICC), pp. 666–682. Springer, 2019. *First author; subject matter of US Patents 11,368,280 and US 2022/0085970 A1. 20 citations.*
- **Al Badawi, A.**, B. Veeravalli, and K. M. M. Aung. "Faster number theoretic transform on graphics processors for ring learning with errors based cryptography." IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 26–31, 2018. *First author. 18 citations.*
- **Al Badawi, A.**, B. Veeravalli, C. F. Mun, and K. M. M. Aung. "High-performance FV somewhat homomorphic encryption on GPUs: An implementation using CUDA." *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2018(2):70–95. *First author. 133 citations.*
- **Al Badawi, A.**, B. Veeravalli, K. M. M. Aung, and B. Hamadicharef. "Accelerating subset sum and lattice based public-key cryptosystems with multi-core CPUs and GPUs." *Journal of Parallel and Distributed Computing* 119:179–190, 2018. *First author. 10 citations.*
- **Al Badawi, A.**, and A. Shatnawi. "Static scheduling of directed acyclic data flow graphs onto multiprocessors using particle swarm optimization." *Computers & Operations Research* 40(10):2322–2328, 2013. *First author. 27 citations.*

Patents

- H. Yang, D. M. Kang, **Al Badawi, A.**, and K. M. M. Aung. "Device for Processing Homomorphically Encrypted Data." U.S. Patent 12,489,602, granted Dec 2025.
- **Al Badawi, A.**, and K. M. M. Aung. "Homomorphic Encryption Using Discrete Galois Transforms." U.S. Patent 11,368,280, issued Jun 21, 2022. *First inventor.*
- **Al Badawi, A.**, and K. M. M. Aung. "Multiplication Methods, Non-Transitory Computer-Readable

Media, and Multiplication Devices." PCT/SG2018/050366 (2018); U.S. Application US 2022/0085970 A1. Priority date 2017. *First inventor.*

Invited Talks, Lectures and Public Speaking

- Aug 2026. "Multi-Skill Coding Agent for Encrypted Computation in OpenFHE." Privacy-Preserving Machine Learning Workshop (PPML), affiliated with CRYPTO 2026, UC Santa Barbara, CA.
- Jun 2026. Invited talk, "Private LLM Inference using Fully Homomorphic Encryption." OpenFHE Monthly Webinar Series, BrightTALK. Recording available.
- Sep 2024. "Code and Community in the OpenFHE Project." NUMFOCUS Project Summit 2024, Microsoft NERD Center, Cambridge, MA.
- Feb 2024. Keynote on OpenFHE, FHEllo World! FHE Community Workshop. Recording available.
- Aug–Sep 2023. Instructor, enCRYPTON Summer School on Cryptographic Solutions for Privacy-Enhancing Technologies, Sabancı University, Istanbul. Five lectures on the CKKS scheme, the OpenFHE library and machine learning on encrypted data; organized the closing hackathon.
- Nov 2022. "OpenFHE: Open-Source Fully Homomorphic Encryption Library." WAHC 2022 at ACM CCS, Los Angeles, CA.
- May 2022. Invited speaker, "Fully Homomorphic Encryption on GPUs: Design, Implementation & Performance Evaluation." NVIDIA research seminar.
- Oct 2021. "Privacy-Preserving Computing." Cyber Wales Cluster Webinar in the Middle East, Abu Dhabi.
- Jul 2020. "Trustless Computing on Encrypted Data." National Cybersecurity Research and Development (NCR) Program, Singapore.
- Sep 2018. "High-Performance FV Somewhat Homomorphic Encryption on GPUs: An Implementation using CUDA." Conference on Cryptographic Hardware and Embedded Systems (CHES), Amsterdam. Recording available.

Skills

Cryptography and privacy. Classic cryptography (symmetric and asymmetric key cryptography, digital signatures, elliptic-curve cryptography, authentication, access control) in design, implementation and hardware acceleration; modern cryptography (lattice-based cryptography, fully homomorphic encryption, secure multi-party computation, post-quantum cryptography) in design, implementation and hardware acceleration; FHE schemes BFV, BGV, CKKS and TFHE; bootstrapping; threshold FHE; private information retrieval; private set intersection; differential privacy; federated learning; synthetic data; secure enclaves.

Applied cryptographic mathematics. Number theory; linear algebra; group, ring and field theory; digital arithmetic; residue number systems and multi-precision arithmetic; modern computer algebra (Discrete Fourier Transform, Number Theoretic Transform, Discrete Galois Transform, Chinese Remainder Theorem). *Tools:* Mathematica, SageMath.

Hardware acceleration and high-performance computing. Cryptographic accelerator architecture; ASIC hardware-software co-design; custom instruction set architecture and microcode scheduling; GPGPU programming (CUDA, OpenCL, multi-GPU clusters); FPGA design (High-Level Synthesis, VHDL); vectorization (SSE, SSE2, AVX2, AVX-512); multi-threading (OpenMP, Pthreads, NUMA). *Profiling:* Nsight Systems/Compute, nvprof, VTune, Intel Advisor, gprof, valgrind.

Machine learning and artificial intelligence. Privacy-preserving and trustworthy machine learning; supervised, unsupervised and deep learning; transformers and language models (BERT, GPT-2, LLaMA-3); NLP and text classification; computer vision; neural network families (MLP, SVM, CNN, RNN, LSTM, autoencoders, GANs); anomaly and intrusion detection; time-series analysis. *Tools:* PyTorch, TensorFlow, Keras.

Software engineering. C/C++ (14/17/20, STL), CUDA, Python (NumPy, Pandas, C extensions), Java, Assembly (x86/x64), VHDL, Matlab/Octave, Perl, PL/SQL and SQL; network programming (TCP/UDP sockets, SS7, CAMEL, Diameter, SIP); source code review, version control and collaborative development; build systems (make, CMake, GCC, clang, Intel Compiler). *FHE libraries:* OpenFHE, PALISADE, Microsoft SEAL, Intel HEXL, FIDESlib.

Analytical modeling and optimization. Roofline modeling; queueing theory for open and closed systems; capacity planning; convex, combinatorial, evolutionary and swarm optimization; backtracking and constraint-propagation search.

Research and programme management. Grant and proposal writing; intellectual property disclosures; project scoping, budgeting and scheduling (WBS, MS Project, ProjectLibre); technical writing for academic, legal and industry audiences; survey design and evidence synthesis; peer review.

Languages. English (full professional proficiency); Arabic (native proficiency).

Professional Service

Program and Organizing Committees

- ISPASS 2026. IEEE International Symposium on Performance Analysis of Systems and Software, Seoul.
- IVSP 2026. 8th International Conference on Image, Video and Signal Processing, Tokyo.
- WAHC 2025. 13th Workshop on Encrypted Computing & Applied Homomorphic Cryptography at ACM CCS, Taipei.
- IVSP 2025. 7th International Conference on Image, Video and Signal Processing, Kawasaki.
- WAHC 2023. 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography at ACM CCS, Copenhagen.
- ICBIP 2021. 6th International Conference on Biomedical Signal and Image Processing, Suzhou.

Journal Peer Review

- Reviewer for 26 scholarly journals, including *Journal of Cryptology*; IEEE *Transactions on Information Forensics & Security*; IEEE *Transactions on Dependable and Secure Computing*; IEEE *Transactions on Computers*; IEEE *Transactions on Computer-Aided Design of Integrated Circuits and Systems*; IEEE *Transactions on Parallel and Distributed Systems*; IEEE *Transactions on Pattern Analysis and Machine Intelligence*; ACM *Transactions on Privacy and Security*; *International Journal of Information Security*; *Artificial Intelligence Review*; *Journal of Medical Internet Research*; *Neural Computing and Applications*.

Standards and Community

- Co-author, "Building Blocks for Threshold FHE," submitted to the NIST Workshop on Multi-Party Threshold Schemes, 2023.

- Co-author and maintainer of OpenFHE (2022–present); contributor to PALISADE and Intel HEXL. Contributor to the OpenFHE Discourse forum, providing technical guidance to researchers and practitioners.
- Challenge designer for the FHERMA FHE challenge platform: "Ethereum Fraud Detection via SVM" and "House Price Prediction."
- Member, I2R Technical Expert Panel, A*STAR (2018–2021). ABET accreditation committee, Taif University (2011–2014).

Engagement Information

Services offered. Expert witness and litigation support: patent infringement and validity analysis, source code review, technical report preparation. Technical due diligence for investors and acquirers. Technical advisory. Executive briefings and professional training.