Habib Yajam

Tehran, Iran
+98 (938) 260 5725 • habib.yajam@gmail.com
Google Scholar: h-index 5, 85 citations
ORCiD: 0000-0003-4344-7446 • linkedin: habibyajam

Profile

I am a researcher passionate about building trustworthy digital systems. My work in applied cryptography sits at the intersection of theory and real-world impact, focusing on **privacy-enhancing technologies** like zero-knowledge proofs and **verifiable systems** such as blockchain consensus protocols. I thrive in **interdisciplinary** environments, having connected cryptography with AI (through federated learning) and economics (via game-theoretic analysis) to solve complex problems. My approach spans the entire research lifecycle—from drafting a security proof on paper to implementing robust protocols in Golang and Python. I enjoy the challenge of leading projects, whether in academia or industry, and am deeply committed to having a tangible, positive effect on society.

Research Interests

- Privacy-Preserving Cryptographic Protocols
- Zero-Knowledge Proofs and Verifiable Computation
- Cryptographic Protocol Design and Applied Cryptography
- Decentralized Trust and Digital Identity Systems
- Consensus Protocols and Scalable DLT Architectures
- Formal Security Modeling and Game-Theoretic Analysis.
- Interdisciplinary intersections of AI, Data Privacy, and Decentralized Systems

Education

University of Tehran **Tehran, Iran**
PhD in Telecommunication Engineering - Secure Communications, 19.45/20 *2015–2023*
Current area of research "Analysis and Improvement of Consensus Protocols in Blockchain Technology"

Sharif University of Technology **Tehran, Iran**
Master of Science in Telecommunication Engineering - Cryptography, 15.82/20 *2011–2013*
Thesis entitled "Analysis and Improvement of Secret Handshake Protocols"

Bahonar University of Kerman **Kerman, Iran**
Bachelor of Science in Electrical Engineering - Communication Eng., 16.01/20 *2006–2011*
Thesis entitled "Image Hash in Radon Transform Domain"

National Organization of Exceptional Talents **Kerman,Iran**
High School Diploma in Mathematics and Physics *2002–2006*

PhD Thesis

Title: *Analysis and Improvement of Scalable Consensus Protocols in Blockchain Technology*

Supervisor: MahammadAli Akhaee

Description: This thesis investigates the scalability of consensus algorithms in blockchain systems. It mathematically demonstrates the performance limitations of the "Tangle" protocol under high transaction loads. A modular simulation framework, "JABS," was developed to facilitate research and testing of various consensus mechanisms. Additionally, a novel protocol, "GhostBFT," was proposed—combining features of GHOST and BFT algorithms—to achieve asynchronous safety, leaderless operation, pipelining, and high transaction throughput.

Selected Publications

A complete publication list with 15+ papers is available via Google Scholar

JABS: A Blockchain Simulator for Researching Consensus Algorithms
IEEE Transactions on Network Science and Engineering *2023*
Habib Yajam, MohammadAli Akhaee

Abstract: The paper introduces JABS (Just Another Blockchain Simulator), a highly efficient and accurate simulator for researching large-scale blockchain consensus algorithms. JABS outperforms other frameworks in simulating real-world blockchain networks and enables the easy substitution of components due to its modularity.
doi: https://doi.org/10.1109/TNSE.2023.3282916

A Scalable Decentralized Privacy-preserving E-voting System based on Zero-Knowledge Off-Chain Computations
Journal of Information Security and Applications *2023*
Ashkan Emami, **Habib Yajam**, Mohammad Ali Akhaee, Rahim Asghari

Abstract: This paper introduces a unique, decentralized e-voting scheme that employs zero-knowledge off-chain computations to efficiently handle large-scale elections while maintaining a constant on-chain storage requirement.
doi: https://doi.org/10.1016/j.jisa.2023.103645

Federify: A Verifiable Federated Learning Scheme based on zkSNARKs and Blockchain
IEEE Access *2023*
Ghazaleh Keshavarzkalhori, Cristina Pérez-Solà, Guillermo Navarro-Arribas and Jordi Herrera-Joancomartí, **Habib Yajam**
Abstract: Federify is a decentralized federated learning framework based on blockchain that employs homomorphic encryption and zero knowledge proofs to provide security, privacy, and transparency. The scheme preserves the confidentiality of both the data used for training and the local models using homomorphic encryption.
doi: accepted waiting for publication

Analysis of IOTA Tangle Stability in High Transaction Rates
The ISC International Journal of Information Security (ISeCure) *2023*
Habib Yajam, Elnaz Ebadi, MohammadAli Akhaee

Abstract: This paper proves that the stability of the Tip Selection Algorithm (TSA) in IOTA's Tangle consensus mechanism, vital for processing high volumes of IoT transactions, depends on the probability of selecting all unconfirmed blocks (tips) being at least 1/(2n). It also highlights that the existing IOTA TSA may not maintain stability under high transaction rates.
doi: https://doi.org/10.22042/isecure.2023.380480.904

ZharfSima: Benchmarking Vision Language Models for Persian Language and Culture
2025 29th International Computer Conference, Computer Society of Iran (CSICC) *2025*
Ali Edalat, Hadi Kamkar, Amir Mohammad Rasekh Mehrabi, Sadjad Nojavan, Saeed Aghamiri, S. Mohammad Fakhraie, **Habibollah Yajam**, Mohammadsadegh Alizadeh
Abstract: This paper presents *ZharfSima*, the first benchmark for evaluating Vision-Language Models (VLMs) in Persian. It assesses models on reasoning, cultural understanding, and text generation, revealing key challenges in multimodal AI for low-resource languages.
doi: https://doi.org/10.1109/CSICC65765.2025.10967416

Improvements on Easypaysy: The Bitcoin's Layer-2 Accounts Protocol
2020 17th International ISC Conference on Information Security and Cryptology (ISCISC) *2020*
Elnaz Ebadi, **Habib Yajam**, MohammadAli Akhaee

Abstract: The paper proposes two enhancements to the Easypaysy protocol, a blockchain layer-2 system aimed at improving Bitcoin's user-friendliness and privacy. The first enhancement introduces a new payment type offering deniable authentication, while the second introduces a hierarchical account system.
doi: https://doi.org/10.1109/ISCISC51277.2020.9261905

Improvement on Bitcoin's Verifiable Public Randomness with Semi-Trusted Delegates
2018 9th International Symposium on Telecommunications (IST) *2018*
Habib Yajam, Elnaz Ebadi, MohammadTaghi Badakhshan, MohammadAli Akhaee

Abstract: The paper introduces a new scheme to enhance the security of Verifiable Public Randomness derived from any public blockchain. The scheme, based on Verifiable Secret Sharing protocols and Threshold Cryptosystems, utilizes semi-trusted third parties to protect against biases introduced by adversaries.
doi: http://dx.doi.org/10.1109/ISTEL.2018.8661008

Work Experience

ZharfaTech - Enterprise Generative AI Solutions **Tehran**
Co-Founder and CTO, https://www.zharfa.tech/ *2023–Present*
- Co-founded and scaled the startup from 5 to 40 employees, securing over 5 major contracts with government agencies and enterprises through direct client engagement and proposal development.
- Led R&D in generative AI, publishing research on Vision-Language Models while maintaining cutting-edge expertise through continuous team training and technology updates.
- Implemented agile project management methodologies to drive product development and ensure delivery of relevant, state-of-the-art AI solutions.
- Mentored and trained new employees, developing talent to meet evolving project requirements in fast-moving AI landscape.

Investech Venture Capital **Tehran**
DLT and Cyber Security Consultant, https://investech.fund/ *2023–Present*

- Evaluated blockchain and cybersecurity business proposals, providing technical due diligence and investment recommendations to guide venture funding decisions.
- Assessed technological viability and security postures of early-stage startups in decentralized systems and cybersecurity sectors.

Arg Group Industry Co. **Tehran**
Manager of Cryptographic Protocols R&D *2022–2024*

- Led a team of 6+ researchers and developers in cryptographic protocol design and implementation.
- Managed development of large-scale Certificate Authority system in Golang, from architecture to deployment.
- Gained extensive experience with GPU clusters and HPC, sparking interest in computational requirements of generative AI.

Muon Network Open-Source Project **Remote**
Cryptography and Security Advisor, https://www.muon.net/ *2022–2024*

- Conducted security audit of threshold signature protocol, identifying critical vulnerability and designing a secure concurrent implementation fix.
- Gained deep experience in open-source community dynamics and decentralized project security challenges.

Ministry of ICT Research Institute **Tehran**
Blockchain and DLT Consultant, https://en.itrc.ac.ir/ *2018–2019*

- Served as sole PhD-level technical consultant on national blockchain regulatory framework project.
- Conducted comprehensive analysis of diverse blockchain platforms and cryptocurrencies to inform government policy and regulation.

Arg Group Industry Co. **Tehran**
Cryptography Researcher and Back-end Programmer *2016–2022*

- Developed and analyzed security protocols, gaining hands-on experience in cryptographic implementation and assessment.
- Built foundation in practical cryptography that informed later leadership roles and research directions.

Technical Skills

Programming: Golang, Python, C, CUDA, MATLAB

Blockchain/DLT: Solidity, Hyperledger Fabric; Consensus Protocols, DLT Architecture

Tools & Platforms: Docker, Linux, CUDA, LaTeX

Cryptographic Expertise: Zero-Knowledge Proofs (zkSNARKs), MPC, Identity-Based Cryptography, Protocol Design & Analysis

Academic Service

Reviewer of The ISC International Journal of Information Security **Tehran**
iSecure Journal, https://www.isecure-journal.com/reviewer?_action=info *2021–2025*

Executive Committee Member in Hyperledger Workshop **Tehran**
University of Tehran *May 2018*

Executive Committee Member in Code-based Cryptography Workshop **Tehran**
Sharif University of Technology, http://ee.sharif.edu/~code/ *May 2015*

Executive Committee Member in Lattice-based Cryptography Workshop **Tehran**
Sharif University of Technology, http://ee.sharif.edu/~lattice/ *May 2014*

Executive Committee Member in Security Protocols Formal Modeling Workshop **Tehran**
Sharif University of Technology *Feb 2013*

Standardized Test Scores

TOEFL
Total Score: 109/120 *Jun 2014*

- Reading: 28/30
- Listening: 30/30
- Speaking: 24/30
- Writing: 27/30

GRE
Score: 319 *Oct 2014*

- Verbal Reasoning: 152 (54%)
- Quantitative Reasoning : 167 (94%)
- Writing: 3.0

Languages

English: Professional Working Proficiency *TOEFL:109/120*

Persian: Native Language

Certifications

Cryptography I **Coursera.org**
http://www.coursera.org/course/crypto *December 2012*

CS191x Quantum Mechanics and Quantum Computation **edX.org**
https://verify.edx.org/cert/240016ff63094c9b899f0dde61e01e2a *April 2013*

Other Interests

hobbies: Hiking, Mountaineering, Photography, Amateur Astronomy

References

- Dr. Mohammad Ali Akhaee `akhaee@ut.ac.ir`
- Dr. Mahmoud Salmasizadeh `salmasi@sharif.edu`
- Dr. Taraneh Eghlidos `teghlidos@sharif.edu`