

# Mohammad Ferry Husnil Arif

✉ ferryhusnil07@gmail.com    🌐 swusjask.github.io    🌐 mohammad-ferry-husnil-arif    🌐 swusjask

## Education

---

Universitas Indonesia

Aug 2021 – July 2025

BSc in Computer Science

- **CGPA:** 3.93 / 4.00 (8th semester)
- **Thesis:** KZG Polynomial Commitment Scheme on zk-SNARKs Construction and Its Implementation. Supervised by Lim Yohanes Stefanus. [Paper](#) [Slides](#)
- **Relevant Coursework:** Cryptography & Information Security, Algorithms Design & Analysis, Data Structures & Algorithm, Discrete Mathematics, Linear Algebra, Statistics & Probability, Operating Systems, Computer Networks

## Publications

---

**On the Classical Hardness of the Semidirect Discrete Logarithm Problem in Finite Groups**

Aug 2025

M.F.H. Arif, M. Imran

[arxiv.org/abs/2508.05048](https://arxiv.org/abs/2508.05048) (Accepted at Indocrypt 2025)

## Selected Achievements

---

- #82 Global / #3 Indonesia ranking on [CryptoHack](#) (Current)
- Third Prize in International Mathematics Competition 2024 (IMC, Aug 2024)
- Honorable Mention in International Olympiad in Cryptography 2024 (NSUCRYPTO, Oct 2024)
- Honorable Mention in ONMIPA-PT 2024, Mathematics (Ministry of Education, May 2024)
- 2nd Place in Cyber Jawa 2024 Open Category (CSIRT and IdNSA, Feb 2025)
- 2nd Place in ISITDTU CTF 2024 (Duy Tan University, Vietnam, Dec 2024)
- 2nd Place in National Cyber Week 2023 CTF (Binus University, Dec 2023)

## Experience

---

**Backend & AI Engineer**

Jakarta (Remote)

Veritask

May 2025 – present

- Developed [Veritask](#) platform, a legal compliance management system for companies, utilizing FastAPI for the backend.
- Integrated AI agent with LangChain/LangGraph to enable chatbot capabilities for retrieving relevant regulations, conducting web searches, and integrating company compliance data.
- Designed and implemented RAG (Retrieval-Augmented Generation) pipeline with vector database for efficient semantic search and document retrieval.
- Processed over 100,000+ raw PDF regulatory documents through OCR, cleaning, formatting, and summarization.
- Implemented Celery-based distributed task queue for document processing and long-running operations

**Teaching Assistant**

Depok, West Java, Indonesia

Universitas Indonesia

sia

Aug 2022 – May 2024

- Cryptography & Information Security (Jan–May 2024)
- Numerical Analysis (Aug–Dec 2023)

- Statistics & Probability (Aug–Dec 2022)

## Projects

---

### [kzg-snark](#) (Thesis Implementation)

2024-2025

- Implemented KZG polynomial commitment scheme for zk-SNARKs (Marlin and PLONK protocols) in Python/SageMath, including complete prover/verifier workflows.

## Non Degree Academic Programs

---

- [CIMPA Research School: Arithmetic in Action](#) (July 14-25, 2025): Number Theory and its Applications to Cryptography and Coding Theory. Hosted by Gadjah Mada University, Yogyakarta, Indonesia.
- [QWorld: Fundamentals of Quantum Computing & Programming](#) (Sep-Dec 2024): 3 ECTS undergraduate course covering quantum systems, entanglement, quantum protocols, and Bloch sphere. Organized by QWorld in collaboration with University of Latvia and Unitary Fund.