Mamun R. Akand

mamun@mamunakand.ca | 403-499-9267 | mamunakand.ca | Waterloo, ON

Work Experience

Huawei Technologies Canada

*Huawei is a **Fortune 500** global ICT leader with **$100B+** in annual revenue and operations in **170+** countries.*

Security Research Engineer **Nov. 2022 - Present**

- Cut decryption key size by **60%+** and reduced complexity from **O(N) to O(1)** by leading design of a scalable **encryption** scheme for multi-recipient secure file sharing; **mentored** 4 engineers and **partnered** with product for secure integration.
  - **Stack**: *C++ | Pairing-based cryptography (MCL) | Linux (Ubuntu) | Git | Valgrind (benchmarking) | GoogleTest*
- Reduced insider leak investigation time and storage footprint by delivering **forensic watermarking** and **tamper-evident metadata chaining** systems for enterprise **DLP**, seamlessly integrated into production workflows.
  - **Stack**: *C++ | OpenSSL | Linux (Ubuntu) | Git | Docker*
- Eliminated uniform-share weaknesses and lowered insider collusion risk by introducing **dynamic, risk-based** weights in a **weighted secret sharing** framework; **managed** 3-engineer team and integrated solution into product line.
  - **Key Results**: Incorporated **MCDM** scoring to adjust shares in real time based on device trust posture; applied **threat modeling** and a full **cryptographic refactor** while preserving **O(1)** reconstruction performance.
  - **Stack**: *C++ | OpenSSL | Linux (Ubuntu) | Git | MCDM-AHP (decision scoring) | Valgrind (benchmarking) | GoogleTest*
- Drove **AI security** research securing both **local AI models** and **agentic systems** against extraction, inversion, tampering, **data poisoning**, backdoors, and **prompt injection**.
  - **Key Results**: Built agentic **threat taxonomy** (perception, cognition, memory, action); evaluated defenses including **TEE**, privacy-preserving inference, and tamper-resistant deployment; proposed new R&D project on secure model delivery.
- Reduced manual analysis time for academic conferences by **50%+** through an **AI research assistant** pipeline that surfaces goal-aligned research, extracts key technologies, identify research-gaps, and auto-generates professional reports/presentations.
  - **Stack**: *Python | LangChain | LangGraph | Ollama | Docker | Git | Confluence*
- Developed **Privacy-Preserving AI Proxy (PPAP)**, a modular reverse proxy that strips **PII** from user prompts before routing to on-prem/cloud LLMs.
  - **Key Results**: Reduced data leakage risk; integrated deterministic redaction (**Microsoft Presidio** + **spaCy**) with context-aware masking using **TinyLlama** & **Mistral**; containerized for self-service deployment.
  - **Stack**: *FastAPI | Python | Microsoft Presidio | spaCy | TinyLlama | Mistral | Ollama | Docker*

University of Calgary

*The University of Calgary is a leading Canadian research university, consistently ranked among the **top 10** in Canada.*

Research & Teaching Assistant **Sep. 2014 - Apr. 2023**

- Researched **anonymous credentials**, **zero-knowledge proofs**, and **blockchain-based identity systems** (Sovrin, Namecoin), as well as **Ethereum**-based **FOAM** for secure location proofs.
- Built secure Android proof-of-concepts using **IBM Idemix** and region-based verifiers; strengthened geo-tamper resistance in protocol design; achieved **96.4% location verification** accuracy with cryptographic **distance bounding**.
- Published in top-tier venues (**IEEE TDSC**, **ACM CCS**, **ACNS**, **ACISP**, **IEEE Access**); presented at major security conferences.
- Taught and supported undergraduate courses in cryptography; delivered tutorials and labs on **number theory**, **information theory**, and applied cryptographic principles to classes of **40+** students, improving comprehension through hands-on exercises.
- **Stack**: *Java (Android) | MATLAB | IBM Idemix | OpenSSL | Linux (Ubuntu) | Git | LaTeX*

Education

Ph.D., Computer Science, University of Calgary, *Calgary, AB* **Apr. 2023**

M.Sc., Computer Science, University of Calgary, *Calgary, AB* **Sep. 2016**

Skills

Programming: C++, Java (Android), Python, Bash
Cryptography: OpenSSL, Pairing-based crypto (MCL), IBM Idemix, Zero-Knowledge Proofs
AI/LLM: LangChain, LangGraph, Ollama, TinyLlama, Mistral, Microsoft Presidio
Secure Systems: Attribute-Based Encryption, Weighted Secret Sharing, TEE, Secure File Sharing, Threat Modeling, DLP
DevOps: Docker, Git, Valgrind, GoogleTest
Documentation: LaTeX, Confluence, Markdown