Amina Bassit

Privacy-preserving Machine Learning Postdoctoral Researcher at MSU
Ph.D. in ML-based Biometrics and Applied Cryptography | EAB Industry Award 2024 Winner

bassitam@msu.edu | github.com/aminabassit | linkedin.com/in/amina-bassit-1197681b1/ | Amina Bassit

Personal Profile

With over 8 years of experience, my career has been dedicated to integrating advanced machine learning and applied cryptography to design scalable, secure, and privacy-preserving solutions that build trust in AI technologies for both users and service providers. As AI technologies continue to evolve, my research mission is to ensure that they remain aligned with our core human values, preserving our fundamental rights in the digital world and protecting the intellectual properties of business owners. Specifically, I designed provably secure fully homomorphic encryption (FHE) based solutions for large-scale embedding search (filed a patent application and won the EAB Industry Award 2024) and data-and-circuit privacy (developed as PrivaCT, which operates in constant time). I am committed to designing privacy-preserving solutions for AI technologies that are not only provably secure but also verifiable, ensuring accountability for all stakeholders.

Experiences

Postdoctoral Researcher
May 2024 - Current

Human Analysis Lab - Michigan State University
East Lansing, MI, United States

- **Research mission:** Designing privacy-preserving machine learning solutions that are provably secure using applied cryptography and promoting awareness, through tutorials, on the critical importance of ensuring AI technologies are secure and privacy-compliant to utilize.
- **Accomplished projects:**
  - **SecureRAG** an end-to-end secure RAG framework that enforces access control over retrieved documents while preventing prompt injection data extraction and embedding inversion attacks.
  - **PrivaCT** an FHE-based solution that protects the privacy of both data and circuit (e.g., proprietary model) and runs in constant time.
  - **Tutorial IJCB 2024** Biometric Privacy and Security with hands-on session `https://biometric-privacy-security.github.io/`

Doctoral Researcher
May 2020 - Apr 2024

DMB and SCS groups - University of Twente
Enschede, Netherlands

- **Accomplished research mission:** Developed privacy-preserving solutions to integrate deep learning-based biometric recognition systems with homomorphic encryption that are provably secure against semi-honest and malicious adversaries.
- **Outcomes:** Contributed to over 10 peer-reviewed publications in journals and conferences, filed 3 patent applications, and won 2 awards.
- **Teaching Assistance:** Secure Data Management Master course.
- **Co-supervision:** Master thesis of Martijn P. de Vries on 'Private Information Retrieval applied to Biometric Verification' in 2022.

Visiting Doctoral Researcher
Oct 2022 - Jan 2023

Mobai - a SaaS-based biometric technology Company
Gjøvik, Norway

- **Description:** Knowledge transfer of our solution entitled "Multiplication-Free Biometric Recognition for Faster Processing under Encryption" to help Mobai adapt our solution to their products and accompanied Mobai to deploy our solution in their product. This resulted in the collaboration on a joint patent. Filing this patent is a work in progress.

Visiting Doctoral Researcher
May 2022 - Jul 2022

Secunet Security Networks AG - Division Homeland Security
Essen, Germany

- **Description:** Design of a multi-modality biometric fuzzy vault scheme to address the unbalanced modalities problem.

Visiting Doctoral Researcher
Nov 2021 - Jan 2022

Norsk Regnesentral (NR)
Oslo, Norway

- **Description:** Interdisciplinary collaboration with an ESR fellow on privacy analysis of biometric authentication methods.

Applied Cryptography Researcher
Jun 2019 - Apr 2020

DMB and SCS groups - University of Twente
Enschede, Netherlands

- **Accomplished research project:** OBRE: Optimal Biometric Recognition under Encryption
- **Description:** This was a joint project between the University of Twente and GenKey B.V. where I designed a biometric verification system in the encrypted domain using additively homomorphic ElGamal secure against malicious adversaries. I implemented its proof-of-concept in C++ and studied its log-likelihood ratio-based biometric recognition model in Python.

Applied Cryptography Engineer *Apr 2016 - May 2019*

Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) *Rabat, Morocco*

- **Accomplished projects:** Implementation of a C Cryptographic Library and Cryptographic algorithm validation tests.
- Conducted training sessions in symmetric cryptography, digital signatures, and pseudorandom generators (PRGs).

Applied Cryptography Engineer - Internship *Mar 2015 - Sep 2015*

R&D Worldline - Secure payment solutions *Lille, France*

- **Description:** Design and implementation of a cryptographic group signature scheme as a solution that enables pseudo-anonymous users belonging to a group to authenticate without revealing their identities and merely by proving their membership to the group.

Education

Ph.D. in ML-based Biometric Recognition and Applied Cryptography *May 2020 - Apr 2024*

DMB and SCS groups - University of Twente *Enschede, Netherlands*

- **Ph.D. thesis:** Fast and Accurate Biometric Search under Encryption
- **Ph.D. defence date:** December 15th, 2023.
- **Ph.D. project:** Integration of ML-based Biometric Recognition and Homomorphic Encryption.
- **Description:** This Ph.D. is part of the PriMa (Privacy Matters) project funded by Marie Skłodowska-Curie grant agreement No. 860315. Investigated the integration of deep learning-based biometric recognition with homomorphic encryption to achieve efficient and accurate biometric recognition solutions in the encrypted domain that are privacy-preserving and secure against semi-honest and malicious adversaries.

Dual Master's Degree in Cryptography and Information Security *Sept 2013 - Sept 2015*

C2SI (Mohammed V University) and CRYPTIS (Limoges University) *Morocco and France*

- **Final project:** Designed and implemented a cryptographic group signature scheme for anonymous authentication.

Bachelor's Degree in Discrete Mathematics *Sept 2010 - Jun 2013*

Hassan II University *Casablanca, Morocco*

- **Final project:** Research paper on finite field theory focusing on Galois fields.

Patent Applications

1st Patent	Fast and accurate biometric comparator under encryption. Filed on Sep 15th, 2023, by the University of Twente.
2nd Patent	Fast and accurate biometric search under encryption. Filed on Sep 15th, 2023, by the University of Twente.
3rd Patent	Fast and accurate biometric verification under encryption for mobile devices. In the process of filing jointly between Mobai and the University of Twente.

First Author Publications

IEEE TIFS	Fast and Accurate Likelihood Ratio-Based Biometric Verification Secure Against Malicious Adversaries. (2021)
BIOSIG 2021	Bloom Filter vs Homomorphic Encryption: Which approach protects the biometric data and satisfies ISO/IEC 24745? (2021)
IET Biometrics	Hybrid Biometric Template Protection: Resolving the Agony of Choice between Bloom Filters and Homomorphic Encryption (2022)
IJCB 2022	Multiplication-Free Biometric Recognition for Faster Processing under Encryption (2022)
IJCB 2023	Template Recovery Attack on Homomorphically Encrypted Biometric Recognition Systems with Unprotected Threshold Comparison (2023)
IEEE T-BIOM	Improved Multiplication-Free Biometric Recognition for Faster Processing under Encryption (2023)
IEEE T-BIOM	Practical Biometric Search under Encryption: Meeting the NIST Runtime Requirement without Loss of Accuracy (2025)
Frontiers	Template Recovery Attack on Encrypted Face Recognition Systems with Unprotected Decision using Synthetic Faces (2025)

Remaining Publications

BIOSIG 2021	Transferability Analysis of Adversarial Attacks on a Gender Classifier to Face Recognition. (2021)
IET Biometrics	Transferability Analysis of Adversarial Attacks on a Gender Classifier to Face Recognition: Fixed and Variable Attack Perturbation (2022)
BIOSIG 2023	Remote Cancelable Biometric System for Verification and Identification Applications (2023)
BIOSIG 2024	A Study on the Next Generation of Digital Travel Credentials (2024)

Services

Program Chair	IWBF 2025
Special Session Co-org	EUSIPCO 2025: Trustworthy Biometrics
Journal Reviewer	IEEE TIFS, IEEE T-BIOM, IJIS, VCJ
Conference Reviewer	PoPETs, BIOSIG, IJCB, IWBF

Awards

2024	**EAB Industry Award 2024,** Ph.D. dissertation - Fast and Accurate Biometric Search under Encryption.	*Germany*
2021	**Best Paper Award BIOSIG 2021,** BF vs HE: Which approach protects the biometric data?	*Germany*
2015	**Regional Academic Award of Master Student's Excellence,** Mohammed V University	*Morocco*
2013	**Regional Academic Award of Bachelor Student's Excellence,** Hassan II University	*Morocco*

Skills

Languages	C, C++, Python, and Matlab.
Research Skills	Establishement of original research, understanding and formulation of research problems, innovative problem-solving.
General skills	Polyglot (English, French, Arabic), fast learner and detail-oriented, interpersonal skills, highly organized and ethical.

Disseminations

Girls Day 2023	Invented a card game called *Find my match* that teaches young girls the basics of face recognition and encryption.
1st PriMa Blog post	Hello, device! Can you recognize me without violating my privacy? (2022)
2nd PriMa Blog post	A Reflection on Privacy, Security, and Anonymity in the Context of Biometrics. (2023)

References

dr. Vishnu Naresh Boddeti	vishnu@msu.edu
prof.dr.ir. Raymond Veldhuis	r.n.j.veldhuis@utwente.nl
prof.dr. Andreas Peter	andreas.peter@uol.de
dr.ing. Florian Hahn	f.w.hahn@utwente.nl