MONIKA TRIMOSKA

Temporary Research and Teaching Assistant (ATER)

@ monika.trimoska@u-picardie.fr +33789922644 github.com/mtrimoska mtrimoska.com

EDUCATION AND QUALIFICATIONS

Qualification for a position as an assistant professor at a French University

by the French National Council of Universities
Section: Computer Science (27), Qualification number: 21227354085

19 February 2021

PhD in Computer Science - Combinatorics in Algebraic and Logical Cryptanalysis

University of Picardie Jules Verne, France

October 2017 – January 2021

Master's Degree in Information Systems and Network Security

University of Picardie Jules Verne, France

September 2015 – August 2017

Licence (BSc equivalent) in Computer Science

University of Picardie Jules Verne, France

September 2012 – August 2015

EMPLOYMENT / RESEARCH EXPERIENCE

Temporary Research and Teaching Assistant (ATER)

Faculty of Science, University of Picardie Jules Verne

September 2020 – Present Amiens, France

Studying the use of SAT solving techniques for the MQ problem as part of the ANR project POSTCRYPTUM lead by Sorina Ionica. In addition, I have teaching duties at the Department of Computer Science.

Teaching Assistant

Faculty of Science, University of Picardie Jules Verne

January 2018 – August 2020 Amiens, France

Teaching undergraduate courses.

R&D engineer

SATT Nord

September 2016 – September 2017 Amiens, France

Working on CrypTonAuth, a novel authentication method.
Contributions and experience:

- Developing the proof-of-concept and implementations on different platforms (UNIX PAM module, web, Bluetooth communication microcontroller - Arduino).
- Developing a C library for ANSSI standardisation.
- Research valorisation.

Research Intern

MIS Laboratory, University of Picardie Jules Verne

November 2015 – August 2016 Amiens, France

Security analysis of elliptic curve based cryptosystems. More precisely, I worked on a parallel version of Pollard's rho collision search algorithm.
Contributions:

- Proposing an alternative memory structure, which yields a better memory complexity.
- Obtaining a better bound for the time complexity.

PUBLICATIONS

Journal papers and international conferences:

Logical cryptanalysis with WDSat
Monika Trimoska, Gilles Dequen, Sorina Ionica
In: Li CM., Manyà F. (eds) Theory and Applications of Satisfiability Testing – SAT 2021. SAT 2021
Lecture Notes in Computer Science, vol 12831. Springer, Cham
doi: 10.1007/978-3-030-80223-3_37

Time-Memory Analysis of Parallel Collision Search Algorithms
Monika Trimoska, Sorina Ionica, Gilles Dequen
IACR Transactions on Cryptographic Hardware and Embedded Systems - TCHES, Volume 2021, Issue 2
doi: 10.46586/tches.v2021.i2.254-274

Parity (XOR) Reasoning for the Index Calculus Attack
Monika Trimoska, Sorina Ionica, Gilles Dequen
In: Simonis H. (eds) Principles and Practice of Constraint Programming. CP 2020.
Lecture Notes in Computer Science, vol 12333. Springer, Cham.
doi: 10.1007/978-3-030-58475-7_45

A SAT-Based Approach for Index Calculus on Binary Elliptic Curves
Monika Trimoska, Sorina Ionica, Gilles Dequen
In: Nitaj A., Youssef A. (eds) Progress in Cryptology - AFRICACRYPT 2020. AFRICACRYPT 2020.
Lecture Notes in Computer Science, vol 12174. Springer, Cham.
doi: 10.1007/978-3-030-51938-4_11

Book chapters:

HappyKidz: Privacy Preserving Phone Usage Tracking
Benjamin M. Case, Marcella Hastings, Siam Hussain, Monika Trimoska
In: Lauter K., Dai W., Laine K. (eds) Protecting Privacy through Homomorphic Encryption
link: https://www.microsoft.com/en-us/research/event/private-ai-bootcamp/#!tech-reports
to appear in August 2021, doi: 10.1007/978-3-030-77287-1

TALKS

A SAT-based approach for index calculus on binary elliptic curves

Arithmetic, Geometry, Cryptography and Coding Theory Conference

1 June 2021 — online (CIRM, Marseille Luminy, France)

Logical cryptanalysis of the ECDLP

Seminar at Inria Nancy

12 March 2021 — online (INRIA Nancy)

Index calculus for elliptic curves defined over extension fields

Arithmetic and Information Theory Seminar

18 February 2021 — online (University Aix-Maseille)

Parity (XOR) Reasoning for the Index Calculus Attack

CP 2020

9 September 2020 — online (Louvain-la-Neuve, Belgium)

A SAT-based approach for index calculus on binary elliptic curves

IMACC 2019

17 December 2019 — St Anne's College, University of Oxford, Oxford, UK

A SAT-based approach for index calculus on binary elliptic curves

Seminar at the Microsoft Reasearch Lab

5 December 2019 — Microsoft Research, Redmond, Washington, USA

HappyKidz: Privacy Preserving Phone Usage Tracking

Private AI Bootcamp Competition 2019

4 December 2019 — Microsoft, Redmond, Washington, USA

Analysis of the hardness of cryptosystems using the minimal vertex cover problem

Journée des Jeunes Chercheurs du MIS 2019

5 July 2019 — Amiens, France

A SAT-based approach for index calculus on binary elliptic curves

Seminar at Groupe de Travail "Butte aux Cailles"

16 May 2019 — l'ENST (Télécom ParisTech), Paris, France

Time-Memory Trade-offs for Parallel Collision Search Algorithms

Journées Codage & Cryptographie 2018

11 October 2018 — CAES du CNRS, Aussois, France

Logical cryptanalysis of the discrete log problem

Journée des Jeunes Chercheurs du MIS 2018

29 May 2018 — Amiens, France

A new OTP-based authentication scheme

Journées Réseaux de l'Enseignement et de la Recherche 2017

15 November 2017 — Nantes, France

CrypTonAuth authentication protocol

Journée des Jeunes Chercheurs du MIS 2017

30 May 2017 — Amiens, France

TEACHING EXPERIENCE

Object-oriented programming 2 and Reactive programming

Third year - lectures, tutorials and laboratory work

Advanced algorithms

Second year - tutorials and laboratory work

C programming

Second year - laboratory work

Propositional logic

First year - tutorials and laboratory work

Algorithms and programming

First year - tutorials and laboratory work

Elements of formal logic and mathematical reasoning

First year - tutorials

Introduction to databases

First year - tutorials and laboratory work

Introduction to programming

First year - tutorials and laboratory work

Internet and web

First year - tutorials and laboratory work

STUDENT SUPERVISION

Master internship

MIS Laboratory, University of Picardie Jules Verne

February 2020 – July 2020 — Amiens, France

Ambroise Fleury
M2 internship (6 months)
Parallel collision search on multiple users

Undergraduate internship

MIS Laboratory, University of Picardie Jules Verne

June 2017 – July 2017 — Amiens, France

Florian Saby

L3 internship (2 months)
OTP authentication application

SOFTWARE

WDSat
A SAT solver dedicated to solving instances derived from a Weil descent.
https://github.com/mtrimoska/WDSat

PCS - Published as TCHES 2021 Artifact
Implementation of a Parallel Collision Search algorithm for solving the ECDLP.
https://artifacts.iacr.org/tches/2021/a10/

Weil descent
A Weil descent implementation for binary elliptic curves over prime-degree extension fields.
https://github.com/mtrimoska/EC-Index-Calculus-Benchmarks

CrypTonAuth
A C library for implementing the CrypTonAuth authentication method, submitted to ANSSI standardisation.
(Proprietary software)

CrypTonID
A C library for implementing the CrypTonID hashed data retrieval technology , submitted to ANSSI standardisation.
(Proprietary software)

PRIZES AND DISTINCTIONS

- I was part of the winning team of the Private AI Bootcamp organised by Microsoft Research (December 2019, Seattle, US).

RESPONSIBILITIES

- I was a student member of the Research Committee of the University of Picardie Jules Verne from April 2018 to March 2020.
- I was part of the Organising Committee of the Young Researchers of MIS Day 2019.
- I am/was an external reviewer for Crypto 2019, SAT 2021 and Latincrypt 2021
- I was involved in the organisation of the JFPC/JIAF 2018 event (National Constraint Programming Days in France / National Artificial Intelligence Days in France).
- I animated, with Sorina Ionica, a laboratory visit for primary school students who have participated in the Alkindi cryptography competition.

LANGUAGES

English
(TOEIC) - 980/990, Cambridge First Certificate in English

French
Bilingual

Macedonian
Native

TECHNICAL (IT) SKILLS

C | Shell-script | JAVA | RxJAVA | Python | OpenMP | HTML | CSS | JavaScript | PHP | MySql | Linux System Administration

REFERENCES

Gilles Dequen
Professor, University of Picardie Jules Verne
gilles.dequen@u-picardie.fr

Sorina Ionica
Associate Professor, University of Picardie Jules Verne
sorina.ionica@u-picardie.fr