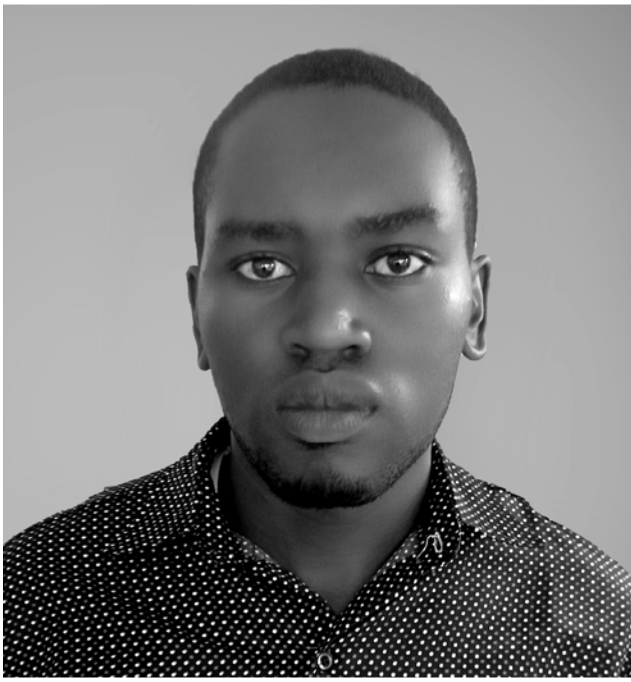
EPFL

UM6P
University
Mohammed VI
Polytechnic

Initiative
Excellence
in Africa
100 PhDs
for Africa

Gustave TCHOFFO SAAH

University of Bamenda, Cameroon



Research field

Cybersecurity

PhD title

Arithmetic of algebraic curves and post quantum cryptography

Keywords

- Isogeny
- Post quantum cryptography
- Supersingular elliptic curve
- Higher dimension isogeny

Summary

The aim of cryptography is to ensure the information confidentiality, undeniability and data integrity. Modern cryptographic protocols are based on pairs (public key, private key), a public key being linked to the associated private key by mathematical properties. For such a protocol to be secure, it must be difficult to find the private key from its public key. In this thesis, we are interested in protocols for which finding a private key from the associated public key involves computing an isogeny between two elliptic curves. More precisely, we study the arithmetic of algebraic curves in a general way with their impacts on the security of protocols based on isogeny computation.

Supervisor
Prof. Emmanuel FOUOTSA
University of Bamenda, Cameroon

Co-supervisor
Prof. Serge VAUDENAY
EPFL