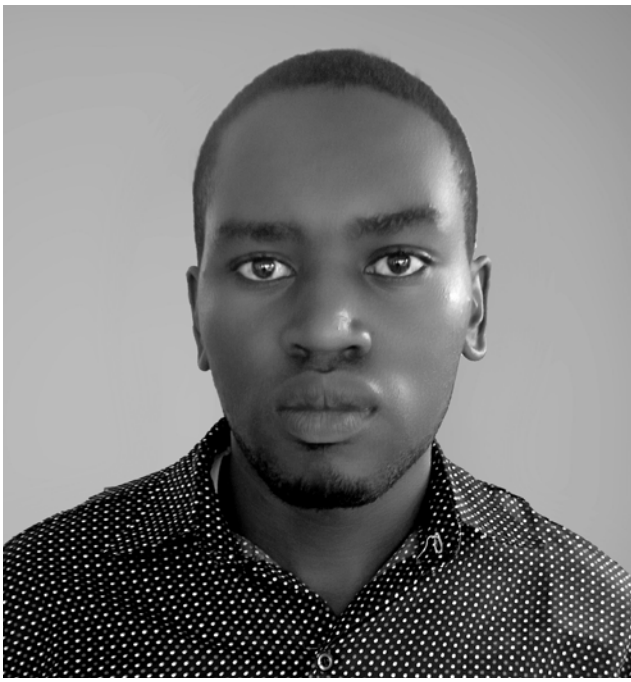
Initiative
Excellence
in Africa
100 doctorats
pour l'Afrique

University
Mohammed VI
Polytechnic

Gustave TCHOFFO SAAH

University of Bamenda, Cameroun



Domaine de recherche
Cybersécurité

Titre du doctorat
Arithmétique des courbes algébriques et cryptographie post-quantique

Mots-clés
- Isogenie
- Cryptographie post-quantique
- Courbe elliptique supersingulière
- Isogenie de dimension supérieure

Résumé

L'objectif de la cryptographie est d'assurer la confidentialité des informations, l'indéniable et l'intégrité des données. Les protocoles cryptographiques modernes reposent sur des paires (clé publique, clé privée), une clé publique étant liée à la clé privée associée par des propriétés mathématiques. Pour qu'un tel protocole soit sécurisé, il doit être difficile de trouver la clé privée à partir de sa clé publique. Dans cette thèse, nous nous intéressons aux protocoles pour lesquels trouver une clé privée à partir de la clé publique associée implique le calcul d'une isogenie entre deux courbes elliptiques. Plus précisément, nous étudions l'arithmétique des courbes algébriques de manière générale et leur impact sur la sécurité des protocoles basés sur le calcul d'isogenies.

Directeur de thèse
Prof. Emmanuel FOUOTSA
University of Bamenda, Cameroun

Co-directeur de thèse
Prof. Serge VAUDENAY
EPFL