AVIS DE SOUTENANCE DE THESE

Le Doyen de la Faculté des Sciences Dhar El Mahraz –Fès – annonce que

Mr **ASSOUJAA Ismail**
Soutiendra : **le Samedi 27/09/2025** à **10H00**
Lieu : ***Centre des Etudes Doctorales - USMBA – Amphi 1***

Une thèse intitulée :

« Pairing based cryptography »

En vue d'obtenir le ***Doctorat***

FD : ***Mathématiques et Applications***
Spécialité : **Algèbre**

Devant le jury composé comme suit :

Nom et prénom	Etablissement	Grade	Qualité
KADAOUI ABBASSI Mohamed Tahar	Faculté des Sciences Dhar EL Mahraz, Fès	PES	Président
BEN-AZZA Hussain	Ecole Nationale Supérieure d'Arts et Métiers, Meknès	PES	Rapporteur
SAHMOUDI Mohammed	Faculté des Sciences, Meknès	MCH	Rapporteur
BEN ABBOU Rachid	Faculté des sciences et techniques, Fès	PES	Rapporteur
CHILLALI Abdelhakim	Faculté Polydisciplinaire, Taza	PES	Examinateur
ELFADIL Lhoussain	Faculté des Sciences Dhar EL Mahraz, Fès	PES	Examinateur
MOUANIS Hakima	Faculté des Sciences Dhar EL Mahraz, Fès	PES	Co-directeur de thèse
EZ-ZOUAK Siham	Faculté des Sciences Dhar EL Mahraz, Fès	MCH	Directeur de thèse

Résumé :

La cryptographie, l'art et la science de la communication sécurisée, a longtemps été utilisée pour protéger les échanges confidentiels entre des parties comme Alice et Bob, en présence d'un adversaire, Eve. Au fil du temps, la cryptographie a évolué pour répondre aux besoins de services de sécurité critiques, tels que la confidentialité, l'authentification, l'intégrité et la non-répudiation. Parmi les techniques cryptographiques émergentes, la cryptographie basée sur l'appariement (Pairing-Based Cryptography, PBC) se distingue comme un protocole puissant qui exploite des couplages bilinéaires et non dégénérés sur des courbes elliptiques. Ces propriétés rendent la PBC particulièrement efficace dans les applications cryptographiques modernes. Depuis les années 1990, la PBC a suscité un intérêt considérable dans le domaine de la cybersécurité, avec de nombreuses études proposant des méthodes novatrices pour renforcer la sécurité et la confidentialité.

Cette thèse contribue au développement de la PBC en présentant trois avancées majeures. Tout d'abord, le protocole traditionnel d'échange de clés Diffie-Hellman est étendu pour prendre en charge des environnements multi-utilisateurs. Nous introduisons une nouvelle approche qui intègre des mécanismes de points aléatoires et un double chiffrement pour améliorer la sécurité. Ces innovations permettent de remédier aux vulnérabilités courantes, telles que les attaques de type homme du milieu (MITM) et les attaques par canaux auxiliaires, en offrant un protocole d'échange de clés plus résistant, adapté aux scénarios multi-utilisateurs. Ensuite, nous nous concentrons sur les techniques de compression de points sur les courbes elliptiques dans des champs de caractéristiques variées (2, 3, et différentes de 2 et 3). En développant de nouveaux algorithmes de compression pour les coordonnées Affine, Jacobienne, Projective, Edwards et Montgomery, nous obtenons une réduction de 17% à 50% de l'utilisation de la mémoire sans sacrifier la précision des calculs. Ces méthodes améliorent l'efficacité de la cryptographie sur les courbes elliptiques et offrent une analyse comparative des différentes caractéristiques de champs. Enfin, nous explorons la technique de construction par tour pour des champs avec des degrés de plongement de la forme 2i:3j . En optimisant les opérations arithmétiques sur les courbes elliptiques avec des degrés d'incorporation plus élevés et en utilisant des twists de degré 2 et 3, nous réduisons considérablement le coût computationnel des opérations. Nos résultats contribuent à des implémentations de la PBC plus efficaces et sécurisées. Grâce à ces contributions, cette thèse fait progresser la cryptographie basée sur les couplages en améliorant à la fois la sécurité et l'efficacité computationnelle, en apportant des solutions pratiques aux défis cryptographiques modernes.

Mots clés :

Corps fini, courbes elliptiques, cryptographie, couplage...

PAIRING BASED CRYPTOGRAPHY

Abstract :

Cryptography, the art and science of secure communication, has long been used to safeguard confidential exchanges between parties like Alice and Bob in the presence of an adversary, Eve. Over time, cryptography has evolved to address critical security services, including confidentiality, authentication, integrity, and non-repudiation. Among the emerging cryptographic techniques, Pairing-Based Cryptography (PBC) stands out as a powerful protocol that leverages bilinear and non-degenerate pairings on elliptic curves. These properties make PBC particularly effective in modern cryptographic applications. Since the 1990s, PBC has garnered significant attention in the cybersecurity field, with numerous studies proposing novel methods to enhance security and privacy. This thesis contributes to the ongoing development of PBC by presenting three key advancements. First, the traditional Diffie-Hellman key exchange protocol is extended to support multi-user environments. We introduce a new approach incorporating randomized point mechanisms and double encryption to enhance security. These innovations address common vulnerabilities, such as man-in-the-middle and side-channel attacks, by providing a more resilient key exchange protocol suitable for multi-user scenarios. Second, we focus on point compression techniques across elliptic curves in fields of various characteristics (2, 3, and different from 2 \& 3). By developing new compression algorithms for Affine, Jacobian, Projective, Edwards, and Montgomery coordinates, we achieve between 17% to 50% reduction in memory usage without sacrificing computational accuracy. These methods improve elliptic curve cryptography's efficiency and offer a comparative analysis of different field characteristics. Lastly, we explore the tower building technique for fields with embedding degrees of the form $2^i.3^j$. By optimizing arithmetic operations on elliptic curves with higher embedding degrees and using degree-2 and degree-3 twists, we significantly reduce the computational cost of pairing operations. Our findings contribute to more efficient and secure implementations of PBC. Through these contributions, this thesis advances Pairing-Based Cryptography by enhancing both security and computational efficiency, providing practical solutions for modern cryptographic challenges.

Key Words :
finite field, elliptic curves, cryptography, pairing...