AVIS DE SOUTENANCE DE THESE

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

Mr **EL BARAKA Mohammed**
Soutiendra : **le Mercredi 15/07/2026** à **10H00**
Lieu : ***FSDM – Centre Visioconférence***

Une thèse intitulée :

Cryptographie post-quantique : contributions à la construction et à l'amélioration de protocoles fondés sur les isogénies supersingulières

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

FD : ***Sciences et Techniques***
Spécialité : **Algèbre et cryptographie**

Devant le jury composé comme suit :

Nom et prénom	Etablissement	Grade	Qualité
Pr. MOUANIS Hakima	Faculté des Sciences Dhar El Mahraz, Fès	PES	Président
Pr. CHILLALI Abdelhakim	Faculté Polydisciplinaire, Taza	PES	Rapporteur
Pr. SAHMOUDI Mohammed	Faculté des Sciences, Meknès	MCH	Rapporteur
Pr. BOUZKOURA Khadija	Faculté des Sciences, Ben M'sik, Casablanca	MCH	Rapporteur
Pr. ELFADIL Lhoussain	Faculté des Sciences Dhar El Mahraz, Fès	PES	Examinateur
Pr. BEN ABBOU Rachid	Faculté des Sciences et Techniques, Fès	PES	Examinateur
Pr. DEMBA Sow	Université Cheikh Anta Diop, Dakar, Sénégal	MC	Invité
Pr. EZZOUAK Siham	Faculté des Sciences Dhar El Mahraz, Fès	MCH	Directeur de thèse

Résumé :

Cette thèse s'inscrit dans le contexte de la transition vers la cryptographie post-quantique, rendue nécessaire par les progrès de l'informatique quantique, susceptibles de compromettre les systèmes cryptographiques classiques fondés sur la factorisation et le logarithme discret. Elle porte plus particulièrement sur la cryptographie basée sur les isogénies de courbes elliptiques supersingulières, qui constitue aujourd'hui l'une des approches les plus prometteuses pour la conception de primitives résistantes aux attaques quantiques.

Dans un premier temps, cette thèse établit les fondements mathématiques nécessaires à l'étude des isogénies, des courbes elliptiques supersingulières, de leurs graphes associés, ainsi que des structures algébriques qui gouvernent leurs endomorphismes et leurs actions de groupe. Elle présente ensuite le cadre cryptographique général dans lequel s'inscrivent les protocoles fondés sur les isogénies, notamment les constructions de type SIDH et CSIDH, ainsi que les principaux problèmes difficiles sur lesquels repose leur sécurité.

Les contributions originales de ce travail sont de quatre types. La première consiste en une adaptation du schéma de signature ECDSA au contexte post-quantique, à travers des approches hybrides, en couches et des ajustements algorithmiques internes permettant une transition progressive depuis les systèmes existants. La deuxième contribution porte sur l'optimisation du calcul des isogénies supersingulières, grâce à des techniques fondées sur la transformée de Fourier rapide et sur l'exploitation d'endomorphismes explicites, conduisant à une réduction significative du coût algorithmique.

La troisième contribution est la conception d'un schéma de signature numérique fondé sur les isogénies, inspiré de constructions de type Schnorr et reposant sur des hypothèses de sécurité adaptées au cadre des actions de groupes. Enfin, la quatrième contribution propose un protocole PAKE fondé sur les isogénies, destiné à assurer une authentification sécurisée par mot de passe dans un environnement post-quantique.

Dans son ensemble, cette thèse met en évidence le potentiel des isogénies supersingulières comme base de constructions cryptographiques à la fois compactes, efficaces et mathématiquement solides. Elle contribue ainsi au développement de solutions post-quantiques rapprochant rigueur théorique, optimisation algorithmique et applicabilité pratique.

Mots clés :

cryptographie post-quantique, isogénies supersingulières, courbes elliptiques, ECDSA, signatures numériques, PAKE, graphes d'isogénies, CSIDH, SIDH, optimisation algorithmique.

POST-QUANTUM CRYPTOGRAPHY: CONTRIBUTIONS TO THE CONSTRUCTION AND IMPROVEMENT OF PROTOCOLS BASED ON SUPERSINGULAR ISOGENIES

Abstract :

This thesis is developed in the context of the transition toward post-quantum cryptography, driven by the progress of quantum computing, which threatens classical cryptographic systems based on integer factorization and discrete logarithms. It focuses in particular on isogeny-based cryptography over supersingular elliptic curves, which has emerged as one of the most promising directions for the design of quantum-resistant cryptographic primitives.

First, the thesis establishes the mathematical foundations required for the study of isogenies, supersingular elliptic curves, their associated graphs, and the algebraic structures governing their endomorphisms and group actions. It then introduces the general cryptographic framework for isogeny-based protocols, including SIDH- and CSIDH-type constructions, together with the main hard problems underlying their security.

The original contributions of this work are fourfold. The first contribution is a post-quantum adaptation of the ECDSA signature scheme through hybrid approaches, layered security mechanisms, and internal algorithmic refinements, allowing a progressive transition from existing systems. The second contribution addresses the optimization of supersingular isogeny computations using fast Fourier transform techniques and explicit endomorphisms, leading to a significant reduction in computational cost.

The third contribution is the design of a digital signature scheme based on isogenies, inspired by Schnorr-type constructions and relying on security assumptions related to group actions. Finally, the fourth contribution introduces an isogeny-based PAKE protocol aimed at providing password-authenticated key exchange in a post-quantum setting.

Overall, this thesis highlights the potential of supersingular isogenies as a foundation for compact, efficient, and mathematically sound cryptographic constructions. It therefore contributes to the development of post-quantum solutions that combine theoretical rigor, algorithmic efficiency, and practical applicability.

Key Words :

post-quantum cryptography, supersingular isogenies, elliptic curves, ECDSA, digital signatures, PAKE, isogeny graphs, CSIDH, SIDH, algorithmic optimization.