جامعة محمد الخامس بالرباط
Université Mohammed V de Rabat

École Nationale Supérieure d'Informatique et d'Analyse des Systèmes
Centre d'Études Doctorales en Sciences des Technologies de l'Information et de l'Ingénieur

AVIS DE SOUTENANCE DE THÈSE DE DOCTORAT

Meryem CHERKAOUI SEMMOUNI

Soutiendra publiquement sa thèse de Doctorat en Informatique

Le Vendredi 28 Octobre 2022 à 9H30 à l'Amphi 1 de l'ENSIAS

Intitulé de la thèse

CONTRIBUTIONS À LA SÉCURITÉ DES SYSTÈMES BASÉS SUR LA CRYPTOGRAPHIE CLASSIQUE ET POST-QUANTIQUE

Devant le Jury composé de :

Président :

Pr. Mohamed ESSAAIDI, PES, ENSIAS, Université Mohammed V de Rabat

Directeur de thèse :

Pr. Mostafa BELKASMI, PES, ENSIAS, Université Mohammed V de Rabat

Co-directeur de thèse :

Pr. Abderrahmane NITAJ, Professeur des Universités, Université de Caen Normandie, France

Rapporteurs :

Pr. Abdelhamid BELMEKKI, PH, Institut National des Postes et Télécommunications, Rabat

Pr. Olivier BLAZY, Professeur des Universités, Ecole Polytechnique, Palaiseau, France

Pr. Christophe PETIT, Professeur des Universités, Université libre de Bruxelles, Belgique

Examinateur :

Pr. Omar KHADIR, PES, FST-Mohammedia, Université Hassan II, Casablanca

UNIVERSITE MOHAMMED V - RABAT ★ ENSIAS

Résumé : La sécurité de la plupart des nouvelles technologies repose sur la cryptographie qui fournit des outils permettant d'assurer des fonctions de sécurité telles que la confidentialité, l'intégrité, l'authenticité et la non-répudiation. Une bonne partie de cette thèse va porter sur les mesures d'amélioration de la sécurité des systèmes Bitcoin et de vote électronique avec la cryptographie classique à base des courbes elliptiques, et par la suite avec la cryptographie post-quantique à base des réseaux euclidiens pour être protéger contre les ordinateurs quantiques. Une autre approche pour améliorer la sécurité est la cryptanalyse, dans le but d'éviter par la suite les paramètres qui sont vulnérables. En effet RSA est un cryptosystème qui intervient dans les plupart des nouvelles technologies. Une partie de notre thèse va porter sur la cryptanalyse de ce cryptosystème en utilisant des méthodes avancées à base des réseaux euclidiens, des fractions continues, et des courbes elliptiques.

Mots-clés : Bitcoin, cryptologie, quantique, RSA, vote électronique.

.

Abstract: The security of most new technologies is based on cryptography which provides security functions such as confidentiality, integrity, authenticity, and non-repudiation. A good part of this thesis will focus on cryptographic techniques to improve the security of Bitcoin and electronic voting systems by moderne cryptography based on elliptic curves, and by postquantum cryptography based on lattices to be protected against quantumcomputers. Another approach to improve security is cryptanalysis, by avoiding parameters that are vulnerable. Indeed RSA is a cryptosystem that is involved in most new technologies. Another part of our thesis will focus on the cryptanalysis of this cryptosystem using advanced methods based on Lattices, continued fractions, and elliptic curves.

Keywords: Bitcoin, cryptology, electronic voting, quantique, RSA.