



# From hardness assumptions to energy-secure protocols: A systematic survey of Euclidean lattice-based cryptography

Mourad Yessef <sup>a</sup>\*, Youness Hakam <sup>b</sup>, Mohamed Tabaa <sup>b</sup>, Lhoussaine Ahessab <sup>c</sup>, Z.M.S. Elbarbary <sup>d,e</sup>, Salman Arafath Mohammed <sup>d,e</sup>, Naim Ahmad <sup>f</sup>

<sup>a</sup> Higher School of Technology in Nador, Mohammed First University, Nador, 62000, Morocco

<sup>b</sup> Multidisciplinary Laboratory of Research and Innovation, Moroccan School of Engineering Sciences (EMSI), Casablanca, 20000, Morocco

<sup>c</sup> National Higher School of Arts and Crafts (ENSAM-Meknes), Moulay Ismail University, Meknes, 50000, Morocco

<sup>d</sup> Department of Electrical Engineering, College of Engineering, King Khalid University, Abha, 61421, Saudi Arabia

<sup>e</sup> Center for Engineering and Technology Innovations, King Khalid University, Abha, 61421, Saudi Arabia

<sup>f</sup> College of Computer Science, King Khalid University, Abha, 61421, Saudi Arabia



## ARTICLE INFO

### Keywords:

Euclidean lattices  
Key encapsulation  
Lattice-based cryptography  
Lightweight cryptography  
Post-quantum cryptography  
SCADA systems  
Smart grids

## ABSTRACT

The fast development of quantum computing poses major challenges for classical cryptographic techniques, hence post-quantum cryptography is needed. Emphasizing their fit for securing energy-critical infrastructure, this work methodically reviews lattice-based cryptographic systems. Theoretically strong and practically relevant fundamental lattices including the Shortest Vector Problem (SVP), Learning with Errors (LWE), and Module-LWE are investigated in limited environments including smart grids and IoT devices. Examined are important advancements in hardware implementations, algorithmic optimizations, and cryptanalysis with an eye toward programs including Falcon, Dilithium, and CRYSTALS-Kyber. Over systems including Vehicle-to-Grid (V2G) networks and Supervisory Control and Data Acquisition (SCADA) systems, lattice-based cryptography's efficacy and deployability are shown. The review ends with a discussion of future research paths to support long-term quantum-safe infrastructure security and newly arising theoretical hazards.

## Contents

1. Introduction .....	2
2. Evolution of lattice-based cryptography .....	3
2.1. Historical milestones: From Ajtai to modern constructions .....	3
2.2. Mathematical background: Lattices, SVP, CVP, SIS, LWE .....	3
2.3. Structured lattices: Ring-LWE, Module-LWE, NTRU .....	4
2.4. Trapdoors, sampling, and reduction techniques .....	5
3. Cryptographic constructions and implementation strategies .....	6
3.1. Public-key encryption and key encapsulation .....	6
3.2. Digital signatures: Trapdoor-free and Fiat-Shamir paradigms .....	7
3.3. Zero-knowledge proofs and identification schemes .....	8
3.4. Optimization techniques: Polynomial multiplication, modular arithmetic, platform adaptation .....	9
4. Security estimation and cryptanalysis .....	9

\* Corresponding author.

E-mail addresses: [mourad.yessef@usmba.ac.ma](mailto:mourad.yessef@usmba.ac.ma) (M. Yessef), [y.hakam@emsi.ma](mailto:y.hakam@emsi.ma) (Y. Hakam), [m.tabaa@emsi.ma](mailto:m.tabaa@emsi.ma) (M. Tabaa), [l.ahessab@edu.umi.ac.ma](mailto:l.ahessab@edu.umi.ac.ma) (L. Ahessab), [albrbry@kku.edu.sa](mailto:albrbry@kku.edu.sa) (Z.M.S. Elbarbary), [salman@kku.edu.sa](mailto:salman@kku.edu.sa) (S.A. Mohammed), [nagqadir@kku.edu.sa](mailto:nagqadir@kku.edu.sa) (N. Ahmad).