CyBOK

The Cyber Security Body Of Knowledge

# Accessible Post-Quantum Cryptography University Syllabus

Dr Essam Ghadafi

contact@cybok.org
www.cybok.org

# Outline

- Project Overview
- Why Teach Post-Quantum Cryptography?
- Sample Teaching Materials & Approach
- Stakeholder Validation

# About the Project

- Aims to develop teaching resources on Post-Quantum Cryptography (PQC) to help universities in teaching PQC

- Designed for CS/Engineering students without advanced math or theory background

# CyBOK Mapping

The outputs of the project map to the following CyBOK KAs:

- Systems Security ➔ Cryptography
- Infrastructure Security ➔Applied Cryptography

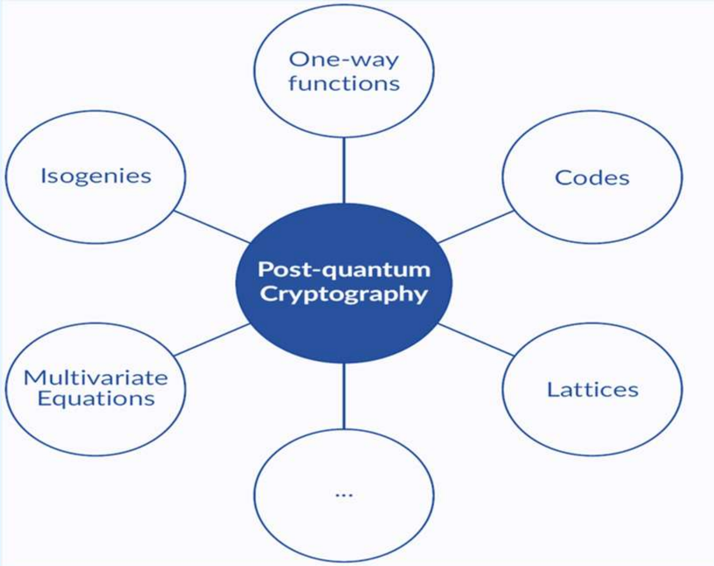
# Academic Need for PQC

Universities must train for PQC readiness

PQC still absent in many curricula

- Quantum advances threaten classical crypto
- NIST finalised PQC standards in 2024, initiating global adoption
- NCSC urges full PQC migration by 2035
- PQC ensures compliance, resilience, and future security

# PQC Approaches




- Various intractability assumptions
- Sometimes not easy to compare like-for-like

# Motivation: The Challenge

Cryptography Courses often require substantial background, e.g.

- Abstract Algebra (e.g. groups, rings) ad polynomial algebra
- Number Theory (e.g. modular arithmetic)
- Complexity Theory (e.g. hardness assumptions)
- Linear Algebra (e.g. vectors and matrices)
- Mathematical maturity for formal reasoning and notation

**Challenge:**

- Extensive maths prerequisites restrict access for many CS/Eng students
- Time constraints make overing all prerequisites within a crypto module impractical

# Challenges in Teaching PQC

- Complexity & Breadth: Multiple hard problems and assumptions, e.g. lattices, code-based, multivariate, isogeny-based, hash-based, etc.
- Depth: Some topics (e.g., lattice-based crypto) can fill entire modules on their own
- Scope Dilemma: Should a PQC module cover all approaches or focus on key ones (e.g., lattice-based)?
- Balance Needed: Depth vs. breadth, foundational understanding vs. practical implementation

# Our Contribution

- Lecture and Practice Materials on:
  - Introduction to PQC and quantum computing's implications for Cryptography
  - Lattice-Based Cryptography

- Future drafts will detail other PQC approaches, including isogeny-based cryptography

# Our Design Approach for the Syllabi

- Intuition First: Simplified explanations and analogies before formal definitions to aid understanding (e.g., visualising lattice points from basis vectors before formal definitions)

- Gradual Formalism: Proof sketches and informal reasoning precede full proofs to build rigour progressively

- Hands-On Learning: Concepts practised using SageMath (https://www.sagemath.org/) to connect theory with application (e.g. exploring lattice structure and shortest vectors computationally)

# Sample Slide from Material - 1

## Lattice Definition – Intuition (Excerpt)

**Lattice:** A a set of points in n-dimensional space that exhibits a periodic structure, i.e. A lattice is just a grid of points

**Intuition:** The lattice is an infinite grid of points arranged in a regular, repeating pattern that extends in multiple dimensions

- The position of each point is determined by the lattice basis
- The basis vectors define the directions and distances to reach the lattice points

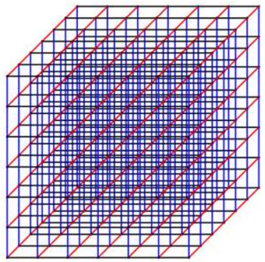


FIGURE: An example of 3D Lattice

# Sample Slide from Material - 2

## Lattice Basis – Intuition (Excerpt)

**Intuition:** The basis of a lattice defines the directions (or vectors) you can use to reach any point in the grid

- Each point in the lattice (grid) can be reached by combining the basis vectors, using some integer multiples

# Sample Slide from Material - 3

## LATTICE BASIS – INTUITION (EXCERPT)

Example: Consider the 2D lattice generated by the basis $\mathbf{b}_1 = (2, 1)$ and $\mathbf{b}_2 = (1, 3)$

- Point $(3, 4)$ (in red) is obtained as $\mathbf{b}_1 + \mathbf{b}_2$
- Point $(5, 5)$ (in blue) is obtained by $2\mathbf{b}_1 + \mathbf{b}_2$
- ...

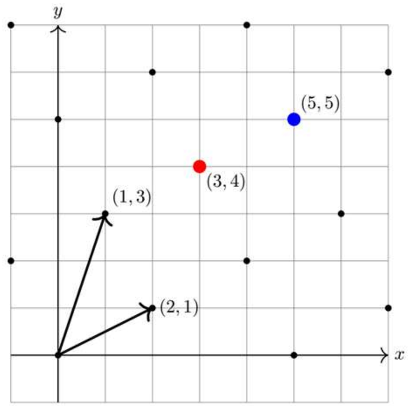



FIGURE: 2D-Lattice generated by the basis $\mathbf{b}_1 = (2, 1)$ and $\mathbf{b}_2 = (1, 3)$

# Stakeholder Validation

Our curriculum design has been validated through a stakeholder workshop (https://conferences.ncl.ac.uk/apqcus/) involving:

- Students from relevant programmes
- Academics
- Industry representatives, including PQShield and CyberNorth

Feedback was positive and students liked the approach

# Thank You! Questions?

contact@cybok.org
www.cybok.org