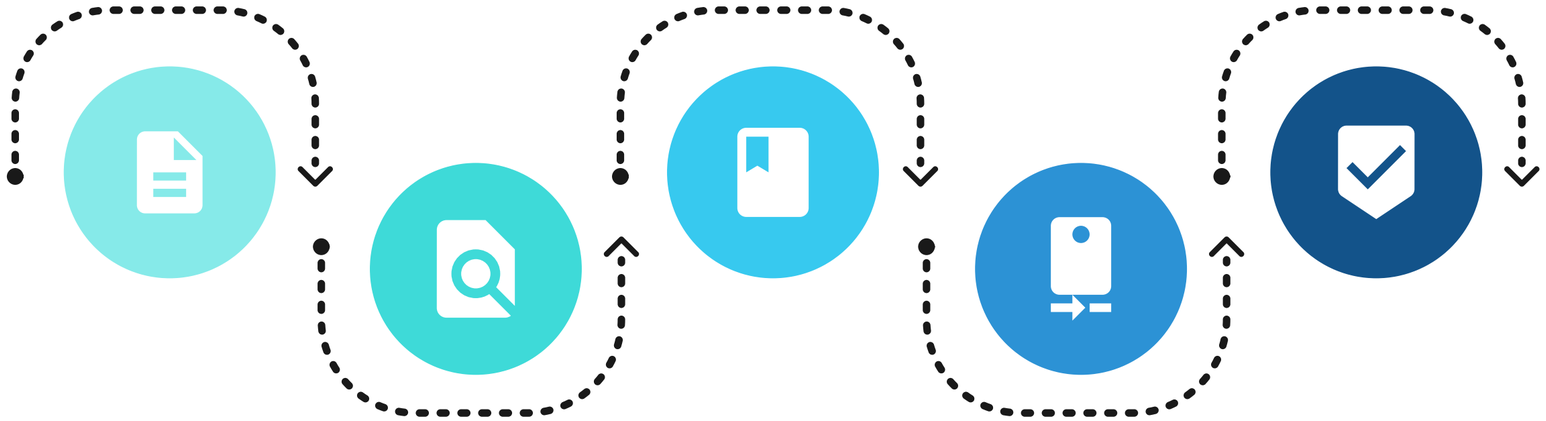
Zyber Chat Project

README.TXT

A table of contents.



1-Introduction to Zyber Chat

A brief overview of Zyber Chat and its purpose

2-Key Features

Highlighting the main features that make Zyber Chat stand out

3-How Zyber Chat works

A concise explanation of the functionalities and operations of Zyber Chat

3-Project Flow

An overview of the steps and stages involved in our Zyber Chat project

5- Main Objectives

Summarizing the primary goals and objectives of Zyber Chat

K-DEA

Kyber - Database Encryption Algorithm

Zyber Chat

Chat Application

Java based Chat Application using TCP/IP connection protocol

About Kyber(CRYSTALS)

CRYSTALS | Kyber Home | Resources | Software

Introduction

Kyber is an IND-CCA2-secure key encapsulation mechanism (KEM), whose security is based on the hardness of solving the learning-with-errors (LWE) problem over module lattices. Kyber is one of the finalists in the NIST post-quantum cryptography project. The submission lists three different parameter sets aiming at different security levels. Specifically, Kyber-512 aims at security roughly equivalent to AES-128, Kyber-768 aims at security roughly equivalent to AES-192, and Kyber-1024 aims at security roughly equivalent to AES-256.

For users who are interested in *using* Kyber, we recommend the following:

- Use Kyber in a so-called *hybrid mode* in combination with established "pre-quantum" security; for example in combination with elliptic-curve Diffie-Hellman.
- We recommend using the Kyber-768 parameter set, which—according to a very conservative analysis—achieves more than 128 bits of security against all known classical and quantum attacks.

MAJOR FEATURES

What our project has to offer

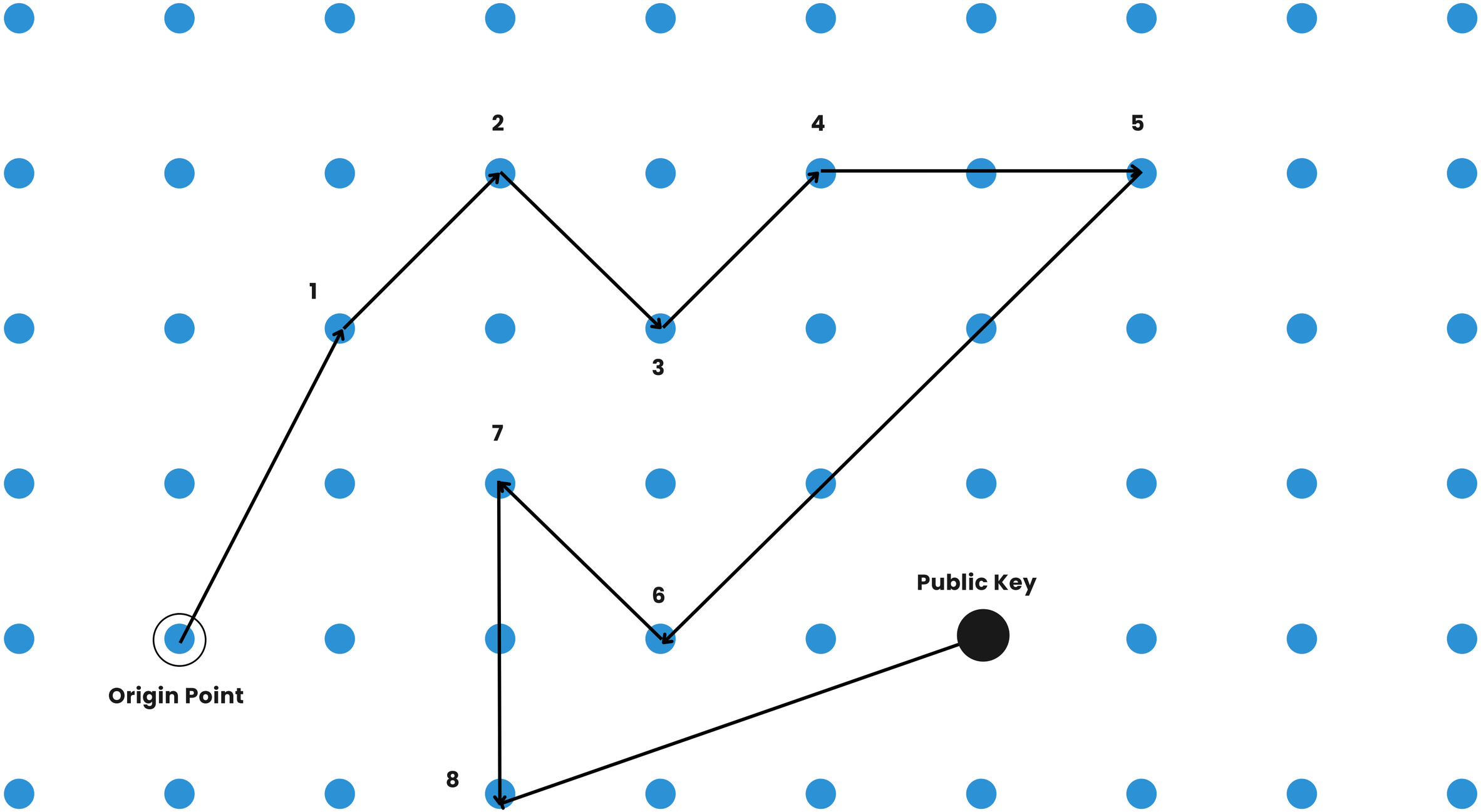
1 - Database Security — Securing database through K-DEA

2 - Uniqueness of algorithm — Difficult to decode the lattice path

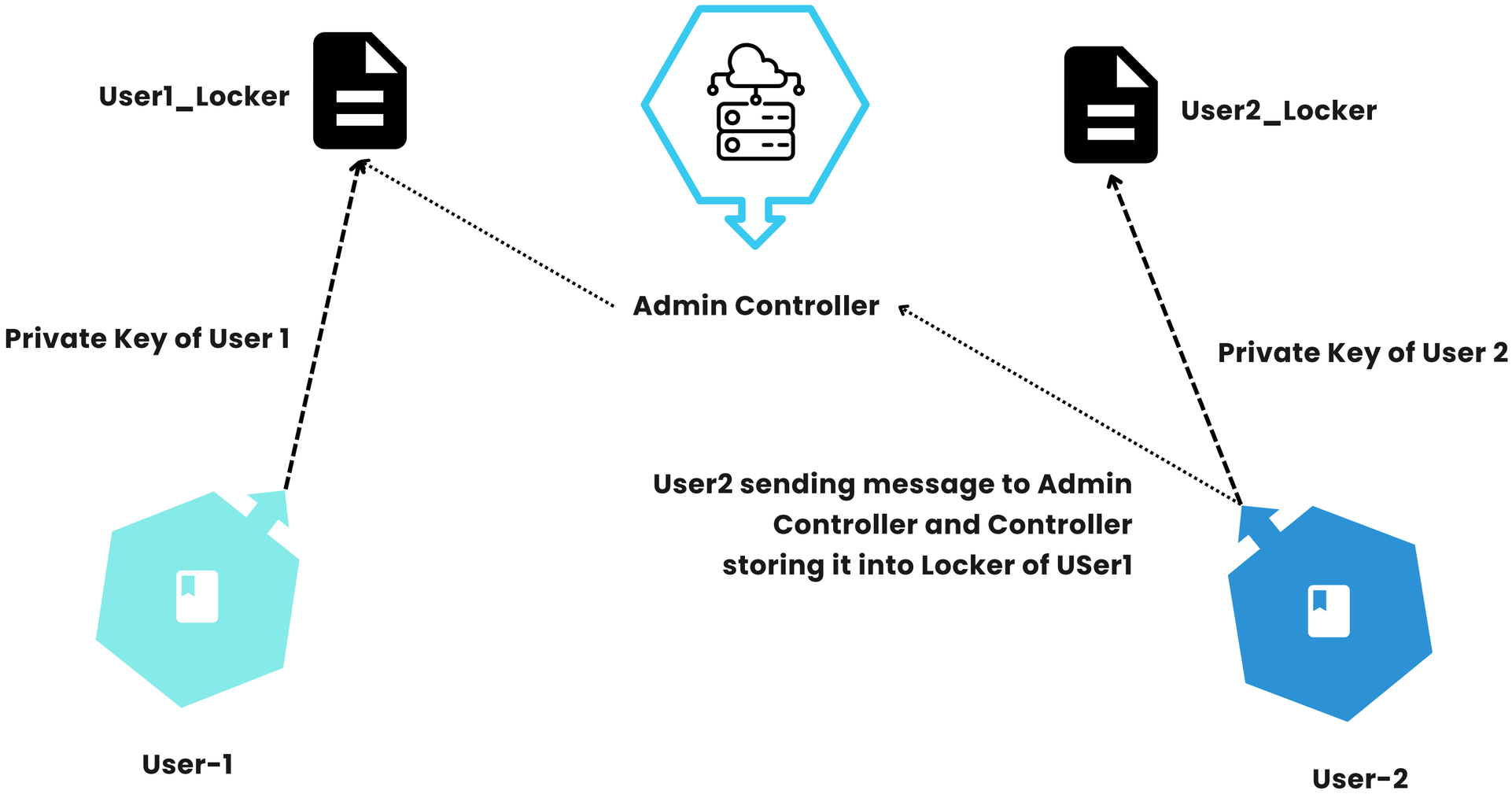
3 - Based on CRYSTALS — Uses the advance Cryptographic Suite for Algebraic Lattice, designed to withstand attacks by large quantum computers

4 - Scalable — Can handle a large user base.

5 - Practicality — No visible time delay for message transmission.


1
2
3
4
5
6
7
8
Origin Point
Public Key

Zyber Chat : Working



PROJECT FLOW

Zyber Chat

Receiver can access its Locker with its Private key path.

5 - Receiver's Locker

The receiver's system gets an Acknowledge, about the message stream

4 - Ack for Receiver

The Admin controller access' the Log and Updates the locker

3 - Admin rewriting Locker

The message sent is stored in Sender's Log file

2 - Sender's Log file

The Message sent by Sender while Chatting

1 - The Sender

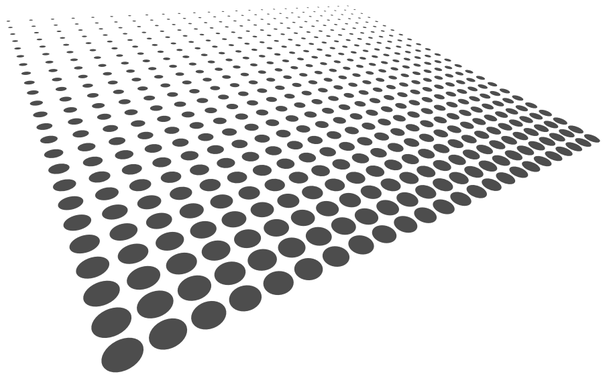
#CRYPTANALYSIS

Complexity in breaking the Algorithm

INCREASING COMPLEXITY

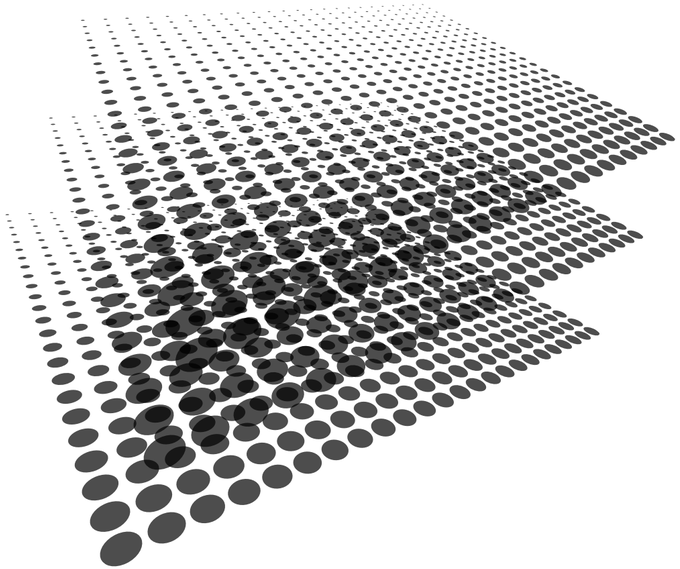
LEVEL-1

2D Lattice



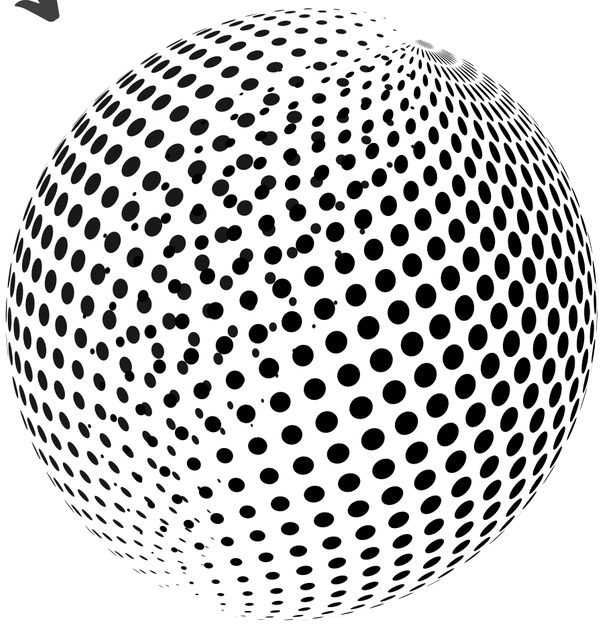
LEVEL-2

Multi Dimensional Lattice



LEVEL-3

Infinite Dimensional Lattice



REAL LATTICE MATRIX

Main Objectives

Security is not a concern, not anymore

With the presence of 2 private keys, database security just acquired new heights.

Robustness

Though it may look like a normal chat app, the backend is anything but normal.

Complexity of decoding

Decoding lattice path makes it very difficult for an attacker to access the contents

Easy to use

The entire system is very user friendly. A user does not need to know the underlying complexities.

In other words, this is why you should use our project.