THE QUANTUM QUEST

THE FOSS FILES | SEASON 5 | EPISODE 4

THE CIPHER FILES

Ajinkya Madane

Shreyash Patil

Aditya Aparadh

WLUG
COMMUNITY | KNOWLEDGE | SHARE

TABLE OF CONTENT

WLUG
COMMUNITY | KNOWLEDGE | SHARE

STEGANOGRAPHY

- Practice of concealing information within another medium.
- Derived from Greek words steganos (covered) and graphia (writing).
- Types:
  - Image Steganography
  - Audio Steganography
  - Network Steganography

WLUG
COMMUNITY | KNOWLEDGE | SHARE

IMAGE COMPARISON

WLUG
COMMUNITY | KNOWLEDGE | SHARE

DECODING IMAGES

- Scan the QR for the Steganography Encoder and Decoder
- https://stylesuxx.github.io/steganography/

LSB IMAGE STEGANOGRAPHY

- Change the least significant bits of each pixel to encode our data
- Lets assume our data to be 10-01-11
- Lets assume the pixel information is
  - 10010111 for first pixel
  - 11010110 for second pixel
  - 11011000 for third pixel

LSB IMAGE STEGANOGRAPHY

- The data is 10-01-11
- If the pixel information is
  - 10010111 => 10010110
  - 11010110 => 11010101
  - 11011000 => 11011011
- Max change in value for each pixel is 3, so the overall effect on the image is very imperceptible
- So there is no change in image metadata or size

LSB IMAGE STEGANOGRAPHY

- Limitations:
  - Very less data holding capacity
  - Sensitive to image compression techniques
  - Cropping, rotate or re-sizing can destroy the data
- There are better alternatives like Discrete Cosine transform(DCT), Masking and Filtering etc.
- Used for copywrite protection and digital watermarking, usually masking data in less important area of images.

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HOMOMORPHIC ENCRYPTION

- A type of encryption that allows computations on encrypted data without decrypting it.
- The result, when decrypted, matches the result of operations performed on the original unencrypted data.

Magical box

Locked box

HOMOMORPHIC ENCRYPTION

TYPES

- **Fully Homomorphic Encryption (FHE)**

  Both addition and multiplication any(infinite) no. of times

- **Partially Homomorphic Encryption (PHE)**

  Only addition or multiplication but infinite no. of times

- **Somewhat Homomorphic Encryption (SHE)**

  Both addition and multiplication but limited no. of times

WLUG
COMMUNITY | KNOWLEDGE | SHARE

WHY IS HOMOMORPHIC ENCRYPTION IMPORTANT?

- **Protects Privacy During Processing**

- **Secures Data in the Cloud**

- **Eliminates Trade-Offs Between Security and Functionality**

WLUG
COMMUNITY | KNOWLEDGE | SHARE

- Reduces Risk of Data Breaches

- Revolutionizes Industry Applications

- Empowers Regulatory Compliance

CHALLENGES

- High Computational Overhead

- Large Ciphertext Size

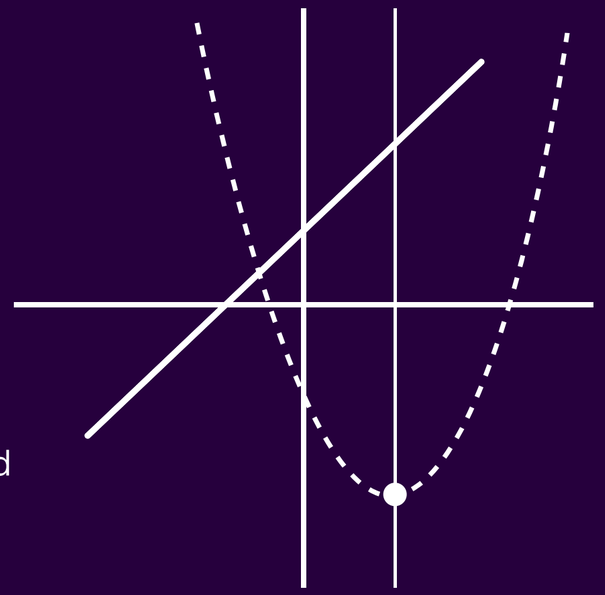
- Limited Practicality and Scalability

SHAMIR'S SECRET SHARING

- Solves the issue of secretly sharing password or a key among individuals with same power to everyone
- If you want a password shared among 5 people so that when 3 come together, the password is cracked
- A (k,n) scheme is where
  - 'n' is number of people the key is shared with
  - 'k' is min number required to crack password

SHAMIR'S SECRET SHARING

- Shared key is generated through points on a polynomial function
- if 'k' is min persons required, 'k-1' polynomial function is used



Three points define a quadratic curve

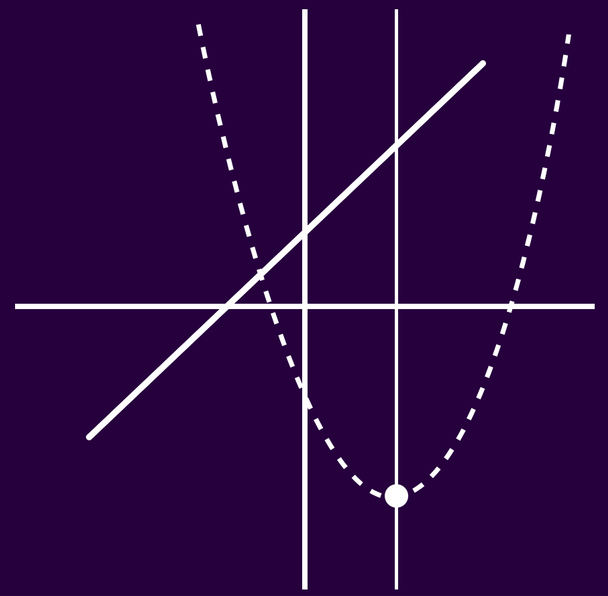
Two points are required for a straight line

SHAMIR'S SECRET SHARING

- Basically equation is the answer to cracking that password

$$ax^2+bx+c=0$$

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$



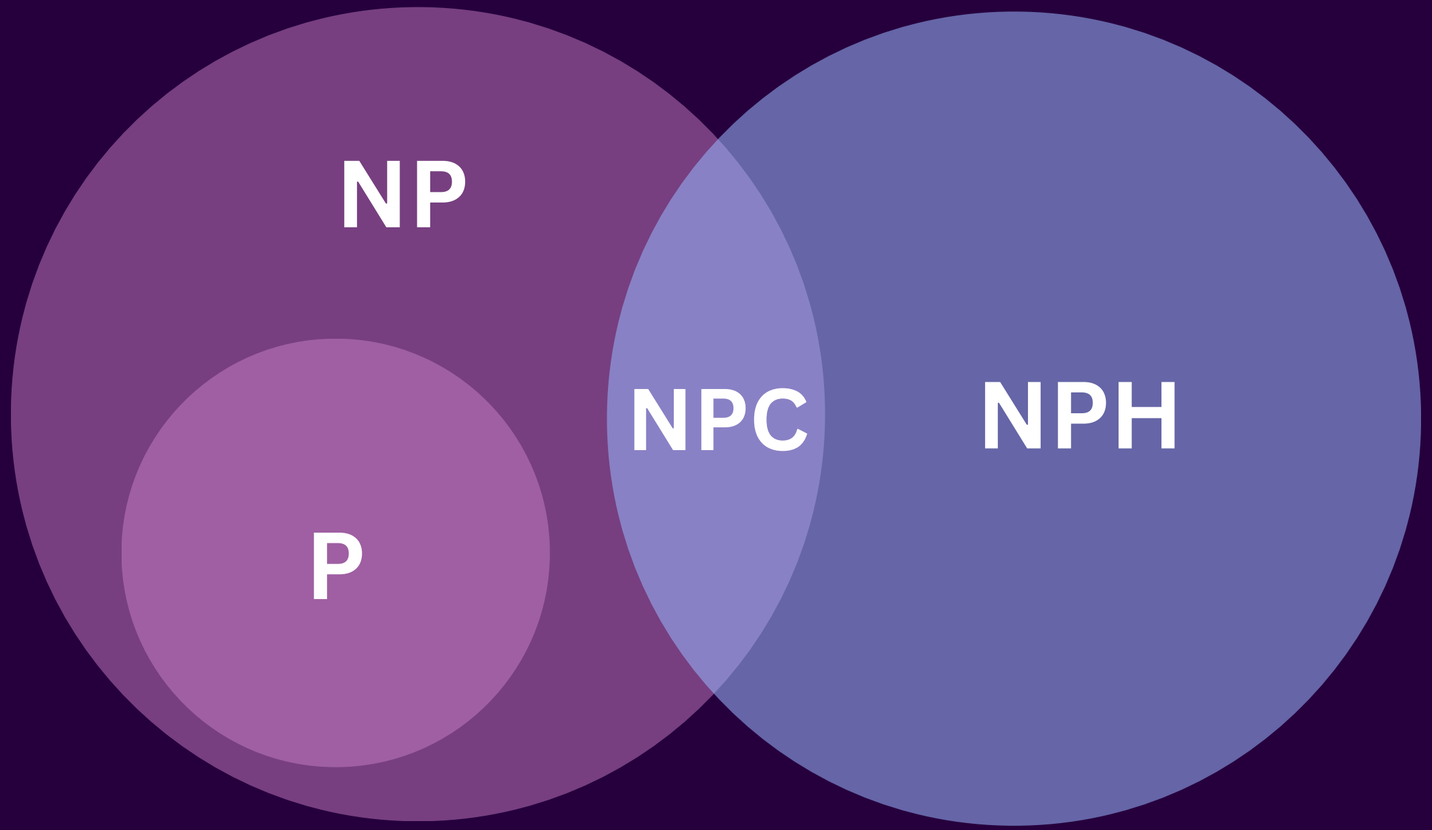
The x and y intercept can be the original

WLUG
COMMUNITY | KNOWLEDGE | SHARE

THE FUTURE OF CRYPTOGRAPHY

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Computational Complexity of Algorithms

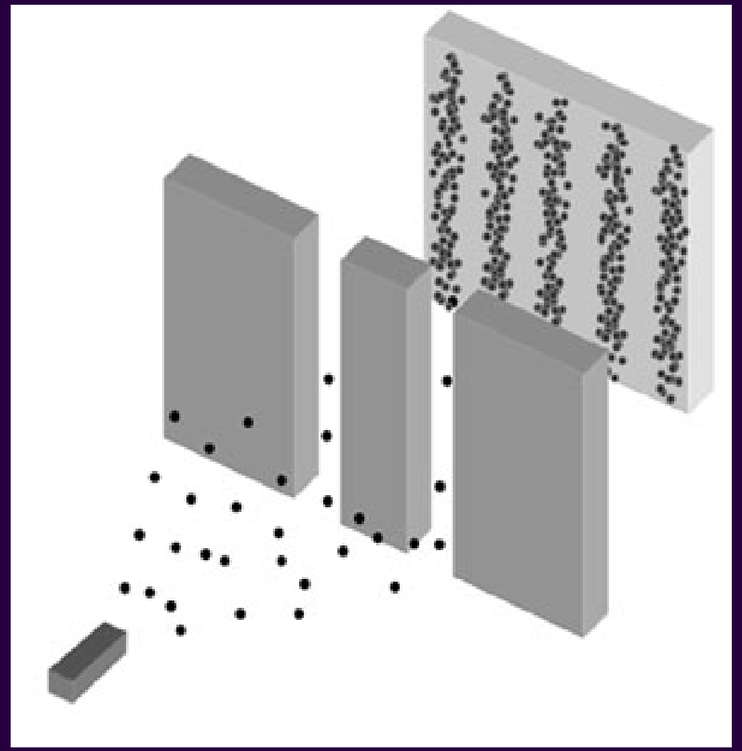


WLUG
COMMUNITY | KNOWLEDGE | SHARE

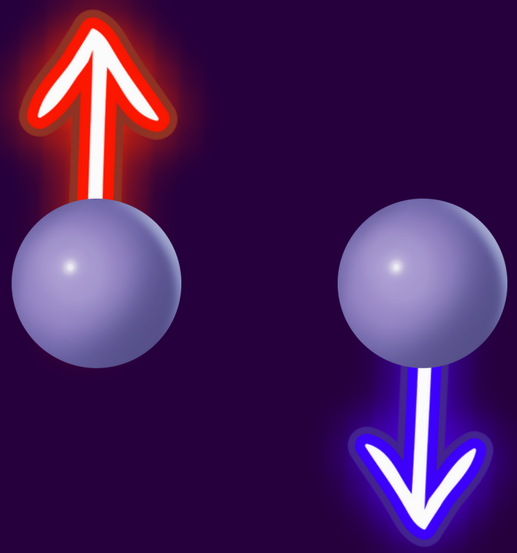
LIGHTWEIGHT QUANTUM MECHANICS

WLUG
COMMUNITY | KNOWLEDGE | SHARE

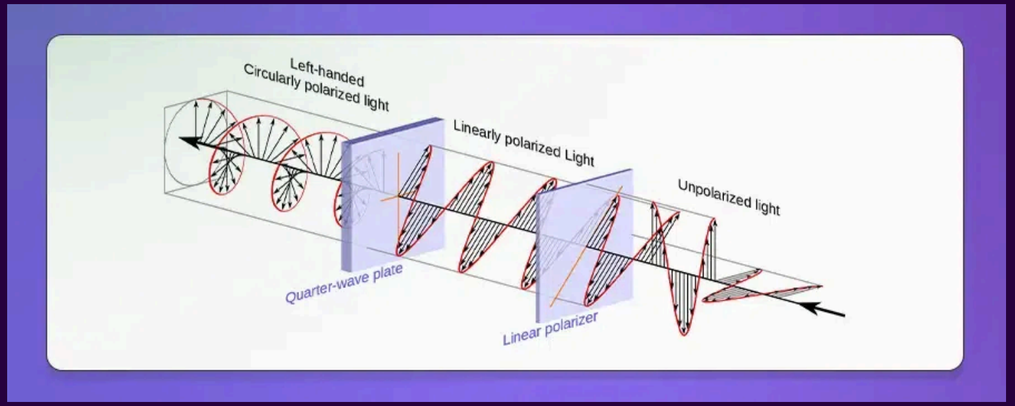
YOUNG'S DOUBLE SLIT EXPERIMENT



SUPERPOSITION

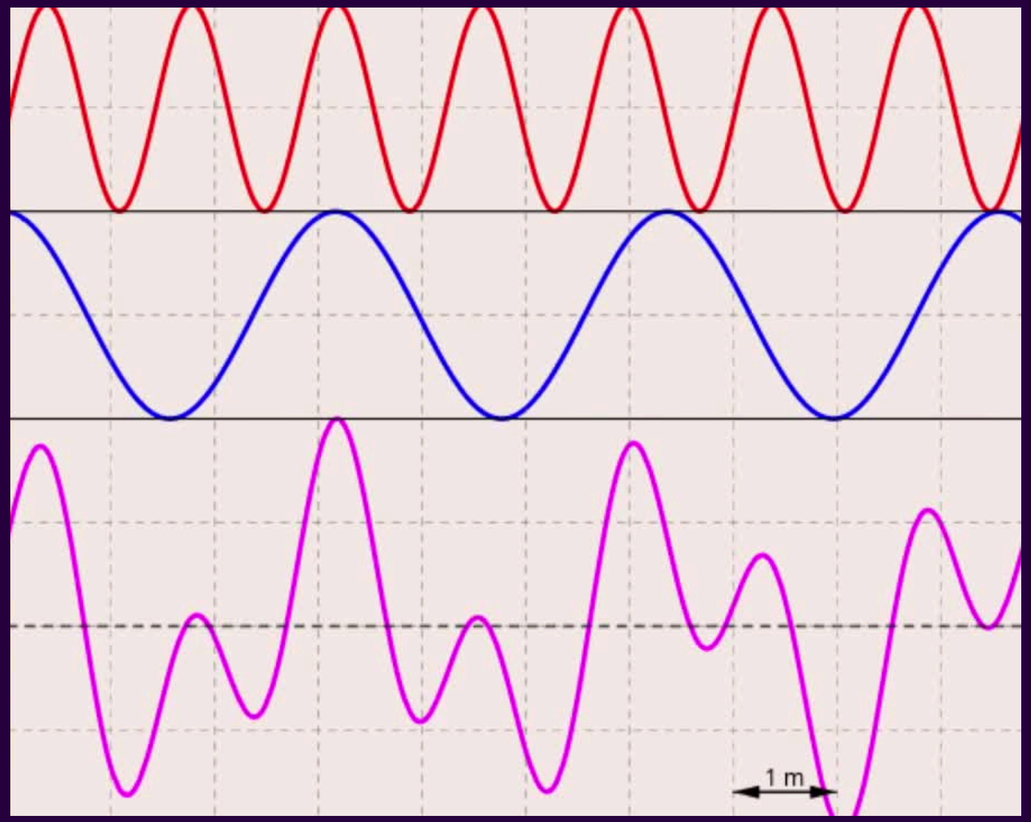


Electron Spin



Polarization of Light

SUPERPOSITION



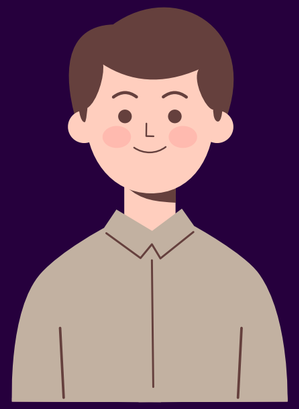
Wave function of spin up

Wave function of spin down

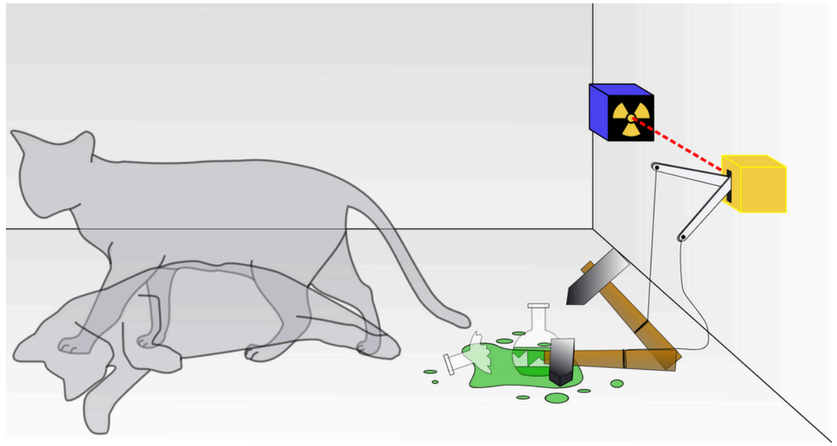
Wave function of electron in superposition

SCHRODINGER'S CAT

- Entanglement
- Copenhagen Interpretation



You

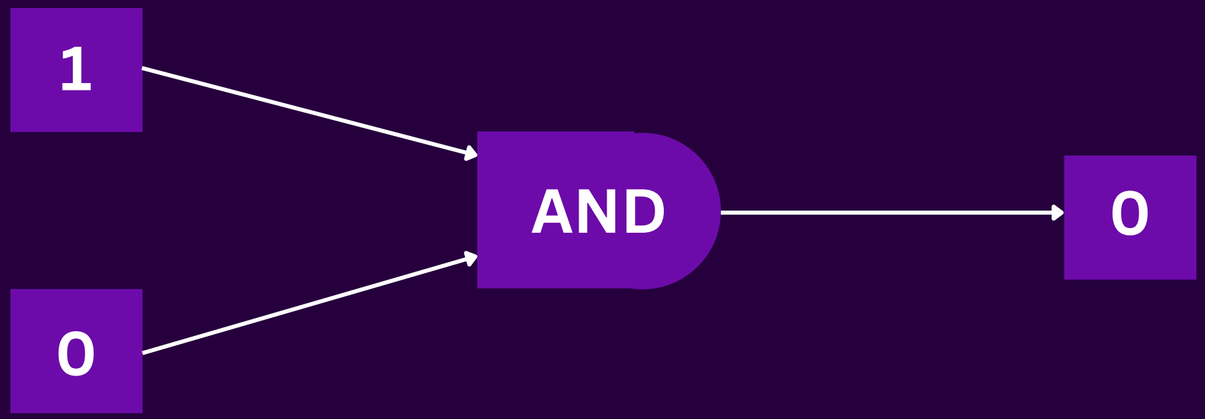


Box

WLUG
COMMUNITY | KNOWLEDGE | SHARE

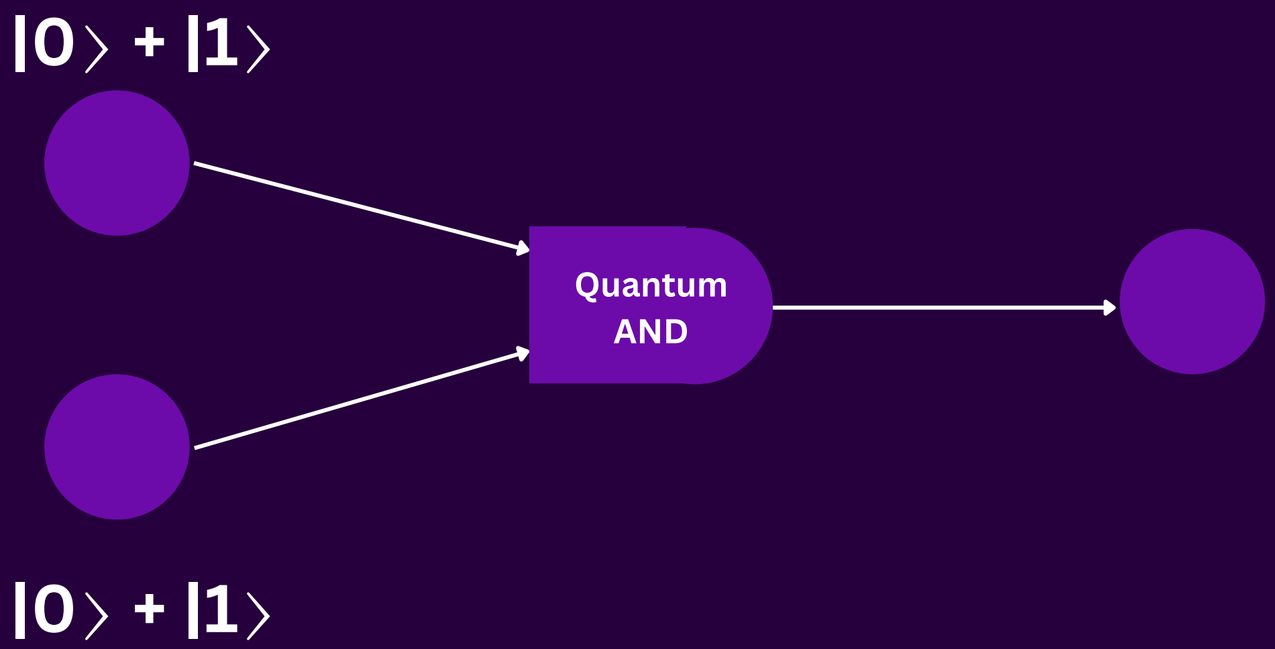
QUANTUM COMPUTING?

CLASSICAL COMPUTERS



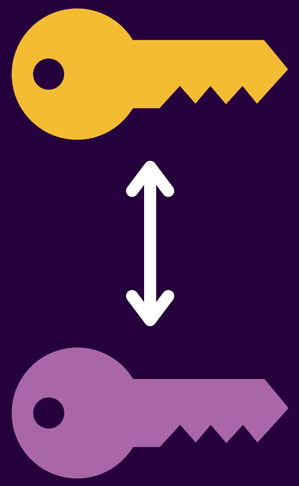
A	B	Y
0	0	0
0	1	0
1	0	0
1	1	1

QUANTUM COMPUTERS



$$|00\rangle + |01\rangle + |10\rangle + |11\rangle$$
$$=$$
$$|0\rangle + |0\rangle + |0\rangle + |1\rangle$$

QUANTUM ALGORITHMS



Shor’s
Algorithm

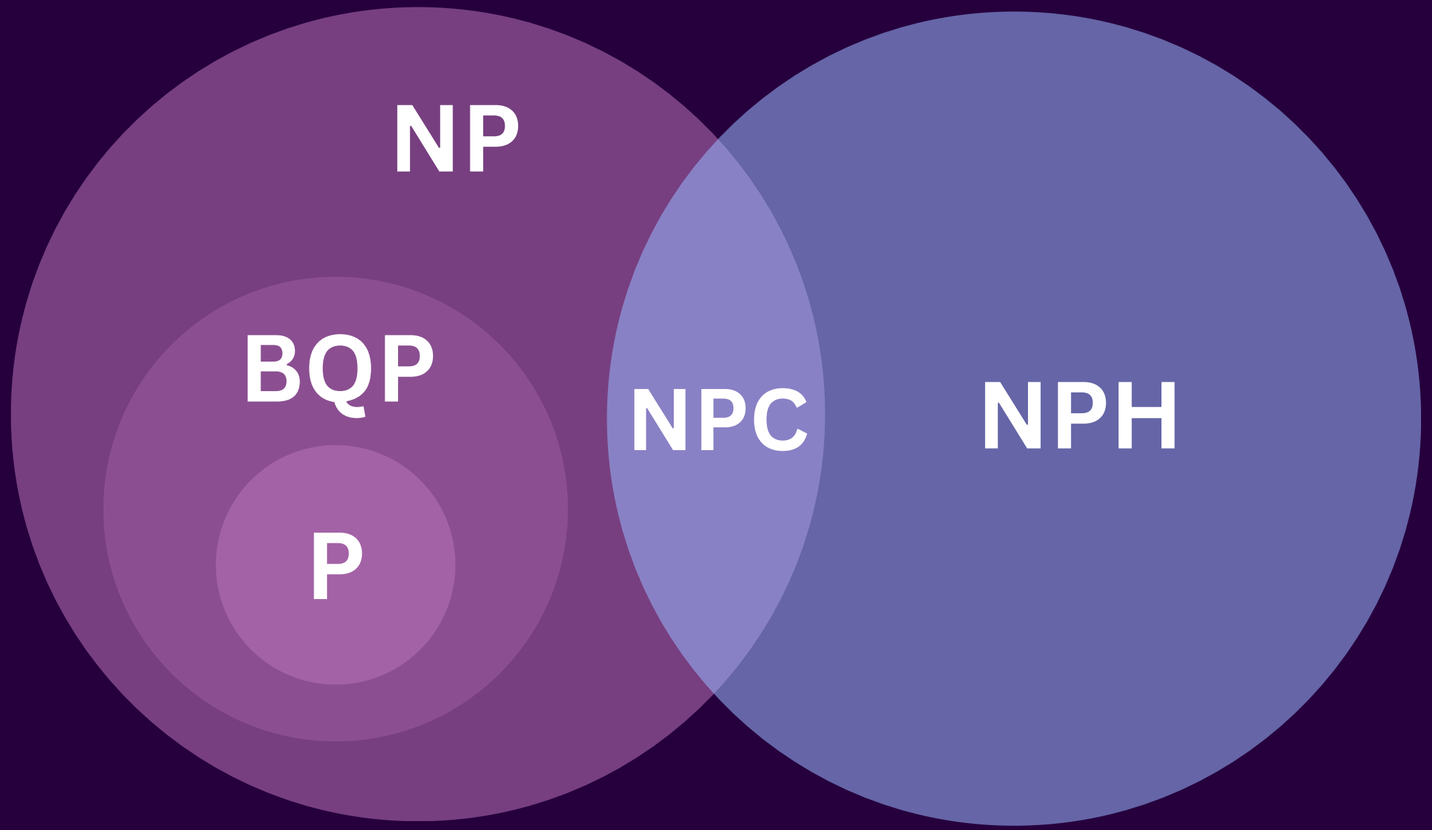
Grover’s
Algorithm

WLUG
COMMUNITY | KNOWLEDGE | SHARE

POST QUANTUM CRYPTOGRAPHY

WLUG
COMMUNITY | KNOWLEDGE | SHARE

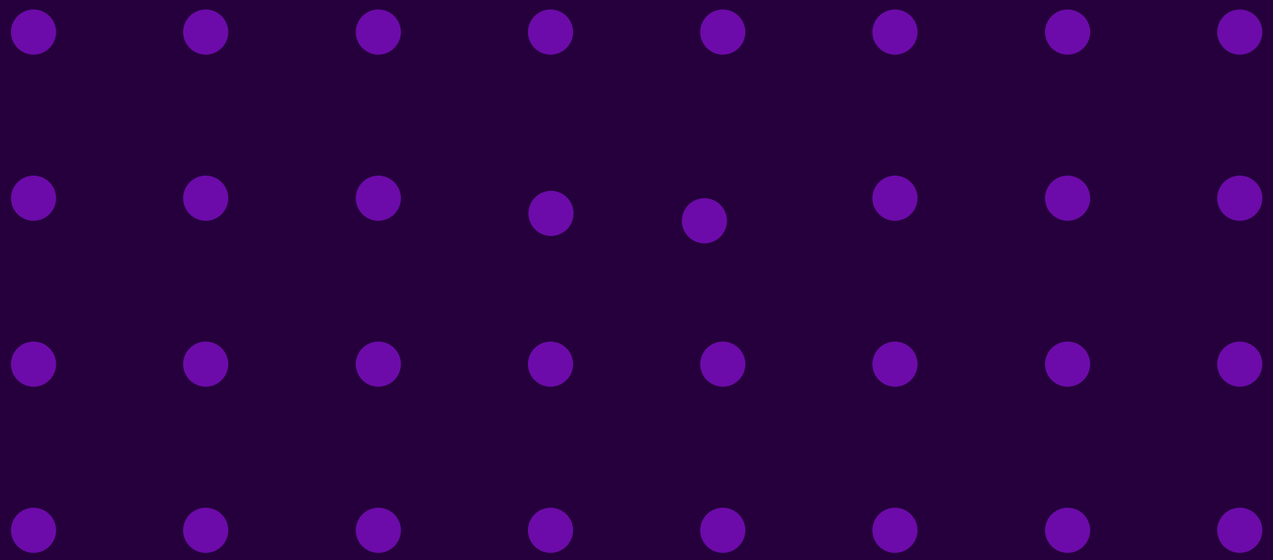
Computational Complexity of Algorithms



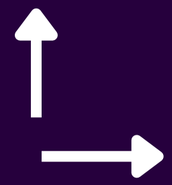
WLUG
COMMUNITY | KNOWLEDGE | SHARE

LATTICE BASED ENCRYPTION

LATTICE BASED ENCRYPTION



2D Lattice

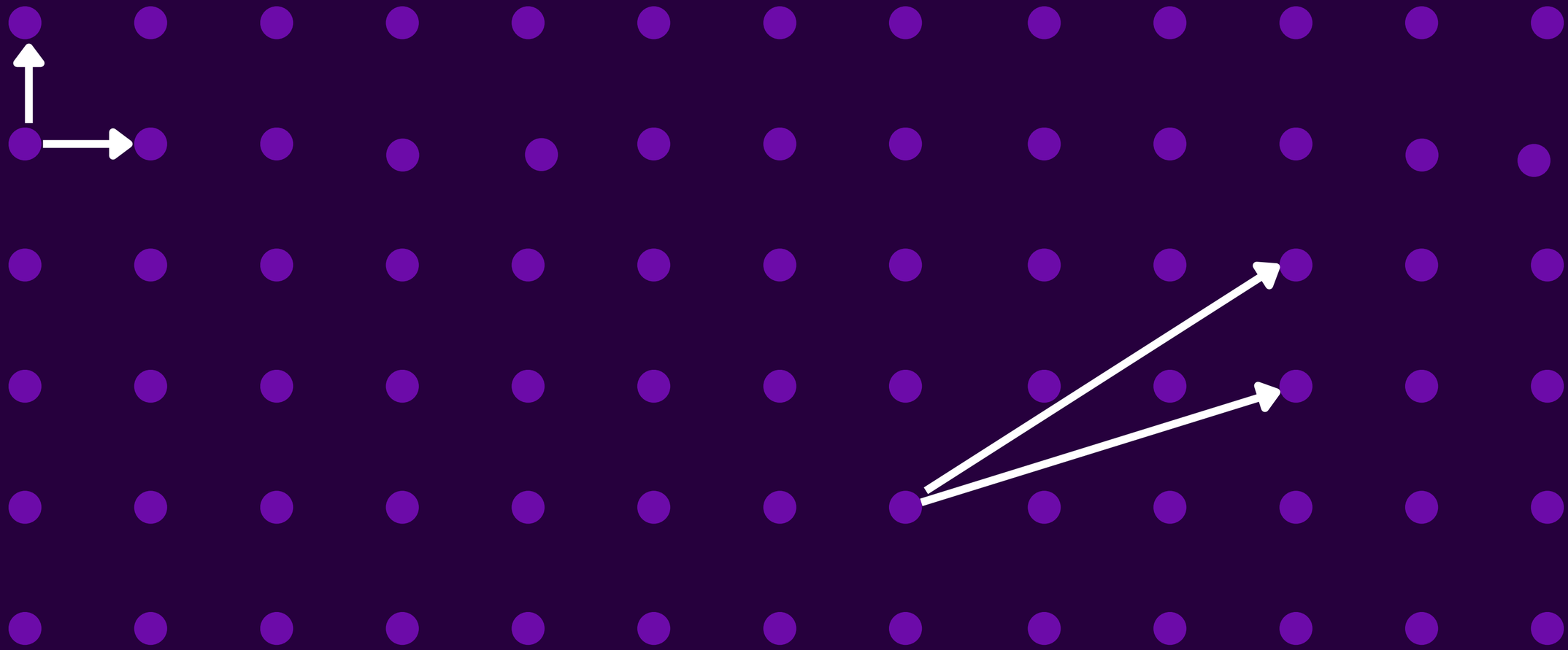


Basis Vectors

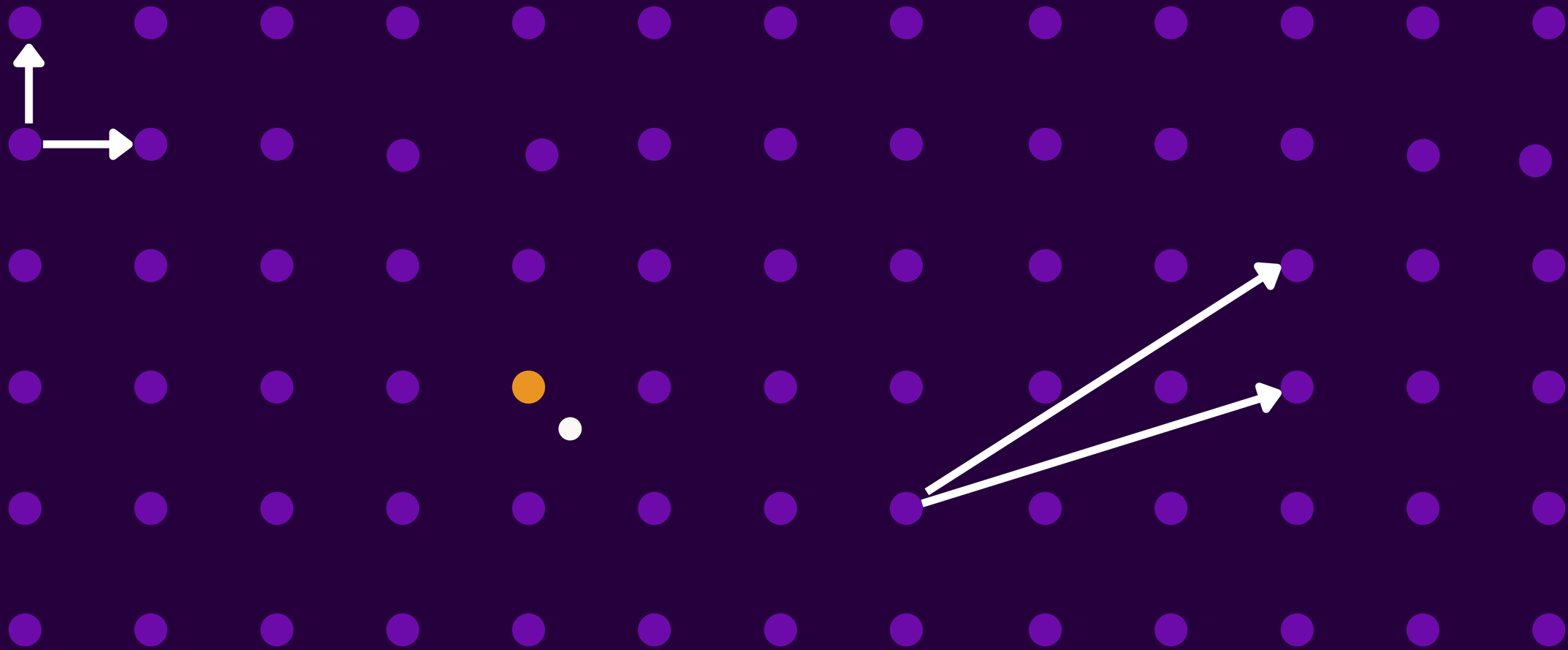
a + b
a + 2b
2a + b
3a+ 4b

Points of Lattice

LATTICE BASED ENCRYPTION

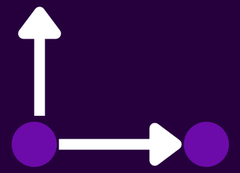


LEARNING WITH ERRORS



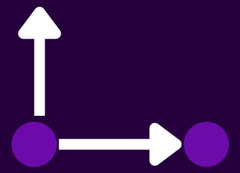
WLUG
COMMUNITY | KNOWLEDGE | SHARE

LEARNING WITH ERRORS



WLUG
COMMUNITY | KNOWLEDGE | SHARE

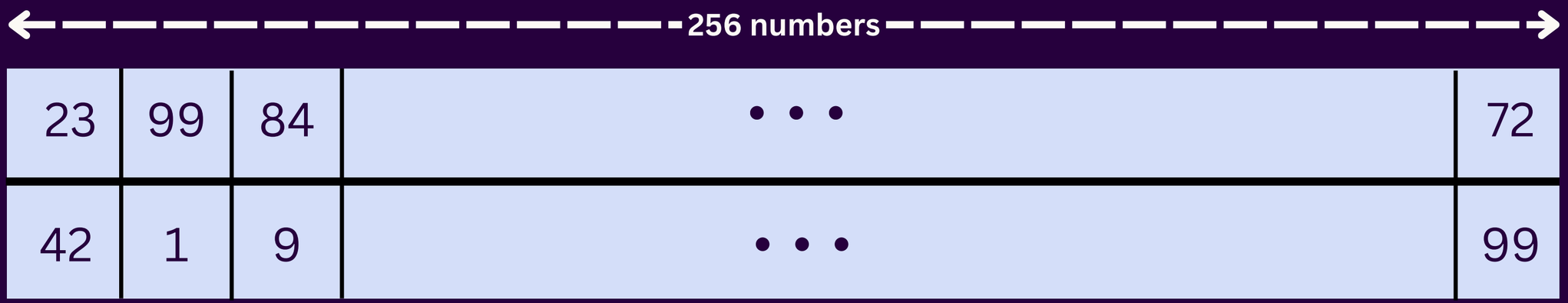
LEARNING WITH ERRORS



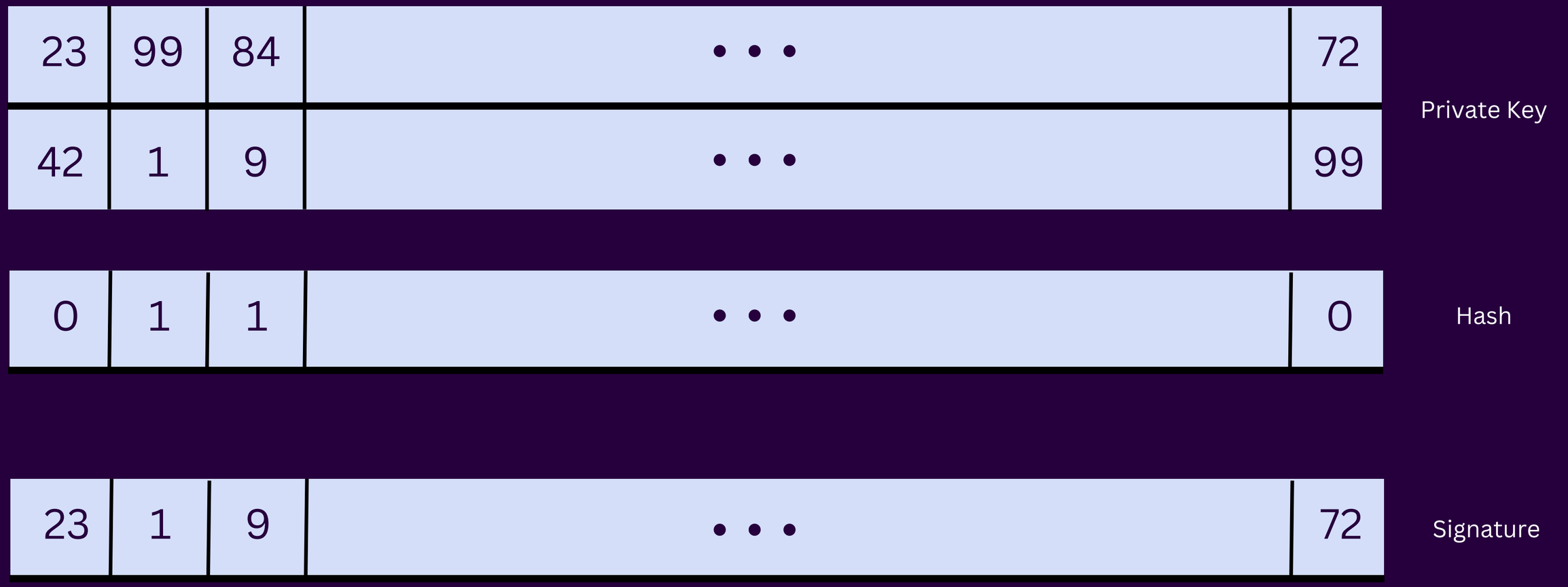
WLUG
COMMUNITY | KNOWLEDGE | SHARE

HASH BASED ENCRYPTION

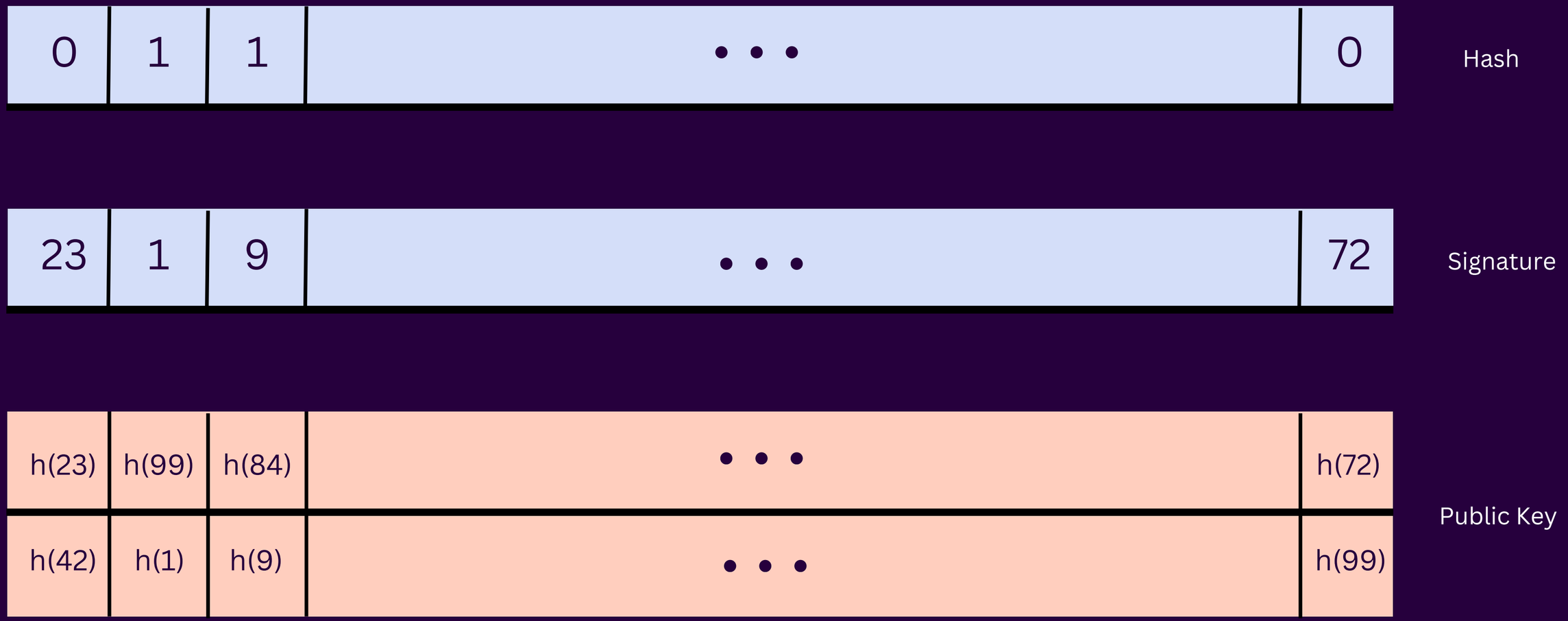
LAMPORT SIGNATURES



SIGNATURES

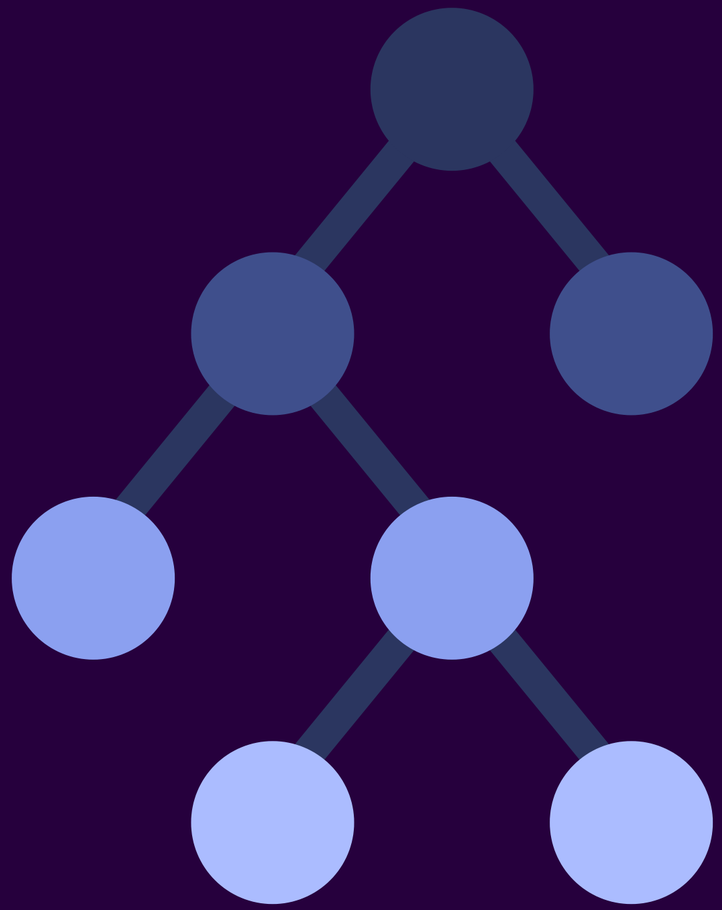


VERIFICATION



MERKLE TREES

- Each node’s value is the hash of its children
- We generate multiple private keys, then construct a Merkle tree from them
- The root of three represents Public key
- Signature consist of the private key, and its path too root node
- Each private key can be used once



WLUG
COMMUNITY | KNOWLEDGE | SHARE

THANK YOU