POST-QUANTUM CRYPTOGRAPHY

By

Gitanjali Venkatraman

INTRODUCTION

WE UNDERSTAND THE POTENTIAL OF QUANTUM COMPUTERS TO THREATEN THE SECURITY OF CURRENT ENCRYPTION SCHEMES.

THE REACTION TO THIS RISK IS THAT MUCH EFFORT HAS BEEN PUT INTO CLASSICAL (NON-QUANTUM) ALGORITHMS THAT CAN RESIST QUANTUM ATTACKS.

THE ILLUSTRATED GUIDE TO POST QUANTUM CRYPTOGRAPHY DESCRIBES THE NATURE OF THESE CLASSICAL ALGORITHMS.

STARTING FROM WHY THIS NEEDS TO BE ADDRESSED, WE GO ON TO EXPLORING A GLOBAL COMPETITION TO IDENTIFY SUITABLE ALGORITHMS.

FAR TOO MANY BRILLIANT MINDS HAVE CONTRIBUTED TO THE RESEARCH TO MENTION INDIVIDUALLY.

ONCE WE'VE COVERED THE WORKINGS OF A HANDFUL OF ALGORITHMS, WE ALSO TAKE A LOOK AT WHAT IT MEANS TO MIGRATE TO A POST QUANTUM CRYPTO SCHEME.

PREREAD THESE ILLUSTRATED GUIDES FROM THOUGHTWORKS

HOW TO TELL SECRETS

THE STORY OF QUANTUM COMPUTING

GUIDE TO AES

WEB 3 — THE PART ON MERKLE TREES

WHAT IS PQC?

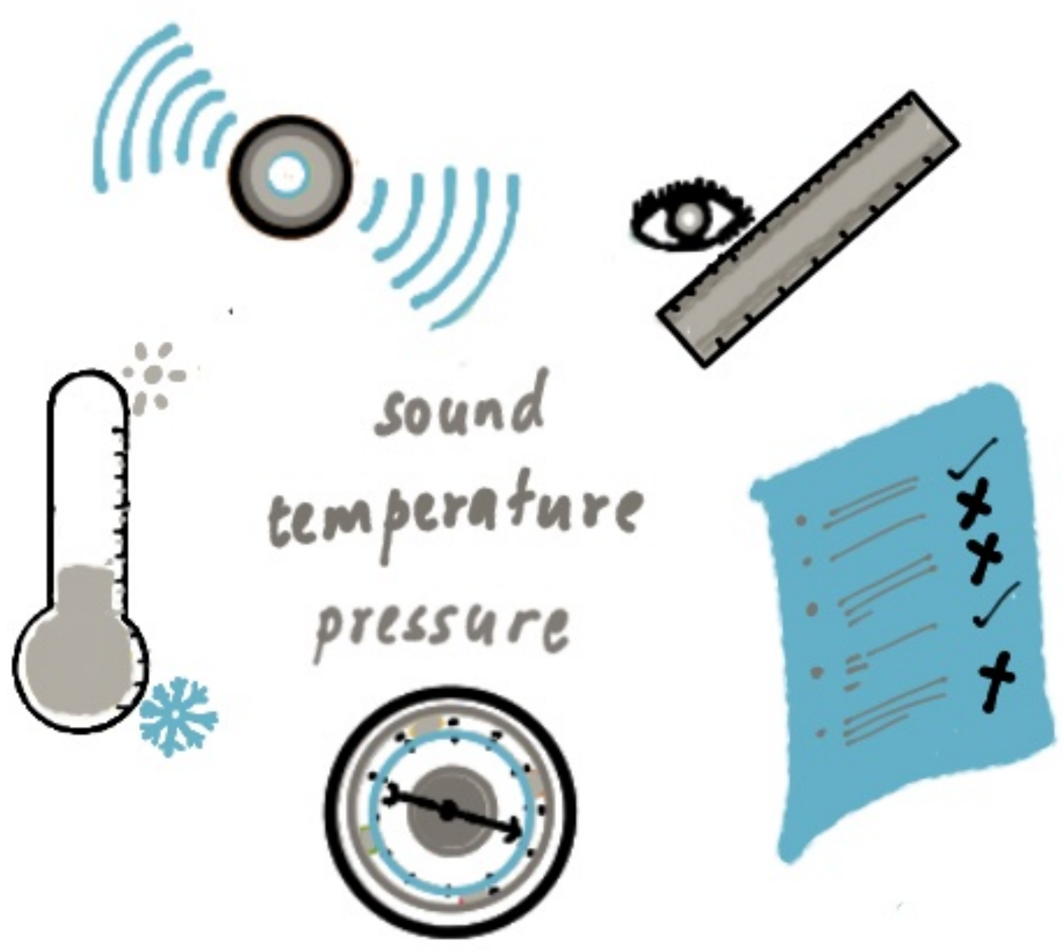
POST QUANTUM CRYPTOGRAPHY OR PQC IS THE FOCUS ON DEVELOPING CLASSICAL ALGORITHMS THAT ARE SAFE FROM ANY DECRYPTION ATTEMPTS BY QUANTUM ALGORITHMS

IS PUBLIC KEY CRYPTOGRAPHY BROKEN?

THE PUBLIC KEY CRYPTOGRAPHY IN USE WORKS ONLY TO DEFEND AGAINST CLASSICAL — NOT QUANTUM COMPUTERS

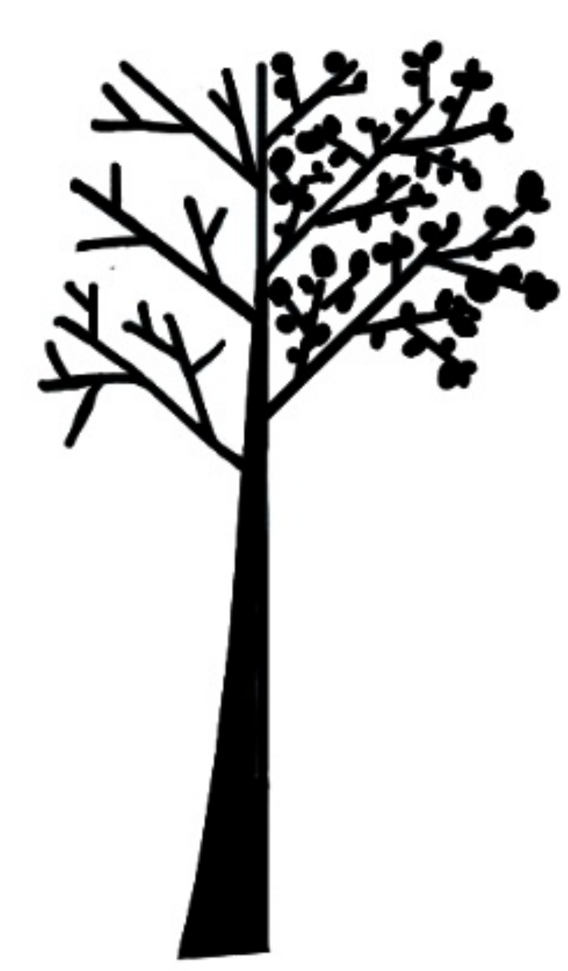
WHY NOW?

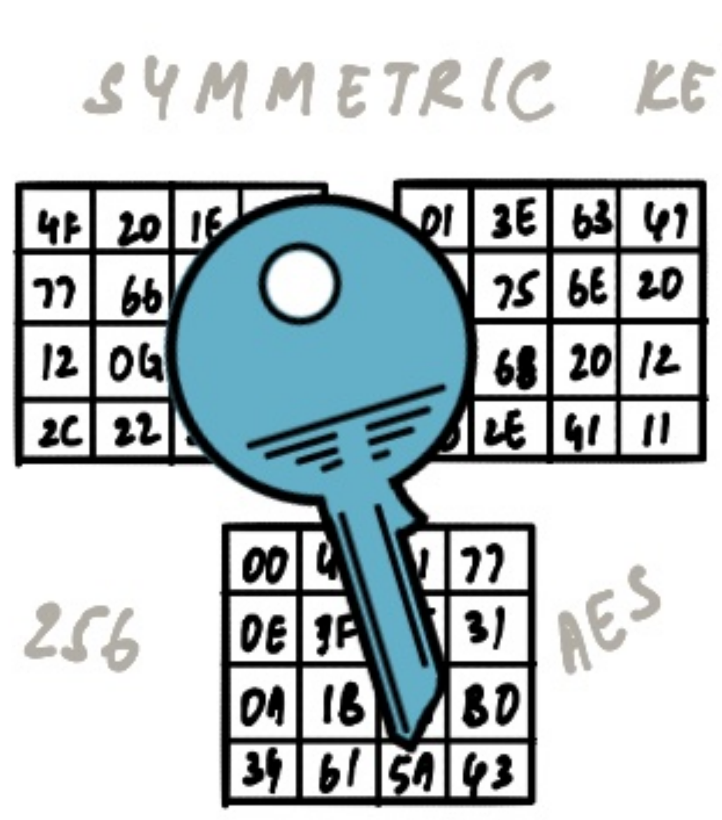
WHY THE SEARCH FOR POST-QUANTUM CRYPTOGRAPHY? A USEFUL QUANTUM COMPUTER ISN'T HERE ... YET!



A QUANTUM COMPUTER IS STILL SUSCEPTIBLE TO NOISE AND ERRORS

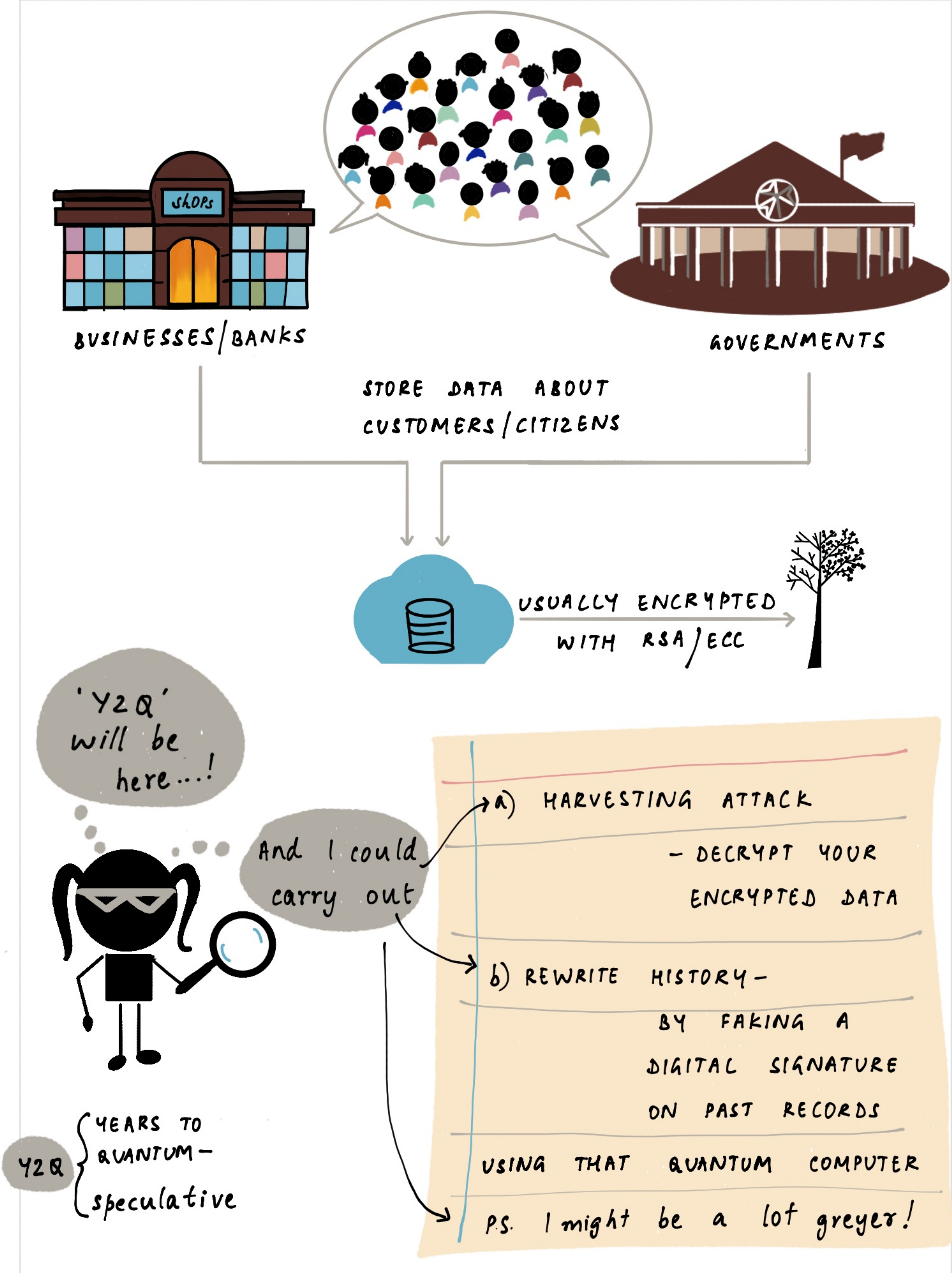
RSA, ECC & OTHER ASYMMETRIC ENCRYPTION & DIGITAL SIGNATURE METHODS ARE STILL STRONG – RIGHT?





BESIDES, AES 256 IS QUANTUM-PROOF!

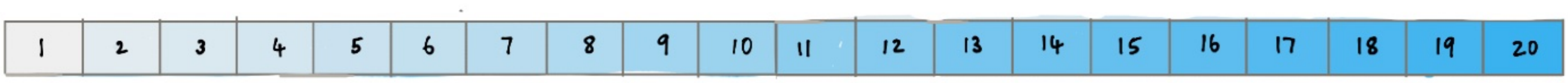
REASON 1: ATTACKS



REASON 2: TIME

ACCORDING TO THE NIST, IT TAKES A LONG TIME TO ROLL OUT NEW ENCRYPTION AT SCALE

MODERN PUBLIC KEY CRYPTOGRAPHY INFRASTRUCTURE HAS TAKEN



20 YEARS TO DEPLOY

SO NOW MIGHT BE A GOOD TIME TO START BEING CURIOUS ABOUT HOW TO PREPARE IT SYSTEMS FOR THE FUTURE

MOSCA'S THEOREM

HOW LONG DOES DATA NEED TO BE SECURE?	HOW LONG UNTIL A QUANTUM SAFE SOLUTION?
x	y

HOW LONG UNTIL A USEFUL AND POWERFUL QUANTUM COMPUTER?
z

IF $x + y > z$

WE HAVE A PROBLEM

Highlights the store now decrypt later problem

MICHELE MOSCA

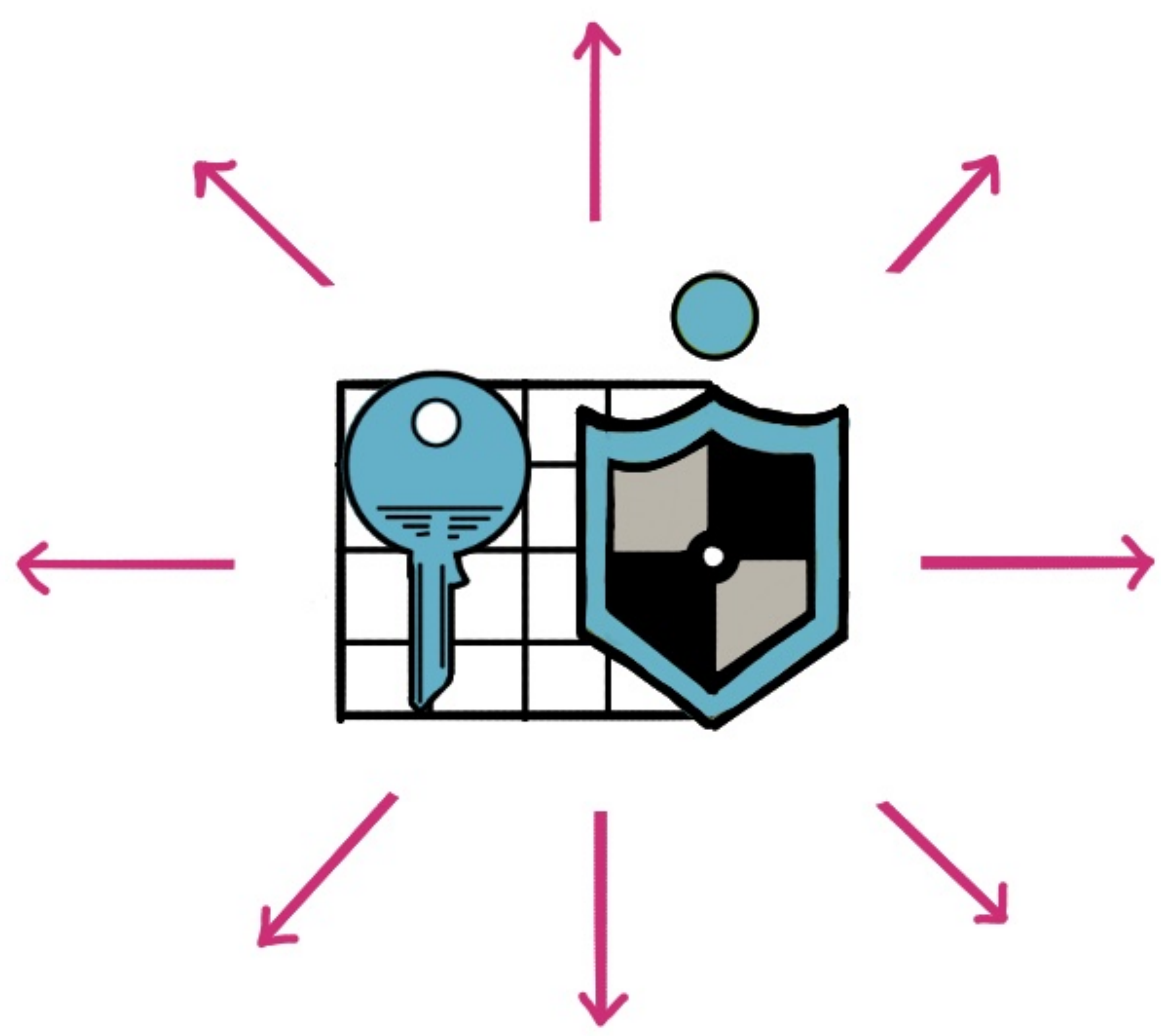
MATHEMATICIAN & COMPUTER SCIENTIST

WHAT OPTIONS DO WE HAVE?

OPTION - 1

USE AES, HOWEVER...

AES IS QUANTUM-SAFE
SYSTEMS AROUND IT ARE NOT



WHAT'S THE SOLUTION?

INCREASE THE SIZES OF AES KEYS

+

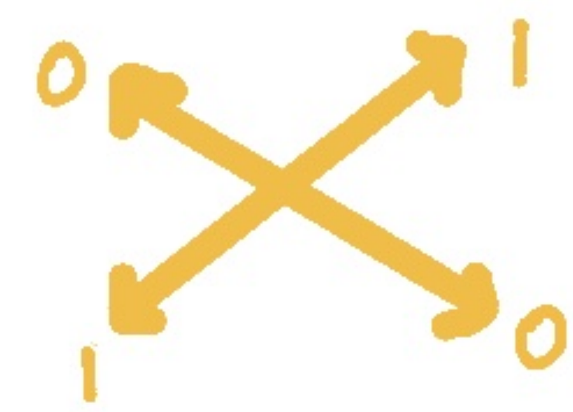
FIND SECURE WAYS TO DISTRIBUTE THE KEY

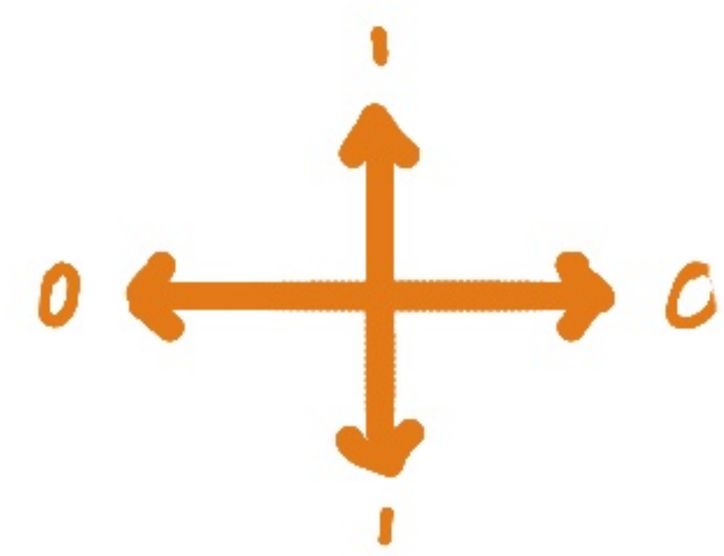
WHAT OPTIONS DO WE HAVE?

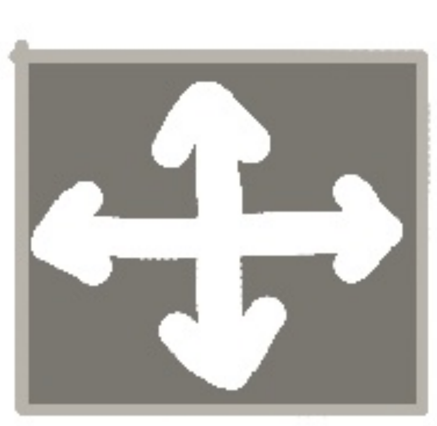
OPTION - 2

USE QUANTUM KEY DISTRIBUTION - QKD

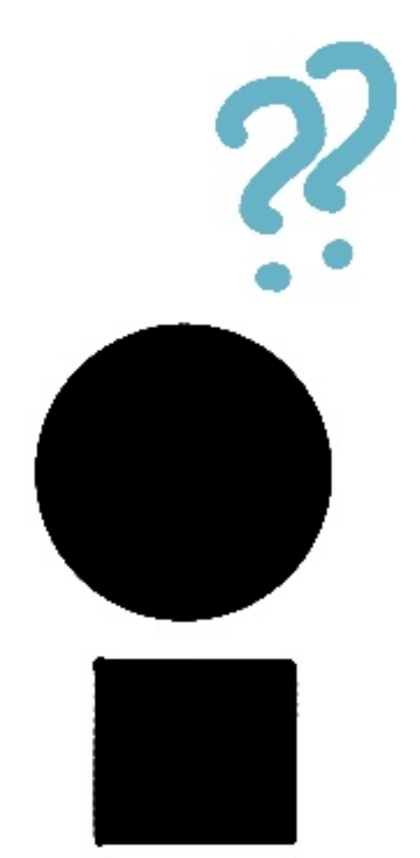
ALICE
SENDS
POLARISED LIGHT
WHICH ENCODES BITS
RANDOMLY
IN ONE
OF 2
METHODS







BOB
MUST GUESS
WHICH METHOD
AND
'READ'
THE PHOTON



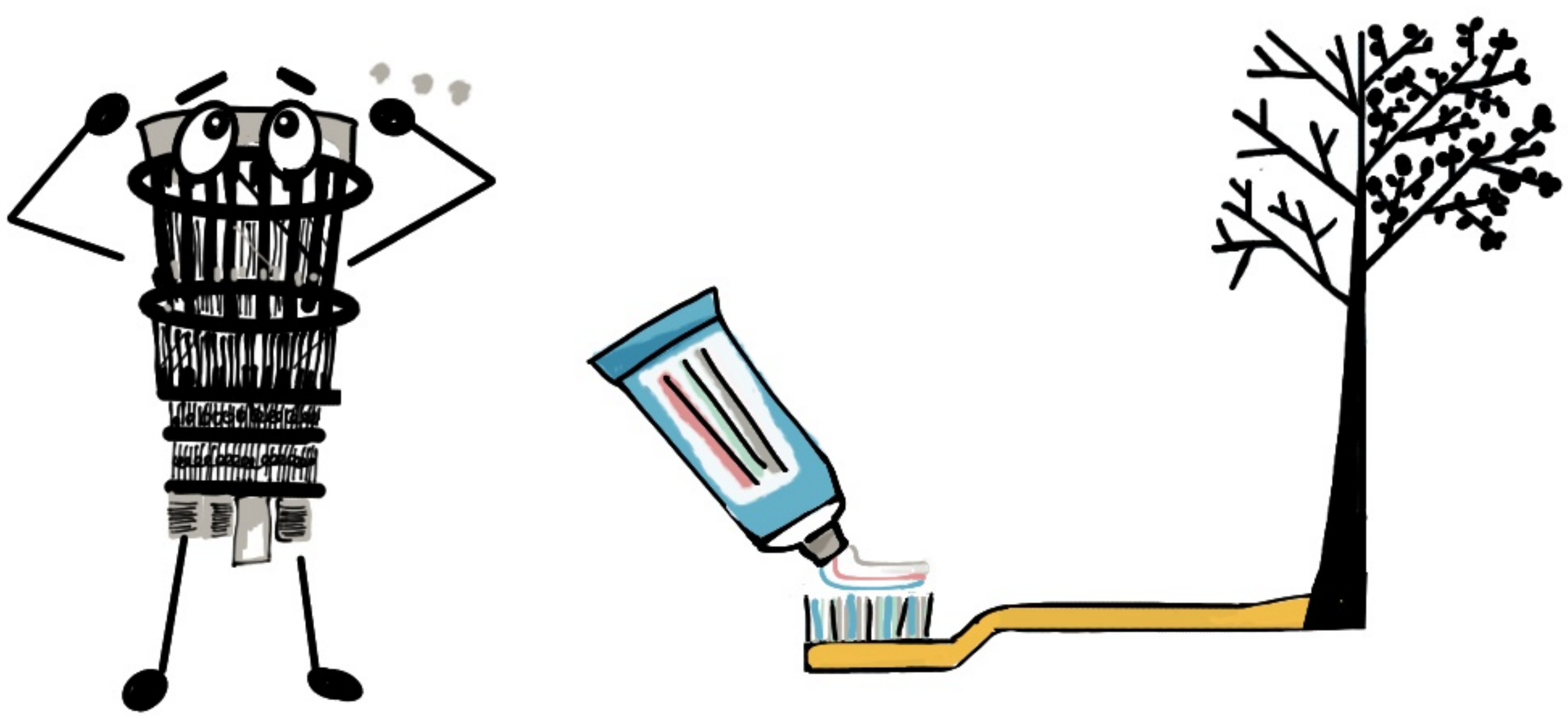
THIS IS NOT YET FEASIBLE AT SCALE

WHAT OPTIONS DO WE HAVE?

OPTION - 3

FIND 'QUANTUM-SAFE' ENCRYPTION

ALGORITHMS HARD FOR QUANTUM COMPUTERS TO CRACK



CONSTRUCT COMPLEX TRAPDOOR FUNCTIONS

EASY TO DO

HARD TO UNDO

FOR CLASSICAL + QUANTUM COMPUTERS

THIS BOOK IS ABOUT QUANTUM-SAFE ALGORITHMS AND HOW THEY WORK

TO CLARIFY

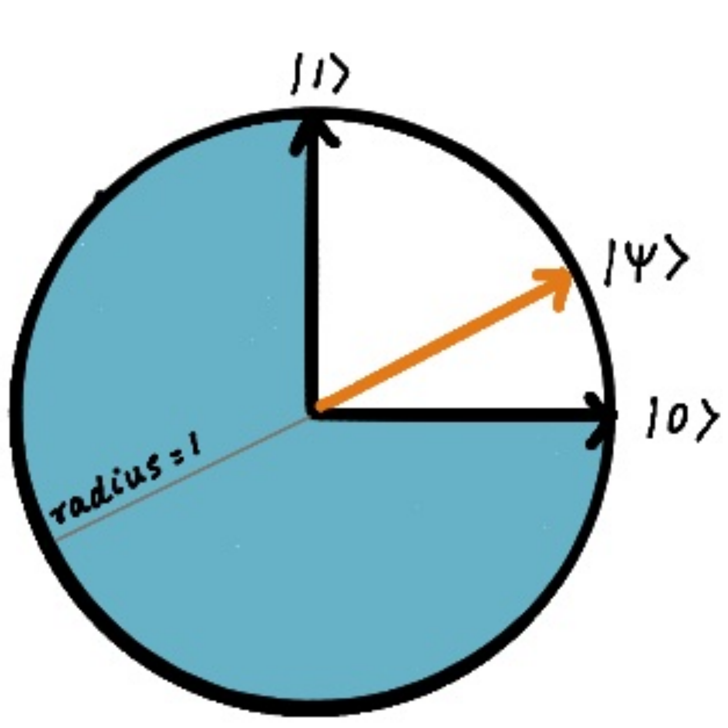
QUANTUM ALGORITHMS ≠ **QUANTUM RESISTANT ALGORITHMS**

QUANTUM ALGORITHMS
- SHOR'S ALGORITHM
- GROVER'S ALGORITHM

QUANTUM RESISTANT ALGORITHMS
- KYBER
- SPHINCS+

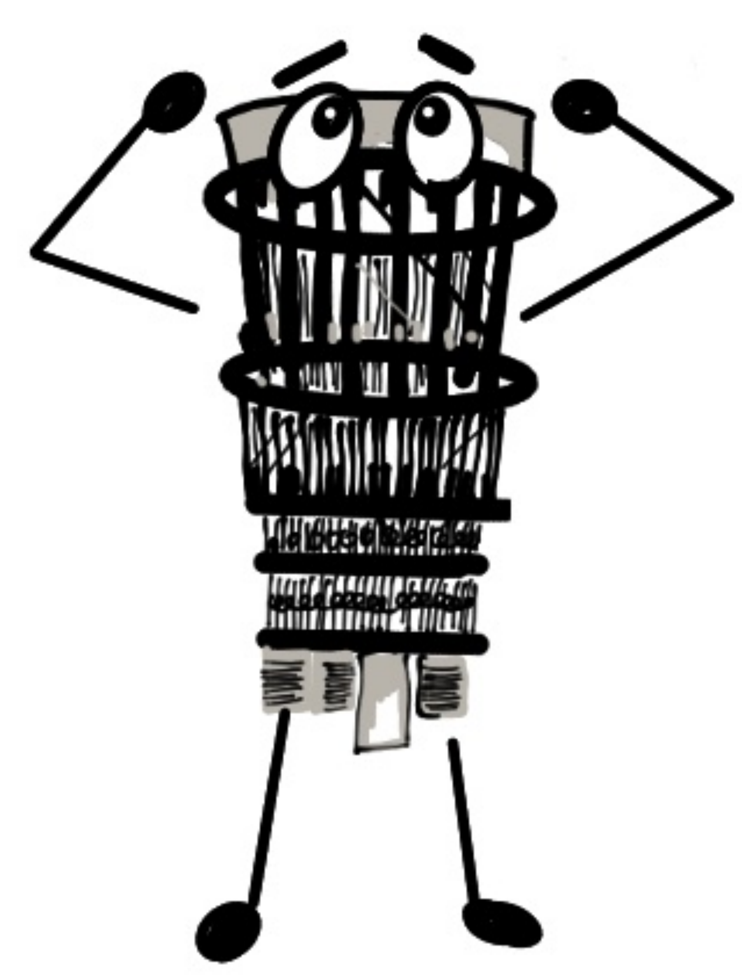
QUANTUM ALGORITHMS USED BY

QUANTUM COMPUTERS TO SOLVE PROBLEMS

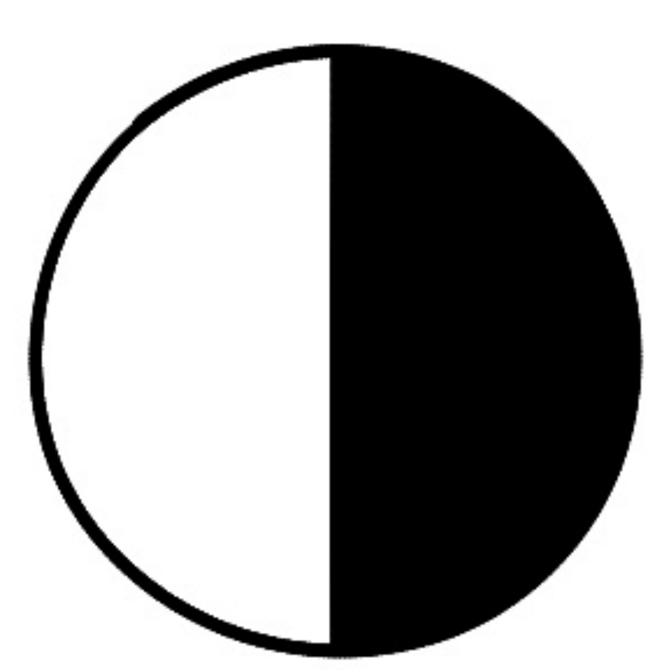


✓ YES, QUBITS ARE USED

CLASSICAL ALGORITHMS THAT



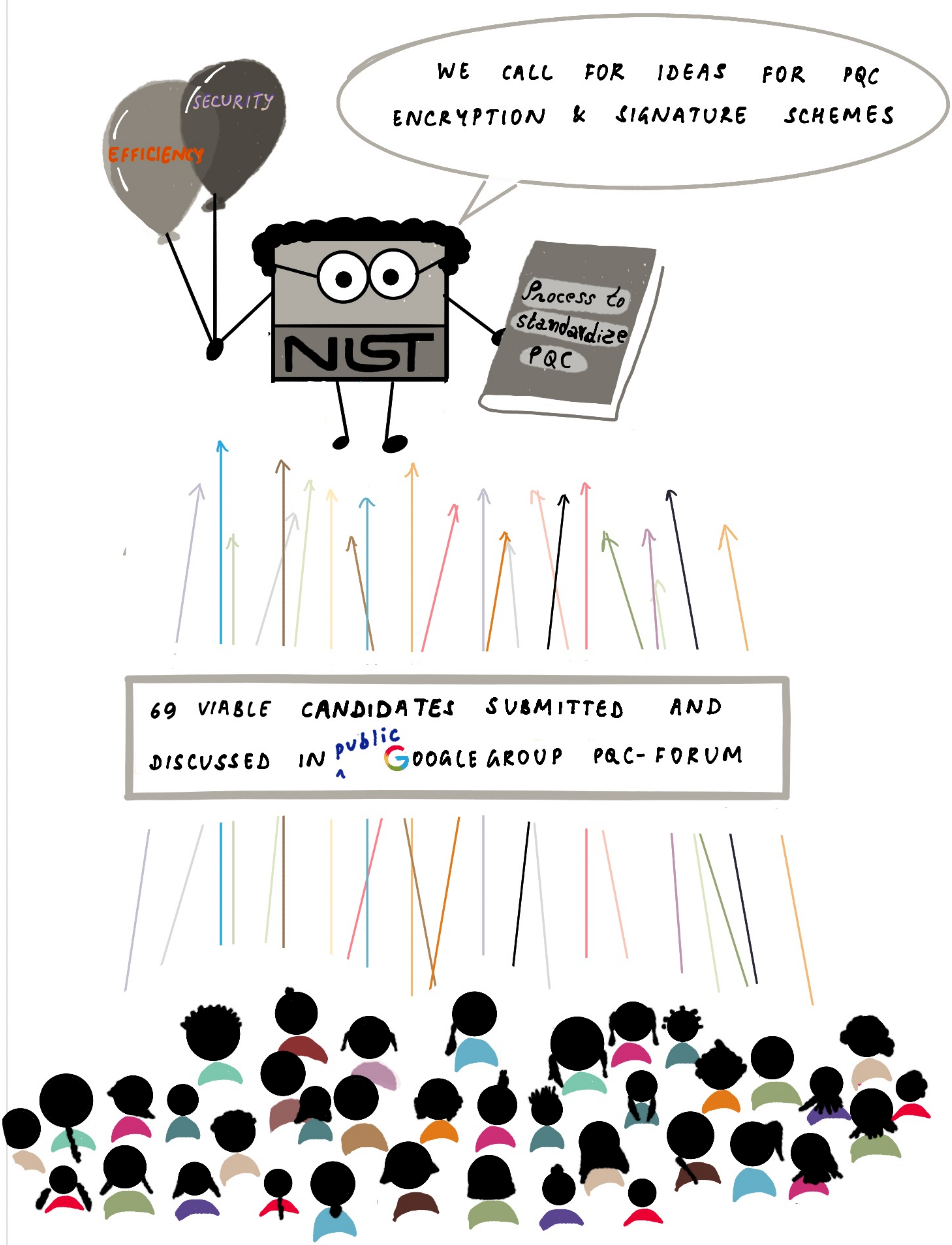
QUANTUM COMPUTERS CANNOT CRACK/SOLVE



✓ GOOD OLD BITS ARE USED

IT BEGAN IN 2016

NIST- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY



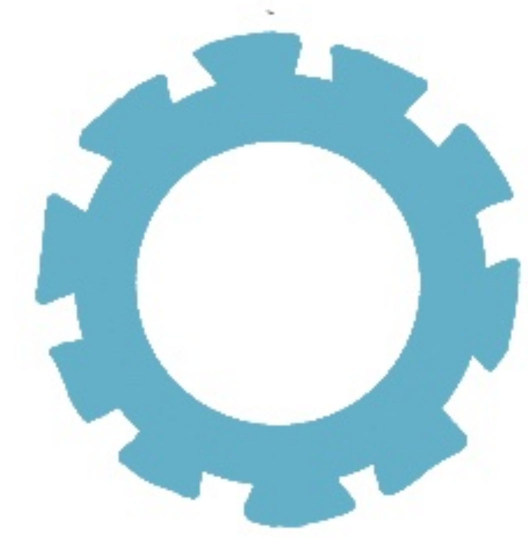
SELECTION CRITERIA

SECURE

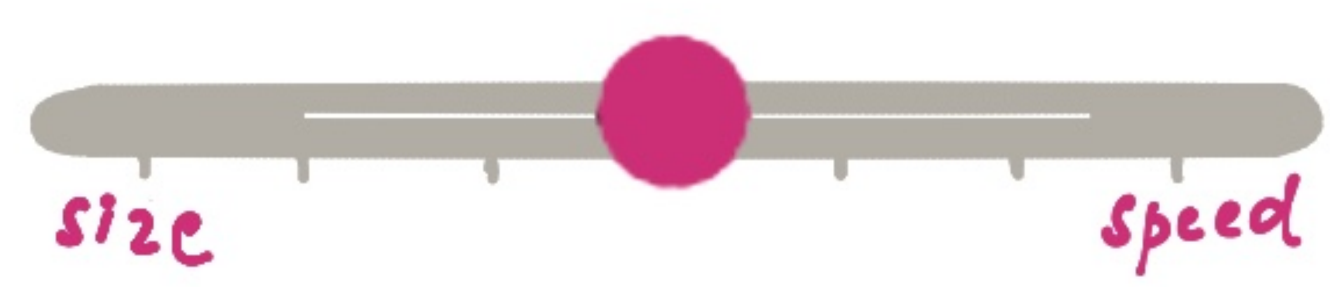
- AGAINST ATTACKS FROM BOTH CLASSICAL AND QUANTUM COMPUTERS
- BASED ON A HARD PROBLEM

CONFIGURABLE

- 5 LEVELS OF SECURITY



- PICK THE TRADEOFFS



EFFICIENCY

- KEY SIZES
- SIGNATURE SIZES
- CIPHER TEXT SIZES
- MEMORY
- BANDWIDTH

OTHERS

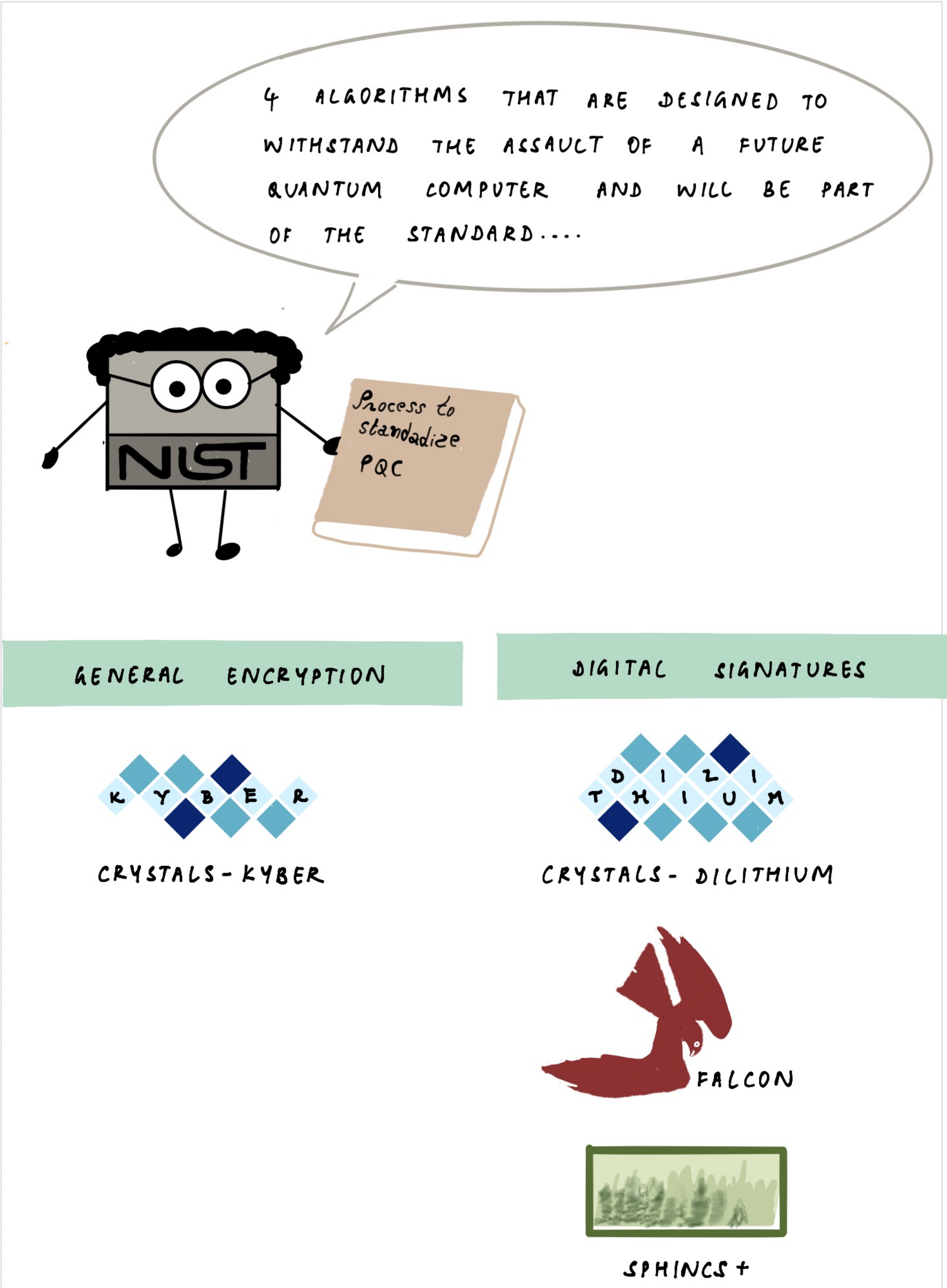
SIMPLICITY

EASE OF ANALYSIS

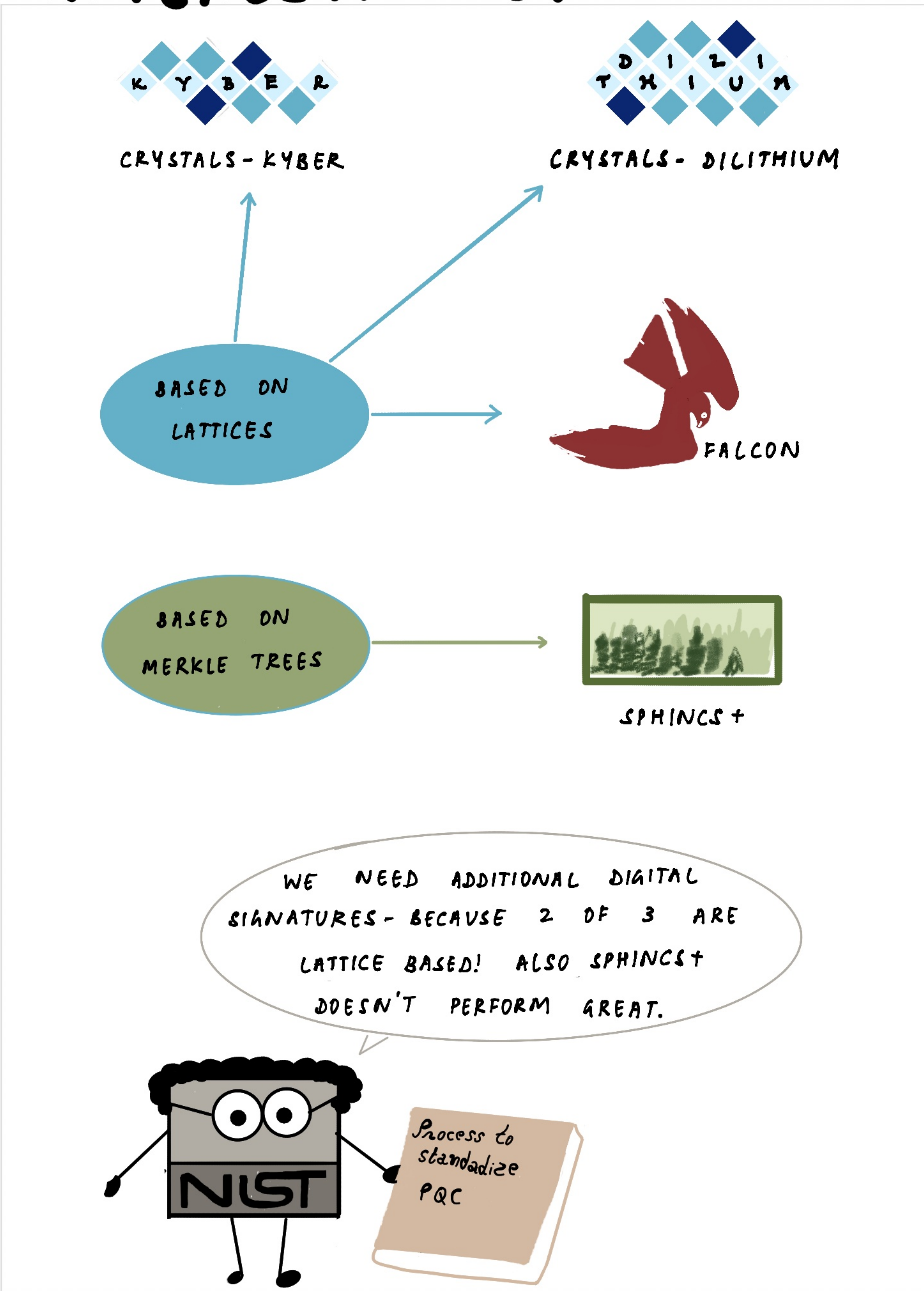
RESILIENCE TO SIDE-CHANNEL ATTACKS

COMPATIBILITY WITH EXISTING PROTOCOLS

IN 2022


4 ALGORITHMS THAT ARE DESIGNED TO WITHSTAND THE ASSAULT OF A FUTURE QUANTUM COMPUTER AND WILL BE PART OF THE STANDARD....
NIST
Process to standadize PQC
GENERAL ENCRYPTION
K Y B E R
CRYSTALS - KYBER
DIGITAL SIGNATURES
CRYSTALS - DILITHIUM
FALCON
SPHINCS +

INTERESTINGLY



IN 2024

HQC

Classic McEliece

BIKE

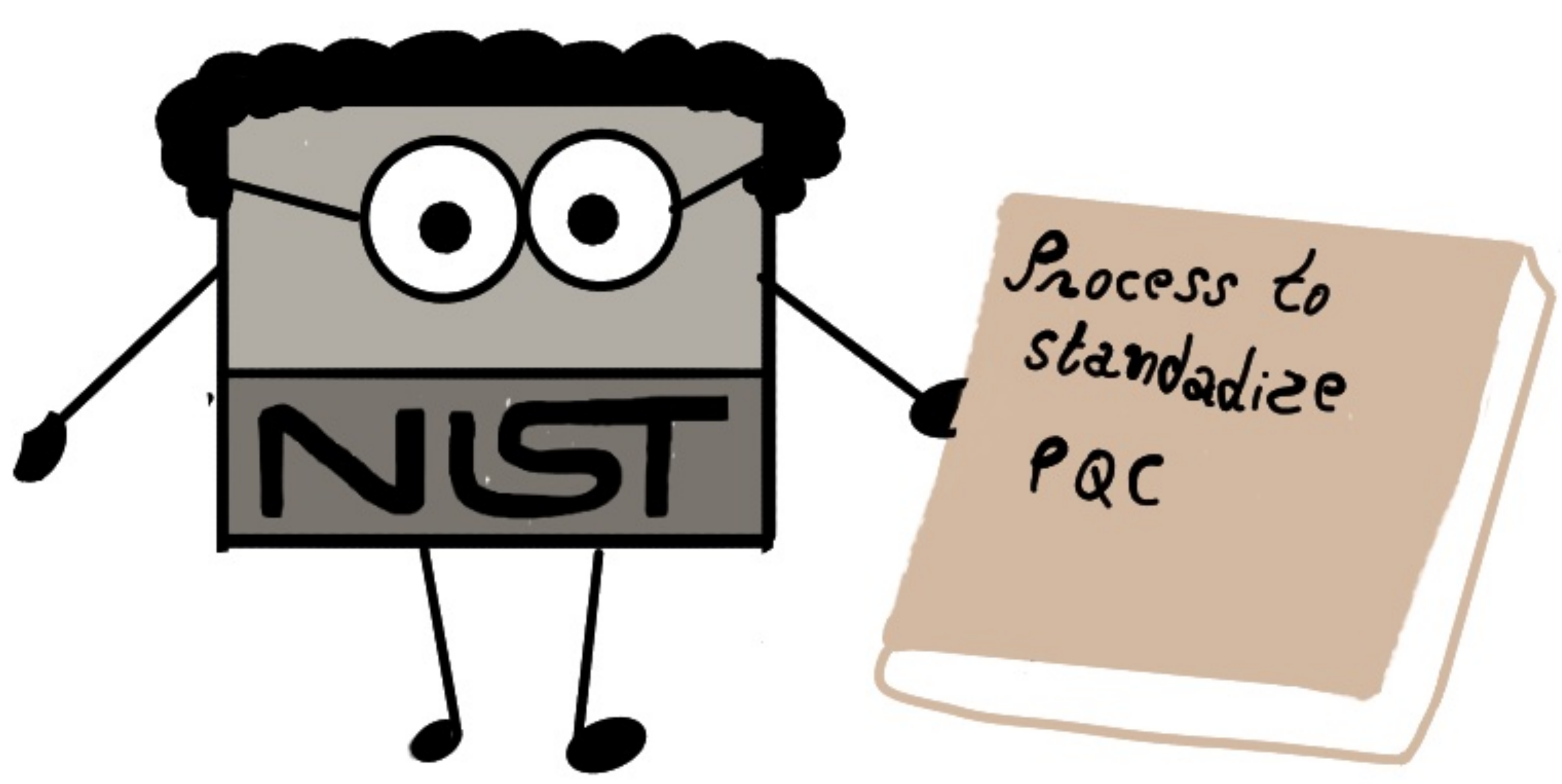
HQC

CLASSIC MCELIECE

BIT FLIPPING KEY ENCAPSULATION

HAMMING QUASI-CYCLE

NAMED AFTER ROBERT J MCELIECE



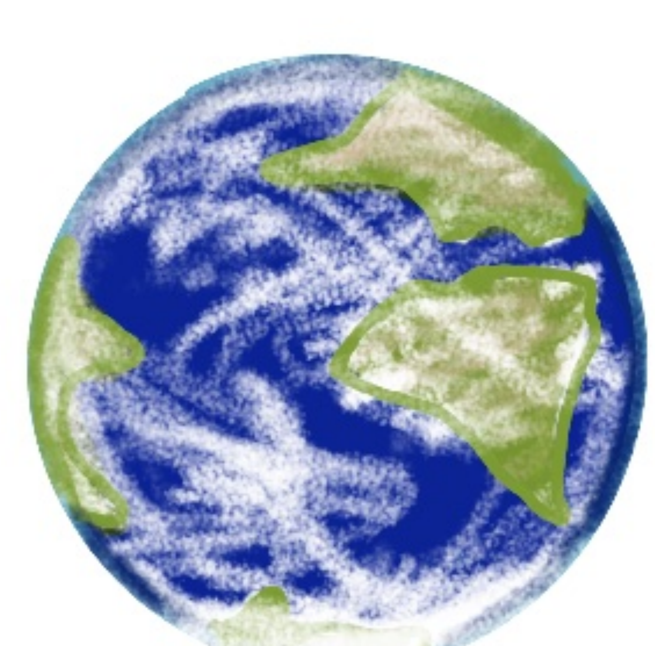
WILL PRESENT THEIR UPDATES TO BE CONSIDERED PART OF THE STANDARD FOR KEY ENCAPSULATION MECHANISM AT THE 5TH NIST PQC STANDARDISATION CONFERENCE

STANDARDS ORGANISATIONS

THESE ARE NAMES OF STANDARDS ORGANISATIONS THAT NIST ALSO WORKS WITH.

- ASC X9
- IEEE
- IETF
- ETSI
- PQCRYPTO
- SAFECRYPTO
- ISO/IEC JTC

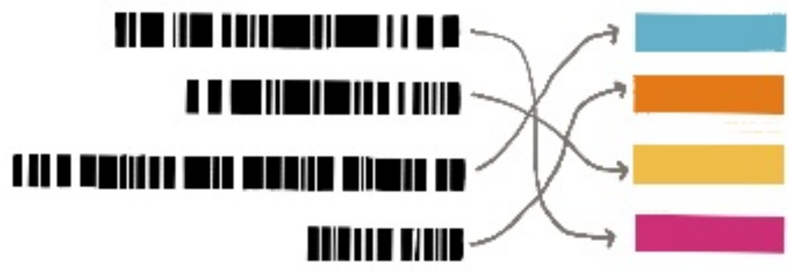
THEY FREQUENTLY PUBLISH GUIDELINES AND PAPERS.



AS AN ASIDE, SOME COUNTRIES LIKE GERMANY, JAPAN, CHINA, RUSSIA, SOUTH KOREA ETC HAVE THEIR OWN STANDARDS.

QUANTUM-SAFE SCHEMES

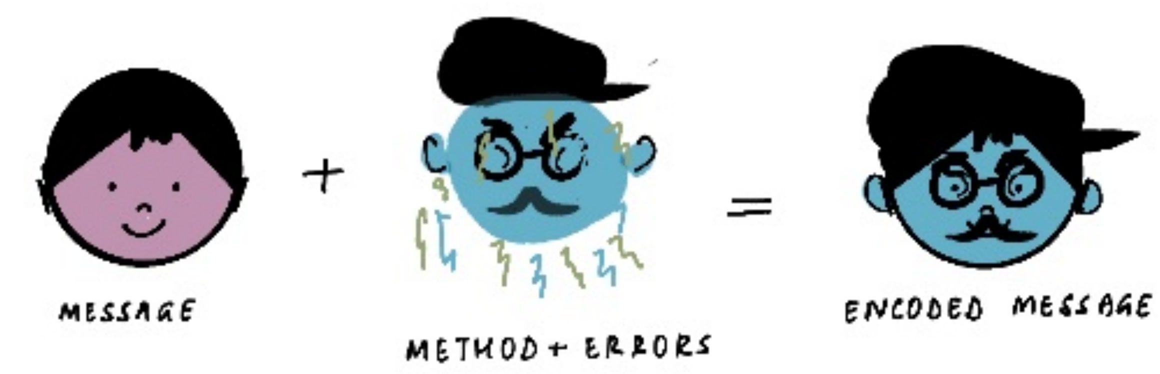
HASH BASED



SPHINCS +

USE HASH FUNCTIONS FOR SIGNATURES

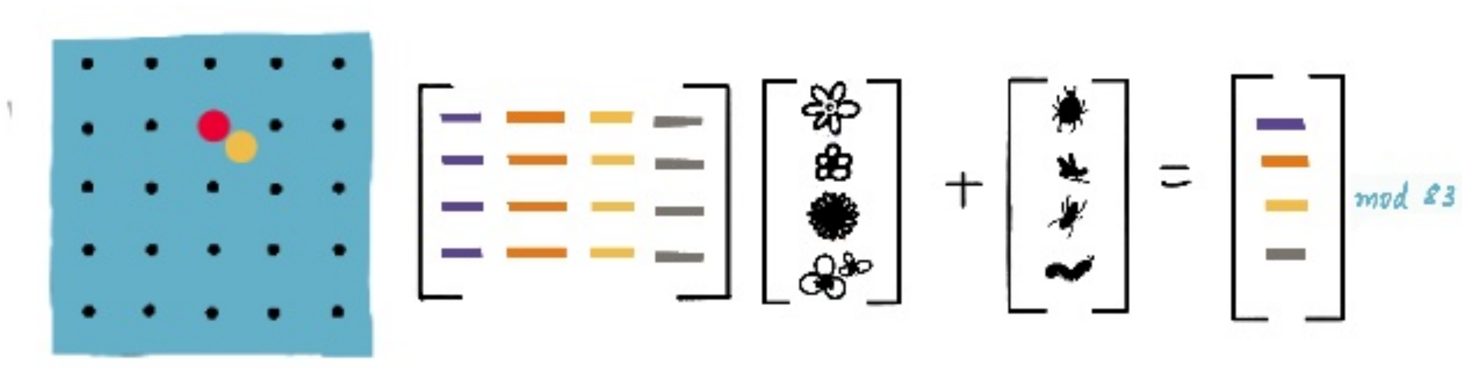
CODE BASED



McELIECE

USES ERROR CORRECTING CODES FOR ENCRYPTION

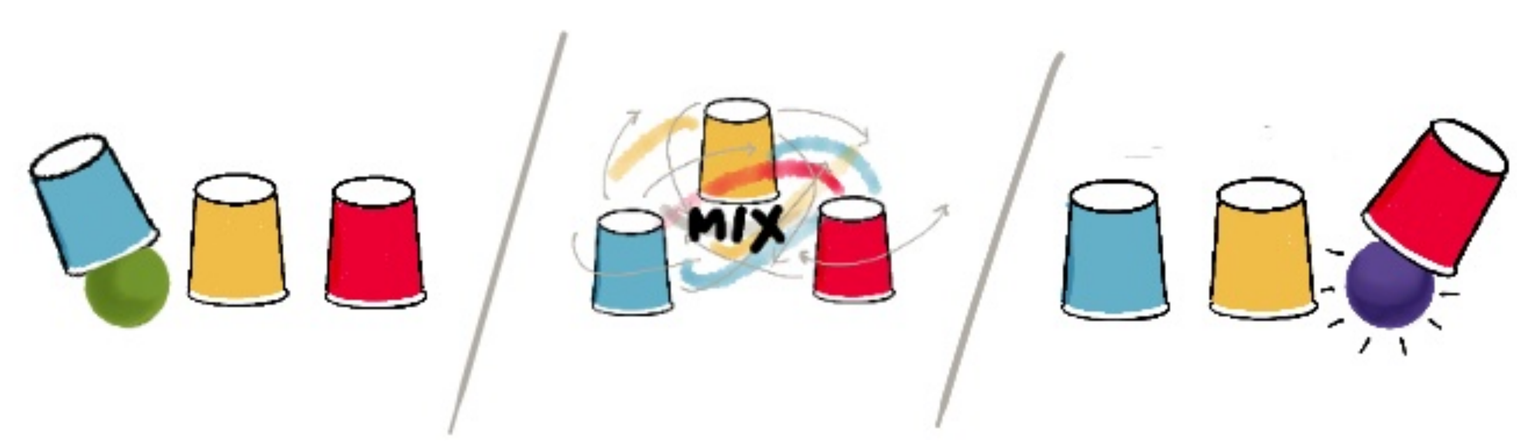
LATTICE BASED



KYBER

USES LATTICE BASED NP HARD PROBLEMS

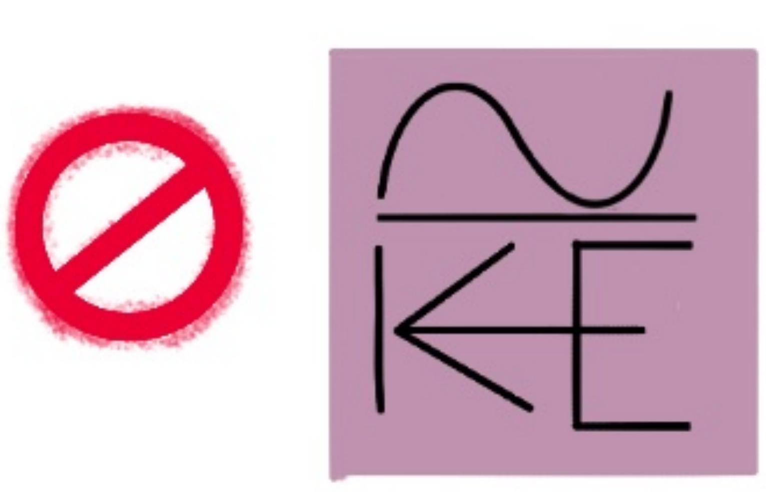
SYMMETRIC KEYS



AES

IDEAS THAT TRIED - AND FAILED - TO BE SECURE

ISOGENY BASED



MATHEMATICAL FUNCTIONS IN AN ELLIPTIC CURVE

SIKE

MULTIVARIATE

USES EQUATIONS WITH MULTIPLE VARIABLES

RAINBOW

DEVELOPING AN INTUITION

IN THE NEXT FEW PAGES, WE WILL VISIT SOME OF THE CANDIDATE ALGORITHMS TO GAIN AN UNDERSTANDING OF THE PRINCIPLES/IDEAS BASED ON WHICH THEY WORK.

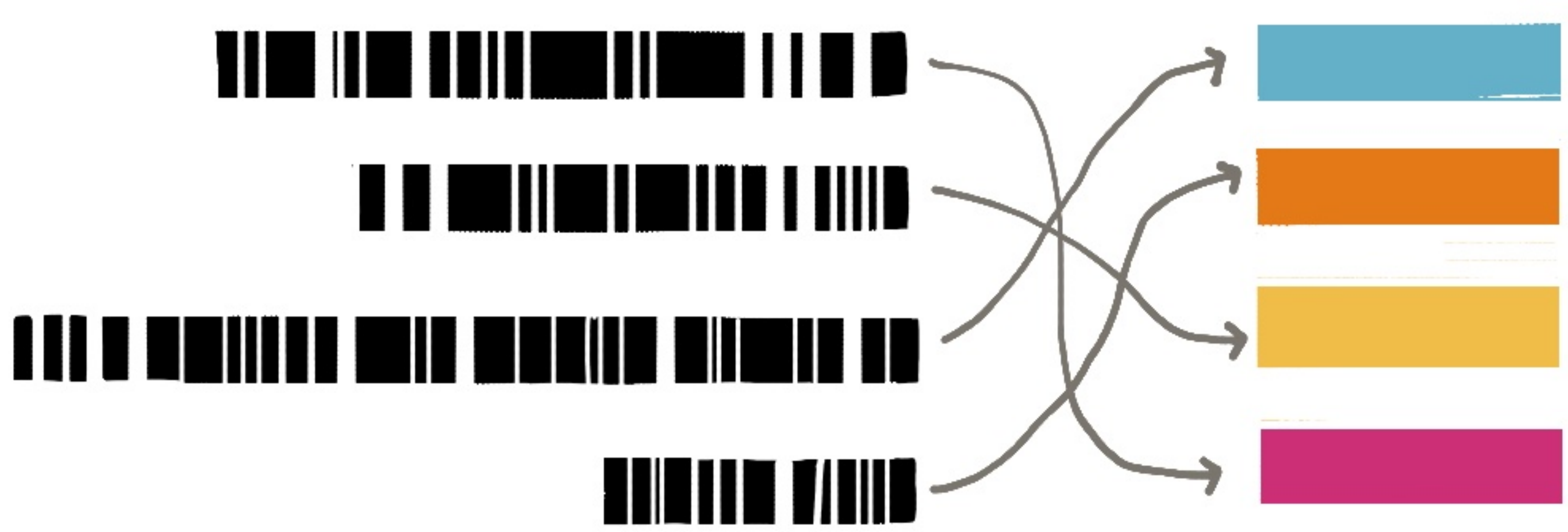
WHILE WE WILL NOT BE GOING INTO STEP-BY-STEP WALKTHROUGH OF THE ALGORITHMS, I HOPE VERY MUCH THAT THE READER WILL GET AN APPRECIATION FOR THE DESIGN OF THE ALGORITHM AND WHAT MAKES IT HARD.

HASH BASED CRYPTOGRAPHY

HASH BASED CRYPTOSYSTEMS

HASH BASED ENCRYPTION SCHEMES USE HASH FUNCTIONS AS THE BASIS FOR CREATING DIGITAL SIGNATURES

A HASH FUNCTION MAPS DATA TO A FIXED LENGTH VALUE



THE HASH IS A ONE WAY MATHEMATICAL FUNCTION

EASY TO DO

INFEASIBLE TO UNDO

HASH: SIMPLE EXAMPLE

A made-up hashing algorithm:	(Data is 41)
Square it	41 × 41 = 1681
split numbers into 2 groups	16 81
Add the 2 groups	16 + 81 = 97

✓ THIS IS EASY TO CALCULATE

Hash (59) = 115

Hash (40) = 16

Hash (42) = 81

HOWEVER, IT IS NEAR IMPOSSIBLE TO WORK OUT WHICH EXACT NUMBERS ADD UP TO 97

ANY OTHER NUMBER PUT THROUGH THIS ALGORITHM WILL RESULT IN A COMPLETELY DIFFERENT HASH

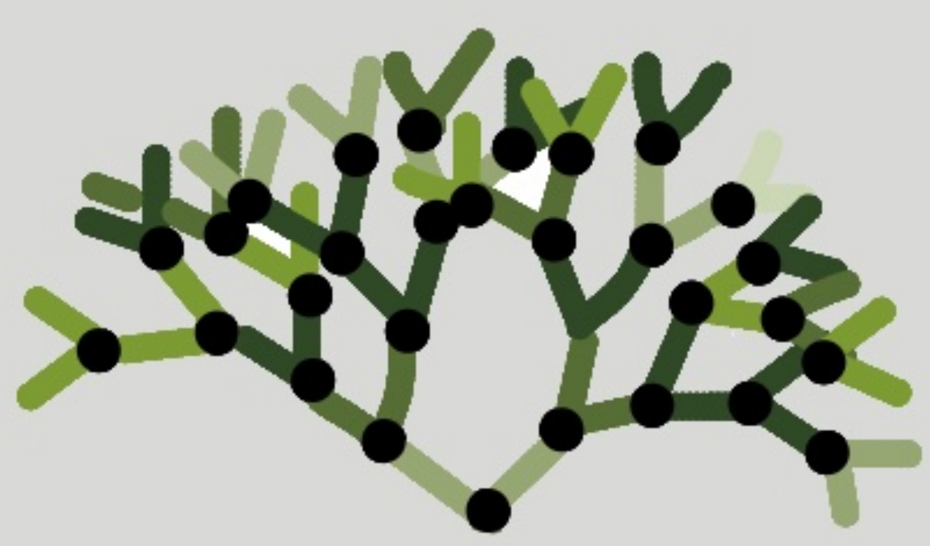
HASHES ARE USED FOR VERIFYING INTEGRITY

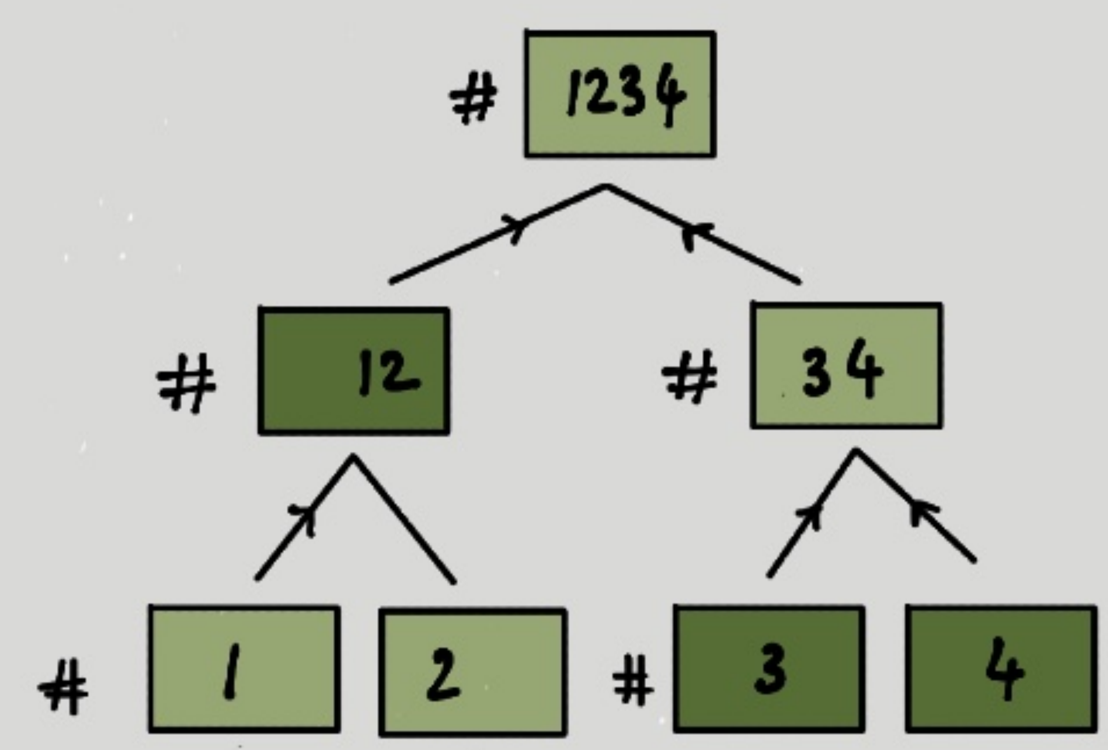
HASH : NIST CANDIDATE

SPHINCS+

SPHINCS+ IN THE NIST LIST IS A HASHING ALGORITHM THAT CENTRES AROUND MERKLE TREES.

A MERKLE TREE IS A TREE OF HASH VALUES.





A NODE IS THE HASH OF ITS CHILD NODES.

HASH BASED ALGORITHMS CAN BE USED IN DIGITAL SIGNATURES.

THE ABSENCE OF STRUCTURE/PATTERNS IN THE HASH MAKES IT HARD FOR QUANTUM COMPUTERS TO EXPLOIT THEM

BENEFITS	CONSIDERATIONS
FAST VERIFICATION SPEEDS	RELATIVELY LARGE SIGNATURE SIZES
WELL UNDERSTOOD BUILDING BLOCKS	DILITHIUM & FALCON PERFORM BETTER

CODE BASED CRYPTOGRAPHY

CODE-BASED CRYPTOSYSTEMS

CODE BASED ENCRYPTION SCHEMES ARE BASED ON THE DIFFICULTY OF DECODING ERROR CORRECTING CODES

AN ERROR CORRECTING CODE ENCODES MESSAGES. SO, EVEN WHEN THE BITS ARE FLIPPED, THEY CAN BE SPOTTED AND RECOVERED!

DECODING A CERTAIN TYPE OF CODE – A LINEAR CODE – IS AN NP COMPLETE PROBLEM.

On the Inherent intractability of certain coding problems

by

E.R. Berlekamp
RJ McEliece
HCA Tilborg, van

Year – 1978

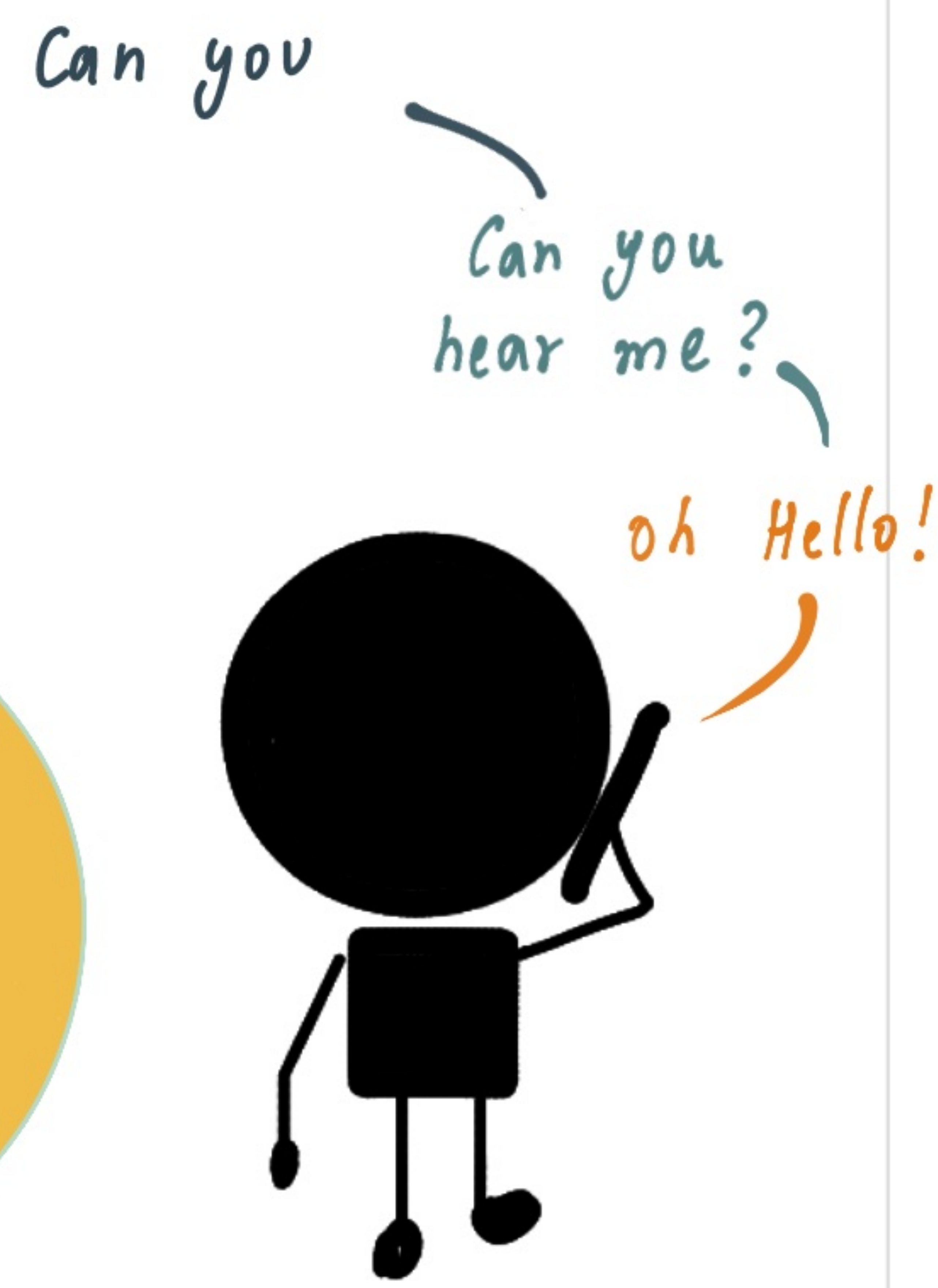
IMPLYING THAT THERE IS NO EFFICIENT POLYNOMIAL-TIME ALGORITHM TO SOLVE IT

CODE: SIMPLE EXAMPLE

LET US TAKE A HIGHLY SIMPLIFIED EXAMPLE USING **HAMMING CODES** TO SEE HOW ERROR CORRECTION WORKS

HAMMING (7,4) CAN CORRECT A SINGLE ERROR

USES PARITY BITS TO BUILD IN REDUNDANCY



ODD PARITY IS ACHIEVED WHEN ADDING BITS

$$(1+0+1+\dots) \bmod 2 = 1$$

EVEN PARITY IS ACHIEVED WHEN ADDING BITS

$$(1+0+1+\dots) \bmod 2 = 0$$

CODE: SIMPLE EXAMPLE

- WE CONSIDER EVEN PARITY FOR THIS EXAMPLE

HAMMING (7,4) USES 4 DATA BITS AND 3 PARITY BITS

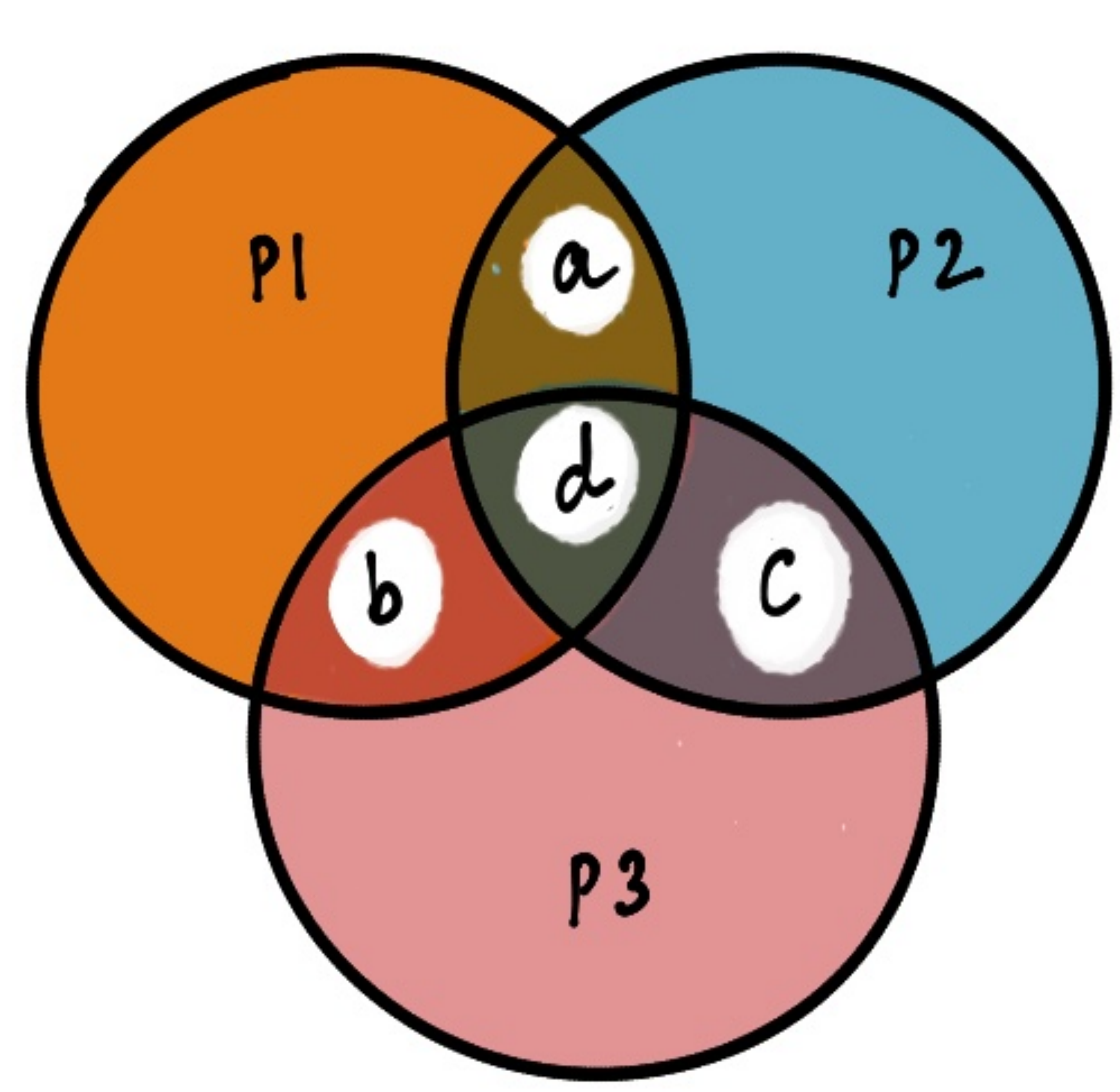
DATA BITS TO ENCODE IS **1011**

PARITY BITS ARE PLACED IN POSITIONS 1,2,4,8....

ENCODING →	P1	P2		P3			
POSITIONS →	1	2	3	4	5	6	7
POSITIONS (BINARY) →	001	010	011	100	101	110	111

DATA BITS ARE PLACED IN THE REST OF THE POSITIONS

P1	P2	a	P3	b	c	d



CODE: SIMPLE EXAMPLE

FINDING VALUES FOR THE PARITY BITS

		a		b	c	d
P1	P2	1	P3	0	1	1
1	2	3	4	5	6	7
001	010	011	100	101	110	111

P1 PARITY

$P1 = a \oplus b \oplus d$

INCLUDES POSITION NUMBERS WITH 1 AS THE LEAST SIGNIFICANT DIGIT

POSITIONS 1, 3, 5, 7 **P1 = 0**

P2 PARITY

$P2 = a \oplus c \oplus d$

INCLUDES POSITION NUMBERS WITH 1 AS THE 2ND LEAST SIGNIFICANT DIGIT

POSITIONS 2, 3, 6, 7 **P2 = 1**

P3 PARITY

$P3 = b \oplus c \oplus d$

INCLUDES POSITION NUMBERS WITH 1 AS THE 3RD LEAST SIGNIFICANT DIGIT

POSITIONS 4, 5, 6, 7 **P3 = 0**

ENCODING IS :

0	1	1	0	0	1	1

CODE: SIMPLE EXAMPLE

ERROR CORRECTION

P1	P2	a	P3	b	c	d
1	2	3	4	5	6	7
001	010	011	100	101	110	111

IF

0	1	1	0	0	1	1

GETS ↓ TRANSMITTED

AS

0	1	1	0	0	0	1

P3 IS POSITIONS → 4 5 6 7 → 0001 → PARITY = 1

P2 IS POSITIONS → 2 3 6 7 → 1101 → PARITY = 1

P1 IS POSITIONS → 1 3 5 7 → 0101 → PARITY = 0

110 — IS POSITION 6 IN BINARY.

FLIP THE BIT IN POSITION 6 TO CORRECT ERROR

CODE: SIMPLE EXAMPLE

HAMMING CODES AND MATRICES

HAMMING CODES SUCH AS THIS

0	1	1	0	0	1	1

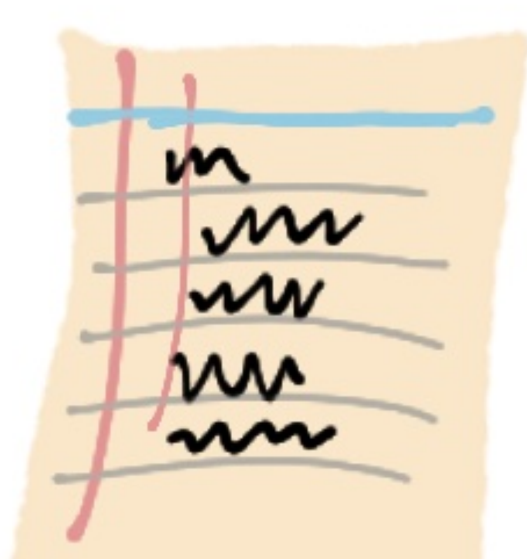
CAN ALSO BE GENERATED USING FORMULAE BASED ON MATRICES

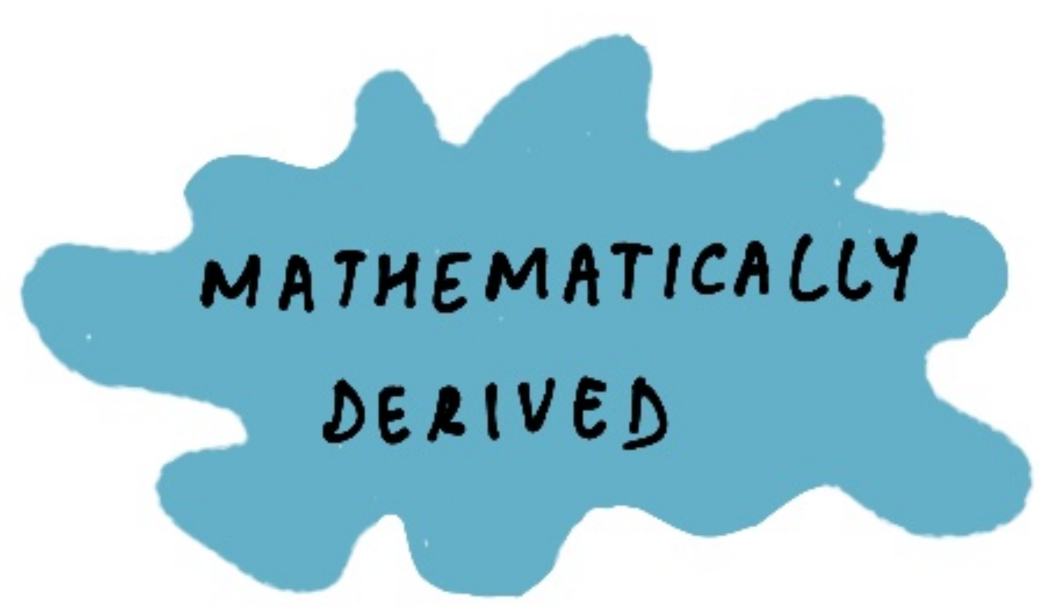
A MATRIX IS DATA ARRANGED IN ROWS AND COLUMNS

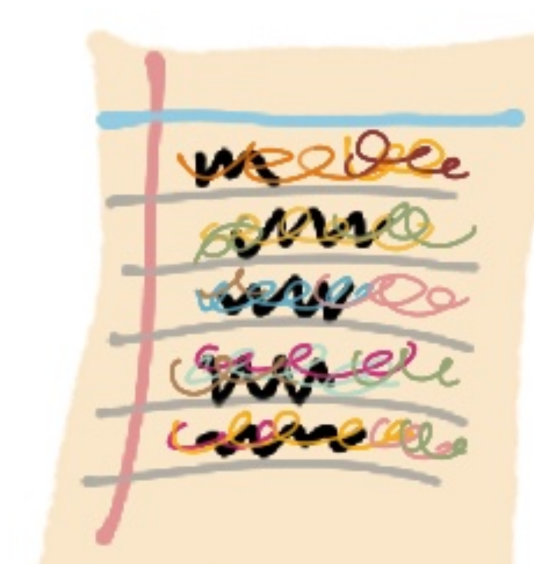
ENCODING A MESSAGE AS A MATRIX

[DATA] · [GENERATOR MATRIX] = [ENCODING]

1×4 · 4×7 = 1×7



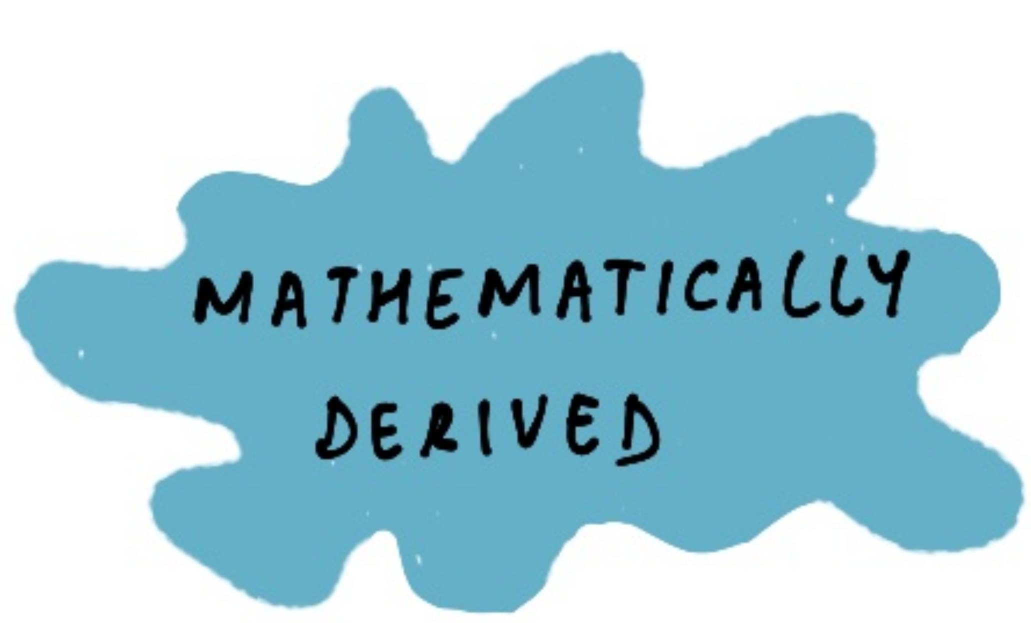




DECODING THE RECEIVED MESSAGE USING MATRICES

[PARITY CHECK MATRIX] · [ENCODING] = [POINTS TO THE ERROR POSITION]

3×7 · 7×1 = 3×1



CODE: SIMPLE EXAMPLE

ENCODING A MESSAGE AS A MATRIX

$$\begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

MATHEMATICALLY DERIVED

DECODING THE RECEIVED MESSAGE USING MATRICES

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

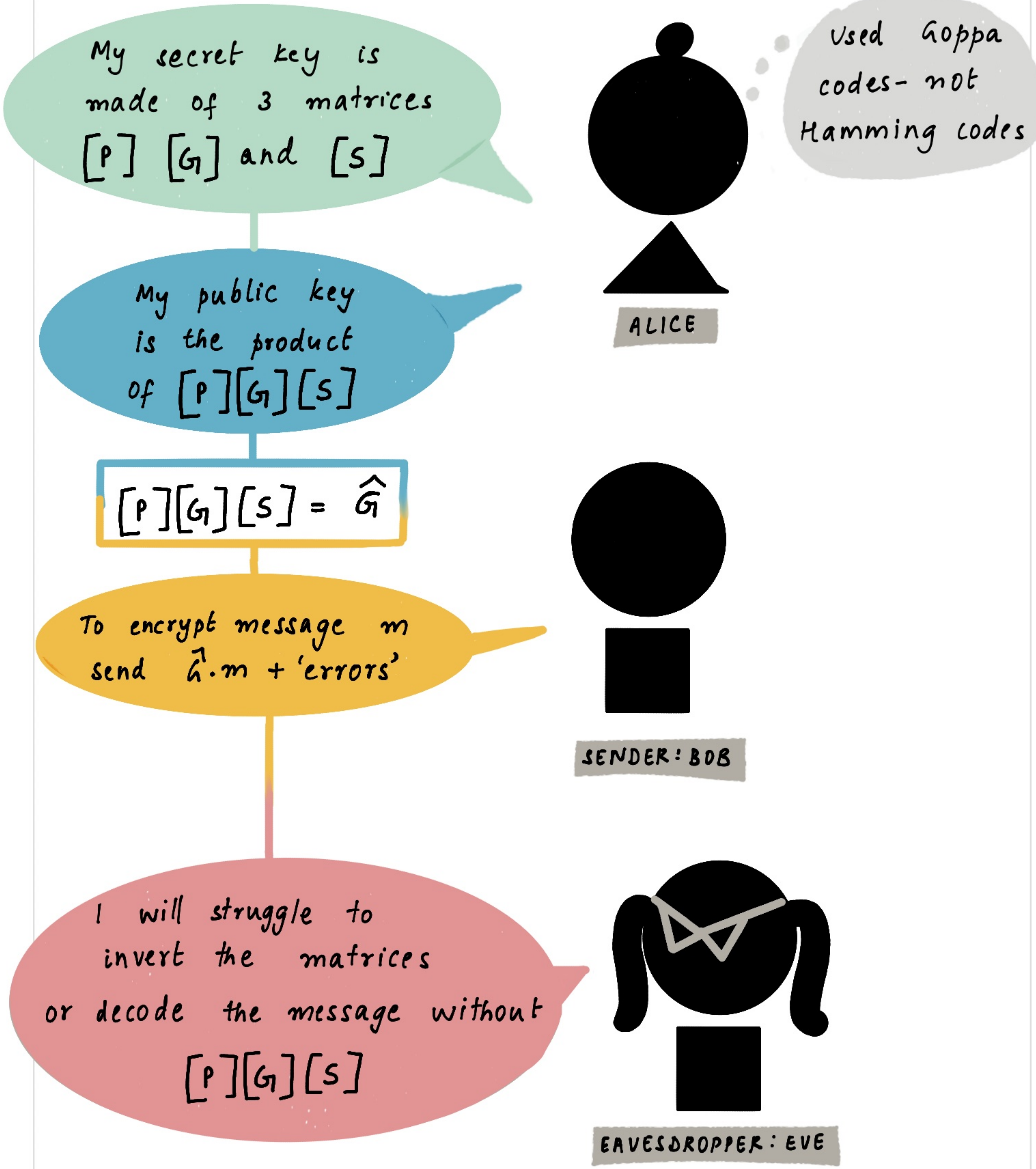
MATHEMATICALLY DERIVED

NOTICE THE ERROR?

THIS POINTS TO A COLUMN NUMBER – i.e. THE POSITION OF THE BIT THAT NEEDS TO BE FLIPPED!

$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ INDICATES NO ERRORS

CODE: APPLICATION



THIS ROUGHLY IS THE BASIS FOR THE MCELIECE CRYPTOSYSTEM
MCELIECE IS IN ROUND 4 FOR CONSIDERATION WITH NIST.

MKPC : NIST CANDIDATE

Classic McEliece

CLASSIC MCELIECE IS NOT YET IN THE STANDARDS LIST - BUT IS BEING CONSIDERED AS A KEY ENCAPSULATION MECHANISM.

BENEFITS	CONSIDERATIONS
UNBROKEN FOR 40 YEARS	LARGE KEY SIZES
FAST ENCRYPTION/DECRYPTION	NOT SUITABLE IN CASE OF LIMITED BANDWIDTHS

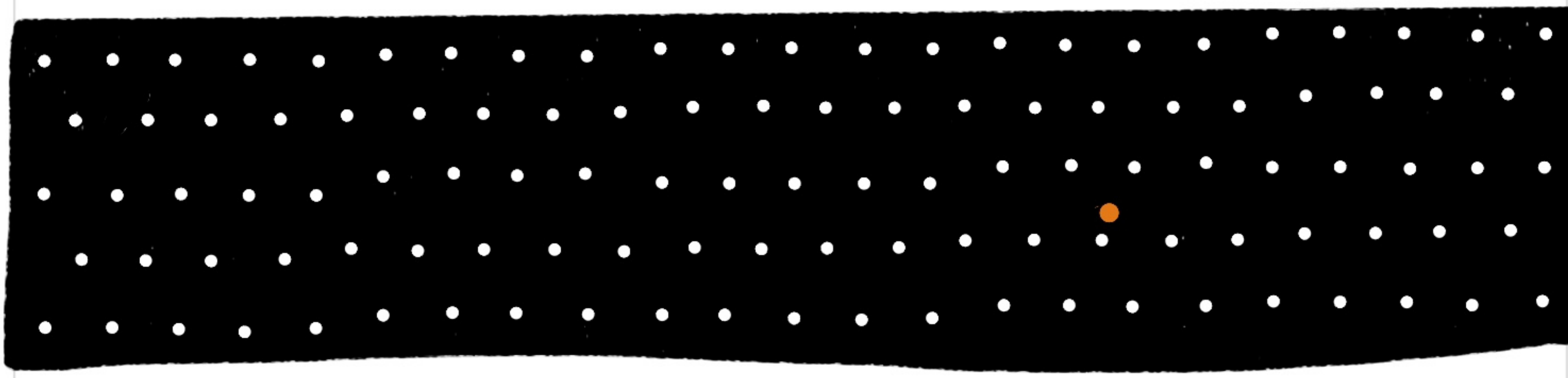
LATTICE BASED CRYPTOGRAPHY

LATTICE BASED SCHEMES

LATTICE BASED CRYPTOSYSTEMS USE WELL STUDIED NP-HARD LATTICE PROBLEMS SUCH AS...

...CLOSEST VECTOR PROBLEM

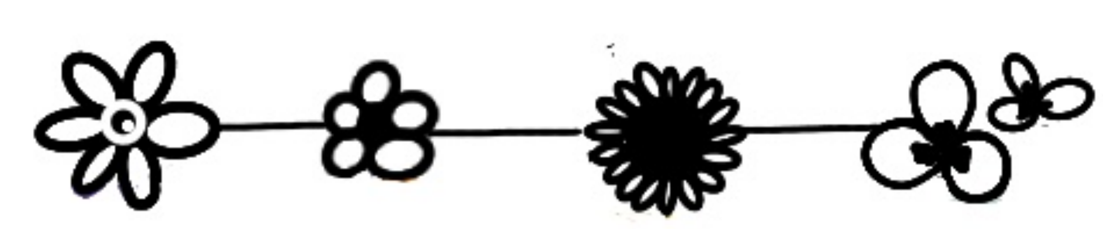
IN AN INFINITE GRID OF DOTS IN HUNDREDS OF DIMENSIONS PICK A POINT IN SPACE AND FIND THE NEAREST DOT.



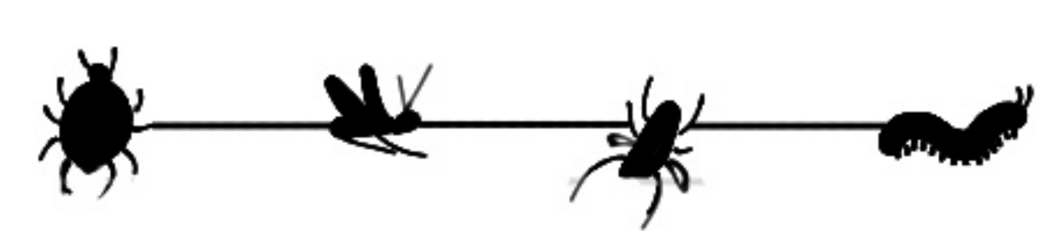
...LEARNING WITH ERRORS

TAKE A SYSTEM OF EQUATIONS

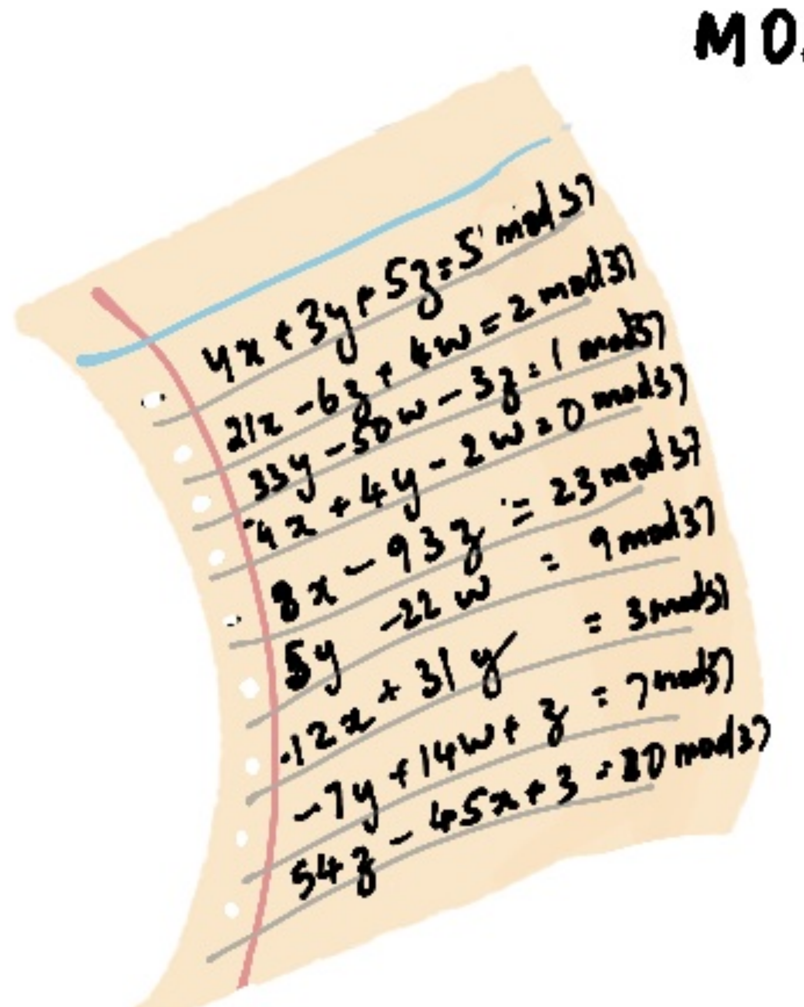
CONSTRUCTED USING SOME SECRET KEYS

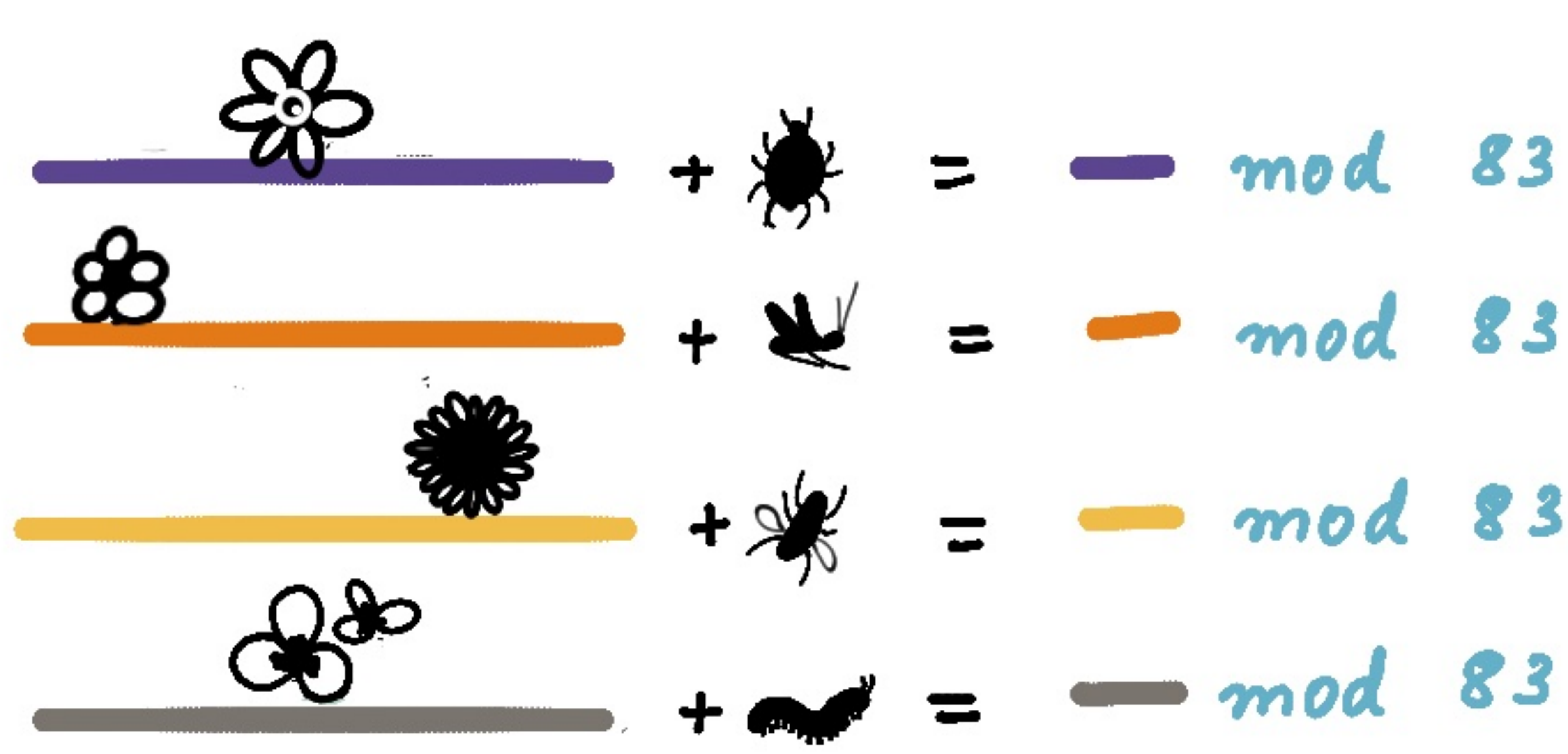


WITH SECRETLY ADDED ERRORS



MOD A PRIME NUMBER MOD 83

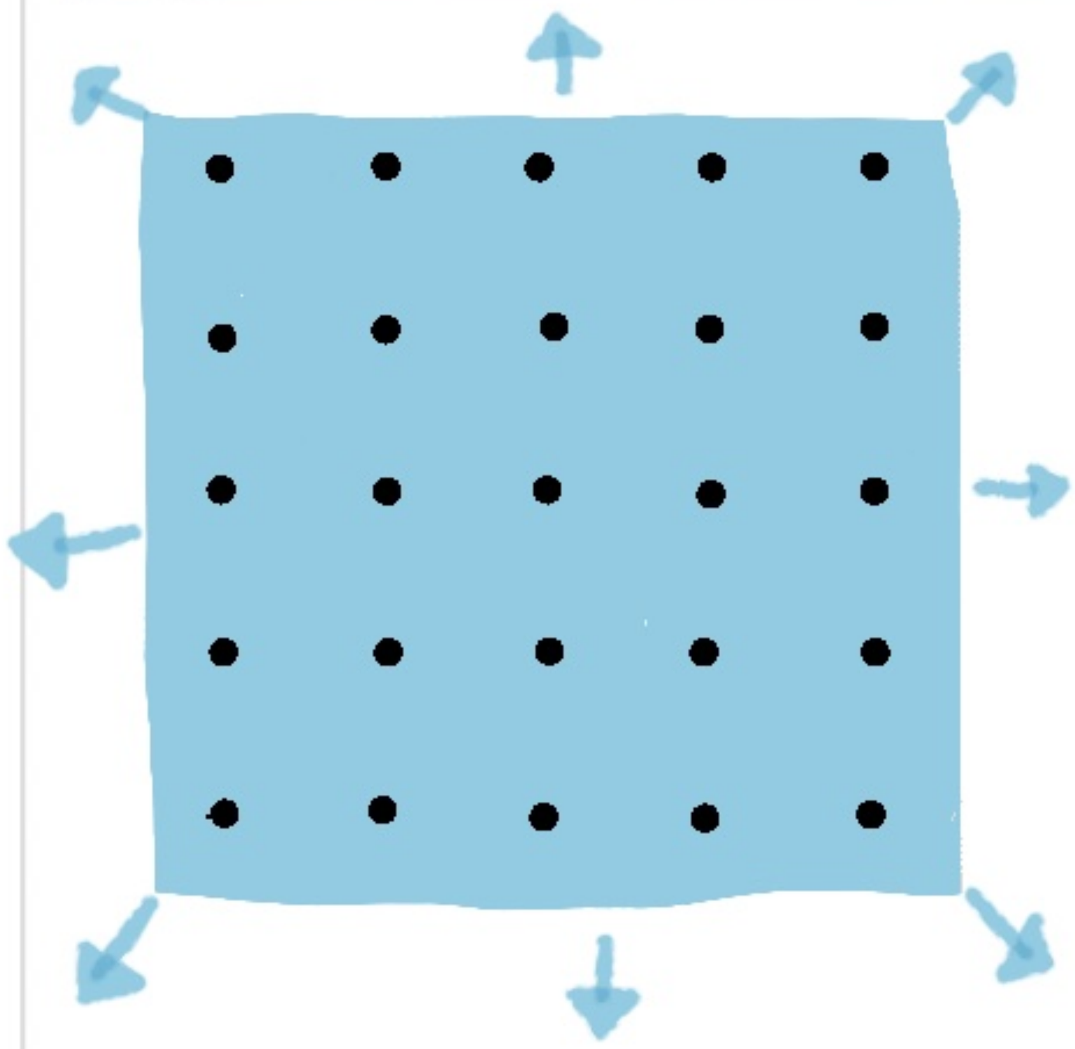


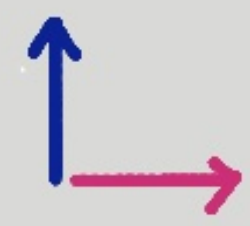


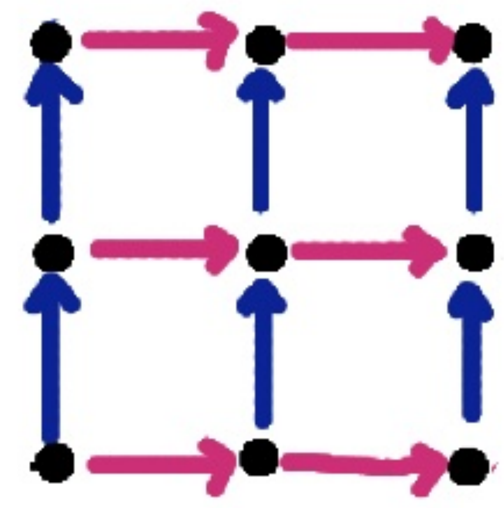
TURNS OUT THEY ARE BOTH SOME VERSION OF EACH OTHER AND ARE HARD FOR QUANTUM COMPUTERS TO SOLVE.

CLOSEST VECTOR PROBLEM

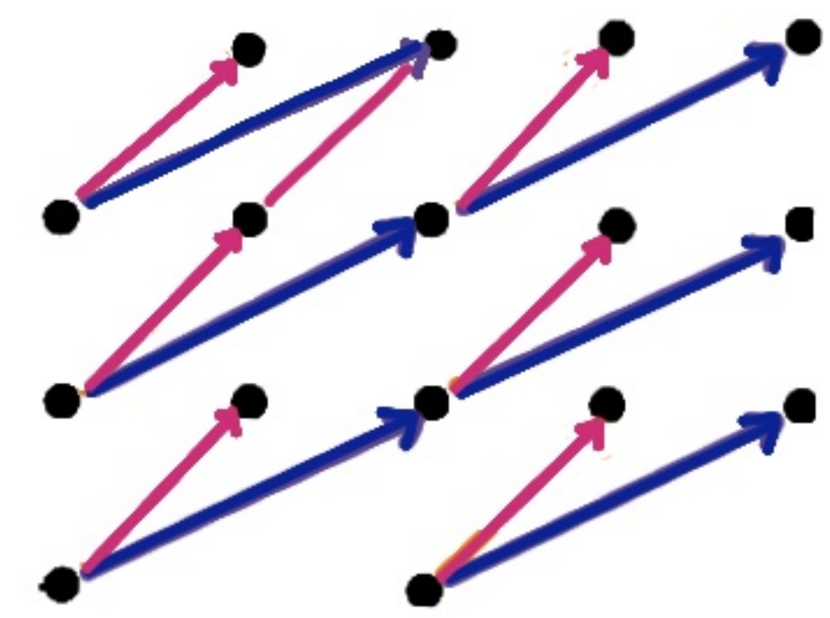
LATTICE :
A GRID OF 'DOTS'



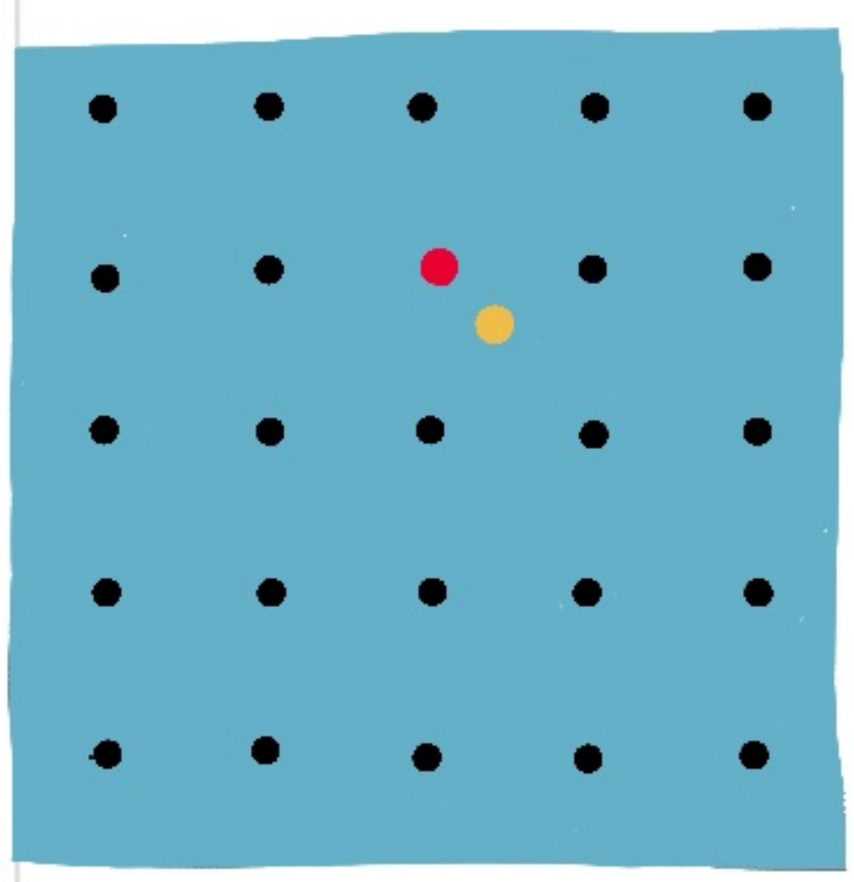
COMPOSED
LIKE THIS 



OR
LIKE THIS 



PICK 2 POINTS



THE YELLOW DOT

A POINT SLIGHTLY
OFF THE LATTICE

THE RED DOT

POINT ON THE
LATTICE CLOSEST TO
THE YELLOW DOT

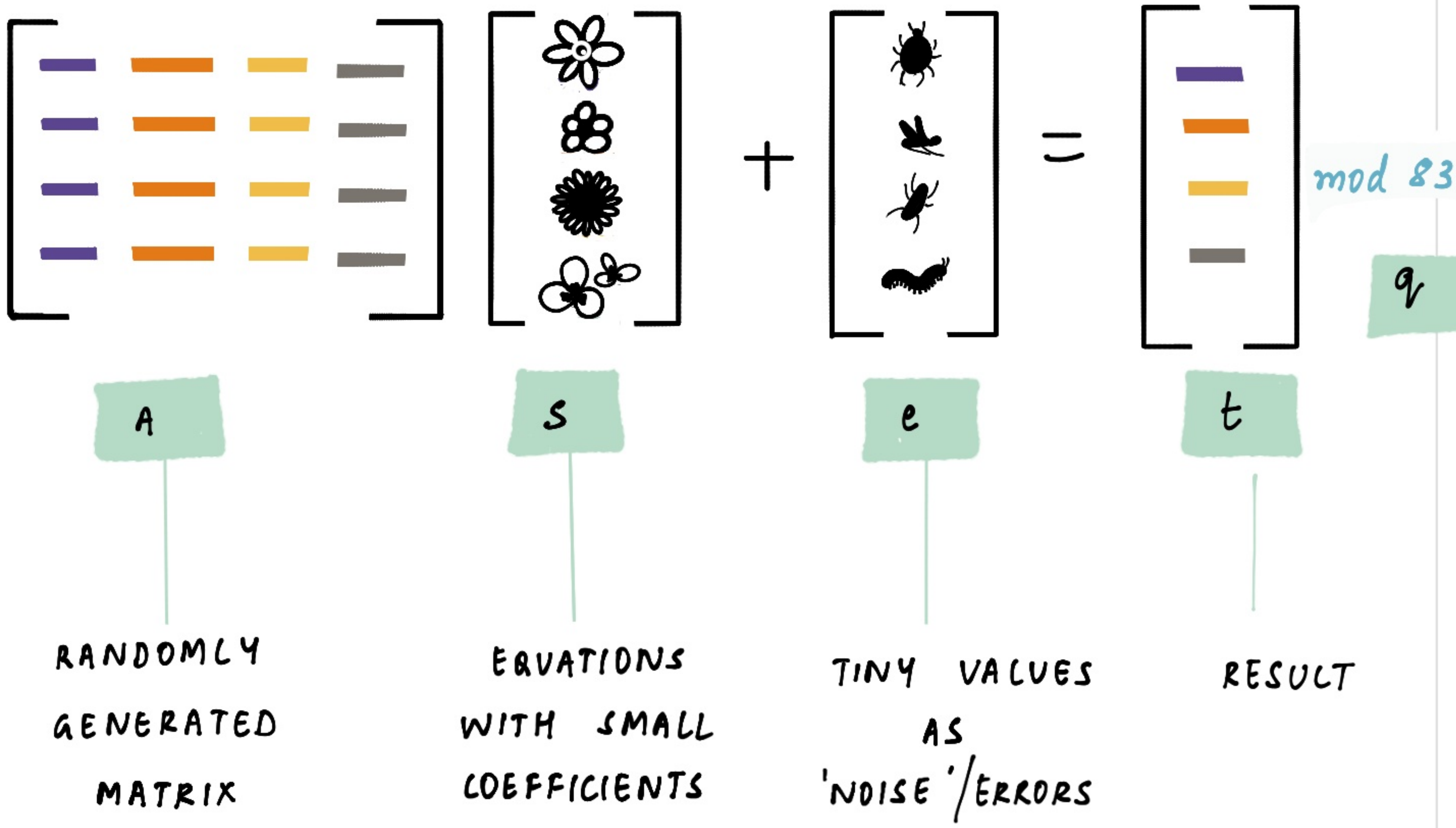
MATHEMATICALLY, GIVEN THE DEFINITION OF A LATTICE 
(ONLY IMAGINE THE LATTICE IN HUNDREDS OF DIMENSIONS)
AND THE YELLOW DOT IT IS HARD TO FIND THE RED DOT

PUBLIC KEY 

SECRET KEY

MODULE LEARNING WITH ERRORS

THE SYSTEM OF EQUATIONS WE SAW EARLIER CAN BE COMPACTLY ARRANGED INTO MATRIX FORMAT AS BELOW



$$A \cdot s + e = t$$

PUBLIC INFORMATION

A, t, q

PRIVATE INFORMATION

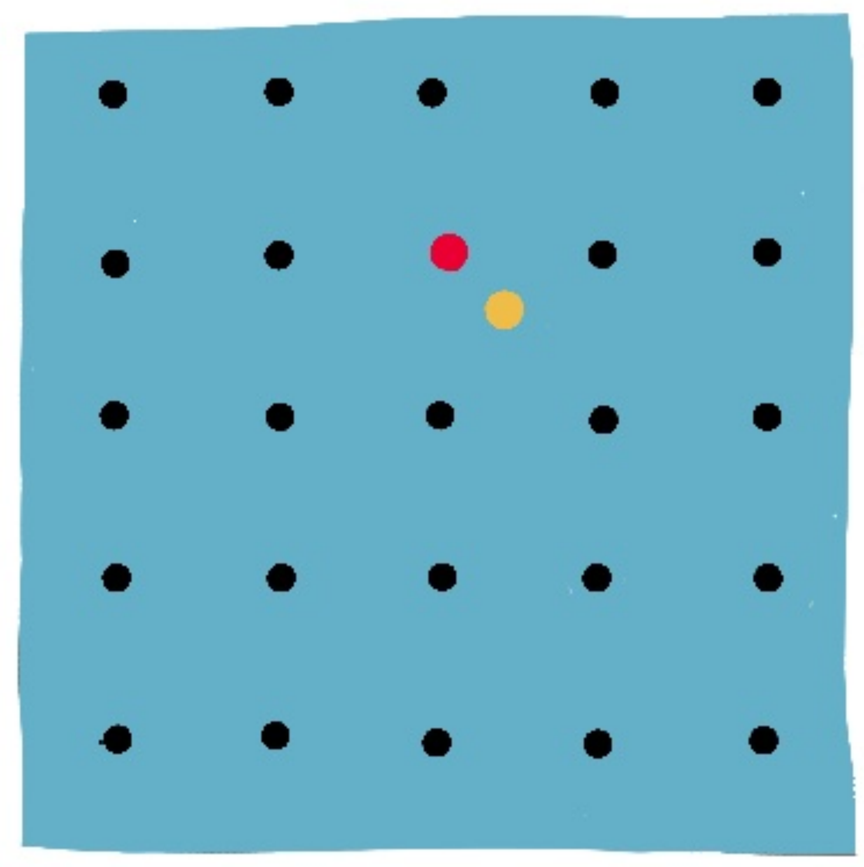
s, e

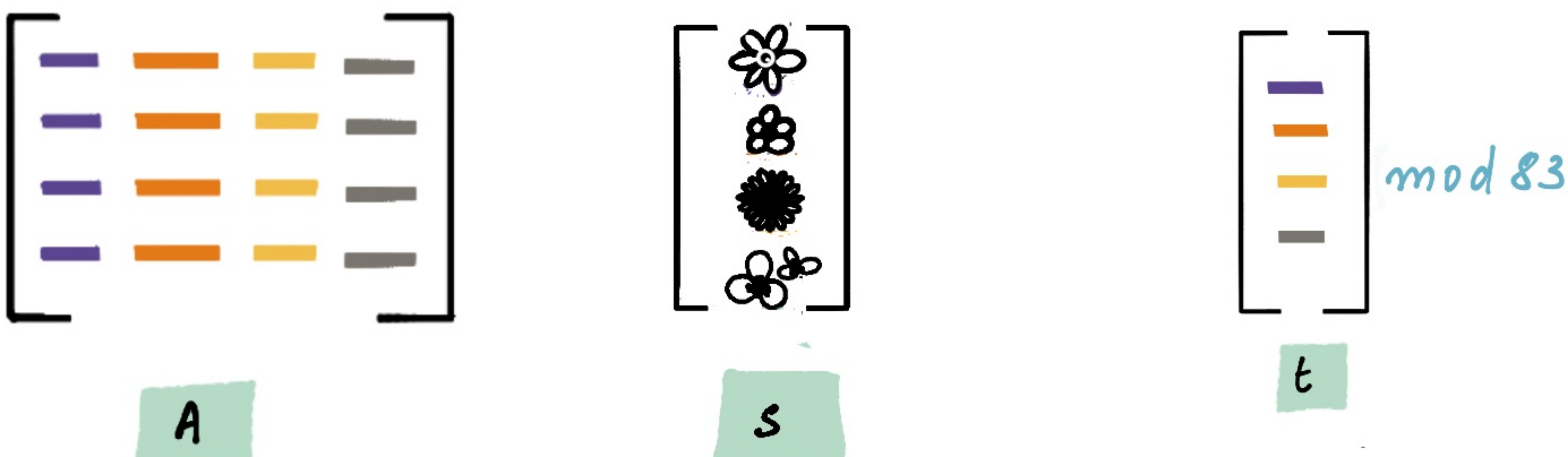
RETRIEVING THE SECRET **s** IS INCREDIBLY HARD IN THE PRESENCE OF **e** AND WHEN DIMENSIONS OF **A** ARE LARGE

THE NAME MODULE LEARNING WITH ERRORS IS THE NAME CHOSEN BY MATHEMATICIANS FOR THIS PROBLEM. SIGH

JOINING THE DOTS

WHAT IS THE CONNECTION BETWEEN THE CLOSEST VECTOR PROBLEM AND LEARNING WITH ERRORS?





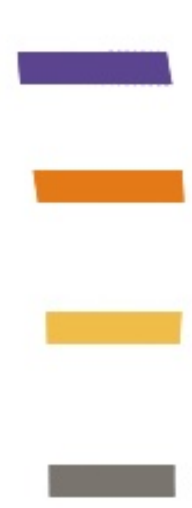
DESCRIBES THE LATTICE

THE LOCATION OF THE SECRET POINT

● RED DOT

IS THE PUBLIC POINT

● YELLOW DOT

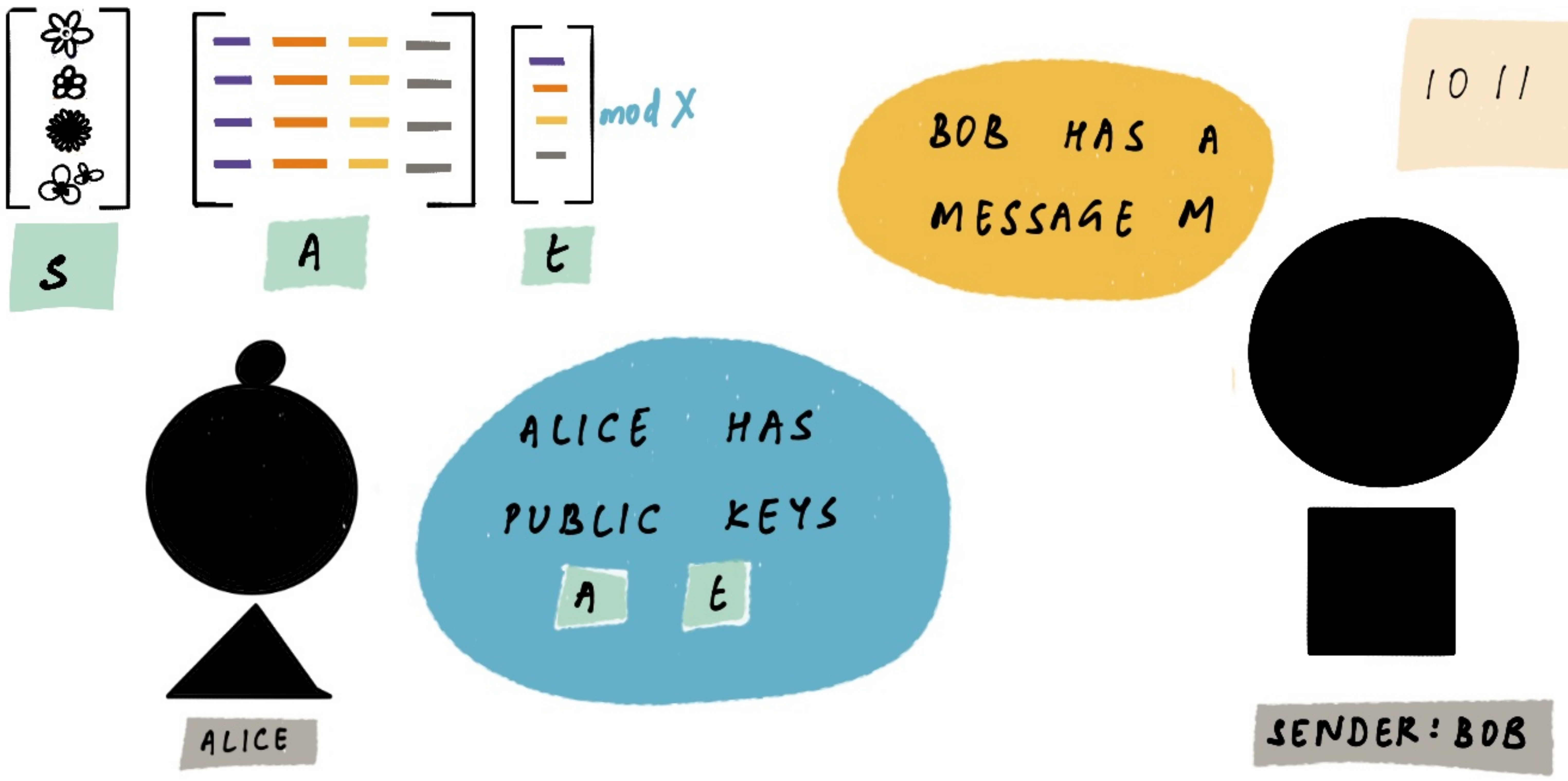


ARE ALL EQUATIONS IN POLYNOMIAL FORM

e.g $5x^6 - 11x^5 - x^4 - 26x^3 + x + 5 = -5$

ARRANGED IN A MATRIX

LATTICE: SIMPLE EXAMPLE

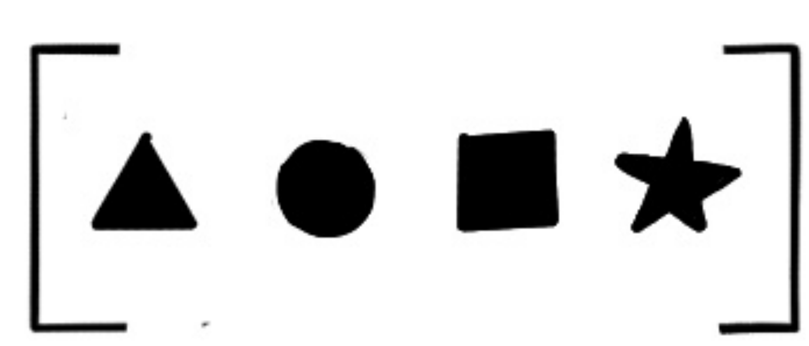


TO ENCRYPT BOB MUST

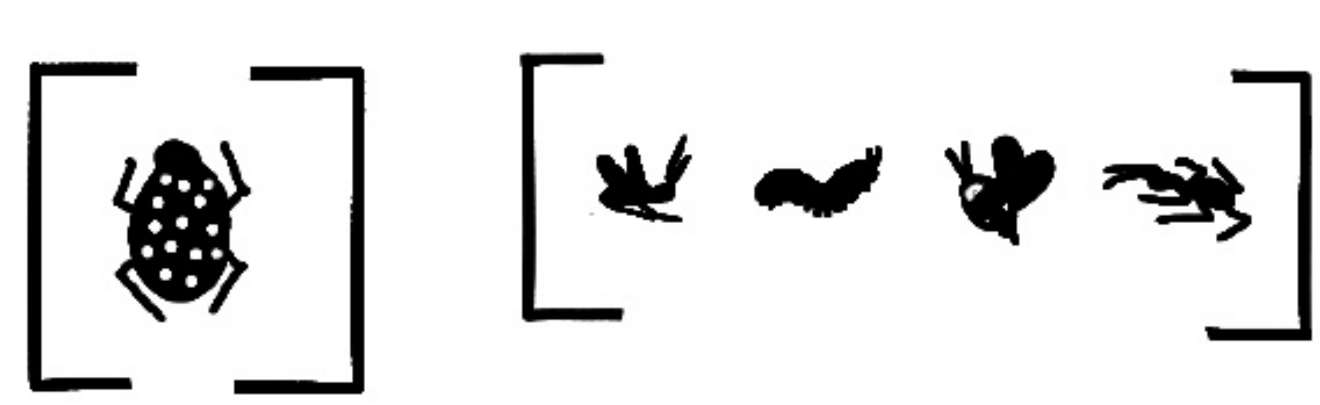
- CONVERT HIS BINARY MESSAGE TO POLYNOMIALS

DECIMAL	BINARY	POLYNOMIAL
1	001	$0+0+1 \longrightarrow 1$
2	010	$0+x+0 \longrightarrow x$
3	011	$0+x+1 \longrightarrow x+1$
4	100	$x^2+0+0 \longrightarrow x^2$
5	101	$x^2+0+1 \longrightarrow x^2+1$
7	111	x^2+x+1
10	1010	$x^3+0+x+1$

- CHOOSE A RANDOM MATRIX r



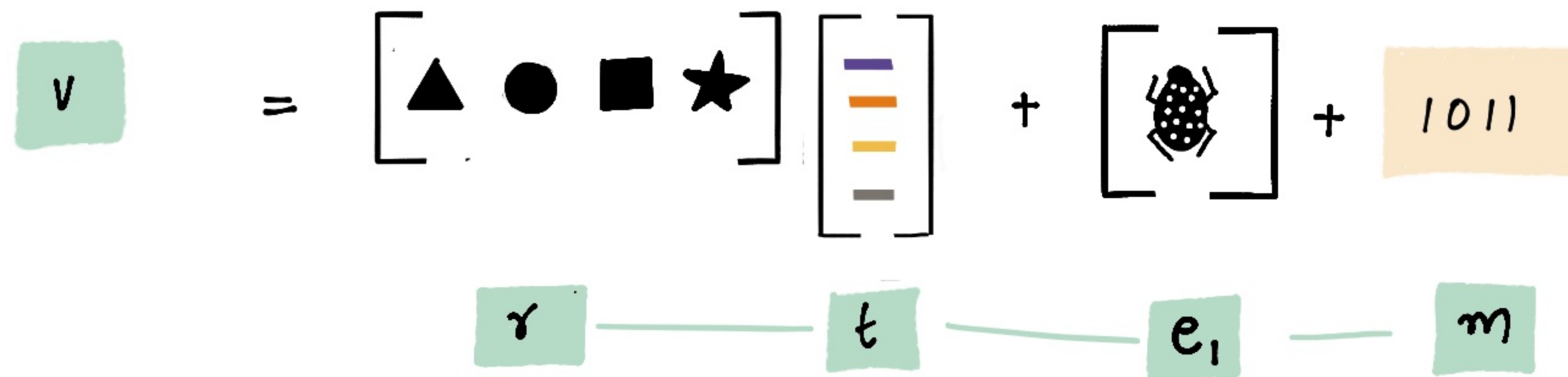
- CHOOSE TWO OTHER SMALL 'ERRORS'

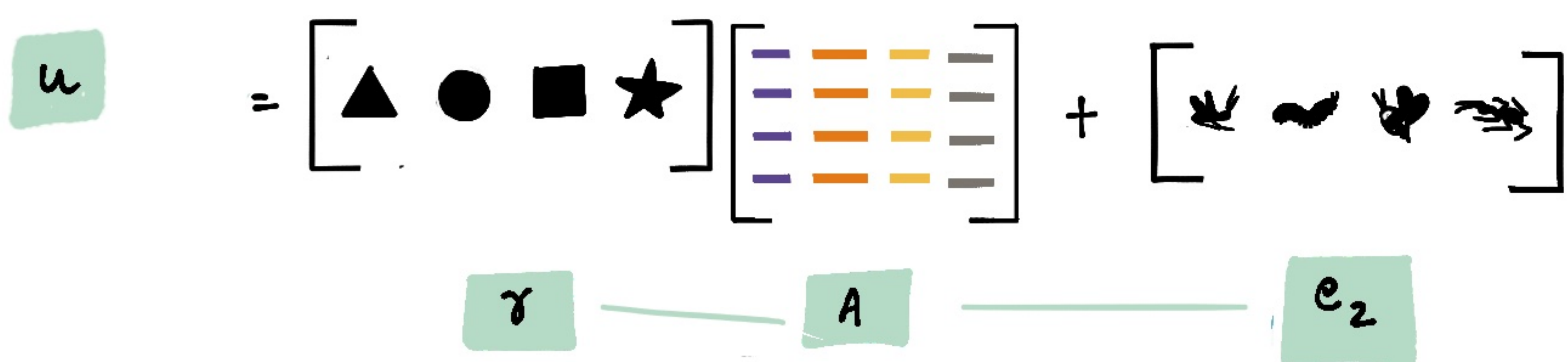


LATTICE: SIMPLE EXAMPLE

ENCRYPTION

BOB SENDS V AND U





DECRYPTION

ALICE FINDS MESSAGE $M = V - US$

$$M = rt + e_1 + m - (rA + e_2)S$$

$$= r(AS + e) + e_1 + m - rAS - e_2 S$$

$$= rAS + re + e_1 + m - rAS - e_2 S$$

VERY SMALL TERMS WITH e, e_1, e_2 ARE IGNORED - LEAVING M

LATTICE: NIST CANDIDATE

CRYSTALS-KYBER

THE ILLUSTRATION IN THE PREVIOUS PAGE IS A SIMPLIFIED VERSION OF THE KYBER CRYPTOSYSTEM.

BENEFITS	CONSIDERATIONS
BASED ON STRUCTURED LATTICES - KNOWN HARD PROBLEM	AS WITH ANY SCHEME, IT REQUIRES CAREFUL IMPLEMENTATION
GOOD PERFORMANCE & SECURITY	LONG TERM SECURITY IMPLICATIONS UNCLEAR

A PQC SCHEME THAT HAS BEEN BROKEN

THE BROKEN SCHEMES

SIKE – AN ISOGENY BASED SCHEME

SIKE IS ROUGHLY SIMILAR TO THE DIFFIE-HELLMAN KEY EXCHANGE DISCUSSED IN THE ILLUSTRATED GUIDE 'HOW TO TELL SECRETS' PUBLISHED BY THOUGHTWORKS.

SIKE WAS BROKEN IN 2022 AUGUST BY WOUTER CASTRYCK AND THOMAS DECRU OF BELGIUM IN UNDER AN HOUR WITH A SINGLE CORE. SIKE MADE IT TO ROUND 4.

RAINBOW – A MULTIVARIATE CRYPTOSYSTEM

RAINBOW IS A MULTIVARIATE CRYPTOSYSTEM. WHICH MEANS THE SECURITY LIES IN THE DIFFICULTY OF SOLVING A LARGE SYSTEM OF EQUATIONS WITH MANY VARIABLES.

RAINBOW WAS BROKEN IN 2022 USING A STANDARD LAPTOP OVER 53 HOURS BY WARD BEULLENS OF IBM, SWITZERLAND. RAINBOW MADE IT TO ROUND 3.

LET'S TAKE A QUICK LOOK AT RAINBOW'S APPROACH TO DESIGNING A QUANTUM-SAFE ALGORITHM – ALBEIT BROKEN.

MULTIVARIATE CRYPTOSYSTEMS

MULTIVARIATE PUBLIC KEY CRYPTOSYSTEMS ARE BASED ON THE HARDNESS OF SOLVING EQUATIONS WITH MULTIPLE VARIABLES

MQ challenge:
Hardness Evaluation of Solving Multivariate Quadratic Problems

T Yasuda, X Dahan, Y Huang, T Takagi, K Sakurai

eprint.iacr.org/2015/275.pdf

FOR EXAMPLE:

$$2x + 3 = 5$$

$$2x + 3xy + 5x^2 = 4 \mod 3$$

$$x^2 - 7xz + 2y^2 = 1 \mod 3$$

find x find y find z

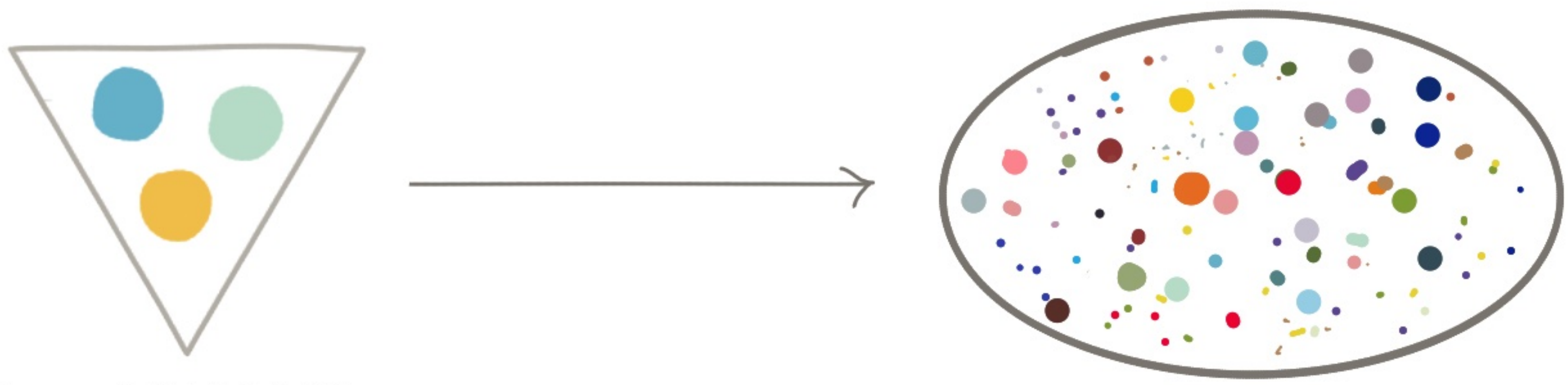
SOLVING MEANS TO FIND THE VALUES OF THE VARIABLES x, y, z THAT WORKS FOR EACH EQUATION.

THE PROBLEM BECOMES HARDER WHEN THE NUMBER OF EQUATIONS AND VARIABLES DON'T MATCH EXACTLY.

MKPC

NOW, INSTEAD OF

IMAGINE :



3 VARIABLES

150 VARIABLES

2 EQUATIONS

50 EQUATIONS

IT TURNS OUT THAT THIS MANY VARIABLES AND POLYNOMIALS (EQUATIONS) COULD CREATE A PROBLEM TOO HARD — EVEN FOR A QUANTUM COMPUTER!

THE RESULT IS MULTIVARIATE PUBLIC KEY CRYPTOSYSTEM — MKPC

THIS SET OF EQUATIONS SERVES AS THE PUBLIC KEY

THE PRIVATE KEY IS A SUBSET OF THE VARIABLES ODDLY NAMED OIL VARIABLES AND VINEGAR VARIABLES.

MKPC : SIMPLE EXAMPLE

TAKE A SINGLE EQUATION WITH VARIABLES a, b, c, d

$$a^2 + 3ab + 3ac + 2ad + b^2 + 6bc + 4bd = 25 \bmod 3$$

POLYNOMIALS CAN BE EXPRESSED AS THE PRODUCT OF MATRICES. SO THE ABOVE BECOMES :

$$\begin{bmatrix} a & b & c & d \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 & 1 \\ 1 & 1 & 3 & 2 \\ 2 & 3 & 0 & 0 \\ 1 & 2 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

The trapdoor!

$$\begin{bmatrix} a+b+2c+d & 2a+b+3c+2d & a+3b & a+2b \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

NOTICE THAT BY THE DELIBERATE PLACEMENT OF THE ZEROES THE VARIABLES c, d DO NOT MULTIPLY WITH EACH OTHER IN THE ORIGINAL EQUATION.

IF YOU KNOW $a = 1$ AND $b = 1$ THEN THE EXPRESSION IS LINEAR – AND A BIT EASIER TO SOLVE THE EQUATION

$$1 + 3 + 3c + 2d + 1 + 6c + 4d$$

MKPC : SIMPLE EXAMPLE

$$a^2 + 3ab + 3ac + 2ad + b^2 + 6bc + 4bd = 25 \mod 3$$

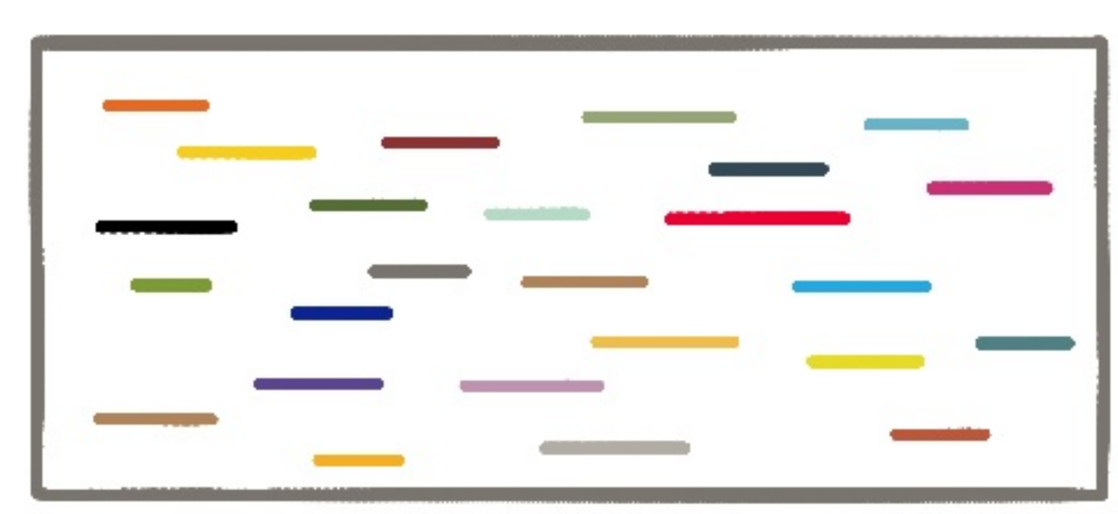
$$\begin{bmatrix} a & b & c & d \end{bmatrix} \begin{bmatrix} 1 & 2 & 1 & 1 \\ 1 & 1 & 3 & 2 \\ 2 & 3 & 0 & 0 \\ 1 & 2 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

The trapdoor!

$a \; b$ → VINEGAR VARIABLES – FORMS THE SECRET

$c \; d$ → OIL VARIABLES

CHOOSE VARIABLES
100 VINEGAR & 50 OIL



CREATE 50 EQUATIONS
EACH WITH THE TRAPDOOR

DECRYPTION WILL INVOLVE
SOLVING 50 EQUATIONS
AND
EXACTLY 50 UNKNOWNS!

THIS IS NOW BROKEN AND IT REMAINS TO BE SEEN IF NEWER SCHEMES WILL APPEAR BASED ON THIS METHOD.

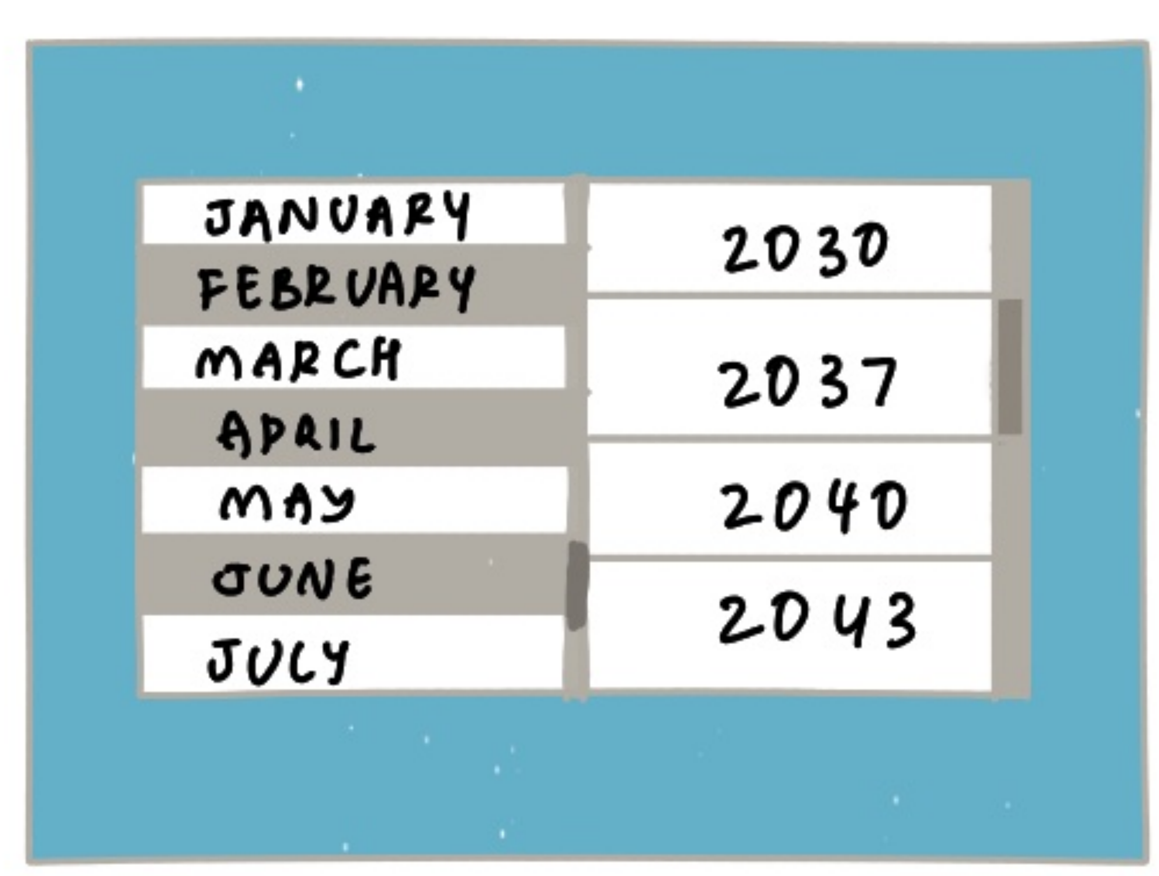
MOVING TO PQC

FIRST STEPS

GATHER AN EXPERT TRANSITION TEAM

CONDUCT A RISK ASSESMENT OF DATA & SYSTEMS

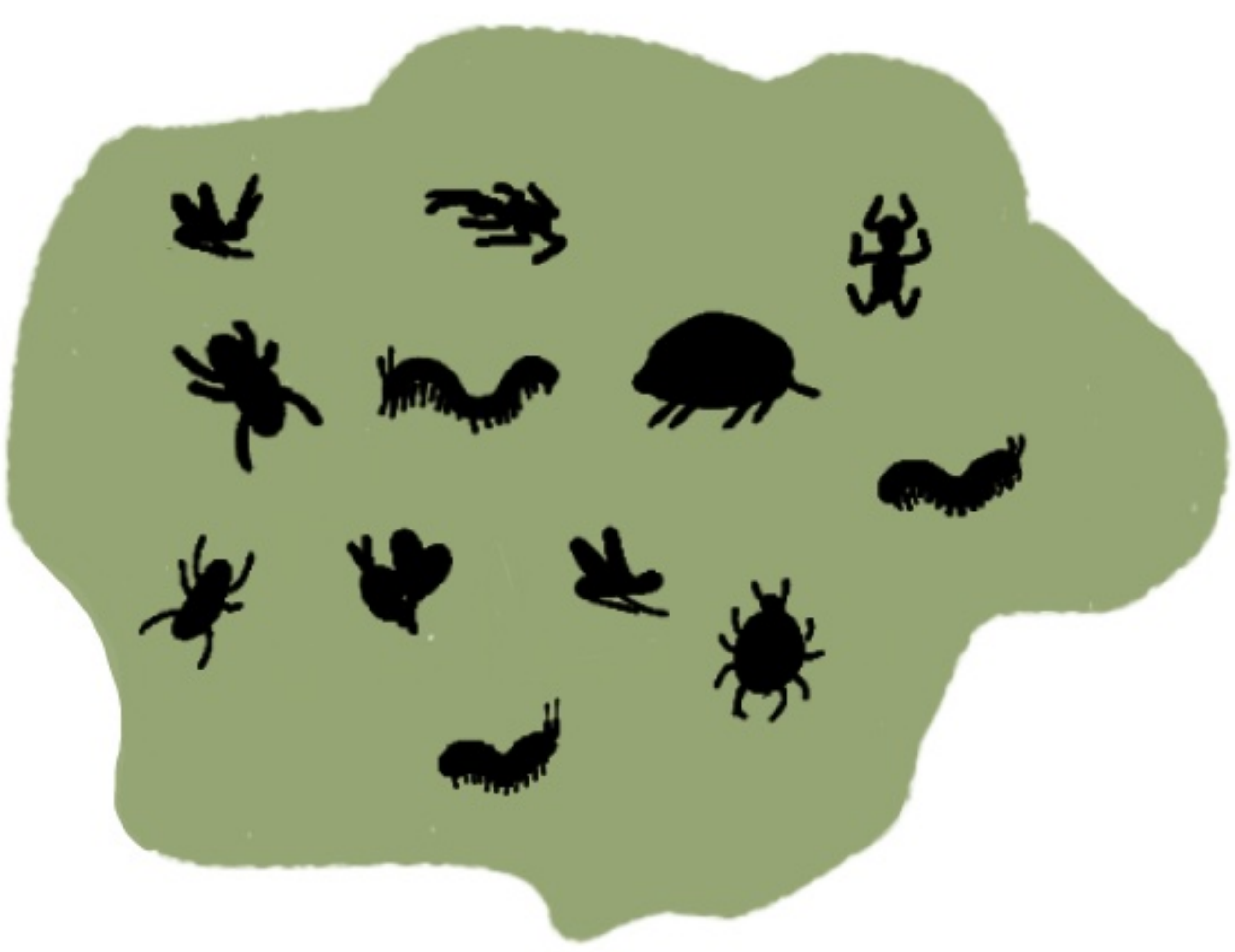
IMAGINE A TIMELINE FOR IMPLEMENTING P&C



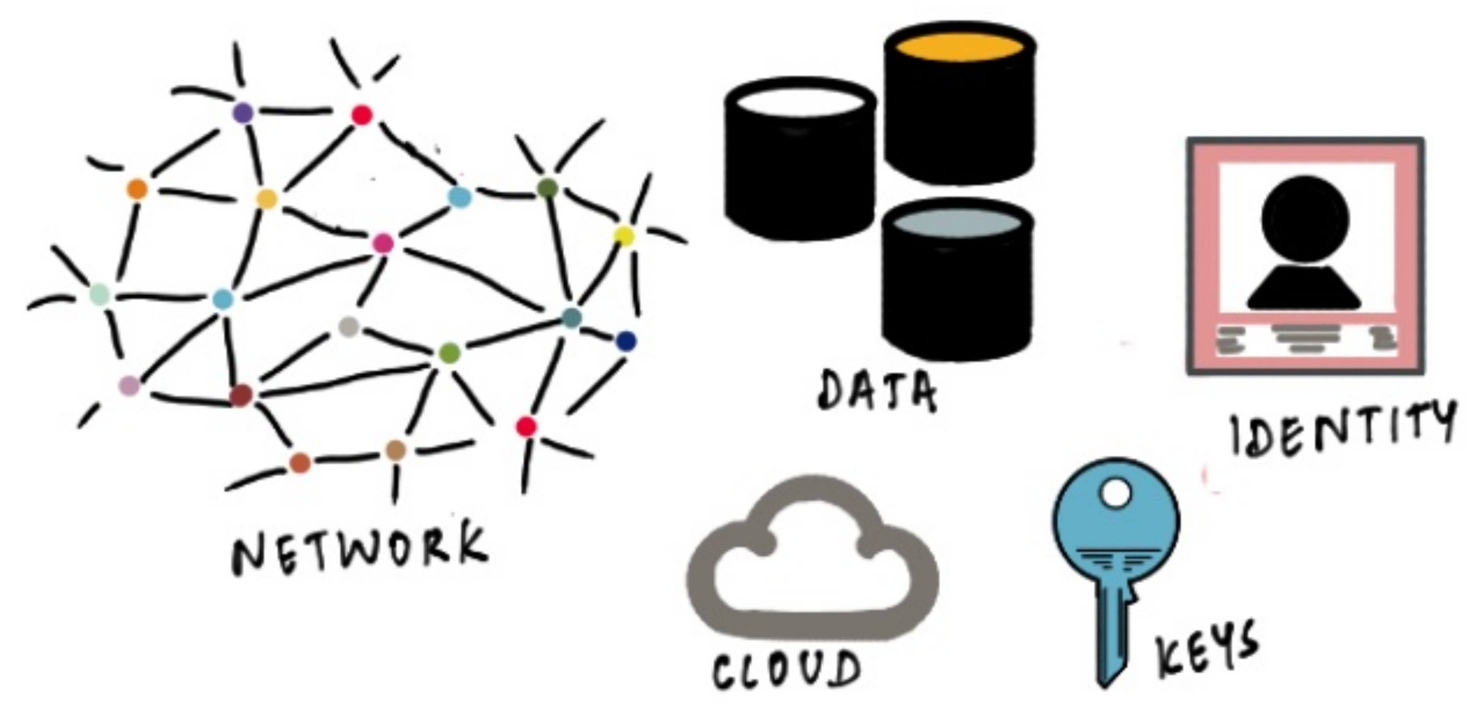
TO IDENTIFY RISK AREAS

IS THERE ANY DATA THAT IS SENSITIVE OR CONFIDENTIAL?

HOW LONG WILL THE DATA NEED TO BE KEPT SAFE?

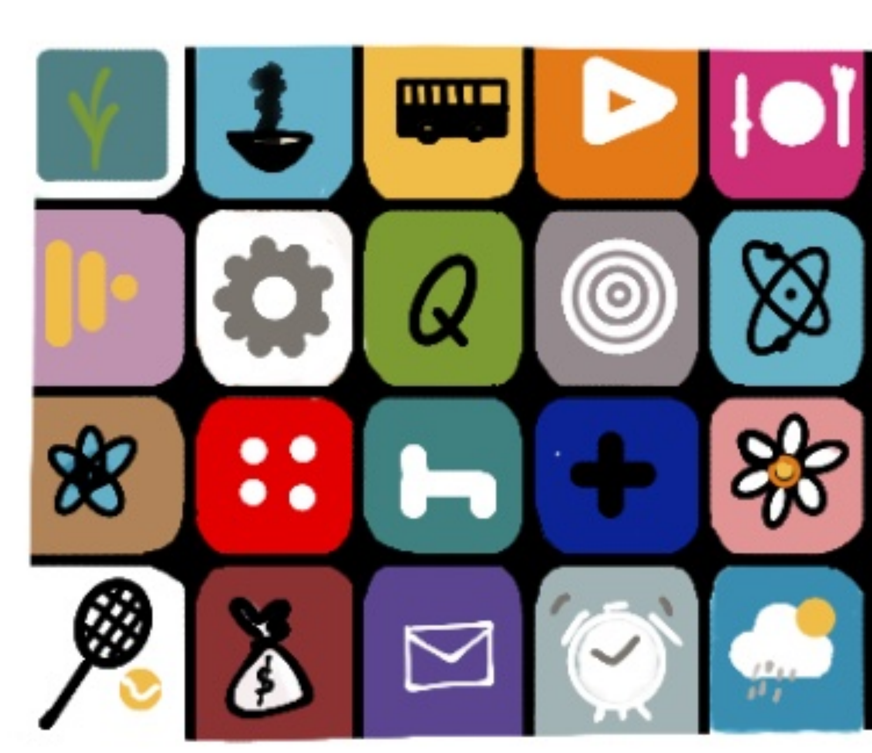


IS THE DATA PUBLIC FACING?



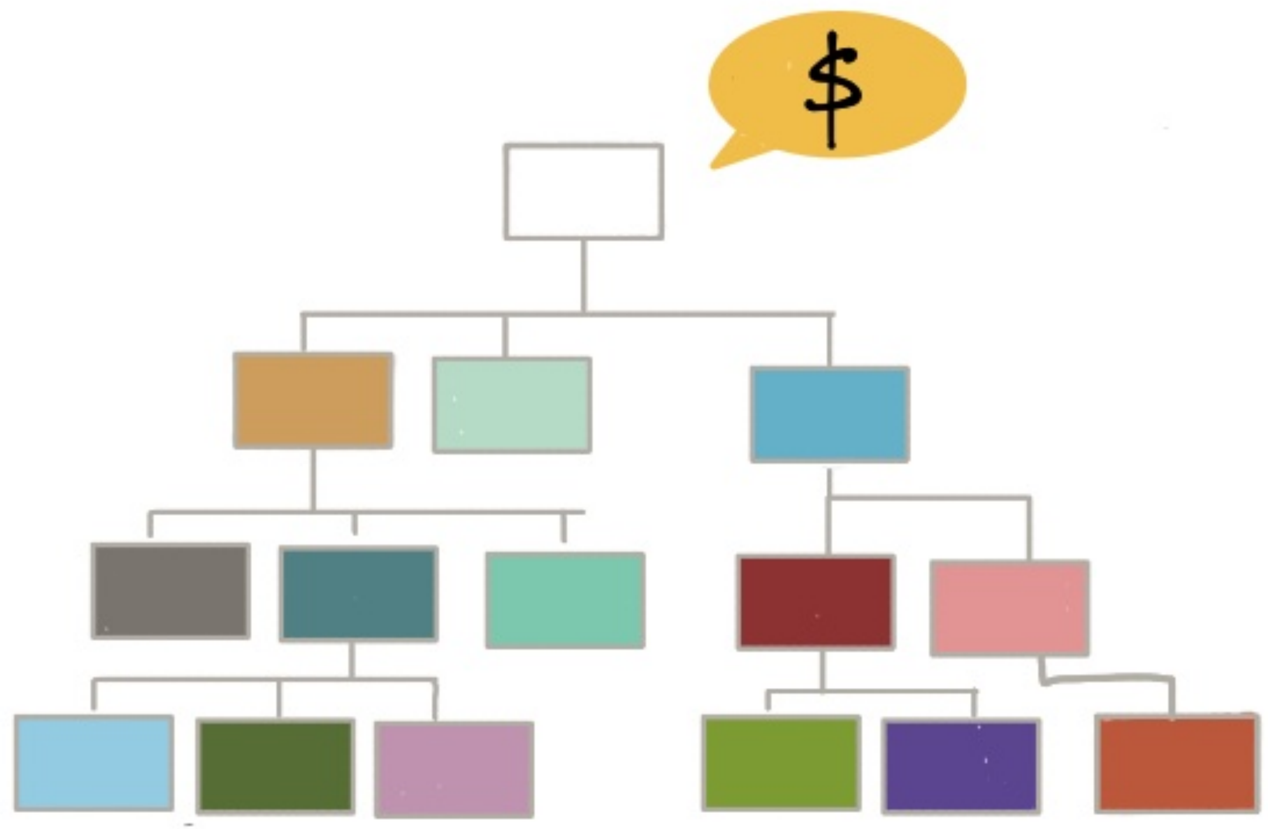
DOES THE INFRASTRUCTURE NEED UPDATE?

WHICH COMMUNICATIONS SYSTEMS NEED TO BE SECURED?

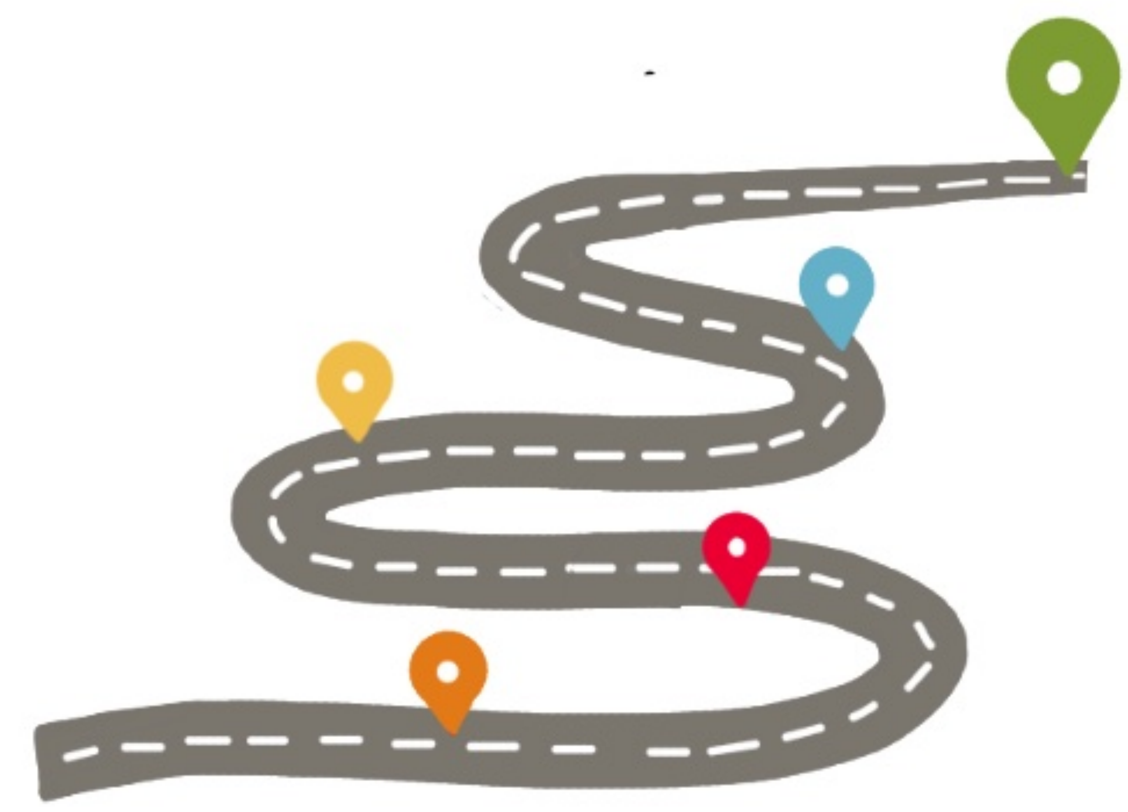


WHICH APPS ARE AFFECTED? (INTERNAL AND EXTERNAL)

OTHER CONSIDERATIONS



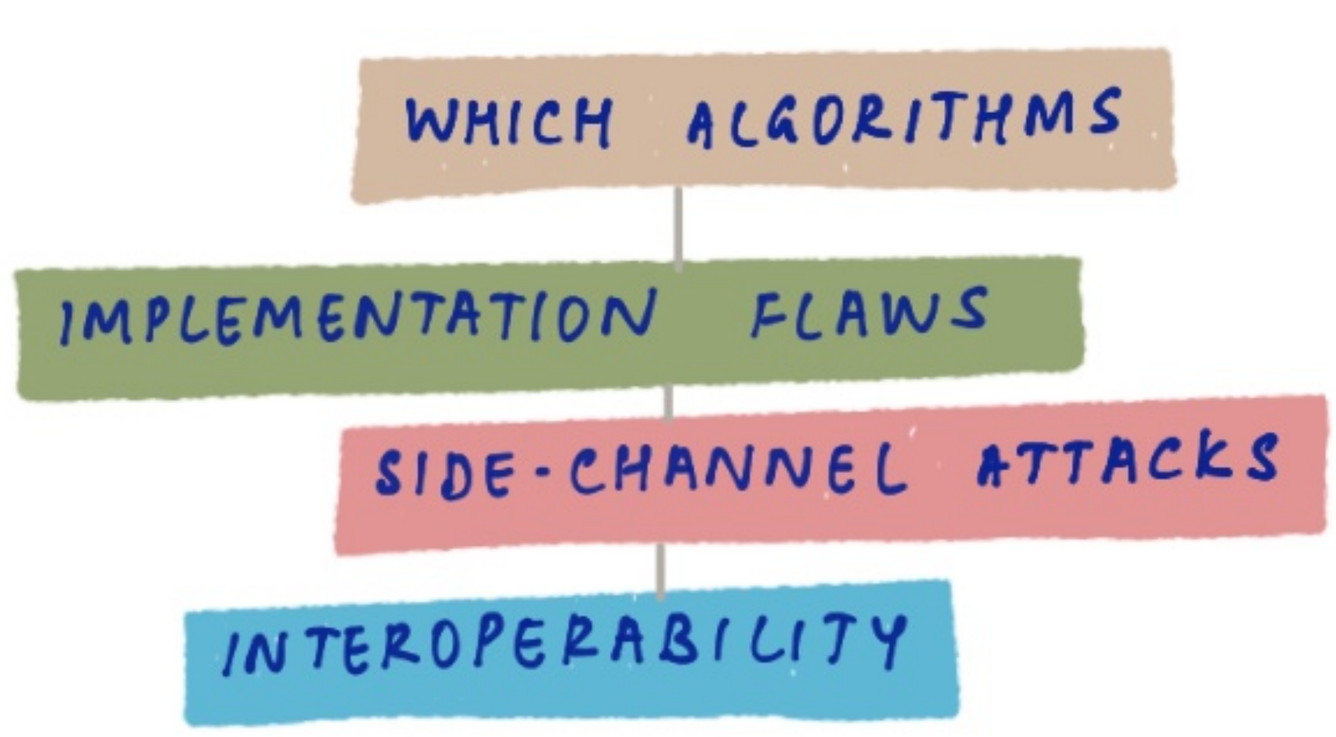
PEOPLE / TEAMS WHO NEED TO BE MADE AWARE



VENDOR ROADMAPS

CRYPTOAGILITY

TRANSITION STRATEGY

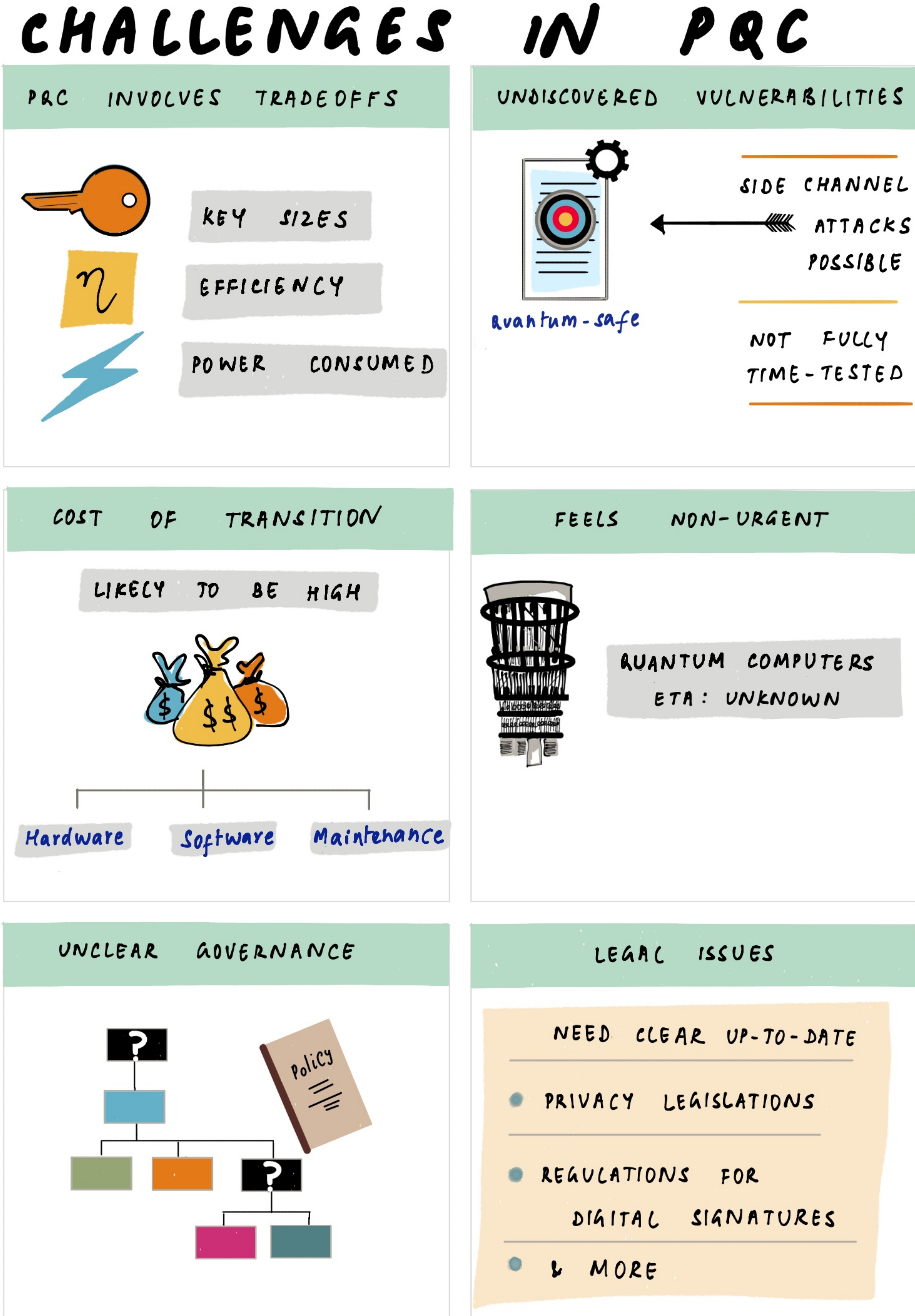


EXPERIMENT, TEST & IMPLEMENT

GUIDANCE FROM REGULATORY BODIES:

NIST ANSSI
BSI IEEE

STAY INFORMED


CHALLENGES IN PQC
PQC INVOLVES TRADEOFFS
KEY SIZES
EFFICIENCY
POWER CONSUMED
UNDISCOVERED VULNERABILITIES
Quantum-safe
SIDE CHANNEL ATTACKS POSSIBLE
NOT FULLY TIME-TESTED
COST OF TRANSITION
LIKELY TO BE HIGH
$$
Hardware
Software
Maintenance
FEELS NON-URGENT
QUANTUM COMPUTERS ETA: UNKNOWN
UNCLEAR GOVERNANCE
?
?
Policy
LEGAL ISSUES
NEED CLEAR UP-TO-DATE
PRIVACY LEGISLATIONS
REGULATIONS FOR DIGITAL SIGNATURES
& MORE

NOT IN SCOPE

SPECIFIC NUMBERS ASSOCIATED TO THE KEY SIZES OR COMPUTATION TIME REQUIRED - AS IT WILL DEPEND ON FINAL IMPLEMENTATION

STEPS FOR NAVIGATING A HYBRID APPROACH TO PQC

EXPLORING OTHER BASES FOR POST QUANTUM CRYPTOGRAPHY SUCH AS CELLULAR AUTOMATA OR DIOPHANTINE EQUATIONS

HOW AI AND QUANTUM MIGHT WORK TOGETHER

WE SHOULD NOT GET TOO COMFORTABLE WITH THE TERM 'SECURE'

— VINT CERF

SEPTEMBER 2023
PRC PANEL DISCUSSION

MY REFERENCES

Fundamental concepts

- Introduction to Post Quantum Cryptography - learning.quantum.ibm.com
- What is it going to take to break cryptography with a quantum computer by **PKI Consortium**
- NIST Pages - csrc.nist.gov/projects/post-quantum-cryptography
- The new millennium bug: everything you need to know about Y2Q : weforum.org
- Panel Discussion: Post-Quantum Cryptography | September 23 youtube.com by Heidelberg Laureate Forum
- Status Update from NIST on youtube.com by PKI consortium

Algorithms : **Videos on Youtube.com**

- Quantum Algorithms and Post-Quantum Cryptography by **Simons Institute**
- ISBA2022: Workshop | Demystifying Quantum Part 2 by **Parallel Chain Lab**
- Lattices and Kyber PQC Presentation by **Mojtaba Bisheh Niasar**
- Kyber and Post Quantum Crypto How does it work by All **Hacking Cons**
- Learning with errors: Encrypting with unsolvable equations by **Chalk Talk**
- Lattices: Algorithms, Complexity, and Cryptography by **Simons Institute**
- Jintai Ding - State of Art of MPKC by **PQCrypto 2016**
- Code-based Cryptography by **PKI Consortium**
- Code based Crypto by **USF Crypto Center**
- Oil and Vinegar variables : **Bill Buchanan**

Implementation

- Paper - Challenges in the Transition towards a Quantum-safe Government : tudelft.nl
- Transitioning Organizations To Post Quantum Cryptography youtube.com by SandboxAQ