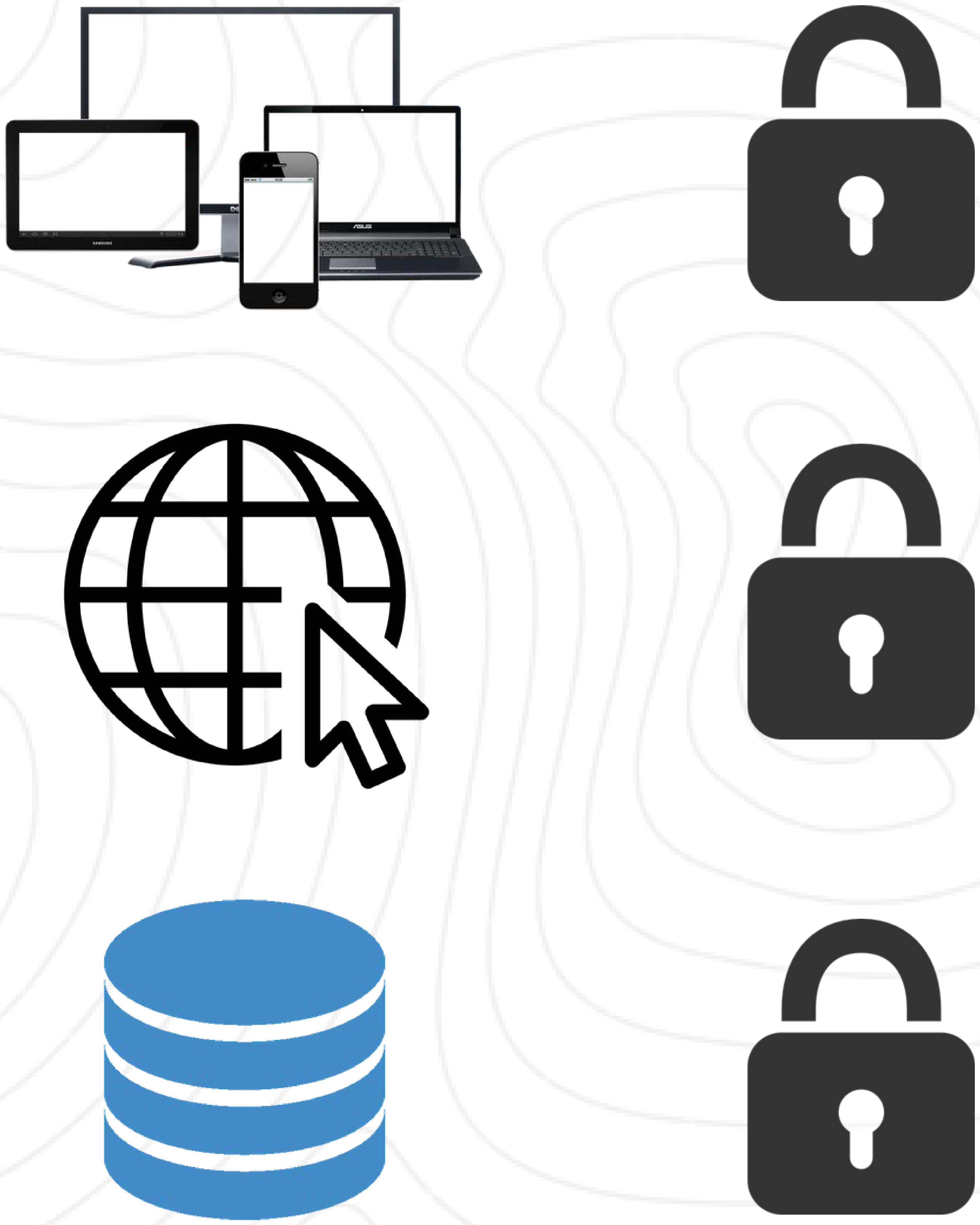
QUAE

x

CONF42

1. Classical Encryption Methods
2. Shor's Algorithm
3. Quantum-Resistant Classical Encryption Methods



MISUSE

OUR FOCUS...

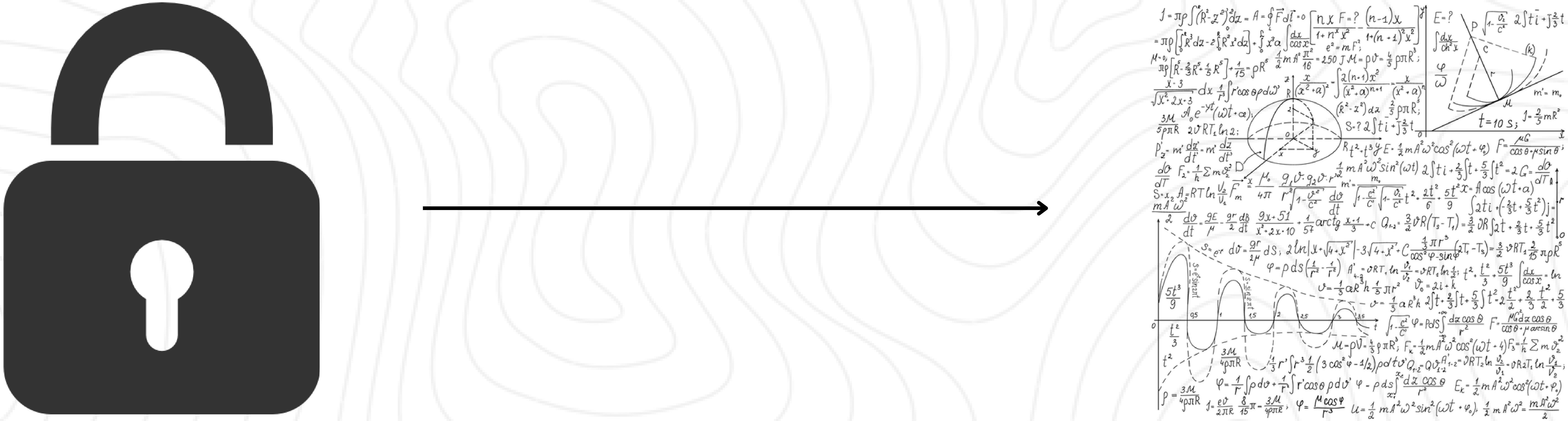
OUR FOCUS...

CRYPTOGRAPHY!

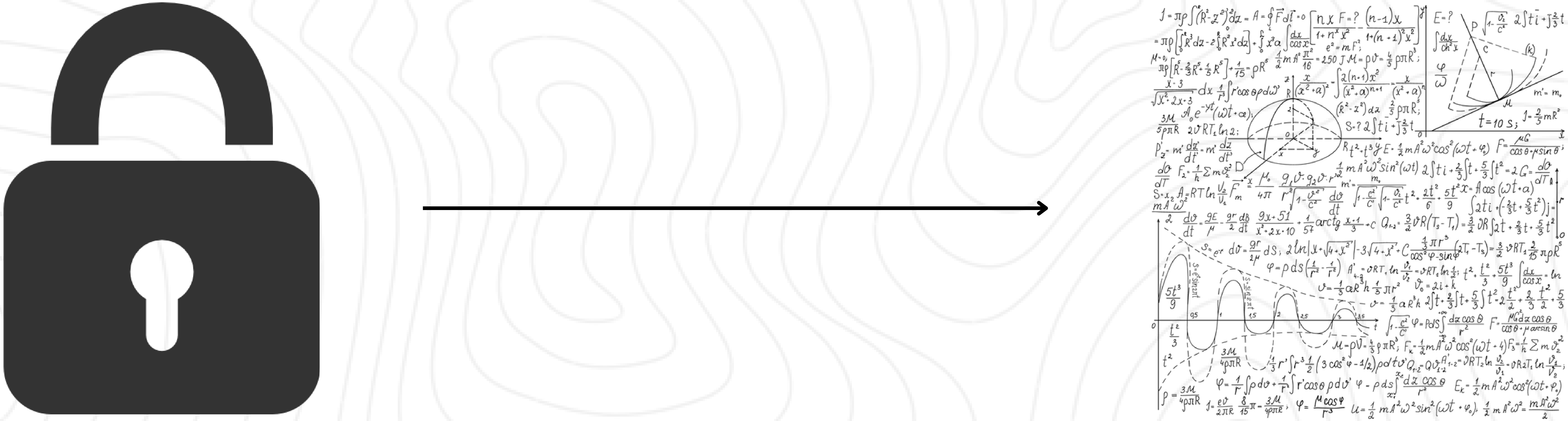
ENCRYPTION

ENCRYPTION

ENCRYPTION



ENCRYPTION

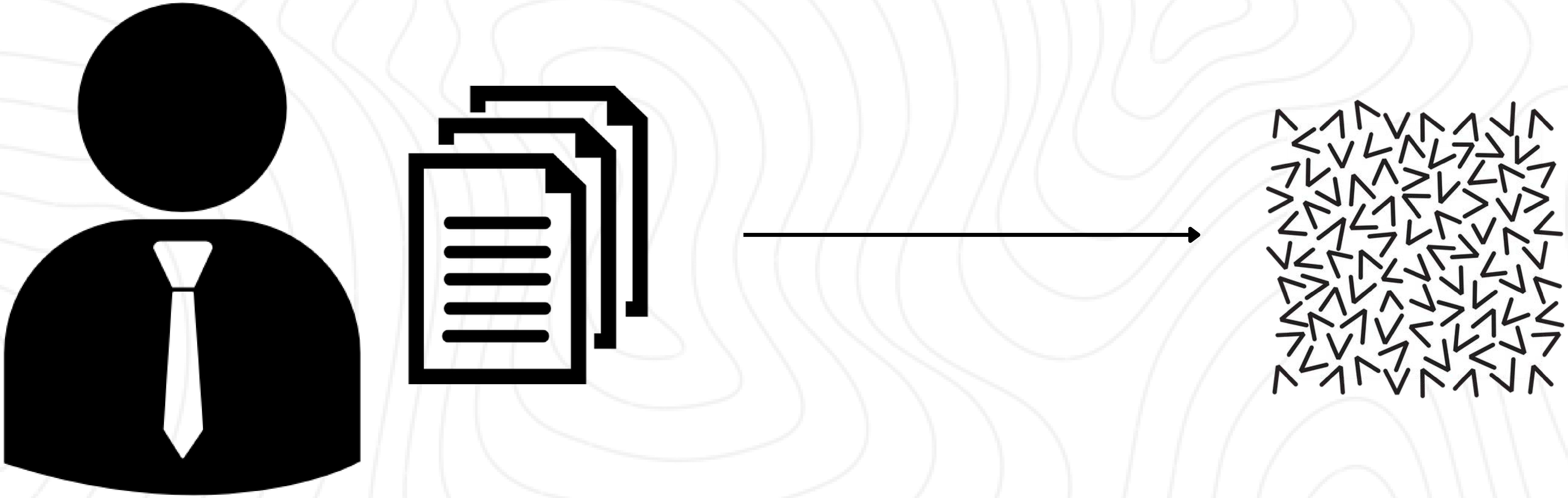


CONFIDENTIALITY

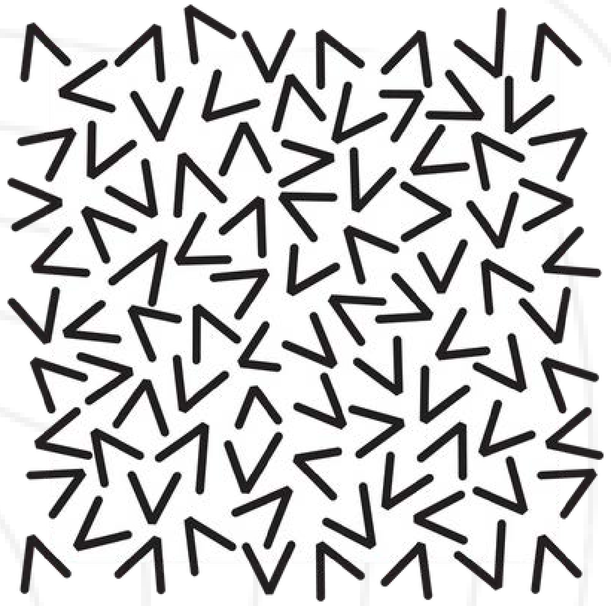
ENCRYPTION

ENCRYPTION

ENCRYPTION

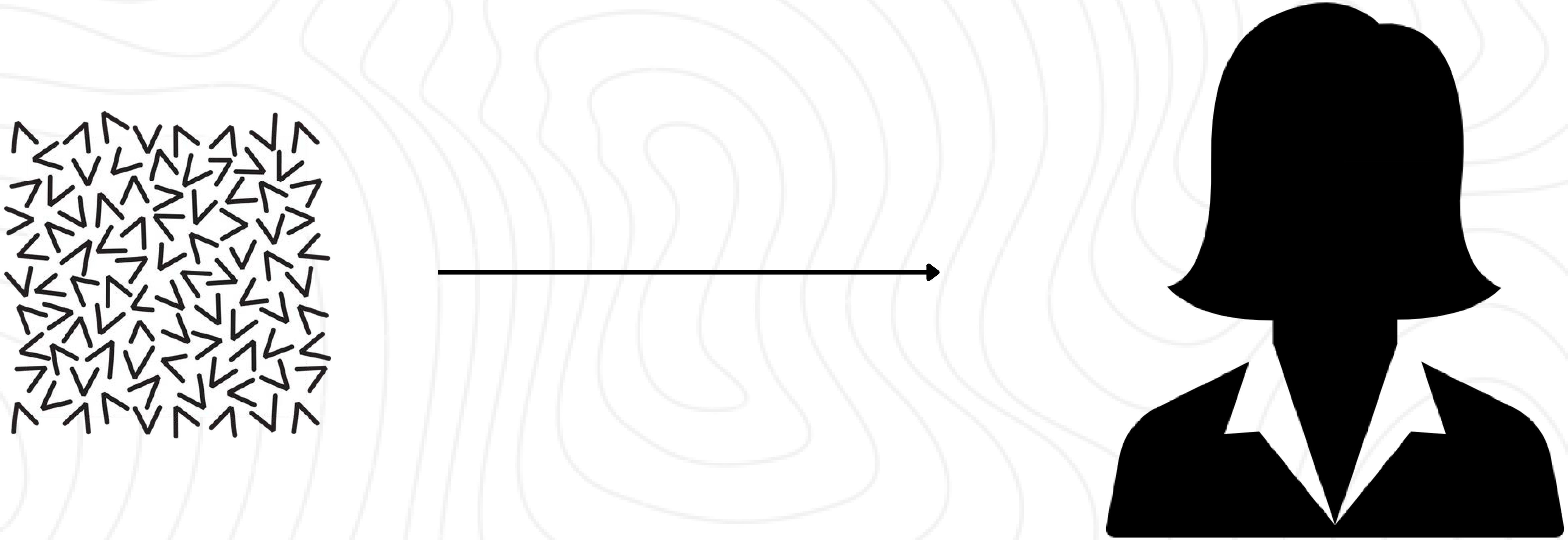


ENCRYPTION

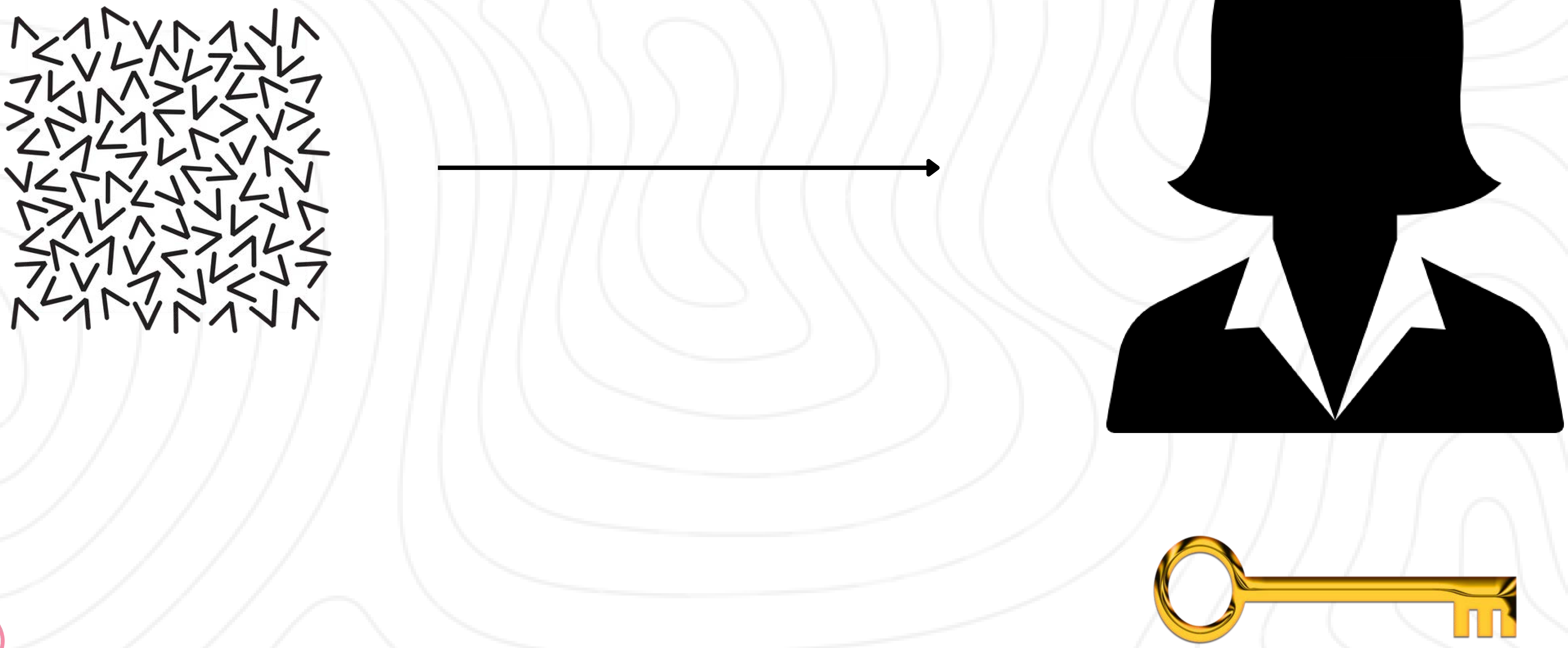


ENCRYPTION

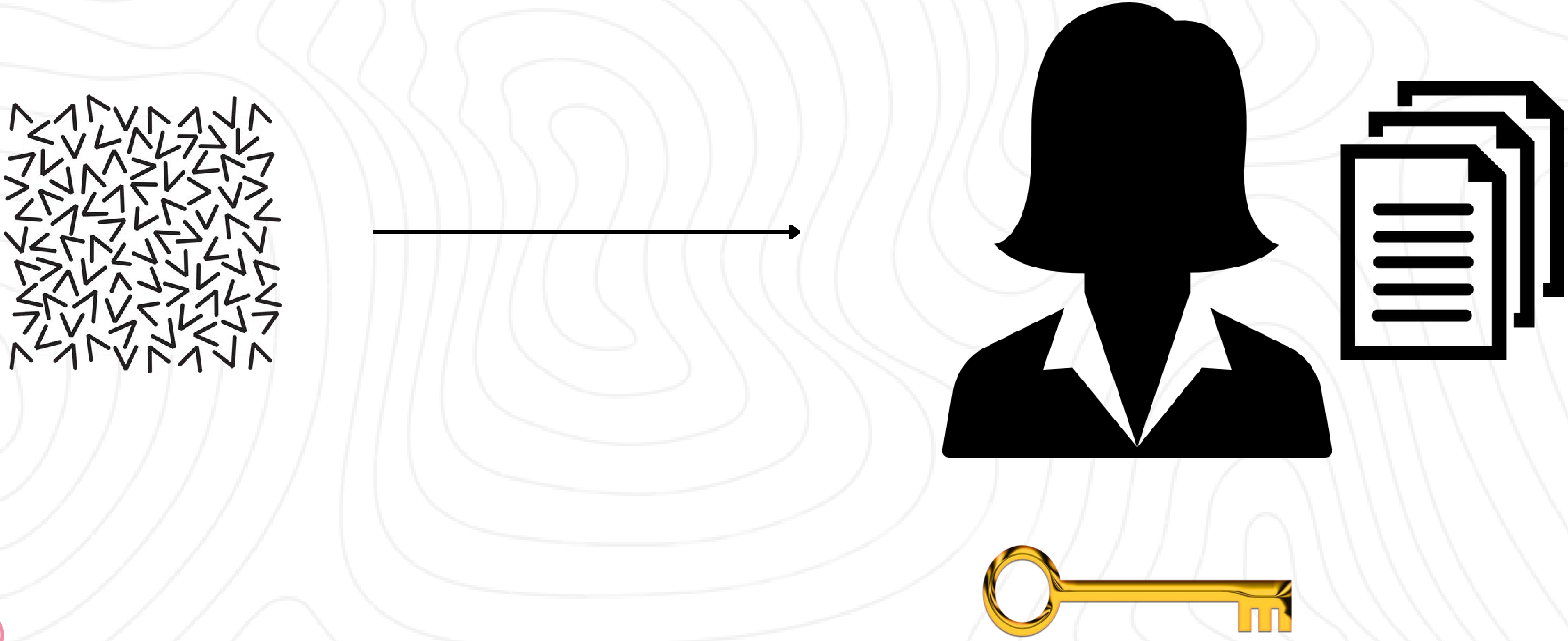
ENCRYPTION



ENCRYPTION



ENCRYPTION



EXAMPLES INCLUDE:

EXAMPLES INCLUDE:

- RSA (RIVEST–SHAMIR–ADLEMAN)

EXAMPLES INCLUDE:

- RSA (RIVEST–SHAMIR–ADLEMAN)
    - WEB BROWSERS, EMAIL, VPNS, ETC

EXAMPLES INCLUDE:

- RSA (RIVEST–SHAMIR–ADLEMAN)
    - WEB BROWSERS, EMAIL, VPNS, ETC
- DH (DIFFIE HELLMAN)

EXAMPLES INCLUDE:

- RSA (RIVEST–SHAMIR–ADLEMAN)
    - WEB BROWSERS, EMAIL, VPNS, ETC
- DH (DIFFIE HELLMAN)
    - TLS, SSH, IPSEC, ETC

EXAMPLES INCLUDE:

- RSA (RIVEST–SHAMIR–ADLEMAN)
    - WEB BROWSERS, EMAIL, VPNS, ETC
- DH (DIFFIE HELLMAN)
    - TLS, SSH, IPSEC, ETC
- ECC (ELLIPTIC CURVE CRYPTOGRAPHY)

EXAMPLES INCLUDE:

- RSA (RIVEST–SHAMIR–ADLEMAN)
    - WEB BROWSERS, EMAIL, VPNS, ETC
- DH (DIFFIE HELLMAN)
    - TLS, SSH, IPSEC, ETC
- ECC (ELLIPTIC CURVE CRYPTOGRAPHY)
    - BITCOIN, ETHEREUM, HASHING

CLASSICAL FACTOR FINDING

15 =

CLASSICAL FACTOR FINDING

15 = 3 X 5

CLASSICAL FACTOR FINDING

15 = 0 X 0

15 = 0 X 1

15 = 0 X 2

15 = 0 X 3

15 = 0 X 4

15 = 0 X 5

...

CLASSICAL FACTOR FINDING

15 = 0 X 0

15 = 0 X 1

15 = 0 X 2

15 = 0 X 3

15 = 0 X 4

15 = 0 X 5

...

CLASSICAL FACTOR FINDING

15 = 0 X 0

15 = 0 X 1

15 = 0 X 2

15 = 0 X 3

15 = 0 X 4

15 = 0 X 5

...

→

256 POSSIBILITIES

CLASSICAL FACTOR FINDING

15 = 0 X 0

15 = 0 X 1

15 = 0 X 2

15 = 0 X 3

15 = 0 X 4

15 = 0 X 5

...

→

256 POSSIBILITIES

15 = 3 X 5

SHOR'S ALGORITHM

4966717015468644898743809727803099326600759587405634476387700299416543377856505885160524455186694917656131614413391383 4
4111182634069624270365694091640192427593115657937659501513615614552675779556158955708954705116911915962635842817178303059 2
08208956058702838908152699771868669790169396099941440211189
=

SHOR'S ALGORITHM

49667170154686448987438097278030993266007595874056344763877002994165433778565058851605244551866949176561316144133913834
41111826340696242703656940916401924275931156579376595015136156145526757795561589557089547051169119159626358428171783030592
08208956058702838908152699771868669790169396099941440211189
=
66648642272608705760441226348132564396639431243755247575229047710793842277261161960013907230107717513242898432544939342
423749395996068801270761636557
X
74520903143886981832121710280039141716957679615802273718717164359634908897124378722007137784688051349637201373900023226 54
19773984391605941947367435977

SHOR'S ALGORITHM

4966717015468644898743809727803099326600759587405634476387700299416543377856505885160524455186694917656131614413391383 4
4111182634069624270365694091640192427593115657937659501513615614552675779556158955708954705116911915962635842817178303 0592
08208956058702838908152699771868669790169396099941440211189

=

6664864227260870576044122634813256439663943124375524757522904771079384227726116196001390723010771751324289843254493934 23
42374939599606880127076 1636557

X

745209031438869818321217102800391417169576796158022737187171643596349088971243787220071377846880513496372013739000232 2654
19773984391605941947367435977

2466827791174576341038729184312293966291470491655577296000584311707770431723559984497721395290503523
320188205655728321455567365417229058580020146756930221953829026274192382797749065942573693919806523
29165447127150148852836373064015690195114902237171616997852162817007398900032298917225560195997849059
5625790222514048772738764310486044489540738441981832298270505683013281302397015729921573941752161466
32984217745539632357536354141932829670228582518649705724017385011872390489921261015808957638718476823
239283720400951260018654929752164956889956401455743769996960986752155789609406151746655889207937 21

POSSIBILITIES

CLASSICAL COMPUTERS CAN'T DO IT IN A REASONABLE AMOUNT OF TIME!

CLASSICAL COMPUTERS CAN'T DO IT IN A REASONABLE AMOUNT OF TIME!

BUT QUANTUM COMPUTERS CAN...

SHOR'S ALGORITHM

15 = 0 X 0

15 = 0 X 1

15 = 0 X 2

15 = 0 X 3

15 = 0 X 4

15 = 0 X 5

...

→

256 POSSIBILITIES

15 = 3 X 5

SHOR'S ALGORITHM

15 = 0 X 0

+

15 = 0 X 1

+

15 = 0 X 2

+

15 = 0 X 3

+

15 = 0 X 4

+

15 = 0 X 5

...

→

256 POSSIBILITIES

15 = 3 X 5

SHOR'S ALGORITHM

15 = 0 X 0

+

15 = 0 X 1

+

15 = 0 X 2

+

15 = 0 X 3

+

15 = 0 X 4

+

15 = 0 X 5

...

→

256 POSSIBILITIES

15 = 3 X 5

8 QUBITS

SHOR'S ALGORITHM

24668277911745763410387291843122939662914704916555772960005843117077704317235599844977213952990503523
32018820565572832145556736541722905858002014675693022195382902627419238279774906594257369391980652 3
29165447127150148852836373064015690195114902237171616997852162817007398900032298917225560195997849059
56257902225140487727387643104860444895407384419818322982705056830132813023970157299215739417521614 66
32984217745539632357536354141932829670228582518649705724017385011872390489921261015808957638718476823
23928372040095126001865492975216495688995640145574376999696098675215578960940615174665588920793721

POSSIBILITIES

=

SHOR'S ALGORITHM

2466827791174576341038729184312293966291470491655577296000584311707770431723559984497721395299050352332018820565572832145556736541722905858002014675693022195382902627419238279774906594257369391980652329165447127150148852836373064015690195114902237171616997852162817007398900032298917225560195997849059562579022251404877273876431048604448954073844198183229827050568301328130239701572992157394175216146632984217745539632357536354141932829670228582518649705724017385011872390489921261015808957638718476823239283720400951260018654929752164956889956401455743769996960986752155789609406151746655889207937 21

POSSIBILITIES

=

BASICALLY INFINITY

SHOR'S ALGORITHM

2466827791174576341038729184312293966291470491655577296000584311707770431723559984497721395299050352 3
3201882056557283214555673654172290585800201467569302219538290262741923827977490659425736939198065 23
2916544712715014885283637306401569019511490223717161699785216281700739890003229891722556019599784905 9
5625790222514048772738764310486044489540738441981832298270505683013281302397015729921573941752161466
3298421774553963235753635414193282967022858251864970572401738501187239048992126101580895763871847682 3
2392837204009512600186549297521649568899564014557437699969609867521557896094061517466558892079372 1

POSSIBILITIES

=

BASICALLY INFINITY

9.2 YEARS

SHOR'S ALGORITHM

24668277911745763410387291843122939662914704916555772960005843117077704317235599844977213952990503523
320188205655728321455567365417229058580020146756930221953829026274192382797749065942573693919806523
29165447127150148852836373064015690195114902237171616997852162817007398900032298917225560195997849059
5625790222514048772738764310486044489540738441981832298270505683013281302397015729921573941752161466
32984217745539632357536354141932829670228582518649705724017385011872390489921261015808957638718476823
23928372040095126001865492975216495688995640145574376999696098675215578960940615174665588920793721

POSSIBILITIES

=

BASICALLY INFINITY

9.2 YEARS
2000 QUBITS

THE REALITY

- 433 QUBIT MACHINE | IBM

THE REALITY

- 433 QUBIT MACHINE | IBM
- ERROR-PRONE

PROBLEMS

- SCALABILITY (DUE TO NOISE)

PROBLEMS

- SCALABILITY (DUE TO NOISE)
- ERROR-CORRECTION

PROBLEMS

SNDL

POST-QUANTUM ENCRYPTION ALGORITHMS

NIST

POST-QUANTUM ENCRYPTION ALGORITHMS

NIST

CRYSTALS

KEY ENCAPSULATION
&
DIGITAL SIGNATURES

POST-QUANTUM ENCRYPTION ALGORITHMS

NIST

CRYSTALS

KEY ENCAPSULATION
&
DIGITAL SIGNATURES

FALCON

COMPACT DIGITAL
SIGNATURES

POST-QUANTUM ENCRYPTION ALGORITHMS

NIST

CRYSTALS

KEY ENCAPSULATION
&
DIGITAL SIGNATURES

FALCON

COMPACT DIGITAL
SIGNATURES

SPHINCS+

HASH-BASED
DIGITAL SIGNATURES

VALUES

Mission

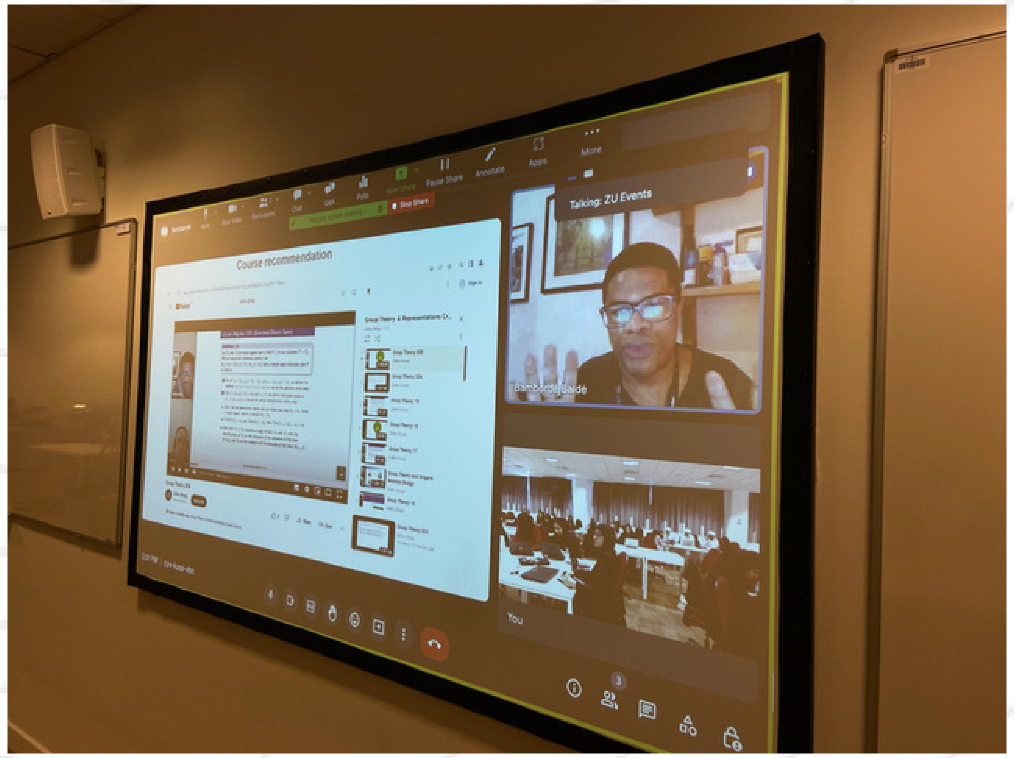
QUAE's mission is to democratize and advance quantum computing education, empowering individuals from diverse backgrounds to explore, understand, and harness the power of quantum technologies.

Vision

QUAE's vision is to create a world where quantum computing is accessible, understood, and harnessed by a broad and diverse community. We envision a future where quantum technologies revolutionize industries, solve complex problems, and unlock unprecedented possibilities.

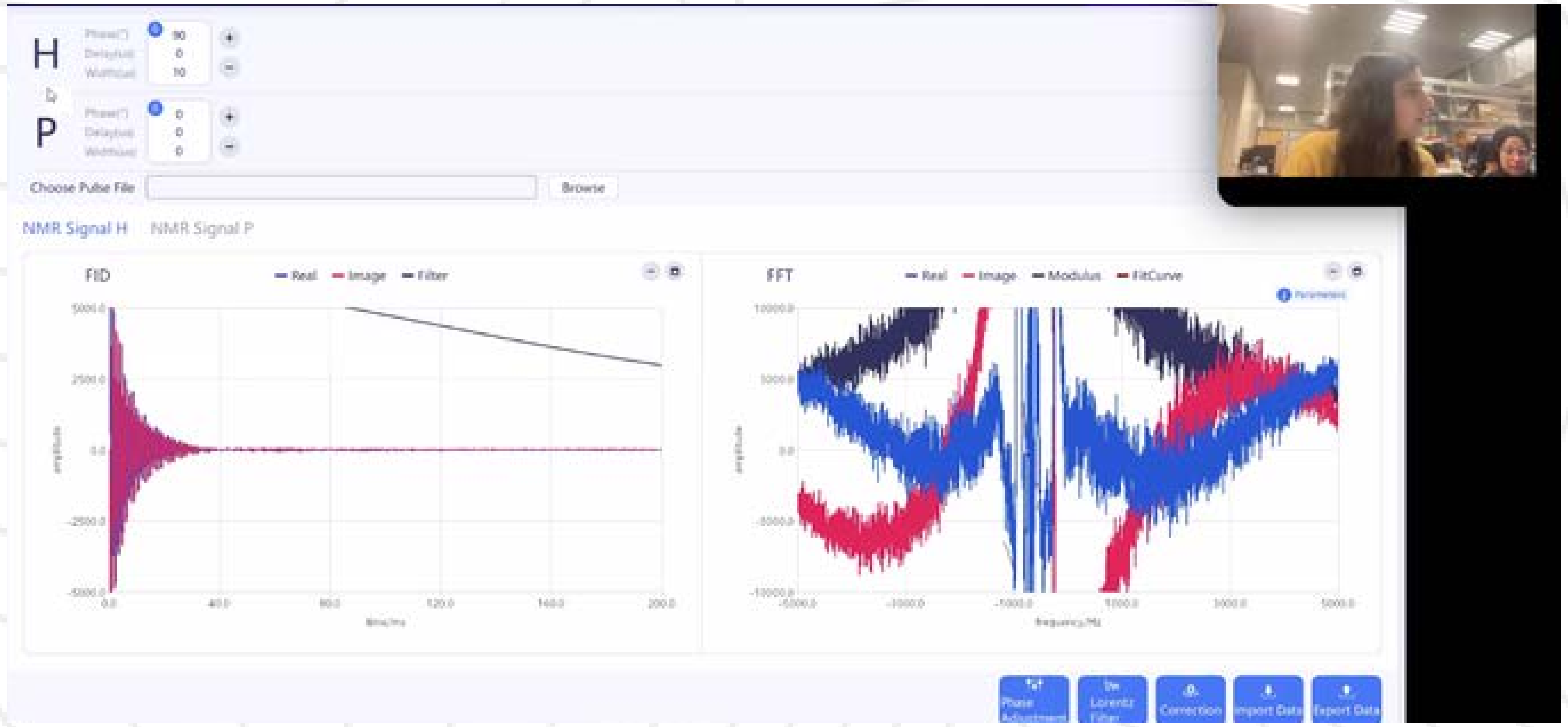
Our Initiatives :

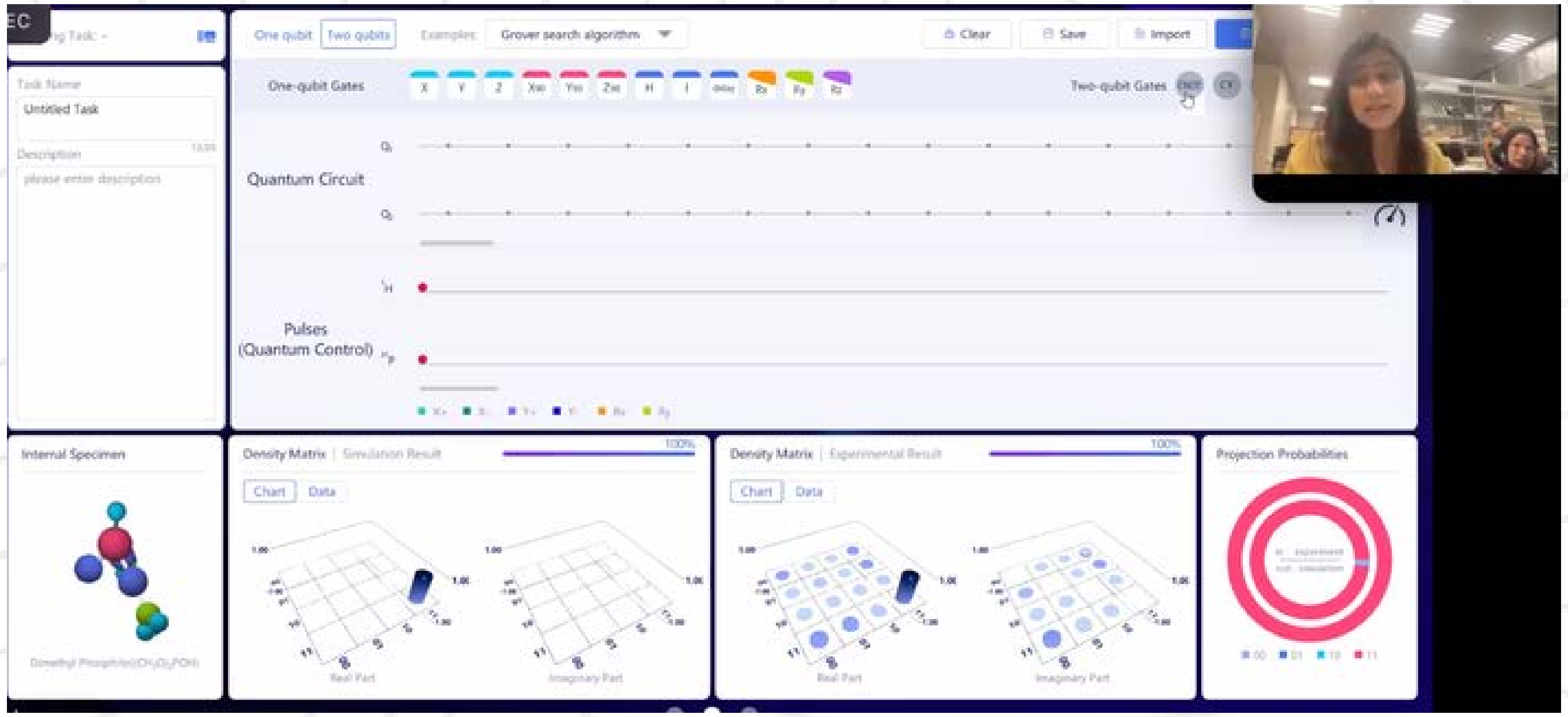
Review and History of Quantum Computing and Quantum Mechanics
Talking: ZU Events



مقر المبرمجين
coders(hq)

جامعة زايد
ZAYED UNIVERSITY


H
Phase(°) 90
Delay(us) 0
Width(us) 10
P
Phase(°) 0
Delay(us) 0
Width(us) 0
Choose Pulse File
Browse
NMR Signal H
NMR Signal P
FID
Real
Image
Filter
5000.0
2500.0
0.0
-2500.0
-5000.0
amplitude
0.0
40.0
80.0
120.0
160.0
200.0
time/ms
FFT
Real
Image
Modulus
FitCurve
Parameters
10000.0
5000.0
0.0
-5000.0
-10000.0
amplitude
-5000.0
-3000.0
-1000.0
1000.0
3000.0
5000.0
frequency/Hz
Phase Adjustment
Lorentz Filter
Correction
Import Data
Export Data


Task Name
Untitled Task
Description
please enter description
One qubit
Two qubits
Examples:
Grover search algorithm
Clear
Save
Import
One-qubit Gates
X
Y
Z
H
I
delay
Two-qubit Gates
CNOT
CR
Quantum Circuit
Pulses (Quantum Control)
Internal Specimen
Dimethyl Phosphite
Density Matrix | Simulation Result
100%
Chart
Data
Real Part
Imaginary Part
Density Matrix | Experimental Result
100%
Chart
Data
Real Part
Imaginary Part
Projection Probabilities
00
01
10
11

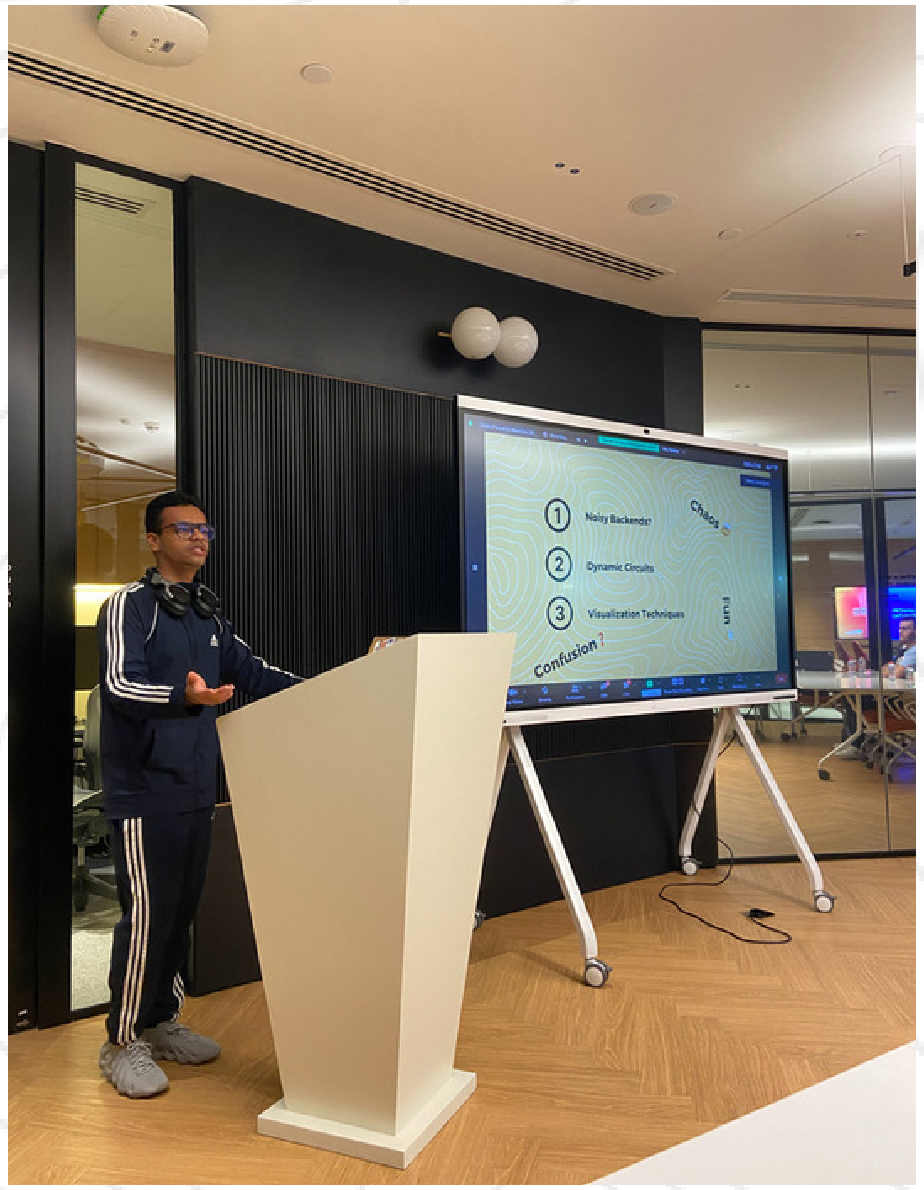
SPINQ
量旋科技
Quantum Computing
Nuclear Magnetic Resonance
Tasks Management
Calibration
Users Management
Knowledge

SPINQ

Meetup #1 on May 31st, 2023

مقر المبرمجين
coders(hq)

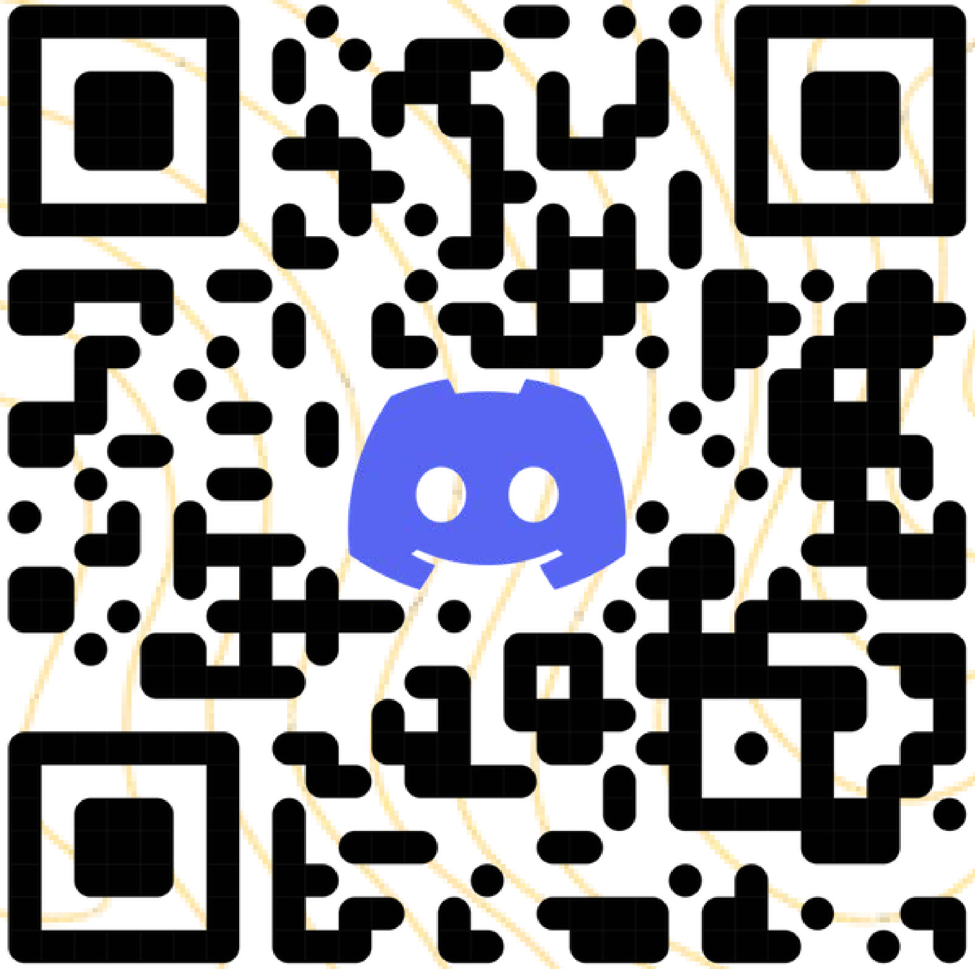
QUAE



QEducation

QIntern

QResearch



Email: quae@qworld.net