Keeping secrets in a post-quantum world

An exploration into encryption and quantum computers



What to expect

Total time ~ 2 hours 30 mins

1	Build some intuition about concepts.	35 mins
2	Code-breaking game, dive into encryption.	50 mins
3	Bring it together with demonstrations.	35 mins
4	Breaks, questions, and biscuits.	20 mins

How many of you know how to encrypt something?

I'll ask you again in a little while!


KLINGON VS UBBI DUBBI

Try speaking in Ubbi-Dubbi!

cat, dog, sun, hat, red, big, cup, pen, fish, box,
key, lock, map, egg, up, pig, bed, milk, desk,
frog, stop, jump, hello, secret, lemon, robot,
panda, pizza, music, banana

How many of you know how to encrypt something?

What is encryption?

Encryption is the process of making information undecipherable to those you don’t want knowing it.

Instructions for doing this are called ciphers / algorithms.

What is an algorithm?

A set of instructions on how to manipulate data to perform a task.

Encryption ciphers are one kind of algorithm.

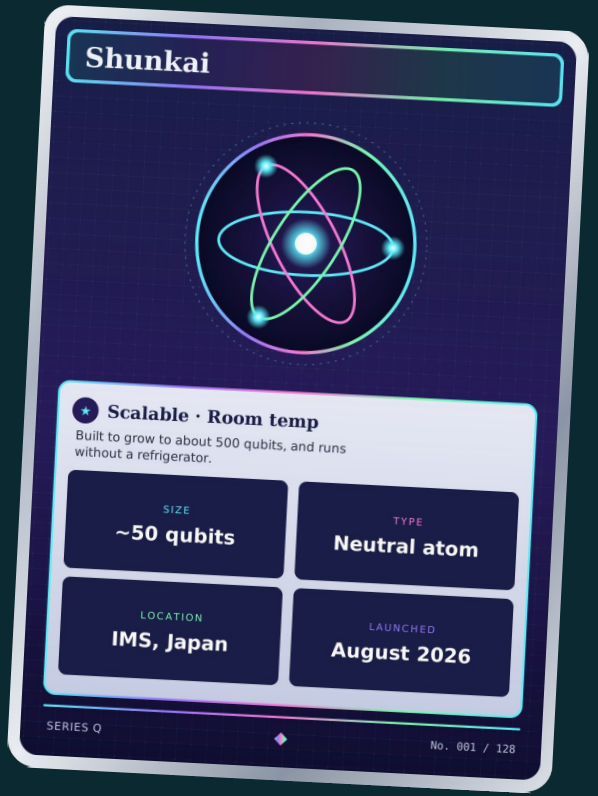
Quantum computers rely on algorithms too.

Quantum

What are some buzz words or concepts you've heard of around quantum physics or computers?

First, what does a quantum computer look like?





What does a quantum computer look like?





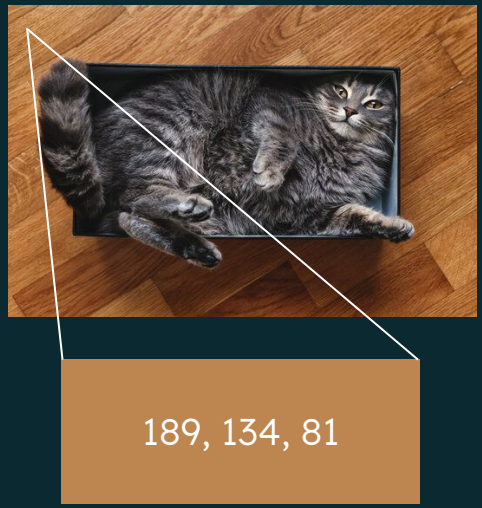
What does a quantum computer look like?





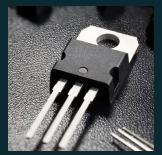
Computers today

Layer	Classical / Regular Computer
Data layer	Boolean, number, etc.
Bit layer	Regular bit - 1 or 0
Hardware layer	Anything that can represent 2 states



11001011, 10100101, 00101100





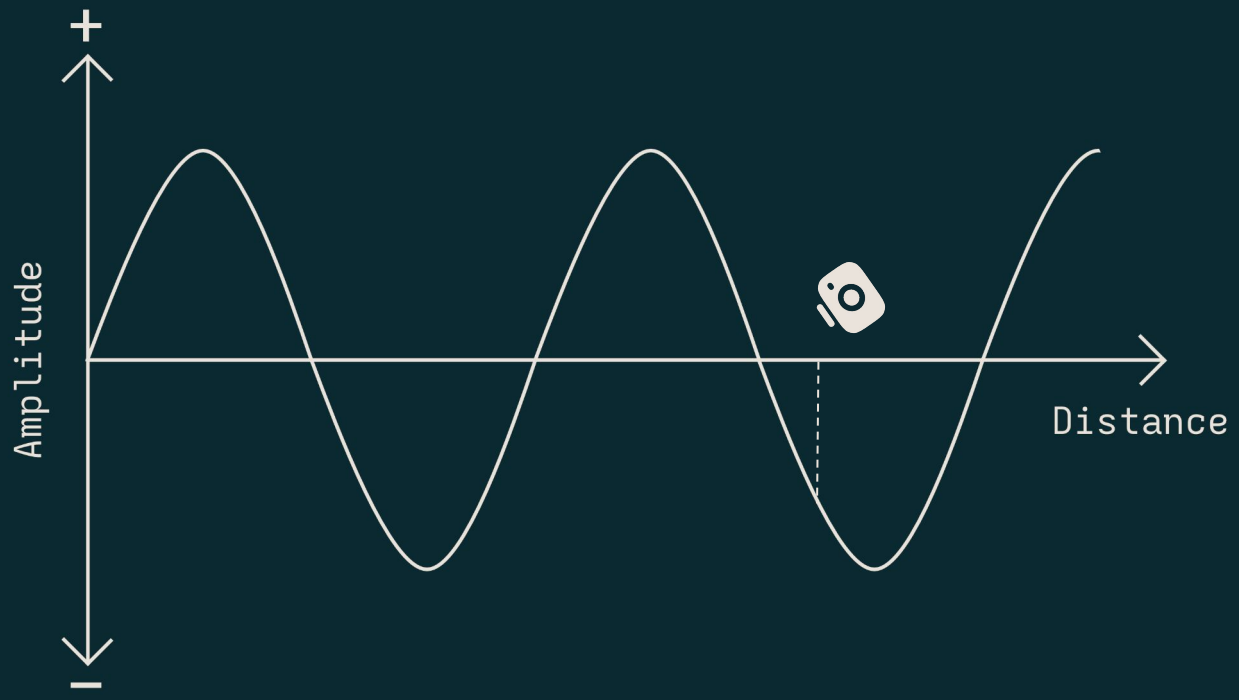
What changes in the quantum realm?

At incredibly small scales or low temperatures, things become less deterministic and more probabilistic.



Quantum probability is the uncertainty built into the very fabric of nature.

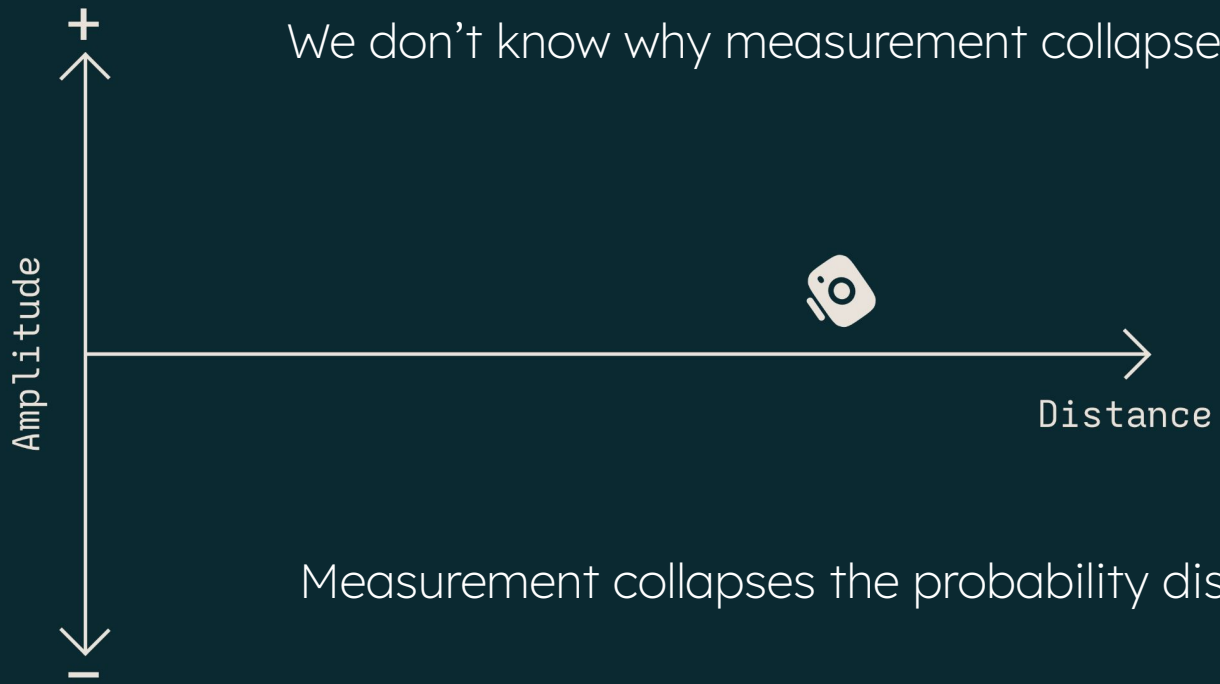
Wave of light frozen in time



Wave-like behaviour

of particles

Wave of light frozen in time

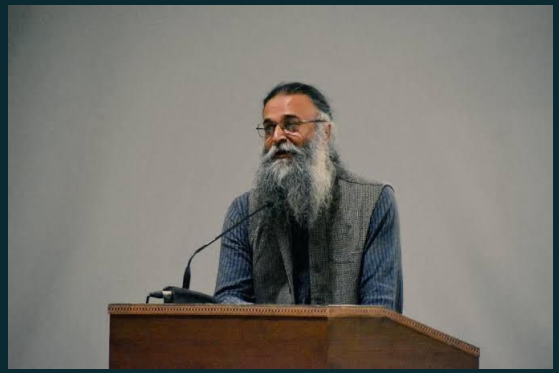


We don’t know why measurement collapses the wave 🤷‍♀️

Measurement collapses the probability distribution

A photon was either detected, or it wasn’t

A Glimpse Into the Quantum World



Dr. Arvind

Theoretical Physicist, IISER Mohali

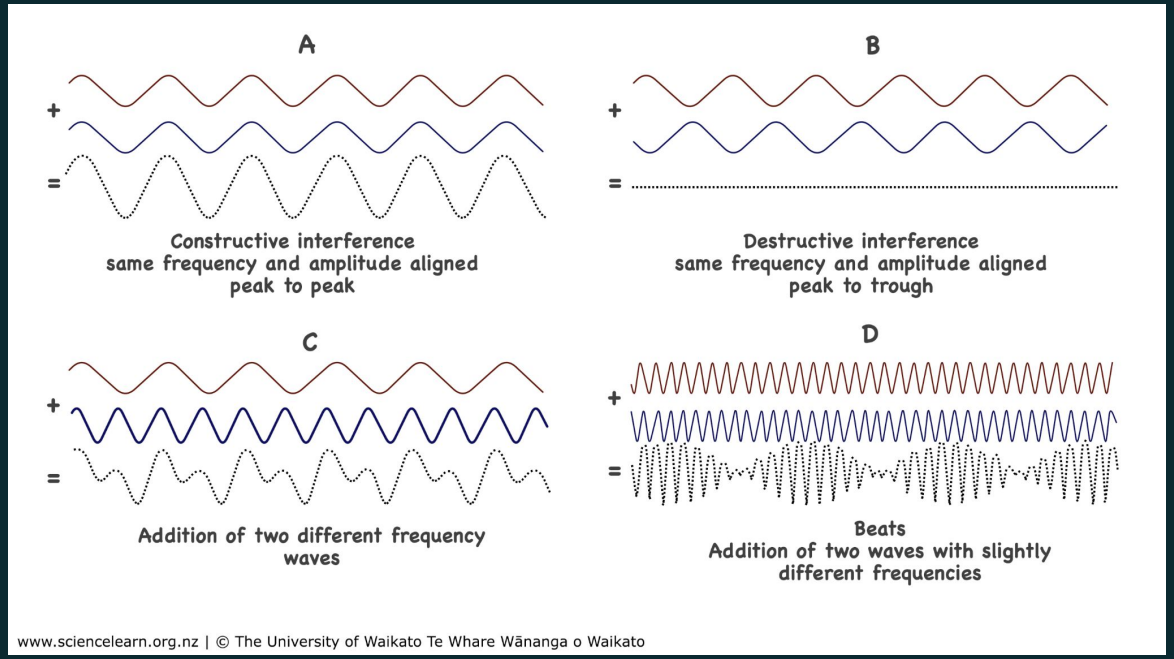
Sun, Oct 18 | 11:00 AM | SGB

How does this relate to quantum computing?

Quantum computing is all about manipulating these probabilities.

How do we do this?

Using interference



Most simple way to think of a quantum algorithm.

Wondering how this connects to encryption?



It will all make sense by the end!

Just remember the idea of interference and negative amplitudes.

That will be important!

The bit layer in a quantum computer

A qubit is made from quantum systems like a photon, atom, etc.

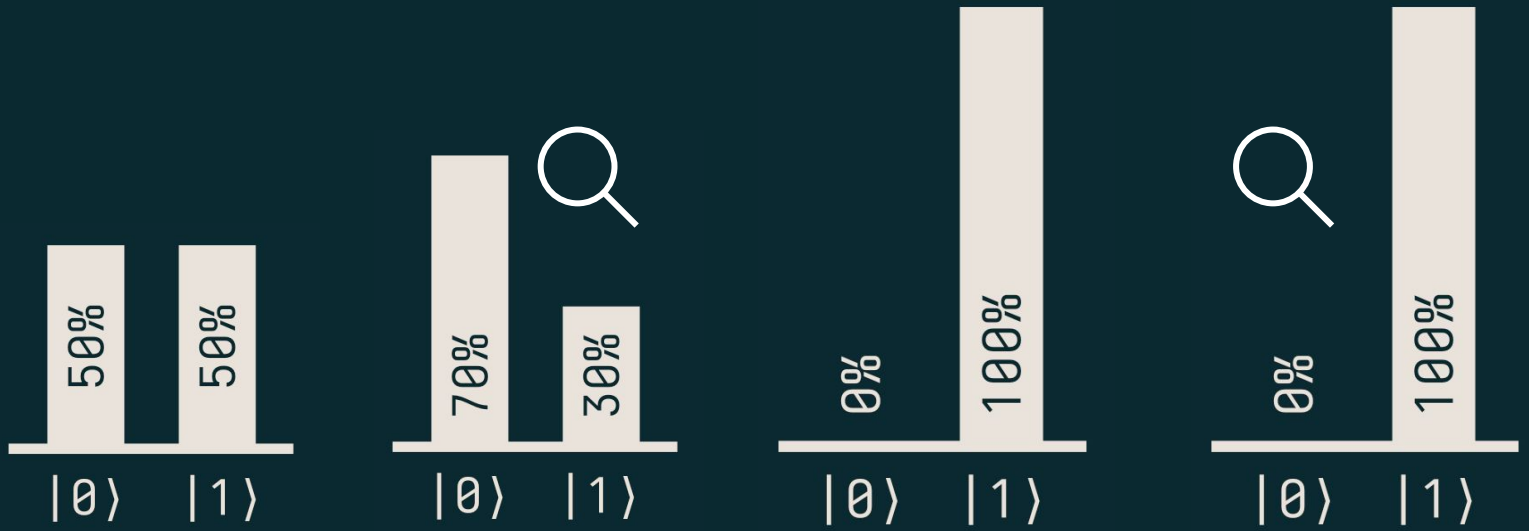
We can take two states that the photon can be in and assign it to a

$|1\rangle$ and a $|0\rangle$

$|?\rangle$ - Represents that something is a state of a quantum system.

The bit layer in a quantum computer

Until measurement, a qubit is in some probability distribution of states.



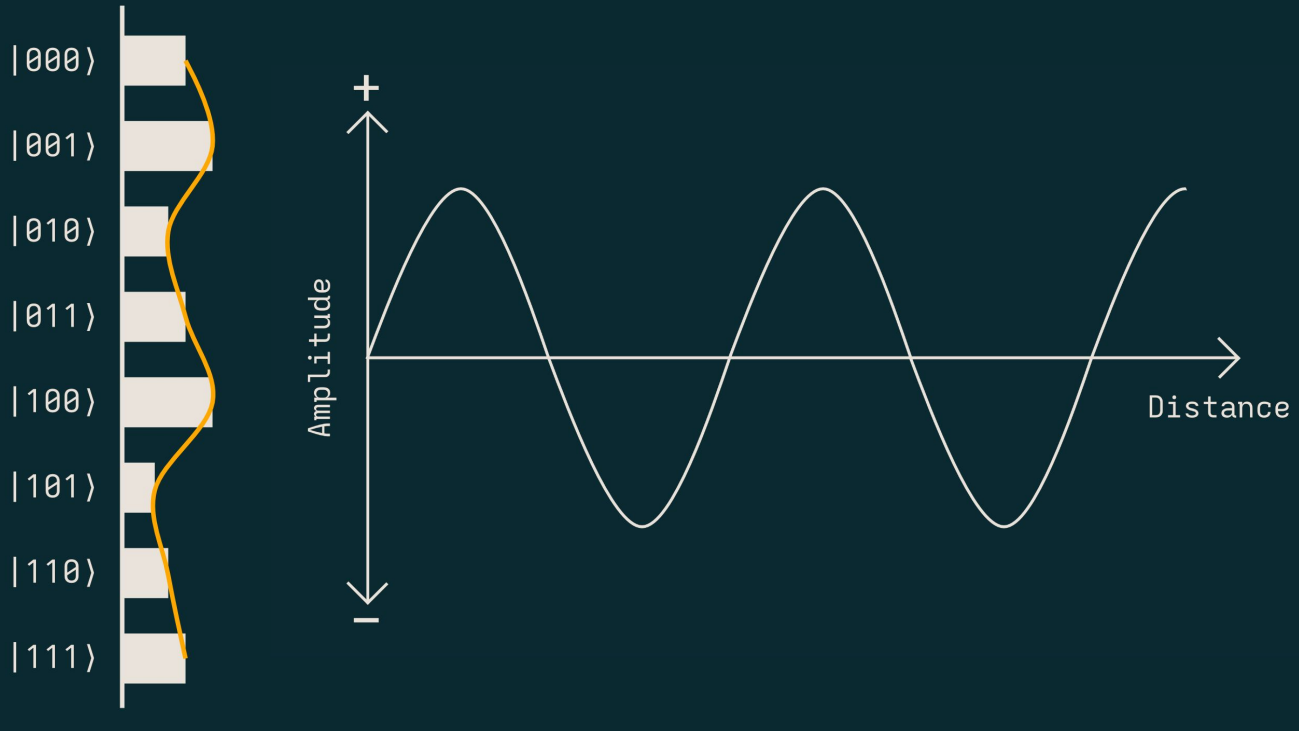
Scaling it up

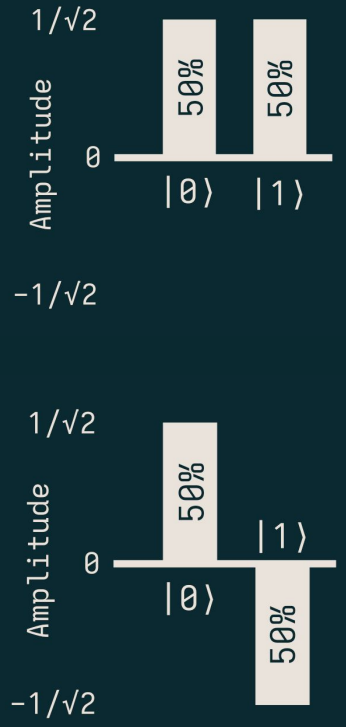


Ability of a quantum system to be spread across different states like this is called superposition.

The job of a quantum algorithm is to maximise the probability of reading out the right answer for a question.

Where do the probabilities come from?



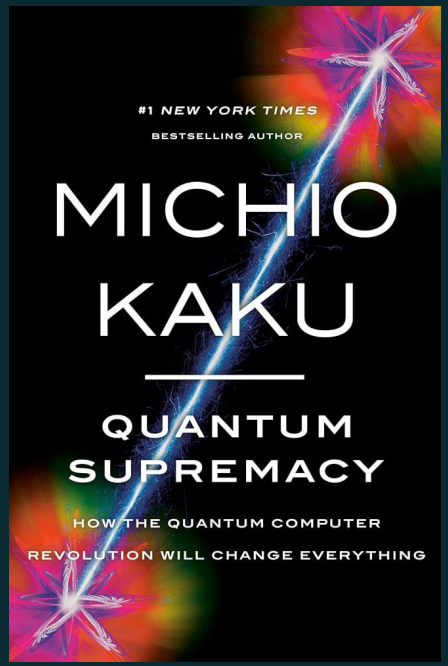


Why aren’t quantum computers everywhere?

Hardware Problems	Software Problems
Isolation.	Very few algorithms exist.
Error correction.	Writing new ones is hard.
Scaling it up.	Not every algorithm gives meaningful speedup.

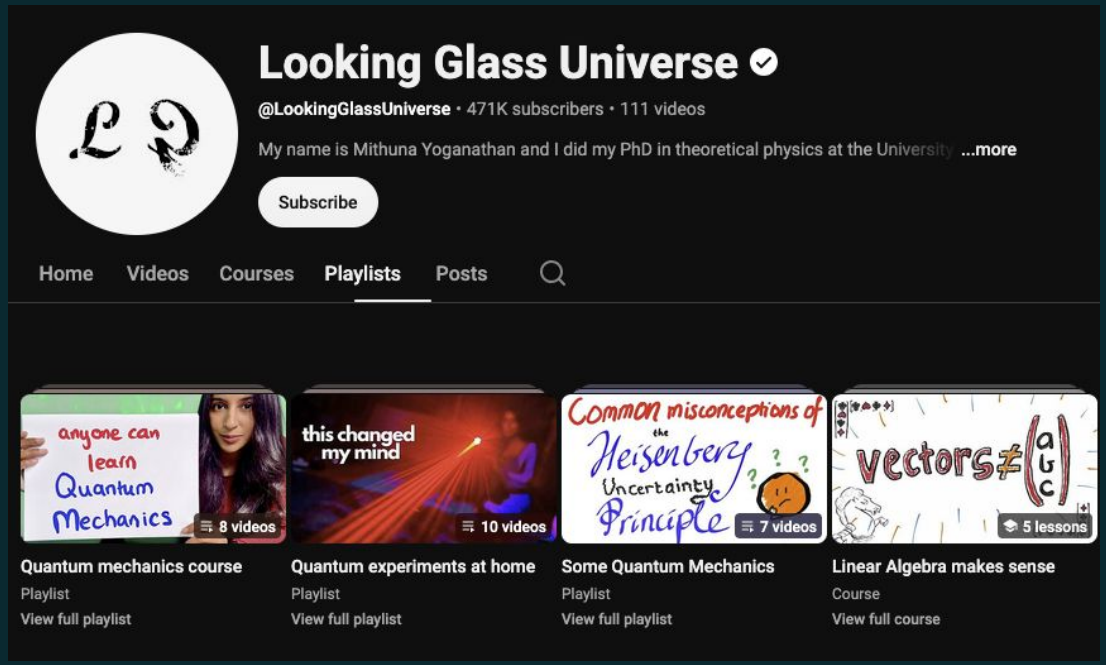


How is this useful?



*Overpromises

How does this work?



Don’t need math to start

Takeaway

A quantum computer is an entirely different model of computation. It is not a faster classical computer.

They only become useful when creatively used to solve a problem faster than a regular computer.

5 minute break & questions

Ready to be a code-breaker?

Inspired by true events after WW2

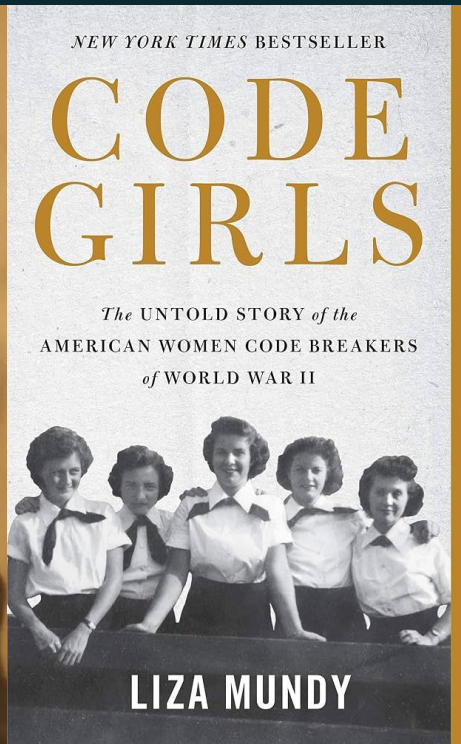
Easier ciphers, simpler messages, condensed plot

1949, Arlington Hall in Virginia - The Venona Project

Gene Grabeel, 22, Founder







Team up!

Groups of two or three

Day 1 - Atbash cipher | A ↔ Z

IVOLXZGV GL OLH ZOZNLH

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Like mirroring the scale in music - Sa, Ni, Da, Pa, Ma, Ga, Ri, Sa.

Spaces have been left in, usually not the case!

Substitution

Safety Slide


THE MANHATTAN
PROJECT

Day 2 - Caesar cipher | Ct = (Pt + Key) mod 26

Decryption : Pt = (Ct - Key) mod 26

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

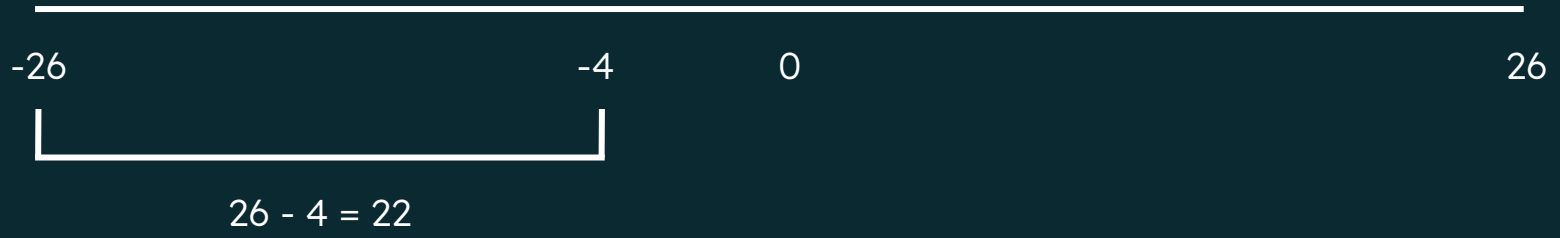
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25



Like playing a song in a different key

Key / noise addition

Modulus of negative numbers



Day 2 - Caesar cipher | Pt = (Ct - Key) mod 26

BTTI HDJGRT PI HPCIP UT

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25



Like playing a song in a different key

Key / noise addition

Safety Slide


5 MILES
285
Los
Alamos
502
4
4
84
285
NEW MEXICO
Santa Fe

Day 3 - Bellaso cipher | $Ct_i = (Pt_i + Key_i) \bmod 26$

KEYWORD → 10,4,24,22,14,17,3

P_i	P	L	A	I	N	T	E	X	T
→	15	11	0	8	13	19	4	23	19
K_i	10	4	24	22	14	17	3	10	4
+=	25	15	24	4	1	10	7	7	23
C_i	Z	P	Y	E	B	K	H	H	X

Like changing each note pitch by a different amount in a song.



Growing the key space

Day 3 - Bellaso cipher | $Pt_i = (Ct_i - Key_i) \bmod 26$

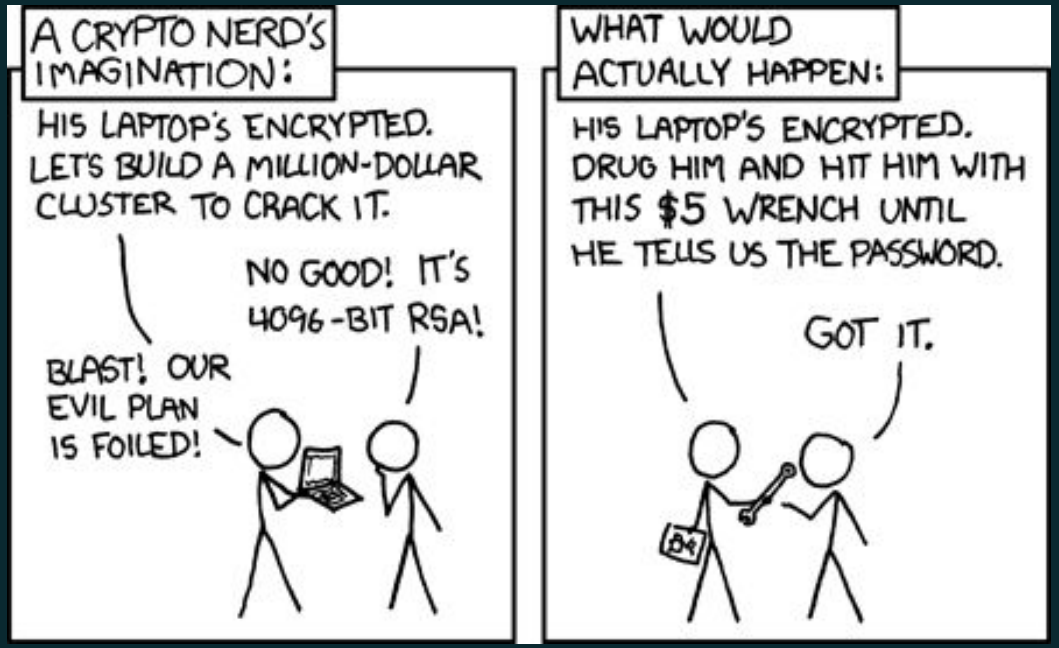
HAUTLPQO DRLHLE LUQI XEEOQH

KEY SPACE → 26^N where N is the length of the unknown keyword.

Solutions → Frequency analysis? parallelisation across computers?

Growing the key space

Reality check!



The key is ‘FACADE’. You’re welcome.

Growing the key space

Day 3 - Bellaso cipher | $Pt_i = (Ct_i - Key_i) \bmod 26$

HAUTLPQO DRLHLE LUQI XEEOQH

FACADE → 5,0,2,0,3,4

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

C_i	H	A	U	T	L	P	Q	O	…
→									
K_i	5	0	2	0	3	4	5	0	…
-=									
P_i									

Remember to subtract, not add!

Coordinate the key index with your team when splitting the work.

Growing the key space

Safety Slide

Courier to handler

CASTILLO BRIDGE JUNE SECOND



Day 4 - Atbash + Scytale cipher

TUCURINLULZCGNH →

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Day 4 - Atbash + Scytale cipher

TUCURINLULZCGNH → GFXFIRMOFOAXTMS



Safety Slide

Courier to handler

GIFT FROM XMAS FOX

Who is XMAS FOX?

Suspect	(Fun) Facts
J. Robert Oppenheimer	Led the Manhattan Project, had communist links.
Leslie R. Groves	Hand-picked Oppenheimer, skipping security checks.
Enrico Fermi	Electrons and similar particles are called “fermions” after him.
John von Neumann	Gave quantum physics solid mathematical ground.
Edward Teller	Feared the fission bomb might set the atmosphere on fire.
Rudolf Peierls	Estimated quantity of U235 needed for a fission bomb.
Richard Feynman	Sent encrypted letters to his wife. Picked locks at Los Alamos.
Klaus Fuchs	Filed patent for a hydrogen bomb trigger with von Neumann.

Klaus Fuchs

German born, British refugee, Soviet spy





Klaus Fuchs and courier Harry Gold met at Castillo Bridge on June 2nd, 1945.

Gave highly detailed technical plans for the “Fat Man” atomic bomb.

MI5 agent guilted him into confessing in 1950.

Separating fact from fiction



Actual cipher used by the Soviets, called the one-time pad, was said to be unbreakable if used properly.

There was no secret agent who got the keys.

There were around 750,000 intercepted messages between 1939 and 1948.

~3000 were decrypted over decades.

The one-time pad | $Ct_i = (Pt_i + Key_i) \bmod 26$

XHVIRZORUG

P_i	K	L	A	U	S	F	U	C	H	S
→										
K_i	23	7	21	8	17	25	14	17	20	6
+=										
C_i										

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25



Key Randomness

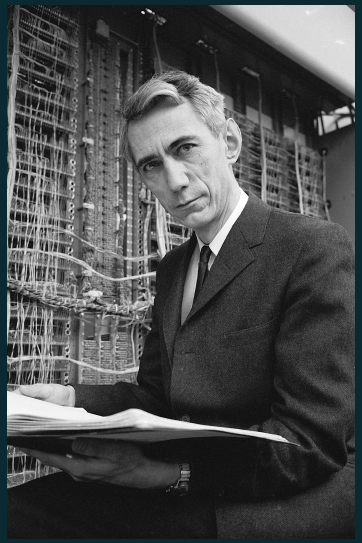
5 minute break & questions

What makes the one-time pad unbreakable?

Immune to frequency analysis and brute force.

However, only when used correctly:

Rule	Reason
No key reuse	Key can be cancelled, Soviets made this mistake.
K length = P length	No repeat patterns to exploit.
Truly random key	Every plaintext is equally likely.
Key must be secret	Only remaining attack surface.



Claude Shannon, 1949

Why don’t we use the one-time pad anymore?

For each of the rules, think of possible implementation hurdles.

Rule	Reason
No key reuse	Need constant supply of fresh keys, Soviets failed at this.
K length = P length	Sending a 1GB file will require a 1GB key.
Truly random key	True random number generation used to be hard. Not anymore.
Key must be secret	Exchanging the keys securely becomes tedious.

We’ll see how we fixed the problems of key reuse and key length first.

Then we’ll explore how we fixed the problem of key exchange.

Advanced Encryption Standard (AES)

128 bit key → 01000111 00111000 10001111 11010001 01111000 ...

0100 1011	1001 1100	1100 0101	1010 1101
1001 1100	1100 0101	0100 1011	1001 1100
1001 1100	1100 0101	1010 1101	1100 0101
1010 1101	1100 0101	1001 1100	1100 0101

128 bit data block

We already know everything needed to encrypt with AES. Loop following steps 10+ times:

- Substitution
- Transposition
- Key addition

Changing just 1 bit of either the plaintext or the key will change a majority of the ciphertext.

Advanced Encryption Standard (AES)

Key reuse: Safe from subtraction. Key is diffused throughout.

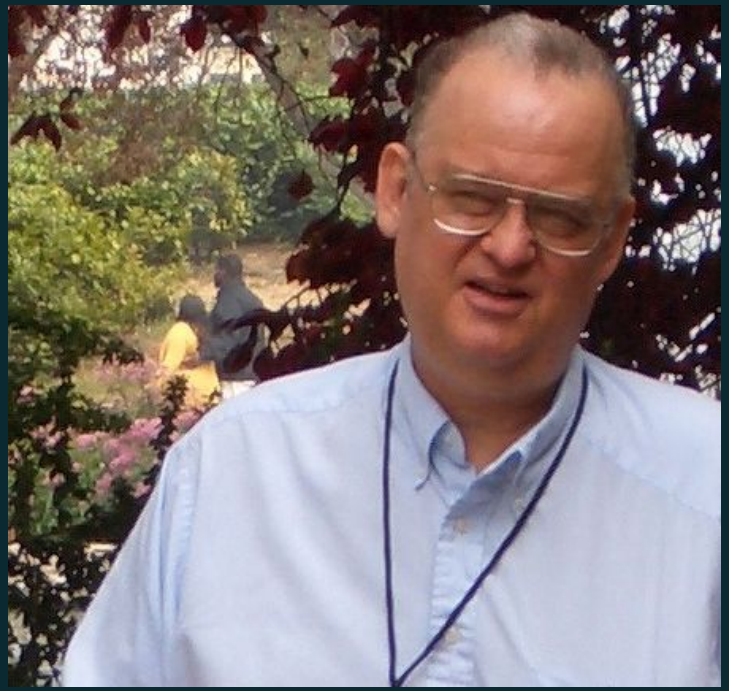
Key length: Can be short. Chain blocks to encrypt longer message.

Brute-force: 3.4×10^{38} possible keys. Astronomically large.

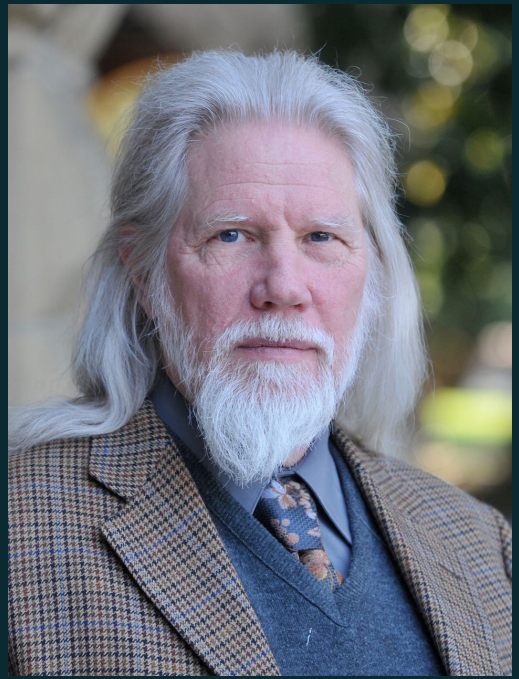
340,000,000,000,000,000,000,000,000,000,000,000.

Would take billions of years even if we put every computer on the task.

Solving the key exchange problem, 1976



Ralph Merkle



Whitfield Diffie

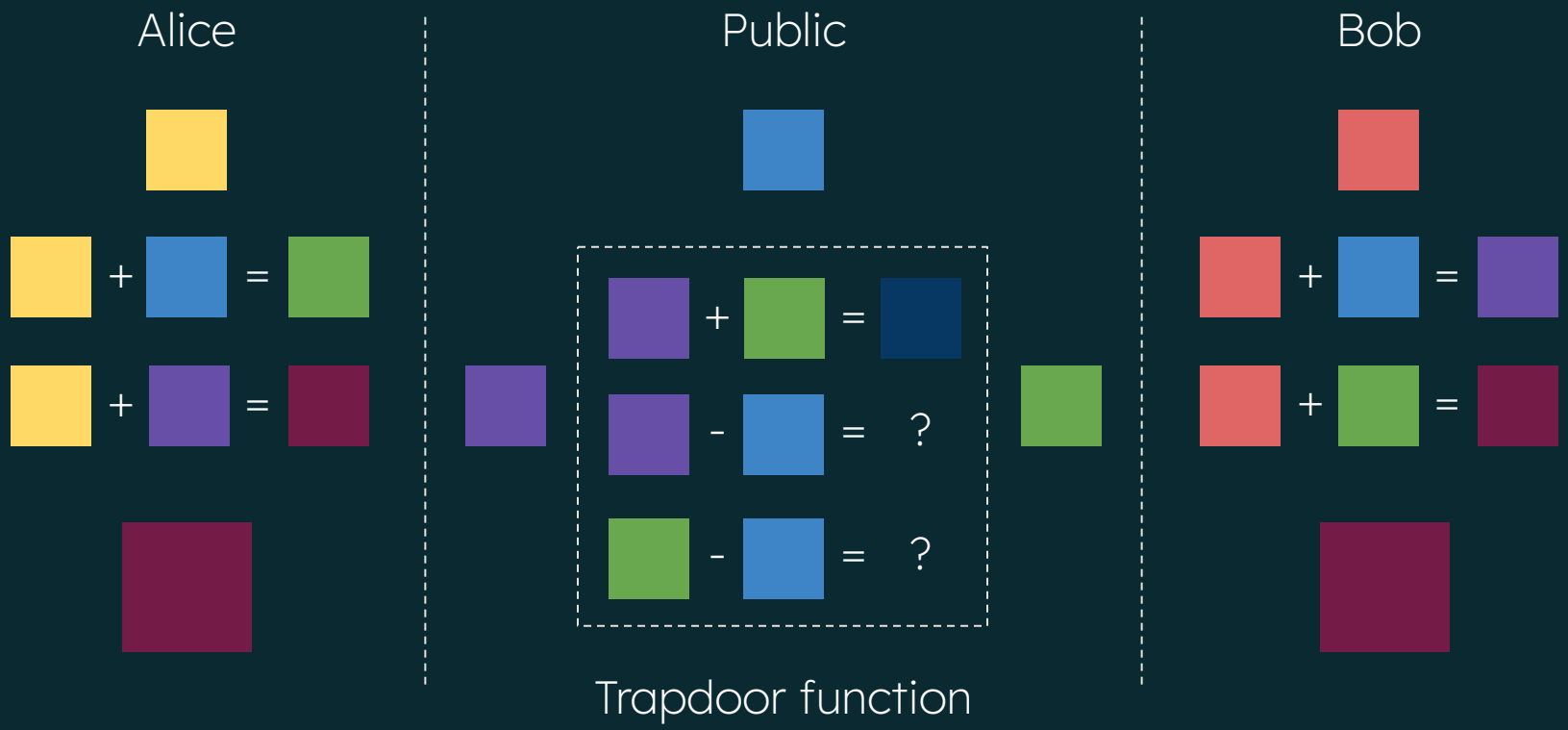


Martin Hellman

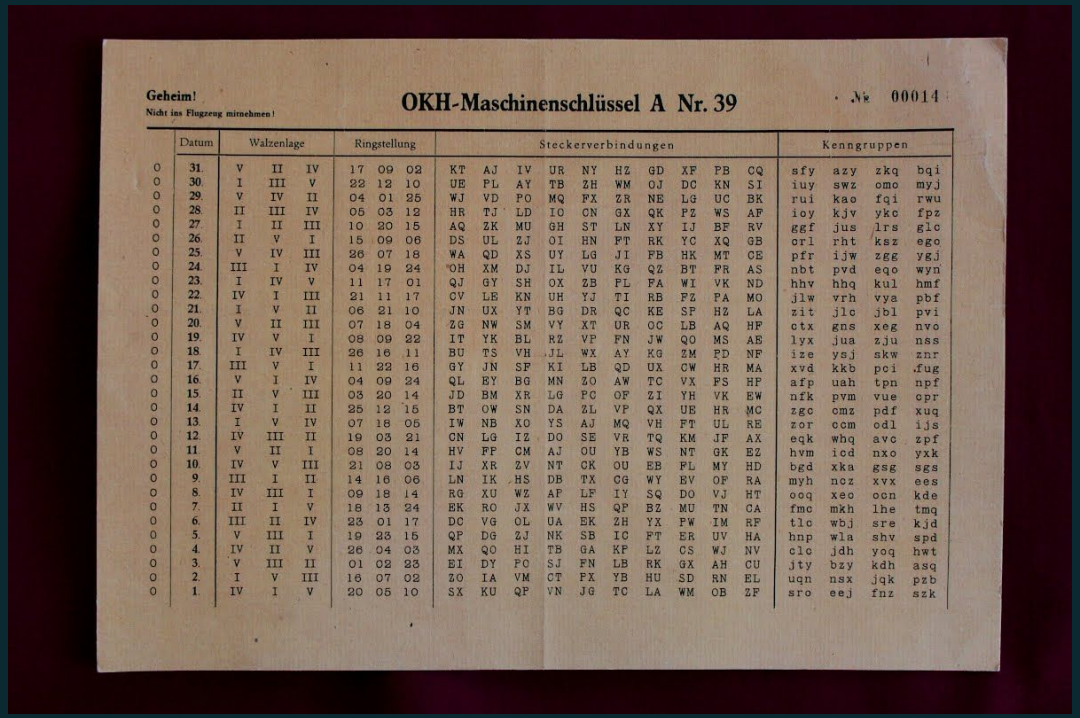
Activity time

Sorry about the cat hair!

Diffie-Hellman Key Exchange, 1976



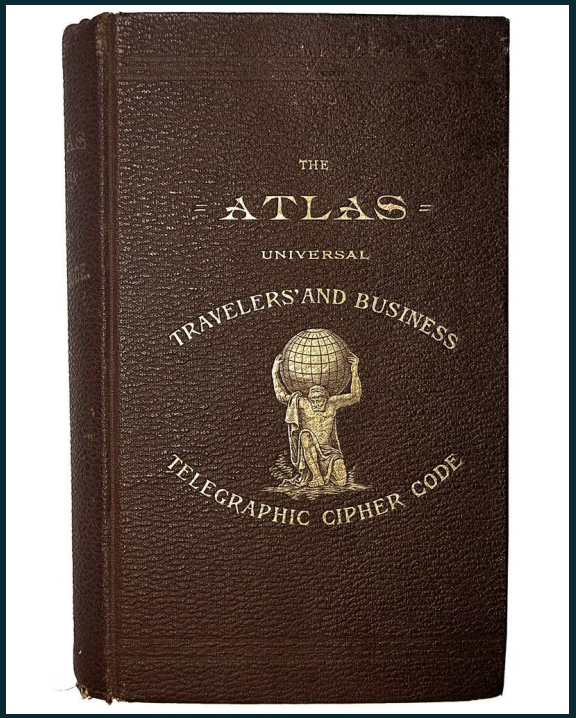
Why is this important?



Geheim!
Nicht ins Flugzeug mitnehmen!

OKH-Maschinenschlüssel A Nr. 39 · № 00014

	Datum	Walzenlage			Ringstellung			Steckerverbindungen								Kenngruppen			
0	31.	V	II	IV	17	09	02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	CQ	sfy	azy	zkq	bqi
0	30.	I	III	V	22	12	10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	swz	omo	myj
0	29.	V	IV	II	04	01	25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu
0	28.	II	III	IV	05	03	12	HR	TJ	LD	IO	CN	GX	QK	PZ	WS	AF	ioy	kjv	yko	fpz
0	27.	I	II	III	10	20	15	AQ	ZK	MU	GH	ST	LN	XY	IJ	BF	RV	ggf	jus	lrs	glc
0	26.	II	V	I	15	09	06	DS	UL	ZJ	OI	HN	FT	RK	YC	XQ	GB	orl	rht	ksz	ego
0	25.	V	IV	III	26	07	18	WA	QD	XS	UY	LG	JI	FB	HK	MT	CE	pfr	ijw	zgg	ygj
0	24.	III	I	IV	04	19	24	OH	XM	DJ	IL	VU	KG	QZ	BT	FR	AS	nbt	pvd	eqo	wyn
0	23.	I	IV	V	11	17	01	QJ	GY	SH	OX	ZB	PL	FA	WI	VK	ND	hhv	hhq	kul	hmf
0	22.	IV	I	III	21	11	17	CV	LE	KN	UH	YJ	TI	RB	FZ	PA	MO	jlw	vrh	vya	pbf
0	21.	I	V	II	06	21	10	JN	UX	YT	BG	DR	QC	KE	SP	HZ	LA	zit	jlc	jbl	pvi
0	20.	V	II	III	07	18	04	ZG	NW	SM	VY	XT	UR	OC	LB	AQ	HF	ctx	gns	xeg	nvo
0	19.	IV	V	I	08	09	22	IT	YK	BL	RZ	VP	FN	JW	QO	MS	AE	lyx	jua	zju	nss
0	18.	I	IV	III	26	16	11	BU	TS	VH	JL	WX	AY	KG	ZM	PD	NF	ize	ysj	skw	znr
0	17.	III	V	I	11	22	16	GY	JN	SF	KI	LB	QD	UX	CW	HR	MA	xvd	kkb	pci	fug
0	16.	V	I	IV	04	09	24	QL	EY	BG	MN	ZO	AW	TC	VX	FS	HF	afp	uah	tpn	npf
0	15.	II	V	III	03	20	14	JD	BM	XR	LG	PC	OF	ZI	YH	VK	EW	nfk	pvm	vue	opr
0	14.	IV	I	II	25	12	15	BT	OW	SN	DA	ZL	VP	QX	UE	HR	MC	zgc	omz	pdf	xuq
0	13.	I	V	IV	07	18	05	IW	NB	XO	YS	AJ	MQ	VH	FT	UL	RE	zor	ccm	odl	ijs
0	12.	IV	III	II	19	03	21	CN	LG	IZ	DO	SE	VR	TQ	KM	JF	AX	eqk	whq	avc	zpf
0	11.	V	II	I	08	20	14	HV	FF	CM	AJ	OU	YB	WS	NT	GK	EZ	hvm	iod	nxo	yxk
0	10.	IV	V	III	21	08	03	IJ	XR	ZV	NT	CK	OU	EB	FL	MY	HD	bgd	xka	gsg	sgs
0	9.	III	I	II	14	16	06	LN	IK	HS	DB	TX	CG	WY	BV	OF	RA	myh	ncz	xvx	ees
0	8.	IV	III	I	09	18	14	RG	XU	WZ	AF	LF	IY	SQ	DO	VJ	HT	ooq	xeo	ocn	kde
0	7.	II	I	V	18	13	24	EK	RO	JX	WV	HS	QP	BZ	MU	TN	CA	fmc	mkh	lhe	tmq
0	6.	III	II	IV	23	01	17	DC	VG	OL	UA	EK	ZH	YX	FW	IM	RF	tlc	wbj	sre	kjd
0	5.	V	III	I	19	23	15	QP	DG	ZJ	NK	SB	IC	FT	ER	UV	HA	hnp	wla	shv	spd
0	4.	IV	II	V	26	04	03	MX	QO	HI	TB	GA	KP	LZ	CS	WJ	NV	clc	jdh	yoq	hwt
0	3.	V	III	II	01	02	23	EI	DY	PO	SJ	FN	LB	RK	GX	AH	CU	jty	bzy	kdh	asq
0	2.	I	V	III	16	07	02	ZO	IA	VM	CT	FX	YB	HU	SD	RN	EL	uqn	nsx	jqk	pzb
0	1.	IV	I	V	20	05	10	SX	KU	QP	VN	JG	TC	LA	WM	OB	ZF	sro	eej	fnz	szk

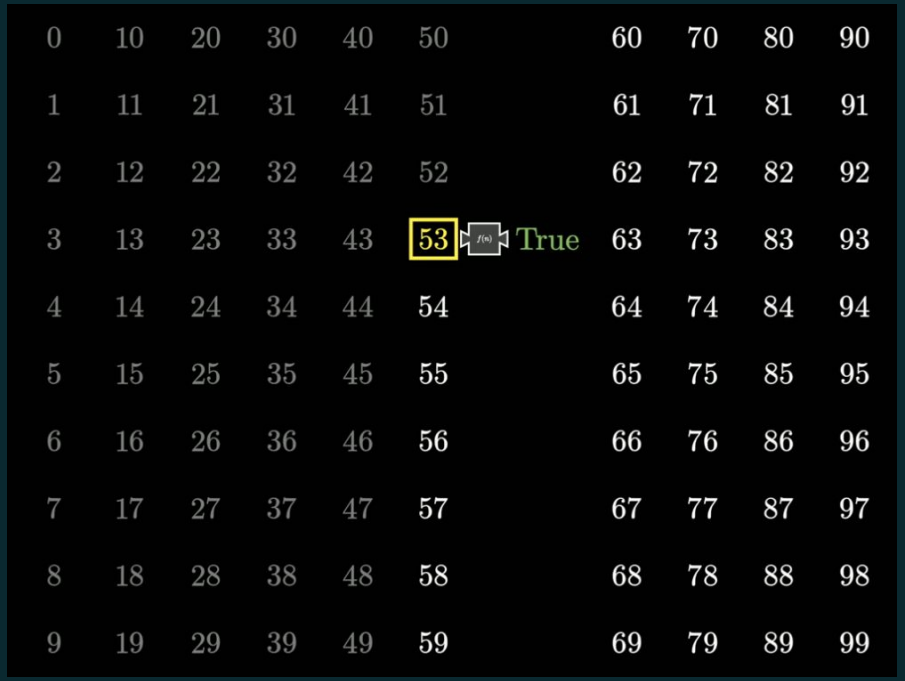


Takeaway

Randomness and trapdoor functions are the bedrock of modern encryption and the entire internet.

5 minute break & questions

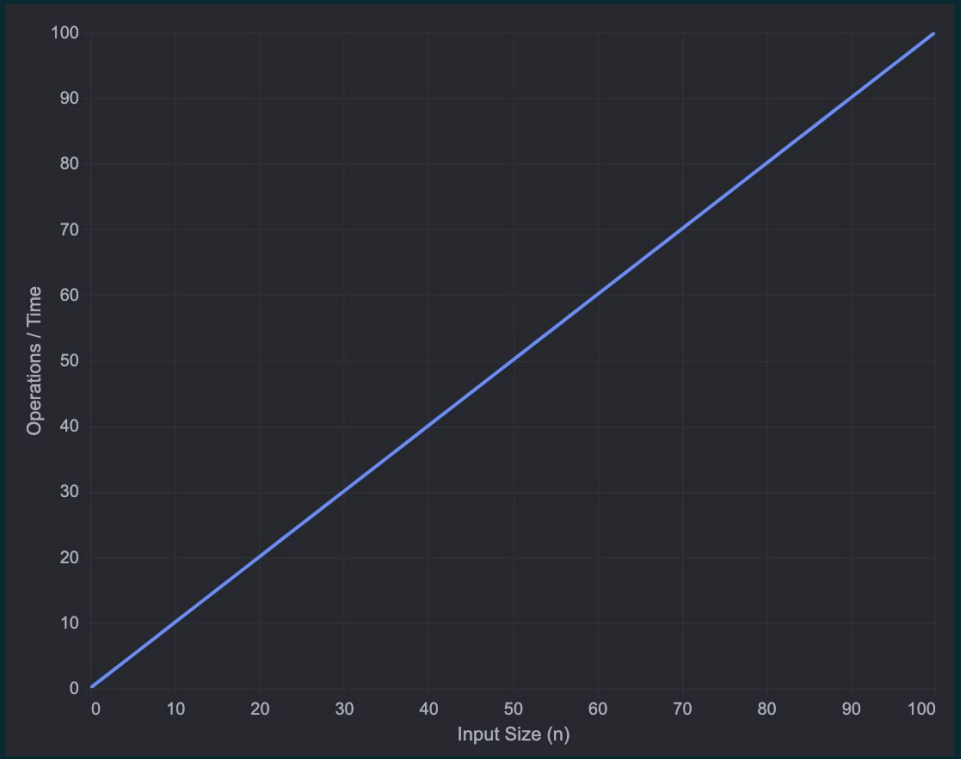
Random key search on a classical computer



Credits: 3Blue1Brown on YouTube

Avg: N / 2 times

How does the compute time grow with N?



Can quantum computers do this faster?

Grover’s quantum search algorithm, 1996



Lov Kumar Grover

Born in Meerut, India.

Alumnus of IIT Delhi.

Worked at Bell Laboratories.

Grover’s quantum search algorithm, 1996

Major milestone in the field of quantum algorithms.

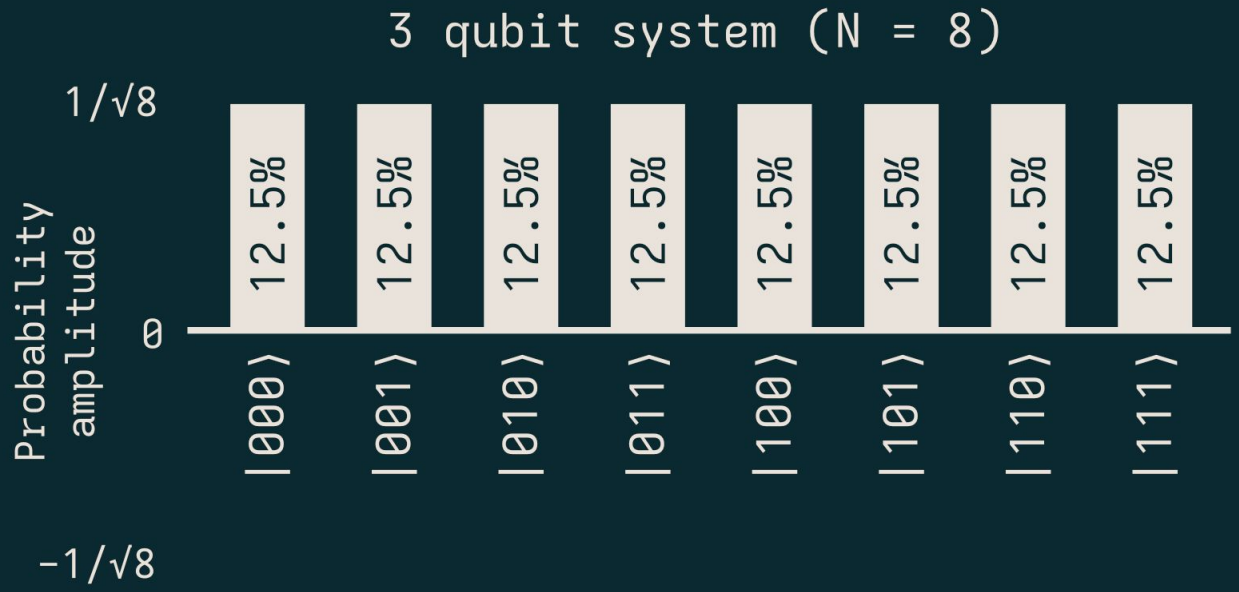
Came out two years after Peter Shor’s algorithm.

Shor’s is the real threat, but Grover’s is simpler to understand.

If there’s enough interest, we can have a follow up workshop.

Grover’s quantum search algorithm

Initialise the qubits in a state of uniform superposition.



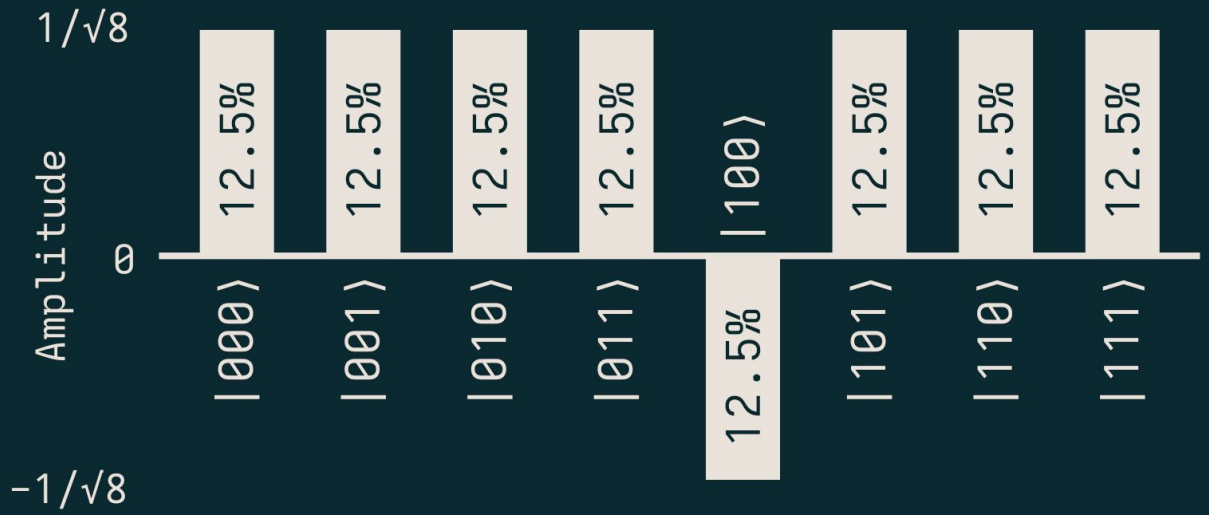
Grover’s quantum search algorithm

Encode constraints of the question into a quantum circuit called the oracle, i.e. answer checker.



Grover’s quantum search algorithm

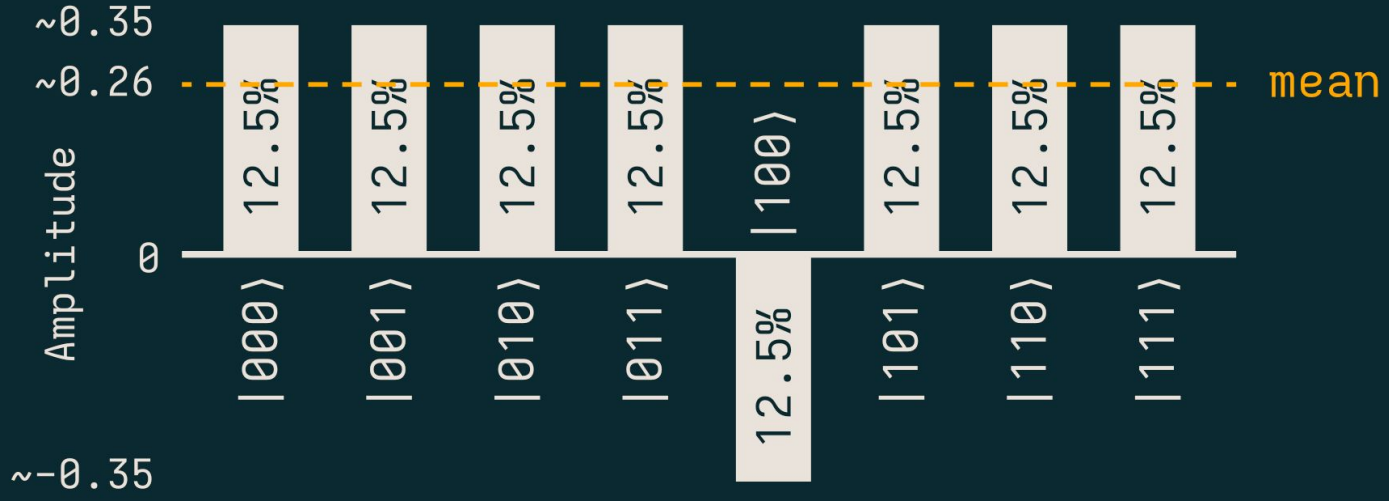
Oracle marks the right answer by flipping its sign.



Does not affect probability, but affects amplitude.

Grover’s quantum search algorithm

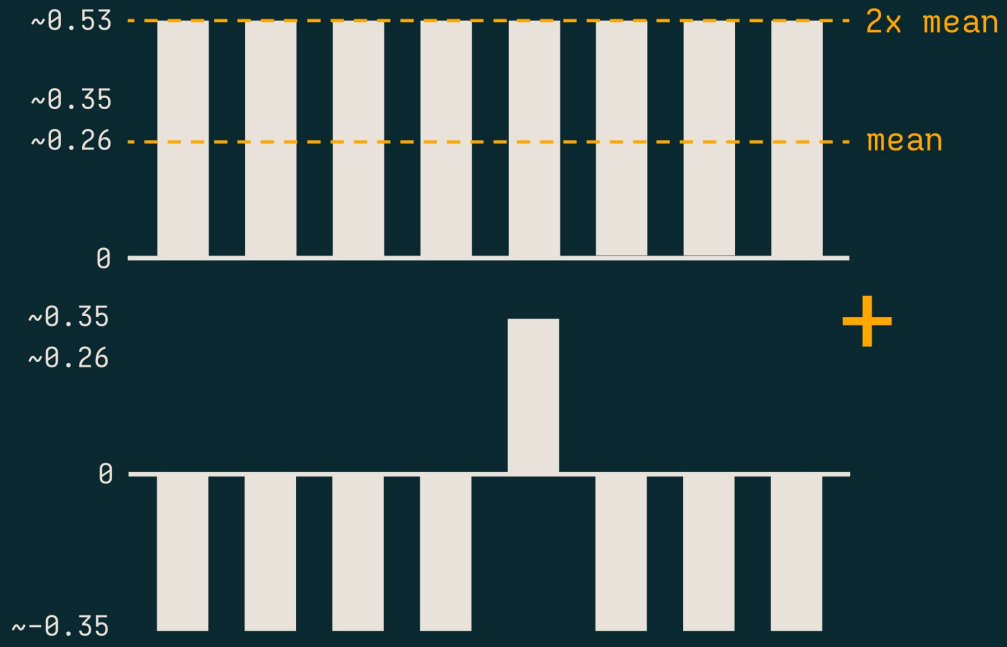
Find the mean, knowing the answer is not relevant for this.

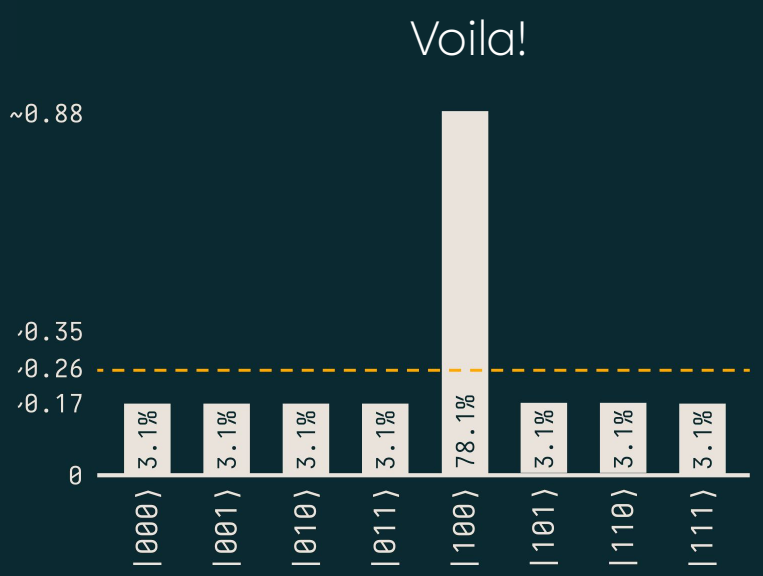


Inversion about the mean => 2x mean - old value

Grover’s quantum search algorithm

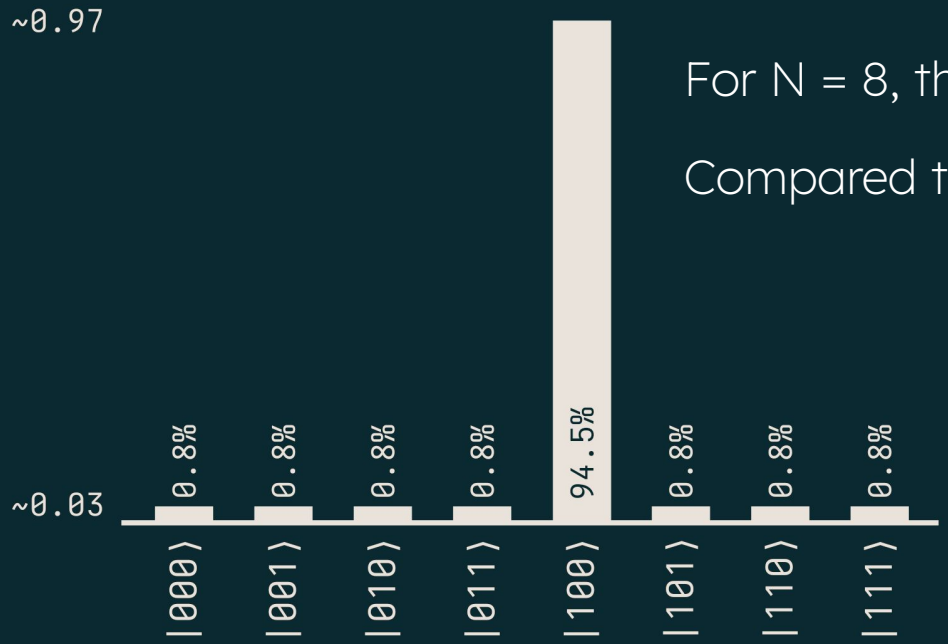
2x mean - old value





Grover’s quantum search algorithm

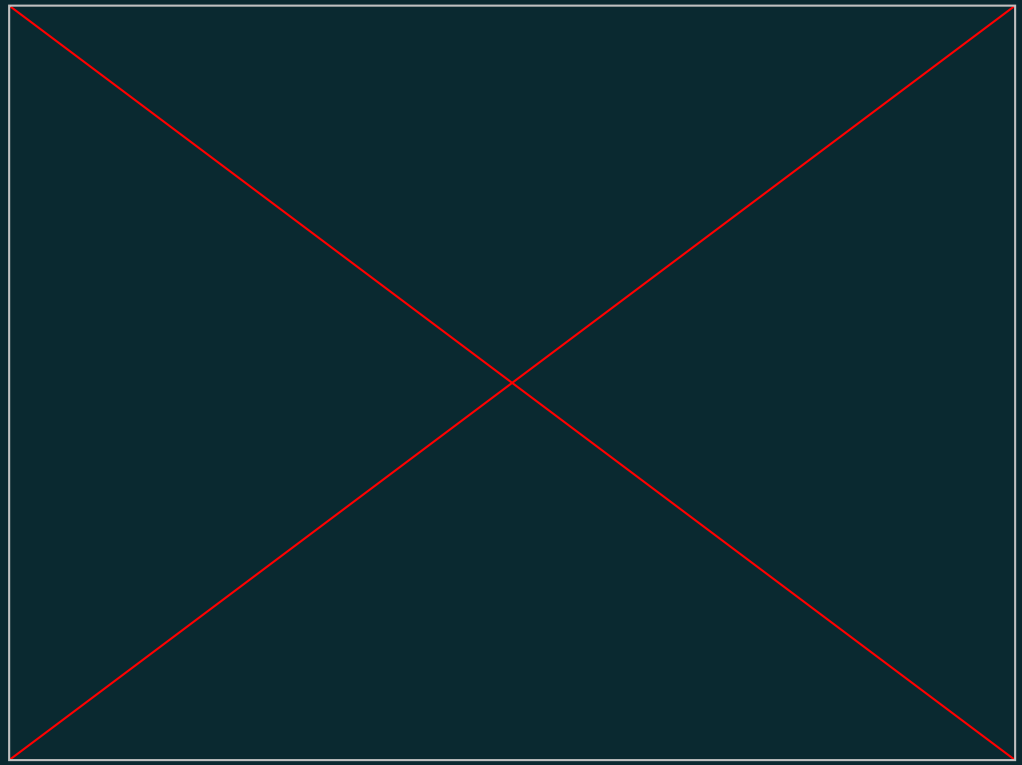
Repeat this process (π/4) x √N times to amplify right answer.



For N = 8, that is ≈ 2 times.

Compared to 8 checks in classical.

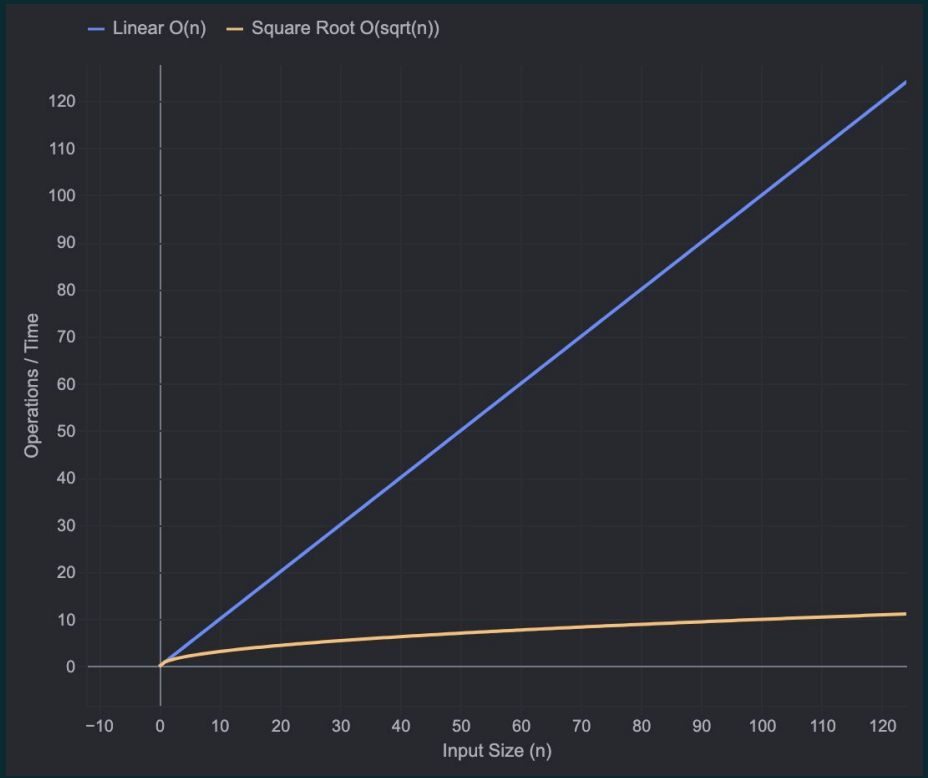
Running Grover’s on IBM’s quantum computer



Error increases as the size of the quantum system grows.

Hardware challenges remain.

What speedup does Grover's algorithm yield?



$2^{128} \rightarrow 2^{64} \approx 1.8 \times 10^{19}$

Cannot be parallelised.

AES 192 and 256 exist.

Where this leaves us

AES is on the whole safe.

Trapdoor functions and Shor’s algorithm.

Quantum resistant trapdoor functions.

Store now, decrypt later.

Quantum Key Exchange

Feedback & Resources

Kindly leave your feedback and contact details

if you are interested in receiving a list of resources

or attending a follow up workshop.

Acknowledgements

Science Gallery Bangalore and Staff

My friends Vagesh & Gautham