COMPUTER & NETWORK SECURITY

Lecture 23:
Quantum Cryptography

Slides originally from Vikram Sharma, QuintessenceLabs

QUANTUM CRYPTOGRAPHY

What is quantum cryptography?

Using quantum computers to do cryptography

What are quantum computers?

Quantum physics applied to computational tasks

What does quantum cryptanalysis mean for classical cryptography?

Is it feasible?

Can we exploit quantum effects to solve our security woes?

WHAT WE ARE NOT DOING

$$H(t)\left|\psi(t)\right\rangle = \mathrm{i}\hbar\frac{d}{dt}\left|\psi(t)\right\rangle$$

$$-\frac{\hbar^2}{2m}\frac{d^2\psi(x)}{dx^2}+U(x)\psi(x)=E\psi(x).$$

$$\mathcal{L}=\frac{i}{2}\overline{\psi}\gamma^\mu\partial_\mu\psi-\frac{i}{2}\left(\partial_\mu\overline{\psi}\right)\gamma^\mu\psi-m\overline{\psi}\psi$$

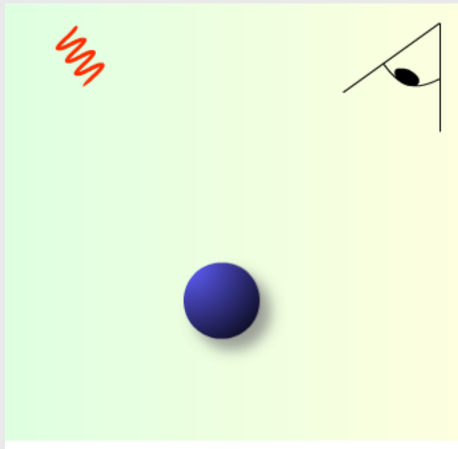
QUANTUM PHYSICS

- Measurements are uncertain
  - Planck Length: 1.6×10^{-35} m
  - Planck Mass: 2.2×10^{-8} kg
  - Planck Time: 5.4×10^{-44} s

- Heisenberg Uncertainty Principle

$$\Delta x \Delta p \geq \frac{h}{4\pi}$$

- It is impossible to make simultaneous precise measurements of a pair of conjugate observables

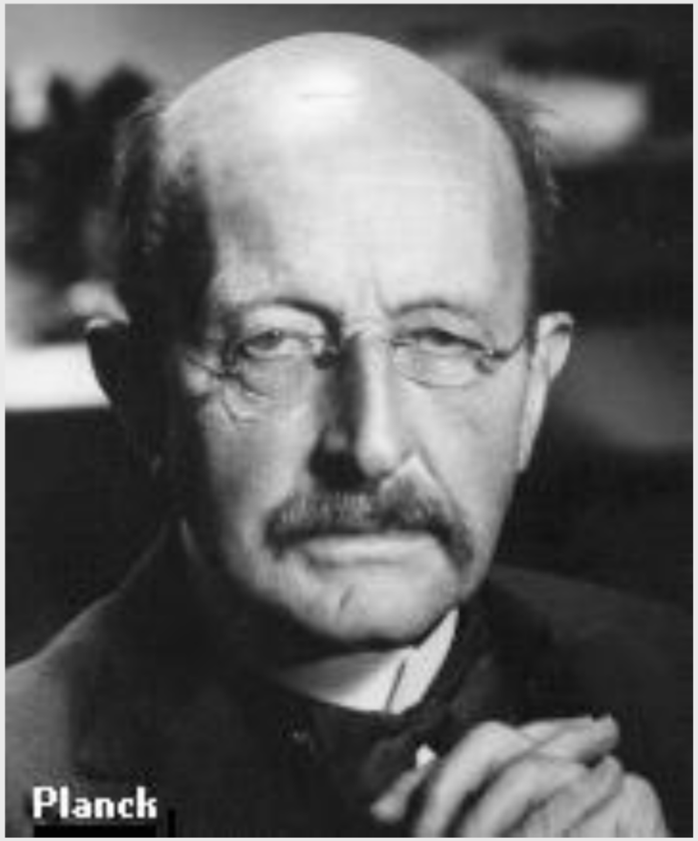


- Accuracy of speed x position is limited to 10^{-34} in SI Unit.
  - $\pm 0.000000000000000000000000000000001 \ m^2/s$

- You cannot know everything about something

QUANTUM PHYSICS

- Stuff is "quantised"
  - Atoms don't behave like little billiard balls
- Atoms emit energy in discrete quanta, called "photons"
- Atoms sometimes interact in unexpected ways
- Atomic properties are often undefined, expressed as a "superposition" of states
  - Atomic spin might be up, down, or *both*
  - Only defined when observed ("decoherence")



QUBITS

Classical bit	qubit
0	0
	?
1	1

HOW WE'VE BEEN DOING CRYPTO

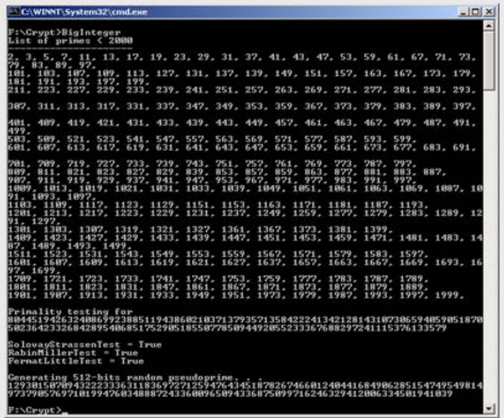
Based on complex mathematics:

- near one-way functions
- easy to compute one-way (encrypt), hard to reverse (decrypt)

$$p, q$$
$$n = pq \qquad \phi(n) = (p-1)(q-1)$$
$$e, \qquad 1 < e < \phi(n) \qquad \gcd\big(e, \phi(n)\big) = 1$$
$$d = e^{-1} \bmod \phi(n)$$

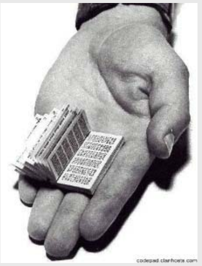
Security reliant on:

- computational intractability
- processing times of best known methods of decryption scale rapidly with the size of key
- difficulty of factoring is at the core of modern methods of encryption

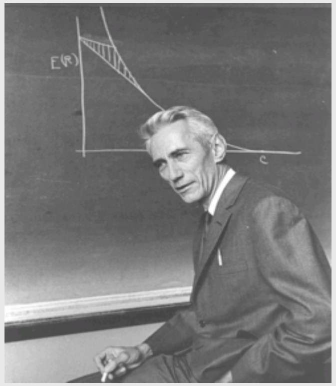


PERFECT SECRECY

- One-Time Pad
  - based on random codes that are only used once
  - *perfect secrecy* proved by Shannon (1949)

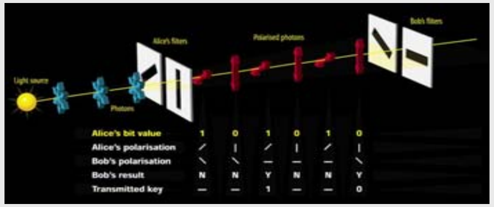


- Problem:
  - code book (one-time pad) needs to be transported from sender to receiver
  - needs to be done securely



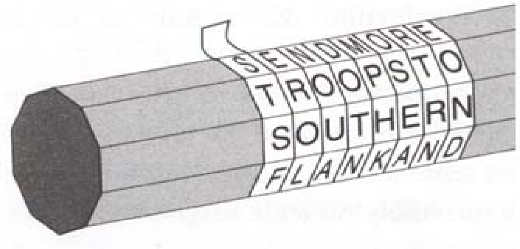
QUANTUM CRYPTOGRAPHY

- Quantum cryptography first conceived by Brassard and Bennett (1984)
    - provides a method to transmit a one-time pad (key) using single photons
    - any eavesdropping (attempt to copy the key) results in detectable variations in quantum states of the photons
    - key can be based on true randomness drawn from nature



- Circa 2000 - proposal to use highly-tuned laser beams instead of single photons
    - ANU QOG amongst one of the first teams in the world to demonstrate a prototype
    - QuintessenceLabs developing this technology for commercial deployment

5TH TO 9TH CENTURY BC



5th Century BC
Spartan scytale (wooden staff).
Transposition cipher.

480 BC
Greece saved from invasion by Persia.
Message hidden under wax on wooden tablets.

Caeser cipher.
Replace each letter with one 3 letters down the alphabet.

abcdefghijklmnopqrstuvwxyz
DEFGHIJKLMNOPQRSTUVWXYZABC

Plaintext: v e n i, v i d i, v i c i
Ciphertext: YHQL, YLGL, YLFL

9th Century
Earliest known description of frequency analysis
Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn 'omran ibn Ismail al-Kindi
("the philosopher of the Arabs")

Letter:	a	b	c	d	e
Percentage:	8.2	1.5	2.8	4.3	12.7

4th Century AD
Kama-sutra art number 45
Mlecchita-vikalpa
Substitution cipher

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

Meet at midnight
⇕
CUUZ VZ CGXSGIBZ

1200 TO 1500 AD

13th Century
First known European book on cryptography.
Epistle on the Secret Works of Art and the Nullity of Magic.
Francis Bacon

14th Century
Cryptography widespread
Geoffrey Chaucer's *Treatise on the Astrolabe* included several encrypted paragraphs.
Substitution using symbols.

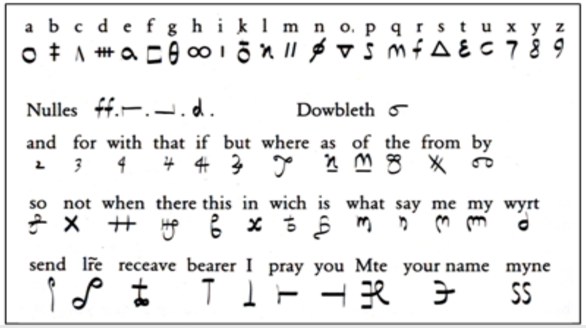
15th Century
European cryptography a burgeoning industry.
Cryptanalysis beginning to emerge in Europe.

1467
Leon Battista Alberti
Cipher machine
Substitution cipher

Plain	abcdefghijklmnopqrstuvwxyz
1	BCDEFGHIJKLMNOPQRSTUVWXYZA
2	CDEFGHIJKLMNOPQRSTUVWXYZAB
3	DEFGHIJKLMNOPQRSTUVWXYZABC
4	EFGHIJKLMNOPQRSTUVWXYZABCD
...	...
26	ABCDEFGHIJKLMNOPQRSTUVWXYZ

1586
A Treatise on Secret Writing
Vigenere cipher
Polyalphabetic cipher

8th February, 1587
Mary, Queen of Scotts beheaded



1600 TO 1800 AD

17th Century
Homophonic cipher

a	b	c	d	e	f	...
09	48	13	01	14	10	...
12	81	41	03	16	31	...
33		62	45	24		...
47			79	44		...
53				46		...
...				...		...

Louis XIII, Louis XIV
The Great Cipher
Not broken until late 19th Century
Multi-syllabic cipher

18th Century
Cryptanalysis becomes industrialised. Geheime Kabinets-Kanzlei in Vienna opened all mail passing through Austria. All monoalphabetic ciphertext messages decrypted.

Cryptographers switch to Vigenere and other polyalphabetic ciphers.

~1854
Charles Babbage breaks Viginere cipher (but not published).

1863
Friedrick Wilhelm Kasiski breaks Viginere cipher.
Secret Writing and the Art of Deciphering

1900 TO 1960 AD

5^{th} March, 1918
German ADFGVX cipher introduced.
Substitution and transposition.

2^{nd} June, 1918
ADFGVX cipher broken by Georges Painvin.

1926
German Enigma machine
Plugboard and scramblers combine to provide over 10,000,000,000,000,000 keys.

Increased to 159,000,000,000,000,000,000 keys in December 1938.

1918
Major Joseph Mauborgne
Concept of a random key leads to the *One Time Pad*, perfect security.
No patterns, no structure. Can be mathematically proven to be absolutely secure.

Problem: impractical to implement in most situations.

Post World War 2
Programmable electronic machines (computers) replace mechanical machines.
Becomes possible to build virtual encryption machines that are extremely complex.
But all still rely on transposition and substitution to create ciphertext.

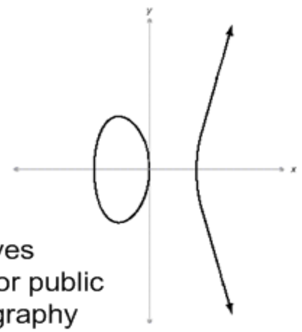
1970 TO 2000 AD

1970s
Lucifer cipher developed at IBM

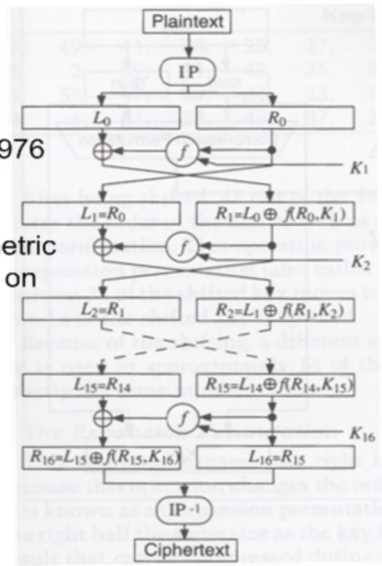
April, 1977
RSA algorithm
Encryption and digital signatures

P & Q PRIME
N = PQ
ED = 1 MOD (P – 1)(Q – 1)
C = M^E MOD N
M = C^D MOD N

1985
Elliptic curves proposed for public key cryptography



23 November, 1976
Data Encryption Standard (DES)
56-bit key symmetric algorithm based on Lucifer



1976
Diffie-Hellman Key Exchange Protocol.
Public key cryptography

1. Alice chooses random x and sends Bob:
$X = g^x$ mod n
2. Bob chooses random y and sends Alice:
$Y = g^y$ mod n
3. Alice computes:
$k = Y^x$ mod n
4. Bob computes:
$k' = X^y$ mod n

$k = k' = g^{xy}$ mod n

26^{th} November, 2001
Advanced Encryption Standard (AES)
128, 192, 256-bit key symmetric algorithm

CLASSICAL ALGORITHMS

- Based on
  - Complex transposition and substitution
  - Hard mathematical algorithms
- Rely on
  - No algorithmic weaknesses
  - Infeasibility of brute force attack
  - Mathematical complexity
- OTP offers provably secure encryption
  - Perfect security

ALICE, BOB & EVE

Eve is omnipresent

- She is always around

“Alice” “Eve” “Bob”

Eve is omniscient

- She knows all the tricks, including those we do not know
- She knows our cryptography algorithm

Eve is omnipotent

- She has perfect interception setups
- She has infinite amount of money
- She has infinite time

Eventually RSA is insecure!!!

1^{ST} INGREDIENT: RANDOMNESS

What is true randomness, what tests are there?

Why is it difficult to get random number from computers

- Because it always relies on fixed algorithm

In Physics, it is dead easy:

- Radioactive decay
- Quantum Decoherence
- Reflection of a photon off a half silvered mirror.

2^{ND} INGREDIENT: IRREVERSIBILITY

There is no known irreversible 1-to-1 mathematical function!

- Many-to-one functions and one-to-many relations cannot work.

Best approximation to irreversible function is factorization.

- It is easier to multiply large numbers, harder to factorize.
- It is easier to differentiate complex functions, harder to integrate.

In Physics, we can rely on concept such as Indistinguishability.

In Physics, we can use Wavefunction Collapse

Reduction of a superposition of eigenstates to a single eigenstate after interaction with an observer

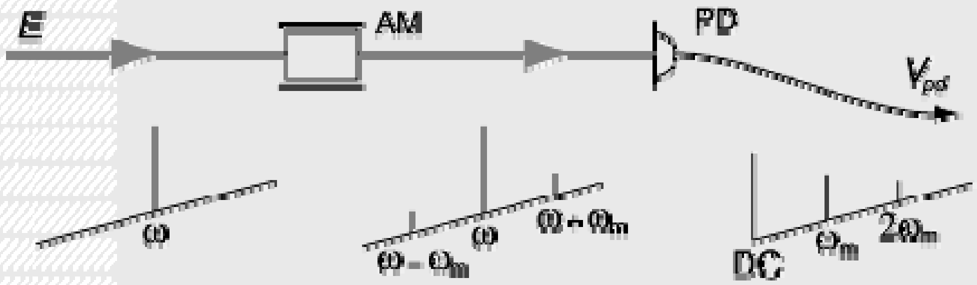
BASIC QUANTUM PHYSICS

1. Heisenberg Uncertainty Principle
2. No cloning theorem
3. Universally pervasive noise - Quantum/Vacuum noise
4. Einstein-Podolsky-Rosen entanglement and Wavefunction Collapse
5. Quieter than vacuum??

QUANTUM LASER BEAM

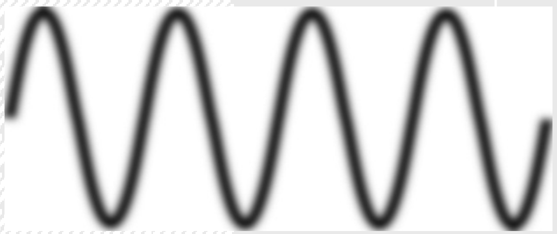
Lasers are ideal for telecommunication.

Information can be encored by varying the amplitude and the phase of a laser: AM and FM encoding.

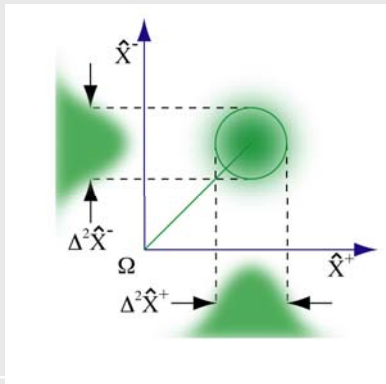


For a laser the amplitude and the phase of a laser beam cannot be simultaneously determined.

•Amplitude

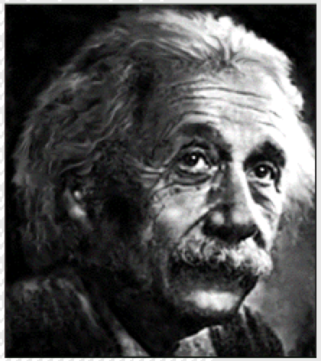
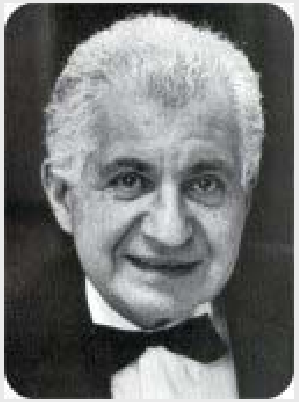
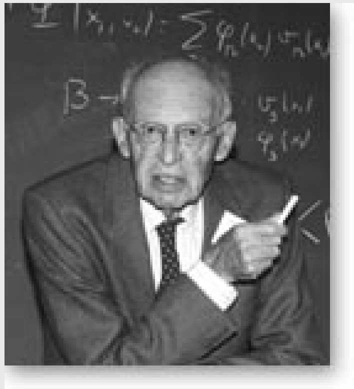


•Phase



Quantum noise can be represented by a Ball and stick diagram

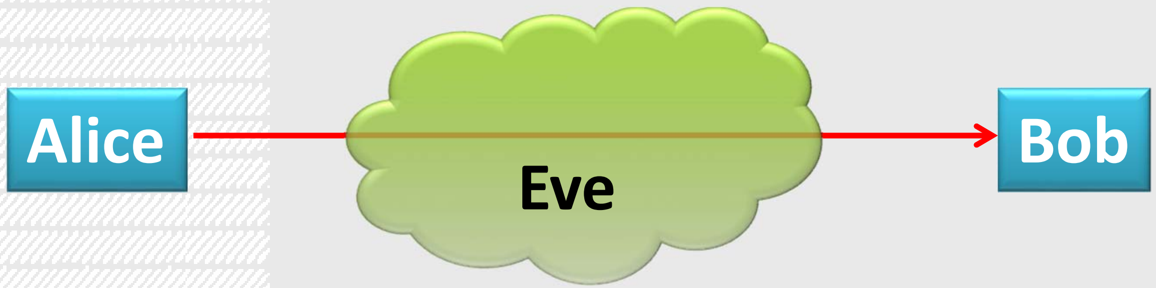
EPR ENTANGLEMENT AND WAVEFUNCTION COLLAPSE

- Entanglement means that the left hand knows what the right hand is doing, even when the hands are very far apart

- Wavefunction collapse is our 2nd ingredient
  - "a one time lock/key".

QKD
THEORY



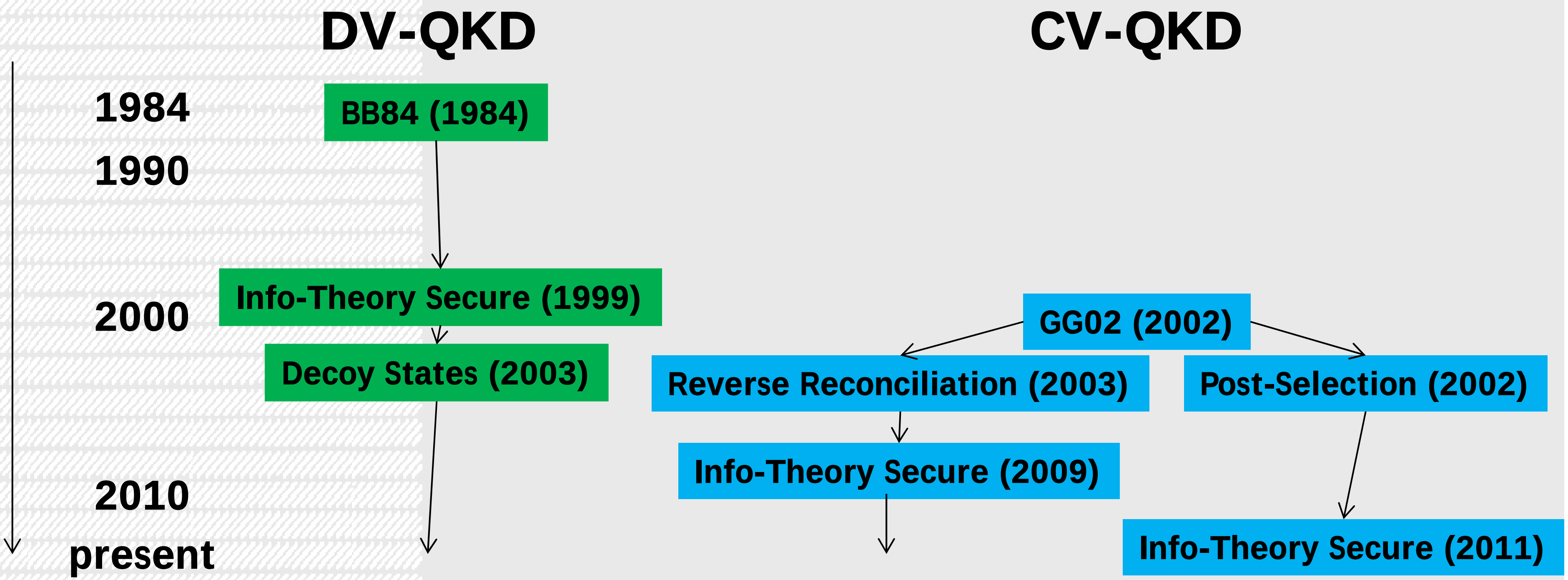
- Secure information

$$\Delta I = I_{AB} - I_E$$

where I_{AB} is the amount of shared information Alice and Bob can agree on and I_E is the maximum amount of information accessible to a third party with total control over the transmission channel

- A QKD device must:
  - Estimate the channel parameters to bound I_E
  - Reconcile efficiently the information shared between Alice and Bob
  - Extract the secure information

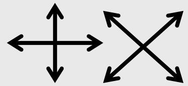
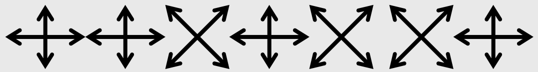
TWO TYPES OF QKD



	DV-QKD	CV-QKD
Sources	Single photons/ Attenuated coherent lasers	Weakly modulated bright coherent laser
Detectors	Single-photon detectors	Homodyne detectors

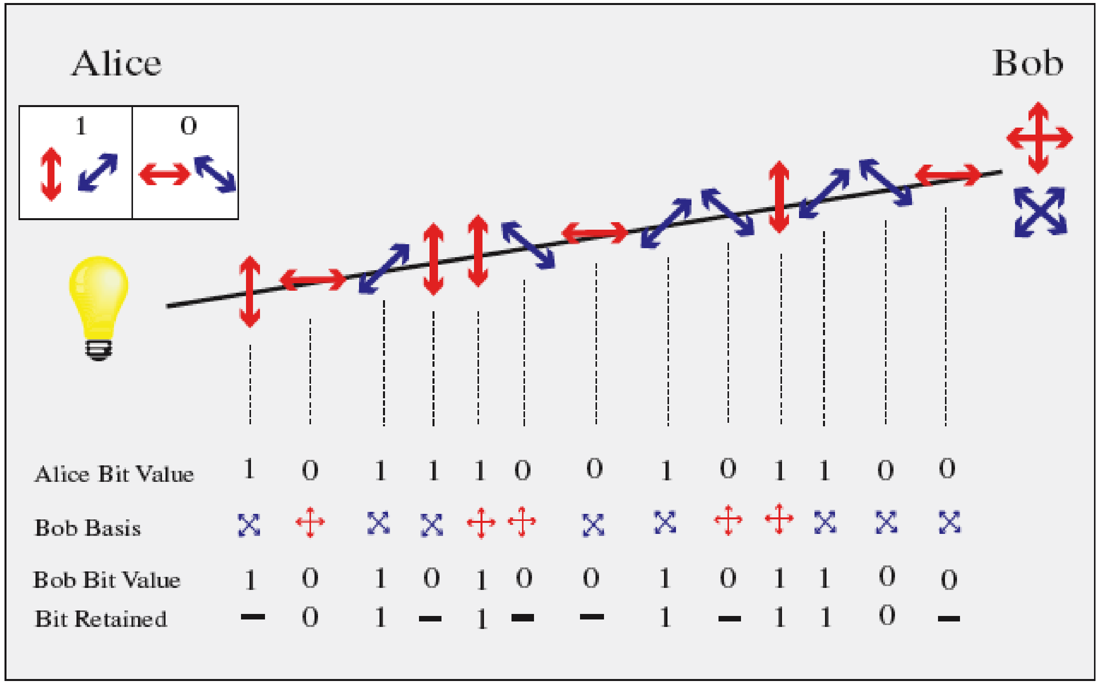
http://www.quintessencelabs.com/wp-content/uploads/2014/11/QL-White-Paper-QKD-Systems-Compared.pdf

BB84: BENNETT & BRASSARD (1984)

- Quantum key exchange with polarised photons
- Two basis pairs of two states (rectilinear and diagonal) 
- Alice generates random bit string, and random basis sequence
  - e.g. 0110101 and 
- Alice sends a photon per bit, polarised with the chosen basis
- Bob randomly picks a basis for each bit
- Alice and Bob compare notes later, only about chosen basis
- Any interception by Eve destroys initial photon state
- Immune to MITM if Alice and Bob can verify each other’s identity

BB84: BENNETT & BRASSARD (1984)

Bennett and Brassard proposed in 1984 that if single photons are sent from Alice to Bob, communication between them can be absolutely secure.

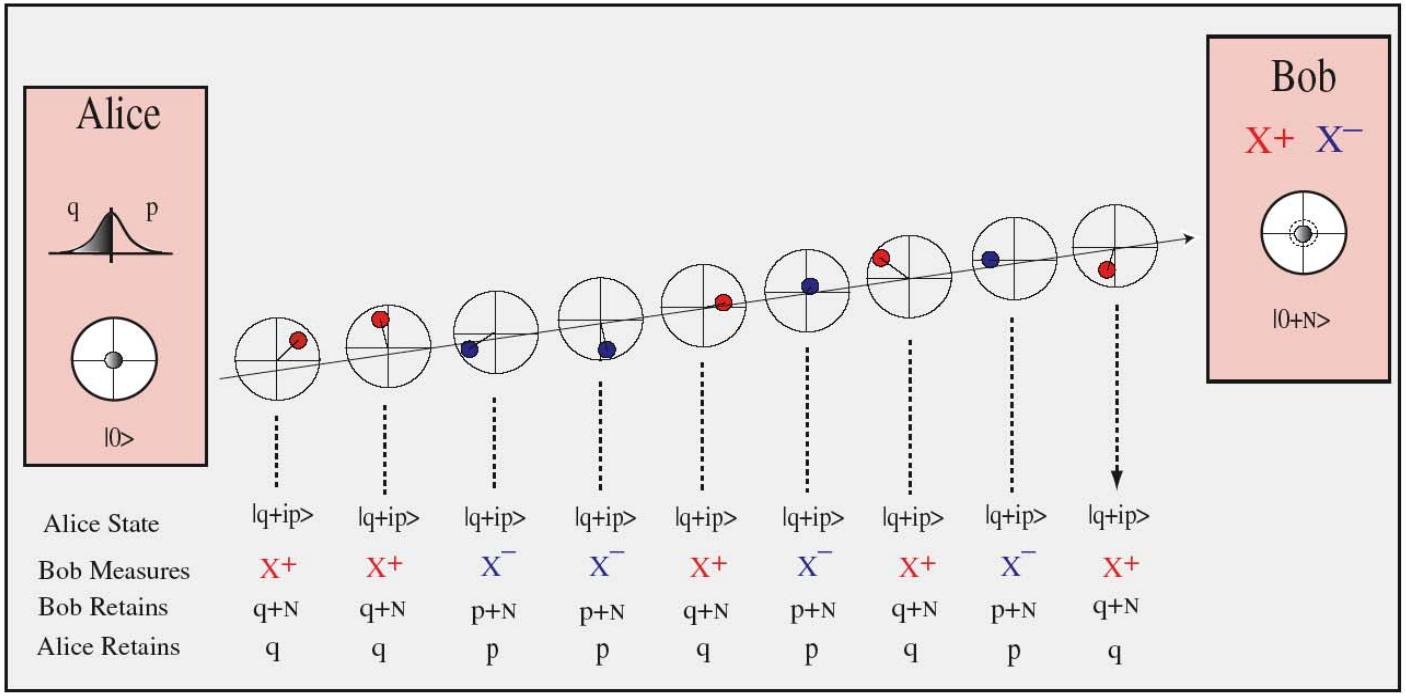


PRACTICALITY OF BB84

- **Implementations are getting better**
  - 1989: 32 cm
  - Now ~200km
  - 144km Free Space
- **Still very slow and difficult, and doesn't solve everything**
  - authentication
  - non-repudiation (digital signatures)
  - and more ...
- **Moral: there are no "silver bullets" for security problems**

BRIGHT LASER BEAM CRYPTOGRAPHY

- Several proposals surfaced after 2000 suggested that whole laser beams can be used for quantum cryptographic communication 1989

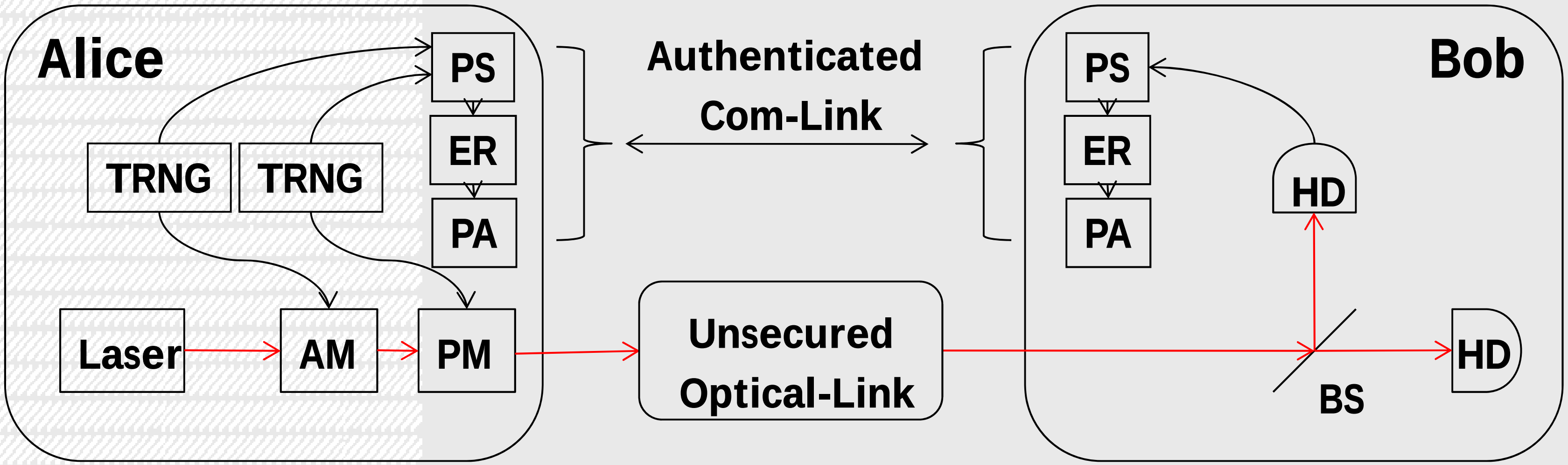


CV-QKD: ADVANTAGES

- Higher detectors efficiencies
- Off-the-shelf components
- Telecommunications compatible
- Higher key rates achievable:

	Optical Device	Bandwidth
Laser	Shot-noise-limited laser	Essentially unlimited*
Modulators	Amplitude and phase modulators	Available: >40 GHz
Detectors	Shot-noise-limited homodyne detectors	Available: 10 GHz

CV-QKD: IMPLEMENTATION



Optics Layout

Coherent Laser

True Random Number Generator (TRNG)

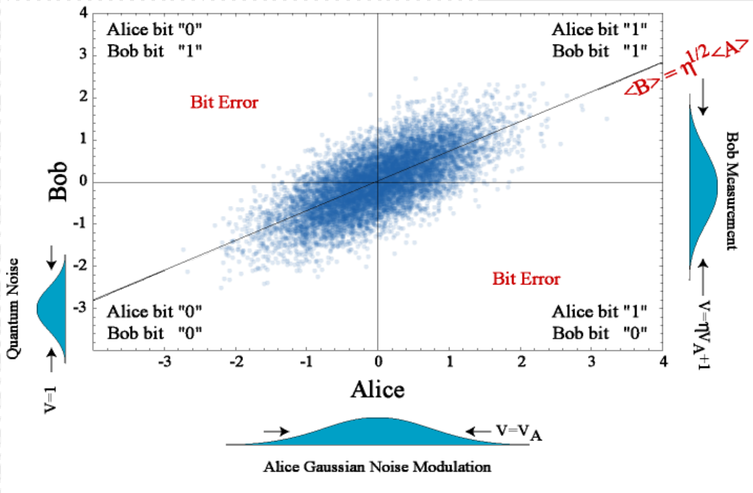
Amplitude (AM) and Phase (PM) Modulators

Beam-splitter (BS)

Homodyne Detectors (HD)

- **Post-processing**
  - **Post-Selection (PS)**
  - **Error Reconciliation (ER)**
  - **Privacy Amplification (PA)**

MATHEMATICAL TRICKS



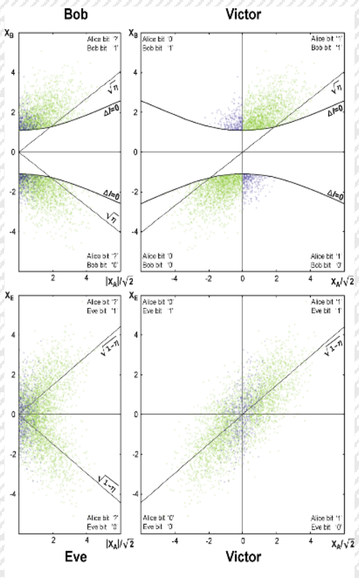
Vacuum noise

Wave function collapse

Post-selection

Cascade reconciliation

Privacy amplification



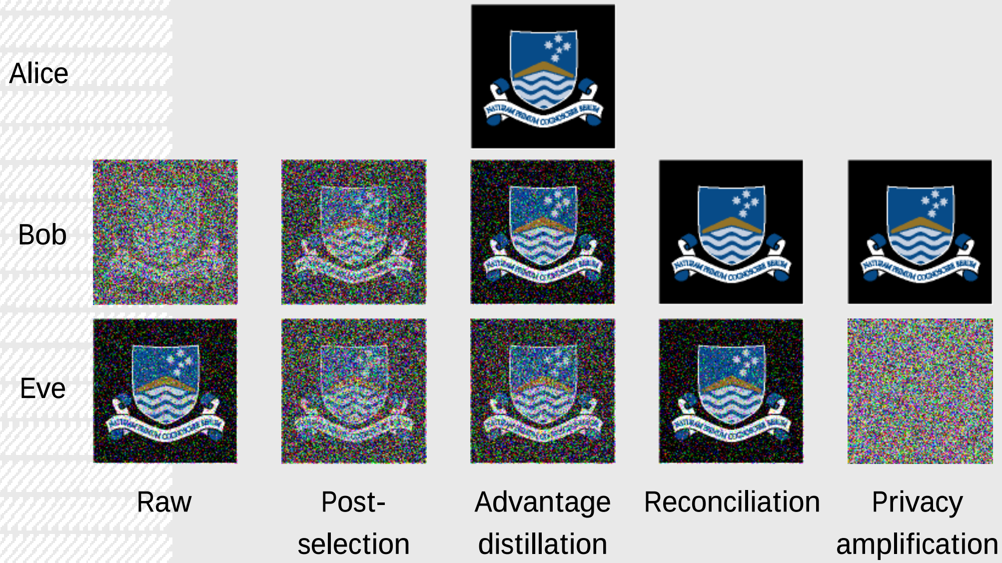
$$\left[(1/0)x^{110503}+(1/0)x^{110502}+\ldots+(1/0)x+(1/0)\right]\times\left[r_{11503}x^{110503}+\ldots+r_0\right]$$

$$\mathrm{mod}\left[x^{110503}+x^{5011}+1\right]$$

$$\left[f_{110503}x^{110503}+f_{110502}x^{110502}+\ldots+f_1x+f_0\right]$$

QUANTUM NOISE ON LASER BEAMS

“It can be squarely asserted that quantum physics can offer a way to generate a cipher key which is absolutely unbreakable”



QUBIT REGISTERS

Classical bit registers		qubits registers (entangled qubits)
000	100	
001	101	???
010	110	
011	111	

QUBIT COMPUTATION
F(X) = 2*X (MOD 8)

Classical bits			qubits
000	001	101	???
$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$
000	010	010	??0

QUBIT COMPUTATION (FACTORING Y) F(X) = Y MOD X

Classical bits (y=15=1111)				qubits
010	011	100	…	???
$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$
001	000	011	…	000

SHOR'S ALGORITHM

Peter Shor, AT&T (1994)

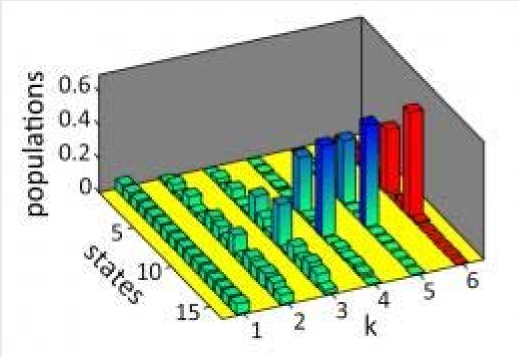
Factors in $O((\log N)^3)$

Efficient factoring of n-bit integers with 2n-qubit registers

The efficiency of Shor's algorithm is due to the efficiency of the quantum Fourier transform, and modular exponentiation by repeated squarings.

Chinese researchers implemented the largest so far

Factored 143 into 11 * 13



QUANTUM COMPUTER COMPLEXITY

BQP (Bounded-error, Quantum, Polynomial time)

“the class of decision problems solvable by a quantum computer in polynomial time, with an error probability of at most 1/3 for all instances” – equivalent of BPP

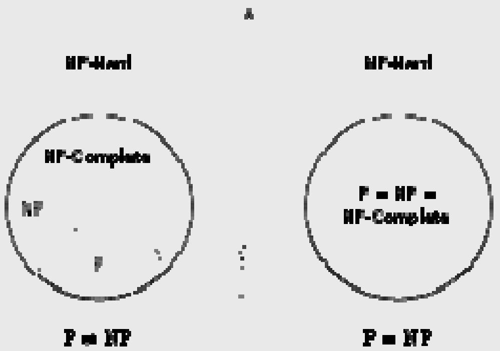
P $\subseteq$ BQP

NP-complete ? BQP (probably disjoint)

Primality testing $\in$ P [Agrawal et al, 2004]

Integer factorisation $\in$ BQP [Shor, 1994]

P vs NP: Informally, it asks whether every problem whose solution can be quickly verified by a computer can also be quickly solved by a computer



IMPLICATIONS

- Anything relying on integer factorisation or the discrete logarithm problem can’t resist quantum cryptanalysis
  - RSA, DSA, Diffie-Hellman, El Gamal, ECC
- One-Time Pad is still fine – why?
- Quantum cryptography offers the possibility of perfect secrecy that cannot be compromised by advances in computational or mathematical capabilities

REFERENCES

Quantiki

www.quantiki.org