INTRODUCTION TO QUANTUM COMPUTATION

What is quantum computation?

- New model of computing based on quantum mechanics.
- More powerful than conventional models.
- Yield new ideas for future computing devices and cryptography

In the beginning…

- Paul Benioff (1980):
  Emulates a TM by quantum devices (sketchy & cryptic)
- Richard Feynmann (1981): *Can a computer simulate physics?* (No)
- Richard Feynmann (1983) *Quantum mechanical computer*

Bibliography

- Nielsen and Chuang: *Quantum Computation and Quantum Information*. Cambridge Univ. Press, 2002.
- C. Williams and S. Clearwater: *Ultimate Zero and One. Computing at the Quantum Frontier*. Copernicus, 2000.

Quantum bit

Consider the 2 dimensional vector space on the complex C^2, with orthonormal basis $|0\rangle=(1,0)^T$ and $|1\rangle=(0,1)^T$.

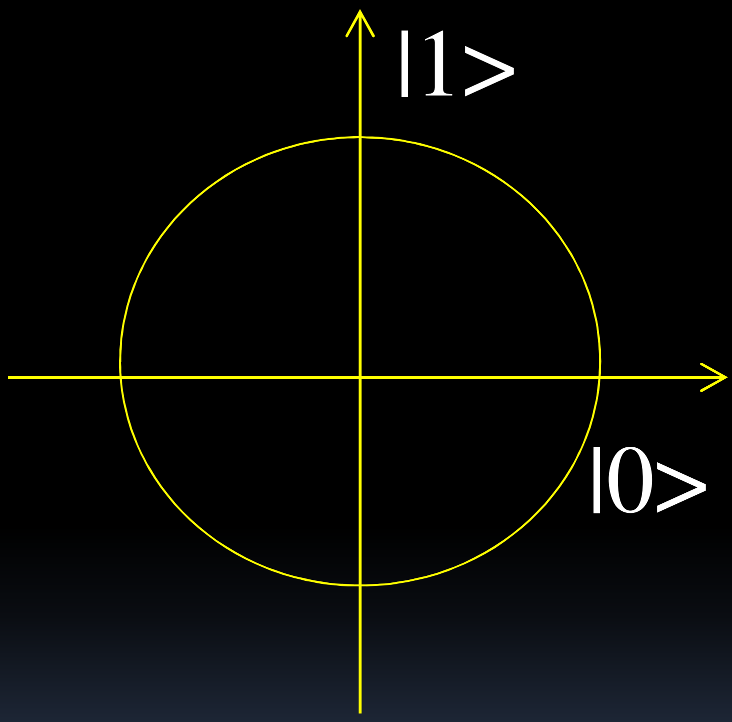
For any $v=(a,b)$, $w=(c,d)$, define the inner product $\langle w|v\rangle=w^*.v^T=a^*c+b^*d$, where a^* and b^* denote the complex conjugate of a and b

Quantum bit

If for any v in the vector space C^2, we define a norm $||v||$, as the square root of $\langle v|v\rangle$, we have a Hilbert space, let denote it H^2.

Any vector $|\psi\rangle$ in H^2 is the state of a quantum bit or qubit

Quantum bit



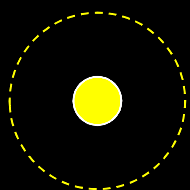
- 2-dimensional vector of length 1.
- Basis states |0>, |1>.
- Arbitrary state:
  $\alpha|0\rangle+\beta|1\rangle$,
- α, β complex
  $|\alpha|^2+|\beta|^2=1$.

Physical quantum bits

- Nuclear spin = orientation of atom's nucleus in magnetic field.
  $\uparrow$ = |0>, $\downarrow$ = |1>.
- Photons in a cavity.
- No photon = |0>, one photon = |1>

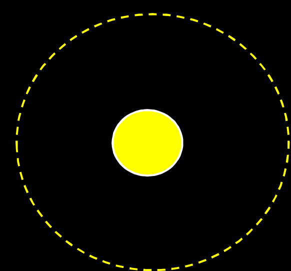
Physical quantum bits

- Energy states of an atom



$|0\rangle$

ground state



$|1\rangle$

excited state

- Polarization of photon

4-dimensional quantum states

- H^4 the 4-dimensional quantum system can be constructed as the tensor product of H^2 x H^2
- Basis |00>, |01>, |10>, |11>, where |00>=|0>x|0>; |01>=|0>|1>; |10>=|1>|0>; |11>=|1>|1>.
- The basis can also be represented by: |0>, |1>, |2>, |3>
- General state

$$\alpha_0|0\rangle+\alpha_1|1\rangle+\alpha_2|2\rangle+\alpha_3|3\rangle,$$

$$\text{with } |\alpha_0|^2+\ldots+|\alpha_3|^2=1$$

General quantum states

- k-dimensional quantum system (as product of two k/2 dimensional quantum systems)
- Basis |0>, |1>, …, |k-1>
- General state

$$\alpha_0|0\rangle+\alpha_1|1\rangle+\ldots+\alpha_{k-1}|k-1\rangle,$$

$$|\alpha_0|^2+\ldots+|\alpha_{k-1}|^2=1$$

- 2^k dimensional system can be constructed as a tensor product of k quantum bits.

Unitary transformations

- Linear transformations that preserve vector norm.
- In 2 dimensions, linear transformations that preserve unit circle (rotations and reflections).

Examples

- Bit flip X: $|0\rangle \rightarrow |1\rangle$

  $|1\rangle \rightarrow |0\rangle$

- Shift Z: $|0\rangle \rightarrow |0\rangle$

  $|1\rangle \rightarrow -|1\rangle$

Examples

- Hamamard-Walsh transform W:

$$\begin{cases} \qquad\qquad \sqrt{2} \qquad\qquad \sqrt{2} \\ |1> \rightarrow \dfrac{1}{\sqrt{2}}|0> - \dfrac{1}{\sqrt{2}}|1> \end{cases}$$

Examples

- Not-controlled C_{10}:

$C_{10}|ab>=|b\ a+b>$ if $b=0$,

$C_{10}|ab>=|ab>$ if $b=1$

i.e. $C_{10}|00>=|00>$ $C_{10}|01>=|01>$

$C_{10}|10>=|11>$ $C_{10}|11>=|10>$

Linearity

- Bit flip

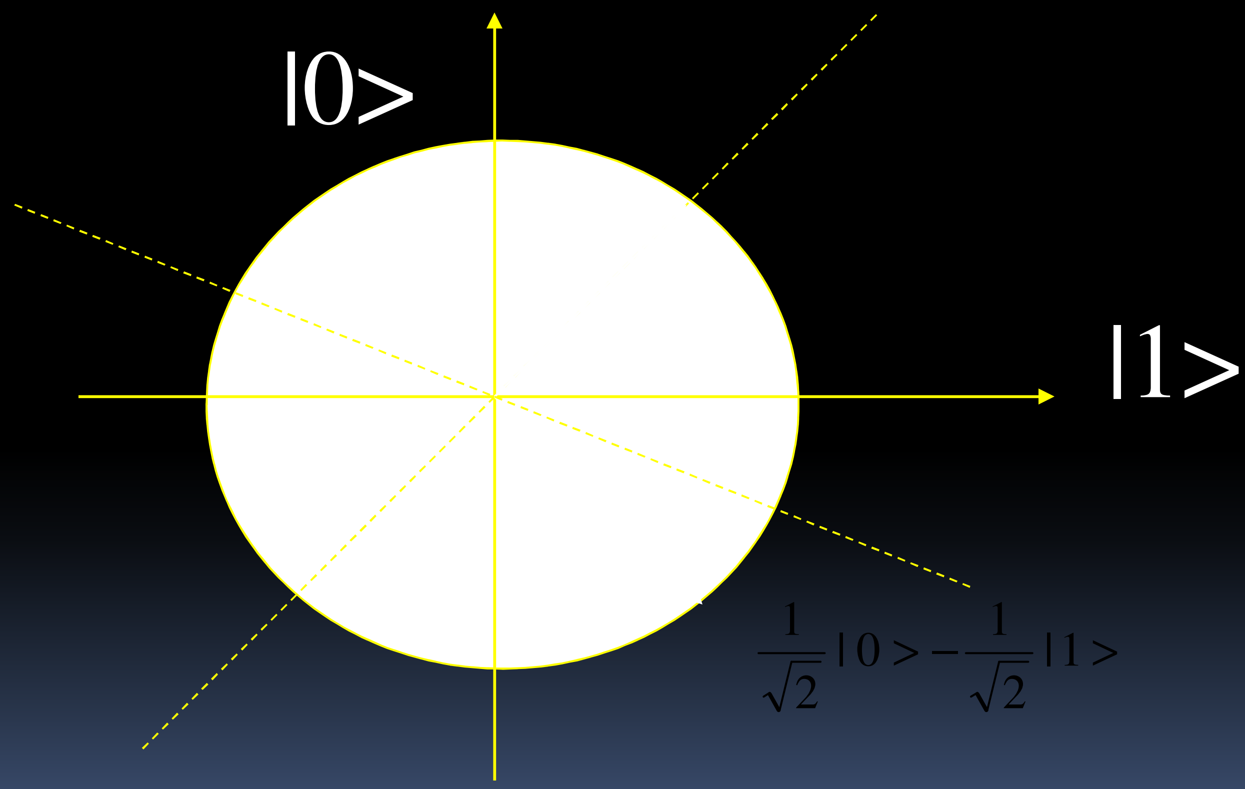
$$X|0\rangle \rightarrow |1\rangle$$
$$X|1\rangle \rightarrow |0\rangle$$

⌘By linearity,

$$\alpha|0\rangle+\beta|1\rangle \rightarrow \alpha|1\rangle+\beta|0\rangle$$

⌘Sufficient to specify $X|0\rangle$, $X|1\rangle$.

Examples



Interference: Constructive-Destructive

Example: W(W|o>)= |o>

Interference: Constructive-Destructive

Example: W(W|o>)= |o>

|o>

Interference: Constructive-Destructive

Example: W(W|0>)= |0>

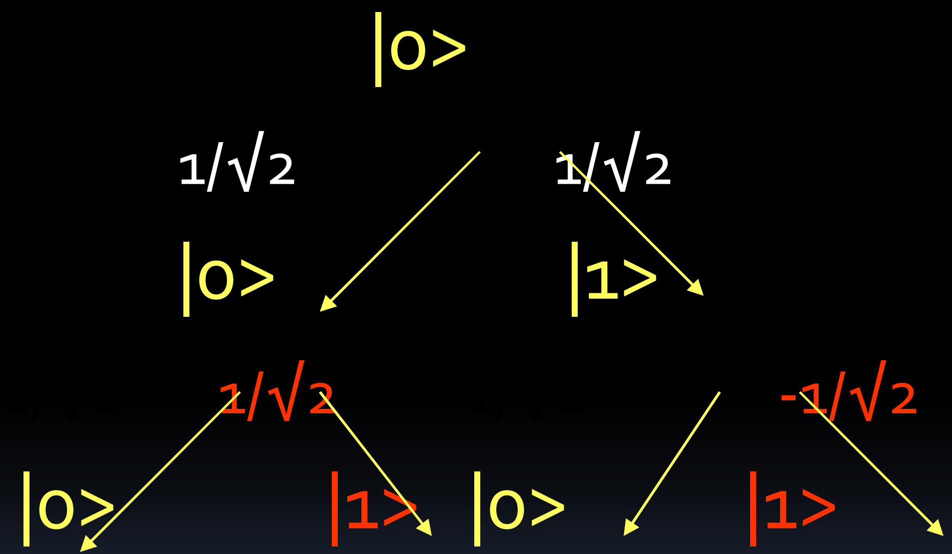
|0>

1/√2 1/√2

|0> |1>

Interference: Constructive-Destructive

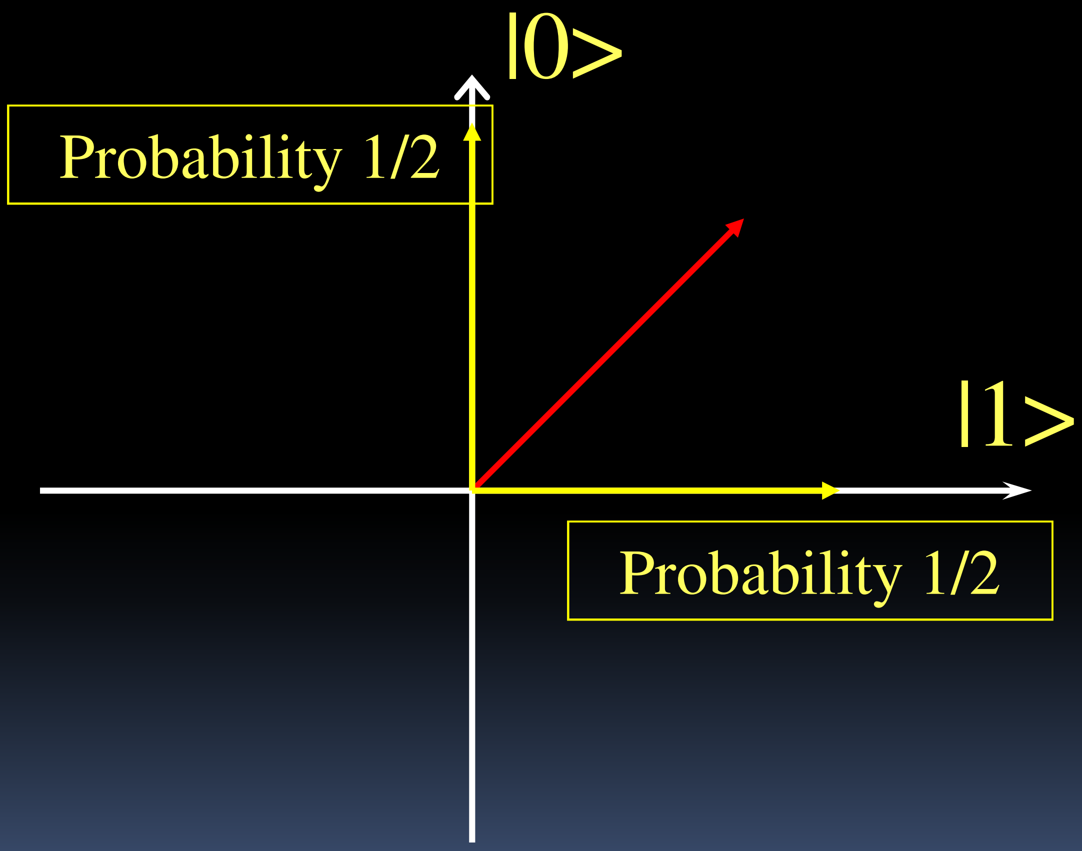
Example: W(W|0>)= |0>



Measurements

- Measuring $\alpha|0\rangle+\beta|1\rangle$ in basis $|0\rangle$, $|1\rangle$ gives:
  0 with probability $|\alpha|^2$,
  1 with probability $|\beta|^2$.
- Measurement changes the state: it becomes $|0\rangle$ or $|1\rangle$.
- Repeating measurement gives the same outcome.

Measurements



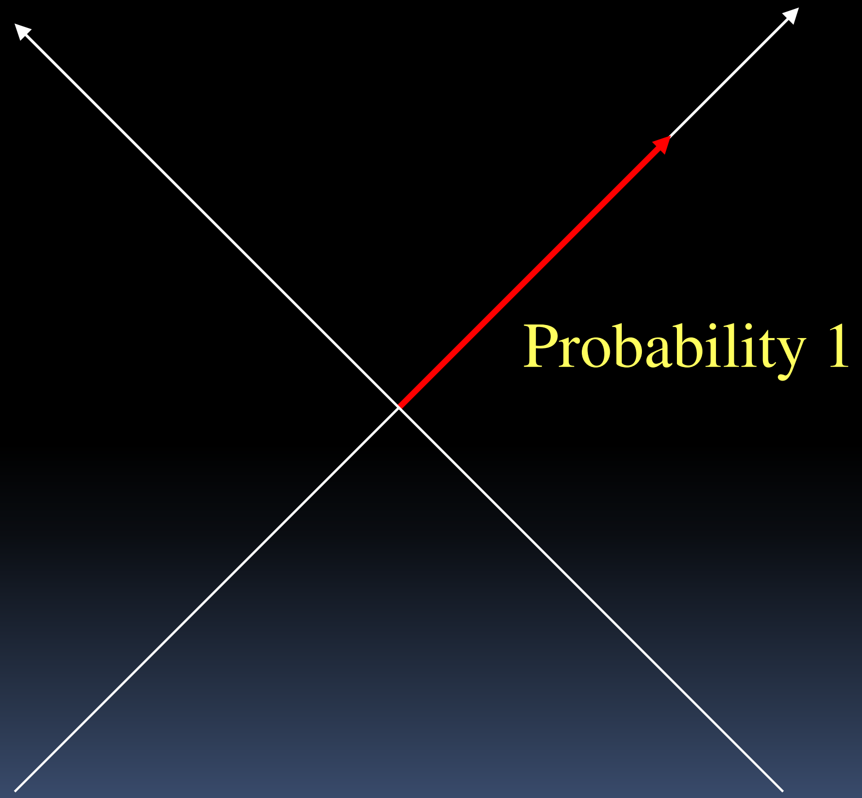
General measurements

- Let $|\psi_0>$, $|\psi_1>$ be two orthogonal one-qubit states.
- Then,

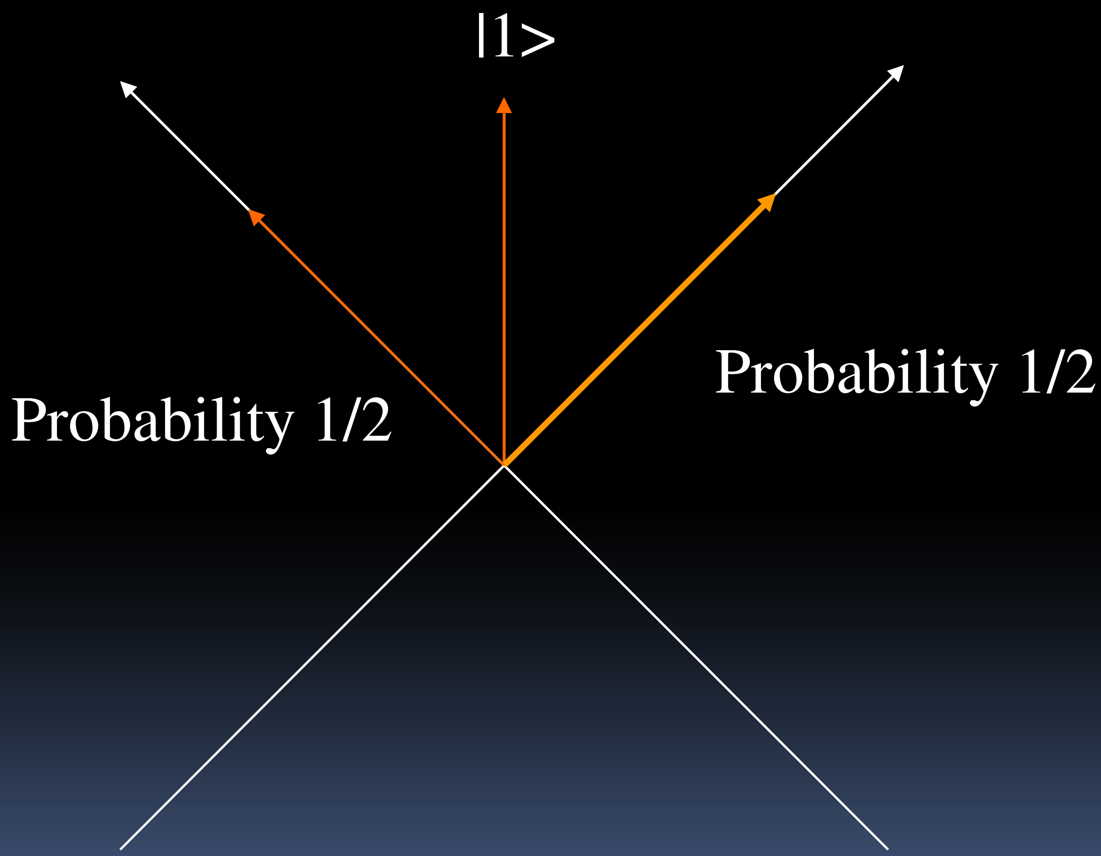
$$|\psi> = \alpha_0|\psi_0> + \alpha_1|\psi_1>.$$

- Measuring $|\psi>$ gives $|\psi_i>$ with probability $|\alpha_i|^2$.
- This is equivalent to mapping $|\psi_0>$, $|\psi_1>$ to $|0>$, $|1>$ and then measuring.

Measurements



Measurements



Measurements

- Measuring

$$\alpha_1|1\rangle+\alpha_2|2\rangle+\ldots+\alpha_k|k\rangle$$

  in the basis $|1\rangle$, $|2\rangle$, ..., $|k\rangle$ gives $|i\rangle$ with probability $|\alpha_i|^2$.
- Any orthogonal basis can be used.

Partial measurements

If in H^4, we have a system in state

$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$,

if we measure the first qubit

- it will yield $|0\rangle$ with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$
- and it will yield $|1\rangle$ with probability $|\alpha_{10}|^2 + |\alpha_{11}|^2$.

Partial measurements: example

Measure the first bit:

1/4+1/4=1/2

1/2

$$\frac{1}{\sqrt{2}}|00>+\frac{1}{\sqrt{2}}|01>$$

$$|10>$$

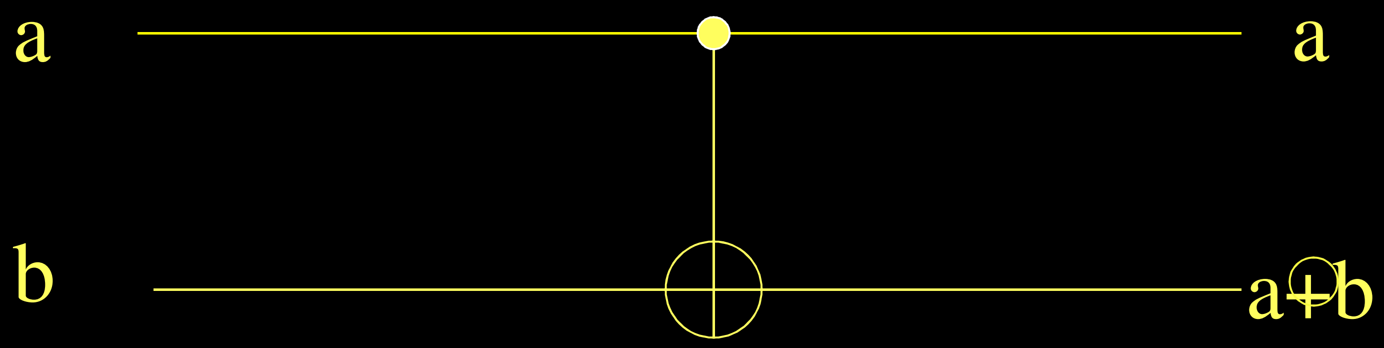
EPR (or Bell) state

- Important state in quantum computing

  $|\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$

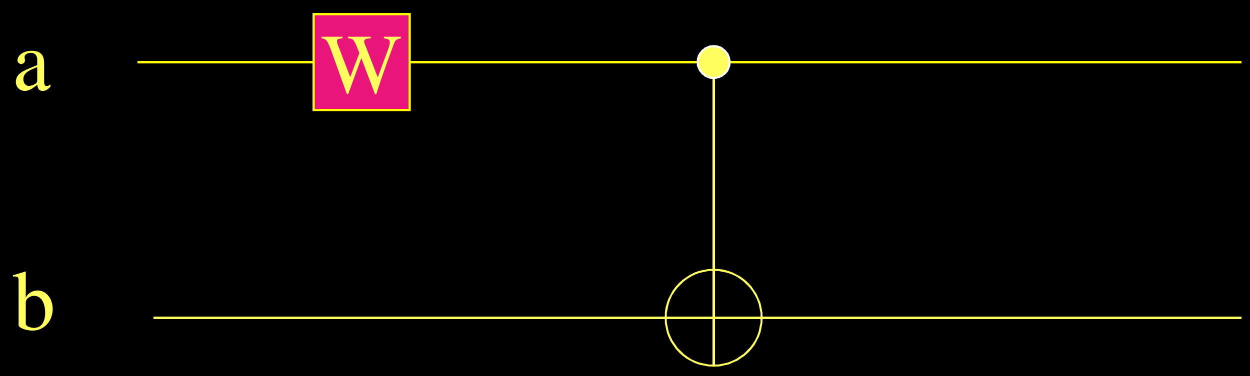
  Important property: if we measure a system in state $|\phi^+\rangle$ then with probability 1/2 will be in state $|00\rangle$ and with probability 1/2 will be in state $|11\rangle$

Quantum gates: C_{10}



Quantum gates are always reversible

Quantum circuits



Input: |ab>

Output: $1/\sqrt{2}(|0b\rangle+(-1)^{b}|1\neg b\rangle)$

EPR-States

The previous circuit gives all EPR-states:

- On |00> gives $|\phi^{+}\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$
- On |10> gives $|\phi^{-}\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$
- On |01> gives $|\varphi^{+}\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$
- On |11> gives $|\varphi^{-}\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$

Classical vs. Quantum

Classical bits:

- can be measured completely,
- are not changed by measurement,
- can be copied,
- can be erased.

Quantum bits:

- can be measured partially,
- are changed by measurement,
- cannot be copied,
- cannot be erased.

No-cloning theorem

- It does not exist any quantum gate U:$H^2 \otimes H^2$ such that for any state general state |ψ> and any chosen |s>: U(|ψs>)=| ψ ψ >.
- (Proof) If so, ∃U s.t. U(|ψs>)=|ψψ>.

Choose a |ψ' > :

$$U(|\psi\rangle \times |s\rangle)=|\psi\rangle \times |\psi\rangle$$

$$U(|\psi'\rangle \times |s\rangle)=|\psi'\rangle \times |\psi'\rangle$$

Taking the dot product of previous system

$<\psi|\psi'> = (<\psi|\psi'>)^2$.

Which only has solution if $|\psi> = |\psi'>$

or $|\psi>$ and $|\psi>$ are orthogonal.

Teleportation

- A and B generate one pair EPR $|\phi^{+}\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, A keeps the first qubit
-

Teleportation

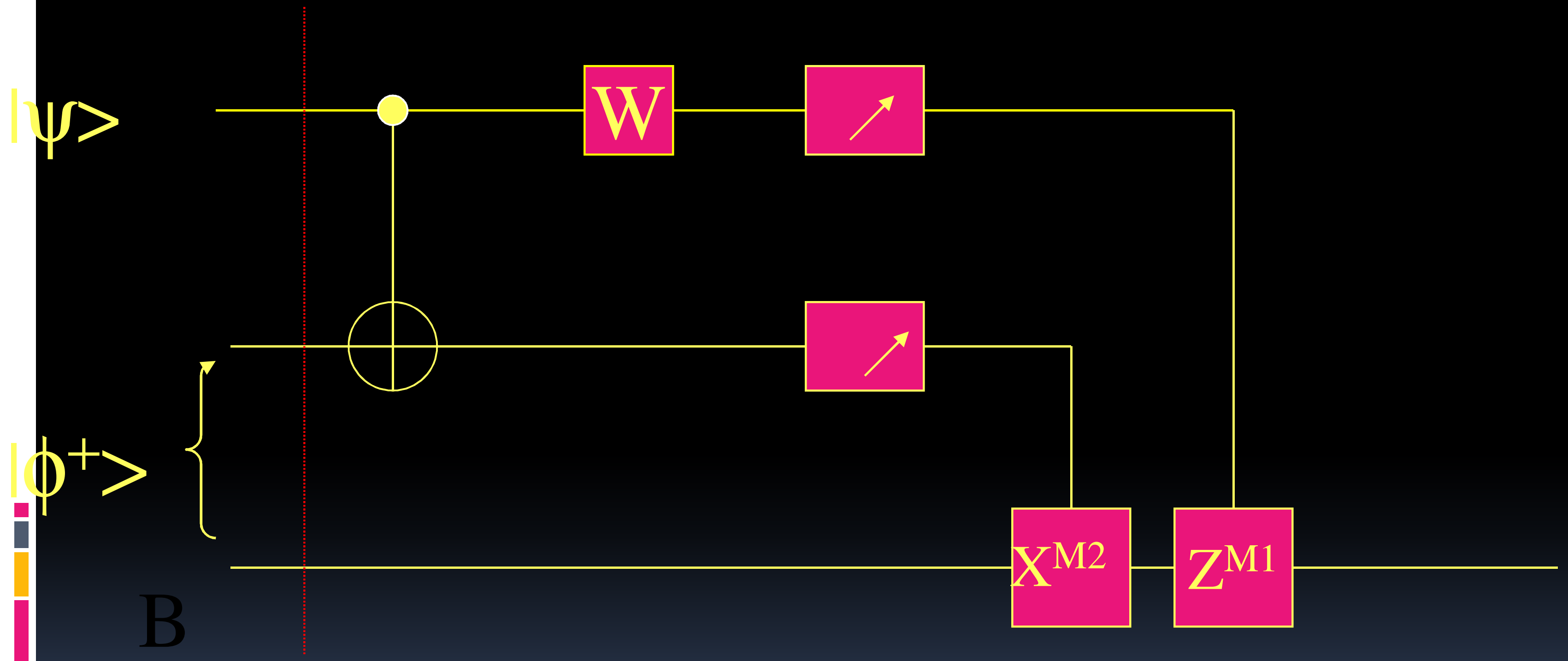
- A and B generate one pair EPR $|\phi^{+}\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, A keeps the first qubit and B keeps the second one
-

Teleportation

- A and B generate one pair EPR $|\phi^{+}\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$, A keeps the first qubit and B keeps the second one
- Later A wishes to send B the state $|\psi\rangle = \alpha_0|\psi_0\rangle + \alpha_1|\psi_1\rangle$.

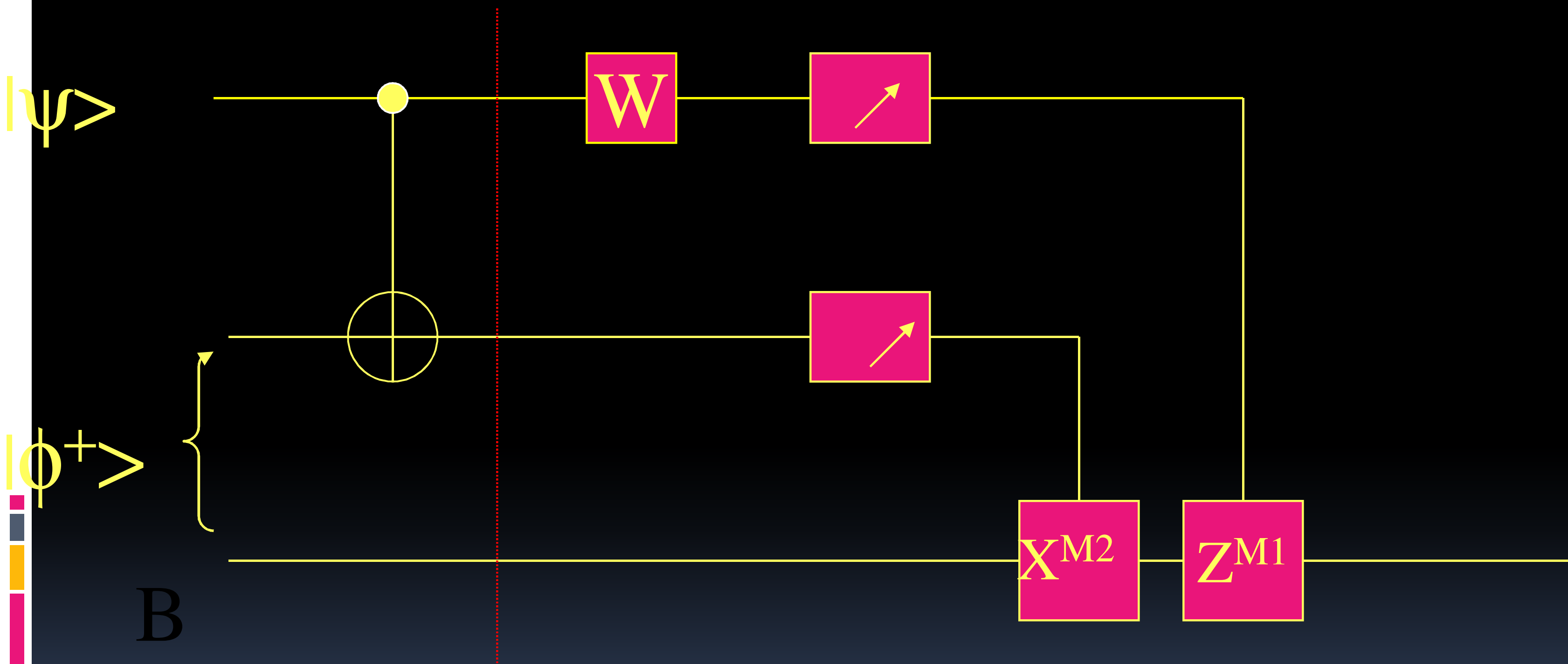
information to B.

Teleportation circuit-1



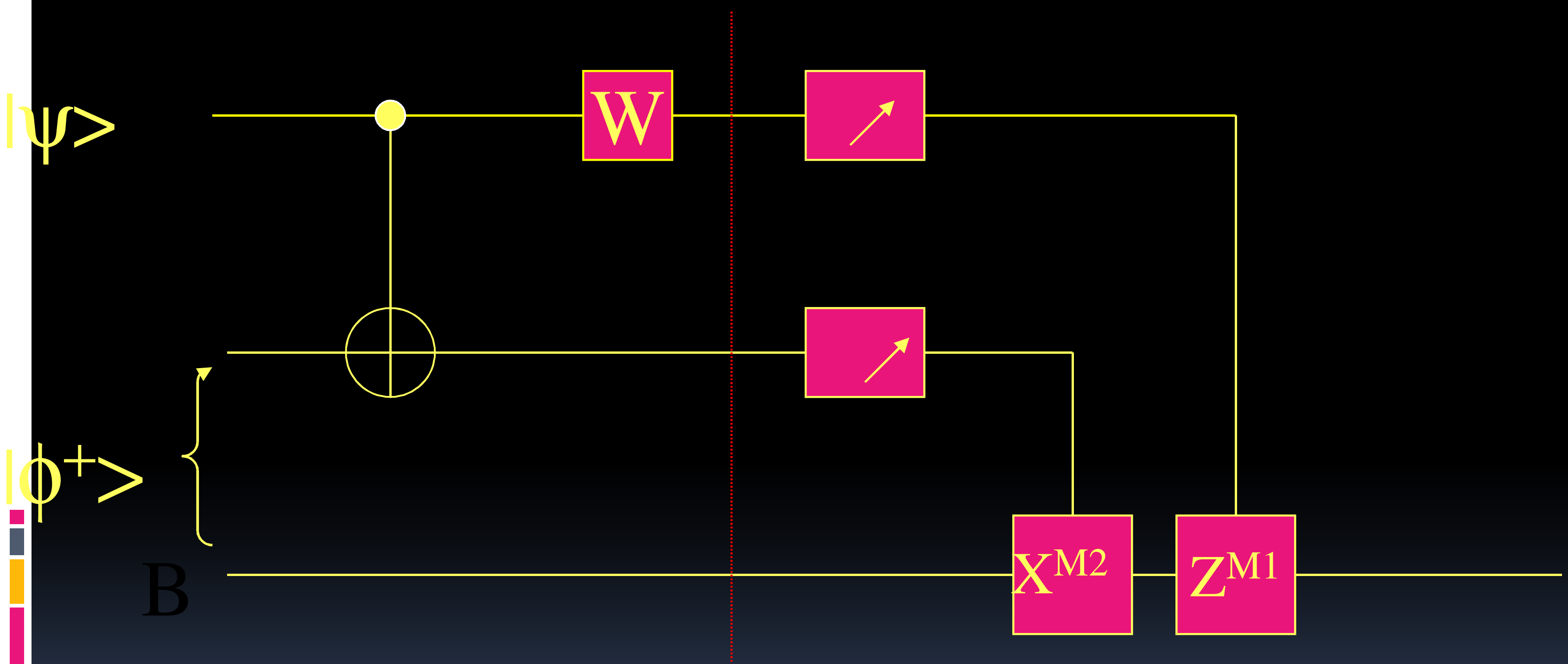
$|\psi_0\rangle = |\psi\phi^+\rangle = 1/\sqrt{2}(\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle))$

Teleportation circuit-2



$$|\psi_1>=1/\sqrt{2}(\alpha|0>(|0>+|1>)+\ \beta|1>(|0>+|1>))$$

Teleportation circuit-3



$|\psi_2\rangle = 1/2[\alpha(|0\rangle + |1\rangle)\ (|00\rangle + |11\rangle) + \beta\ (|0\rangle - |1\rangle)\ (|10\rangle + |01\rangle)]$

Re-arranging:

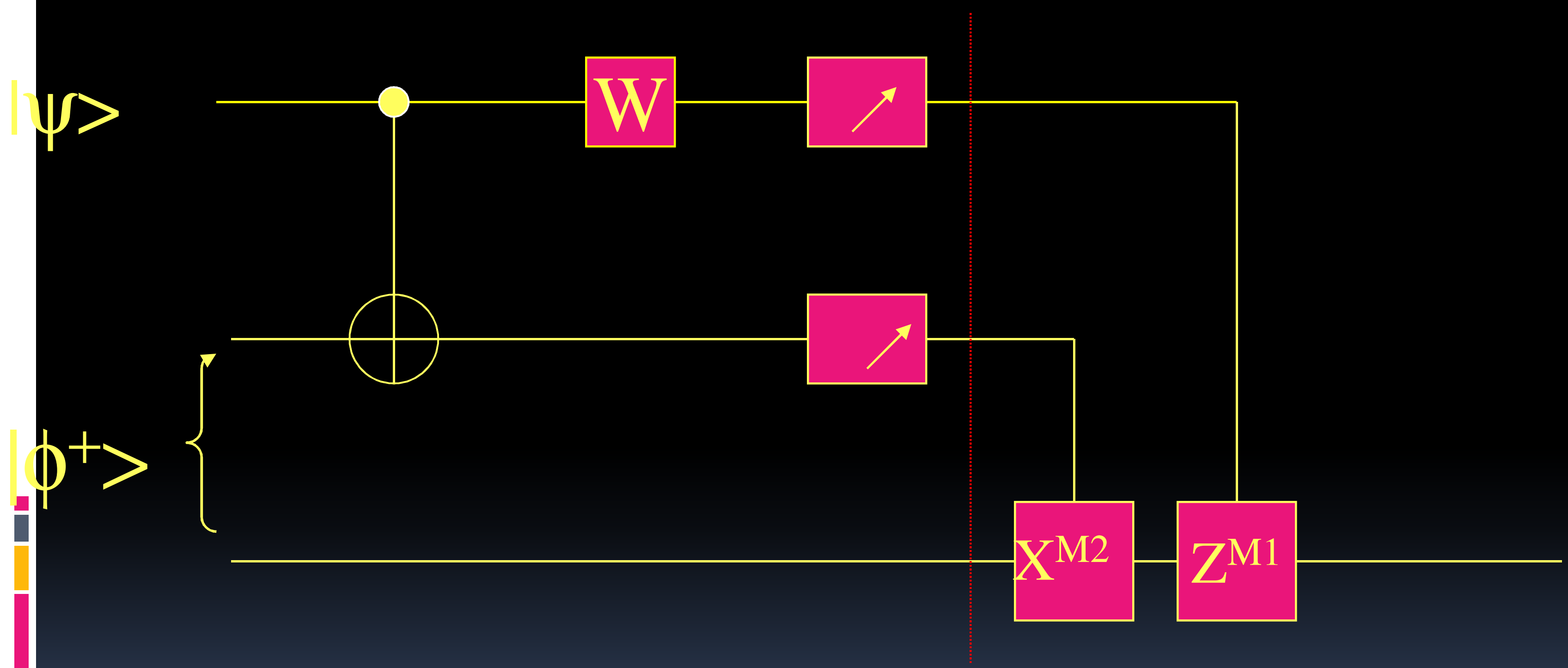
$$|\psi_2\rangle = 1/2[(|000\rangle\overbrace{(\alpha|0\rangle + \beta\,|1\rangle)}^{\gamma_1}]$$

$$+1/2[(|011\rangle\overbrace{(\alpha|1\rangle + \beta\,|0\rangle)}^{\gamma_2}]$$

$$+1/2[(|110\rangle\overbrace{(\alpha|0\rangle - \beta\,|1\rangle)}^{\gamma_3}]$$

$$+1/2[(|111\rangle\underbrace{(\alpha|1\rangle - \beta\,|0\rangle)}_{\gamma_4}]$$

Teleportation circuit-4



A mades measuraments on its two bits

If the measurament gives:

1.- $|00\rangle$ then B has qubit $\alpha|0\rangle + \beta\,|1\rangle = |\psi\rangle$

2.- $|01\rangle$ then B has qubit $\alpha|1\rangle + \beta\,|0\rangle$

3.- $|10\rangle$ then B has qubit $\alpha|0\rangle - \beta\,|1\rangle$

4.- $|11\rangle$ then B has qubit $\alpha|1\rangle - \beta\,|0\rangle$

When B receives the measurament from A:

1.- if |00> then B has $|\psi>$

2.- if |01> then B does $X(\alpha|1>+\beta\ |0>)=|\psi>$

3.- if |10> then B does $Z(\alpha|0>-\ \beta\ |1>)=|\psi>$

4.- if |11> then B does $Z[X(\alpha|1>-\beta|0>)]=|\psi>$

Remarks

- A and B teleport a quantum state (no the qubit)
- Teleportation is not a clonation
- During the teleportation the original state is destroyed
- To implement teleportation of a state is a routine experiment in a Lab.

Quantum Cryptography

Cryptography

Setting: A (Alice) and B (Bob) want to interchange messages, and they send them encrypted with a key.

The message is first converted into a sequence of integers $M=m_1,\ldots m_N$.

One time pad

- Before exchanging messages, A and B meet and create a pad which every page has 100 random integer between 0 and a–1, where a is the size of the alphabet.
- Each one of them, has a copy of the pad.
- The security of the scheme relies in the fact that nobody else should have access to the pad

For A to send M to B:

- A chooses a page p. Chooses the first N integers $k_1 \ldots k_N$ in p.
- A creates an encrypted text E $= \{e_1 \ldots e_N\}$ where $e_i = (m_i + k_i) \bmod a$
- A sends to B (E,p)

For B to recover M :

- B looks p. Finds the first N integers $k_1 \ldots . k_N$ in p.
- For each e_i in E, to recover M,

$$m_i = (e_i - k_i) \bmod a$$

Public key cryptography

A creates a public key P_A and a secret key S_A, s.t. for any message M :

$$P_A(S_A(M)) = S_A(P_A(M))$$

B also creates P_B and S_B

For A to send M to B : sends $P_B(M)$.

When B receives $P_B(M)$, does $S_B(P_B(M)) = M$.

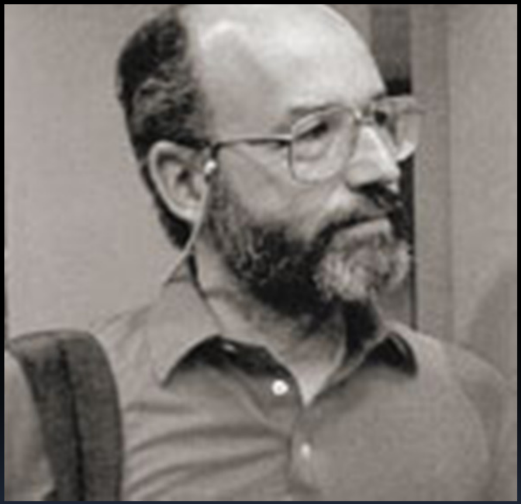
Public key

$P_B(M) \longrightarrow$

A ——————————————— B $\boxed{S_B}$

$\boxed{P_A \; P_B \; P_C \ldots}$

Rivest Shamir Adlerman



RSA

- Choose large p and q. Compute $N = pq$
- Find d which is co–prime with $(p-1)(q-1)$
- Compute e s.t. $ed = 1 \pmod{(p-1)(q-1)}$

$P = (e,N)$

$S = (d,N)$

RSA

- To encrypt $M=m_1,\ldots m_N$. use $P=(e,N)$

  $e_i = m_i^e \bmod N$
- To decrypt $E=\{e_1\ldots e_N\}$ use $S=(d,N)$

  $m_i = m_i^d \bmod N$

The security of RSA is not being able to factorize N

Quantum Crypto : Bennet, Brassard (1984) BB84

Quantum key distribution

Instead of using Q.M. for information storage, apply for information transmission

Key distribution

- Alice and Bob want to create a shared secret key by communicating over an insecure channel.
- Needed for symmetric encryption (one-time pad, DES etc.).

Heisenberg Uncertainty Principle

- *For certain pairs of observables (for ex. Position/momentum) knowing the value of one observable, makes the value of another observable more uncertain.*
- Therefore, any measurement of the output state that yields information in a classical way, produces a destruction of the remaining information.

The Qubit as polarization of photon

- Photon: orthogonal electromagnetic fields.
- Polarized photon: electric field oscillates in desired plane (0, 45, 90, 135)
- Rectilinear polarization: electric field oscillates 0/90
- Diagonal polarization: electric field oscillates 45/135

0 and 1 as polarized photons

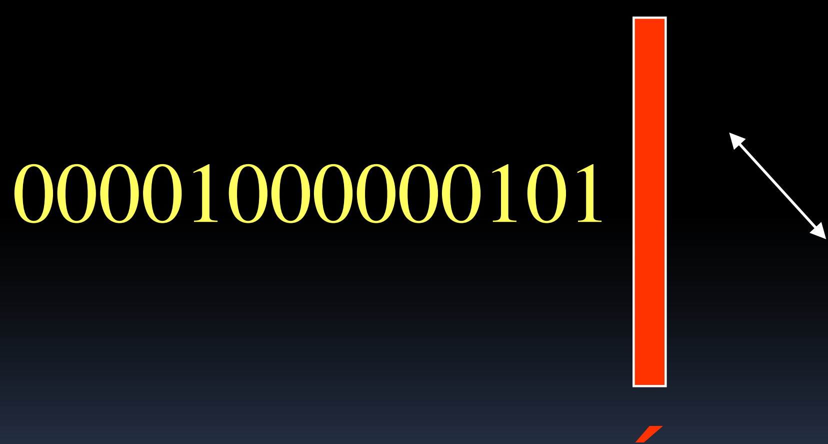
WLOG assume:

- Polarized photon at 0 and 45 represent 0
- Polarized photon at 34 and 135 represent 1
- To encode a {0,1}, place a photon in a particular polarization state. Using a Pockel cell (a polarization dependent switch)

Pockel switch

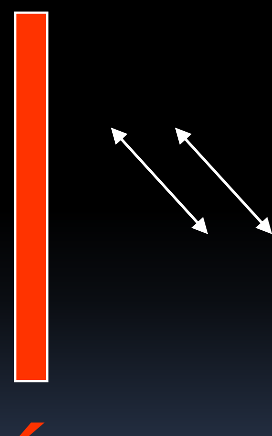
Pockel switch

Diagonal



Pockel switch

0000100000010

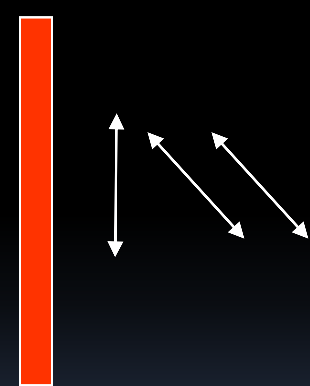


Pockel switch

Rectilinear

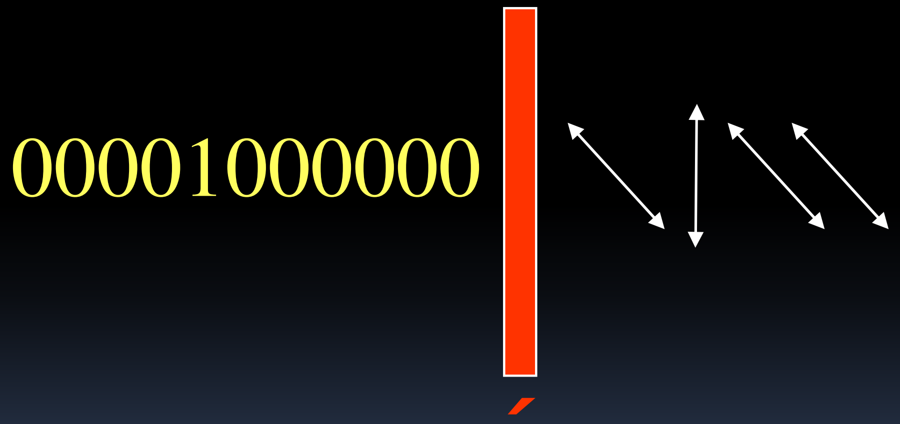
+

000010000001

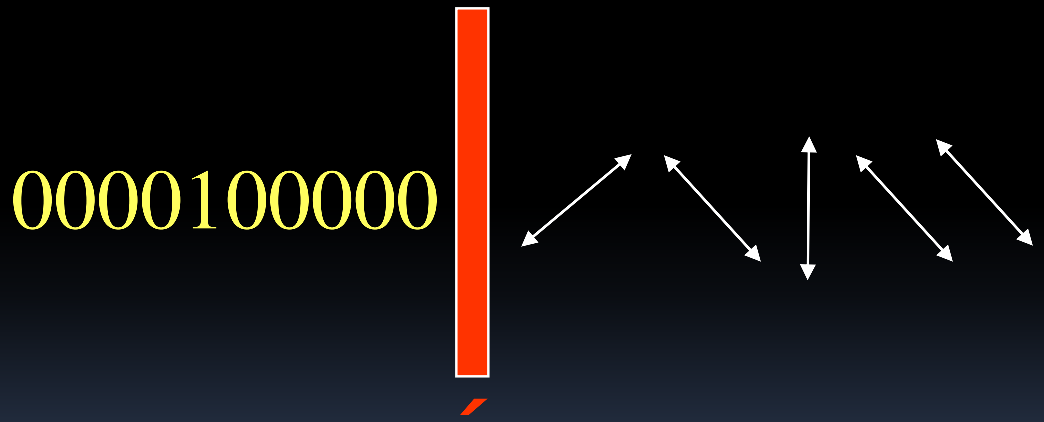


+

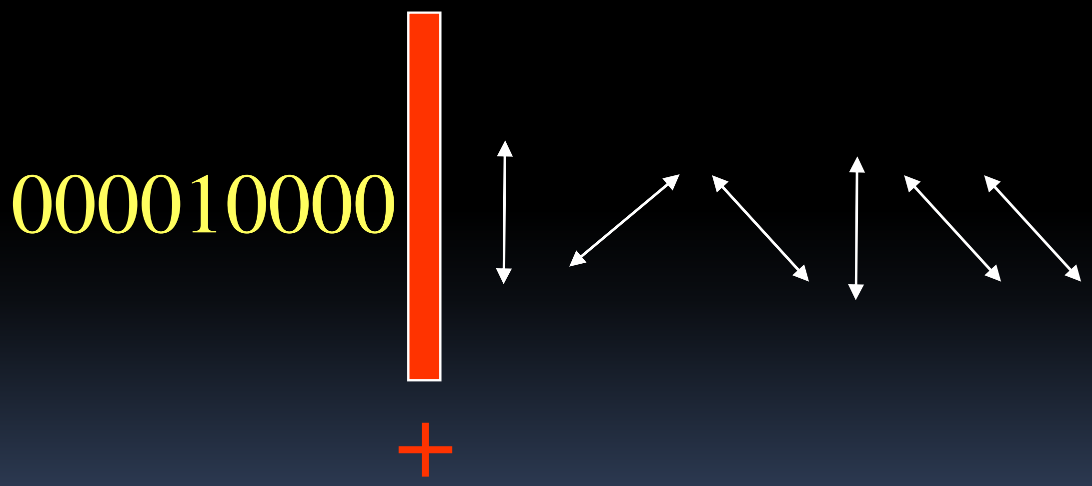
Pockel switch



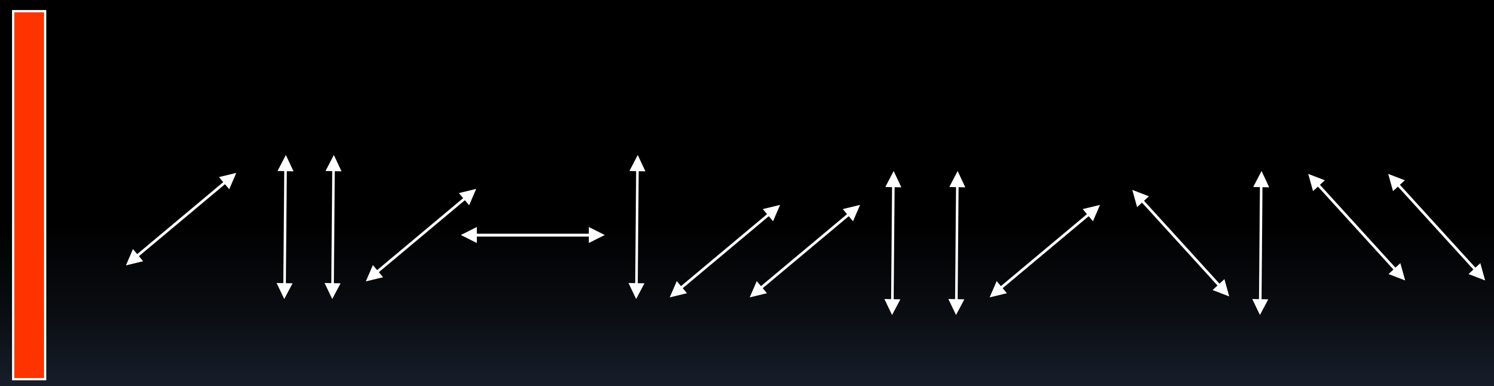
Pockel switch



Pockel switch



Pockel switch



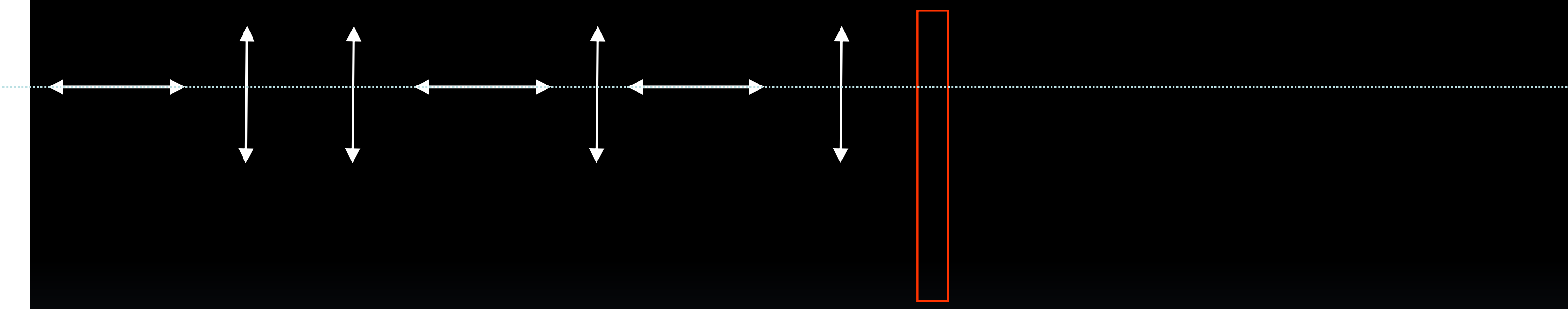
To measure polarization

Given an stream of photons, to measure the polarization use a Calcite (calcium carbonate) which has the property of being *birefringent*

We can set the calcite polarization axis:

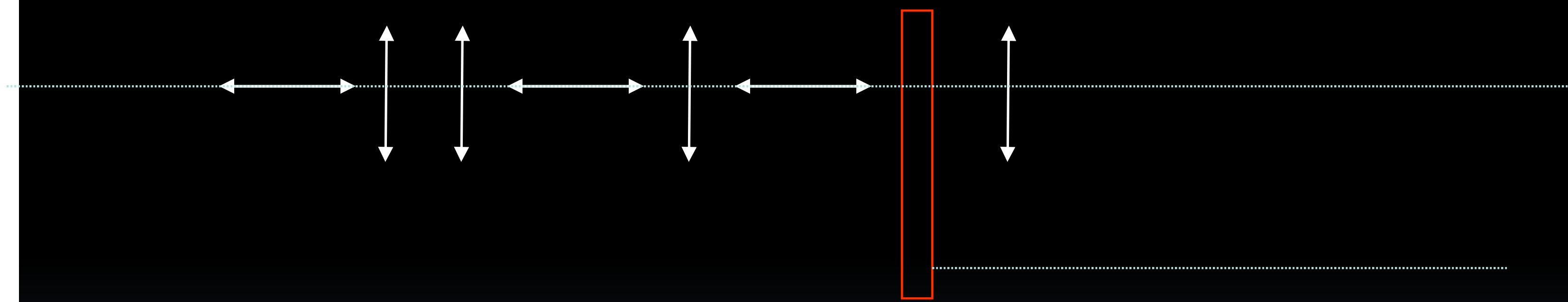
- Rectilinear (+) 0/90
- Diagonal (/) 45/135

Calcite



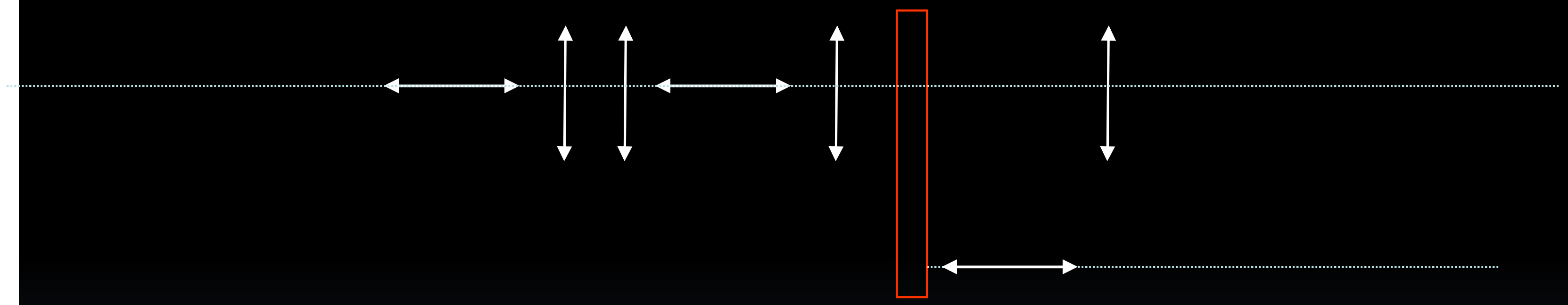
+ (90)

Calcite



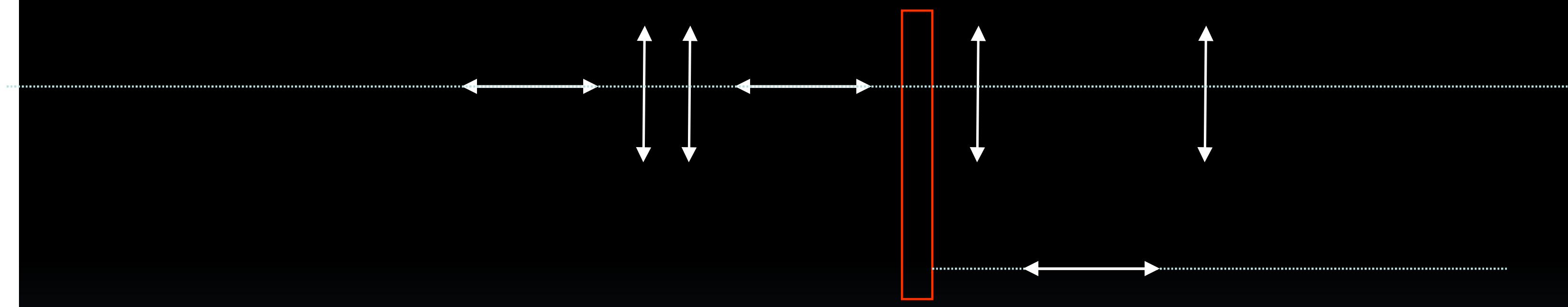
+ (90)

Calcite



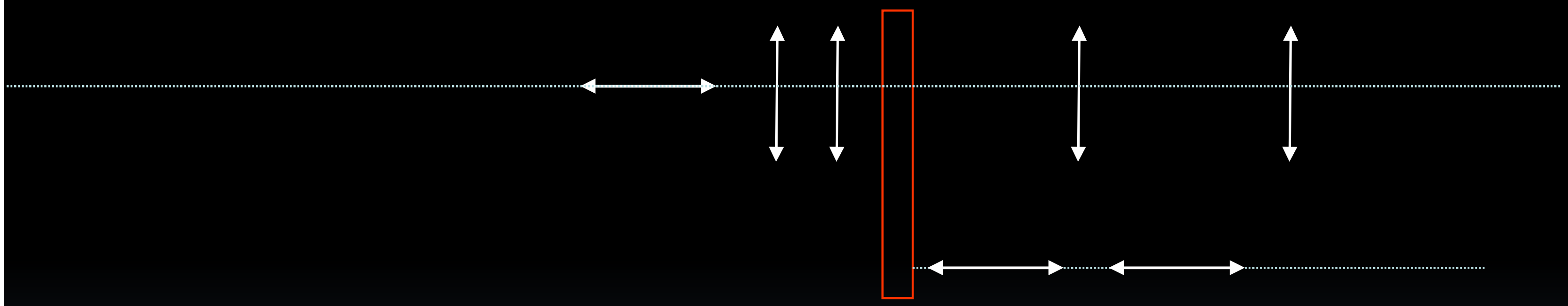
+ (90)

Calcite



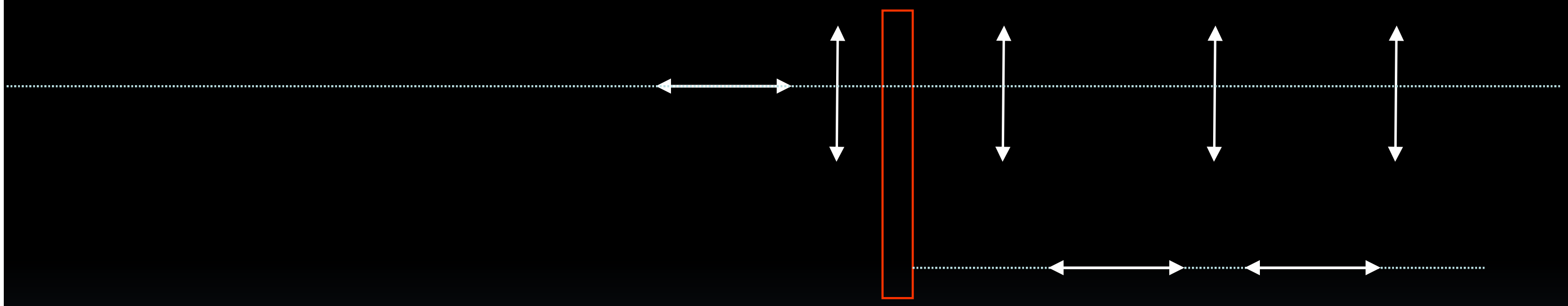
+ (90)

Calcite



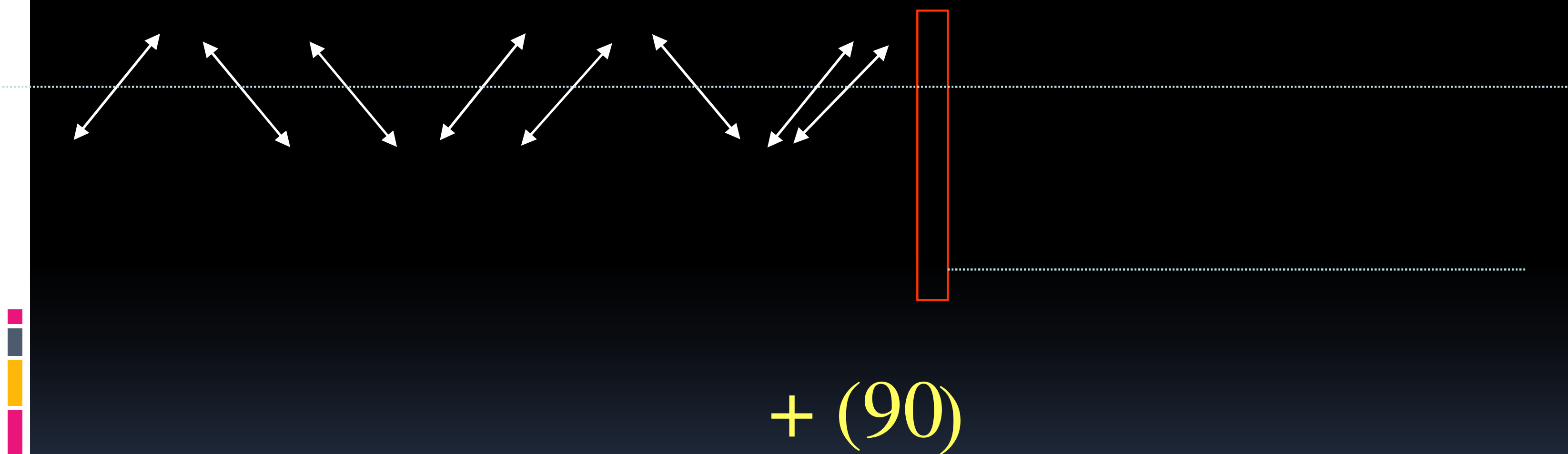
+ (90)

Calcite



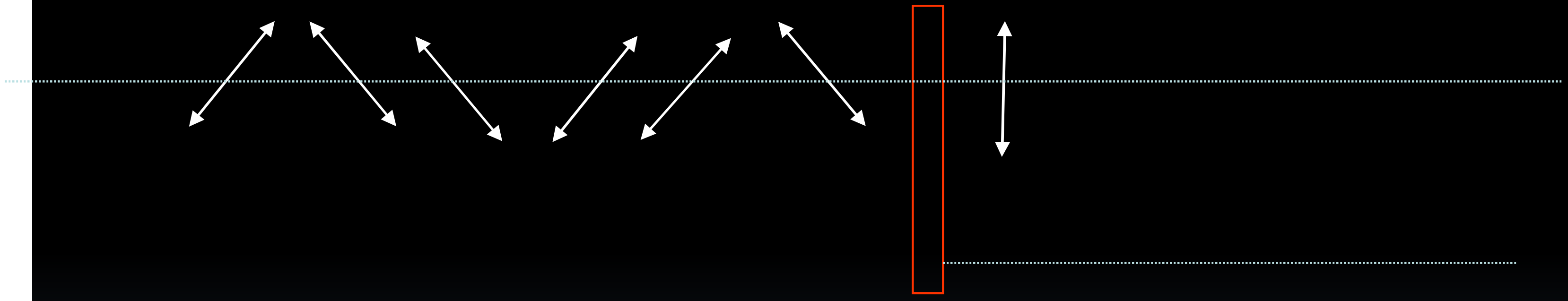
+ (90)

Calcite



Calcite

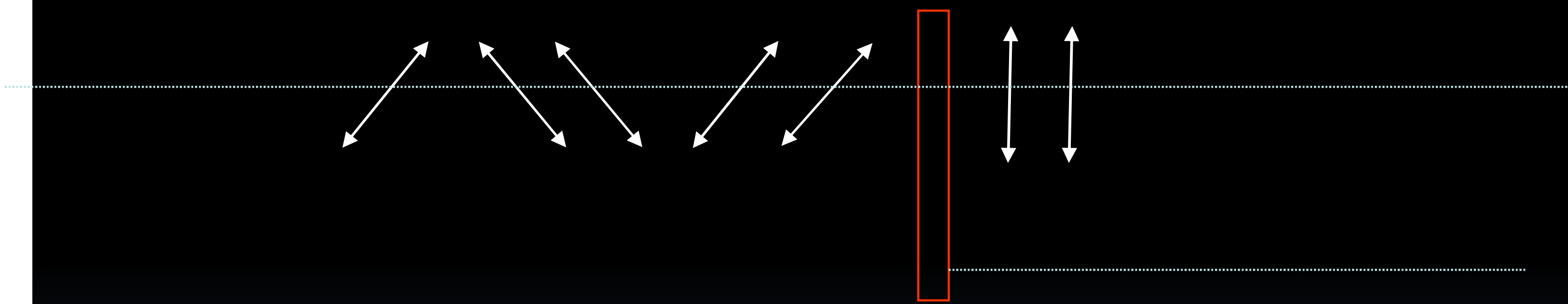
With probability 1/2:



+ (90)

Calcite

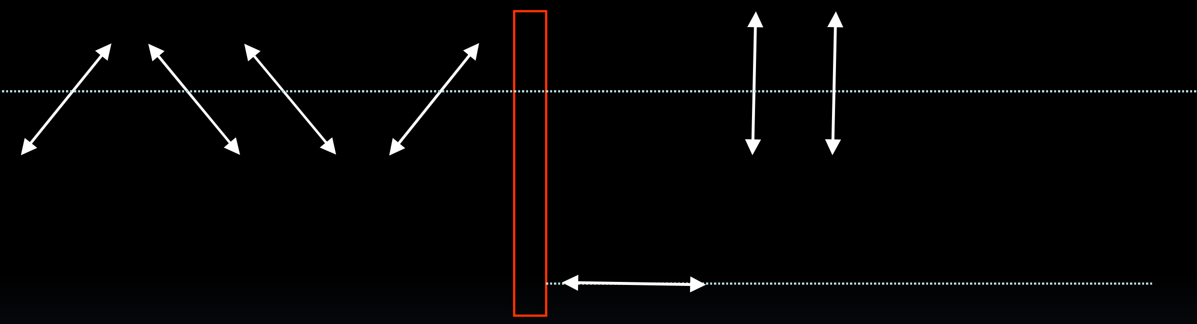
With probability 1/2:



+ (90)

Calcite

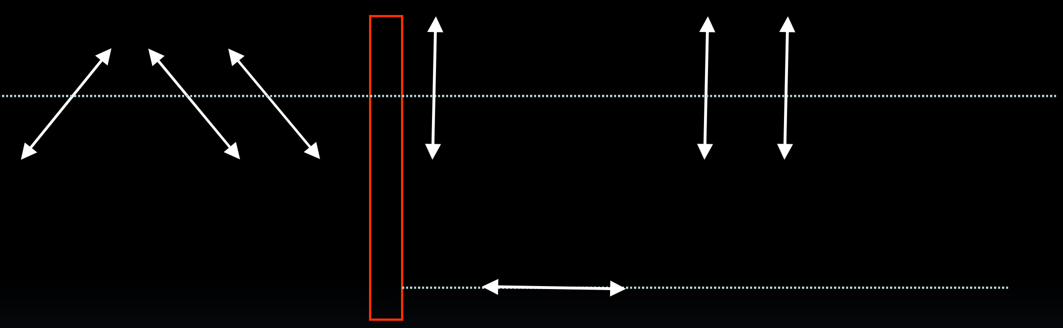
With probability 1/2:



+ (90)

Calcite

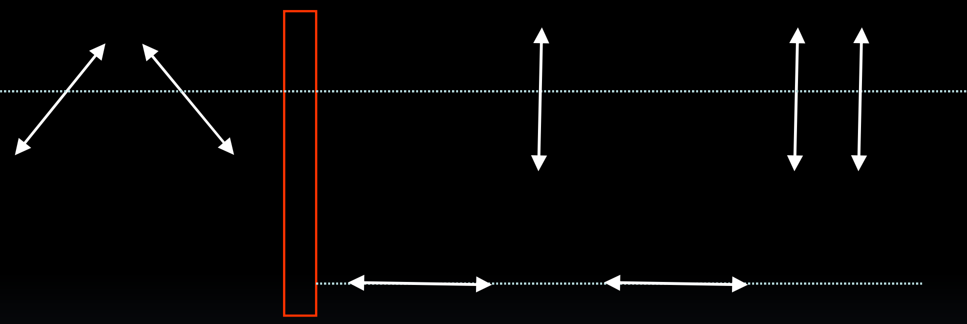
With probability 1/2:



+ (90)

Calcite

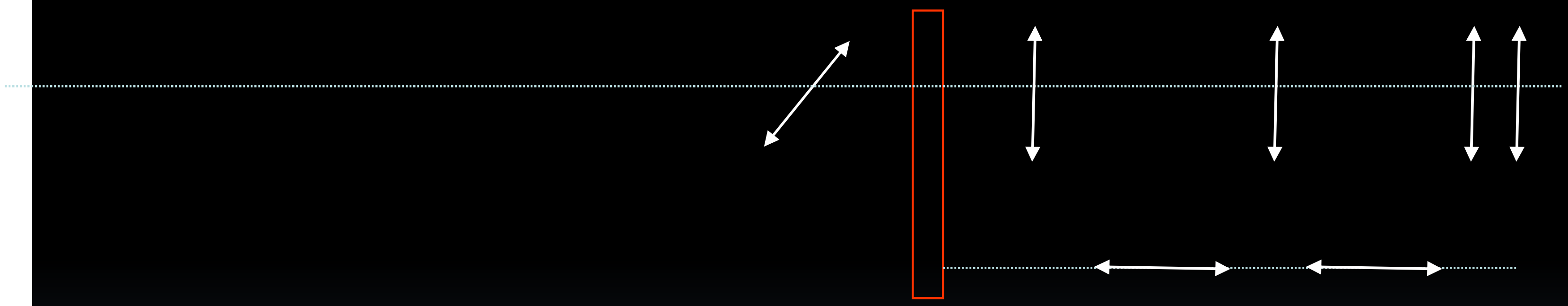
With probability 1/2:



+ (90)

Calcite

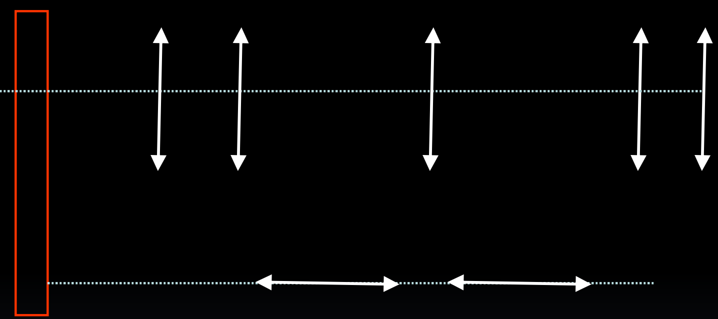
With probability 1/2:



+ (90)

Calcite

With probability 1/2:

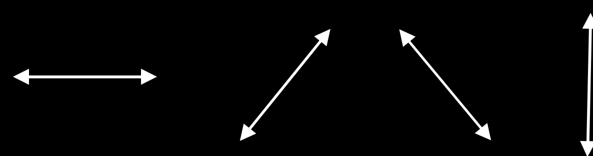


+ (90)

Quantum key distribution(QKD)

Central idea: use non-orthogonal quantum states to encode information.

Given a single photon in one state



Heisenberg principle forbid from simultaneously measuring accurately the polarization of $\times$

and $+$

QKD (BB84)

- A creates a random string of {0,1}.
- For each bit A encodes using / or + (each time selecting / or + randomly)
- A sends to B the created photons (by open channel)

QKD (BB84)

- When B receives the string of polaritzed photons, for each one chooses an orientation for his calcite, and measures the polarization of each photon
- Notice, he must guess the correct / or + for the calcite

BB84

- Over an insecure channel, A tells B the polarizer orientation of a subset S of bits
- B tells A the calcite orientations he used for bits in S.
- For the bits in S they agree in the orientation, A tells B what bit should he have obtain

BB84

- If they disagree in one bit (which both set to the same polarization, this means E has read the polarization sent by A (with the wrong orientation of the calcit) , which will happen with probability 1/4.
- Therefore if they agree in 100%, the probability of eavesdropping is $1-(3/4)^S$, which for large S is small

BB84

- Once the channel is secure, A tells B what orientations used for each bit
- B compares his orientations with A, in the ones they agree the bit B has must coincide with A.
- Those bits form the key

Example QKD A:

1 1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 1

Example QKD A:

Generates random orientations (Pockell)

1 1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 1

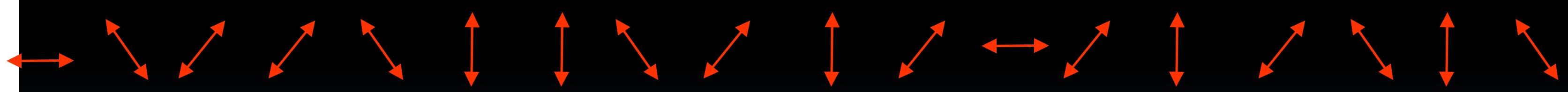
+×× ××++×× +×+×+ ××+×

Example QKD A:

POLARIZED OUTPUT

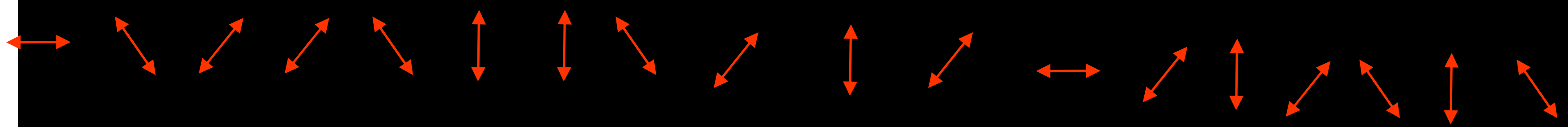
1 1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 1

+ × × × × + + × × + × + × + × × + ×



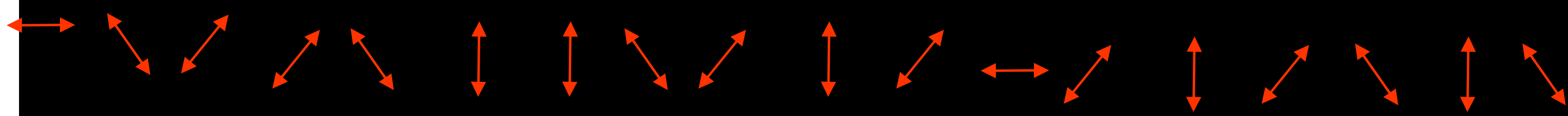
Example QKD B:

B gets a stream:



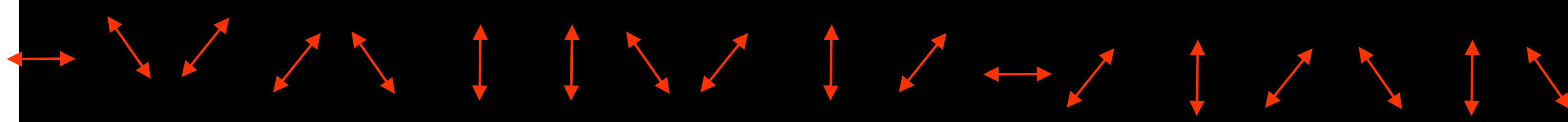
Example QKD B:

Chooses randomly orientations to calcite



+ × + + × + × + × × × + + + + × × +

Example QKD B:



+ × + + × + × + × × × + + + + × × +

1 1 1 1 1 0 1 0 0 0 0 1 1 0 1 1 0 1

Example QKD:

A selects S:

1 0 1 0 1 0

× × × ×+ ×

Example QKD:

B proves which orientations coincide for S:

1	0	1	0	1	0
×	×	×	×	+	×
×	+	+	×	+	+

Example QKD:

B proves which orientations coincide for S:

1 0 1 0 1 0

× × × × + ×

× + + × + +

Example QKD:

To test for eavesdroppers:

1 0 1 0 1 0

× × × ×+ ×

× + + ×+ +

1 0 1

Example QKD A:

A reveals her orientations:

+ × × × + ×   × +   × + × × + ×

Example QKD A:

B checks his orientations:

\+ × ×++ ×+ ×+××+×

\+ × ×+× ×× +++××+

Example QKD A:

B checks his orientations:

+	×	×	+	+	×	+	×	+	×	×	+	×
+	×	×	+	×	×	×	+	+	+	×	×	+

Example QKD A:

B looks at his bits:

+	×	×	+	+	×	+	×	+	×	×	+	×
+	×	×	+	×	×	×	+	+	+	×	×	+
1	0	1	0		0			0		1		

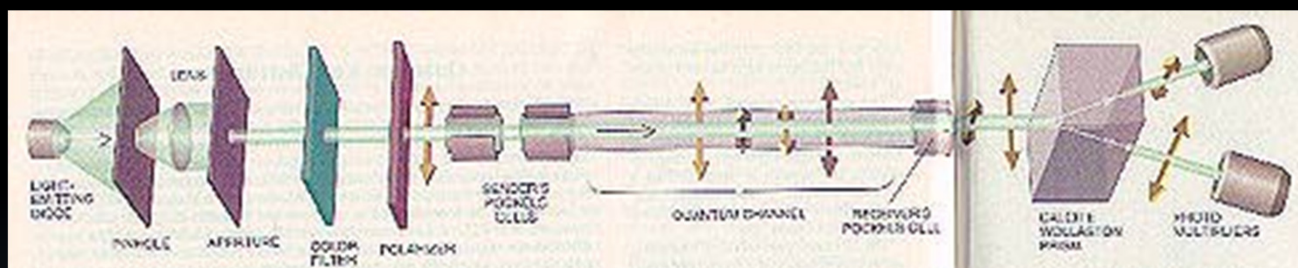
The key (for one time pad)

+ × ×++ ×+ ×+××+×

+ × ×+× ×× ++++××+

1 0 1 0 0 0 1

MIT implementation of BB84



QKD summary

- Key distribution requires hardness assumptions classically.
- QKD based on quantum mechanics.
- Higher degree of security.

QKD implementations

- MIT (BB84), 1992.
- Many others
- Currently: 67km, 1000 bits/second.
- Commercially available: Id Quantique, since 2002.

Id Quantique: QKD

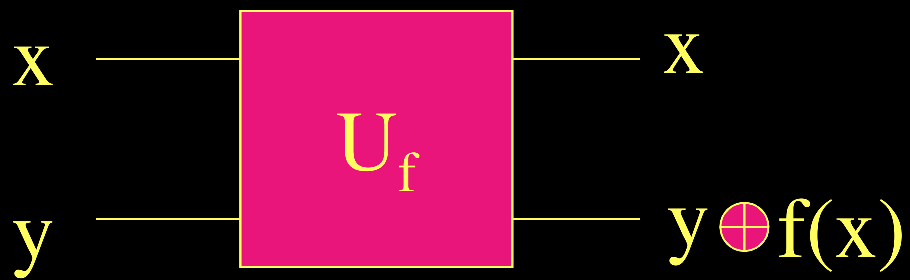
Quantum Computation

Deutsch Problem and Deutsch Jozsa solution

Quantum parallelism: Deutch Problem

- Let $f:\{0,1\} \rightarrow \{0,1\}$, which takes 24h. to compute with a classical computer. We wish to decide if $f(0)=f(1)$ or they are different.

Gate U_f:



Input: $|xy\rangle$

Output: $|x\, y \oplus f(x)\rangle$

Power of Quantum Paralleism

Input: $|x\rangle \otimes (|0\rangle - |1\rangle)/\sqrt{2}$

Output: $|\Psi\rangle = |x\rangle \otimes (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)/\sqrt{2}$

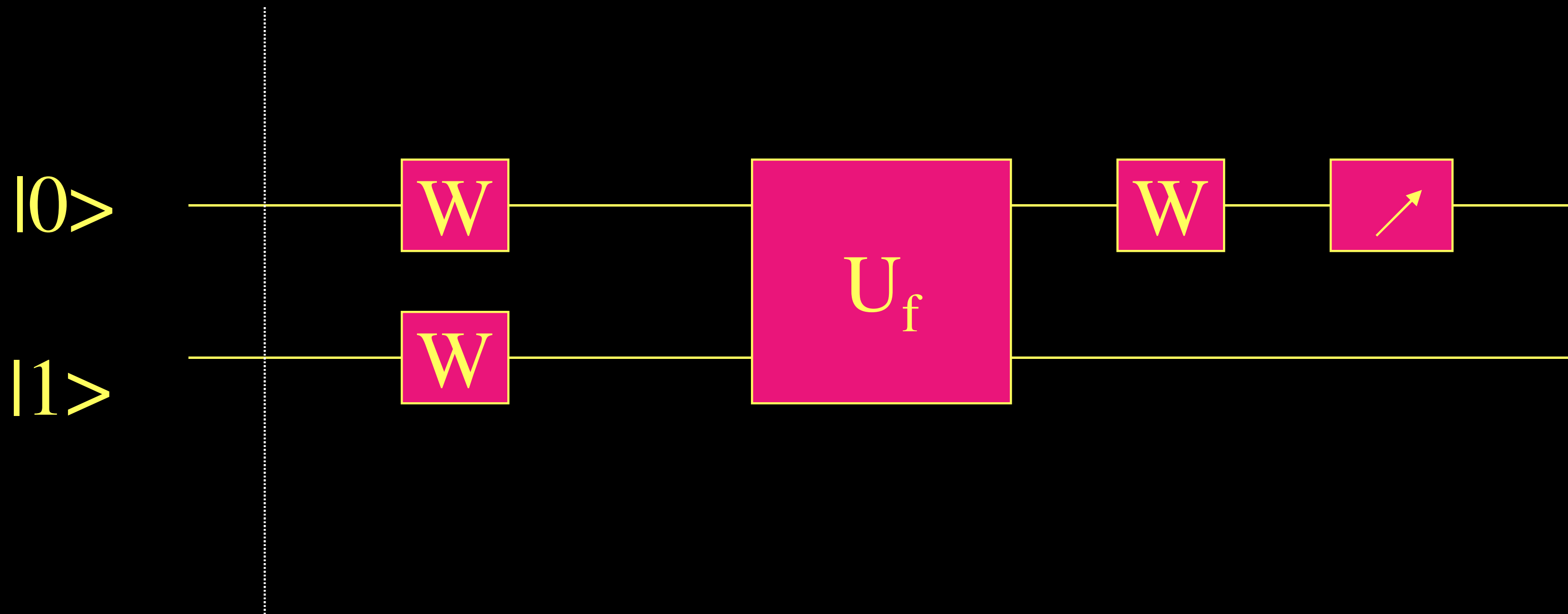
As $f(x)=\{0,1\}$

If $f(x)=0$ the second qubit is $(|0\rangle - |1\rangle)/\sqrt{2}$

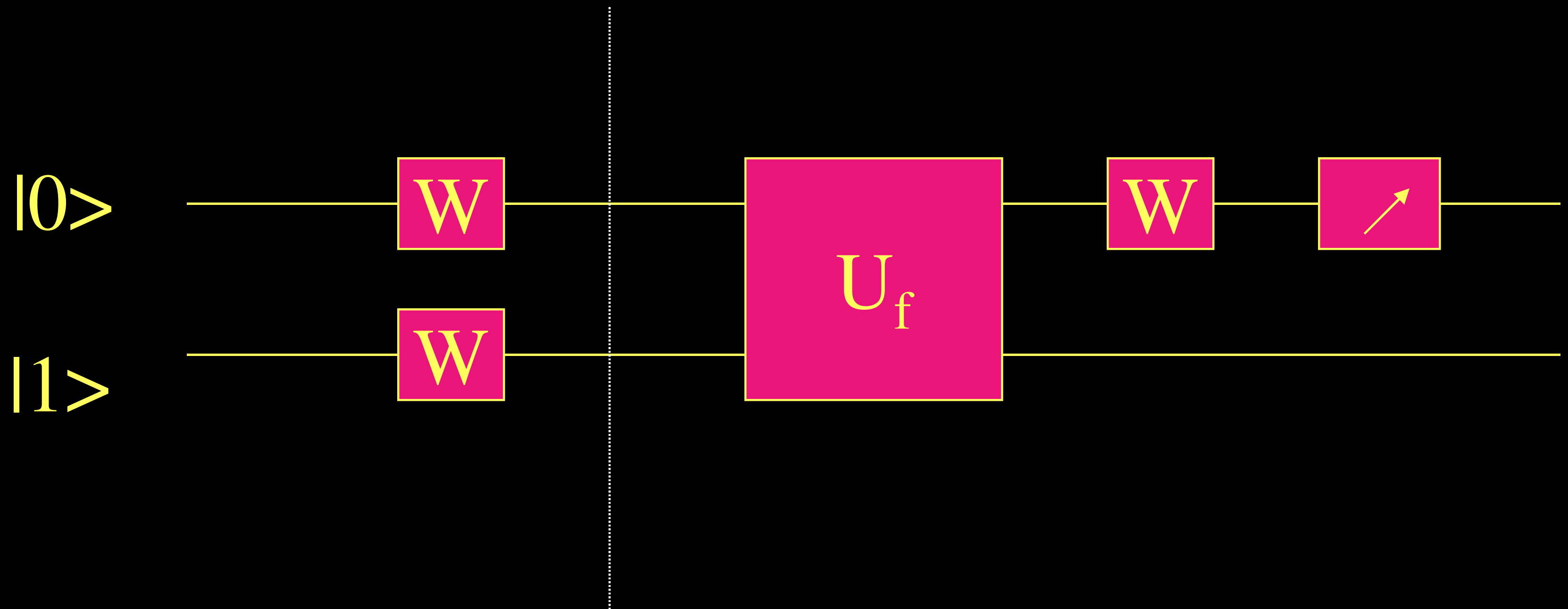
If $f(x)=1$ the second qubit is $(|1\rangle - |0\rangle)/\sqrt{2}$

$$|\Psi\rangle = |x\rangle \otimes (-1)^{f(x)} \; (|0\rangle - |1\rangle)/\sqrt{2}$$

Therefore, we could decide the output of U_f with only one computation of f(x)

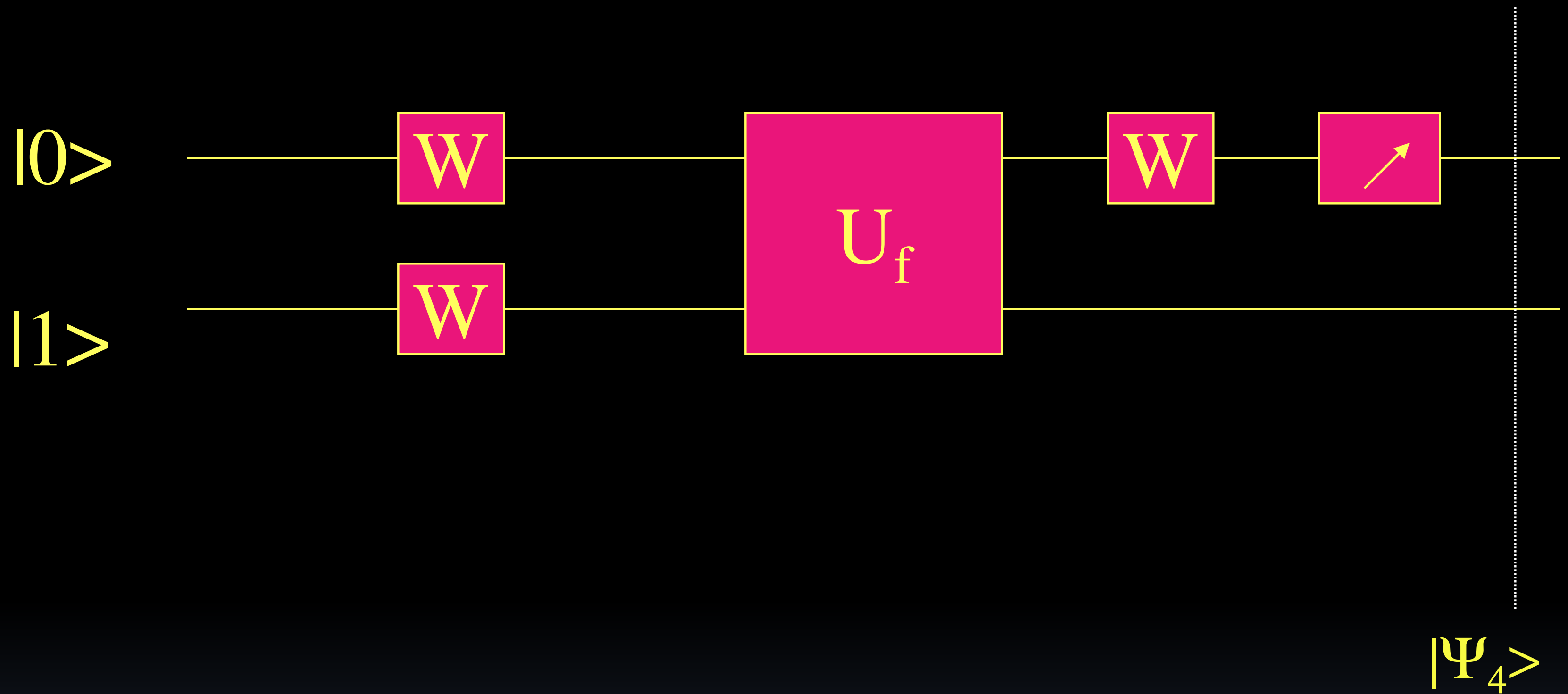


$|\Psi_0\rangle = |01\rangle$



$$|\Psi_1\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \otimes (|0\rangle + |1\rangle)/\sqrt{2}$$

Problem: find the expresion for $|\Psi_4\rangle$



Further Lines of study/research

- Shor algorithm for factorization
- Grover's algorithm for search
- Quantum walks

Andris Ambainis: Quantum walks and their algorithm applications