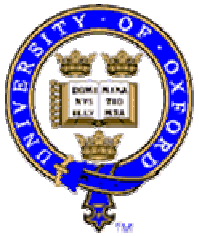


Quantum Cryptography
Applications in Electronic Commerce

Jonathan Jones

Oxford Centre for Quantum Computation

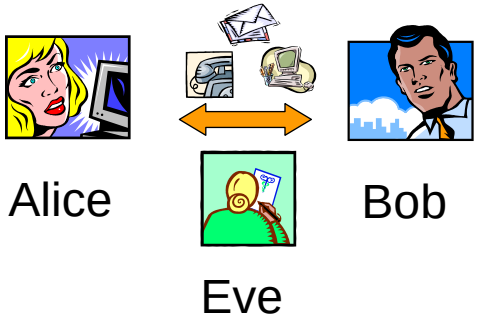
http://www.qubit.org

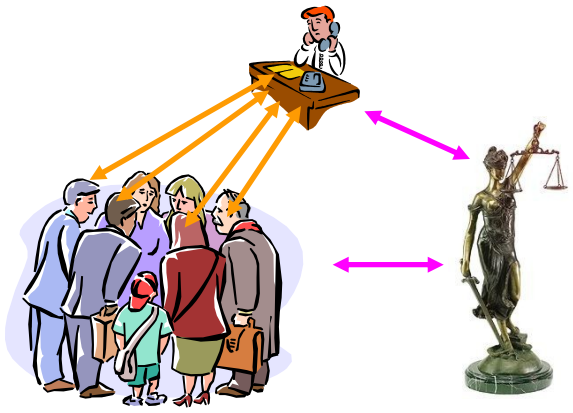
jonathan.jones@qubit.org

Outline of this talk

- A brief introduction to cryptography and the main issues
- How does quantum cryptography work?
  - The Vernam cipher (one time pad).
  - Quantum money
- The BB84 protocol (Bennett and Brassard, 1984)
- The intercept-resend attack
- Practicalities and time scales
- Man in the middle attacks

Issues in cryptography





- One to one (b2b) or many to many (b2c)?
- Secrecy or authenticity?
- Authentication or non-repudiation?
- What threat model?
- Secret key or public key?

Secret key cryptography

- Alice and Bob share a common “key” (large number)
  - Security of the system depends on keeping the key secret
  - Recovering the key is “computationally infeasible”
  - Vernam ciphers (one time pads): absolutely secure
  - Self-authenticating
- Key distribution problem
  - Particularly difficult for one time pads
- Non-repudiation is difficult or impossible

Public key cryptography

- Use two different keys for encryption and decryption
  - No key distribution problem
- Private key also used for digital signatures
  - Third parties can verify signatures: non-repudiation!
  - Can sign public documents: digital contracts
- Security depends on the difficulty (?) of factoring
  - Vast sums of money rest on a mathematical hypothesis!
  - Factoring is known to be easy on a quantum computer
- Quantum computers are very hard (but not impossible!) to build

Quantum cryptography

- Should be called quantum key distribution
  - Allows two people to come to an agreement on a very long secret key, which is used as a one time pad (unbreakable).
- Uses the fact that quantum particles cannot be observed without being affected
  - Any attempt to eavesdrop on this process will be detected and can be partially overcome
- Theoretically could permit “unconditionally secure” cryptography (if quantum mechanics is correct)

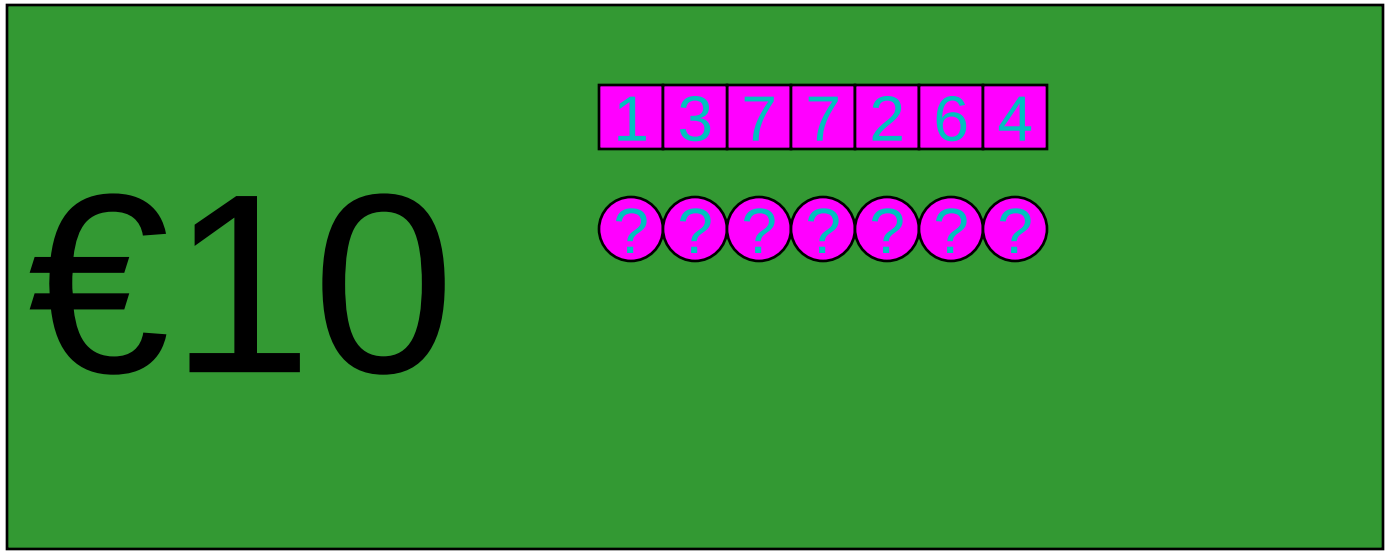
Vernam cipher

- Use a trivial encryption scheme with a very long key
  - Gilbert Vernam, AT&T, 1917
  - Vernam encrypted Baudot teletype code using bitwise addition modulo 2
- For complete security must use a *random* key, as *long as the message*, and used *only once*
  - Joseph Mauborgne, US Signal Corp, 1918
  - The “one time pad”: provably secure
- Really only used for diplomatic and espionage traffic
  - Even these weren’t always done properly!

Quantum money

- The oldest known quantum information scheme, invented by Stephen Wiesner c. 1970, but not published until 1983.
  - As yet pure theory: completely impossible to implement!
- Quantum money *cannot* be forged or copied (guaranteed by the laws of physics as we know them)
  - Quantum objects cannot be observed without being affected
- Any attempt to copy a note will damage the original
  - True tamper proof system
  - Fakes can only be detected by the issuing bank

Quantum money

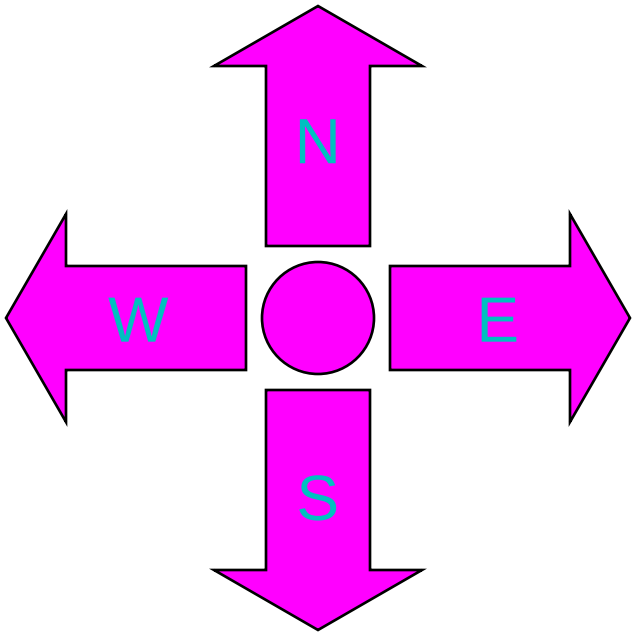


- Every note has a public serial number and a private check number
  - A forgery will have the wrong check number

Quantum money

- Issuing bank *must* be able to read the check number
  - Otherwise they can't check for forgeries
- Other people *must not* be able to read the check number
  - Otherwise they could (in principle) copy notes
- Need some sort of "magic" ink!
- Quantum mechanics provides a solution
  - You can only read a check number if you already know what it says!

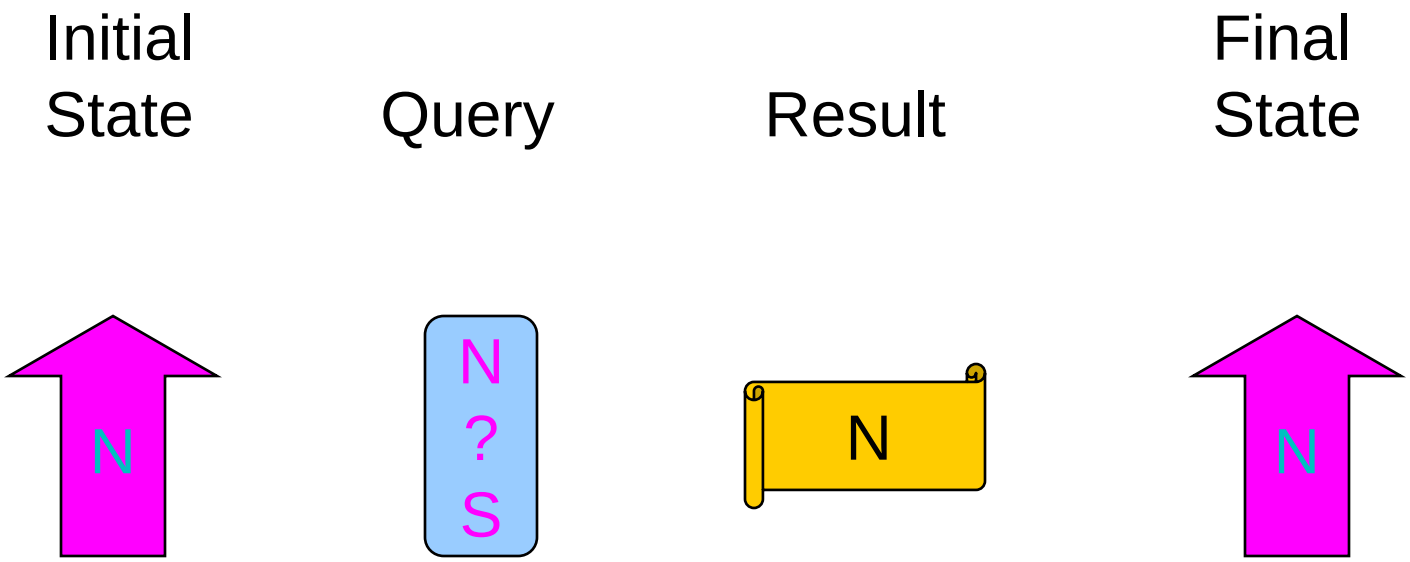
Quantum labels



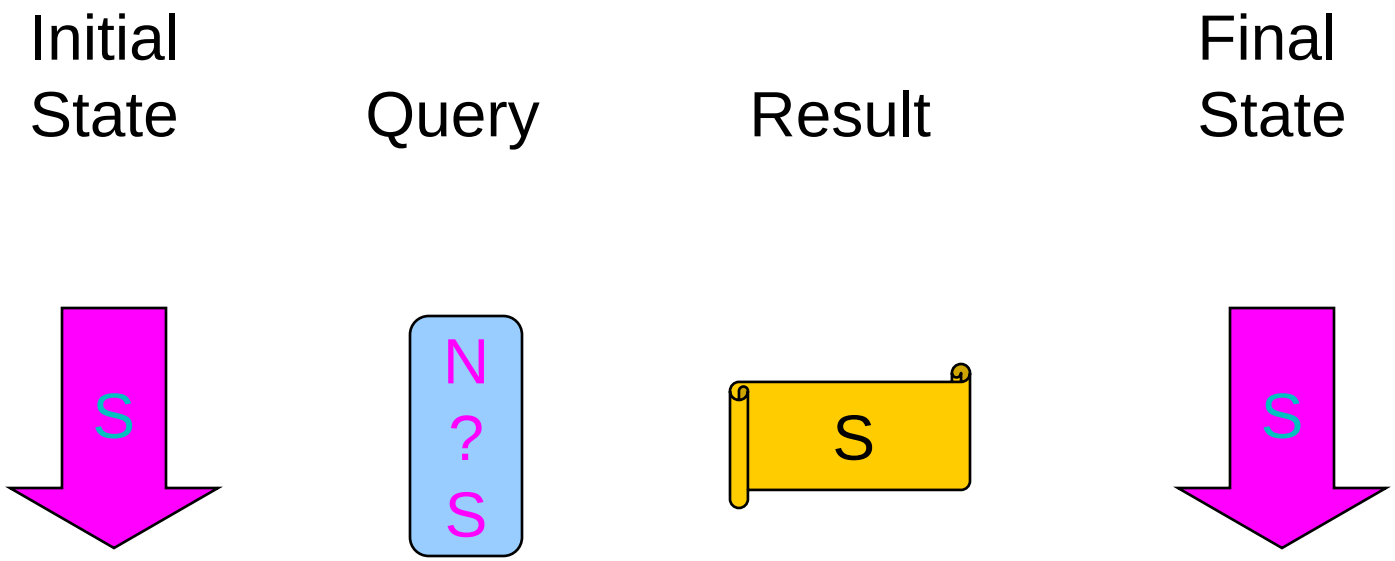
- Each label is a quantum system which can be in one of four states: North, South, East and West
- Only possible measurements are of the form “North/South?” or “East/West”.

The magic labels can be thought of as single photons with polarisations of 0° (N), 90° (S), 45° (E), or 135° (W). Measurements on them are made using polarising beam splitters and single photon detectors. Alternatively any four equivalent states on a Poincarre or Bloch sphere will do.

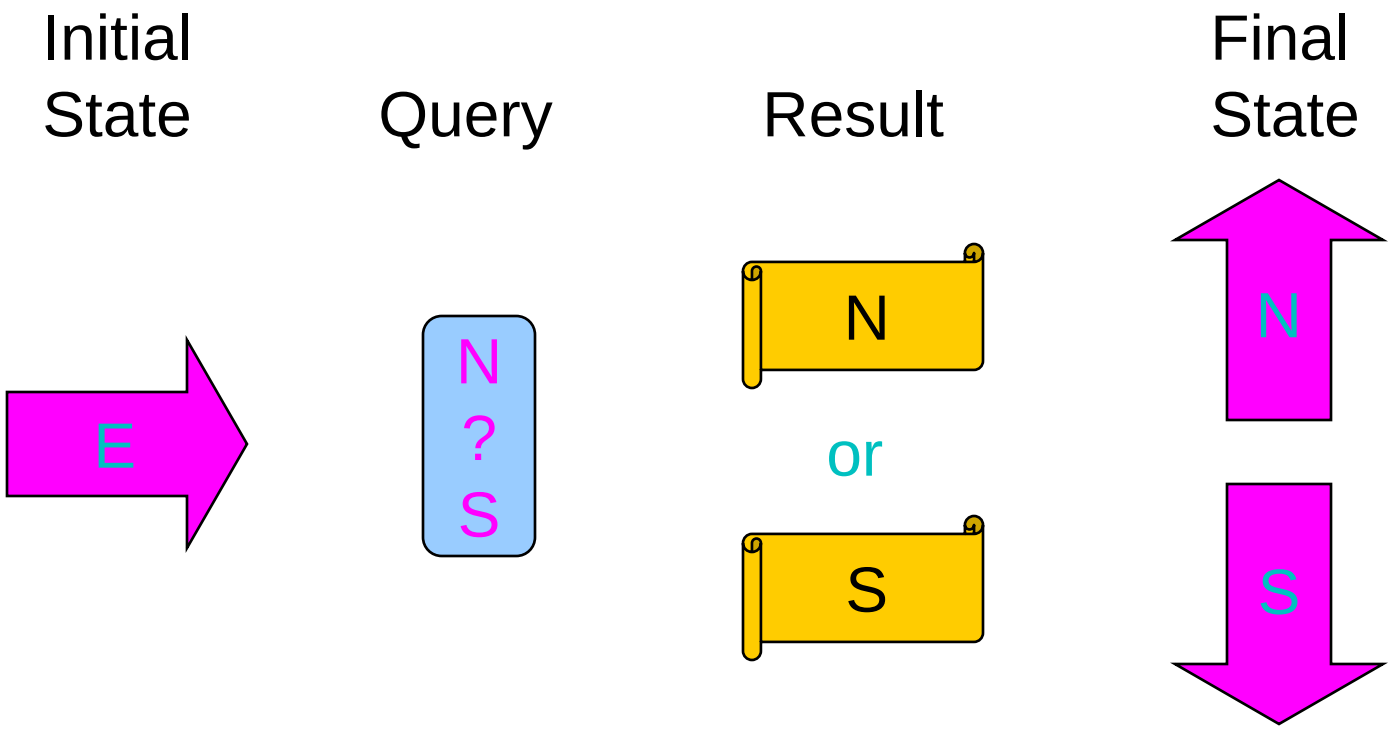
Quantum labels



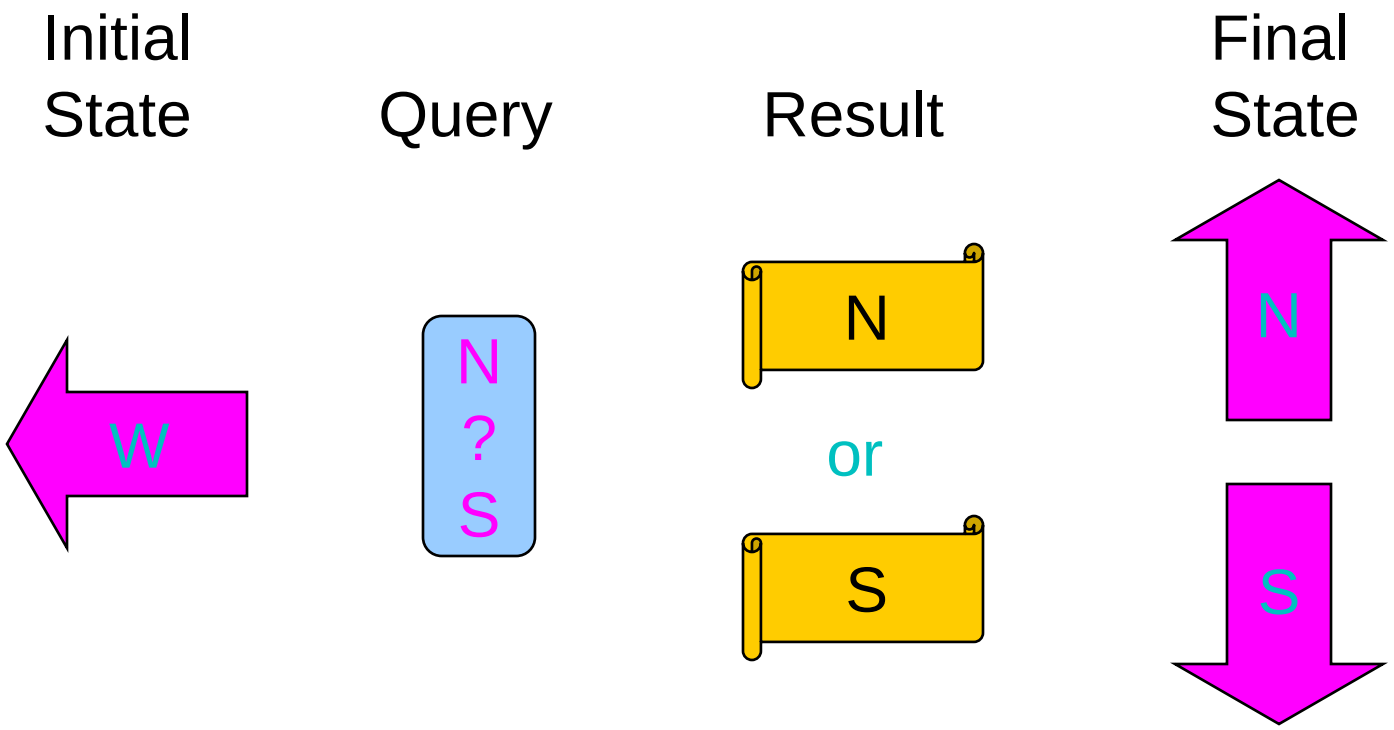
Quantum labels



Quantum labels



Quantum labels



Quantum labels

- If you ask the right question, you get the right answer
  - The Bank knows what questions to ask, and so can check the number against its records
- If you ask the wrong question, you get the wrong answer
  - Nobody else can read the number accurately
  - With a long check number you're bound to make a mistake
- Asking the wrong question damages the original
  - You don't get a second chance at reading the number
  - It is impossible to copy the number!
  - Quantum "No Cloning" theorem

Quantum key distribution

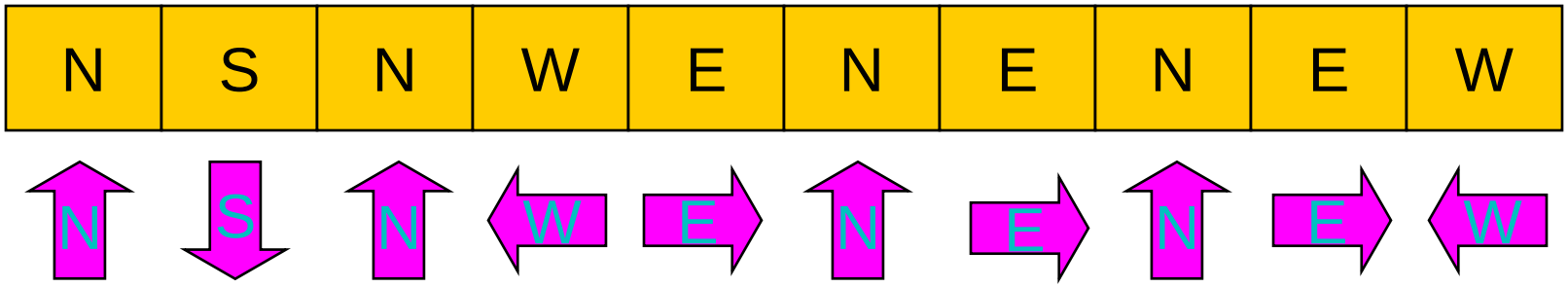
- Alice prepares a long string of quantum labels (N, S, E, W) and sends them to Bob.
  - Labels randomly chosen, but Alice knows what they are.
- Bob measures each label, choosing between “N?S” and “E?W” measurements at random
  - Bob chooses right half the time
- Bob tells Alice what questions he asked
- Alice tells Bob which questions were right
  - When Bob asked the right question he got the right answer!
  - Alice and Bob now agree about a random string of labels

Quantum key distribution

N	S	N	W	E	N	E	N	E	W

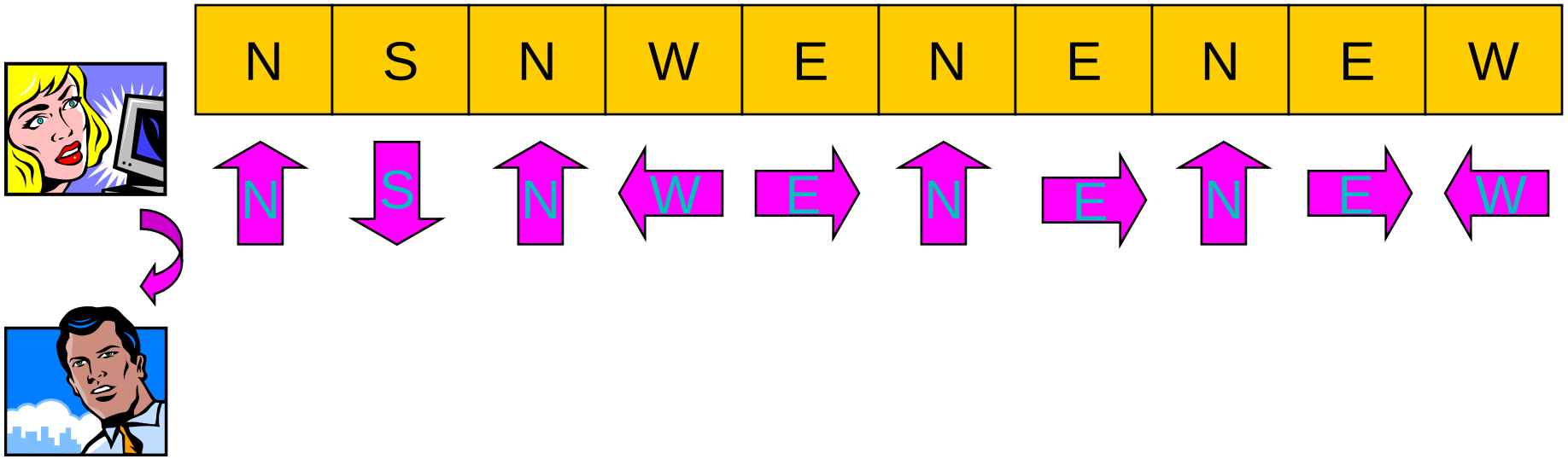
Alice chooses a random string of directions

Quantum key distribution



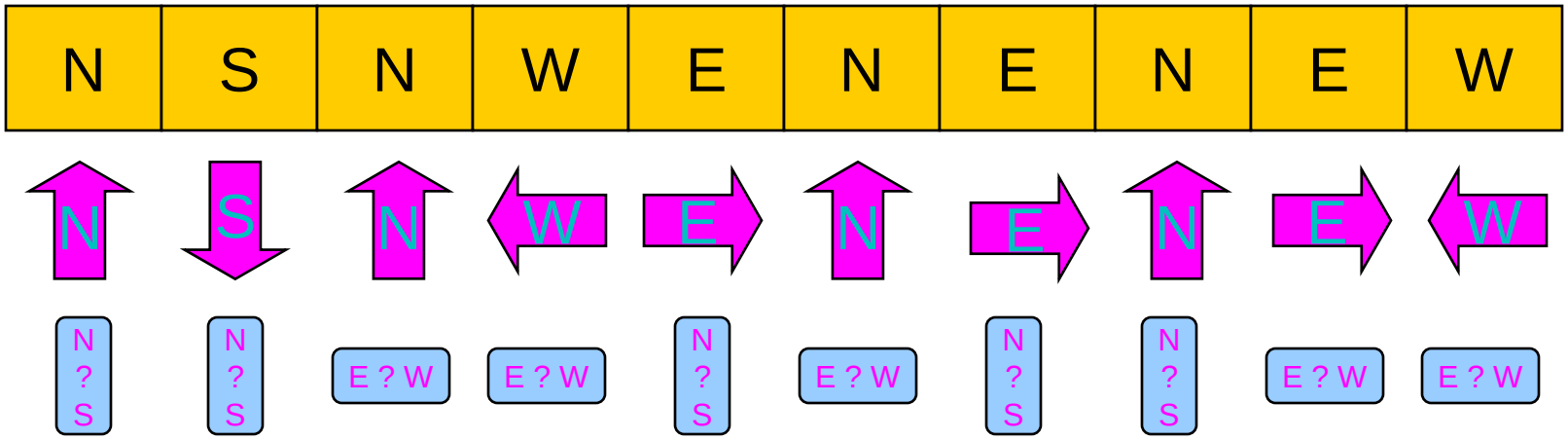
Alice prepares quantum labels in the right states

Quantum key distribution



Alice sends her labels to Bob

Quantum key distribution



Bob chooses a random set of measurement directions

Quantum key distribution

N	S	N	W	E	N	E	N	E	W

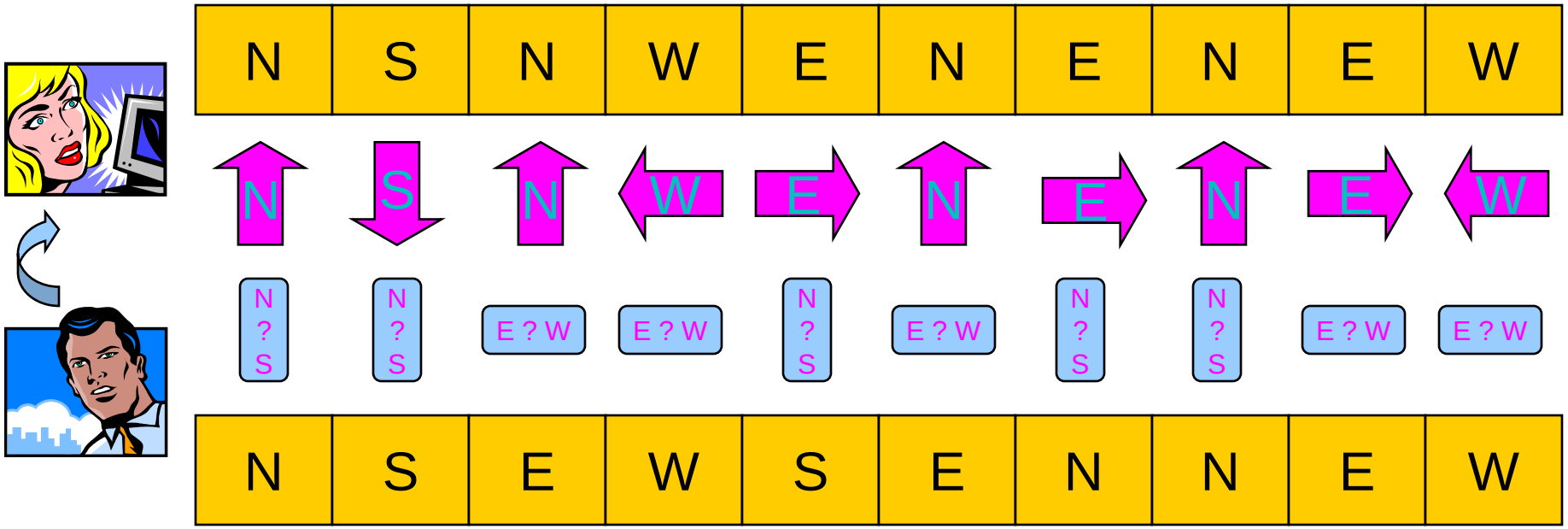
N	S	N	W	E	N	E	N	E	W

N ? S	N ? S	E ? W	E ? W	N ? S	E ? W	N ? S	N ? S	E ? W	E ? W

N	S	E	W	S	E	N	N	E	W

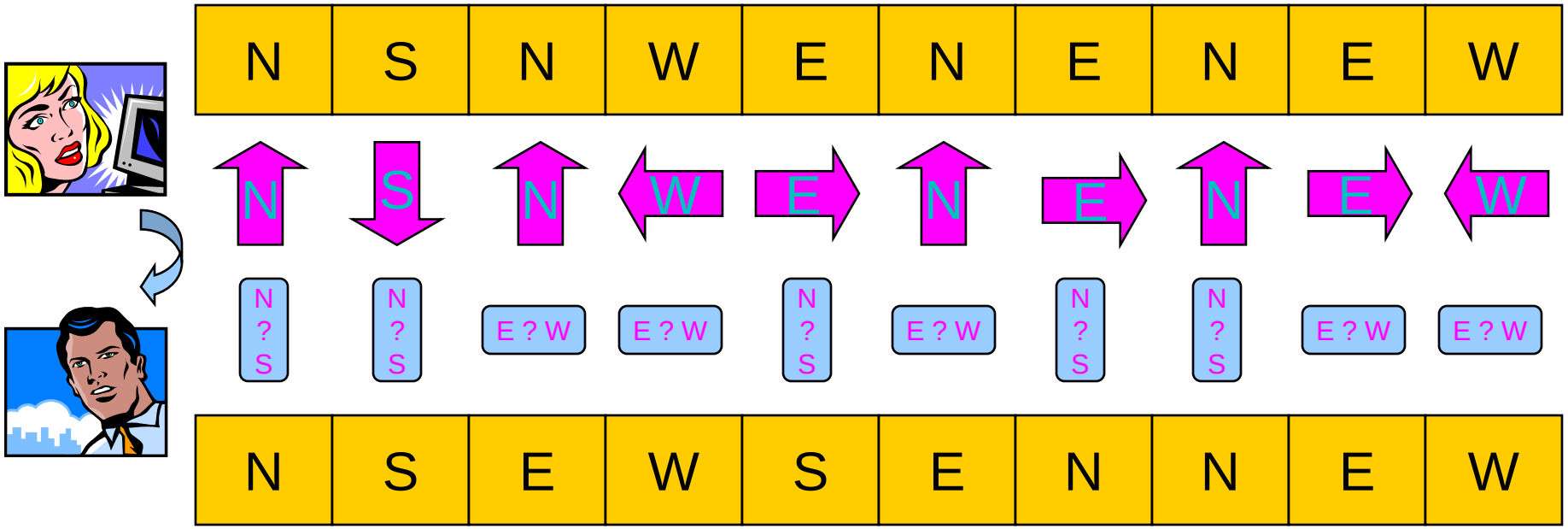
Bob notes down his results

Quantum key distribution



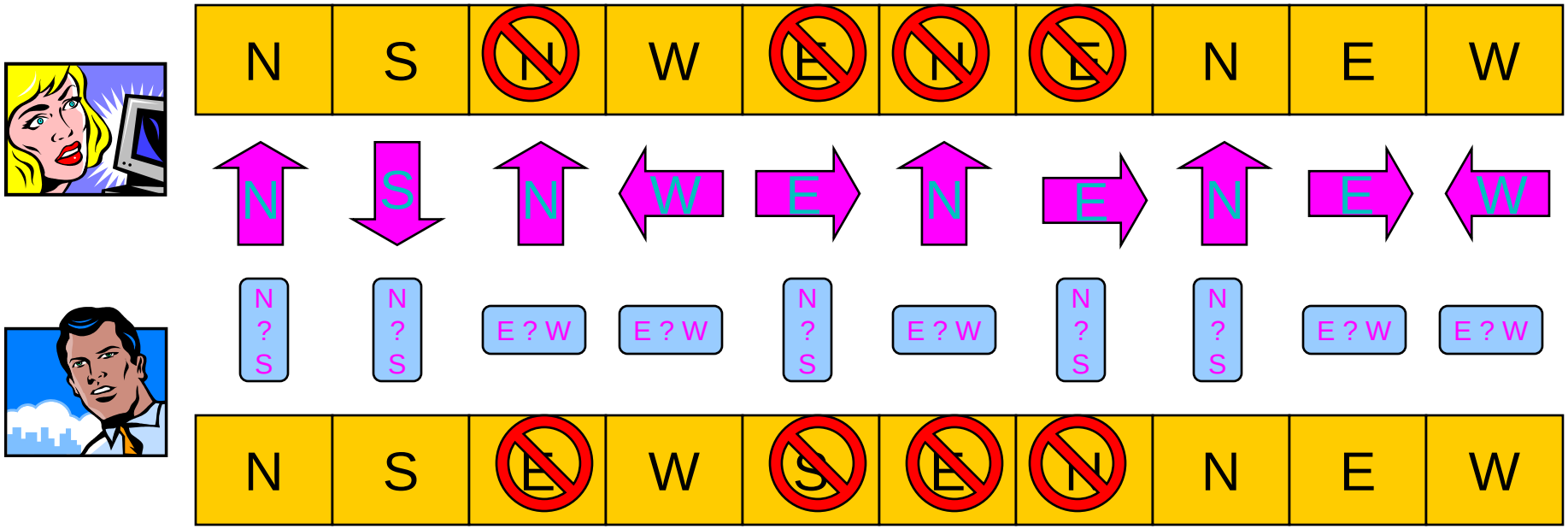
Bob sends Alice his list of measurement directions

Quantum key distribution



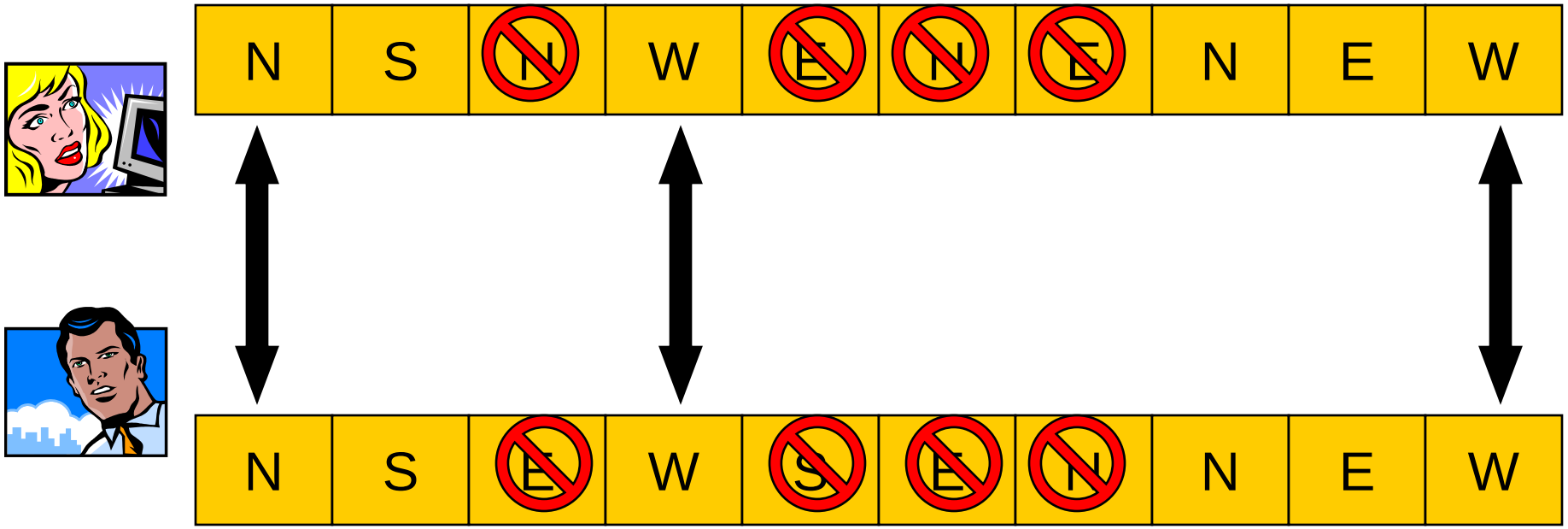
Alice tells Bob when he got it right

Quantum key distribution



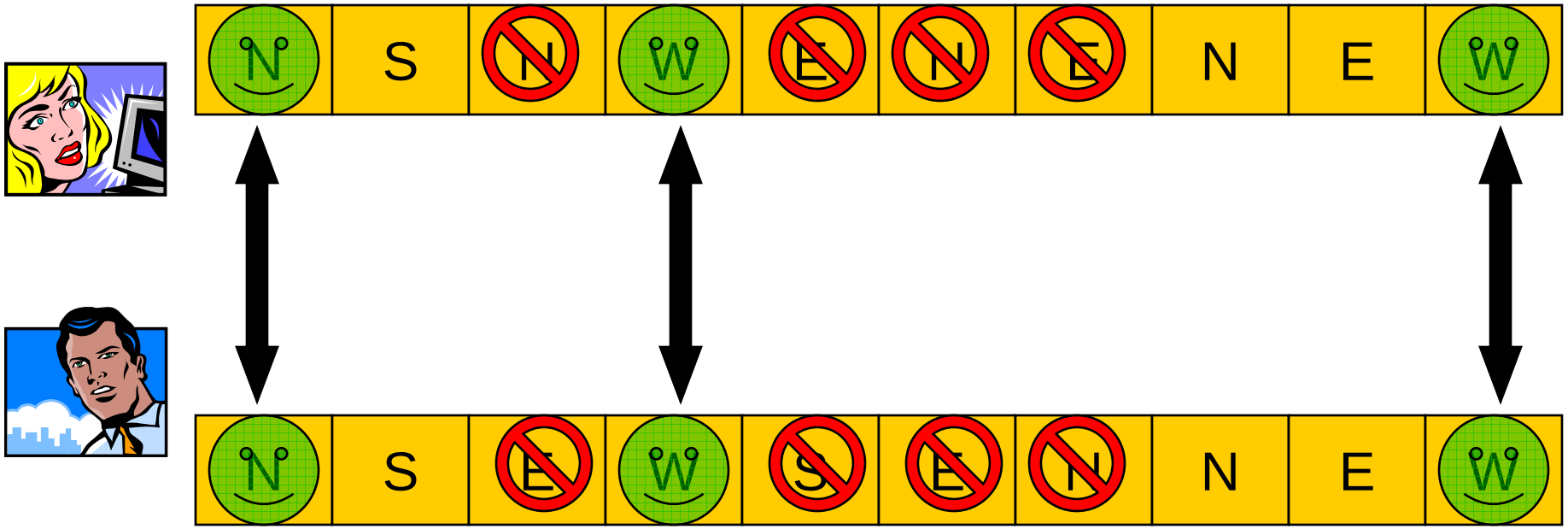
“Sifted Key” now shared by Alice and Bob

Quantum key distribution



Check the sifted key to make sure it worked

Quantum key distribution



Alice and Bob agree so everything is OK

Quantum key distribution

N	S	N	W	E	N	E	N	E	W

N	S	E	W	S	E	N	N	E	W

Alice and Bob can now use the yellow labels as a secure shared secret key

Eve's attack

- Eve's simplest attack scheme is "intercept-resend"
  - This assumes that Eve can intercept, analyse, and create single labels using the same methods as Alice and Bob
- More general attacks are available if Eve has more powerful technology
- If Eve's technology is restricted to the laws of quantum mechanics as we know them, these general attacks are ultimately no better than intercept-resend
  - If Eve could do quantum cloning, then she could break quantum cryptography. Fortunately quantum cloning is impossible!

N	S	N	W	E	N	E	N	E	W

N S N W E N E N E W

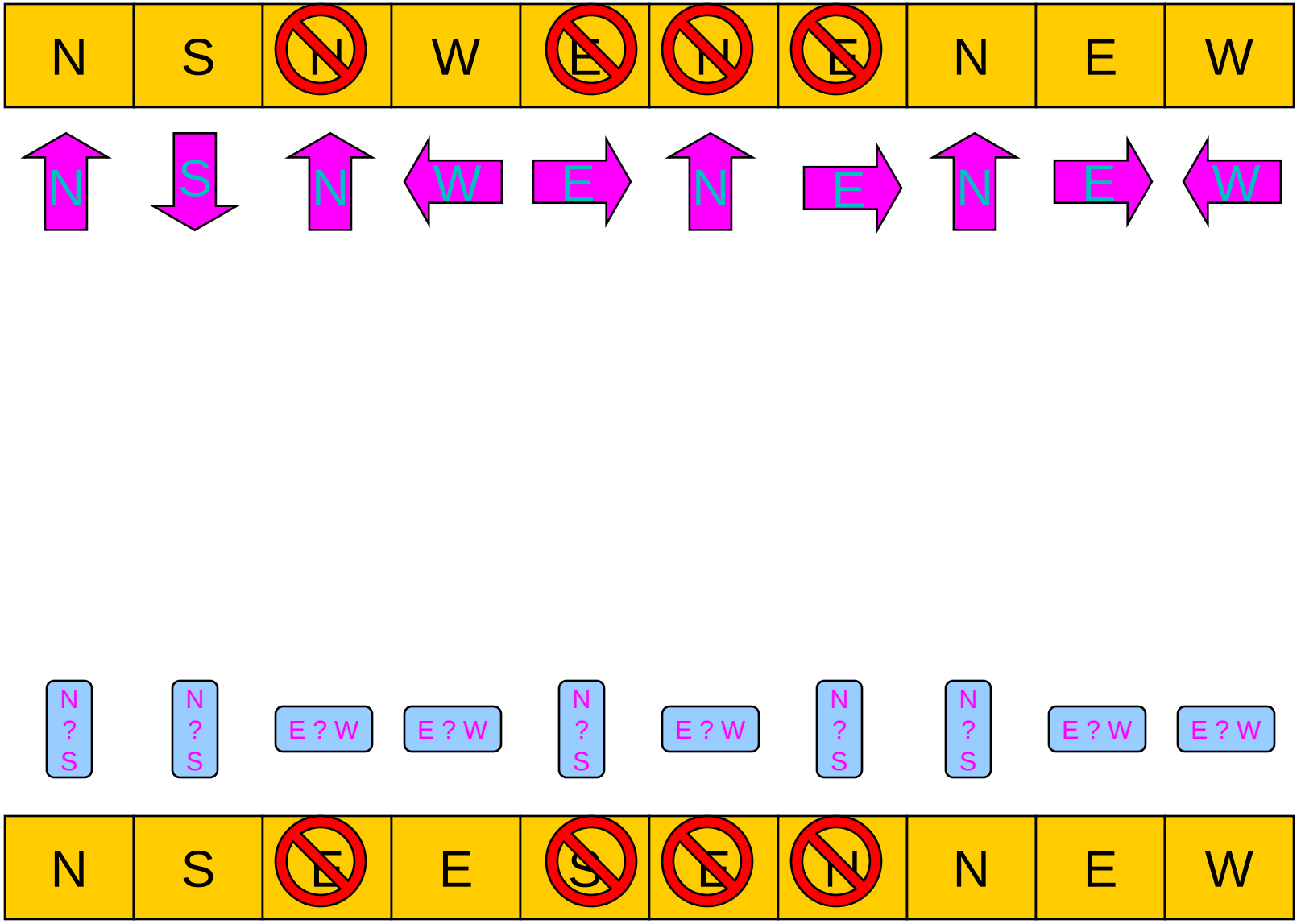
N ? S | N ? S | N ? S | N ? S | E ? W | N ? S | N ? S | E ? W | N ? S | E ? W

N	S	N	S	E	N	N	E	S	W

N S N S E N N E S W

N ? S | N ? S | E ? W | E ? W | N ? S | E ? W | N ? S | N ? S | E ? W | E ? W

N	S	E	E	S	E	N	N	E	W


N S N W E N E N E W
N S N W E N E N E W
N ? S N ? S E ? W E ? W N ? S E ? W N ? S N ? S E ? W E ? W
N S E E S E N N E W

N S N W E N E N E W

N S E E S E N N E W

N	S	N	W	E	N	E	N	E	W

Eve was listening!

N	S	E	E	S	E	N	N	E	W

Experimental imperfections

- In any real implementation of quantum cryptography there will be experimental imperfections that are manifested as errors (noise)
  - Such errors are hard to distinguish from eavesdropping
  - If the error rate is unexpectedly high, suggests that Eve is listening in, but it is wise (paranoia principle) to assume that any errors (even at normal rates) arise solely from Eve
- As long as the error rate is not too high can use a combination of classical error detection and classical privacy amplification to produce a secure clean key

Experiments

- Experimental quantum cryptography is fairly easy
  - First demonstration by Bennett *et al.* (1992), 32cm path
- Has been demonstrated using optic fibre links
  - MagiQ and ID Quantique provide commercial systems
- Free space implementations also possible
- Fairly short distance (<50km) and low rates (1kHz), but both limits could in principle be improved
- Some interest already from the military and intelligence communities and some central banks

Limitations

- Quantum cryptography is good for secrecy but cannot be used to sign public documents (some authentication of private messages is possible)
- It is a “point to point” technique and so is suited to b2b communications, not b2c
  - “Quantum telephone exchange” would solve this, but this needs the more complex Ekert scheme, not just BB84
- It is highly vulnerable to denial of service attacks
  - Quantum cryptography does not guarantee that you can communicate securely: only that you can *detect* Eve.

Impersonation attacks

- Eve could try to trick Alice by simply pretending to be Bob (or *vice versa*)
  - A problem with *any* cryptographic scheme
- Solution: Alice and Bob must exchange shared secrets (passwords) at the start of their conversation
  - Alice and Bob must meet up to exchange passwords before hand; also Alice and Bob must trust each other
  - It is essentially impossible to be sure who you are talking to *unless* you have met them before *and* you trust them!
  - Need to ensure that Eve hasn't taken over from Bob after the initial password exchange.

“Man in the Middle” attacks

- Eve could try to trick Alice and Bob by pretending to Alice that she is Bob and to Bob that she is Alice.
  - With quantum cryptography this involves setting up completely separate QC links with Alice and with Bob
  - Eve establishes separate quantum keys with Alice and Bob
  - Eve can simply pass on passwords that Alice and Bob send
  - A general problem for any cryptographic scheme
- Two main defences
  - True public channels
  - Shared secrets

Public channels

- The normal analysis of BB84 assumes that the public channel has the following properties:
  - Anyone can read any message in the channel
  - Anyone can insert any message into the channel
  - Nobody can delete a message from the channel
- Simple examples that come close:
  - Small ads in a newspaper
  - Broadcasts on CB radio
  - Usenet postings
- No-deletion (modification) rule is *extremely* useful!

Public channels

- Messages in public channels must contain sender and recipient information
  - “Hello Alice, this is Bob. My basis was …”
  - “Hello Bob, this is Alice. We used the same basis …”
- Eve must also send out such messages
- Alice will detect *two different* “Hello Alice, this is Bob” messages! Bob will also see two different messages
  - Alice and Bob will know that there is a man in the middle
- They can detect Eve, not stop her

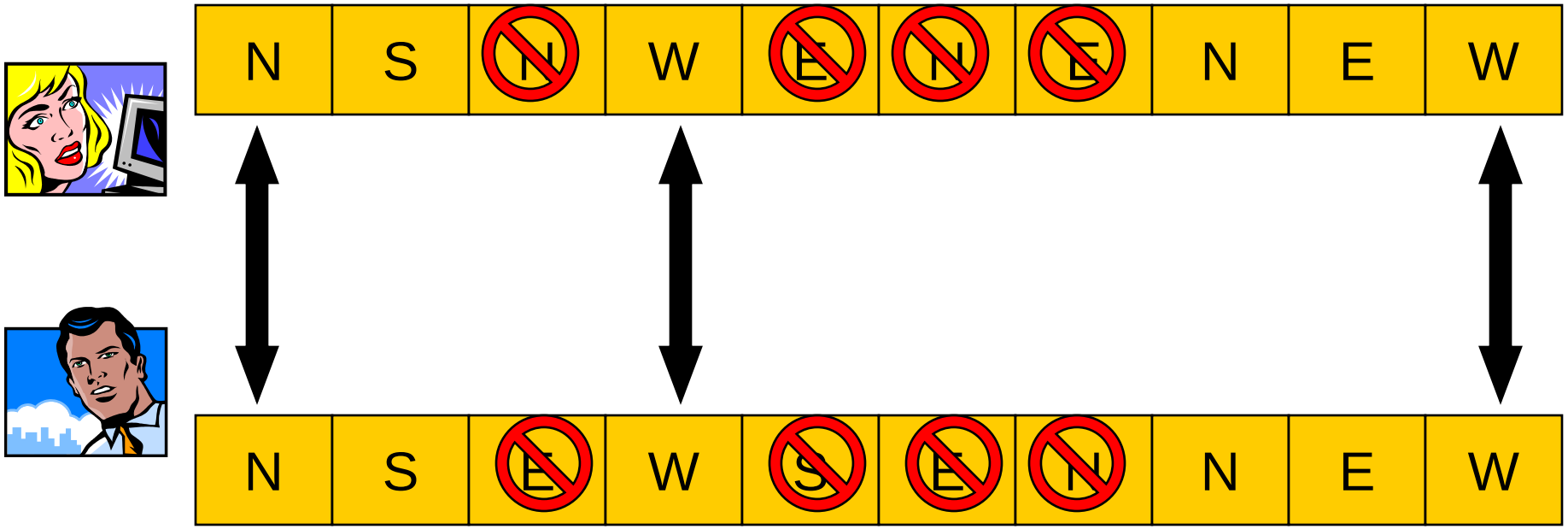
Reality

- True public channels are *extremely* rare: most channels can be silently censored
  - CB radio comes pretty close
- Current “commercial” implementations of quantum cryptography use optic fibres for both public and quantum channels (often the same optic fibre)
  - Completely vulnerable to man in the middle attacks
- Solution: shared secrets
  - Passwords aren’t enough: have to be much more cunning!
  - Somewhat like zero-knowledge proofs

Zero-knowledge proofs

- Peggy has a secret that she want to sell to Victor
  - Peggy must prove that she knows the secret
  - Victor must be able to verify Peggy's proof
  - Peggy must not reveal her secret in the process
- Victor sets random challenges which Peggy can complete if she does indeed know the secret
- This conventional form is itself highly vulnerable to man in the middle attacks, but if Alice and Bob trust one another the idea can be reversed to defeat man in the middle!

Quantum key distribution



Check the sifted key to make sure it worked

How should the check be carried out?

Checking sifted keys

- Naïve method: Bob sends Alice a set of label numbers and label results: Alice checks these. Repeat the other way round
  - Eve can just send Alice and Bob quite different lists of label numbers and results
- Better method: Alice and Bob agree beforehand which labels (chosen at random) they will check
  - Alice sends Bob her results (without numbers)
  - Bob sends Alice his results (without numbers)
  - Alice and Bob compare the sent results with their local results

Checking sifted keys: Eve

- If Eve is playing man in the middle then she has established completely separate sifted keys with Alice and Bob
- When Alice sends “random” label results, Eve doesn’t know what she should send to Bob (and *vice versa*)
  - Eve doesn’t know the pre-agreed random numbers
  - She can’t work them out from what Alice sends
  - Just forwarding Alice’s messages is pointless
- Alice and Bob will detect Eve and so defeat a man in the middle attack!

Maintaining security

- The approach above means that Alice and Bob can be sure that their connection is initially secure, but what is to stop Eve butting in later?
- Need to do repeated authentication
  - Can’t reuse the same authentication keys (Eve will eventually deduce them)
  - Can’t assume an indefinite supply of keys
- Solution: Alice and Bob use part of their secure key to transmit *new* authentication keys to each other
  - Quantum key expansion / Quantum secrecy growing

Summary

- Quantum computers threaten to destroy existing public key cryptography schemes
  - Not yet clear whether/when we can build one
- Quantum cryptography is brilliant for secrecy
  - Experimentally straightforward
  - Need to be very careful with detailed implementation
  - Current forms are b2b not b2c
- Almost useless for authentication
  - No digital contracts, etc.
- Who knows what else is out there?