# A short introduction

# to quantum physics

B. Škorić, Physical Aspects of Digital Security, Chapter 8 and 9

# Bluff your way in quantum physics

- Quantum state is unit-length vector in Hilbert space
  - contains all physical information
  - denoted as $|\text{parameters}\rangle$
- Observable: Hermitian operator
  - eigenvalues $\lambda_i$ = possible measurement outcomes
  - basis of orthonormal eigenvectors $|\lambda_i\rangle$
- "Superpositions", e.g. $|\psi\rangle = ( |0\rangle + |1\rangle )/\sqrt{2}$
- Measurement of A projects state onto eigenstate of A
  - non-deterministic: Prob[outcome $\lambda$] = $| \langle\lambda|\psi\rangle |^2$.
  - destruction of state information!
- Evolution is unitary operator

With his rectilinear logic, Dirac named each part of the bracket after its first and last three letters, *bra* and *ket*, new words that took several years to reach the dictionaries, leaving thousands of non-English speaking physicists wondering why a mathematical symbol in quantum mechanics had been named after an item of lingerie. They were not the only ones to be flummoxed. A decade later, after an evening meal in St John's, Dirac was listening to dons reflecting on the pleasures of coining a new word, and, during a lull in the conversation, piped up with four words: ***I invented the bra***.

-- From *The strangest man* by G. Farmelo

Paul Dirac

# The no-cloning theorem

Wootters+Zurek 1982, Dieks 1982

- Time evolution = unitary operator acting on state.

- There is no generic evolution operator U that achieves

$$U\,|\psi\rangle \otimes |e\rangle = |\psi\rangle \otimes |\psi\rangle \qquad \text{for all } |\psi\rangle$$

Executive summary for cryptographers:

- **measuring kills info**
- **no cloning of unknown state**

# Quantum Key Distribution

*Key distribution for the truly paranoid*

# Quantum Key Distribution

What is achieved:

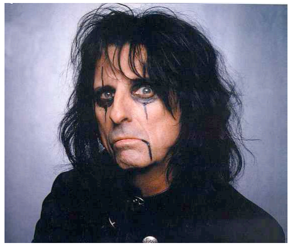
- Alice and Bob generate a random shared key from scratch
- Eavesdropping gets detected
- *Unconditional* secrecy of key
- Requirement: authenticated classical channel

How is this possible?

- Ingenious use of quantum physics
  - unpredictable outcome of measurements
  - inbuilt tamper evidence
- ... and some classical crypto tricks

# The BB84 protocol (Bennett + Brassard 1984)

| basis | b | $\psi$ |
|---|---|---|
| × | 0 | ⤡ |
| × | 1 | ⤢ |
| + | 0 | ↔ |
| + | 1 | ↕ |



Random basis.
Random bit b.

$|\psi\rangle$ →

Random basis.
Measure b'.

repeat n times

← all basis choices

Keep events with equal basis: subset E.
Small random set $S \subset E$.

E, S →

← $b'_S$

Check if $b_S \approx b'_S$.

Shared secret $b_{E\backslash S} \approx b'_{E\backslash S}$.

- Error correction
- Privacy amplification

# BB84: what it achieves

Initial situation

- short initial key for MAC

After running the protocol

- arbitrarily long key
- unconditional security
- tampering gets detected

# Intercept-resend attacks

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Alice's state | $\leftrightarrow$ | $\leftrightarrow$ | $\updownarrow$ | $\updownarrow$ | $\nwarrow\!\!\searrow$ | $\nwarrow\!\!\searrow$ | $\swarrow\!\!\nearrow$ | $\swarrow\!\!\nearrow$ |
| Eve's basis | $+$ | $\times$ | $+$ | $\times$ | $+$ | $\times$ | $+$ | $\times$ |
| Eve's outcome | $\leftrightarrow$ | $\nwarrow\!\!\searrow$ or $\swarrow\!\!\nearrow$ | $\updownarrow$ | $\nwarrow\!\!\searrow$ or $\swarrow\!\!\nearrow$ | $\leftrightarrow$ or $\updownarrow$ | $\nwarrow\!\!\searrow$ | $\leftrightarrow$ or $\updownarrow$ | $\swarrow\!\!\nearrow$ |
| Bob's basis | $+$ | $+$ | $+$ | $+$ | $\times$ | $\times$ | $\times$ | $\times$ |
| Bob's outcome | 0 | 0 or 1 | 1 | 0 or 1 | 0 or 1 | 0 | 0 or 1 | 1 |

*Possible events occurring when Alice and Bob choose the same basis and Eve does an intercept-resend attack.*
*- Where there are two possibilities listed (red columns), the probabilities are 1/2.*
*- Whenever Eve guesses the correct basis, she does not disturb the photon and learns its state.*
*- Whenever she guesses wrong, Bob has a 50% probability of getting the wrong outcome.*

Overall prob. of disturbing a bit: 25%

# State of the art

- QKD demonstrated over more than 140 km
  - through fibre optic cable
  - through air (Canary islands)
  - Earth to orbit should be possible!
- Commercially available
  - ID Quantique (Geneva)
  - Quintessence (Australia)
  - SmartQuantum (France)
  - MagiQ (USA)