

The Cryptography and Security Group

- Quantum Cryptography

Ivan Damgård

DAIMI, Aarhus University



The Cryptography Group



Senior: Ivan Damgård, Jesper Buus Nielsen

Postdoc: Tomas Toft

PhD students: Rikke Bendlin, Jakob Funder, Martin Geisler, Mikkel Krøigaard, Carolin Lunemann, Sigurd Meldgaard, Gert Mikkelsen, Claudio Orlandi, Rune Thorbek.

www.daimi.au.dk/~jbn/crypto

The Cryptography Group

Research:

- Cryptographic protocols (e.g. secure electronic auctions, elections, etc.)
- Public-key cryptography, (e.g. practical systems for digital signatures)
- Quantum Cryptography – the subject today.

Password Based Authentication

A user U wants to identify himself to a computer system, say a server S .

U has a password pw , S also knows pw

How does S check that U has the correct password?

Standard solution: U sends pw to S

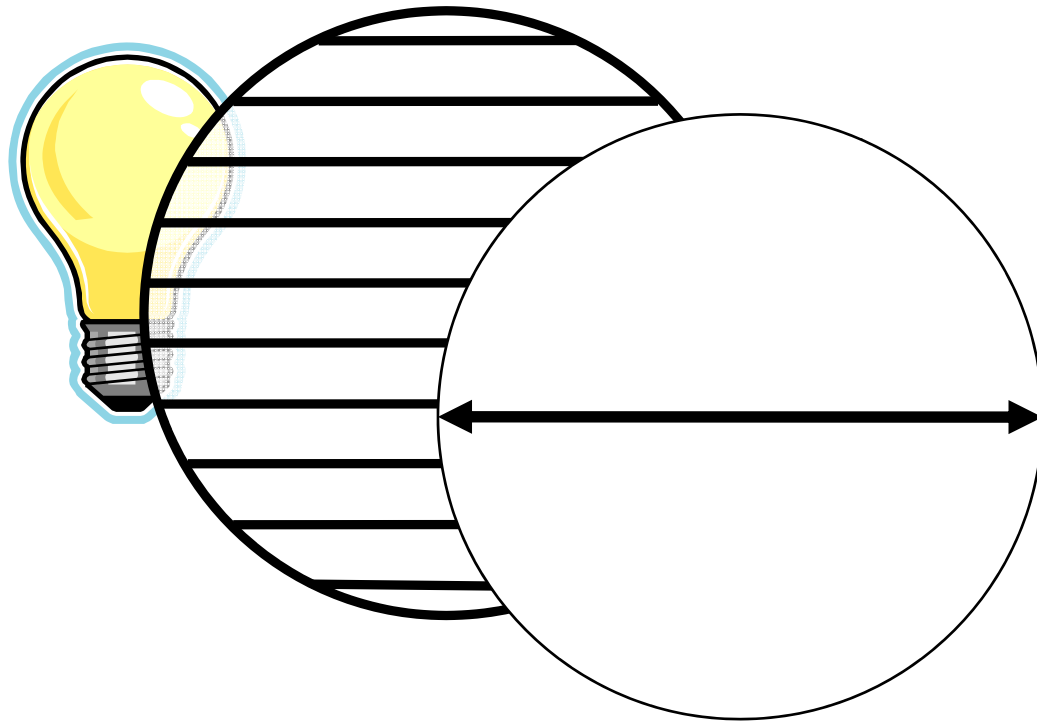
Problems:

- pw could be eavesdropped
- what if U is not really talking to S ?

Several solutions exist, but always based on assumptions we hope are true, we do not know for sure. Quantum cryptography offers an alternative..

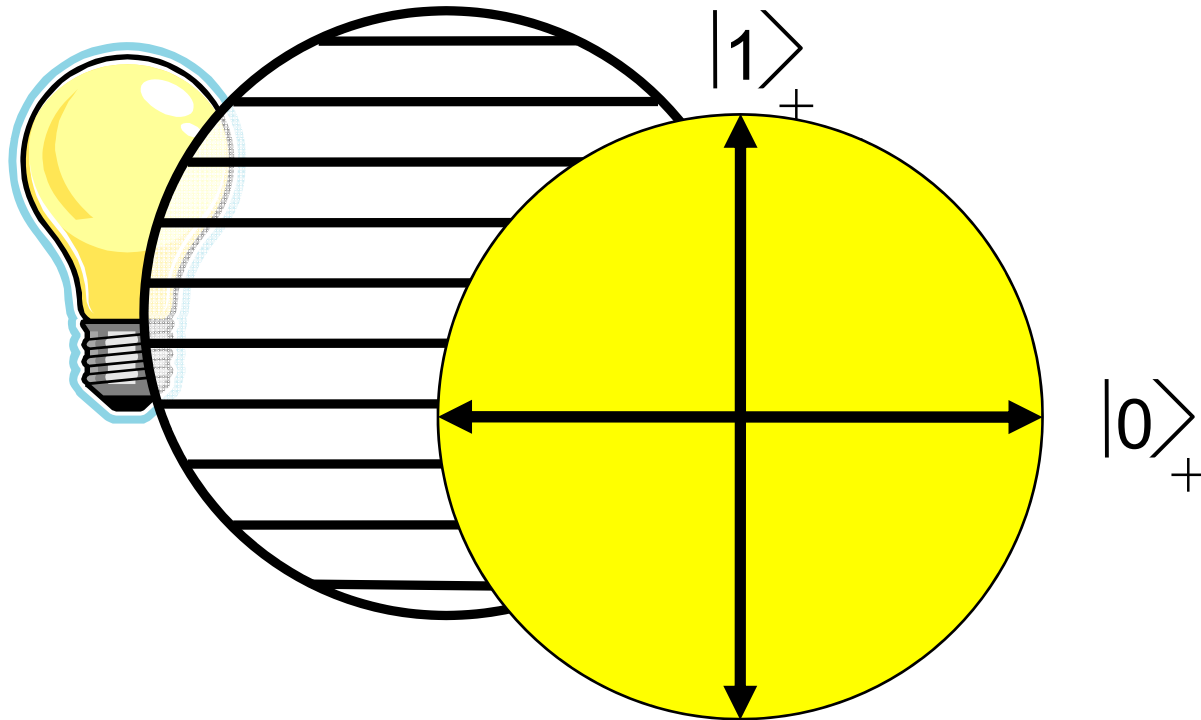
Quantum Communication

- A new way to communicate. Example: Polarized light



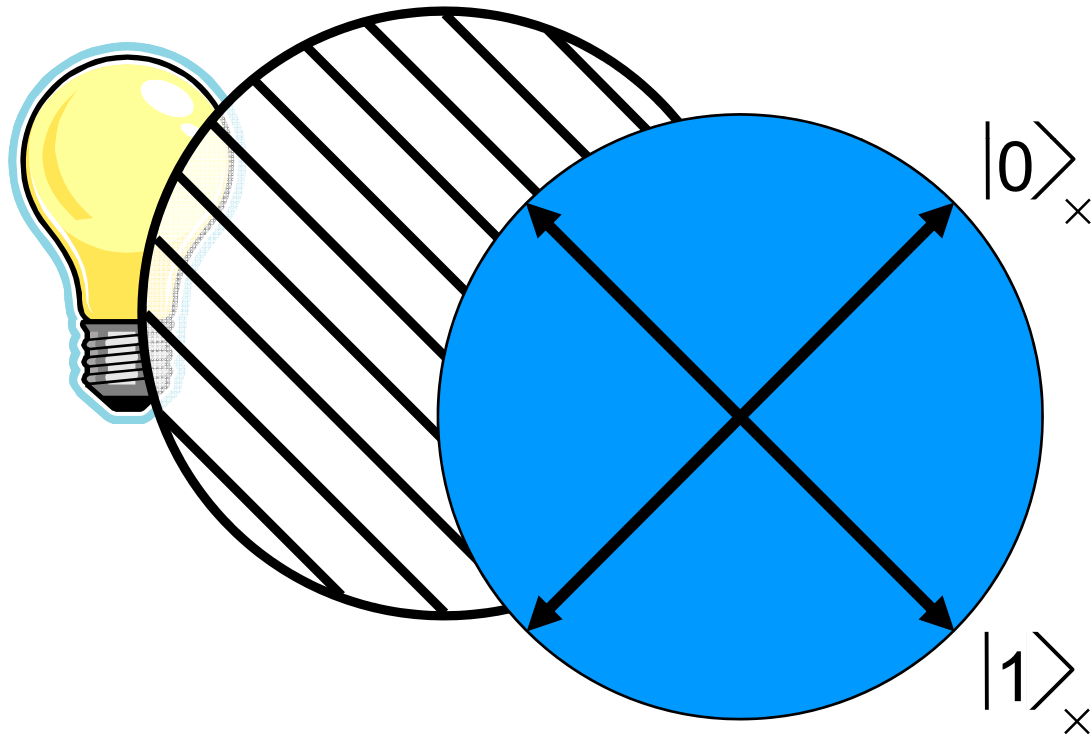
Quantum Communication

- Sending a bit using 1 photon



Quantum Communication

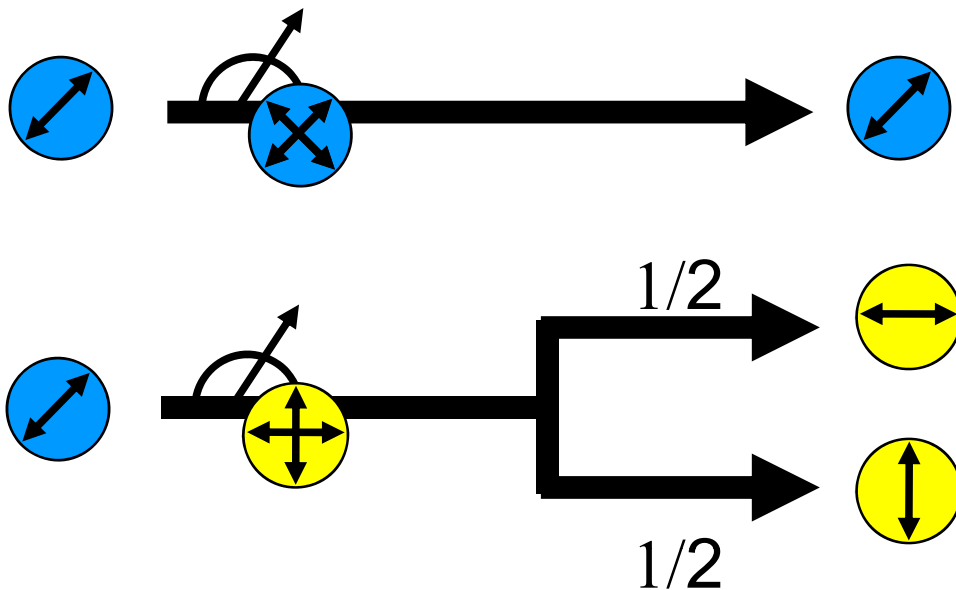
- Sending a bit using a different way to encode.



Receiving Quantum Information

Wrong measurement: useless result

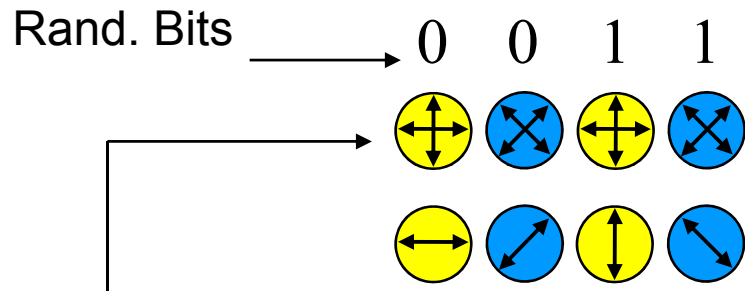
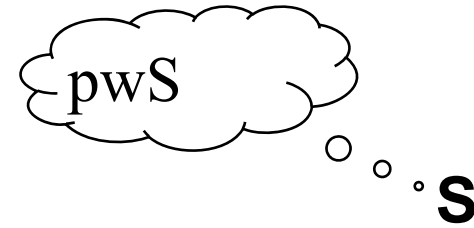
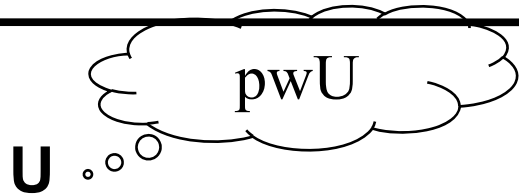
Correct measurement: everything is fine



Quantum Facts

- Once you have looked at photon and received a result, no turning back: the photon forgot what it was like before
- Hence, making the wrong measurement also means you have wiped out the information the photon was carrying
- Make a copy of the photon before you measure? Sorry, not possible, by basic laws of physics!
- We can pack information such that: use the right way to unpack, or lose the information altogether.

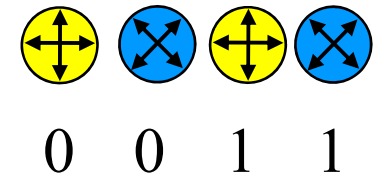
Quantum Password Check



Choose encodings according to pwU

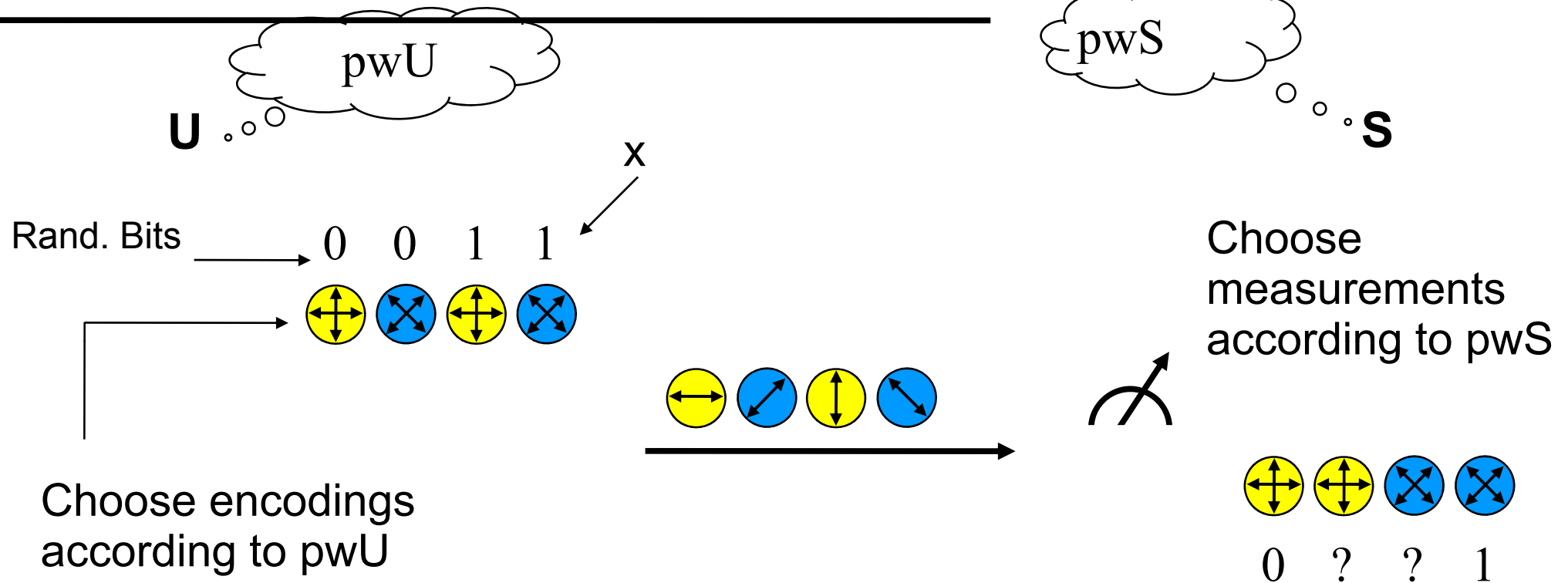


Choose measurements according to pwS



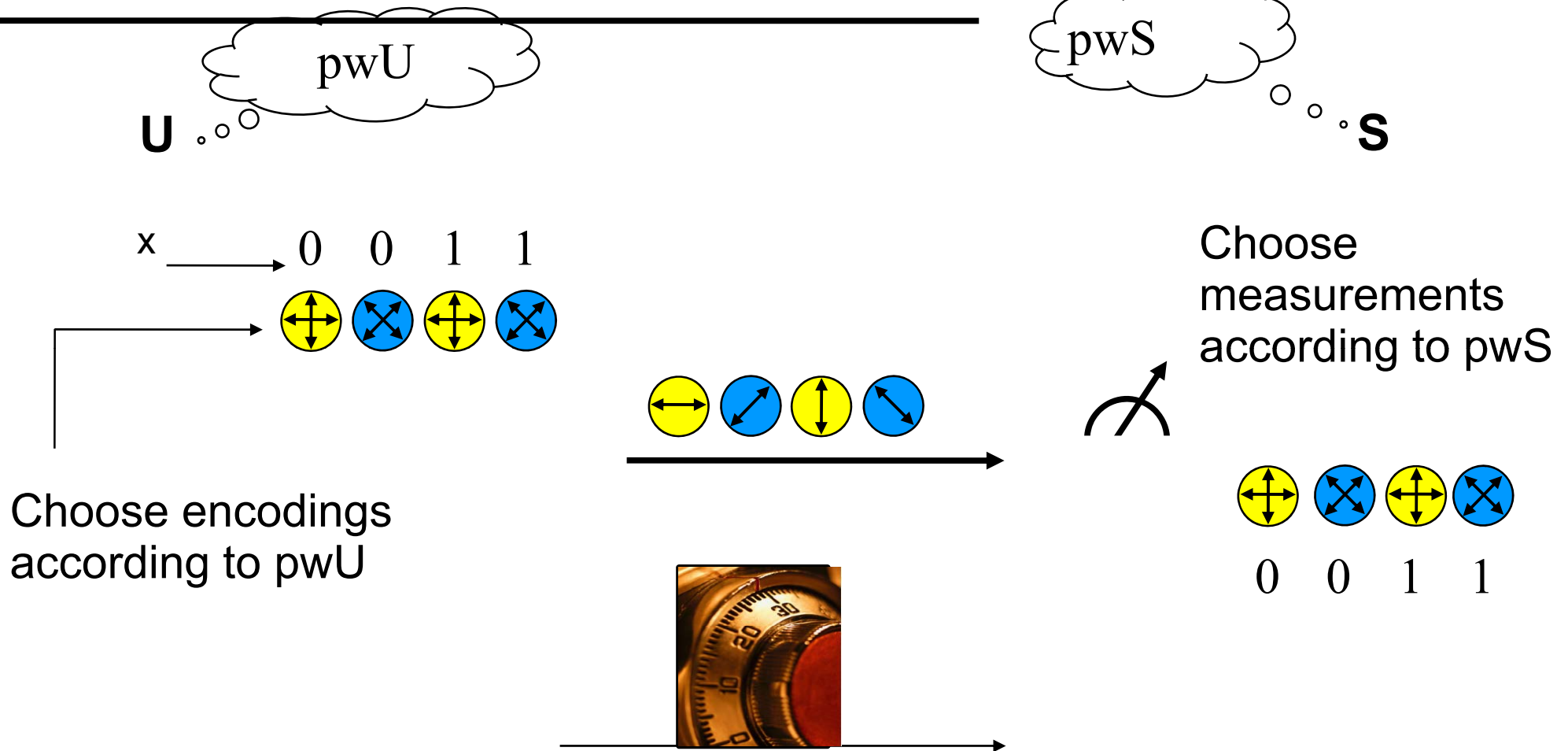
.. if the passwords match

Quantum Password Check



If passwords are different, S does not know how to unpack

Quantum Password Check



Box containing pwU

But locked, and x is the combination!

If S has the right password, can open and see that the right thing is inside

If not, pwU is **completely** hidden

Doing it for real

Mobile quantum security (MOBISEQ)

A project we do with Physics in Aarhus

Implements methods for identification and other tasks using quantum communication.

Use small mobile components.