HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

Kvantuminformatikai rendszerek építőelemei

Kvantuminformatikai alkalmazások, 2025. ősz

2025. október 29.

Dr. Bacsárdi László, Dr. Imre Sándor

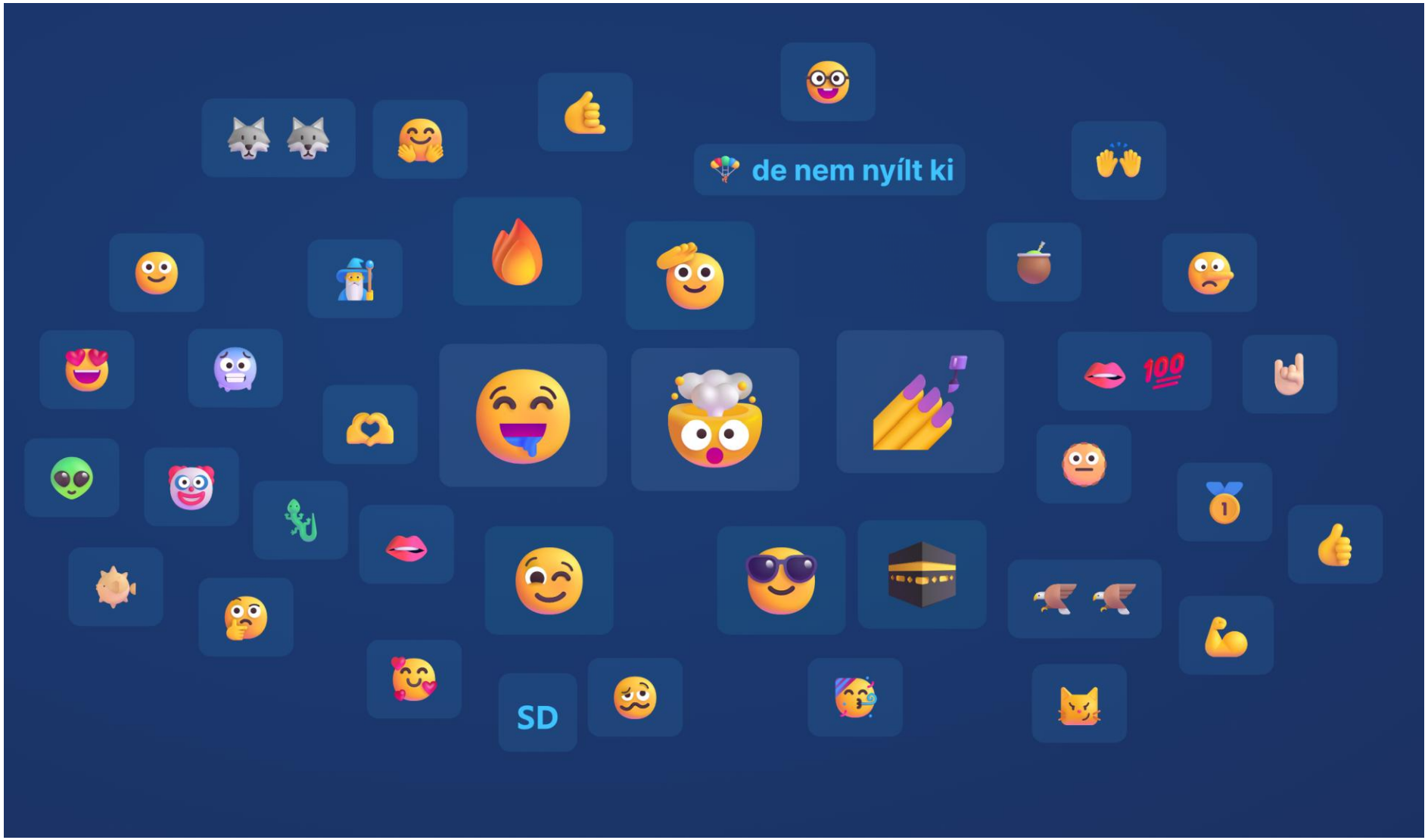
BME Villamosmérnöki és Informatikai Kar

bacsardi@hit.bme.hu

MŰEGYETEM 1782

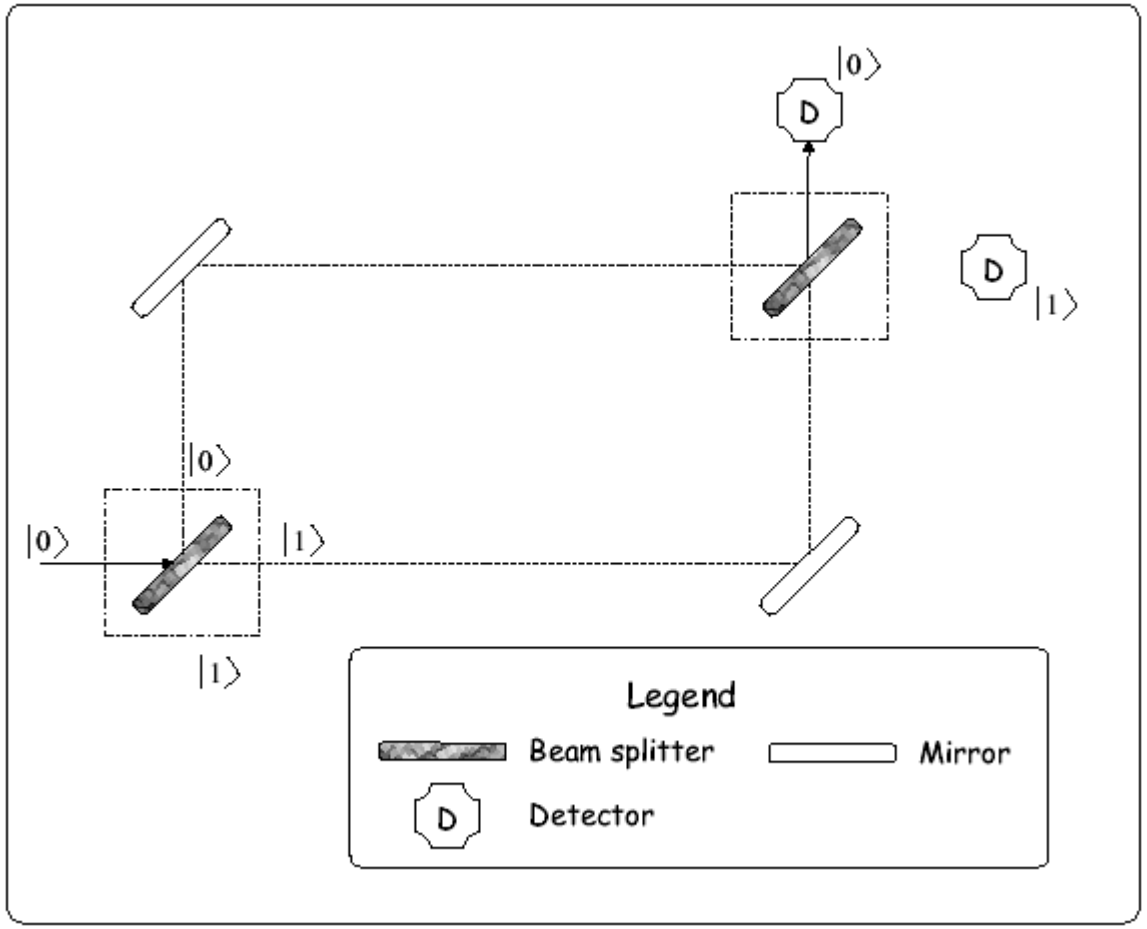
AZ 1. KIS ZÁRTHELYI UTÁN

MENNYIRE VOLT JÓ AZ ELSŐ KIS ZÁRTHELYI?

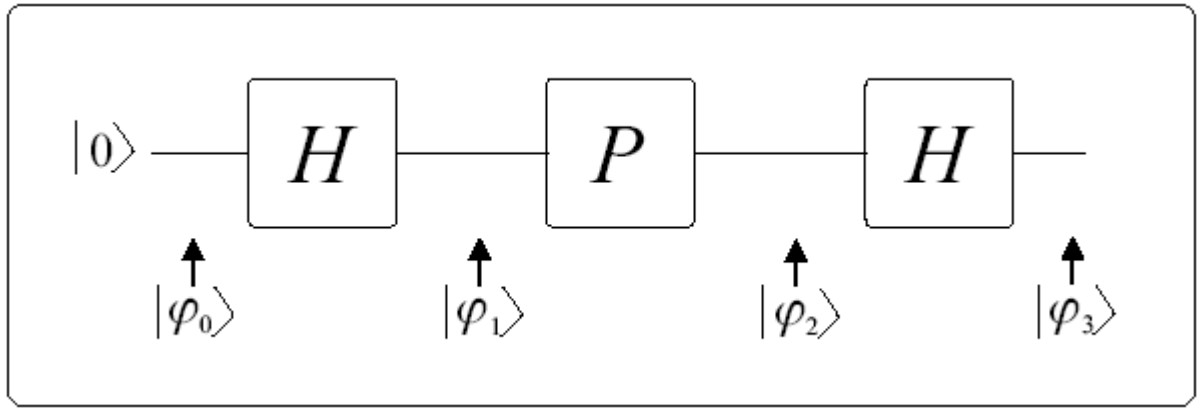


ÖSSZEFOGLALÁS A KORÁBBI ÓRÁKRÓL

INTERFEROMETER – KÍSÉRLET



INTERFEROMETER – ÁRAMKÖR

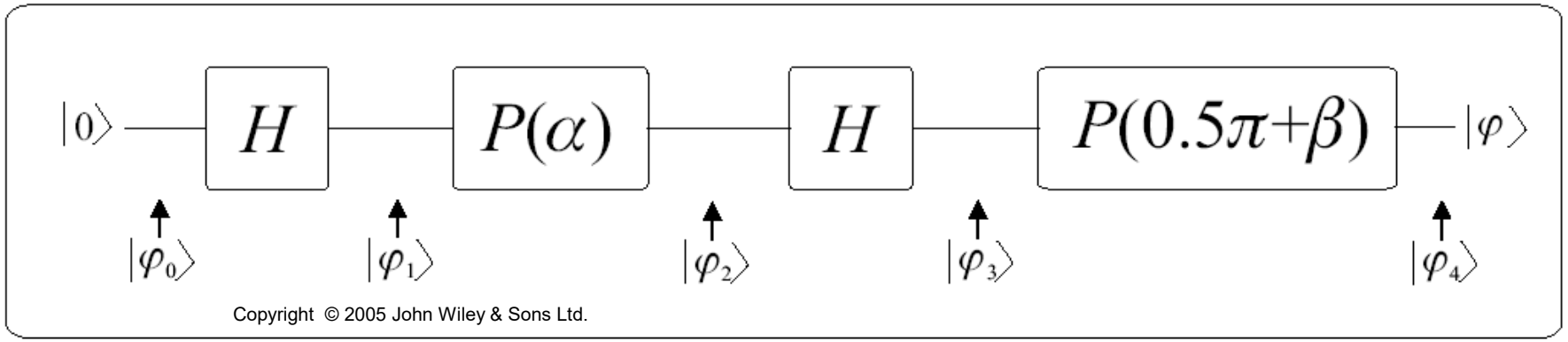


$$\mathbf{P} = \begin{bmatrix} e^{j\alpha_0} & 0 \\ 0 & e^{j\alpha_1} \end{bmatrix}$$

NO CLONING TÉTEL

- Nem készíthető olyan unitér kvantumkapu, amivel tetszőleges kvantumállapot-halmaz hibamentesen másolható.
- De
  - Ortogonális állapotok halmaza másolható!
  - Ismert állapot másolható!
- Hogyan?

TETSZŐLEGES ÁLLAPOT ELŐÁLLÍTÁSA



A KVANTUMKOMMUNIKÁCIÓ EREJE

Most *(és a következő években):*

Kvantum alapú kulcsszétosztás

QKD (quantum key distribution)

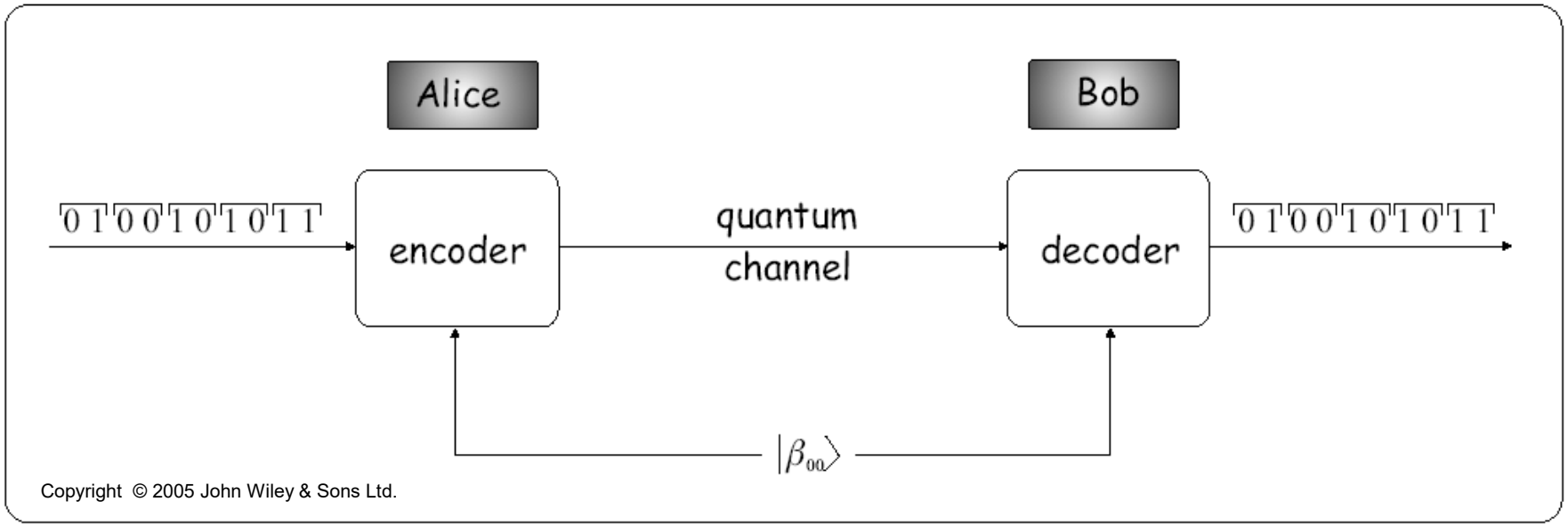
biztonsági szint növelése

A *(nem olyan távoli)* **jövőben:**

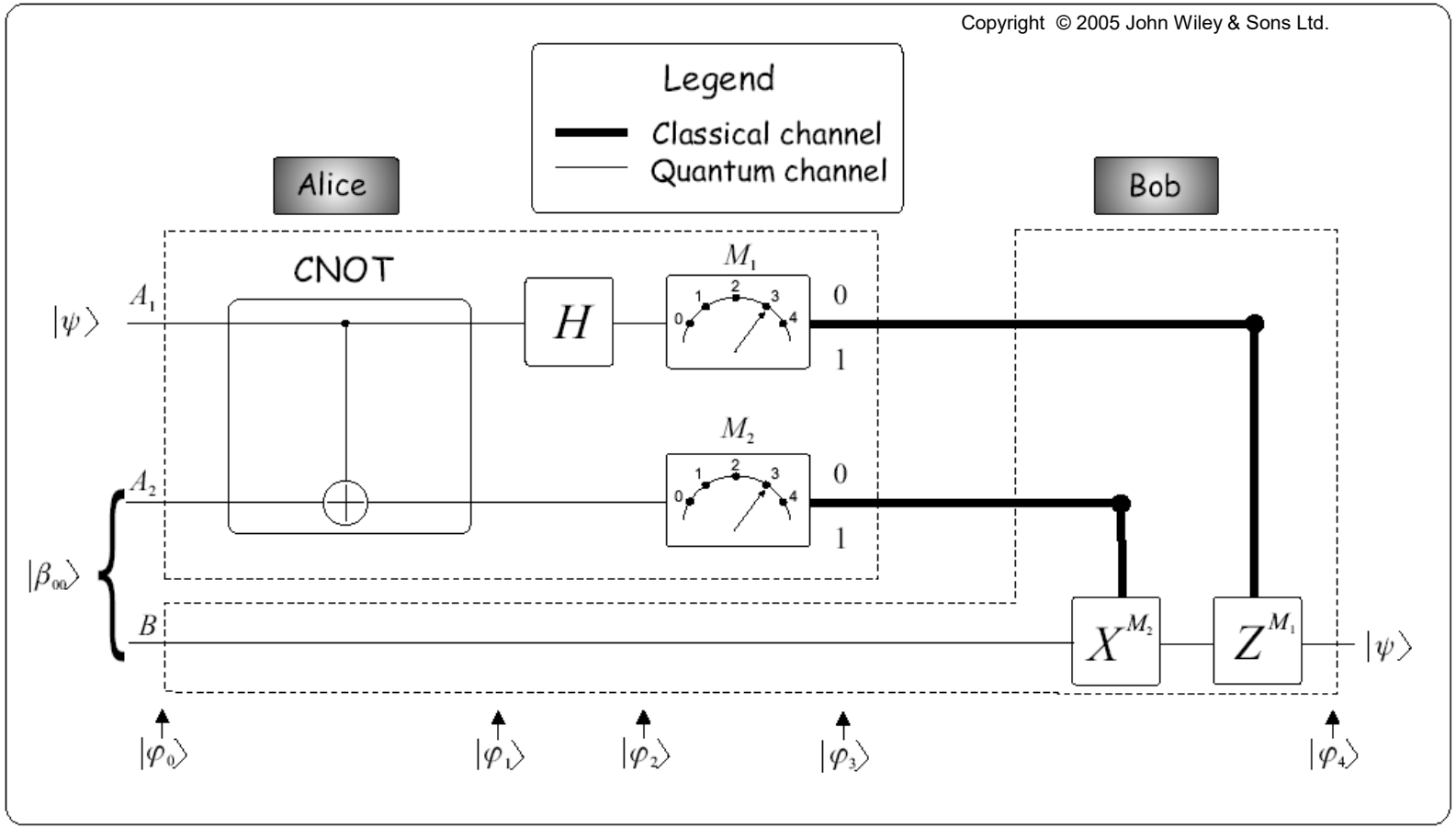
Kvantuminternet

kvantumeszközök összekapcsolása

SZUPERSŰRŰ TÖMÖRÍTÉS



KVANTUMTELEPORTÁCIÓ



PROTOKOLLOK

- **Szupersűrű tömörítés**: klasszikus információ továbbítása kvantumcsatornán összefonódás használatával *(Bell-állapotok)*
- **Teleportáció:** kvantuminformáció továbbítása klasszikus csatornán összefonódás használatával *(Bell-állapotok)*

QKD

Biztonság a kvantumfizika törvényein

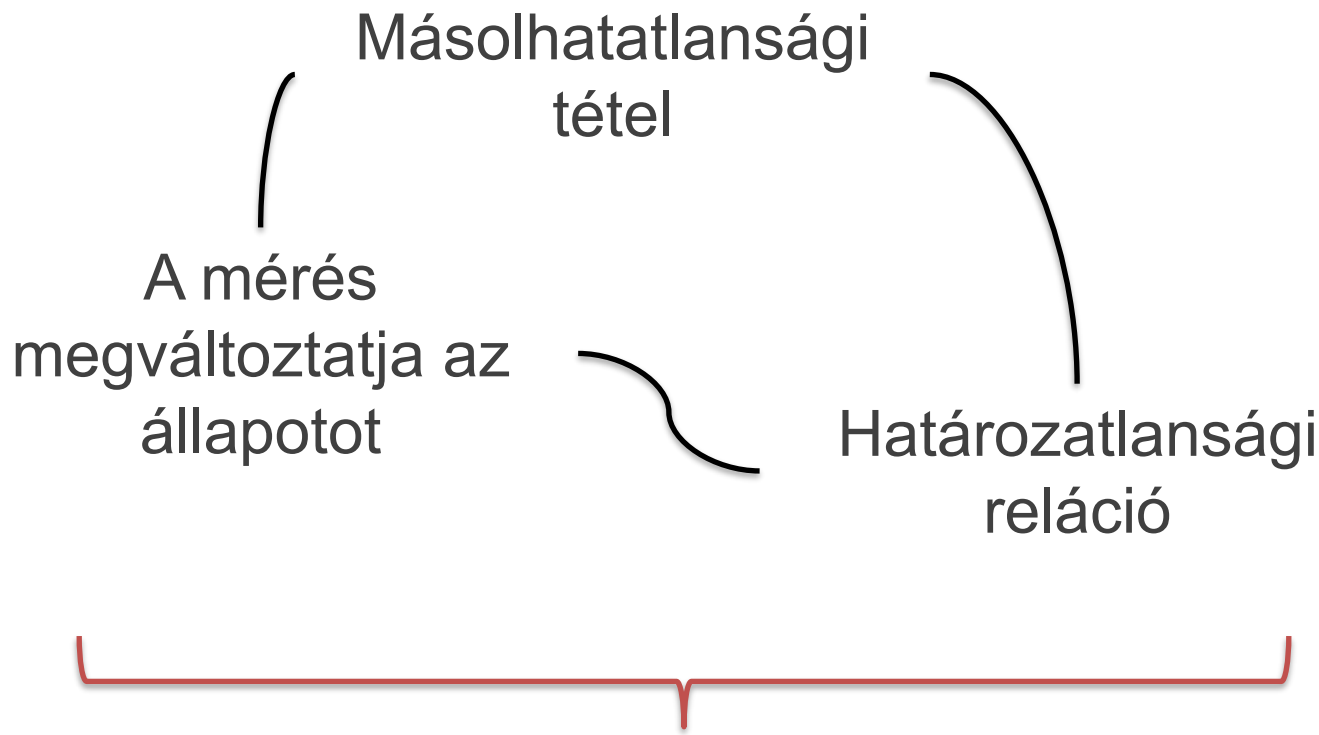
Kompatibilitás a szimmetrikus kulcsú algoritmusokkal

Csatorna optikai szálon vagy szabadtéren

Termékek kereskedelmi forgalomban

Számos startup cég Európában

MÉRÉS

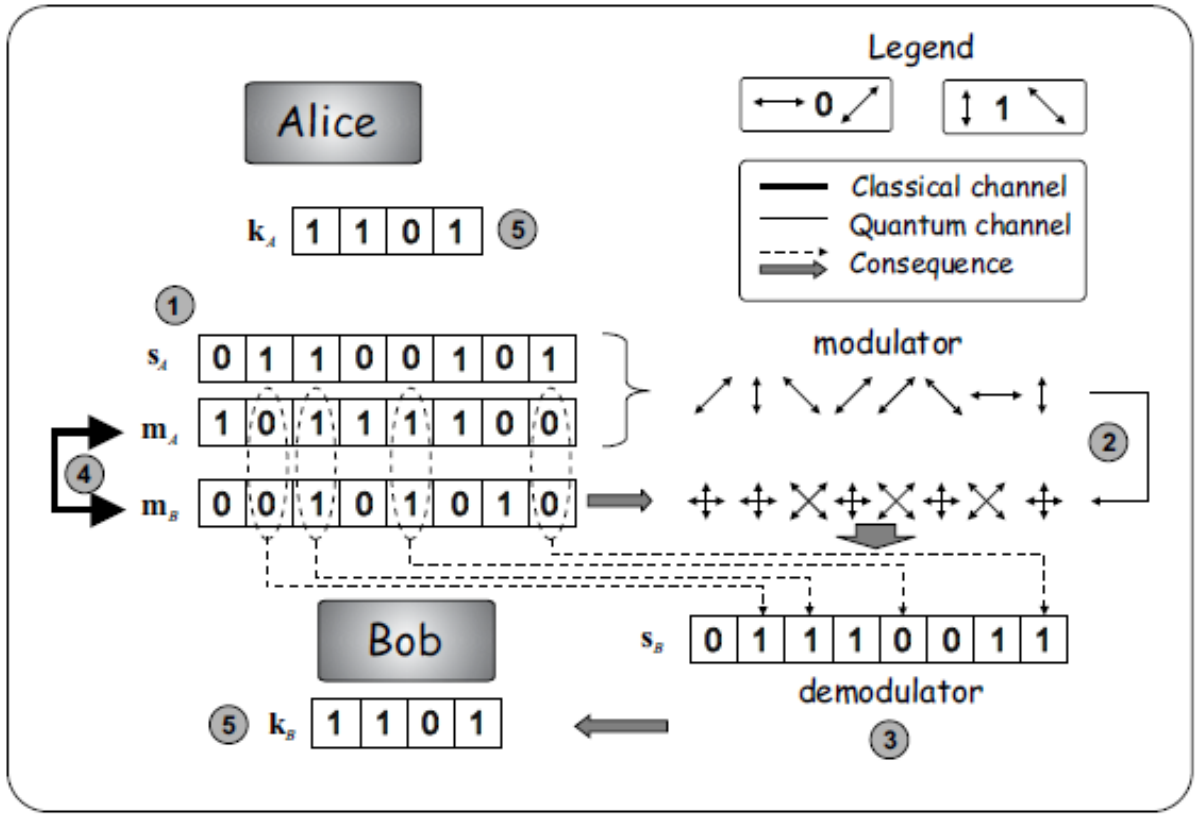


A kvantuminformációt nem lehet tökéletesen megismerni

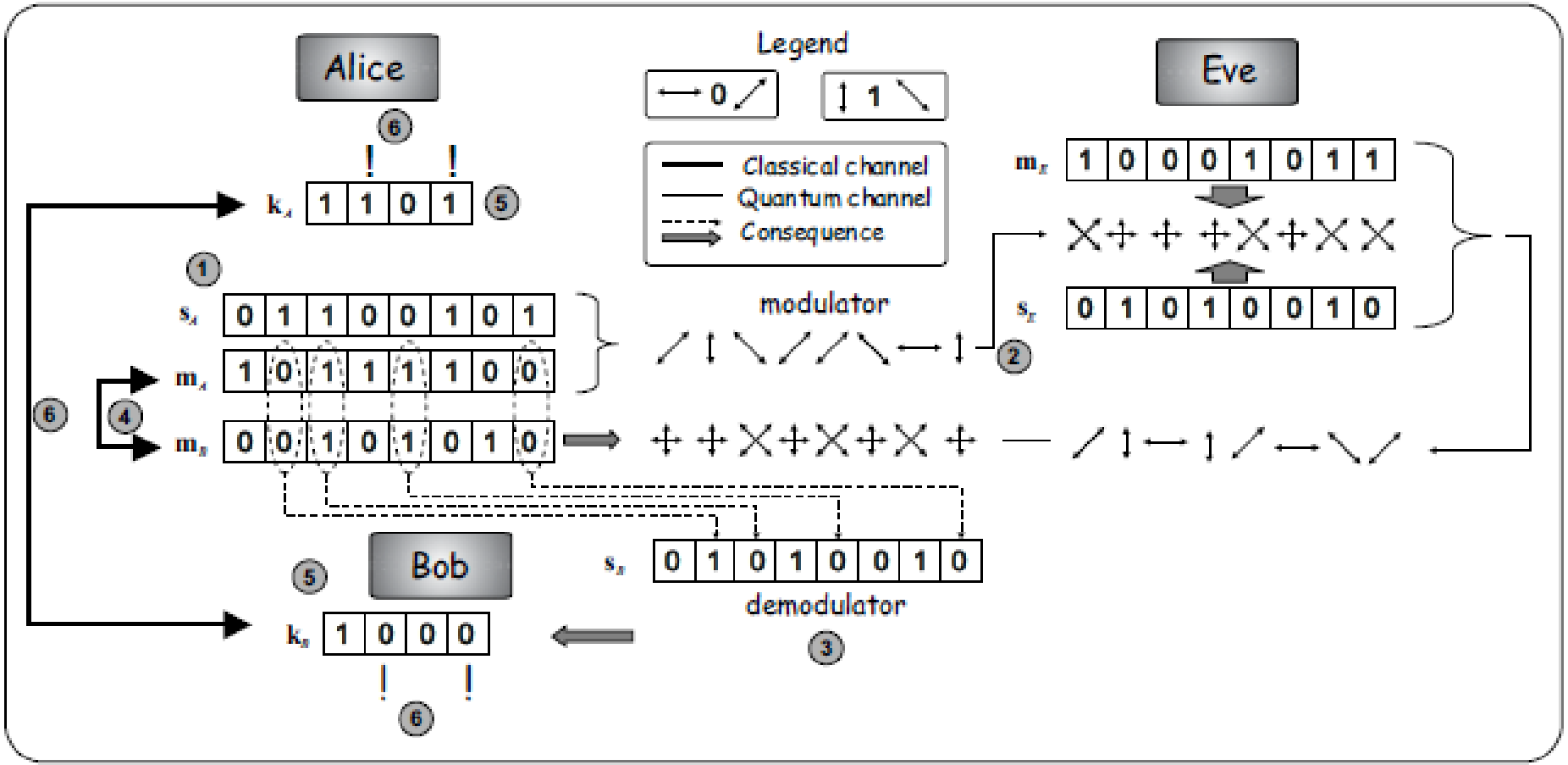
BB84 QKD PROTOKOLL

Első generációs megoldás

- Fotonok polarizációs állapota a kvantumbit
- Kihívás: egyfotonok előállítása és detektálása



TÁMADÁSI KÍSÉRLET



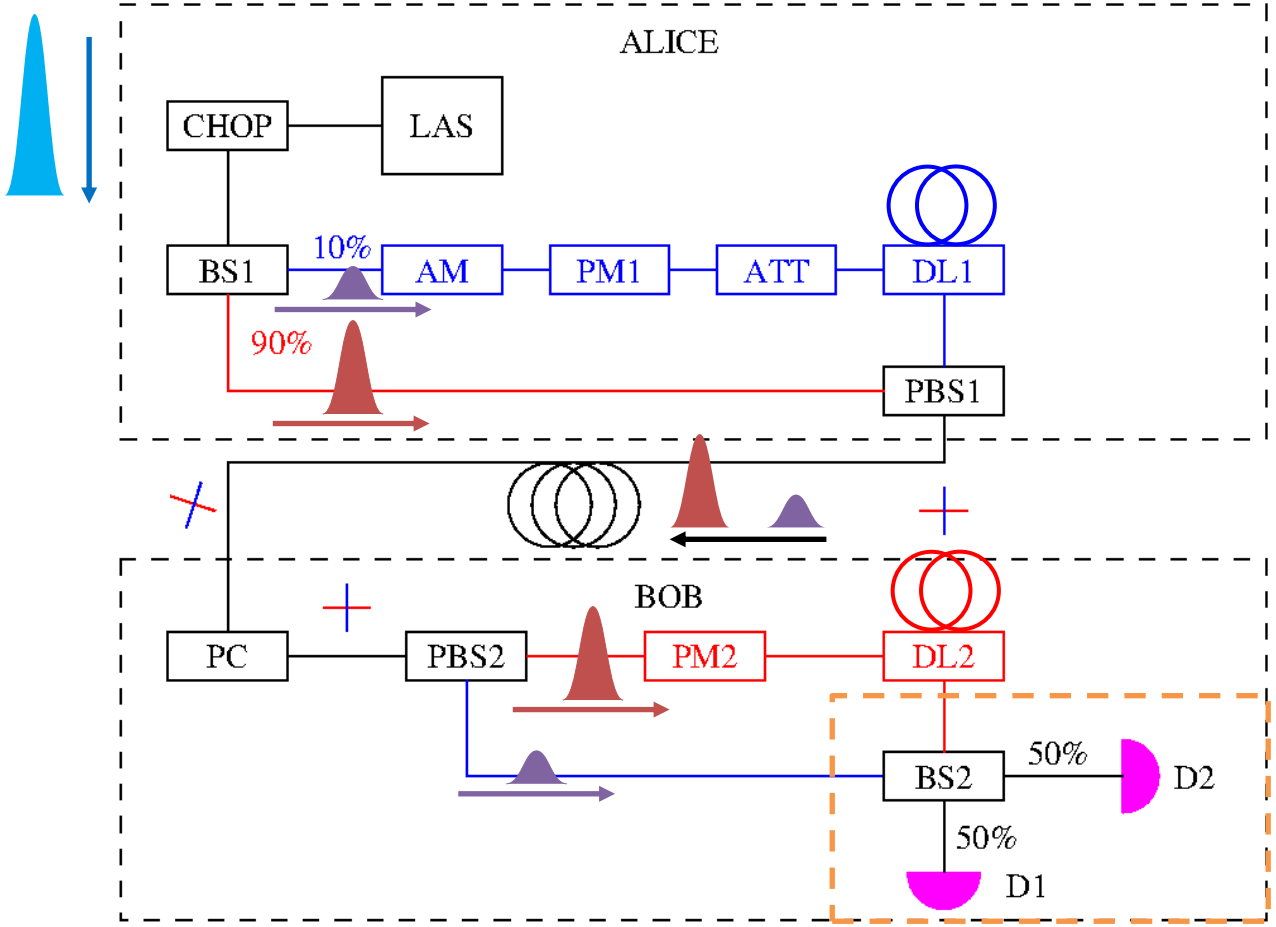
NEM IDEÁLIS KVANTUMCSATORNA

- A lehallgatás növeli a BER-t (bit error rate)
  - Kvantumos esetben: QBER (quantum bit error rate)
- A gyakorlatban a kvantumcsatorna zajos, azaz a QBER lehallgatás nélkül sem nulla
- Hogyan különböztetjük meg a támadót a zajtól?
  - Eve megjelenése megnöveli a csatorna alapzaját

- Amíg csak kevés hiba
  - Privacy amplification
  - Kisebb, de biztonságosabb kulcs
  - Feltétele, hogy Aliz és Bob közti csatorna kapacitása nagyobb legyen mint az Aliz és Éva közti csatornáé

$$C(N) = \max_{p(x)} I(A:B) \qquad C_{AB}\text{-}C_{AE} > 0$$

CSAK ZÁRÓJELBEN: MÁSODIK GENERÁCIÓS QKD



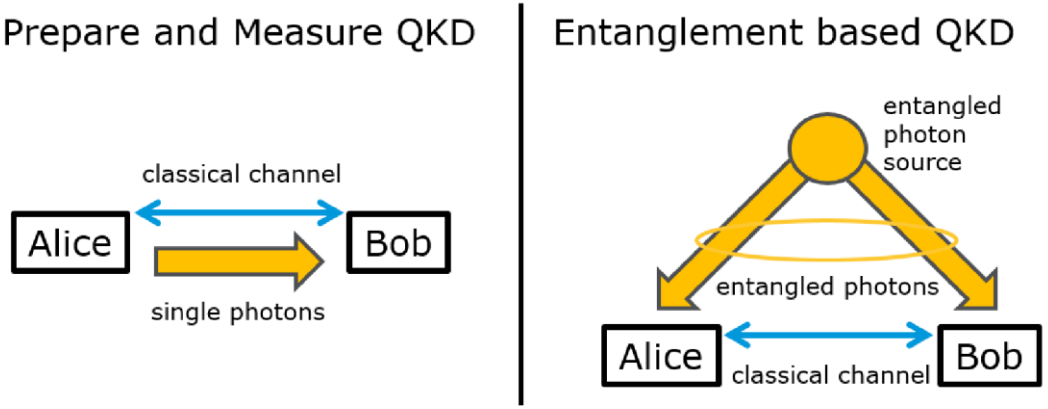
Homodin detektálás

Mráz A, Kis Z, Imre S, Gyongyosi L, Bacsardi L
Quantum circuit-based modeling of continuous-variable quantum key distribution system
Int. Journal of Circuit Theory and Applications 45:(7), 2017

QKD-PROTOKOLLOK

Két típus

① Előállít és megmér ② Összefonódáson alapuló

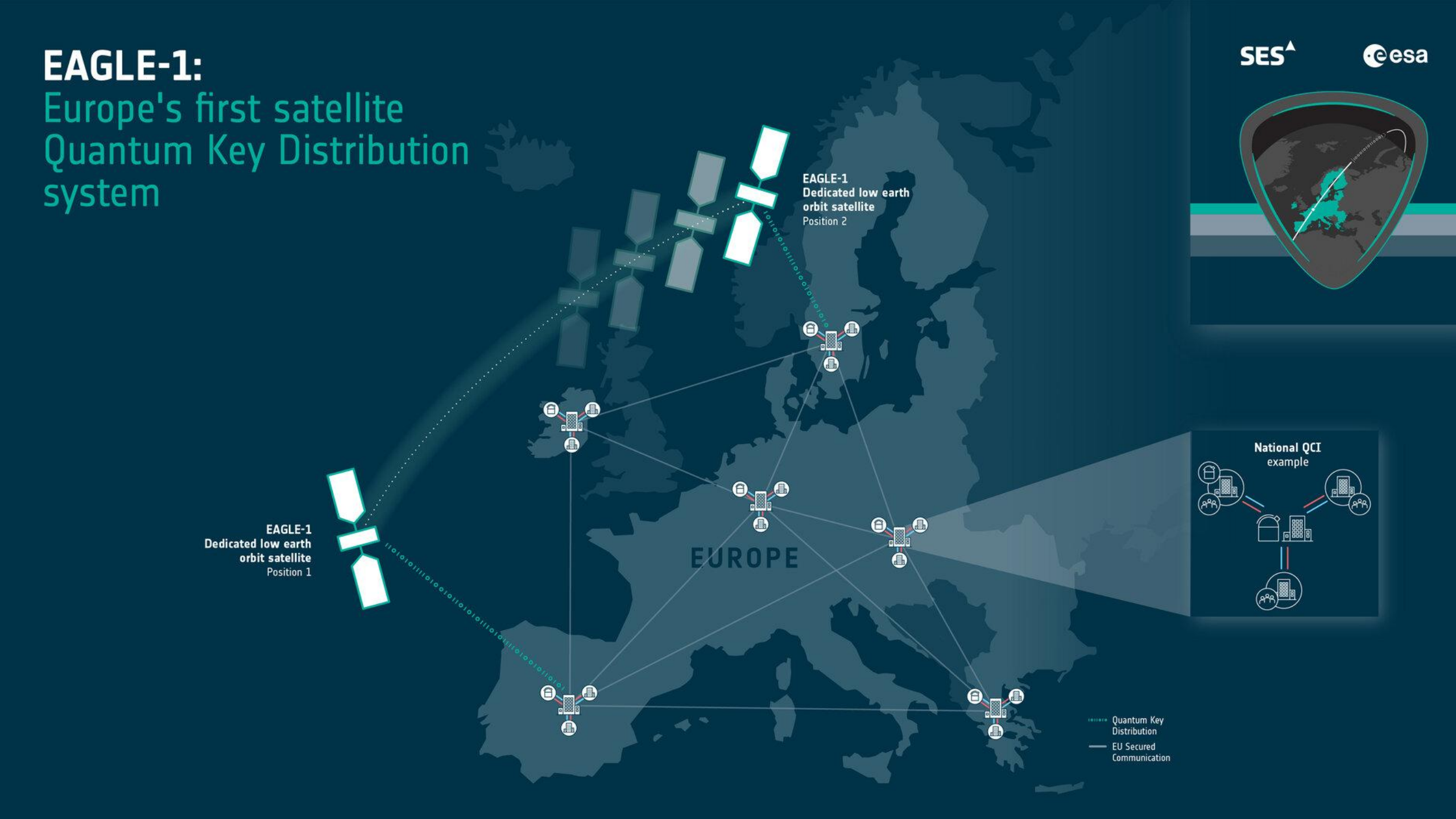


Két generáció

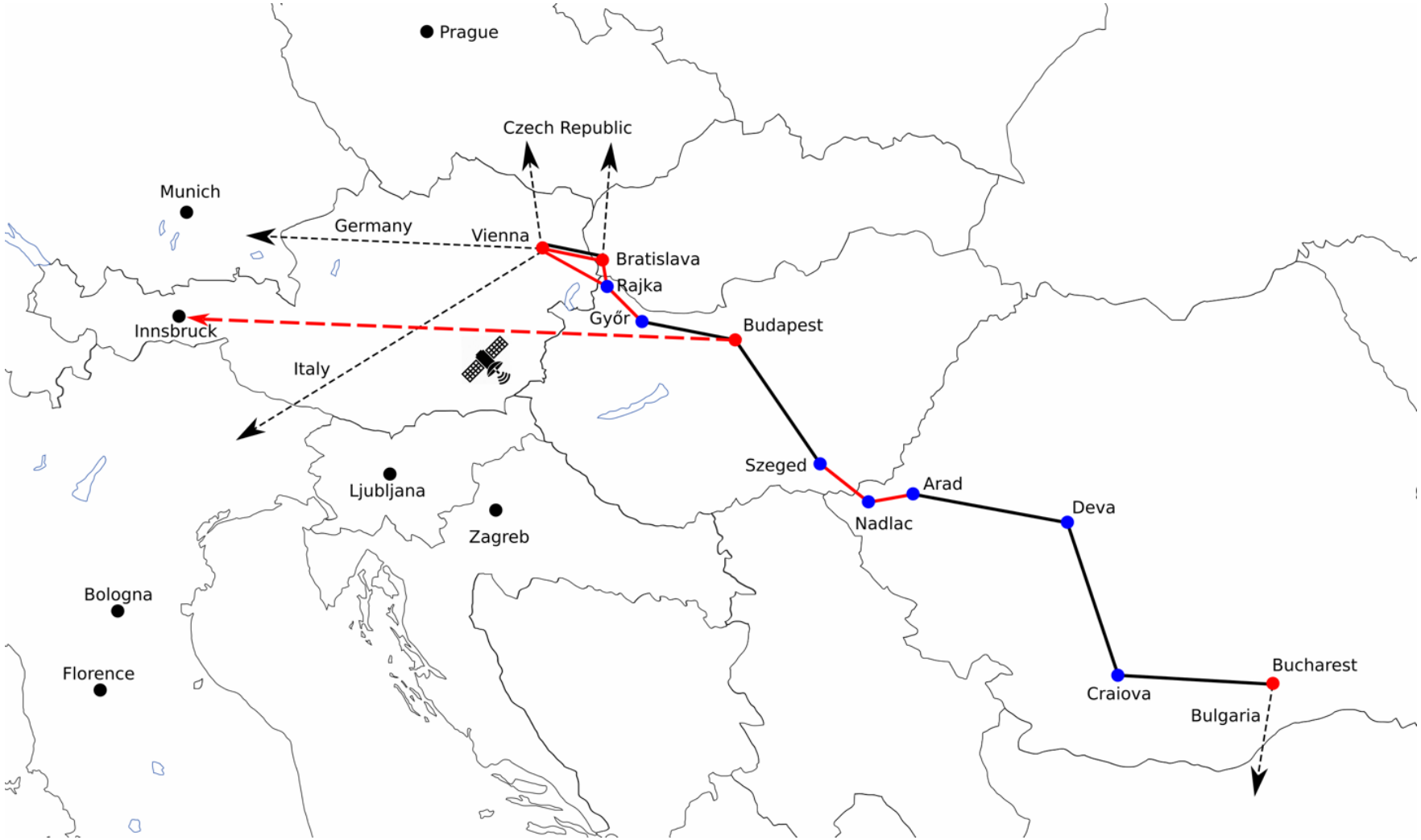
Első generáció: Diszkrét változójú (Discrete Variable, DV QKD)

Második generáció: Folytonos változójú (Continues Variable, CV QKD)

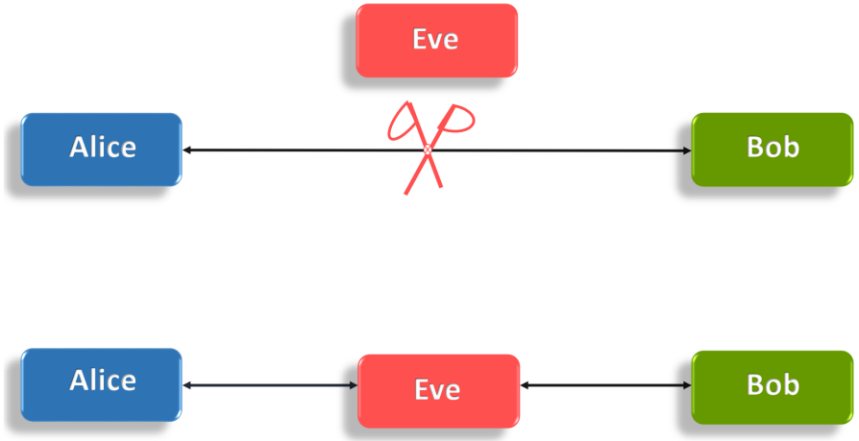
EAGLE-1:
Europe's first satellite Quantum Key Distribution system



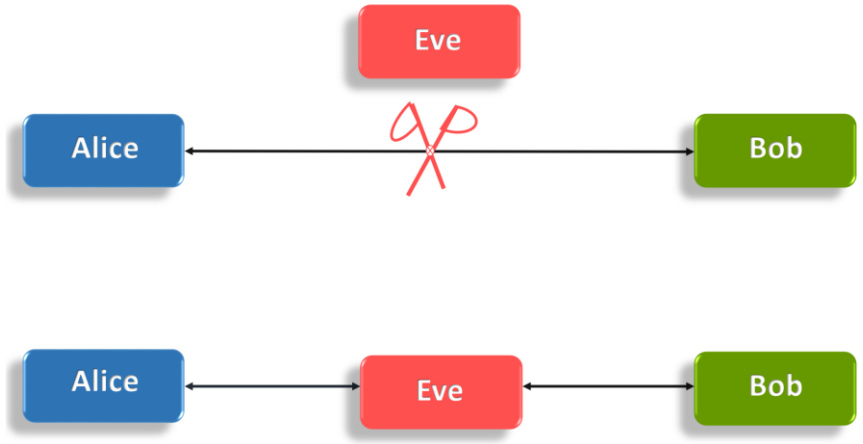
CENTRAL EUROPEAN QUANTUM COMMUNICATION INFRASTRUCTURE



EGY ÉRDEKES KÉRDÉSKÖR



HITELESÍTÉS

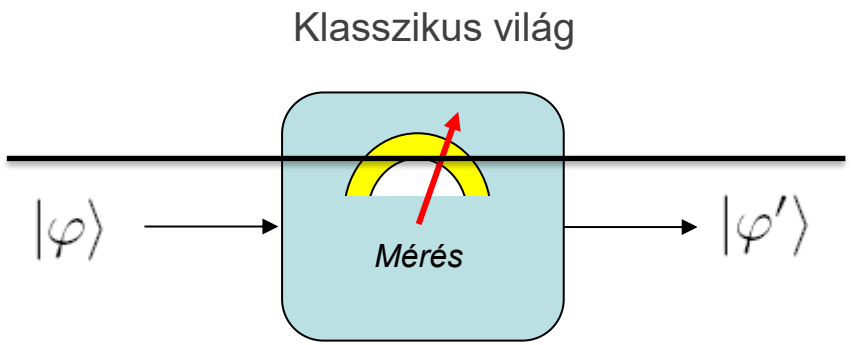


A QKD-protokollok csak a kulcscserét szolgálják, a kommunikáló felek hitelesítését meg kell oldani!

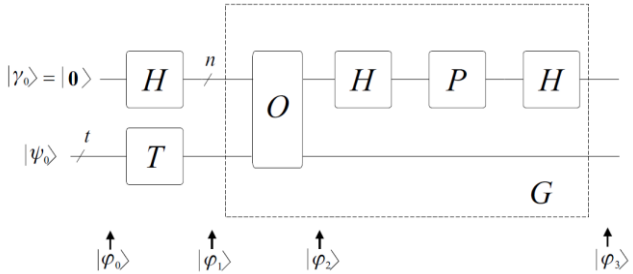
Építőelemek

ÉPÍTŐELEMEINK

- Kvantumbit
- Kvantumregiszter
- Kvantumkapu
- Mérés

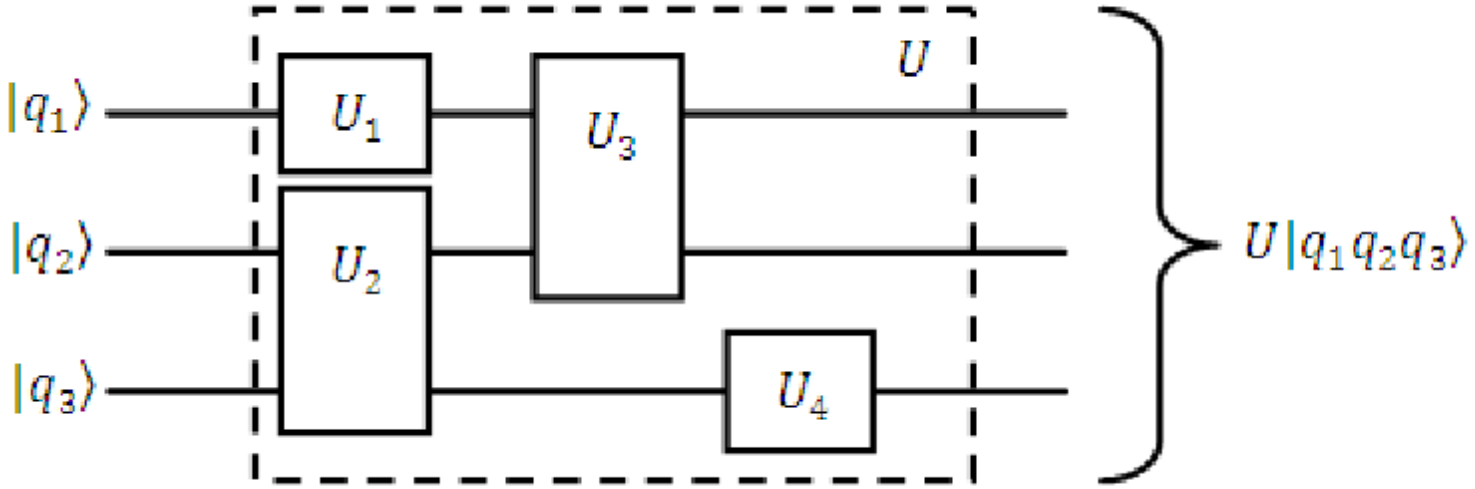


Kvantumáramkör



Kvantumalgoritmus

ÁLTALÁNOS KVANTUMÁRAMKÖRI MODELL



FIZIKAI KVANTUMBITEK

- Kvantumbit:
  - bármilyen kétszintű kvantummechanikai rendszer használható kvantumbitként
- A Szent Grál:
  - a legjobb kvantumbit összetett problémák feldolgozására:
    - egy olyan kvantumbit, amely összekapcsolható más bitekkel, hogy skálázható legyen és képes legyen nagy számítási problémák megoldására.
- Kihívás: hogyan lehet a pontossággal skálázni?
  - Korlátozott a más kvantumbitekkel való kapcsolat
  - Korlátozott a zaj miatt
  - Korlátozott az alkalmazott architektúra miatt

DI VINCENZO CRITERIA

The five criteria

1. A scalable physical system with well-characterized qubit
2. The ability to initialize the state of the qubits to a simple fiducial state
3. Long relevant decoherence times
4. A "universal" set of quantum gates
5. A qubit-specific measurement capability

EGY ÁBRA 2018-BÓL

1. A scalable physical system with well-characterized qubit
2. The ability to initialize the state of the qubits to a simple fiducial state
3. Long relevant decoherence times
4. A "universal" set of quantum gates
5. A qubit-specific measurement capability

QC Approach	#1	#2	#3	#4	#5
NMR					
Trapped Ion					
Neutral Atom					
Cavity QED					
Photonic					
Solid State					
Superconducting					

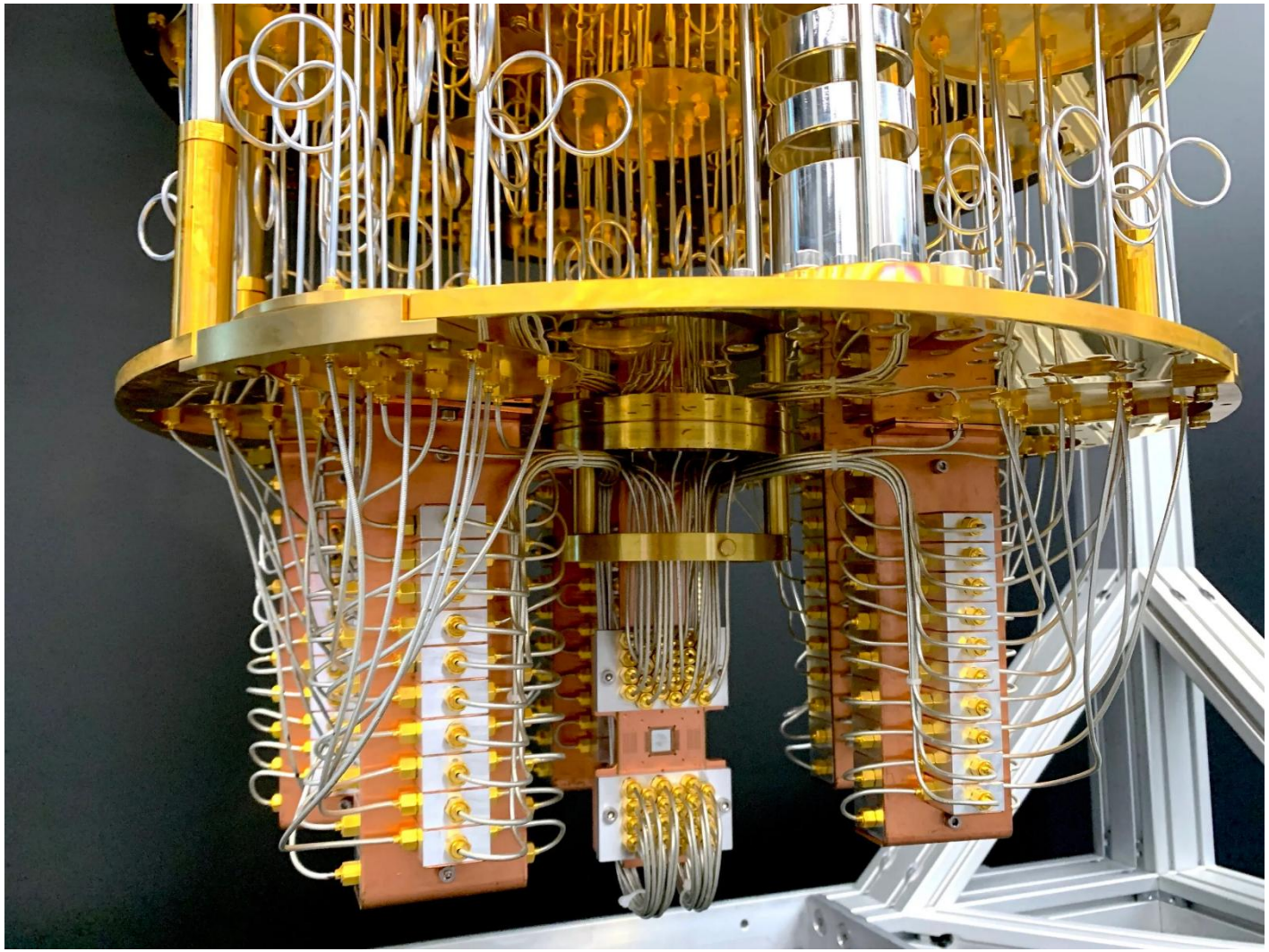
= a potentially viable approach has achieved sufficient proof of principle

= a potentially viable approach has been proposed, but there has not been sufficient proof of principle

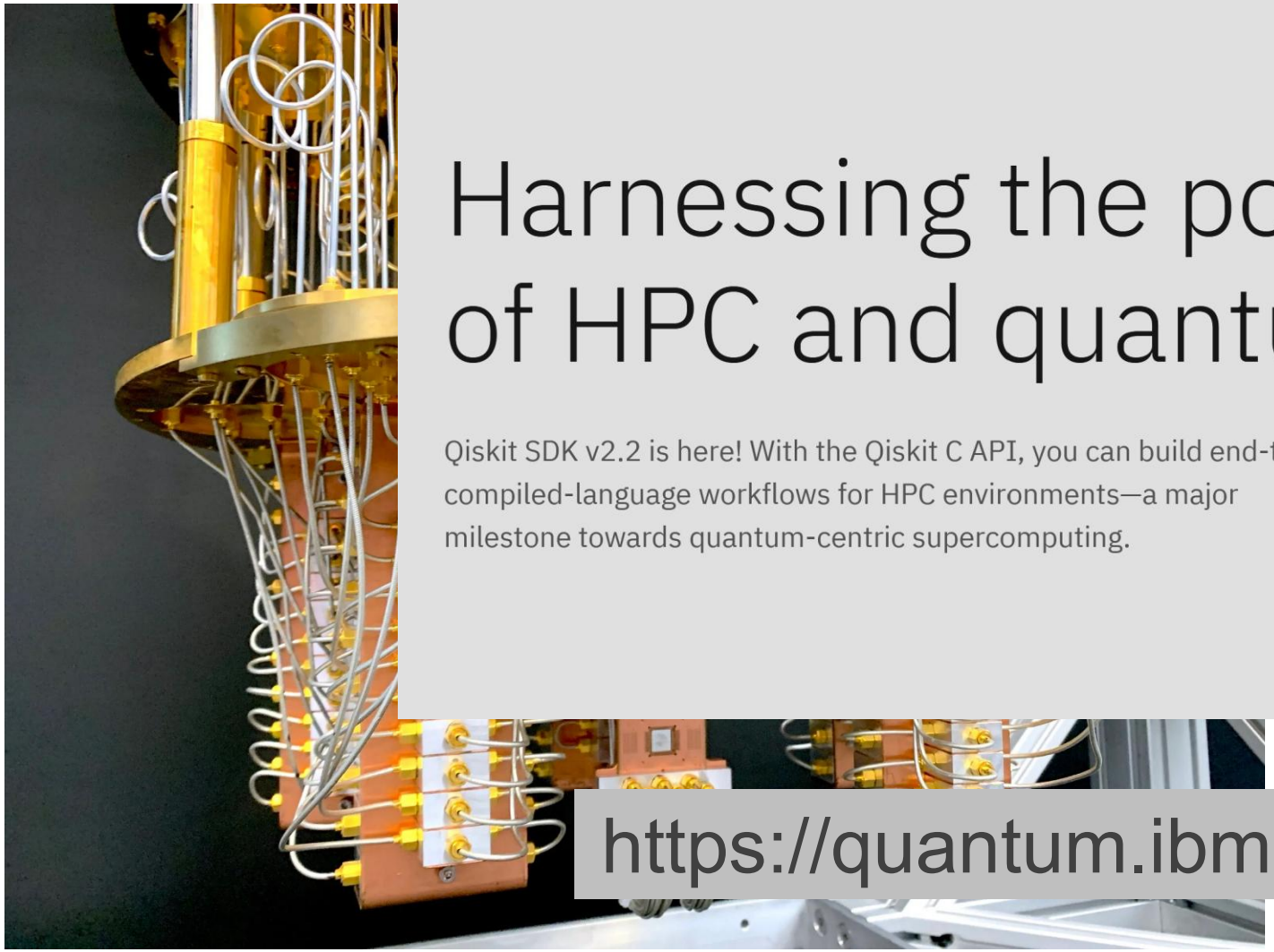
= no viable approach is known

Source: Peter McMahon, Q2B 2018
https://q2b2018.qcware.com/videos-presentations

IBM QUANTUM COMPUTER



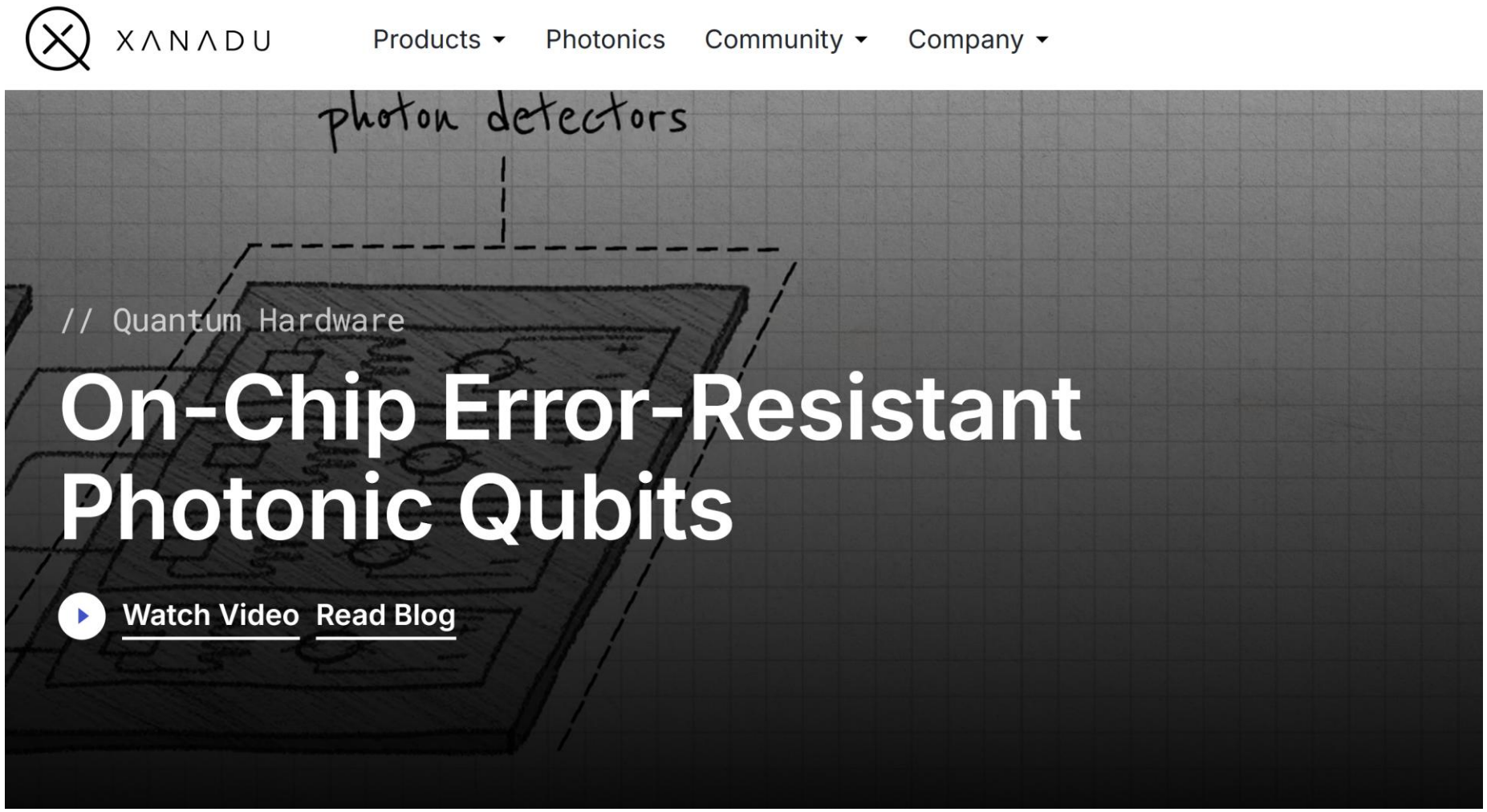
IBM QUANTUM COMPUTER



Harnessing the power of HPC and quantum

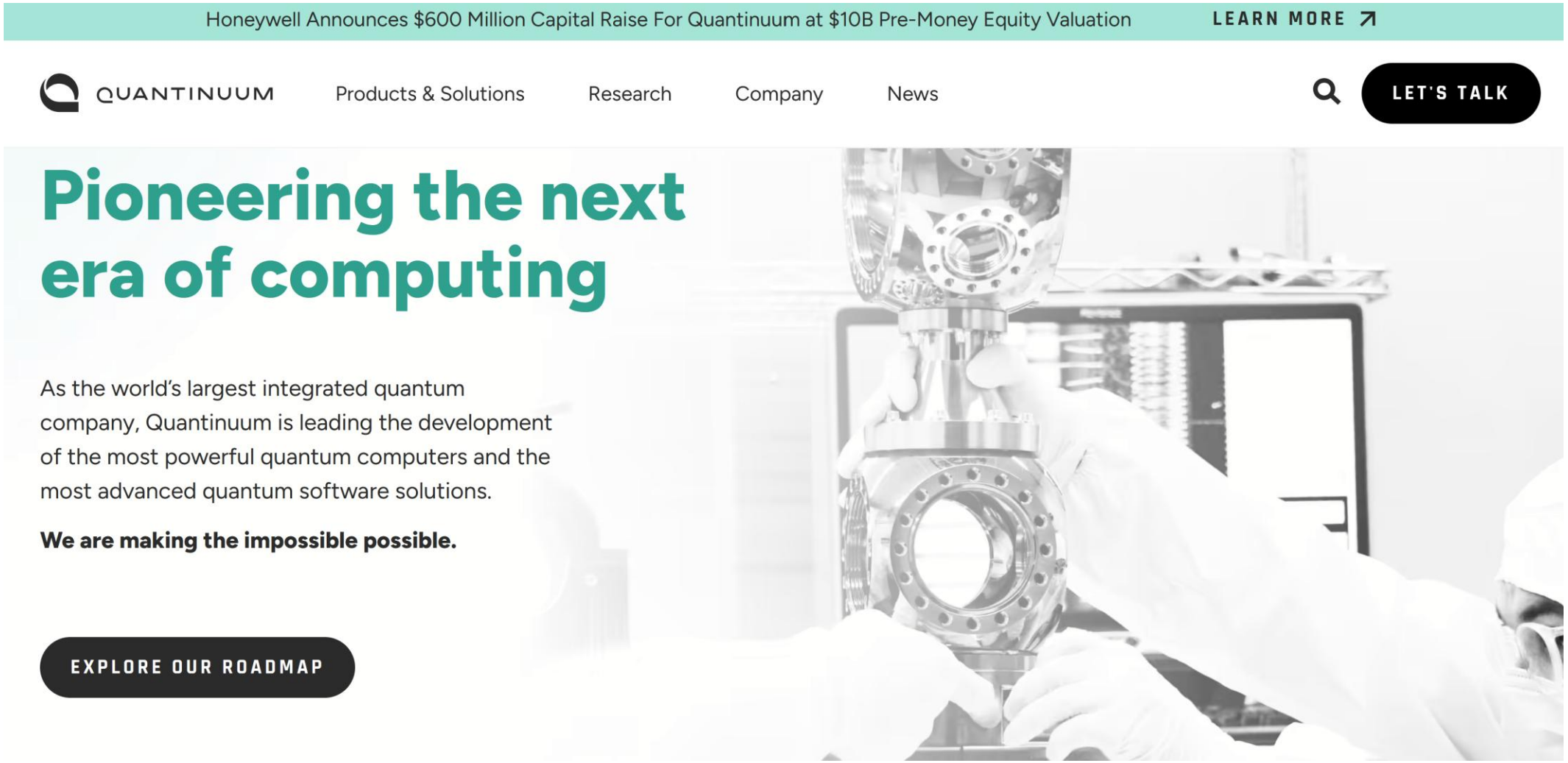
Qiskit SDK v2.2 is here! With the Qiskit C API, you can build end-to-end compiled-language workflows for HPC environments—a major milestone towards quantum-centric supercomputing.

https://quantum.ibm.com



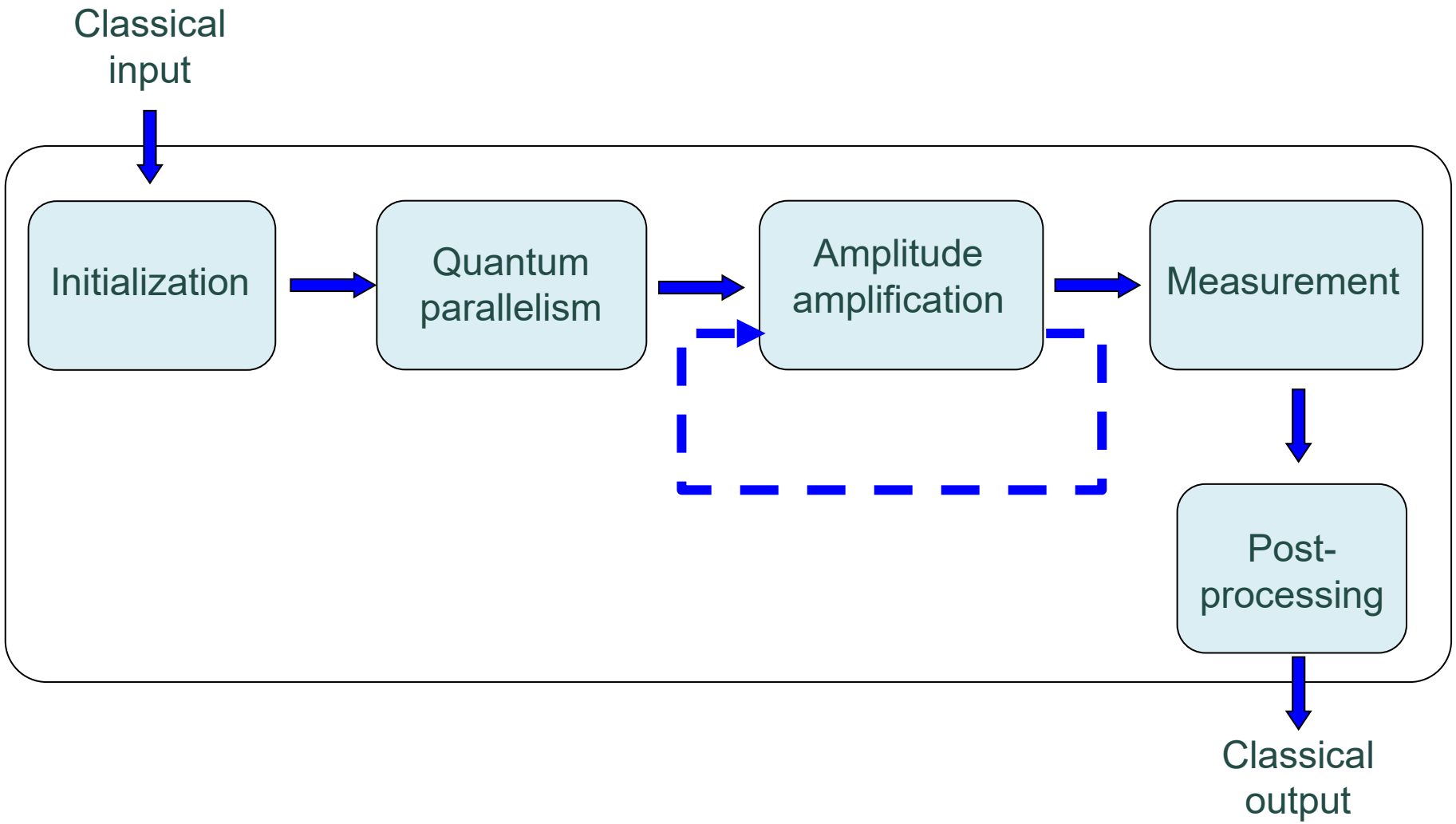
https://xanadu.ai

https://www.meetiqm.com/



https://www.quantinuum.com/

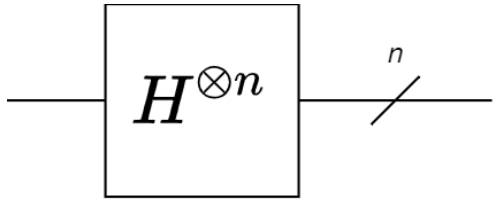
KVANTUMALGORITMUS ÁLTALÁNOS RECEPTJE



INICIALIZÁLÁS

- A probléma megfogalmazása „kvantumos” nyelven
- Hogyan tudom lefordítani a klasszikus világbeli problémámat a kvantumszámítógép világára?
- Milyen áramköri elemekre van szükség hozzá?

- Áramkör kvantumos inicializálása:
  - Szuperpozíció segítségével az összes lehetséges bemenet előállítása



KVANTUMPÁRHUZAMOSSÁG

- A műveleti eredmény kiszámítása az összes lehetséges bemeneten

- Erről a következő előadáson lesz részletesen szó.

AMPLITÚDÓERŐSÍTÉS

- Az amplitúdóerősítés olyan szuperpozíciót hoz létre, amelyben a kívánt állapot(ok) amplitúdója 1 vagy közel 1.
- Ez garantálja, hogy a mérés nagy valószínűséggel a kívánt értéket adja vissza.
- Az amplitúdóerősítés a legtöbb esetben egyetlen lépésben, a Hadamard-transzformáció vagy a kvantum Fourier-transzformáció alkalmazásával érhető el. De lehet iteratív is (azaz több lépést igénylő)
- Az amplitúdóerősítésre nincs egyértelmű recept. Csak példákat tudunk mutatni.
- Ez a lépés a legnagyobb kreativitást és intuíciót igényli.
  - Egy jó ötlet, és máris a nevünket viseli egy algoritmus!

MÉRÉS

- A mérésről korábban már beszéltünk.
- Két nagyobb konstrukciós technika létezik
  - 1. Projektív mérés
    - mikor a mérendő kvantumállapotok ortogonálisak.
  - 2. POVM mérés
    - Positive Operator-valued Measurement
    - amikor az állapotok nem ortogonálisak
    - ezzel a méréssel ebben a kurzusban nem foglalkozunk
- E két technika hatékonyan használható a kívánt klasszikus értékek visszaadására.

KLASSZIKUS UTÓFELDOLGOZÁS

- Az utófeldolgozás során a mérés eredményét a kiindulási probléma megoldására alakítjuk át
- A legtöbb esetben az utófeldolgozás a mért érték egyszerű bejelentését jelenti.
- Néha azonban összetett matematikai levezetésekre van szükség.

ENNYIT AZ ELMÉLETRŐL

Mindezekre számos példát nézünk a következő előadások során

- Deutsch-Jozsa algoritmus
- Kvantum Fourier-transzformáció
- RSA-törés a Shor-algoritmus segítségével
- Hatékony keresés a Grover-algoritmussal