HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

Kvantum alapú kulcsszétosztás
2025. október 22.

Kvantuminformatikai alklamzások, 2025 ősz

Galambos Máté

BME Hálózati Rendszerek és Szolgáltatások Tanszék
galambos.mate@vik.bme.hu

MŰEGYETEM 1782

Ismétlés

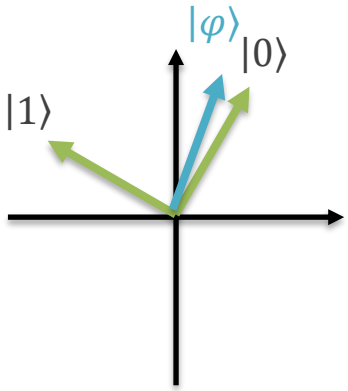
ISMÉTLÉS

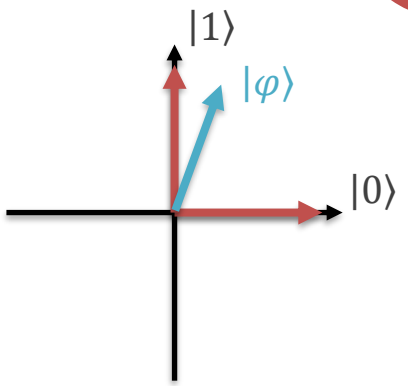
A mérés megváltoztatja az állapotot

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle\,,$$

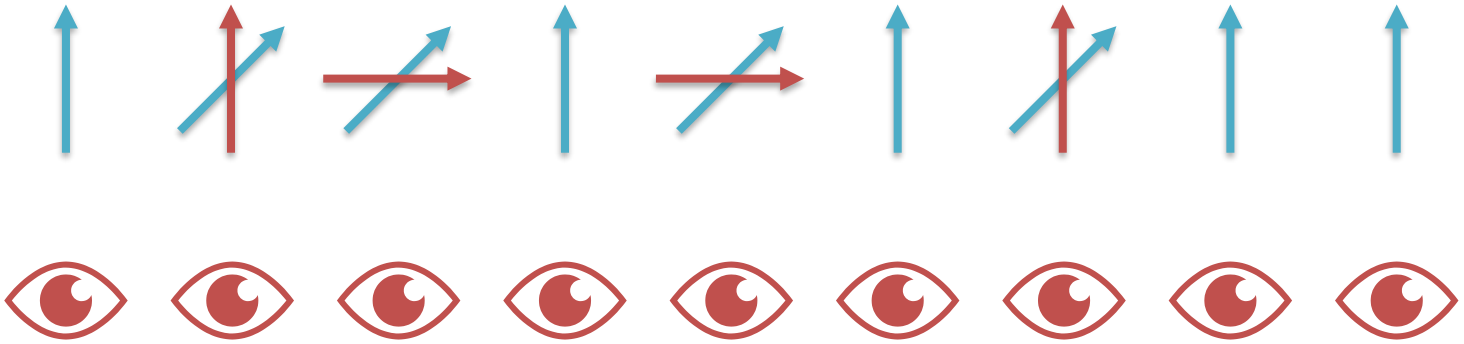
$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}\,.$$

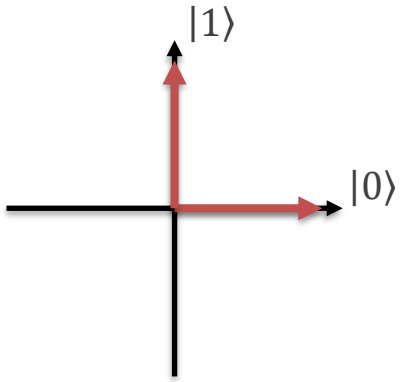
Óvatosan kell megválasztani a bázist



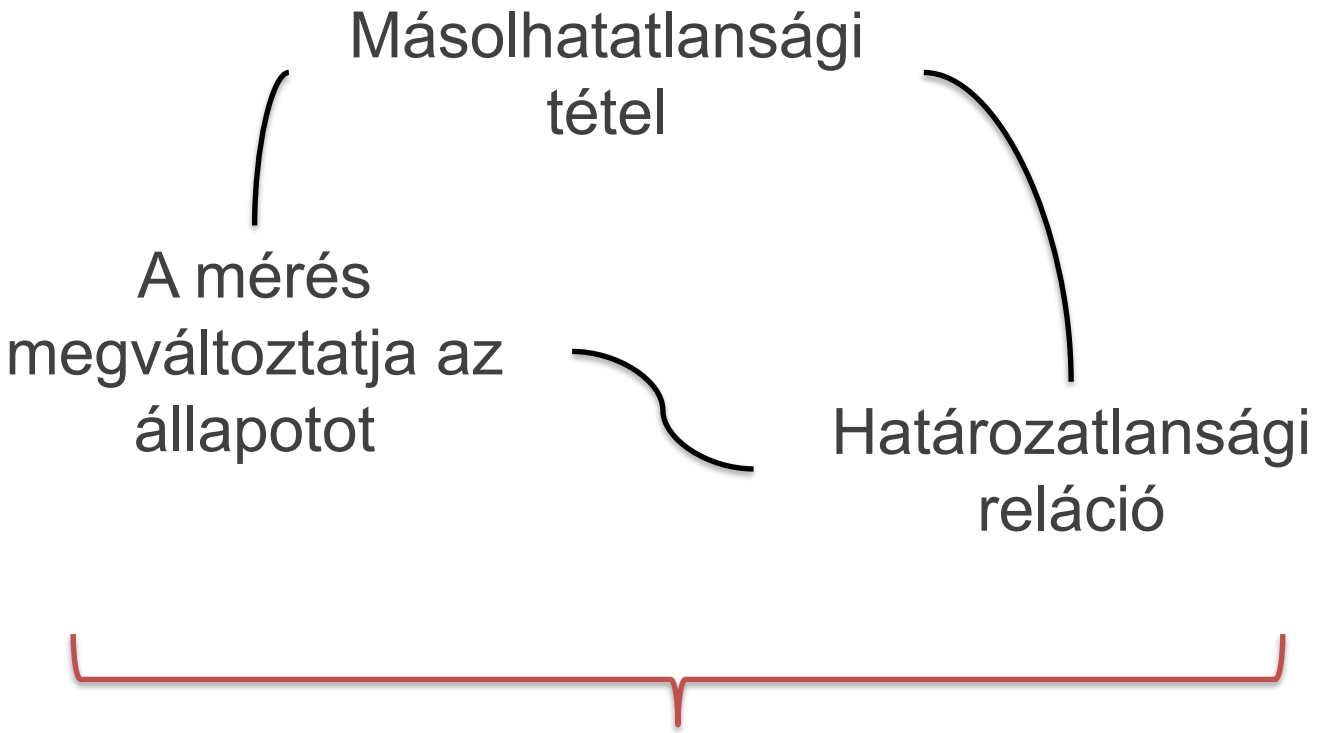


ISMÉTLÉS





ISMÉTLÉS



A kvantuminformációt nem lehet tökéletesen megismerni

ISMÉTLÉS

A kvantuminformációt nem
lehet tökéletesen
megismerni

„Kutya nehéz úgy hazudni,
ha az ember nem ösmeri az igazságot.”

– Eszterházy Péter

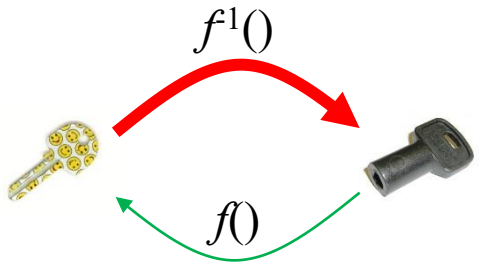
Biztonsági kockázat (motiváció)

MOST

A kritikus infrastruktúrát védeni kell a kibertámadásoktól

Klasszikus kriptográfia

TITKOSÍTÁS



Nyilvános kulcsú titkosítás

- nyilvános titkosítókulcs
- titkos fejtőkulcs

- A mai napig nem sikerült bebizonyítani, hogy nincs hatékony algoritmus a feltörésre
- **Kvantumos fenyegetés: Shor-algoritmus**

Szimmetrikus kulcsú titkosítás

- Egyforma kulcsok mindkét oldalon

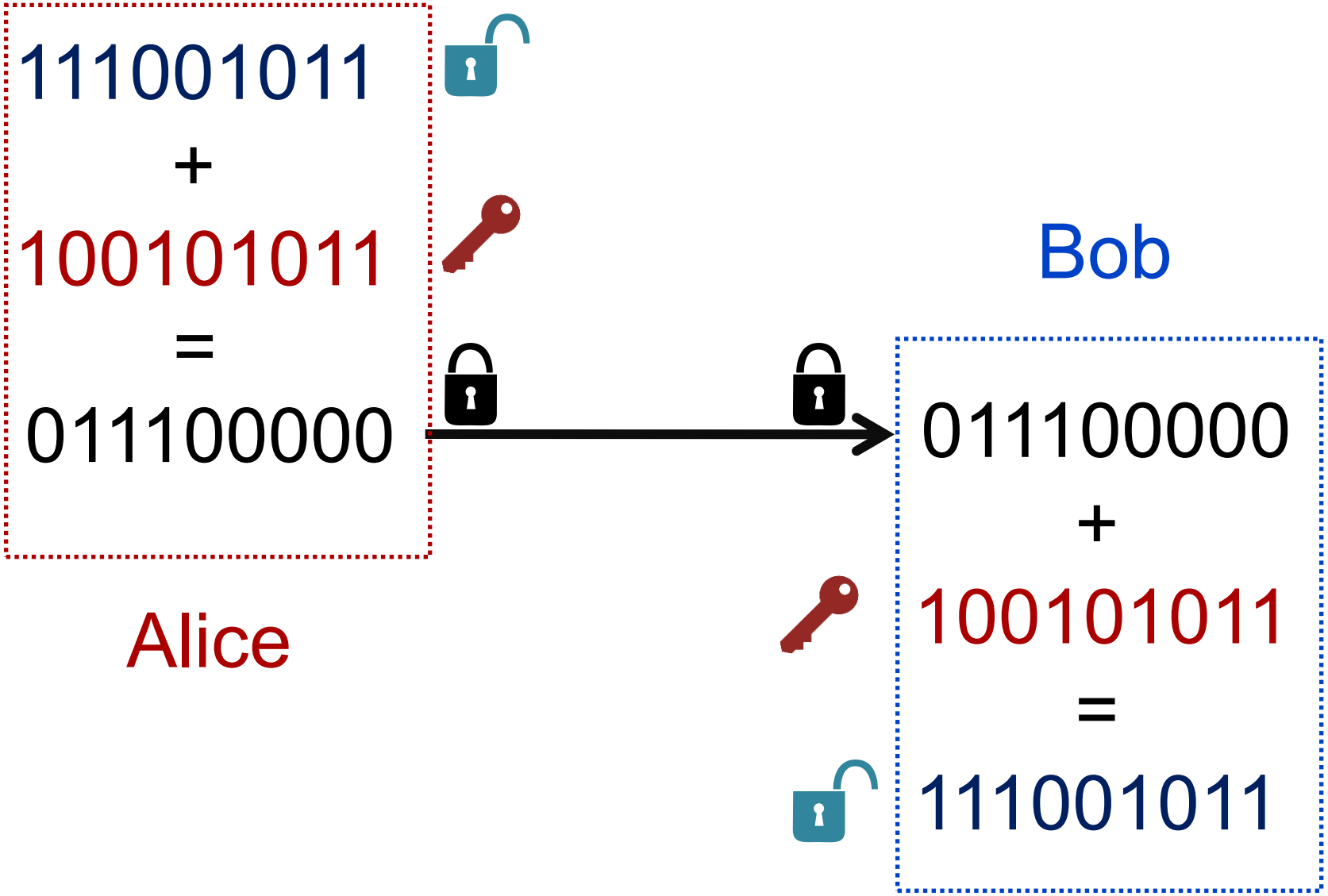
- Abszolút biztonságos, ha bizonyos előírásokat betartunk
- Gond: a kulcsot miként juttassuk el a túloldalra???

TITKOSÍTÁS

Milyen az ideális jelszó?

- Hosszú
  - Olyan hosszú, mint maga a nyílt szöveg
- Kiszámíthatatlan (random)
  - Szimbólumokat azonos valószínűséggel sorsolom
  - Szimbólumok függetlenek egymástól
  - Szimbólumok függetlenek mindentől amihez a támadó hozzáfér

ONE TIME PAD
VERNAM CYPHER



ONE TIME PAD ELŐNYE

01110 


00000


00001


00010


11110


11111


01110


01111


01100

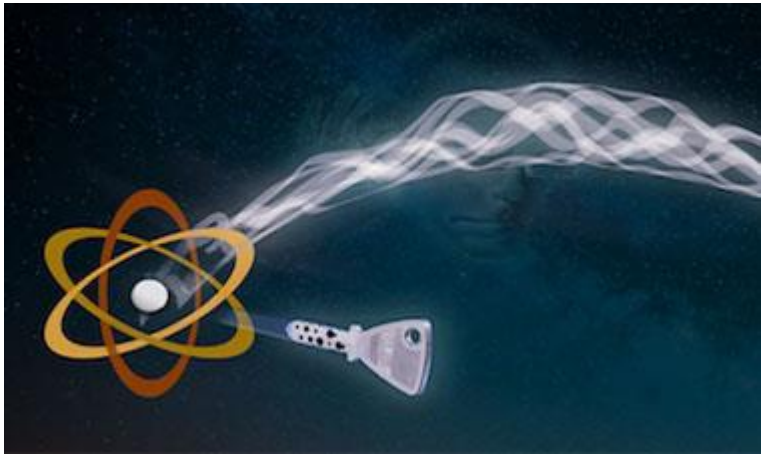

10000


10001

Kulcsmegosztás problémás

Megoldás:

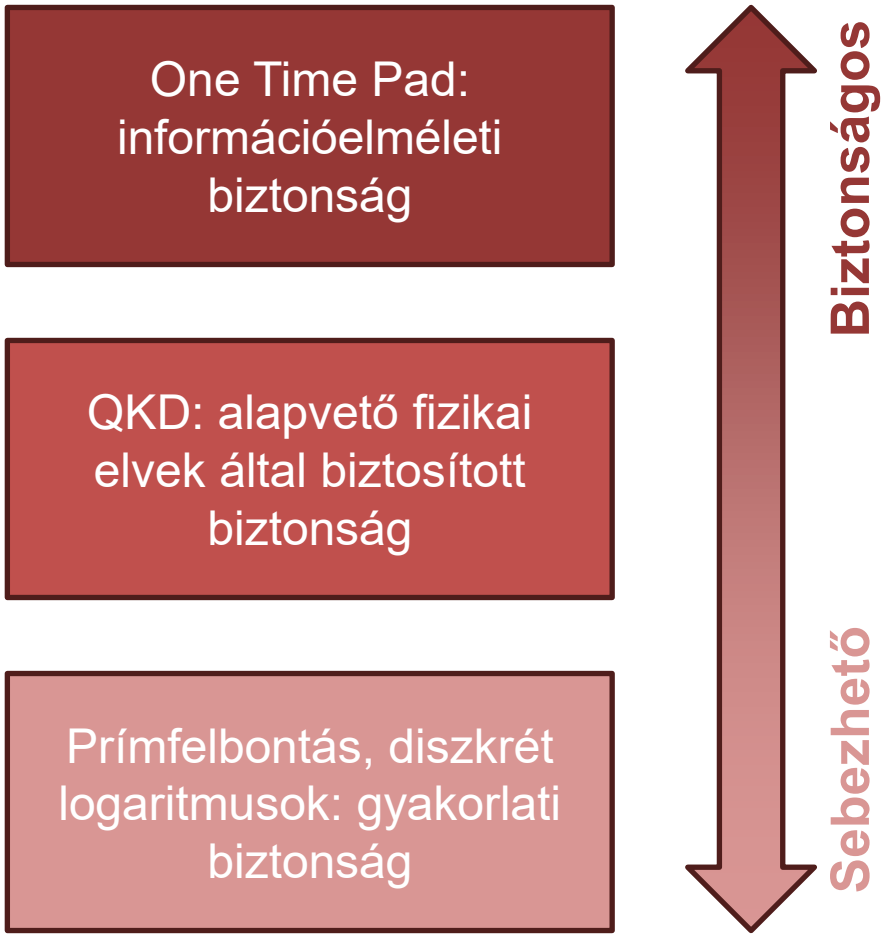
- Kvantum kulcsszétosztás
- Quantum Key Distribution (QKD)



A BIZTONSÁG HIERARCHIÁJA

Feltételek teljesülése esetén:

- Információelméleti biztonság: a támadó csak találgatni tud, matematikailag ***bizonyítottan*** biztonságos
- Alapvető fizikai elvek által biztosított biztonság: nincs matematikai bizonyítás, hogy a fizika elvei helyesek, de hatalmas előrejlző képességük van
  - Jóslataik kísérletekkel tesztelhetőek
- Gyakorlati biztonság: jelenleg nincs széles körben ismert hatékony módszer, amivel meg lehetne támadni
  - Mi lesz holnap? Milyen titkos módszerek vannak a feltörésére? Mit jelent a nem hatékony?



Kvantum kulcsszétosztás
(Más néven kulcsnövesztés)

KULCSSZÉTOSZTÁS ALAPGONDOLATA

- Prepare and measure
- Előkészít és megmér
  - Adó tudja, mit küldött
- Mágikus cetlik:
  - Csak az egyik felét nézhetem meg

- Entanglement based
- Összefonódás alapú
  - Maximálisan összefonódott állapot
- Iker pénzérmék:
  - Egyik dobás eredménye meghatározza a másikat

ELŐKÉSZÍT ÉS MEGMÉR ALAPGONDOLATA

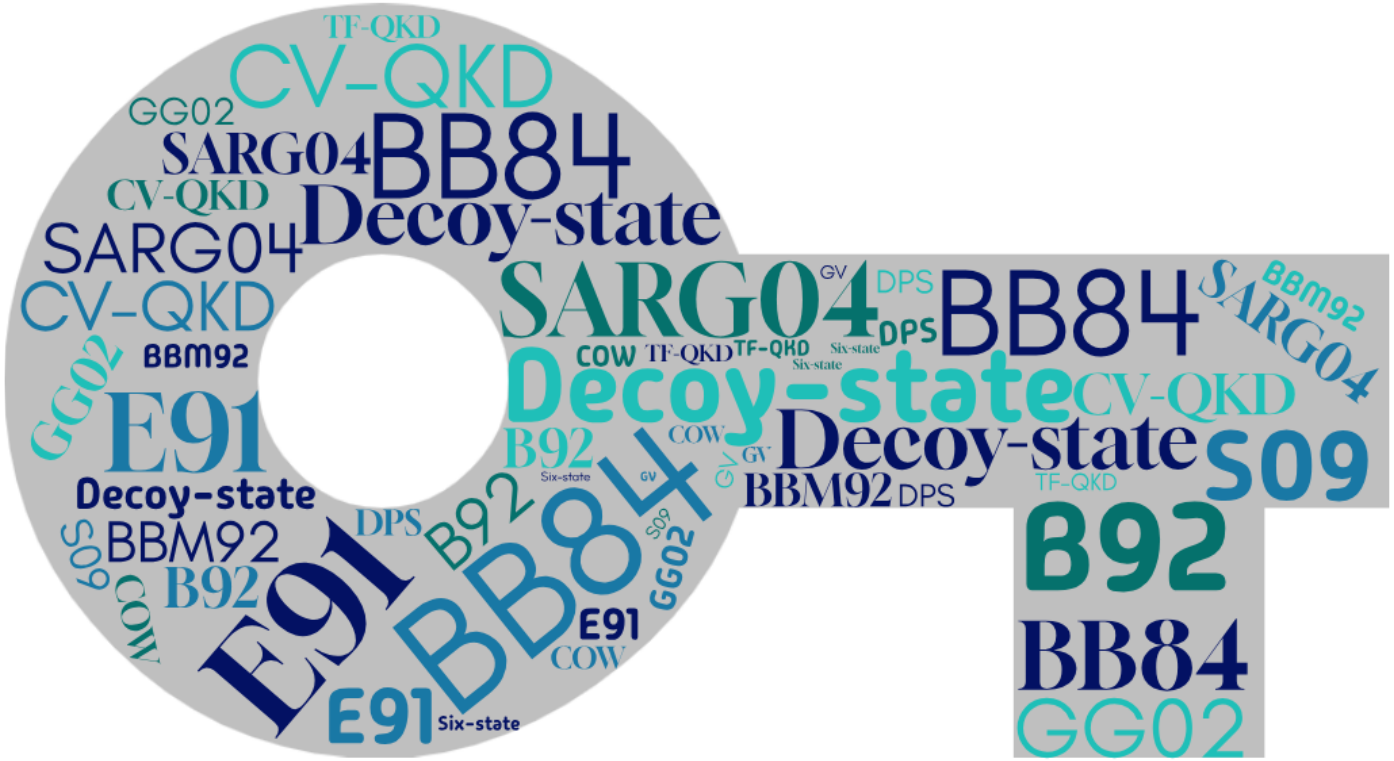
- A mérés megváltoztatja az állapotot
- Mágikus cetlik:
  - Csak az egyik felére írhatok
  - Ha valaki a másik felére néz rá, az üzenet törlődik
    - És véletlen betű jelenik meg az én üzenetem helyén
  - Ráírom a jelszavamat (betűnként)
  - Ha valaki nézegeti, csökken az integritás
  - Kriptográfiára tök jó

Bizalmasság ⟷ Integritás

ELŐKÉSZÍT ÉS MEGMÉR ALAPGONDOLATA

- Kulcsátvitel mágikus cetlikkel:
  - Ha valaki nézegette az átvitt kulcsot, nem használjuk, küldünk újat
- Honnan tudjuk melyik felét kell a cetlinek megnézni?
  - Nem tudjuk
  - Utólag beszéljük meg ki mit használt
  - Azonosakat megtartjuk
  - Különbözőket eldobjuk
  - Hibakeresés
    - Kulcs egy részét feláldozzuk, összehasonlítjuk

SZÁMOS QKD PROTOKOLL



QKD PROTOKOLLOK TÍPUSAINAK ÖSSZEHASONLÍTÁSA

- DV: diszkrét változós
  - A szabadsági fok, amibe a bitértéket kódoljuk, véges számú, diszkrét állapotot vesz fel (pl. fotonszám)
- CV: folytonos változós
  - A szabadsági fok végtelen számú állapotot vehet fel, mérés után diszkretizálva kapunk belőle biteket (pl. hely)

QKD PROTOKOLLOK TÍPUSAINAK ÖSSZEHASONLÍTÁSA

Category	Salient Features	Pros & Cons
Discrete Variable protocols	**Quantum Signal:** Single photons/ Entangled photons with information encoded as polarization, time-bin / linear momentum states[10] **Detectors:** Single Photon Detectors (SPDs) Prepare and Measure (PM) Entanglement Based (EB)	**Pros:** Compared to CV; DV schemes are optimal in case of harsh channel conditions/ attenuations **Cons:** Detector-induced dark counts; multi-photon pulse probability makes the signal more susceptible to photon number splitting PNS attacks.
Continuous Variable protocols	**Quantum Signal:** Amplitude and phase quadrature of electromagnetic fields are exploited for encoding information in coherent states of light **Detectors:** coherent homodyne or heterodyne detection.	**Pros:** Comparative to DV these protocols are easier to implement with standard telecom components offering higher key rates in metropolitan distances. **Cons:** Requires stability against channel imperfections.

- Szabadtér vs Optikai szálas összeköttetés (csillapítás és zavarok)
- Összefonódás vs Előkészít-és-megmér (biztonság)

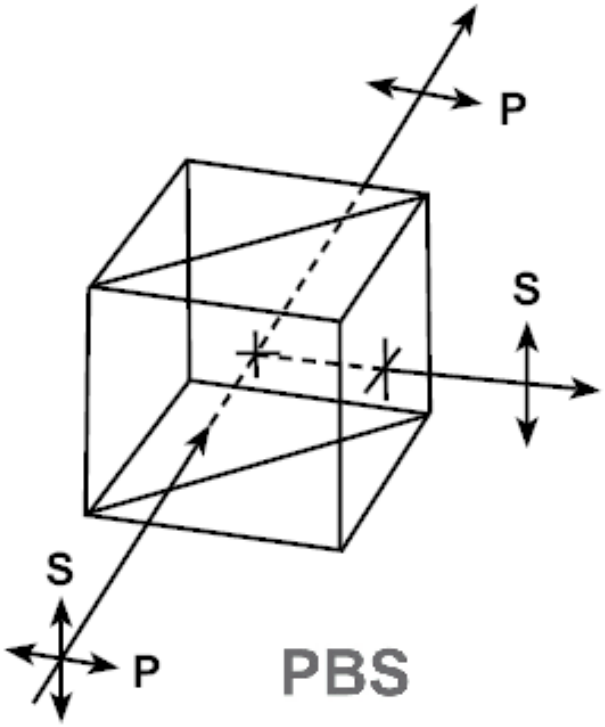
QKD PROTOKOLLOK TÍPUSAINAK ÖSSZEHASONLÍTÁSA

- Előállít és megmér (prepare and measure)
  - Aliz (a küldő) tudja, hogy milyen bitértéket akar küldeni, ő állítja elő a megflelő kvantumállapotot.
- Összefonódás alapú (entanglement based)
  - Aliz (a küldő) egy fizikai folyamatból véletlenszerűen nyer egy állapotot, amiről ő sem tudja előre, hogy mi lesz.

Bennett-Brassard 84 protokoll (BB84)

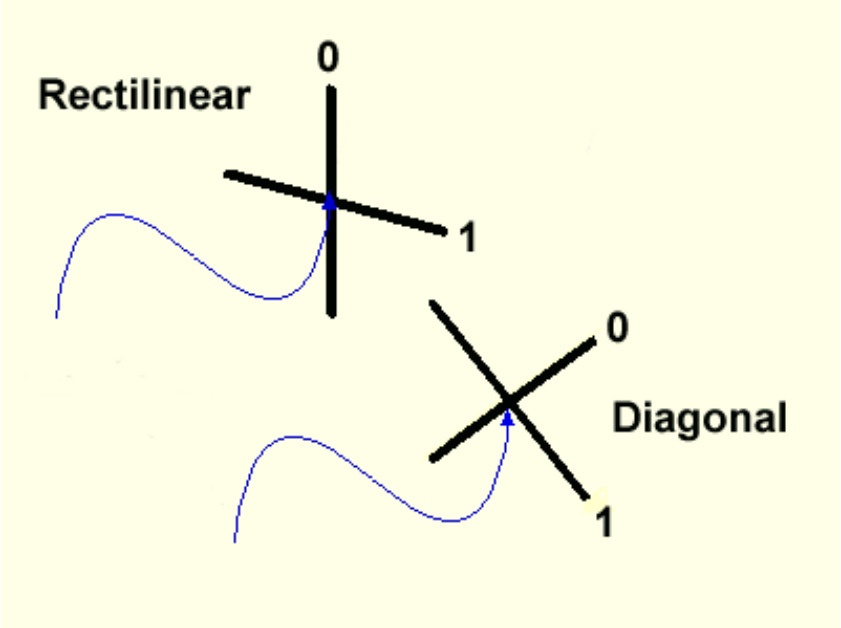
Charles H. Bennett, Gilles Brassard, „Quantum Cryptography: Public Key Distribution and Coin Tossing”, Proc. of. Int. Conf. on Computers, Systems & Signal Processing, Bangalore, India, Dec. 10-12, 1984

MILYEN MÉRÉSI BÁZISOKAT HASZNÁLJUNK?

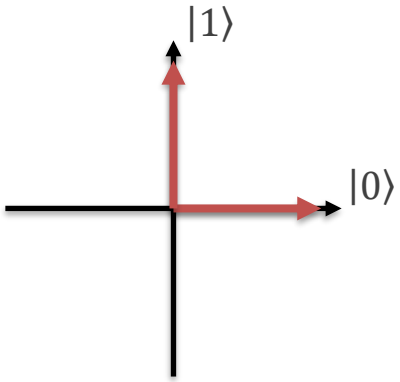


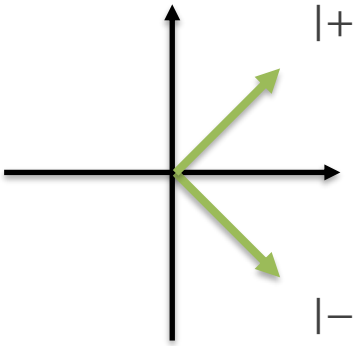
Polarizációba kódolt bitérték

Milyen mérési bázisokat használjunk?



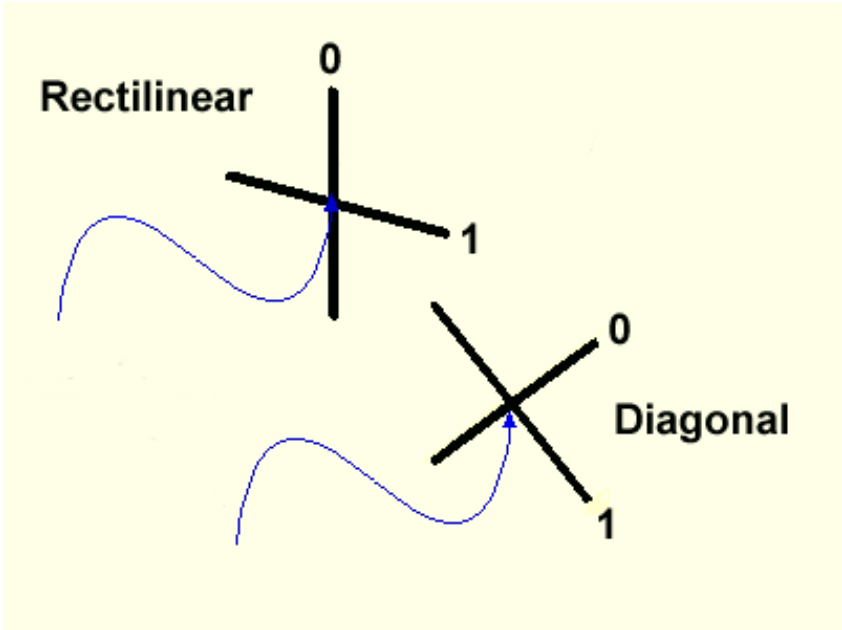
MILYEN MÉRÉSI BÁZISOKAT HASZNÁLJUNK?



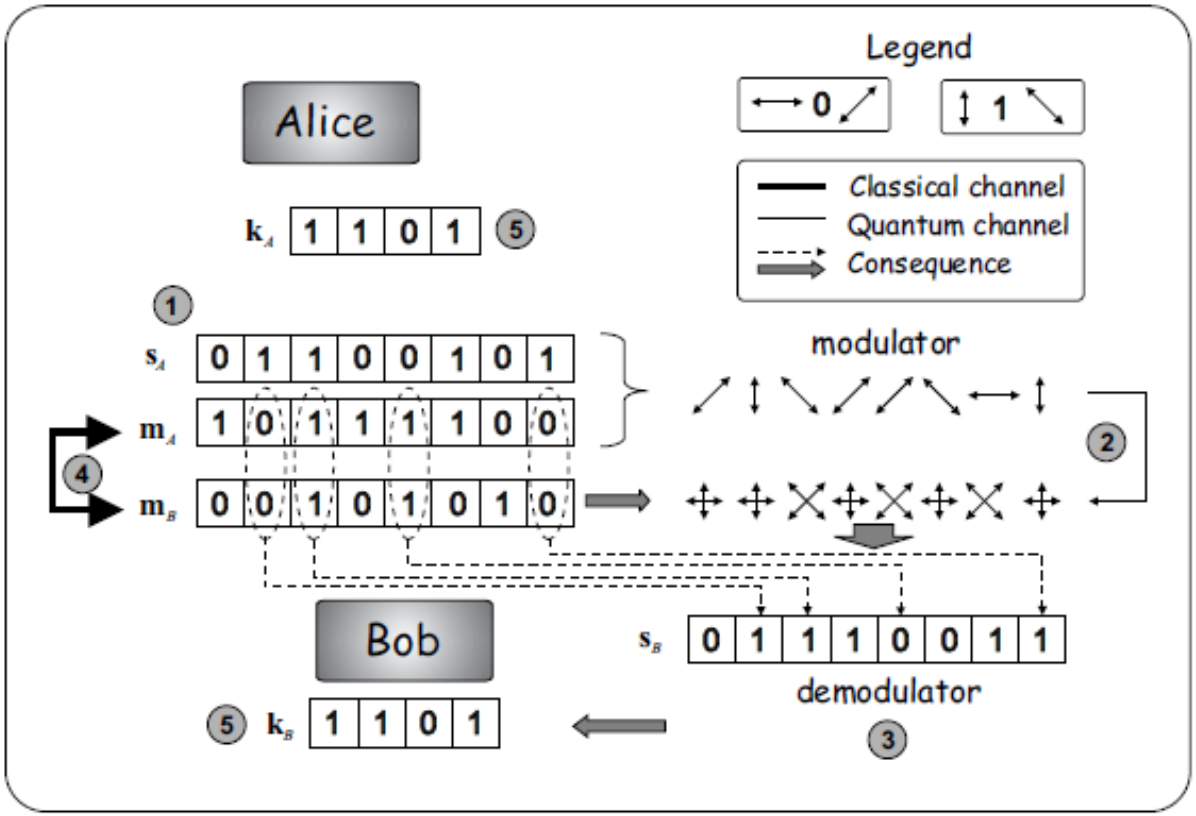


$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = H|0\rangle$$

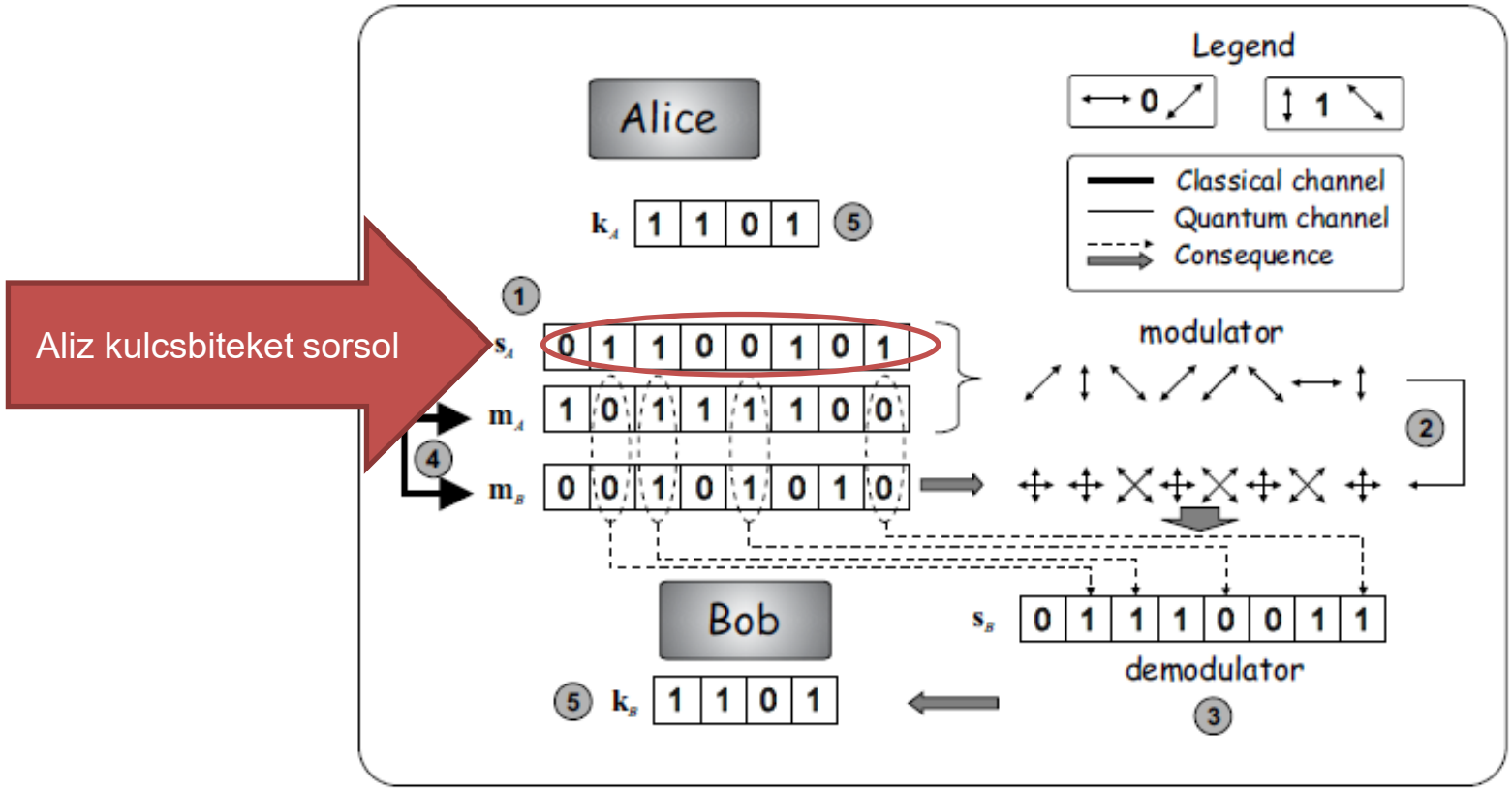
$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = H|1\rangle$$



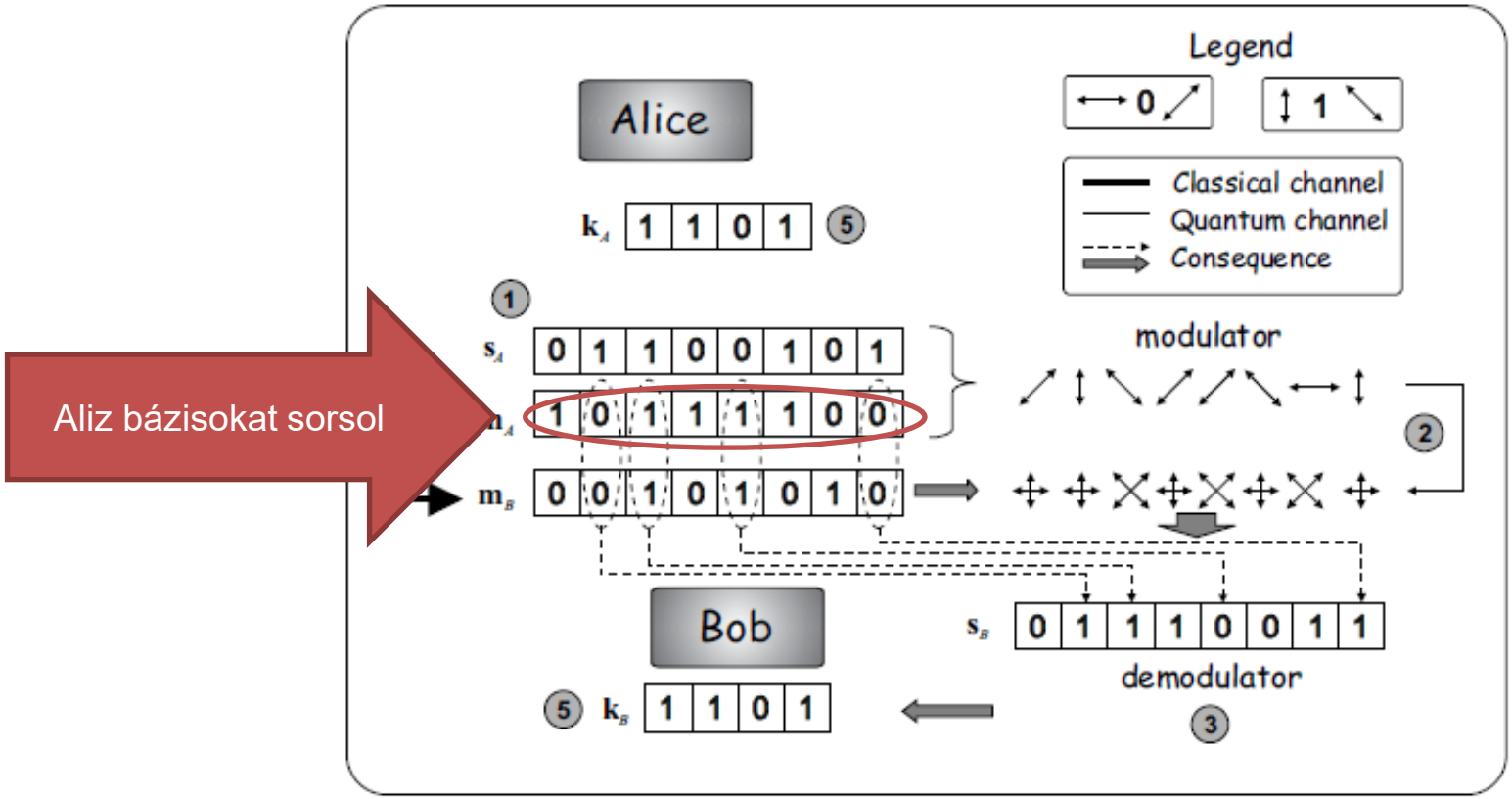
- Első generációs megoldás
  - Fotonok polarizációs állapota a kvantumbit
  - Kihívás: egyfotonok előállítása és detektálása



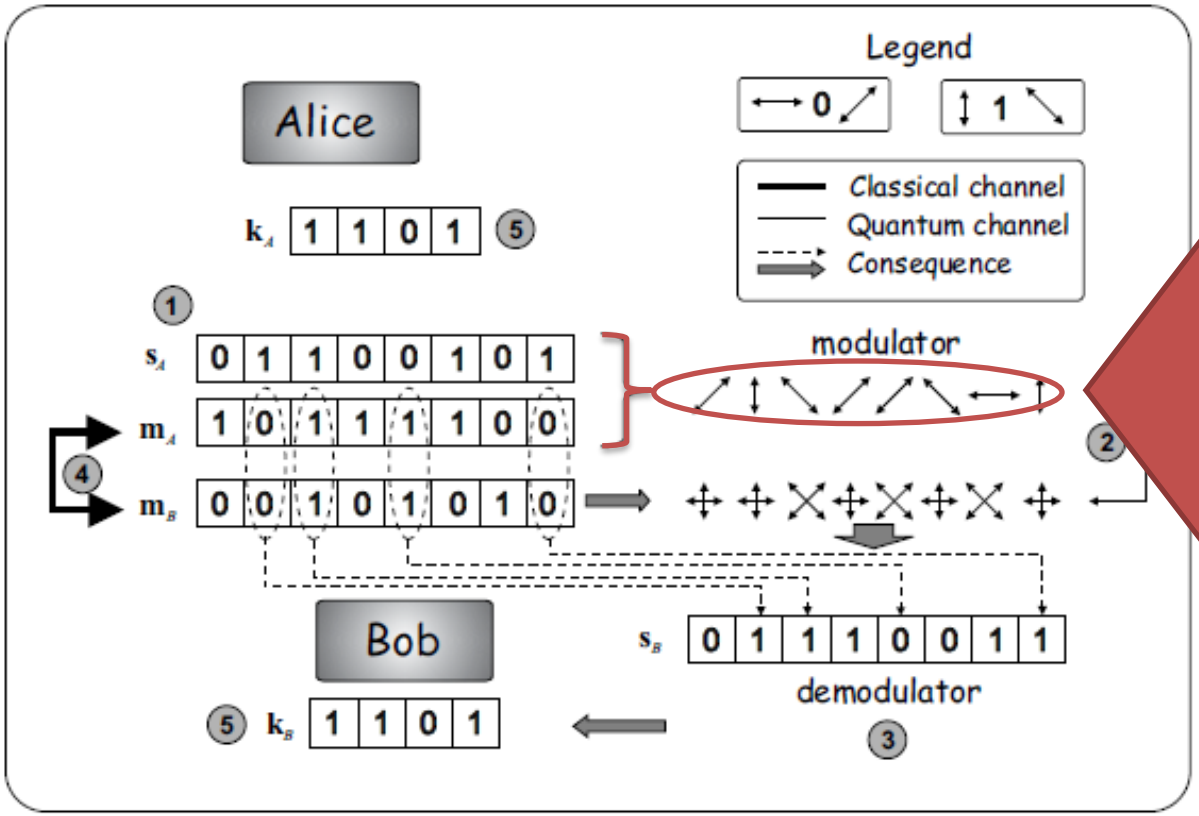
- Első generációs megoldás
  - Fotonok polarizációs állapota a kvantumbit
  - Kihívás: egyfotonok előállítása és detektálása



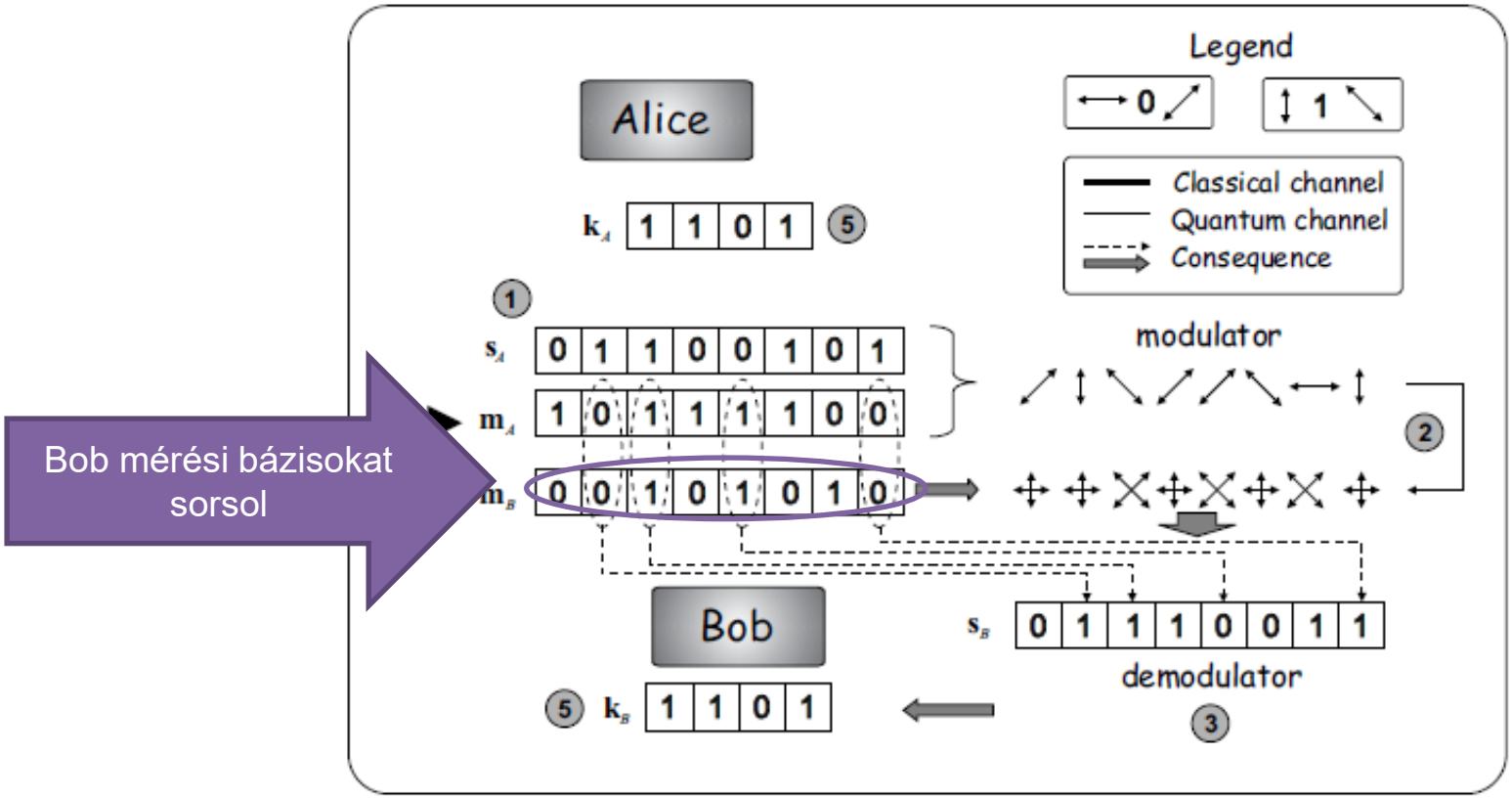
- Első generációs megoldás
  - Fotonok polarizációs állapota a kvantumbit
  - Kihívás: egyfotonok előállítása és detektálása



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

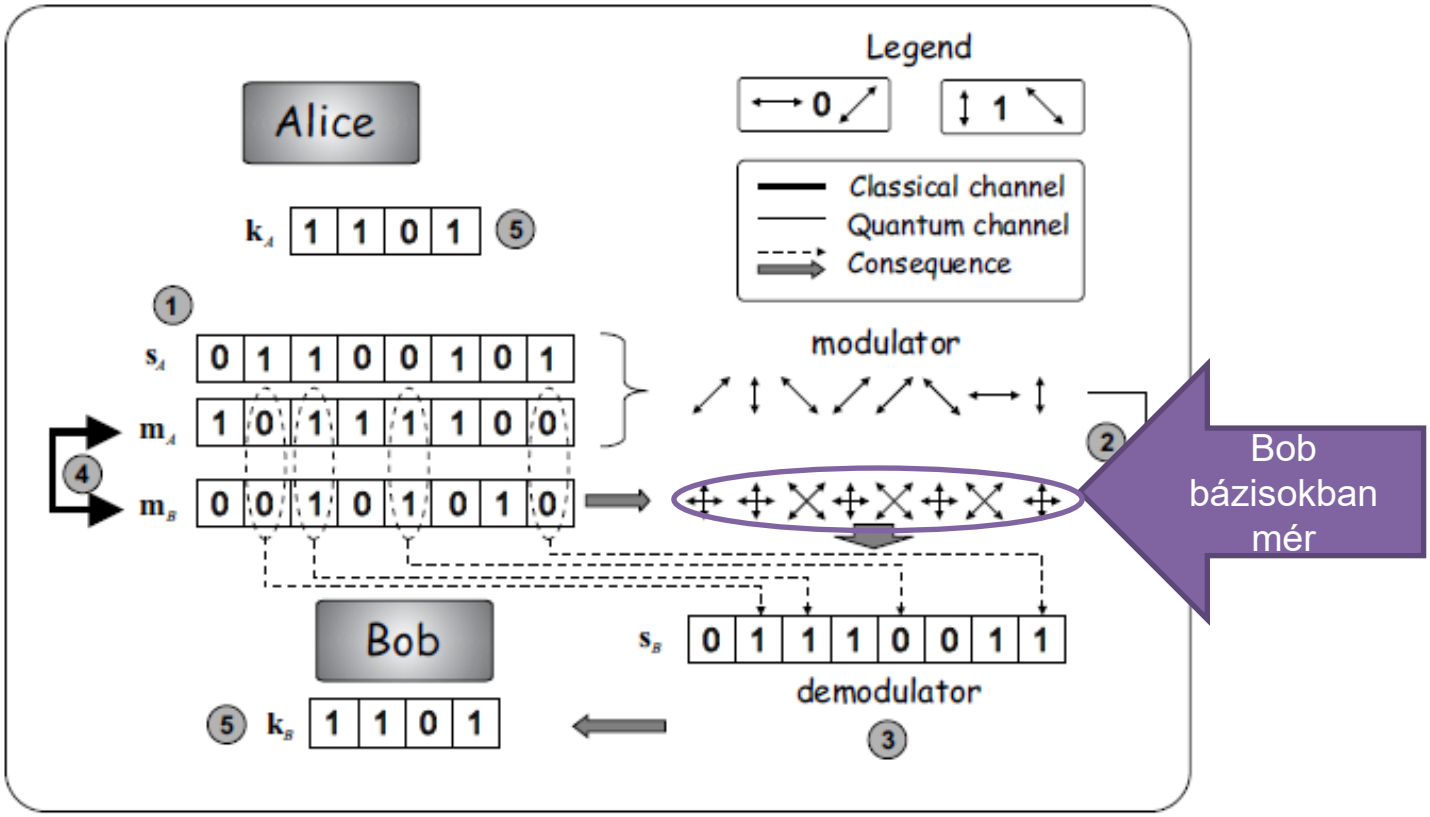


- Első generációs megoldás
  - Fotonok polarizációs állapota a kvantumbit
  - Kihívás: egyfotonok előállítása és detektálása

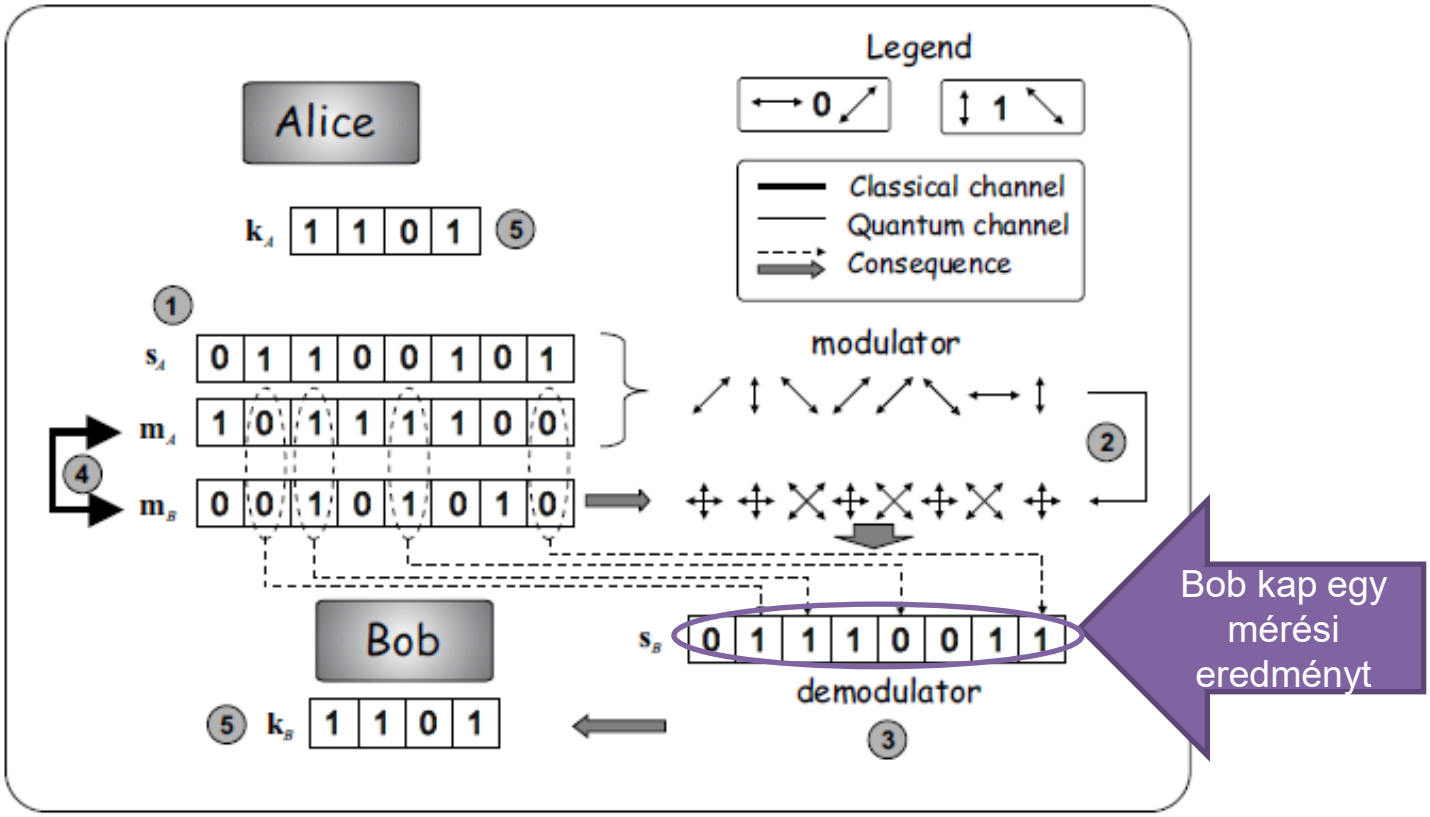


BB84

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



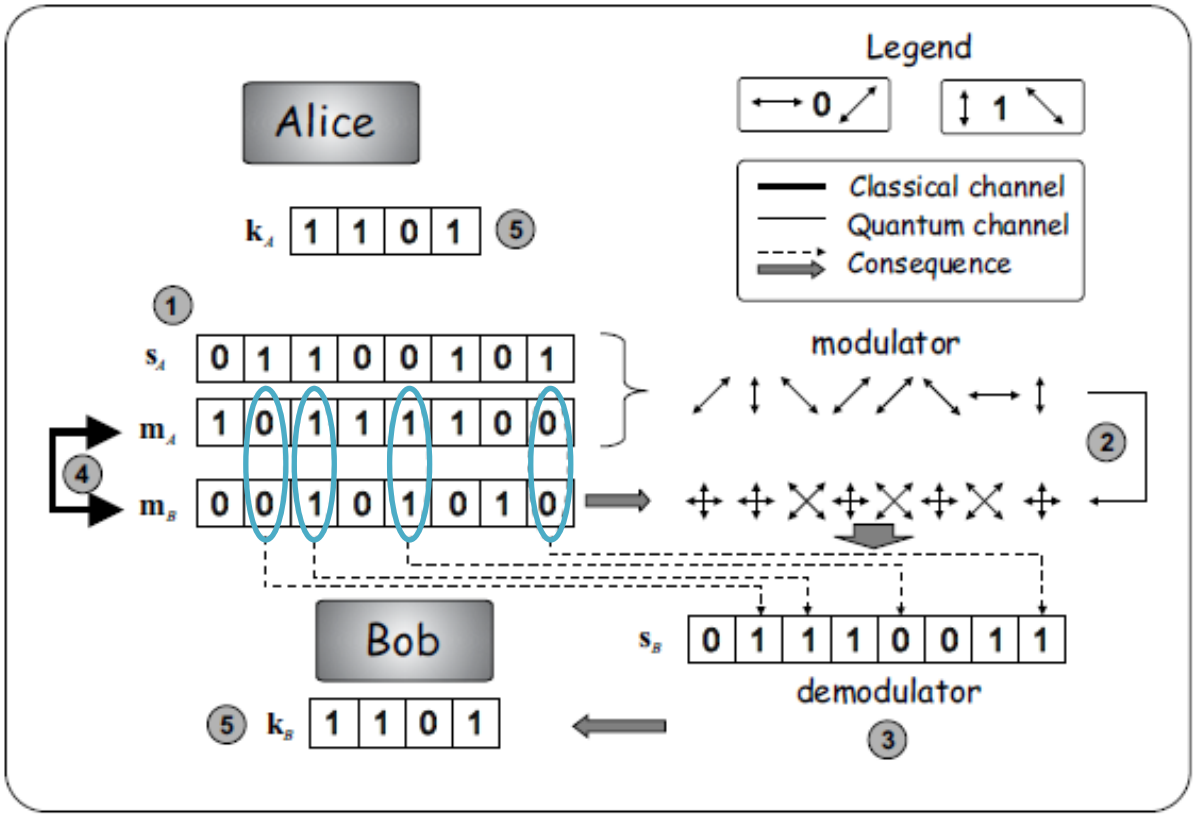
- Első generációs megoldás
  - Fotonok polarizációs állapota a kvantumbit
  - Kihívás: egyfotonok előállítása és detektálása



BB84

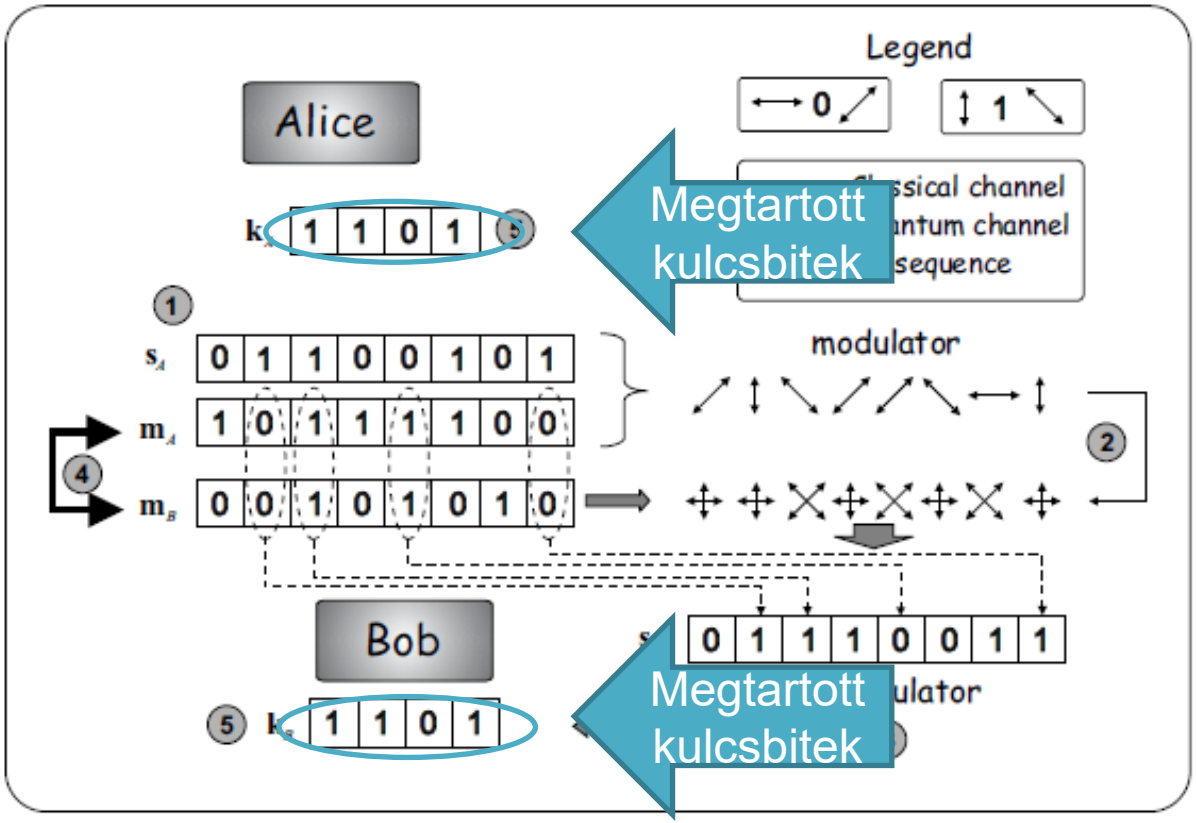
- Első generációs megoldás
  - Fotonok polarizációs állapota a kvantumbit
  - Kihívás: egyfotonok előállítása és detektálása

Ahol a bázisok megegyeznek, ott a küldött és mért bitértékek megegyeznek

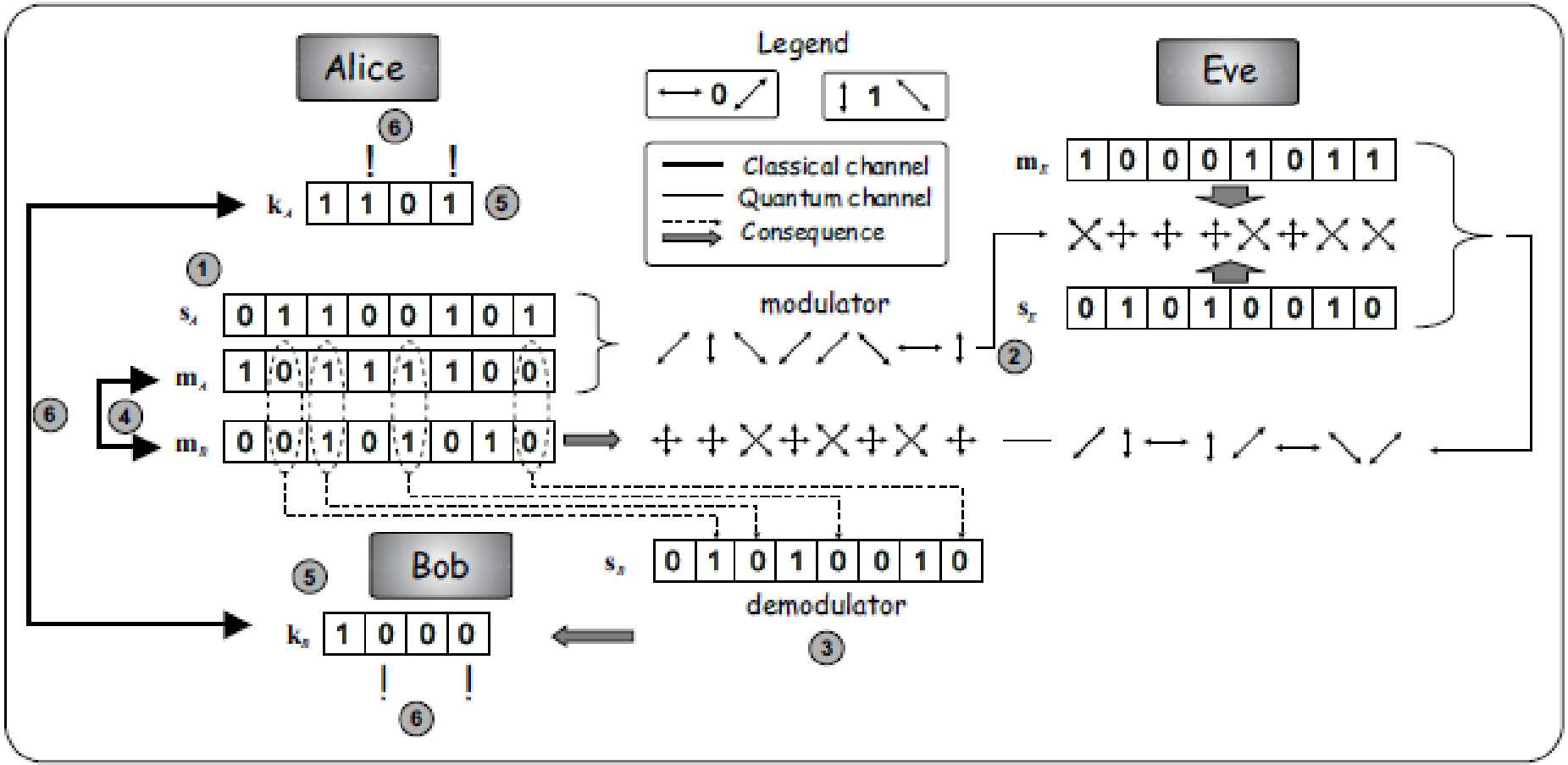


- Első generációs megoldás
  - Fotonok polarizációs állapota a kvantumbit
  - Kihívás: egyfotonok előállítása és detektálása

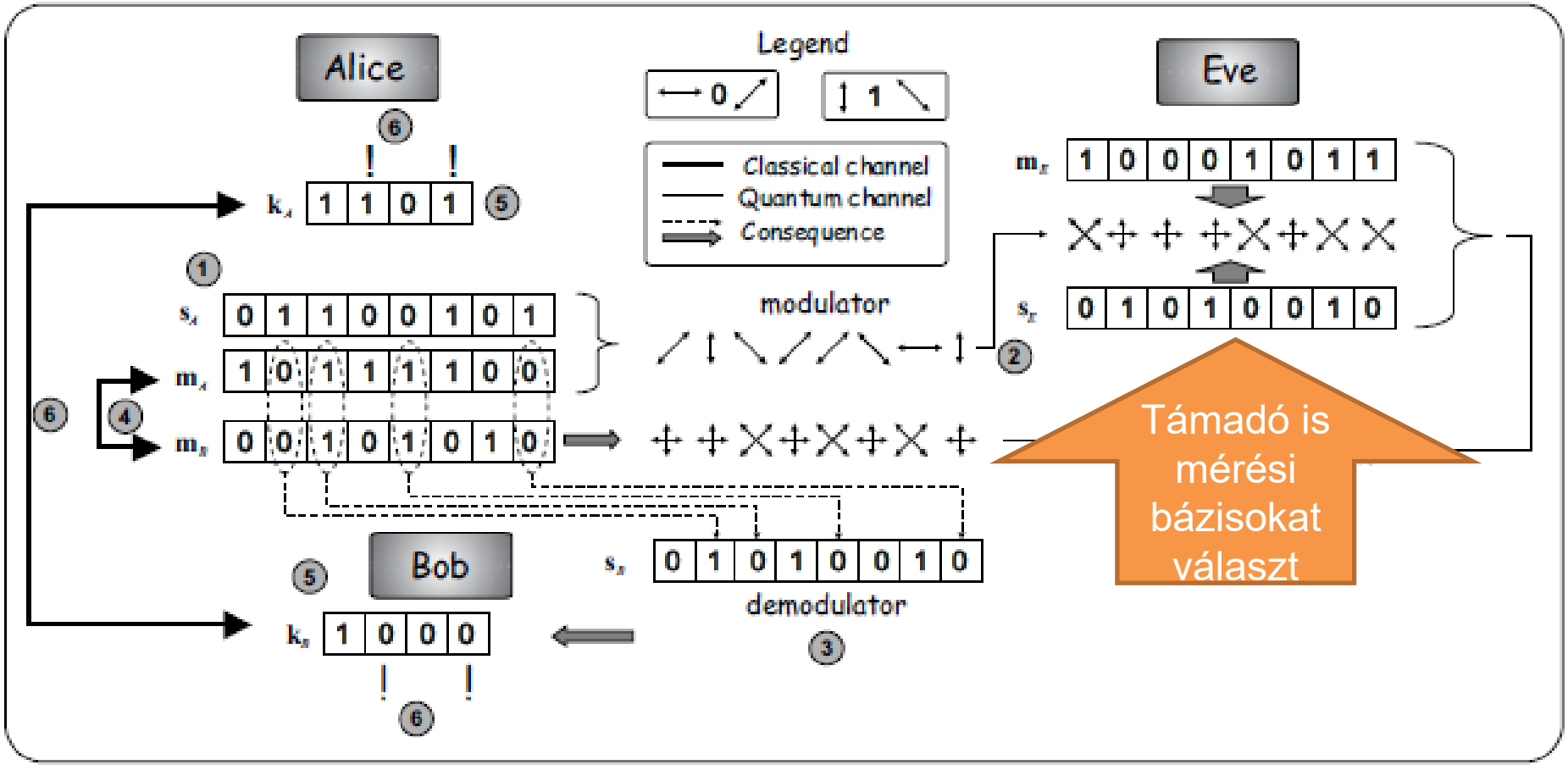
Aliz és Bob nyilvános csatornán egyeztetik a bázisokat. (De a küldött/mért bitértéket nem.) Ha ugyan azt a bázist használták, megtartják a bitértéket.



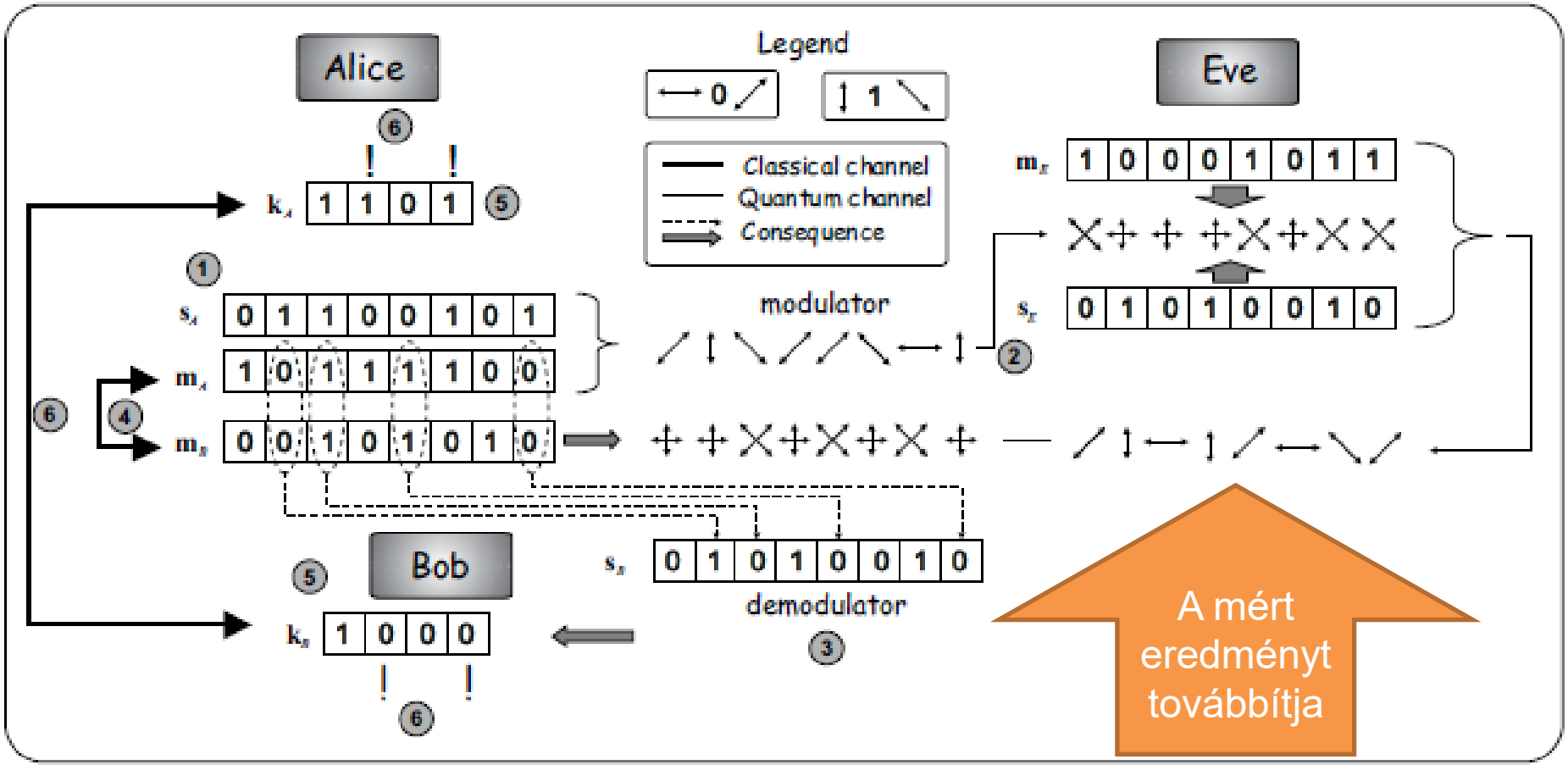
TÁMADÁSI KÍSÉRLET



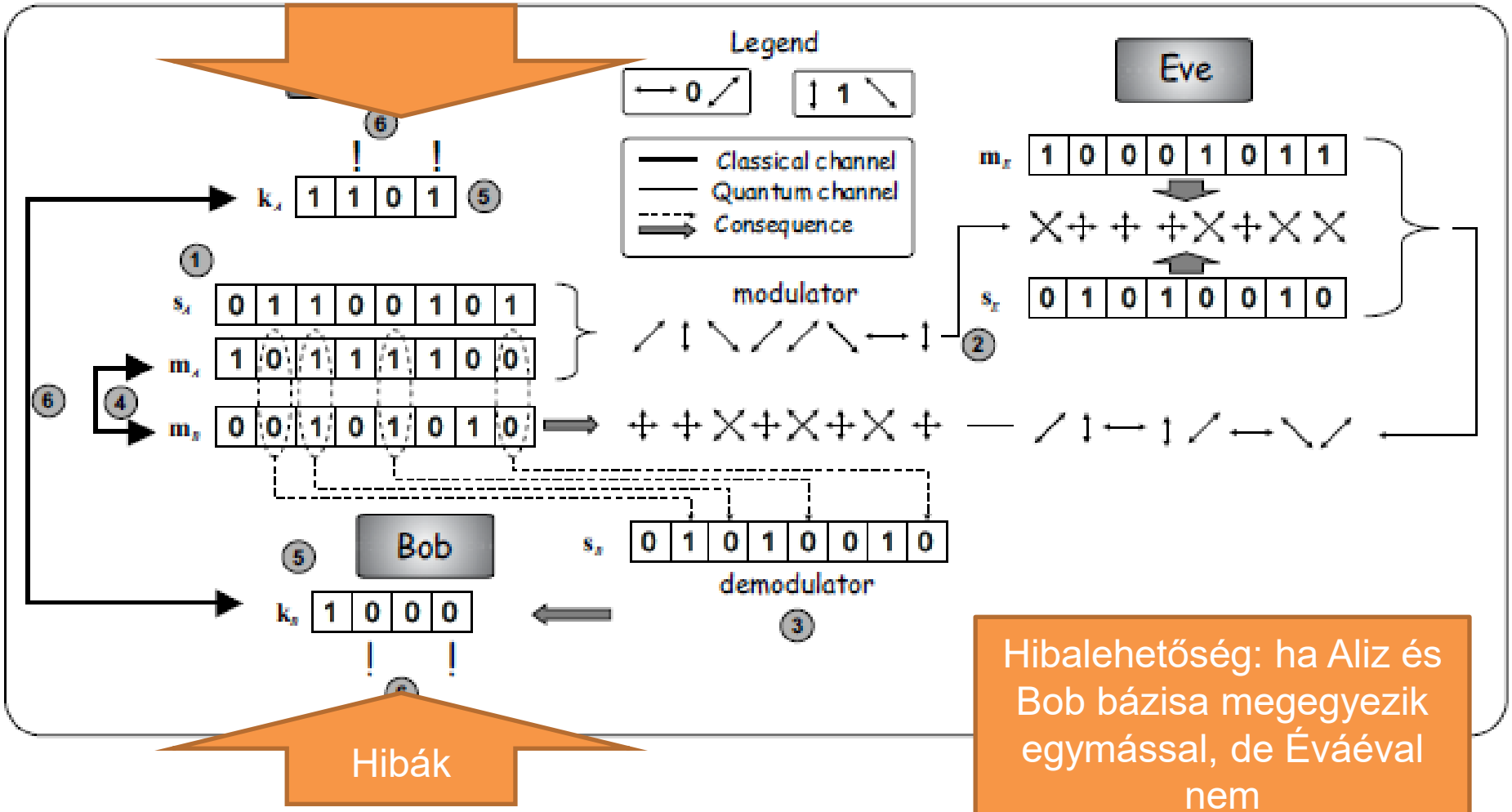
TÁMADÁSI KÍSÉRLET



TÁMADÁSI KÍSÉRLET

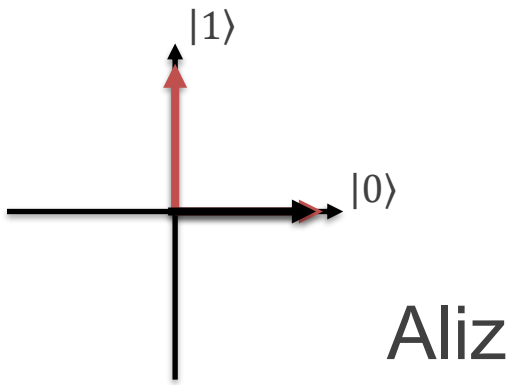


TÁMADÁSI KÍSÉRLET

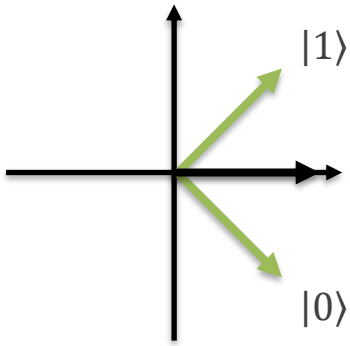


B92 protokoll

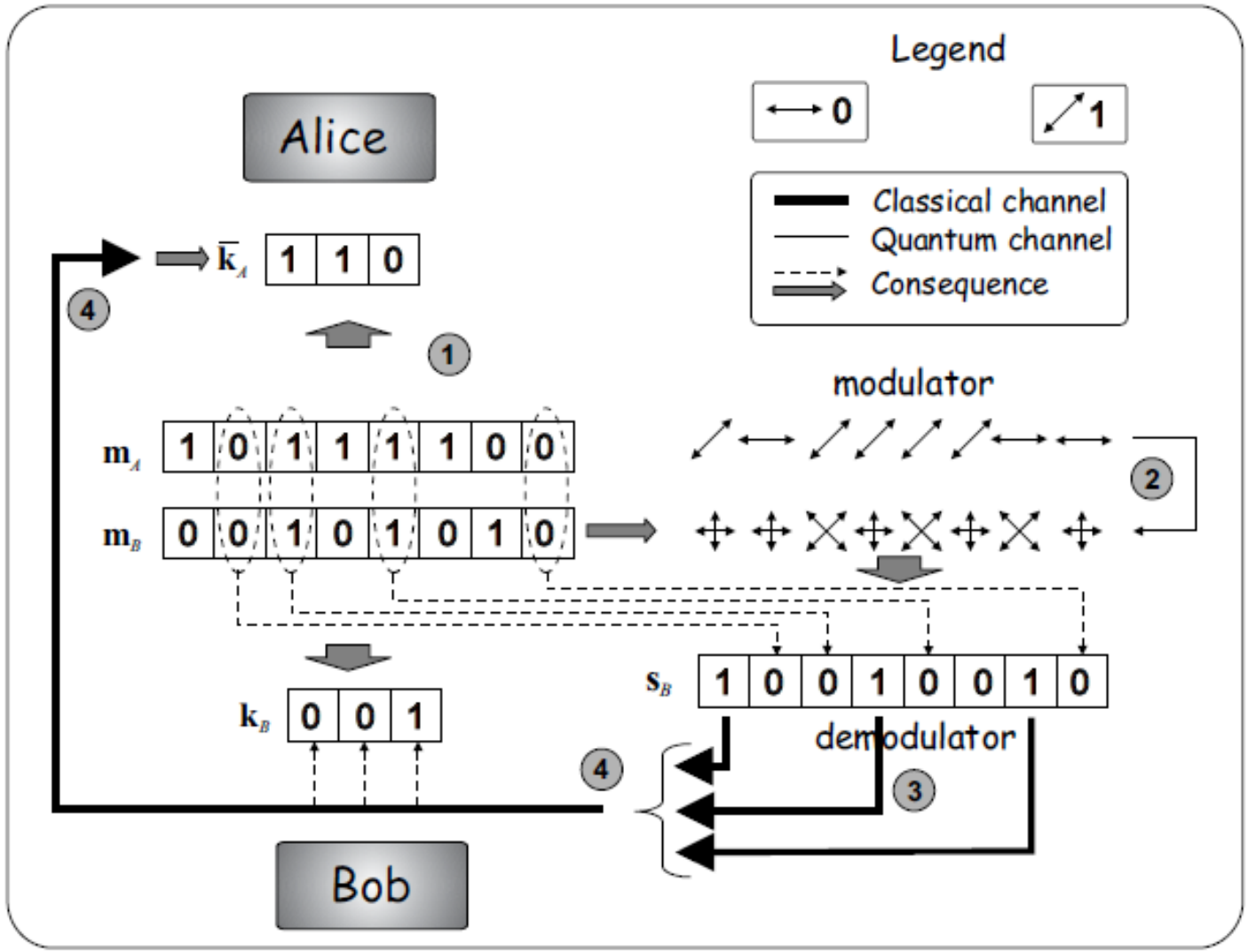
- Alapgondolat:
  - Ha Bob más mérési eredményt kap, mint amit Aliz küld (0 helyett 1), akkor Aliz tudja, hogy Bob rossz bázisban mért
  - Aliz és Bob a bitértéket beszélik meg nyilvánosan, és a bázist tartják titokban
  - **A bázis maga szolgálhat kulcsként**

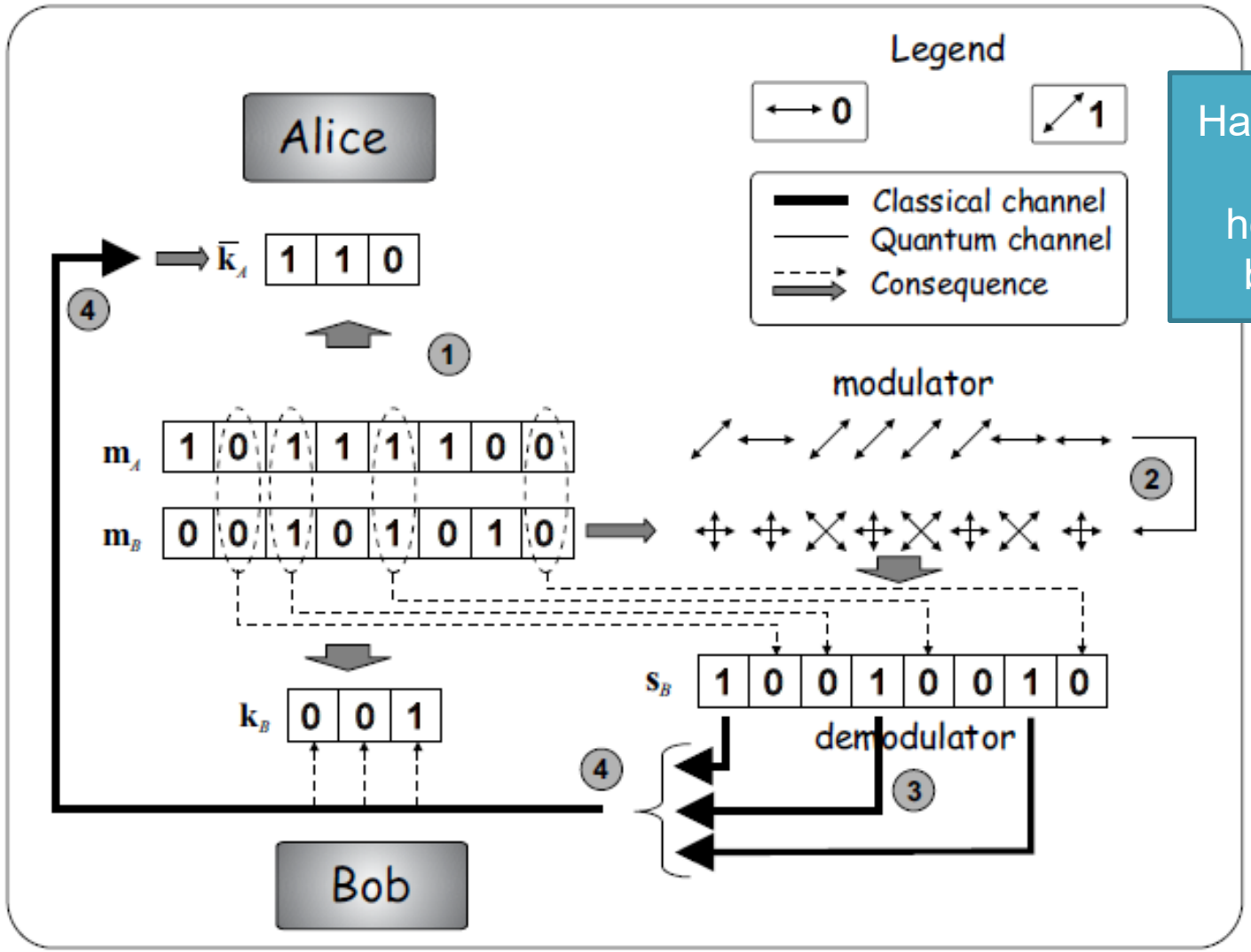


Aliz

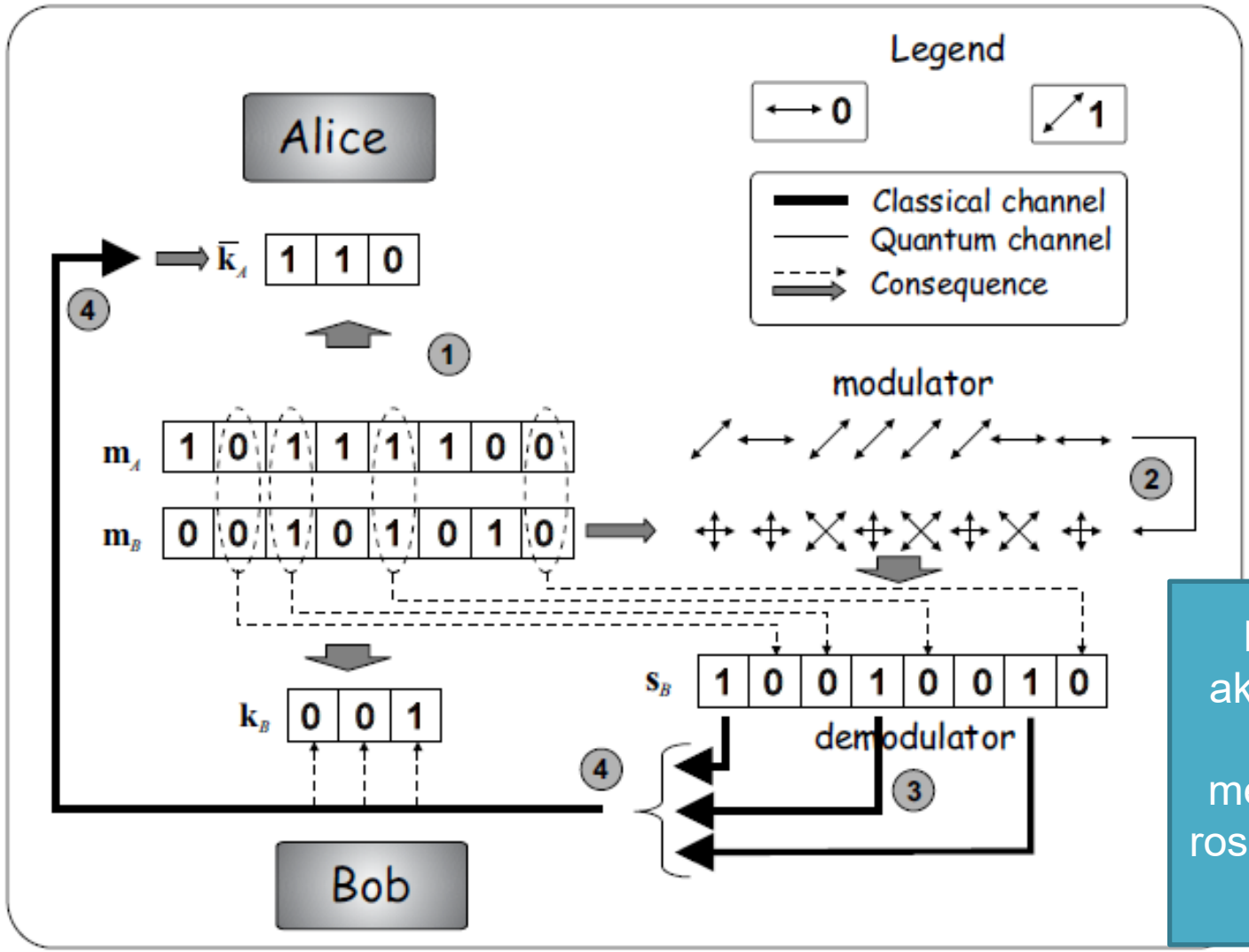


Bob

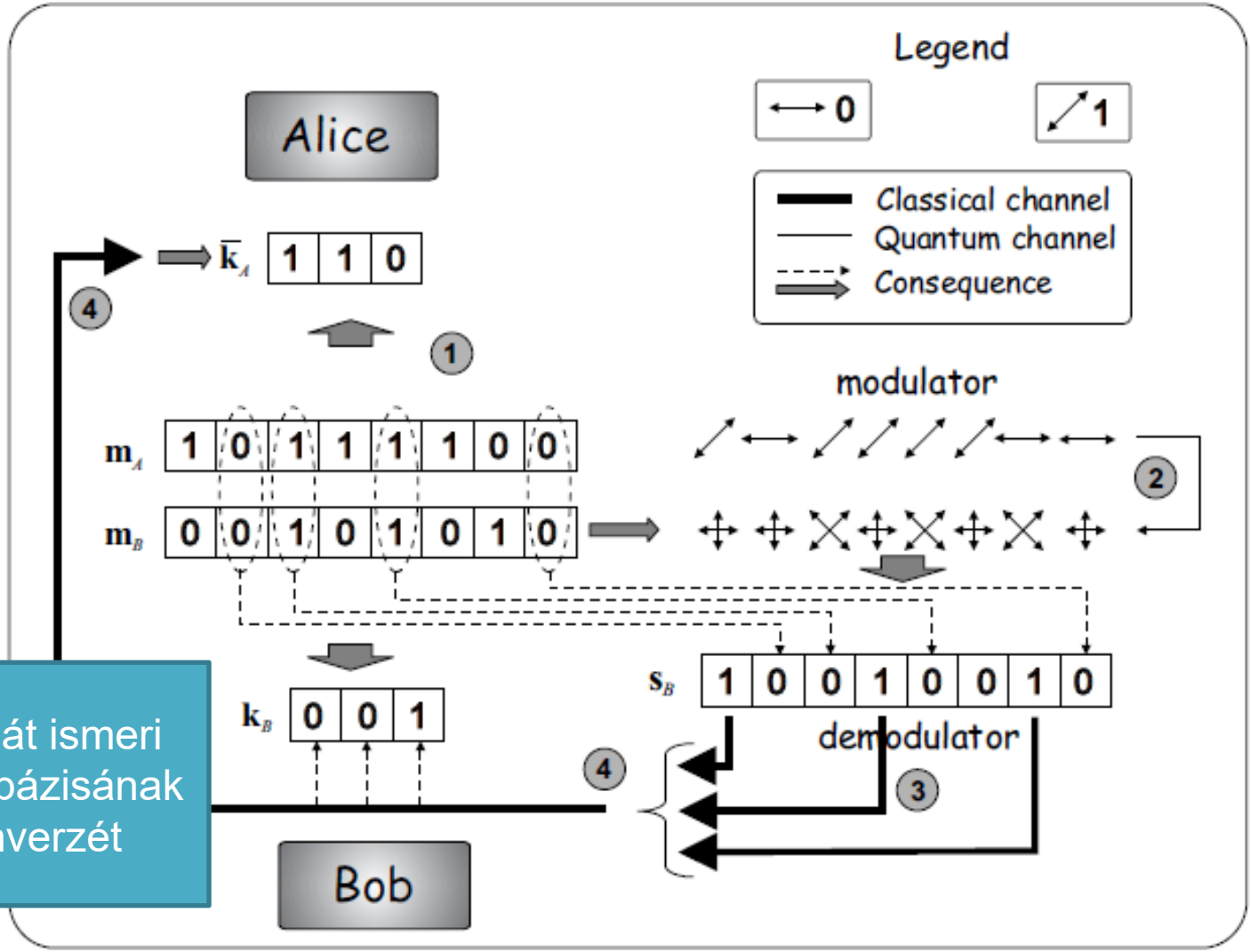

Legend
0
1
Classical channel
Quantum channel
Consequence
Alice
$\overline{k}_A$ 1 1 0
4
1
modulator
m_A 1 0 1 1 1 1 0 0
m_B 0 0 1 0 1 0 1 0
2
s_B 1 0 0 1 0 0 1 0
demodulator
k_B 0 0 1
4
3
Bob



Hasonló, csak a bázis hordozza a bitértéket



Bob csak akkor kaphat 1-est a mérésből, ha rossz bázisban mért



Tehát ismeri Aliz bázisának inverzét

A valóság nem ideális

NEM IDEÁLIS KVANTUMCSATORNA

- A lehallgatás növeli a hibarátát (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

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

HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

KÖSZÖNETNYILVÁNÍTÁS

The development of this course material has received funding from the European Union under grant agreement No 101081247 (QCIHungary project) and has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.