

|                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                    |                                                               |                     |                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|---------------------|------------------------------------------------------------------------------------|
| Óbudai Egyetem<br>Neumann János Informatikai Kar                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                    | Biomatika és Alkalmazott Mesterséges<br>Intelligencia Intézet |                     |                                                                                    |
| Tantárgy neve és kódja:                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                    | Kreditérték: 4                                                |                     |                                                                                    |
| Bevezetés a kvantuminformatikába                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                    | NBVB11HBNE                                                    |                     |                                                                                    |
| Mérnök informatikus BSc/MSc szak                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                    | Nappali tagozat 2022/23 tanév 1. félév                        |                     |                                                                                    |
| Tantárgyfelelős oktató:                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                    | Prof. Kozlovszky<br>Miklós                                    | Oktatók:            | Prof. Kozlovszky Miklós,<br>Dr. Csilling Ákos,<br>Bringye Zsolt,<br>Gottdank Tibor |
| Előtanulmányi feltételek:<br>(kóddal)                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                    |                                                               |                     |                                                                                    |
| Heti óraszámok:                                                                                                                                                                                                                                                                                                                         | Előadás: 1.5                                                                                                                                                                                                                                                       | Tantermi gyak.: 0                                             | Laborgyakorlat: 0.5 | Konzultáció: (külön)                                                               |
| Számonkérés<br>módja (s,v,f):                                                                                                                                                                                                                                                                                                           | F                                                                                                                                                                                                                                                                  |                                                               |                     |                                                                                    |
| A tananyag                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                    |                                                               |                     |                                                                                    |
| Oktatási cél: A kvantuminformatika napjainkban egyre nagyobb teret hódít. Cél a kvantuminformatika, és a benne rejlő lehetőségek megismertetése a hallgatókkal. Betekintés a kvantum számításokat lehetővé tevő architektúrákba, a kvantum elmélet alapjaiba, a kvantum kriptográfiába, a jelenlegi kvantum programozási környezetekbe. |                                                                                                                                                                                                                                                                    |                                                               |                     |                                                                                    |
| Tematika:                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                    |                                                               |                     |                                                                                    |
| Bevezetés a kvantuminformatikába. Kvantum mechanika elméleti alapjai, kvantum kriptográfia alapjai, poszt-quantumkriptográfia. Legfontosabb kvantum számítástechnikai hardverek, architektúrák, kvantum programozási környezetek, programok.                                                                                            |                                                                                                                                                                                                                                                                    |                                                               |                     |                                                                                    |
| Ütemezés:                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                    |                                                               |                     |                                                                                    |
| Oktatási hét<br>(konzultáció)                                                                                                                                                                                                                                                                                                           | Témakör                                                                                                                                                                                                                                                            |                                                               |                     |                                                                                    |
| 1.                                                                                                                                                                                                                                                                                                                                      | Bevezetés a kvantum számítástechnikába: Története, előzmények, Felhasználási területek, előnyök, hátrányok                                                                                                                                                         |                                                               |                     |                                                                                    |
| 2.                                                                                                                                                                                                                                                                                                                                      | Technológiák, architektúrák, megoldások bemutatása, összehasonlítása. Technológia jövőképe, potenciál. Nemzetközi kitekintés, magyarországi és nemzetközi projektek, Kvantum kihívások, versenyek, Kvantumpárhuzamosság, Kvantumregiszter vs. klasszikus regiszter |                                                               |                     |                                                                                    |
| 3.                                                                                                                                                                                                                                                                                                                                      | Fizikai és matematikai alapok I., Hullámfüggvény, Qubit reprezentációk és megvalósítások                                                                                                                                                                           |                                                               |                     |                                                                                    |
| 4.                                                                                                                                                                                                                                                                                                                                      | Fizikai és matematikai alapok II., Részecske-hullám kettősség, Szuperpozíció, Határozatlanság, Alagúteffektus, Összefonódás<br>Kvantumteleportáció, Szupersűrű kódolás, Nem-klónozhatósági tétel                                                                   |                                                               |                     |                                                                                    |
| 5                                                                                                                                                                                                                                                                                                                                       | Kvantum számítástechnika Kvantumszámítási modellek, Kapu (Gate) kvantumszámítási modell, Kvantum hűtés (annealing) modell                                                                                                                                          |                                                               |                     |                                                                                    |
| 6.                                                                                                                                                                                                                                                                                                                                      | Fontosabb szereplők: kvantum szimulációs környezetek, kvantum programozási környezetek és nyelvek. Felhő alapú kvantum erőforrások és szimulátorok (live demo). Programozási alapok (egyszerű feladatok futtatása / megvalósítása).                                |                                                               |                     |                                                                                    |
| 7.                                                                                                                                                                                                                                                                                                                                      | Félévközi szintfelmérő dolgozat                                                                                                                                                                                                                                    |                                                               |                     |                                                                                    |
| 8.                                                                                                                                                                                                                                                                                                                                      | Kvantum programozás alapkoncepciói, Qbit leírása, műveletek definiálása, egyszerűbb programstruktúrák megismerése példákon keresztül (szimulátorokon)                                                                                                              |                                                               |                     |                                                                                    |
| 9.                                                                                                                                                                                                                                                                                                                                      | Kvantum programozás: elterjedt kvantum programozási nyelvek használata és összehasonlítása /Leap™ quantum felhő szolgáltatáson, MS Azure felhő szolgáltatáson (Q# / Qiskit / Google Quantum Cirq)/                                                                 |                                                               |                     |                                                                                    |
| 10.                                                                                                                                                                                                                                                                                                                                     | Kriptográfia, alapok, alapfogalmak: Algoritmus-komplexitás, Kriptológia, Kriptográfiai protokollok, titkosítások, egykulcsos, többkulcsos                                                                                                                          |                                                               |                     |                                                                                    |
| 11.                                                                                                                                                                                                                                                                                                                                     | Kvantumkriptográfia, A kvantumkriptográfia alapfogalmai, Kvantuminformatika és titkosítás, Qubit, Feltörhetetlenség, Kvantumállapot ábrázolása Bloch gömbbel                                                                                                       |                                                               |                     |                                                                                    |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | A kvantuminformatika és a kvantumkriptográfia algoritmusai, Poszt kvantumkriptográfia, A kvantumkriptográfia határai, Polarizációváltás A QKD szerepe a kvantumkriptográfiában, NIST PQC szabványosítás, Az OQS projekt, Kriptográfiai típusok PQC-ben, Kvantumhálózati verem |
| 13.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Féléves feladat leadása                                                                                                                                                                                                                                                       |
| 14.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Félév végi szintfelmérő dolgozat                                                                                                                                                                                                                                              |
| <p style="text-align: center;"><b>Félévközi követelmények</b></p> <p>A hallgató az aláírást csak abban az esetben kaphatja meg, ha a félév során az előadásokhoz kapcsolódó önálló tudásfelmérő tesztet sikerrel (legalább elégséges szinten) megoldotta, és ha a félév során a féléves feladatot megfelelő minőségben elkészítette, és ha a félévközi, valamint félév végi szintfelmérő/számonkérő dolgozata legalább elégséges.</p>                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                               |
| Oktatási hét<br>(konzultáció)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                               |
| 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Félévközi szintfelmérő/számonkérő dolgozat.                                                                                                                                                                                                                                   |
| 13.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Féléves feladat leadása                                                                                                                                                                                                                                                       |
| 14.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Félév végi szintfelmérő/számonkérő dolgozat.                                                                                                                                                                                                                                  |
| <p><b>Pótlás módja</b></p> <ul style="list-style-type: none"> <li>Ha a félévközi szintfelmérő dolgozat minősége nem éri el az elégséges szintet (50%), akkor a dolgozat pótlására pótlási alkalom (14. héten) áll a hallgató rendelkezésére.</li> <li>Ha a hallgató a félév végi zárthelyi dolgozatot megírta, de nem érte el az 50%-ot, akkor a TVSz-ben meghatározott módon vizsgaidőszak első hetében egy alkalommal, egy előre megadott időpontban kísérletet tehet a javítására.</li> </ul>                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                               |
| <p><b>A félévzáró érdemjegy (J) kialakításának módszere:</b><br/>Amennyiben a hallgató a félév során minden követelményt teljesített: a két szintfelmérő/számonkérő dolgozat, és az elkészített féléves feladat alapján kap érdemjegyet.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                               |
| <b>Irodalom:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                               |
| Kötelező:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                               |
| Az előadás fóliák, valamint az előadásokon ismertetett WEB linkek, kiegészítő segédanyagok.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                               |
| Ajánlott:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                               |
| <p>Kozlovsky M., Gottdank T., Bringye Zs., Csilling Á.: Kvantuminformatika és kvantumkriptográfia, OE jegyzet;2022<br/> Jozef Grusk;Quantum Computing;1999; Osborne/McGraw-Hill ;ISBN-10:0077095030;<br/> Ronald de Wolf; Quantum Computing:Lecture Notes, 2021; arXiv:1907.09415v2<br/> ETSI White Paper No. 8 ; Quantum Safe Cryptography and Security<br/> W. Beiglböck J. Ehlers K. Hepp H. Weidenmüller; Lecture Notes in Physics; Vol. 827;Springer;<br/> <a href="http://www.springer.com/series/5304">http://www.springer.com/series/5304</a><br/> Michael A. Nielsen &amp; Isaac L. Chuang; Quantum Computation and Quantum Information; Cambridge University Press;2010; ISBN 978-1-107-00217-3<br/> Eleanor Rieffel and Wolfgang Polak; QUANTUM COMPUTING; A Gentle Introduction; MIT Press; 2011; ISBN 978-0-262-01506-6</p> |                                                                                                                                                                                                                                                                               |