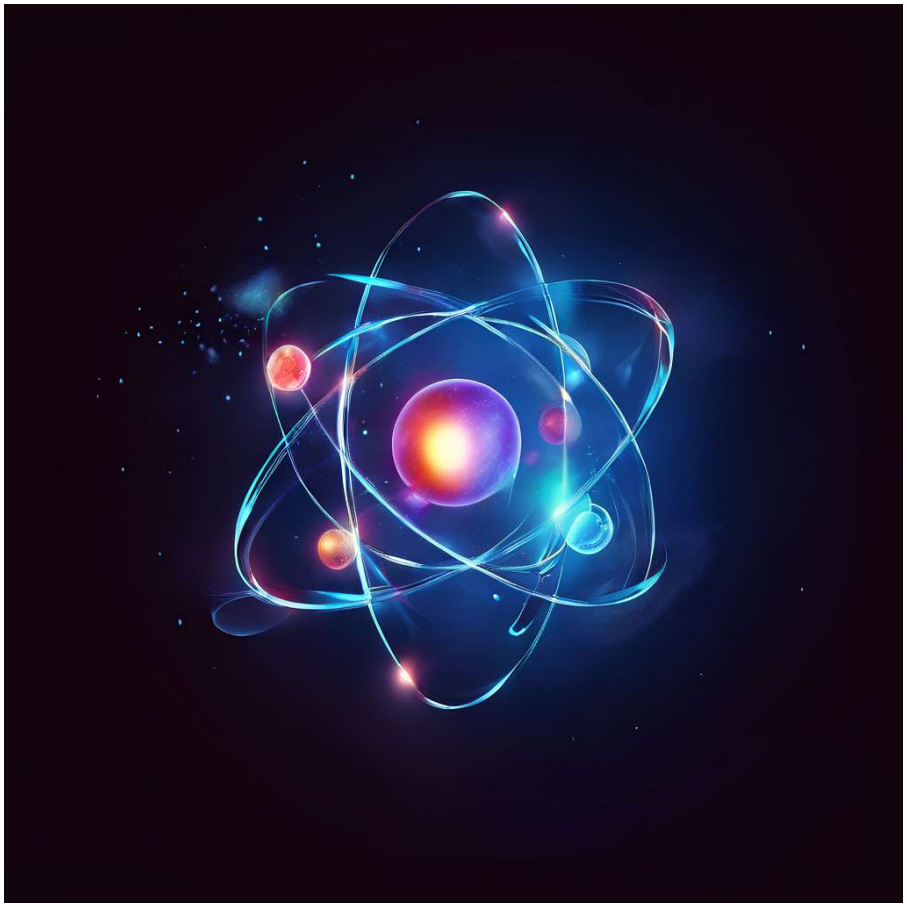
Metode Criptografice Cuantice

Concepte, implementări si descoperiri

UNIVERSITATEA OVIDIUS CONSTANTA
CyberSecurity Ovidius Camp
prof. dr. RACUCIU CIPRIAN
masterand Vlad Belciug

2024

Cuprins



1. Introducere în Criptografie

Criptografia reprezintă o ramură a matematicii care se ocupă cu securizarea informației, precum și cu autentificarea și restricționarea accesului într-un sistem informatic. Securizarea informației se face prin transformarea datelor într-un format sigur, pentru a preveni accesul neautorizat,

De-a lungul timpului, criptografia a evoluat de la simple substituții și permutări la algoritmi matematici complecși.

Termenul criptografie este compus din cuvintele de origine greacă κρυπτός kryptós (ascuns) și γράφειν gráfein (a scrie).

Pentru a-și îndeplini scopul, criptografia utilizează atât metode matematice (profitând, de exemplu, de dificultatea factorizării numerelor foarte mari), cât și metode de criptare cuantică.

Tipuri de criptografie:

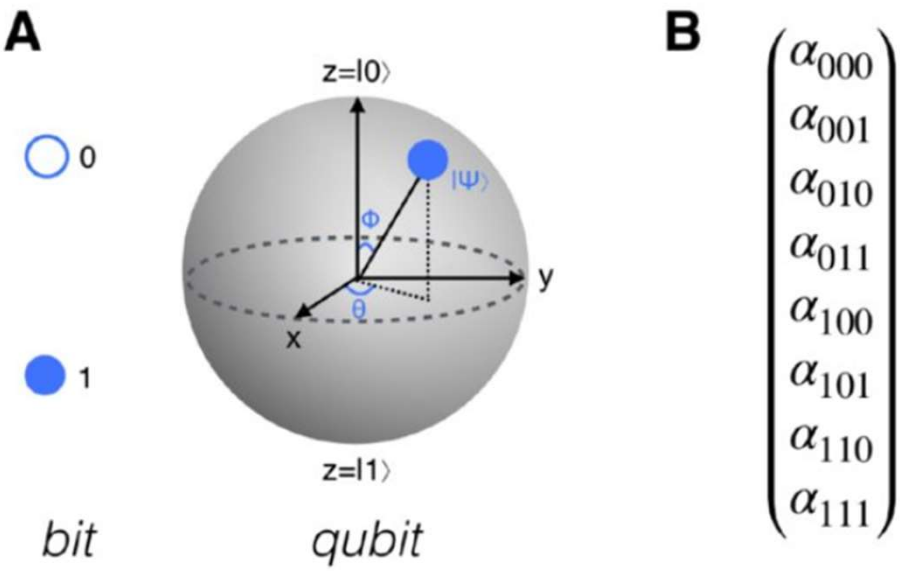
Criptografie simetrică: Utilizează aceeași cheie pentru criptare și decriptare (ex. AES).

Criptografie asimetrică: Utilizează o pereche de chei – una publică și una privată (ex. RSA).

2. Bit și Qubit

Bitul (Binary Digit) este unitatea fundamentală de informație în sistemele de calcul clasice. Un bit poate avea una dintre două valori distincte: 0 sau 1. Aceste două stări sunt utilizate pentru a reprezenta și manipula informația în computerele digitale, rețele și alte sisteme de comunicații.

Qubitul (Quantum Bit) este unitatea fundamentală de informație în calculul cuantic. Spre deosebire de bitul clasic, un qubit poate exista simultan în mai multe stări datorită fenomenului de superpoziție. Aceasta înseamnă că un qubit poate fi 0, 1 sau orice combinație liniară a acestor stări (superpoziție), ceea ce este exprimat matematic ca $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, unde α și β sunt coeficienți complexi care determină probabilitățile fiecărei stări. În plus, qubitul beneficiază și de legătura cuantică, prin care starea unui qubit poate fi corelată cu starea altui qubit, chiar dacă se află la distanță mare unul de celălalt.



3. Criptografia Cuantică

Criptografia cuantică este o ramură avansată a criptografiei care utilizează principiile mecanicii cuantice pentru a îmbunătăți securitatea comunicațiilor. Aceasta promite o siguranță mult mai mare decât metodele tradiționale, datorită proprietăților unice ale particulelor cuantice.

Principii de Bază ale Criptografiei Cuantice

Superpoziția: Particulele cuantice, precum fotonii, pot exista în mai multe stări simultan.

Legarea cuantică: Două particule cuantice pot deveni legate într-un mod în care starea unei particule influențează instantaneu starea celeilalte, indiferent de distanță.

Non-clonarea: o stare cuantică necunoscută arbitrară nu poate fi copiată perfect. (clonată)

Principiul incertitudinii (Heisenberg): Măsurarea unei proprietăți cuantice modifică automat alte proprietăți, prevenind astfel interceptarea fără a fi detectată.

3. Criptografia Cuantică (continuare)

Metodele criptografice cuantice utilizează principiile mecanicii cuantice pentru a asigura securitatea transmisiunii datelor, cea mai cunoscută metodă fiind Distribuția Cuantică a Cheilor (QKD). De asemenea, metodele criptografice cuantice includ Generarea Cuantică de Numere Aleatorii (QRNG) și Comunicarea Directă Securizată Cuantică (QSDC).

Dincolo de aceste metode cuantice directe, există și **tehnici criptografice post-cuantice** proiectate pentru a rezista atacurilor din partea computerelor cuantice.

Pe măsură ce cercetarea avansează, rețelele criptografice cuantice, care încorporează repetitori și routere cuantice, sunt dezvoltate pentru a extinde capacitățile de comunicare securizată la scară largă, astfel preconizându-se a forma coloana vertebrală a infrastructurii de comunicare securizată a viitorului.

4. Distributia Cuantica a Cheilor (QKD)

Distributia cuantică a cheilor este una dintre cele mai promițătoare aplicații ale criptografiei cuantice. Aceasta permite ca două părți să împărtășească o cheie secretă cu un nivel de securitate inatacabil.

Protocolul BB84 este primul și cel mai cunoscut protocol de QKD, dezvoltat de Charles Bennett și Gilles Brassard în 1984. Acest protocol utilizează polarizarea fotonilor pentru a distribui o cheie secretă între două părți, Alice și Bob. Procesul este descris în pași simpli: Alice trimite fotoni către Bob, fiecare foton fiind polarizat în una din patru posibile stări (0°, 45°, 90°, 135°). Bob măsoară fotonii folosind o bază de măsurare aleatorie (0°/90° sau 45°/135°). Alice și Bob comunică public bazele folosite pentru măsurare, fără a dezvălui polarizările efective. Fotonii măsurați cu aceleași baze sunt păstrați, iar restul sunt eliminați, rezultând o cheie partajată sigură.

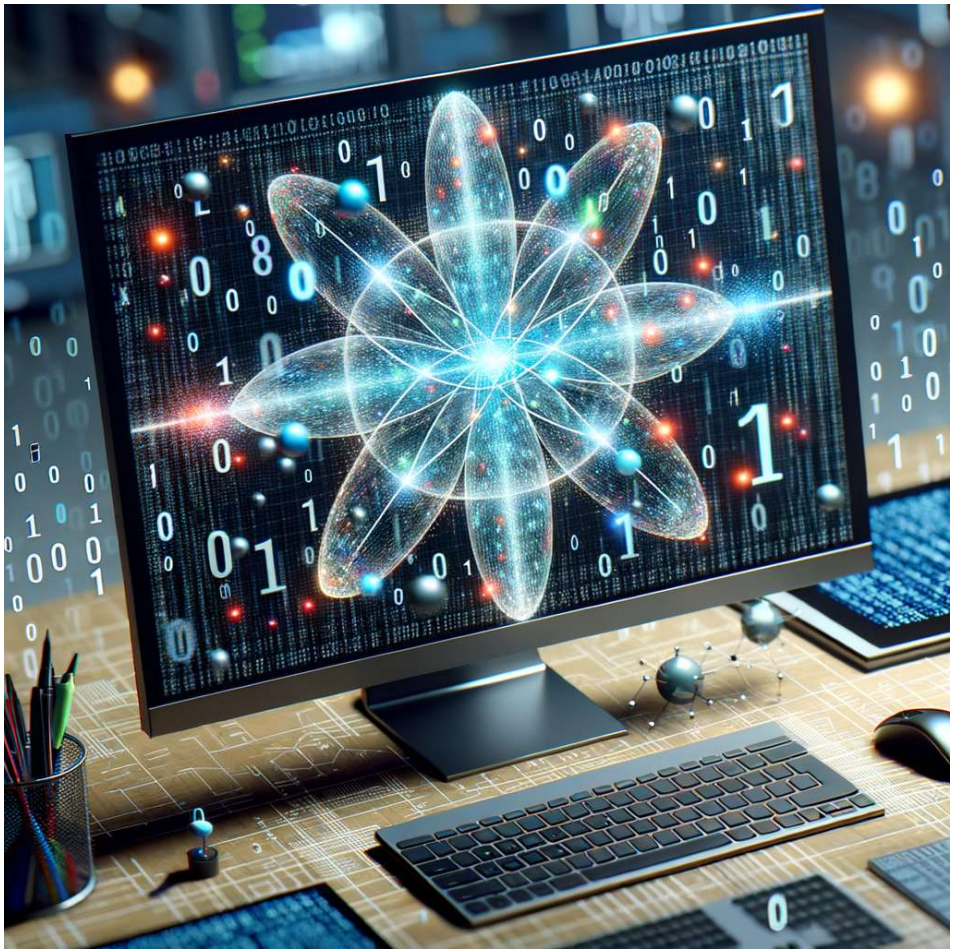
Protocolul E91 dezvoltat de Artur Ekert în 1991, utilizează fenomenul de legătură cuantică. În acest protocol, perechi de fotoni legați sunt distribuite către Alice și Bob. Măsurătorile efectuate pe acești fotoni sunt corelate în așa fel încât pot genera o cheie secretă, iar orice încercare de interceptare va perturba aceste corelații, detectând astfel prezența unui spion.

5. Generarea Cuantică de Numere Aleatorii (QRNG)

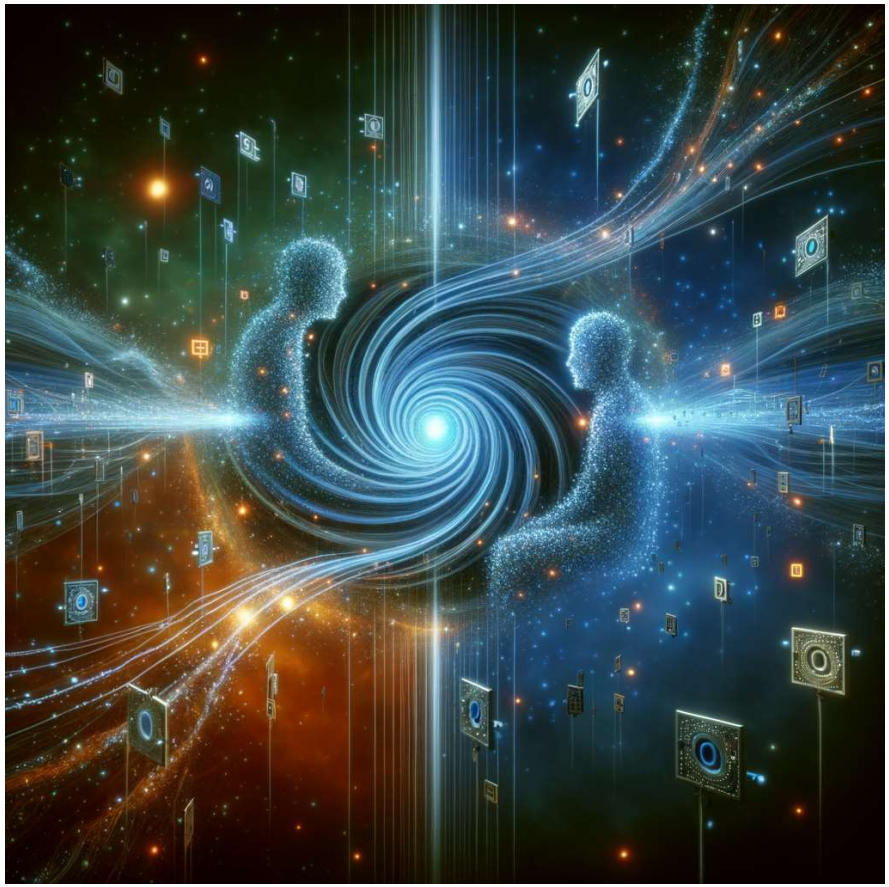
Generarea numerelor aleatorii este esențială în criptografie. QRNG utilizează principiile mecanicii cuantice pentru a genera numere aleatorii cu adevărat imprevizibile:

Principiu de Funcționare:
Se bazează pe măsurarea unor proprietăți cuantice ale particulelor, cum ar fi starea de polarizare a fotonilor.

Securitate:
Deoarece rezultatele măsurătorilor cuantice sunt fundamental imprevizibile, numerele generate sunt cu adevărat aleatorii, oferind un nivel de securitate mai ridicat decât metodele clasice.



6. Comunicarea Directă Securizată Cuantică (QSDC)



Spre deosebire de Quantum Key Distribution (QKD), în QSDC informația este transmisă direct într-o manieră sigură, fără a mai fi necesară o cheie suplimentară pentru decriptare. Informația este codificată **direct în stările cuantice ale particulelor**. Particulele cuantice care poartă informația codificată sunt transmise de la expeditor (Alice) către destinatar (Bob) printr-un canal cuantic. În timpul transmiterii, orice încercare de interceptare va perturba stările cuantice ale particulelor, ceea ce va fi detectat de către Bob.

Bob măsoară stările cuantice ale fotonilor recepționați și recuperează informația originală. Datorită principiului de nedeterminare al lui Heisenberg, orice interferență în procesul de transmisie este imediat detectabilă.

Limitări și Provocări: degradarea canalului, tehnologia actuală, distanța de transmisie.

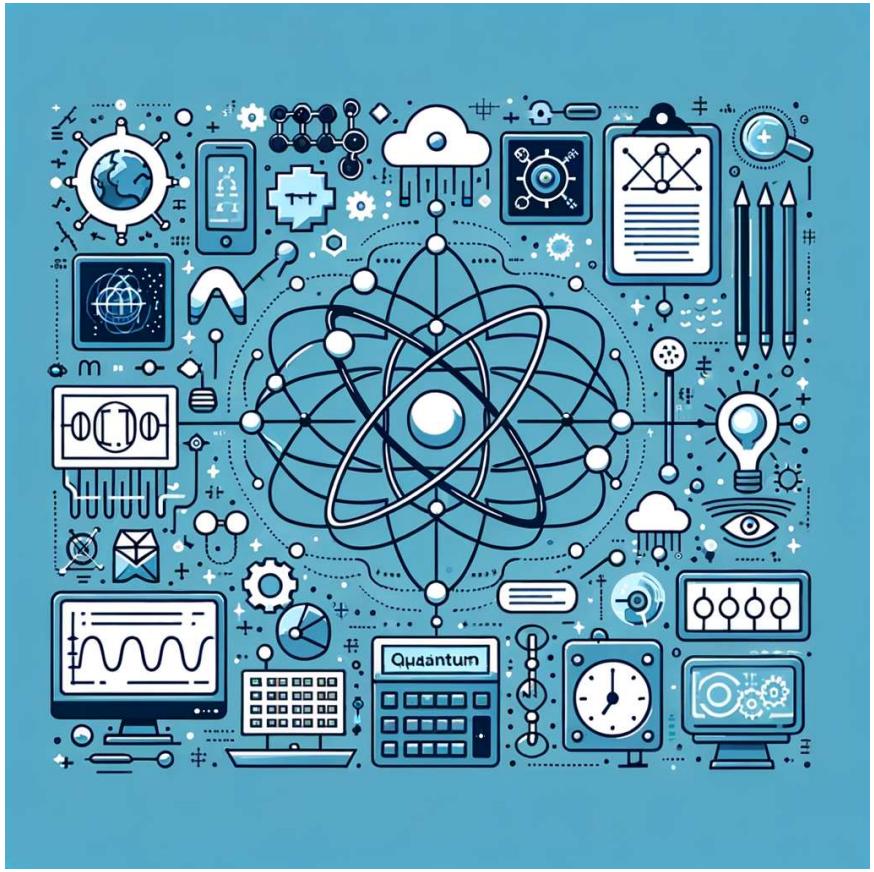
7. Criptografia Cuantică Post-Quantum

Criptografia cuantică post-quantum implică dezvoltarea de algoritmi criptografici care sunt siguri împotriva atacurilor cuantice, dar care nu se bazează pe principiile mecanicii cuantice. Aceștia includ:

Criptografia bazată pe latice: Utilizează structuri matematice numite lattice-uri pentru a crea probleme greu de rezolvat chiar și pentru computerele cuantice. (mulțimea submulțimilor unei mulțimi împreună cu relația de incluziune formează o latice)

Criptografia bazată pe cod: Bazată pe teoria codurilor corectoare de erori, aceasta include algoritmi precum McEliece și Niederreiter.

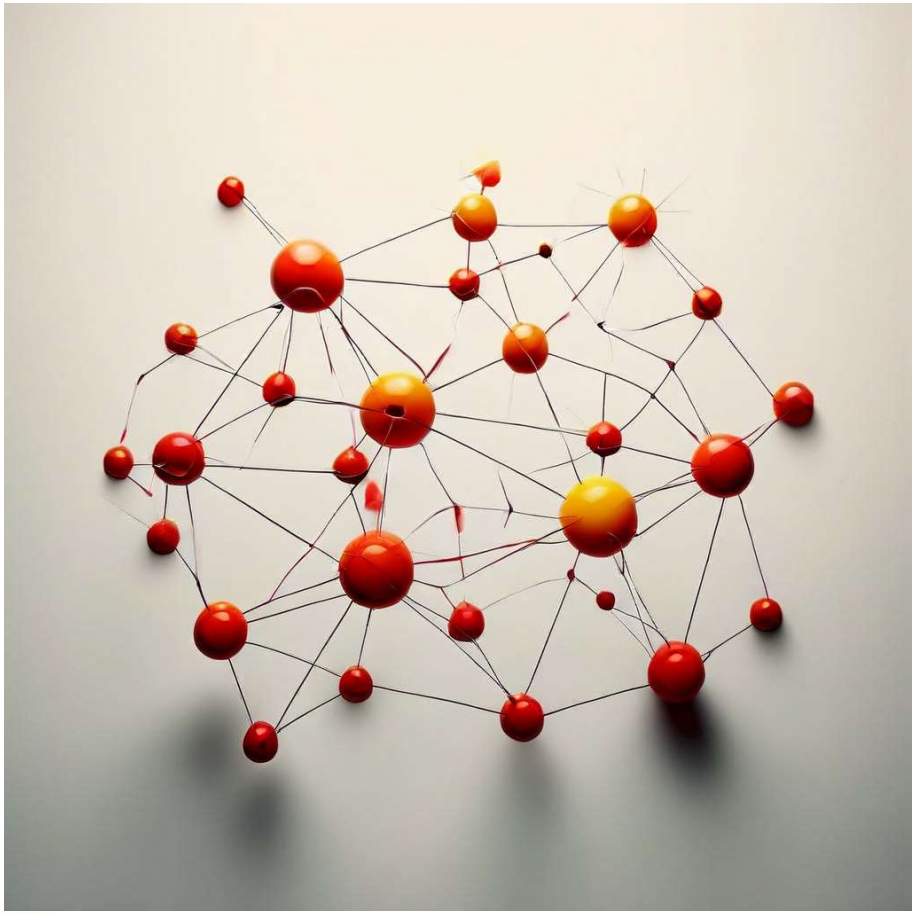
Criptografia multivariată polinomială: Utilizează sisteme de ecuații polinomiale multivariate care sunt dificil de rezolvat pentru computerele cuantice.



8. Rețele Cuantice și Repetitori Cuantici

Rețelele cuantice sunt formate din noduri cuantice, care pot fi computere cuantice, senzori cuantici sau alte dispozitive cuantice, interconectate prin canale de comunicații cuantice. Principalele componente ale rețelelor cuantice sunt qubit-ul, entanglementul cuantic, teleportarea cuantică (un protocol prin care starea cuantică a unui qubit poate fi transferată unui alt qubit aflat la distanță, fără a transfera efectiv qubit-ul în sine) și canalele cuantice (fibrele optice sau spațiul liber).

Repetitorii cuantici - într-o rețea clasică, repetitorii amplifică semnalul pentru a-l trimite pe distanțe mari. În rețelele cuantice, acest lucru nu este posibil direct din cauza principiului mecanicii cuantice care spune că măsurarea stării unui qubit distruge starea sa. În schimb, repetitorii cuantici utilizează protocoale speciale pentru a distribui entanglementul pe distanțe mari fără a măsura efectiv stările intermediare. Funcționarea repetitorilor cuantici se bazează pe anumite procese specifice, precum segmentarea, entanglement swap (transmiterea legăturii cuantice) sau corectarea erorilor cuantice .



9. Ultimele Descoperiri în Criptografia Cuantică

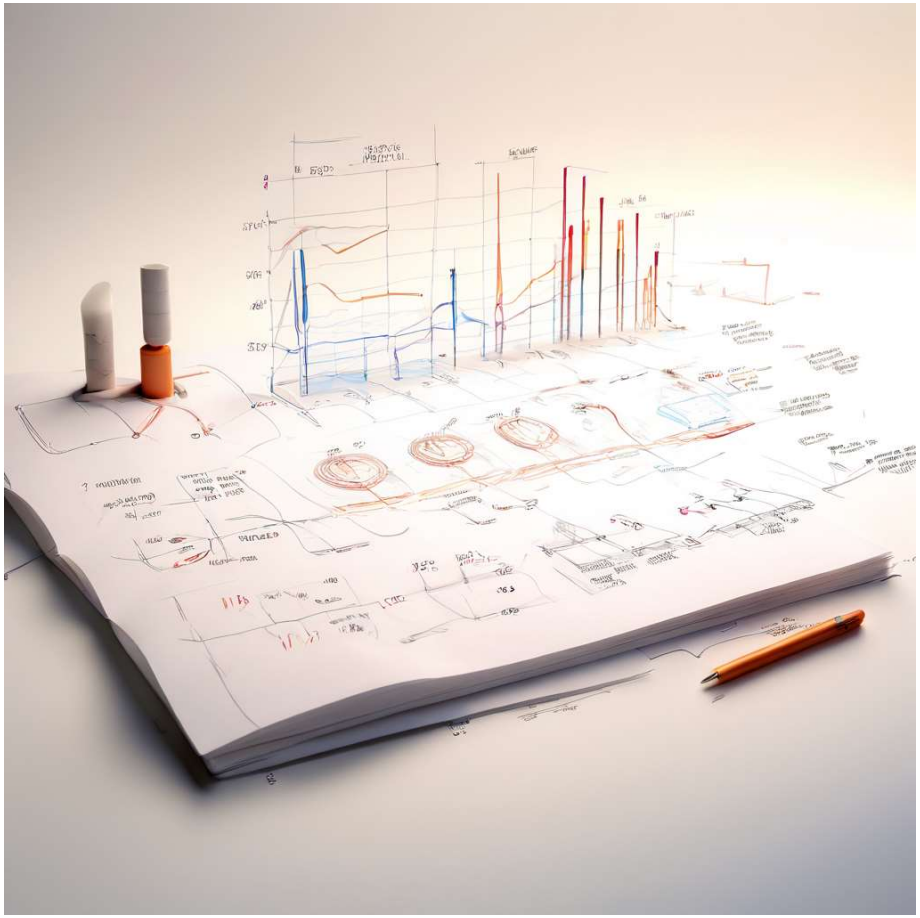
Distributia Cuantica a Cheilor (QKD)

Cercetătorii au dezvoltat un sistem de distribuție a cheilor cuantice (QKD) bazat pe componente fotonice din siliciu care poate transmite chei securizate la viteze fără precedent. - 29 mai 2023

Cercetătorii din mai multe instituții chineze au stabilit un nou record mondial prin realizarea unei distribuții a cheilor cuantice fără releu pe 1.002 km. - 14 iunie 2023

Cercetătorii de la Universitatea Tehnică din Danemarca (DTU) au folosit cu succes criptarea cuantică pentru transmiterea în siguranță a informațiilor pe o distanță de 100 de kilometri printr-un cablu de fibră optică - 5 aprilie 2024

Oamenii de știință pot acum să producă eficient perechi de fotoni legați aproape perfect cu ajutorul surselor de puncte cuantice. - 25 martie 2024



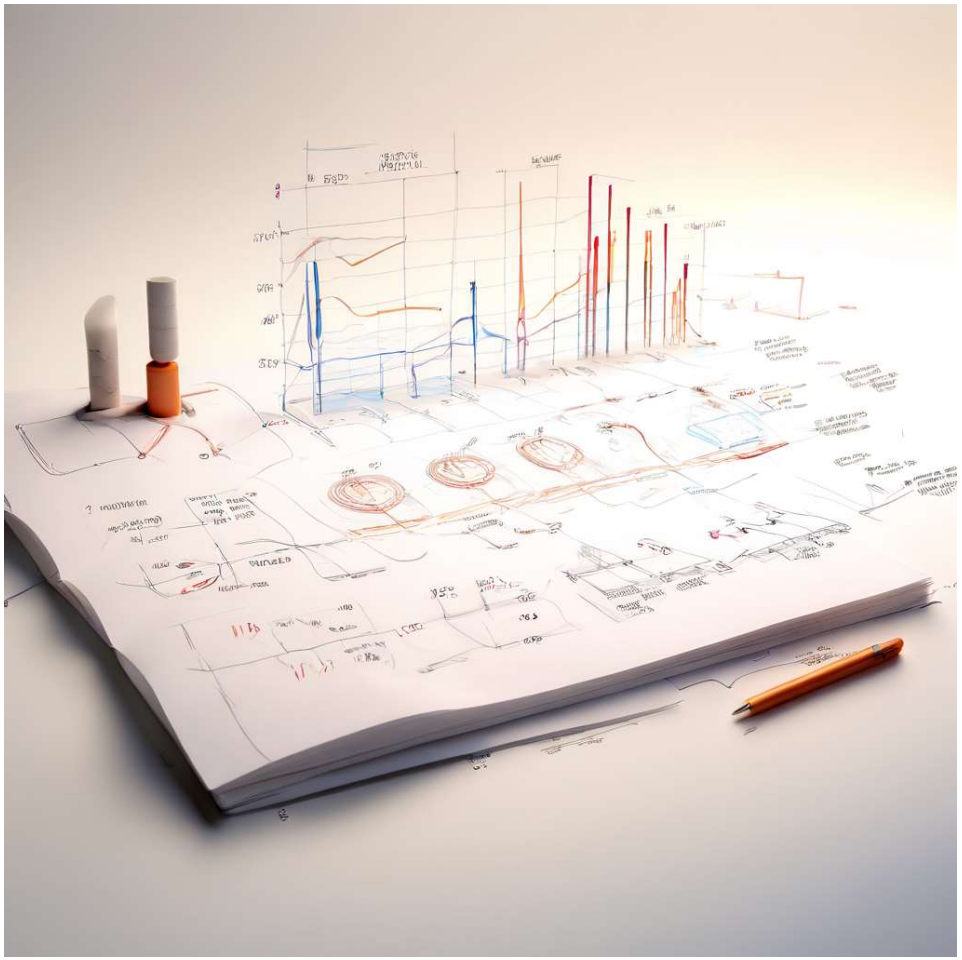
9. Ultimele Descoperiri în Criptografia Cuantică (continuare)

Generarea Cuantică de Numere Aleatorii (QRNG)

Noul generator de numere aleatorii cuantice atinge o viteză de 2 Gbit/s - „Aleatoria este acum o marfă valoroasă, deoarece conduce aproape toate protocoalele digitale care permit comunicarea privată”, - 11 iunie 2024

IDTechEx explorează oportunitățile pentru QRNG pe piața dispozitivelor conectate: “În general, cererea pentru soluții mai bune de securitate cibernetică pe piețele electronice de consum, auto și medical este inevitabilă.” - 10 aprilie 2024

Quantum Dice și BT Group testează generatoarele de numere aleatoare cuantice pentru securitate sporită a telecomunicațiilor: “VERTEX QD-1100 QRNG de la Quantum Dice, așa cum a fost prezentat de BT Group într-un hackathon de dezvoltare a cazurilor de utilizare QRNG în iulie 2023, combină cea mai bună securitate din clasă și o rată de 2,66 Gbps de numere aleatoare post-procesate cu un factor de formă PCIe compact. Dispozitivul profită, de asemenea, de protocolul unic brevetat de autocertificare independentă a dispozitivului sursă (DISC™) al Quantum Dice, care efectuează o verificare continuă a entropiei, oferind astfel o asigurare cuantică în timp real.” - 6 februarie 2024



9. Ultimele Descoperiri în Criptografia Cuantică (continuare)

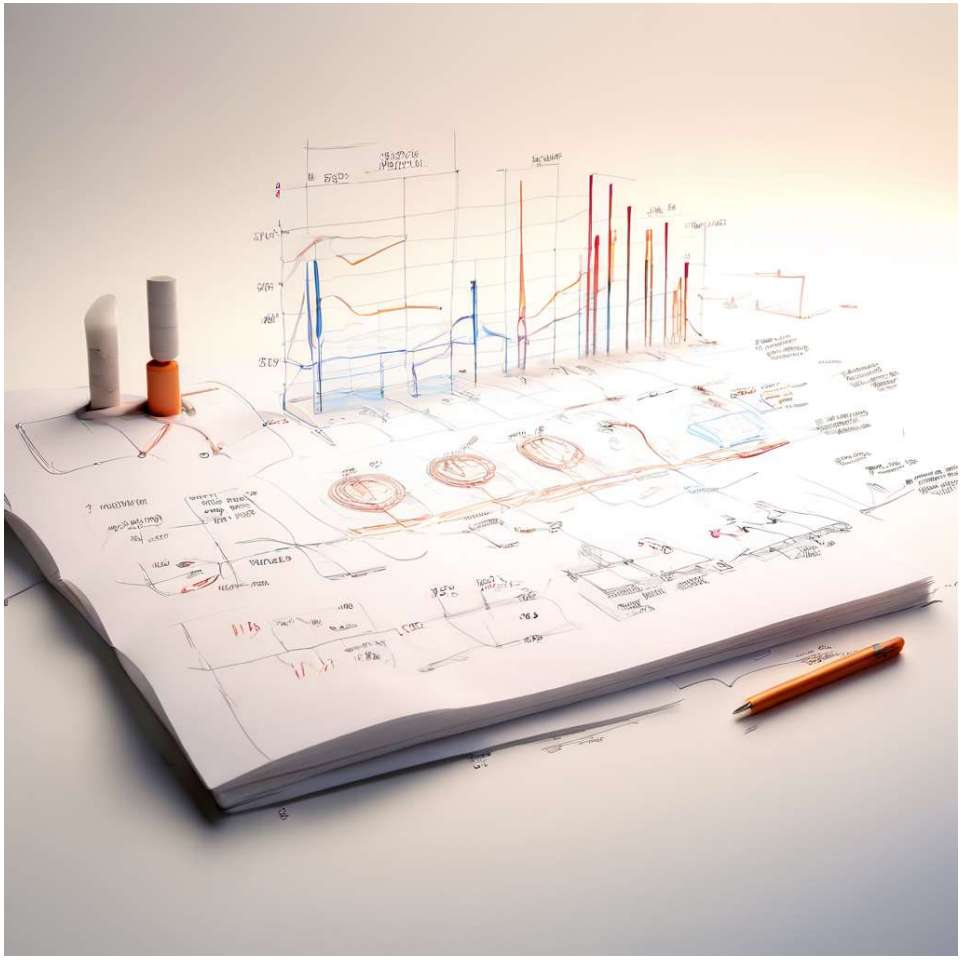
Comunicarea Directă Securizată Cuantică (QSDC)

Cercetătorii LG Electronics dezvoltă o nouă metodă de comunicare securizată cuantică prin introducerea unui protocol QSDC cu dimensiuni mari, bazat pe un singur foton, care utilizează două grade optice de libertate: timpul și starea de fază - 12 ianuarie 2024

O echipă de oameni de știință chinezi a introdus o tehnică de comunicare cuantică despre care spun că ar putea ajuta la securizarea Web-ului 3.0 împotriva amenințării formidabile a calculului cuantic - Long-Distance Free-Space Quantum Secure Direct Communication (LF QSDC) - 27 februarie 2024

Comunicare cuantică directă și sigură, independentă de dispozitiv ce folosește canale cuantice non-Markoviene - zgomotul non-Markovian îmbunătățește securitatea protocolului măsurată prin măsurată prin încălcarea inegalităților Bell, duce la o rată mai mică de eroare cuantică a biților și permite distanțe mai mari de comunicare prin creşterea capacităţii de comunicare secretă. - 06 mai 2024

Cercetătorii au confirmat că încrucișarea cuantică persistă între quarcii de top, cele mai grele particule fundamentale cunoscute. - 24 iunie 2024



9. Ultimele Descoperiri în Criptografia Cuantică (continuare)

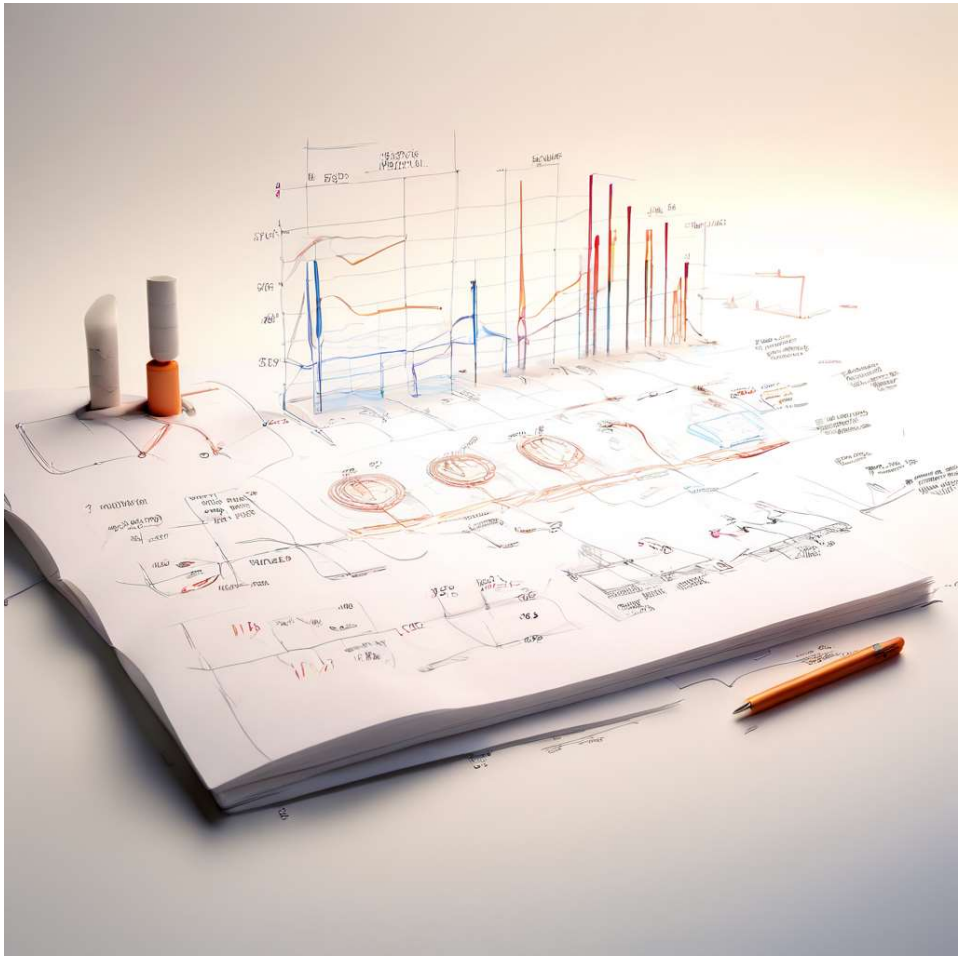
Criptografia Cuantică Post-Quantum

Comisia a publicat o recomandare privind criptografia post-cuantică pentru a încuraja statele membre să dezvolte și să pună în aplicare o abordare armonizată pe măsură ce UE trece la criptografia post-cuantică.- 11 aprilie 2024

Numărătoarea inversă cuantică: experții îndeamnă pentru adoptarea soluțiilor de criptografie post-cuantică - 30 aprilie 2024

Starea internetului post-cuantic - 3 mai 2024

Startup elvețian pune la dispoziție o bibliotecă de criptografie post-cuantică pentru programatori. Acum sunt disponibili pe GitHub algoritmi rezistenți la atacuri cu computere cuantice - 8 mai 2024



9. Ultimele Descoperiri în Criptografia Cuantică (continuare)

Rețele Cuantice și Repetitori Cuantici

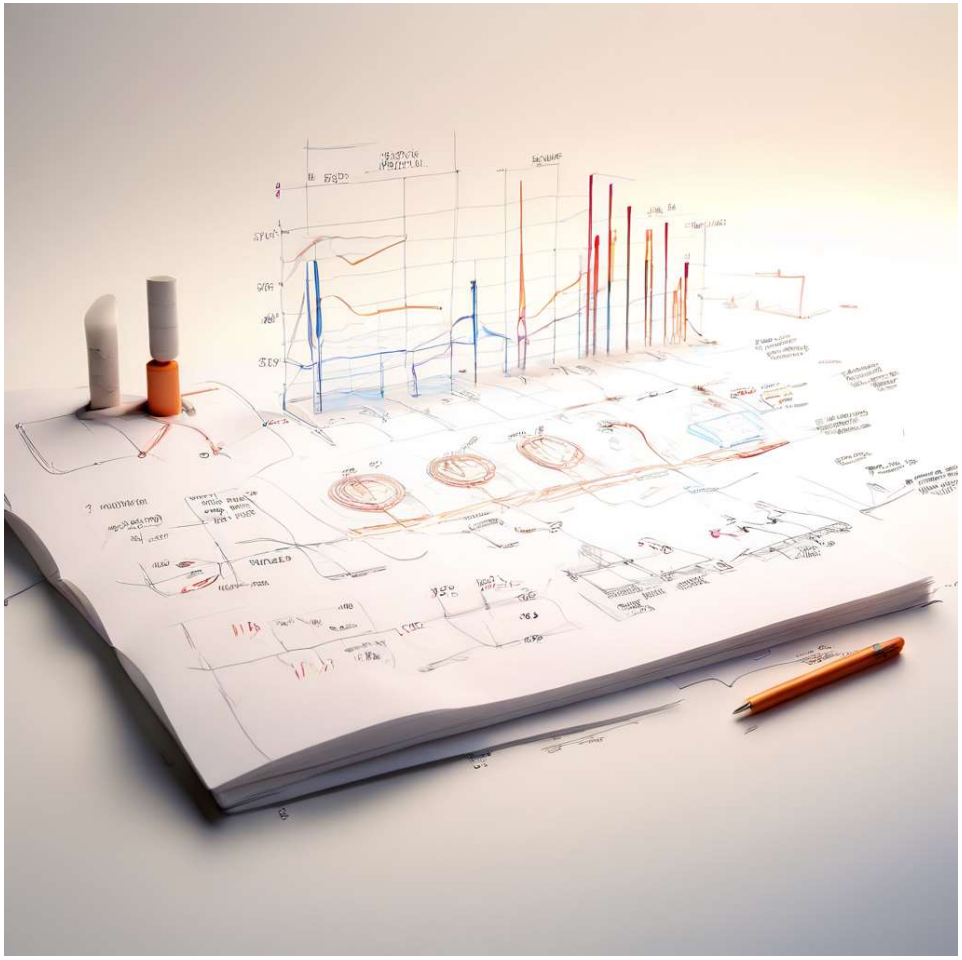
Proof-of-concept quantum repeaters bring quantum networks a big step closer - 21 mai 2024

Repetoarele cuantice folosesc defecte ale diamantului pentru a interconecta sistemele cuantice. Această tehnologie pentru stocarea și transmiterea informațiilor cuantice prin legături cu pierderi ar putea oferi fundația unei rețele cuantice scalabile.

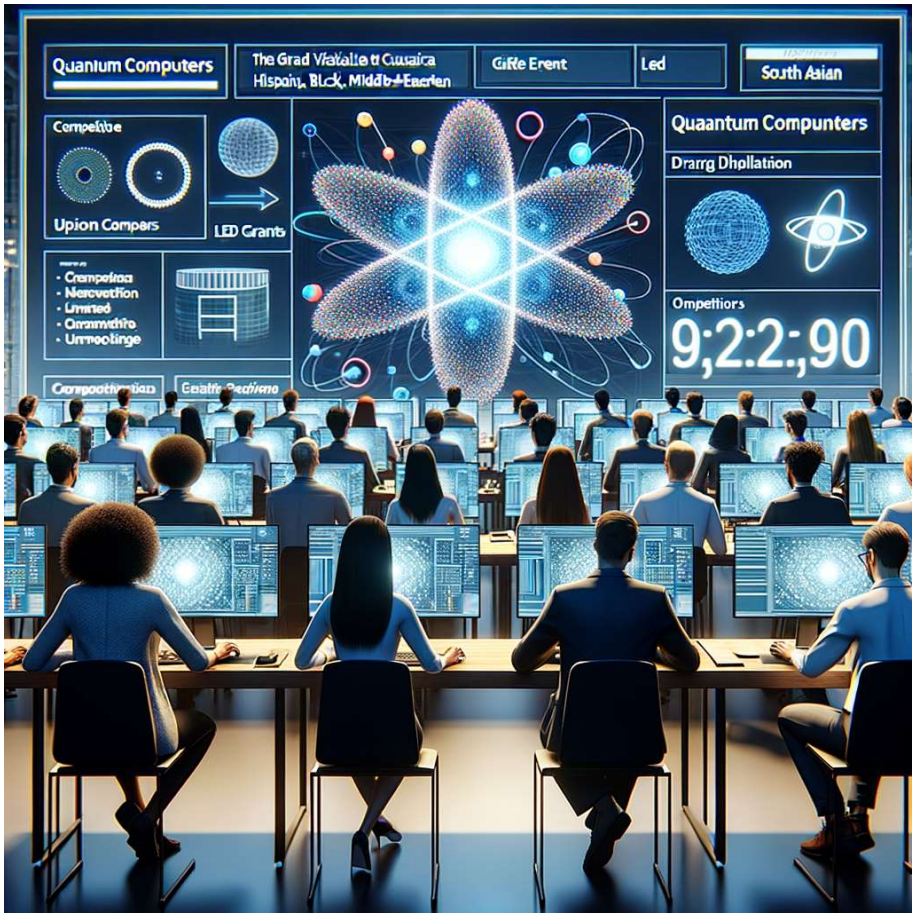
Research Team Takes a Fundamental Step Toward a Functioning Quantum Internet - 6 februarie 2024

Princeton University Researchers Make Breakthrough in Connecting Distant Quantum Devices - 13 aprilie 2024

Prin utilizarea dispozitivelor semiconductoare tradiționale, cercetătorii au deblocat noi posibilitati în comunicarea cuantică, împingându-ne mai aproape de realizarea potențialului vast al internetului cuantic. - 24 iunie 2024



10. Granturi și concursuri de calcul cuantic active în iunie 2024



XPRIZE Quantum Applications Competition: O competiție globală de trei ani, de 5 milioane de dolari, lansată de Google, GESDA și XPRIZE, care urmărește să dezvolte algoritmi de calcul cuantic pentru a aborda provocările din lumea reală, aliniați la Obiectivele de Dezvoltare Durabilă (ODD) ale Națiunilor Unite (blog.google).

NSERC Quantum Alliance Grants: Aceste granturi sprijină diverse proiecte de la Universitatea din Waterloo, cum ar fi dezvoltarea qubiților supraconductori și a senzorilor cuantici. Granturile fac parte din Strategia Națională cuantică a Canadei, investind aproape 7 milioane de dolari în cercetare cuantică (Universitatea din Waterloo).

UK Quantum Catalyst Fund: Parte a Programului Național de Tehnologii Cuantice din Marea Britanie, acest fond de 15 milioane de lire sterline sprijină studii de fezabilitate și prototipuri pentru tehnologiile cuantice din serviciile publice, de la asistență medicală la monitorizarea mediului și apărare (GOV.UK).

CERN Quantum Technology Initiative: Inițiativa de tehnologie cuantică a CERN sprijină diverse proiecte care vizează integrarea tehnologiilor cuantice în fizica energiei înalte. Aceasta include Open Quantum Institute, care se concentrează pe valorificarea calculului cuantic pentru a aborda ODD-urile ONU (CERN).

NVIDIA CUDA-Q Platform: NVIDIA accelerează eforturile de calcul cuantic la centrele naționale de supercomputing din întreaga lume cu platforma sa CUDA-Q, permițând supercalcularea hibridă cuantică-clasică pentru diverse aplicații, inclusiv simulări chimice și probleme de optimizare (NVIDIA Newsroom).

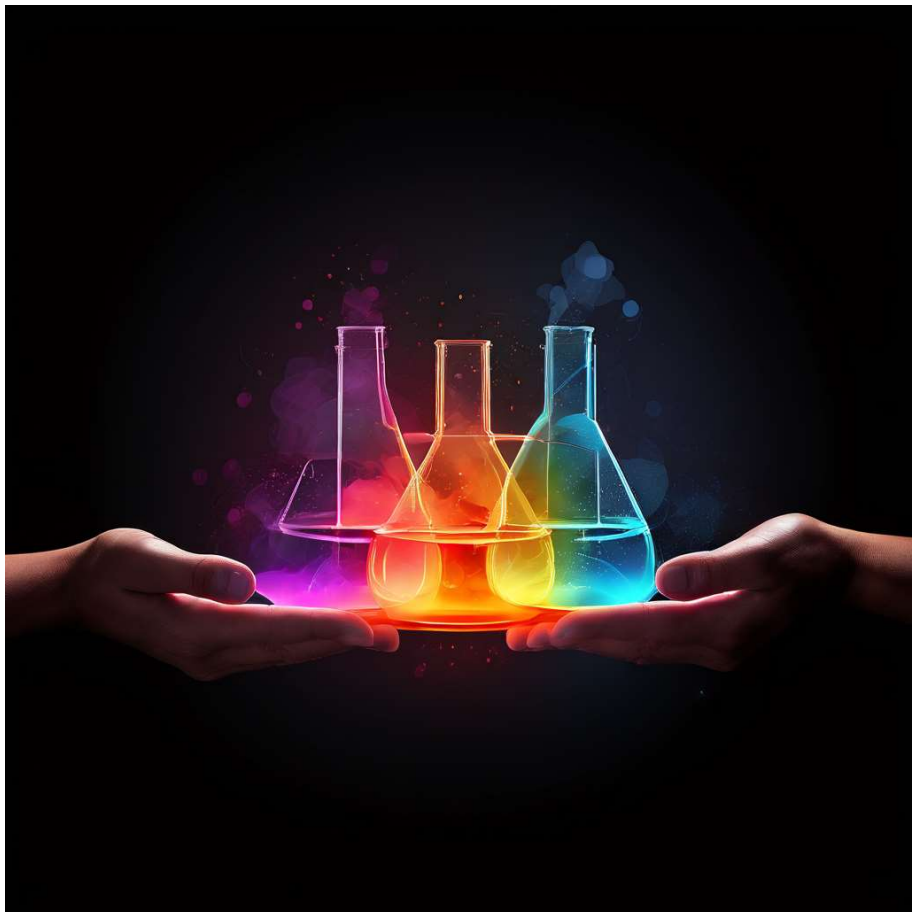
European Quantum Flagship: Acest program include mai multe oportunități de finanțare în cadrul programelor Orizont Europa și Europa digitală, susținând o gamă largă de cercetări și aplicații ale tehnologiei cuantice în întreaga Europă (Quantum Flagship).

11. Concluzie

Metodele criptografice cuantice reprezintă o revoluție în domeniul securității informațiilor, oferind un nivel de protecție fără precedent datorită principiilor fundamentale ale mecanicii cuantice. Aceste tehnologii deschid noi orizonturi pentru securitatea cibernetică, protejând informațiile sensibile de amenințările tot mai sofisticate din era digitală. Pe măsură ce infrastructura pentru rețele cuantice și repetitori cuantici se dezvoltă, putem anticipa o creștere semnificativă a aplicațiilor comerciale și guvernamentale, consolidând astfel protecția datelor la nivel global.

Implementarea criptografiei cuantice în diverse domenii, de la comunicațiile militare și guvernamentale până la tranzacțiile financiare și protecția datelor personale, va transforma radical peisajul securității informaționale. Investițiile continue în cercetare și dezvoltare vor fi esențiale pentru a depăși provocările tehnice și a realiza potențialul complet al acestor tehnologii inovatoare.

În concluzie, criptografia cuantică nu este doar o promisiune a viitorului, ci o realitate emergentă care redefinește standardele de securitate și confidențialitate în era digitală.



12. Bibliografie

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145-195.

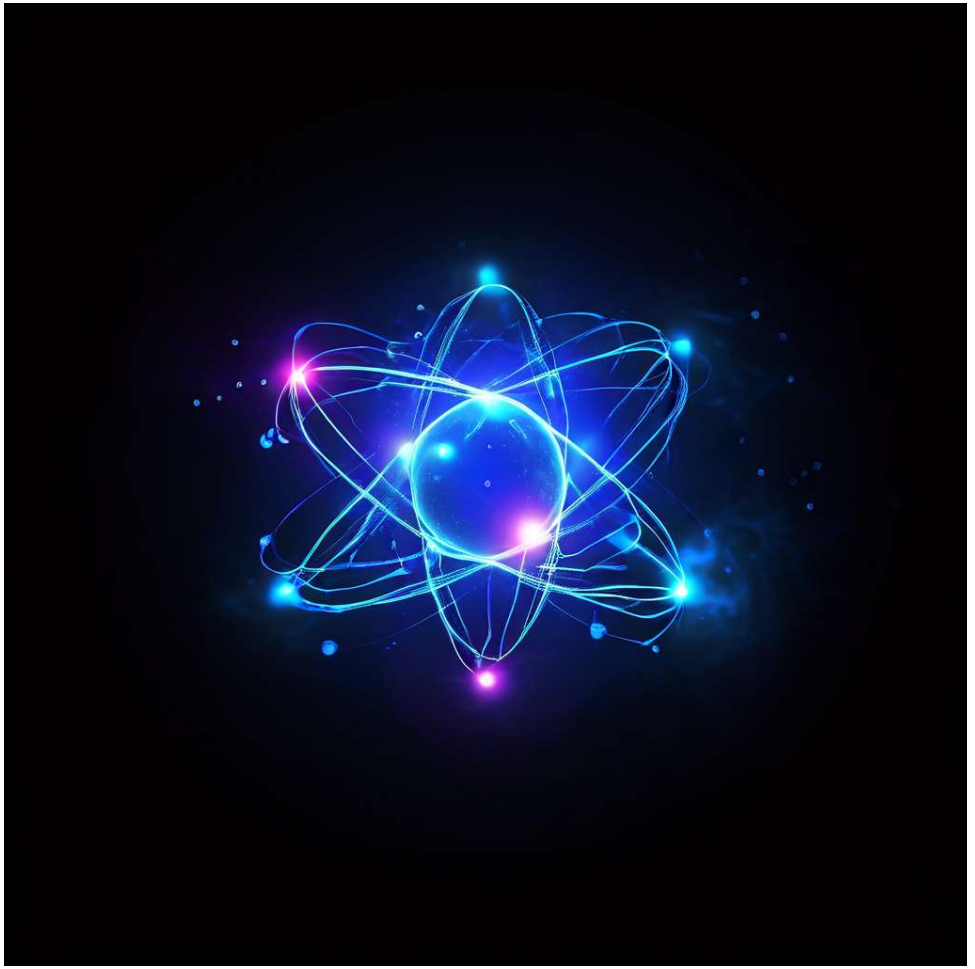
Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301-1350.

Lo, H. K., Curty, M., & Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, 8(8), 595-604.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., & Wehner, S. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, 12(4), 1012-1236.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. Physical Review Letters, 67(6), 661-663.

https://scitechdaily.com/faster-than-the-speed-of-light-information-transfer-through-spooky-action-at-a-distance-at-the-large-hadron-collider/



12. Bibliografie (continuare)

Long, G. L., & Liu, X. S. (2002). Theoretically efficient high-capacity quantum-key-distribution scheme. Physical Review A, 65(3), 032302.

Deng, F.-G., & Long, G. L. (2004). Secure direct communication with a quantum one-time pad. Physical Review A, 69(5), 052319.

Wang, C., Deng, F.-G., Li, Y.-S., Liu, X.-S., & Long, G. L. (2005). Quantum secure direct communication with high-dimension quantum superdense coding. Physical Review A, 71(4), 044305.

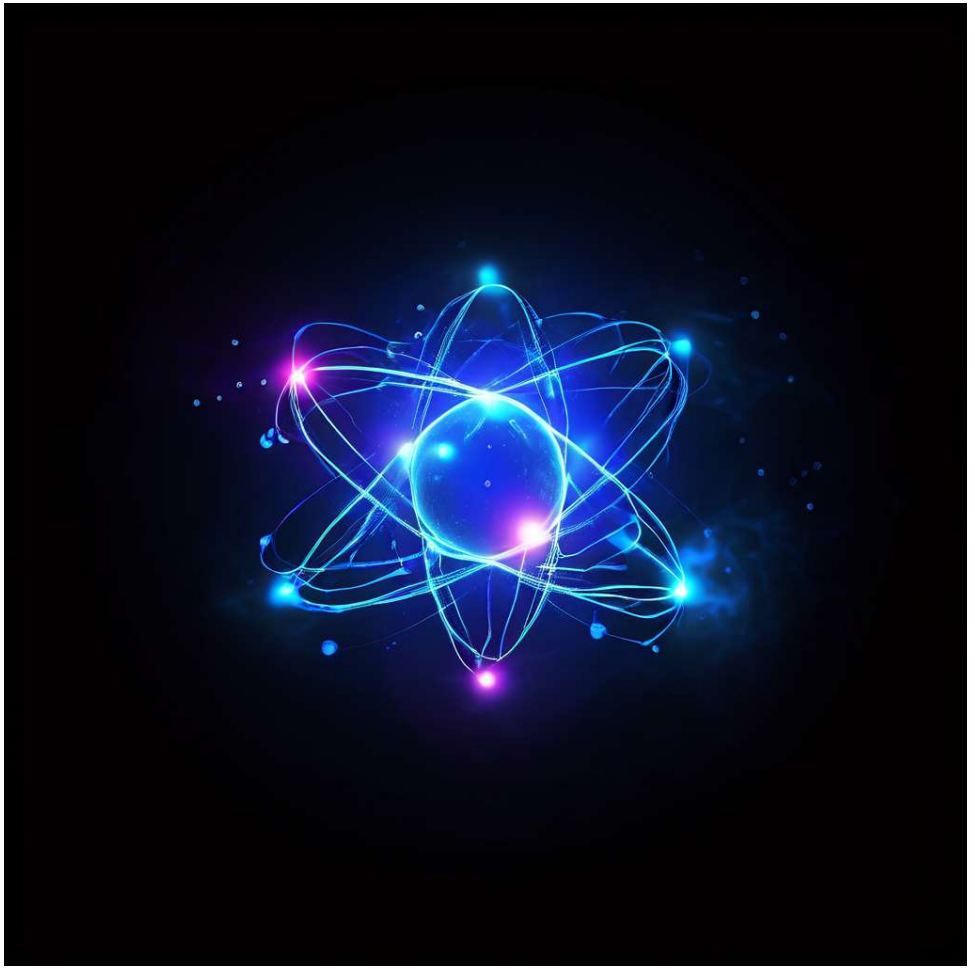
Zhang, W., Ding, D.-S., Sheng, Y.-B., Zhou, L., Shi, B.-S., & Guo, G.-C. (2017). Quantum secure direct communication with quantum memory. Physical Review Letters, 118(22), 220501.

https://thequantuminsider.com/2024/01/12/lg-electronics-researchers-develop-new-method-for-quantum-secure-communication/

https://thequantuminsider.com/2024/02/27/scientists-develop-a-technique-to-protect-a-quantum-era-metaverse/

https://arxiv.org/html/2312.03040v2 - Device-Independent Quantum Secure Direct Communication Under Non-Markovian Quantum Channels

https://scitechdaily.com/silicon-magic-powering-the-quantum-internet-of-the-future/ - Silicon Magic: Powering the Quantum Internet of the Future



12. Bibliografie (continuare)

https://scitechdaily.com/unprecedented-transmission-speeds-scientists-develop-new-quantum-key-distribution-system/

https://scitechdaily.com/secure-communication-breakthrough-1000-km-quantum-key-distribution-achieved/

https://scitechdaily.com/an-unprecedented-100-km-researchers-set-new-distance-record-with-quantum-keys/

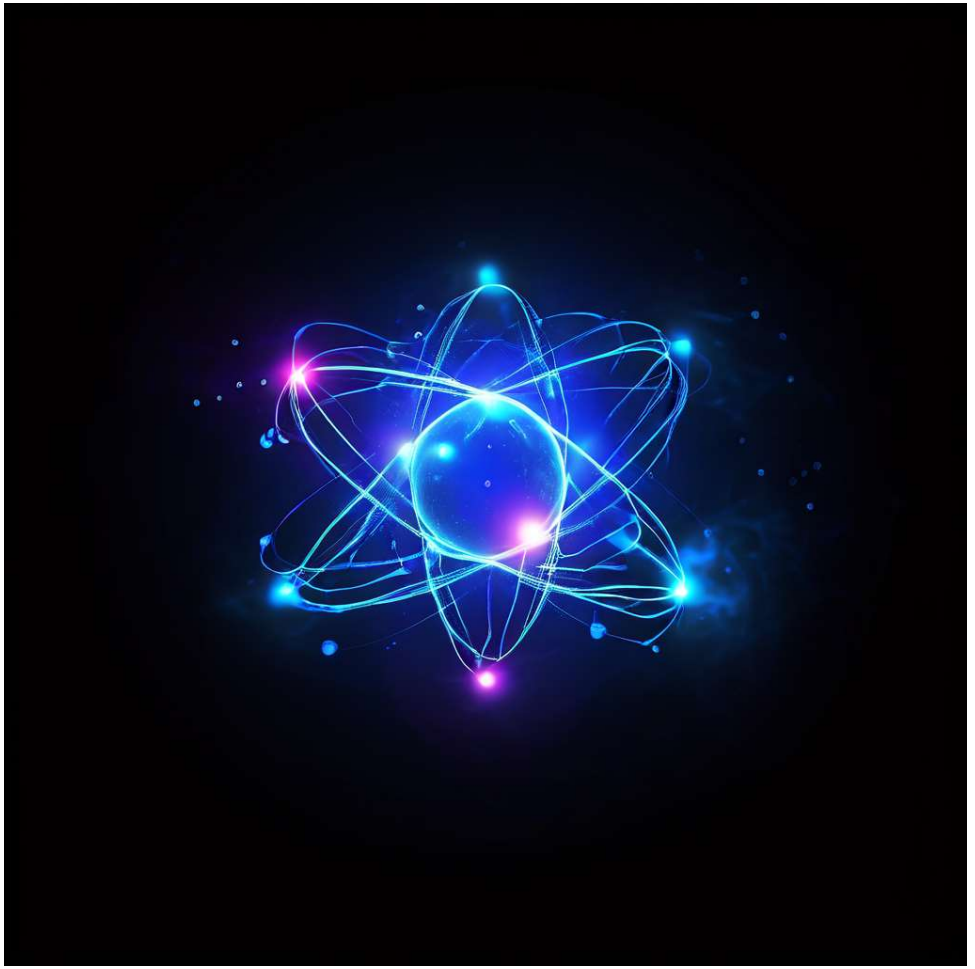
https://phys.org/news/2024-03-world-closer-quantum-communication-global.html

https://digital-strategy.ec.europa.eu/en/news/commission-publishes-recommendation-post-quantum-cryptography

https://thequantuminsider.com/2024/04/30/the-quantum-countdown-expert-urges-for-the-post-quantum-cryptography-solution/

https://blog.cloudflare.com/pq-2024

https://thenextweb.com/news/swiss-startup-post-quantum-cryptography-library-open-source



12. Bibliografie (continuare)

https://techxplore.com/news/2024-06-quantum-random-generator-gbits.html

https://www.prnewswire.com/news-releases/idtechex-explores-opportunities-for-qrng-in-the-connected-devices-market-302110322.html

https://quantumzeitgeist.com/quantum-dice-and-bt-group-test-quantum-random-number-generators-for-enhanced-telecom-security/

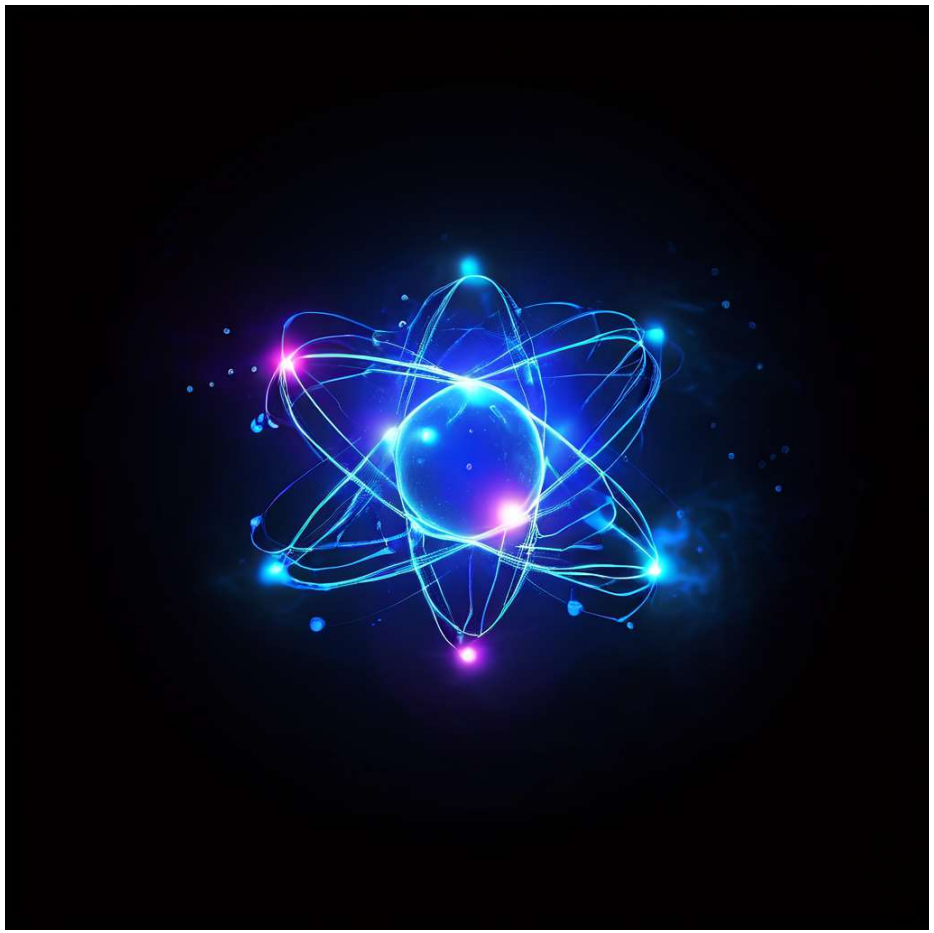
https://www.networkworld.com/article/2114720/proof-of-concept-quantum-repeaters-bring-quantum-networks-a-big-step-closer.html

https://news.mit.edu/2023/quantum-repeaters-use-defects-diamond-interconnect-quantum-systems-0927

https://news.stonybrook.edu/newsroom/research-team-takes-a-fundamental-step-toward-a-functioning-quantum-internet/

https://thequantuminsider.com/2024/04/13/princeton-university-researchers-make-breakthrough-in-connecting-distant-quantum-devices/

https://www.researchgate.net/publication/337336568_Quantum_Computing_at_the_Frontiers_of_Biological_Sciences/figures?lo=1



MULTUMESC!