TEMA BROJA: Umjetna inteligencija u lancu opskrbe

9 771331 283004 01219

za IT profesionalce

MREŽA

broj 12 / god. XXIV.
prosinac 2019.
cijena **29 kn**
BiH: 7 KM
CG: 3,70 EUR
EU: 3,70 EUR

FINTECH

PRIVATNOST I DIGITALNE FINANCIJE

IOT FORUM

Internet stvari ide prema masovnijoj primjeni

ISTRAŽIVANJA Fintech analiza HUB-a i Arhivanalitike

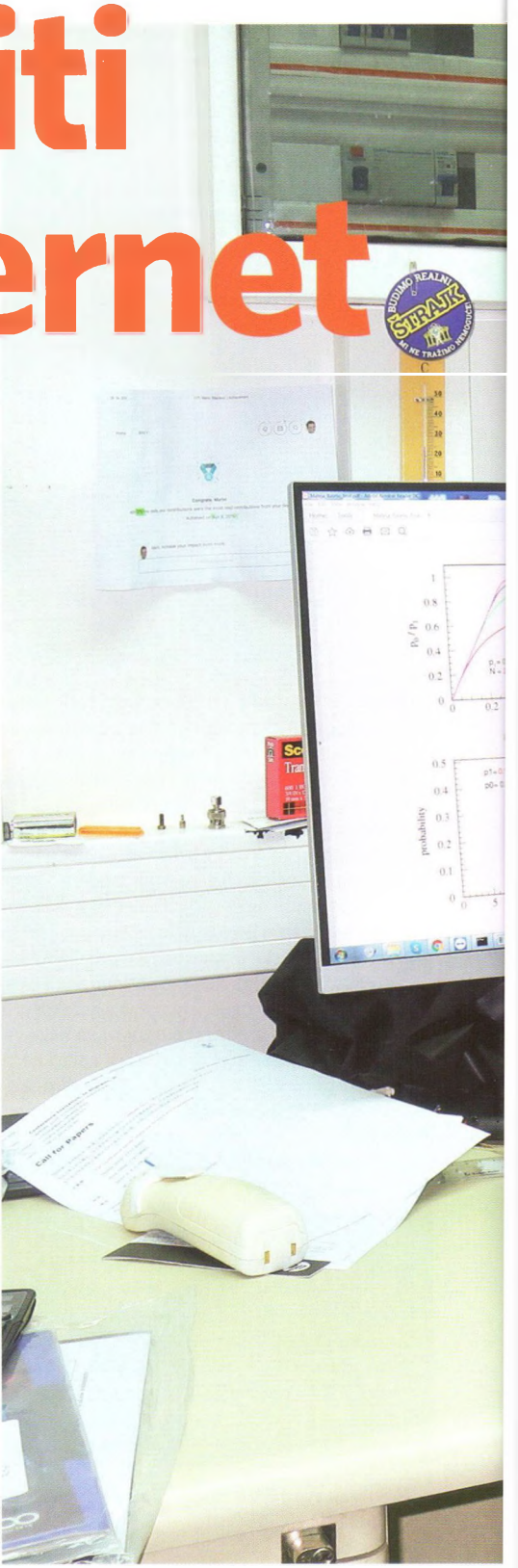
PROXMOX VIRTUAL ENVIRONMENT Open source virtualizacija

INTERVJU MJESECA dr. sc. Mario Stipčević, Institut Ruđer Bošković

MREŽA NA TERENU

Setcor X-day * Sagena Security Day * Power of Data * GetiCon: Ambition 4.0
DevArena * Adacta 8. godišnji susret * My Smart City, Zadar

Očekujemo da će početi graditi kvantni Internet



Za razliku od umjetne inteligencije, ljudi uče neusporedivo brže: dovoljno je svega nekoliko situacija. Znači, ljudska brzina učenja nešto je što se sadašnjim algoritmima umjetne inteligencije ni približno ne može ostvariti

Gorden Knezović

Mario Stipčević voditelj je Istraživačke jedinice Fotonika i kvantna optika unutar znanstvenog centra izvrsnosti CEMS (Centar izvrsnosti za napredne materijale i senzore / Centre of Excellence for Advanced Materials and Sensing Devices), i voditelj ustrojbene jedinice Instituta Ruđer Bošković, Laboratorija Fotonika i kvantna optika.

Objasnite našim čitateljima što je projekt CEMS te čime se bavite u istraživanju fotonike i kvantne optike.

Kako bih objasnio čime se bavimo, dobro bi bilo objasniti zašto su kvantne tehnologije toliko popularne u Europi i zašto u Europi misle da se treba oslanjati na kvantne proizvode. Dakle, Europska komisija je za sljedeće programsko razdoblje od deset godina, vezano za kvantne tehnologije, odlučila financirati tzv. Quantum flagship. *Flagshipi* su značajna područja znanstvenih istraživanja za koja se izdvajaju milijarde eura povrh redovnog financiranja namijenjenog znanosti.

ADMIRALSKI BRODOVI

Primjerice, do sada su postojali *flagshipi* za znanstvena istraživanja mozga i grafena, i tzv. 2D napredne materijale. Nakon pet ili sedam godina takvog financiranja došlo je vrijeme za novi ciklus, novo određivanje prioritetnih područja znanstvenog istraživanja. Još traju konzultacije o tome, koliko znam, ima 16 prijedloga za *flagshipe*. Naravno, razne zemlje članice EU nastoje postići što bolje financiranje za svoje projekte, no jedina stvar o kojoj institucije EU nisu željele raspravljati je kvantna tehnologija, odnosno istraživanje u njoj, ona je zadržala status *flagshipa* praktično dekretom.

I ne samo da je zadržala taj povlašteni status, nego se čini da će iznos novca koji se planira uložiti u istraživanje kvantnih tehnologija u novom proračunskom razdoblju Europske unije narasti na čak 3 milijarde eura. Postavlja se pitanje zašto.

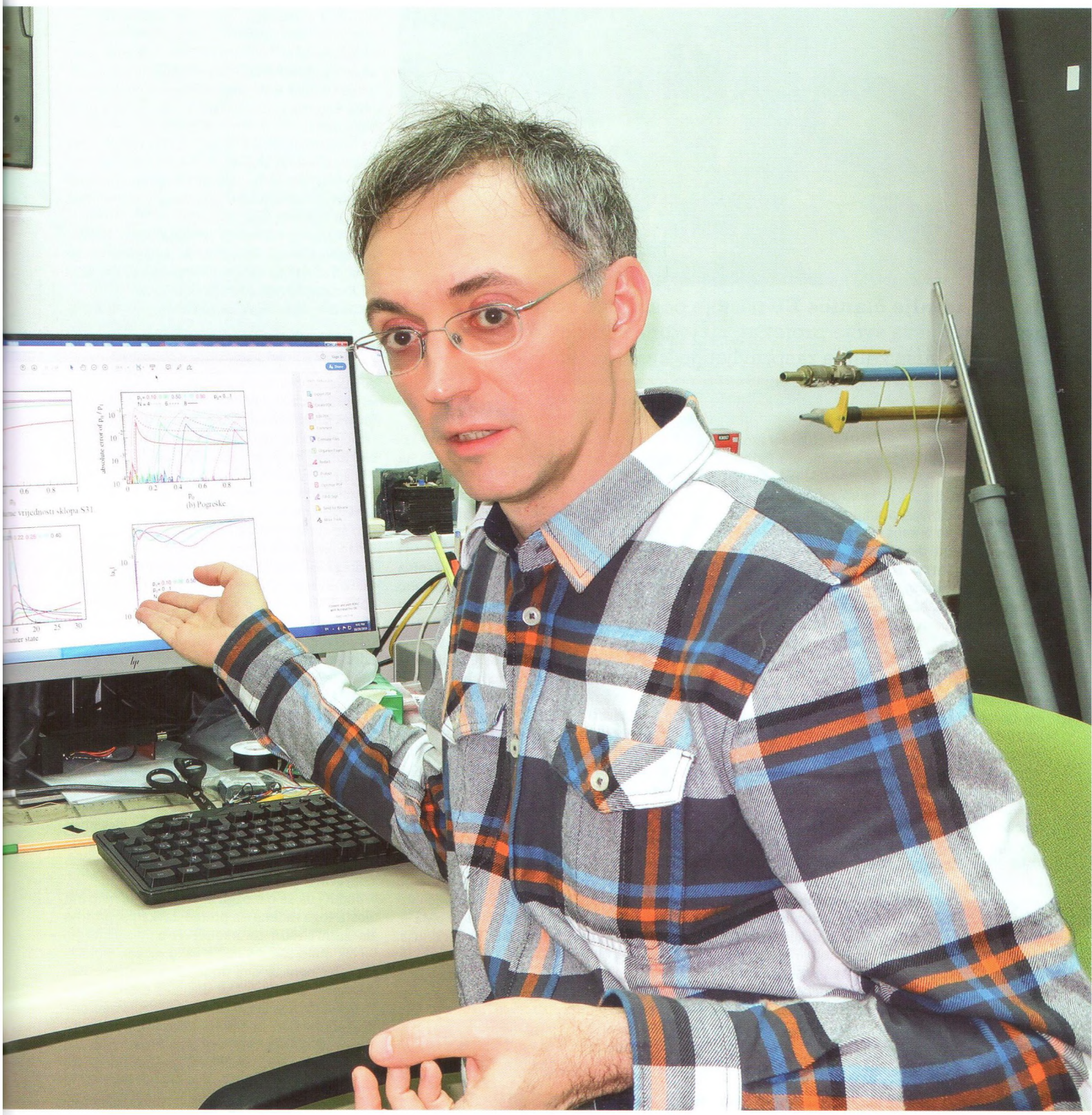
U najkraćem, u suvremenim tehnologijama trend je da se sve minijaturizira, a kvantna tehnologija bavi se objašnjavanjem ponašanja vrlo malih količina materije, poput, primjerice, atoma i subatomskih čestica.

Dobar primjer za minijaturizaciju je informatika, jasno je da su sve manje strukture ključne za daljnji razvoj procesora. Smanjivanje dijelova od kojih se rade procesori i druge računalne komponente vodi u područje gdje će kvantni efekti postati dominantni.

Kvantna fizika nas podučava da je količina informacije koje se može spremiti u atome i elementarne čestice konačna te kako ju pokušaj očitavanja mijenja. Ako se informacija očitava više puta, dobiju se različiti rezultati, koji su samo statistički poznati, ali nije unaprijed određeno koji će se odgovor dobiti u određenom traženju.

To znači da se javljaju nekakav šum i neodređenost u radu komponenti čije su dimenzije usporedive s veličinom atoma. S druge strane, kompjutorske komponente moraju biti ekstra stabilne, odnosno precizne, kako bi kompjutor funkcionirao. Primjerice, moderni

mo za pet godina



Razne zemlje članice EU nastoje postići što bolje financiranje za svoje projekte, no jedina stvar o kojoj institucije nisu željele raspravljati je kvantna tehnologija

kompjutor koji koristi gigahercni procesor mora moći pristupiti memoriji i do milijardu puta u sekundi, i pritom dobiti informaciju koja točno odgovara onome što je tamo zabilježeno: ako bi se pri svakom očitavanju sadržaj statistički mijenjao nastao bi kaos mnogo prije nego što bi prošao i milijunti dio sekunde rada kompjutora.

Živimo i digitalnom dobu pa su nam digitalni čipovi od izuzetnog značenja. Kako postaju sve manji, odnosno minijaturniji, jasno je da će njihov daljnji razvoj isključivo ovisiti od kvantnih efekata.

KVANTNE TEHNOLOGIJE

Kvantne tehnologije prije svega nam omogućuju da napravimo uređaje koji funkcioniraju bolje ili drugačije od onih koje imamo sada, a što je još važnije, kako bismo uopće održali tehnološki napredak, bit će nam potrebna znanja iz kvantne fizike. Dakle, u institucijama EU jasno su shvatili važnost kvantne tehnologije, ona je nešto što nećemo moći izbjeći u daljnjem tehnološkom razvoju.

Ja sam, usto, uvjeren da je nova tehnološka revolucija koja je pred nama, a koju je spominjao i kineski premijer Li Keqiang u Dubrovniku na *summitu* 16+1, održanom u travnju ove godine, upravo kvantna revolucija. Kina je zaprepastila znanstveni svijet kada su uspjeli ostvariti kvantnu komunikaciju između Pekinga i Šangaja te kada su prvi i zasad jedini, lansirali specijalni satelit (nazvan Micius) u orbitu, preko kojega je moguće ostvariti kvantnu komunikaciju. To pokazuje da su u razvoju kvantne komunikacije, odnosno tehnologije, Kinezi za sada najdalje otišli.

Sada da odgovorim na pitanje. CEMS je jedan od deset znanstvenih centara izvrsnosti Europske unije, formiranih na poziv prijava centara izvrsnosti u listopadu 2014. godine. CEMS se sastoji od četiri odjela: fizika i tehnologija ionskih snopova, grafen i srodni dvodimenzionalni materijali, novi funkcionalni materijali te fotonika i kvantna optika.

U našoj jedinici Fotonika i kvantna optika sada se bavimo s tri teme: kvantno sprezanje, kvantna komunikacija i informacija te bio-inspirirano računalo, odnosno računalo čiji je rad inspiriran načinom kako radi ljudski mozak.

Ovdje bih htio napomenuti i da, kada su se 2013. godine tražili centri izvrsnosti, prijavilo se njih 55, a izabrana su 4; jedan od njih je CEMS. Ocjenjivanje prijava radili su znanstveni eksperti iz EU i SAD-a. Uvjet je bio ocjena od najmanje 14 u ukupnoj ocjeni od 15, pri čemu su se zbrajale dvije ocjene: ocjena kvalitete prijavljenih znanstvenika koji čine centar te ocjena kvalitete predloženih istraživanja. Od pristiglih prijava, čak 4 prijave za centar dobile su ocjenu veću ili jednaku od 14,5, i to je ocjenjivačima bilo iznenađujuće, međutim, sva četiri centra bila su iz fizike, i postojala je neka zajednička potka u vezi sa senzorima i materijalima pa su spojeni u jedinstveni centar - CEMS, a pojedini prijedlozi postali su istraživačke jedinice. Pored CEMS-a, odobrena su tada još 3 centra iz STEM područja.

BIO-INSPIRIRANO RAČUNALO

Kako radite na bio-inspiriranom računalu, i kako je to povezano s istraživanjem neuronskih mreža?

Takozvano "računalo sa slučajnim impulsima", odnosno bio-inspirirano računalo, tema je koja se pojavila šezdesetih godina prošloga stoljeća, ali je nakon nekoliko godina zamrla zbog pojave digitalnih kompjutora koja sada dominiraju. No, posljednjih je godina ta tema ponovno postala aktualna. Naime, razvojem algoritama umjetne inteligencije pojavili su se neki problemi koje računala teško mogu rješavati, a ljudi vrlo jednostavno, kao, primjerice, prepoznavanje lica, oblika, nakana, namjera i slično. Dakle, kontekstualno prepoznavanje, obrada slike, ili prepoznavanje kontura u slikama. Primjerice, kada vidite obrise grada u magli, lako prepoznajete grad prepoznavajući konture objekata.

Pokazalo se da se to lako može postići bio-inspiriranim računalom, za razliku od klasičnih računala, pa se negdje 2014. godine počelo obnavljati istraživanje prije svega kao pomoć umjetnoj inteligenciji.

Za sada su takva istraživanja dosta daleko od operabilnosti, istražuju se najjednostavnije stvari kao što su neke jednostavne obrade slike i jednostavne matematičke operacije.

Kakve to veze ima s ljudskim mozgom? Znamo da u mozgu postoje neuroni koji imaju oko 5.000 ulaznih linija i jednu izlaznu liniju. Ono što se kreće po tim linijama nizovi su impulsa za koje se čini da su slučajni u vremenu, kako nemaju nekakve kôdove, nekakvu funkciju. Ono što mi koristimo od tog obrasca jest to da razvijamo sklopove koji kao ulaz imaju niz slučajnih električnih impulsa, a kao izlaz jedan niz impulsa.

Najjednostavniji primjer takvog sklopa je sklop za zbrajanje: imamo dva niza slučajnih impulsa, a nas zanima koliko tu dolazi impulsa u sekundi ako se zbroje impulsi jednog i drugog niza. Ako jedan niz ima, recimo, 1.000 impulsa u sekundi, a drugi 100, mi bismo kao rezultat željeli dobiti niz koji ima 1.100 impulsa. Tražimo sklopove kojima bismo mogli raditi i druge elementarne matematičke operacije: oduzimanje, dijeljenje, množenje, korjenovanje, uspoređivanje brojeva i druge. Problem je postići preciznost izračuna i mogućnost kombiniranja jednostavnih operacija u složene. Ideja je da se pomoću takvih sklopova sačini programabilno računalo, koje bi u principu bilo sposobno riješiti bilo koji zadatak.

To je sada nekakav *state of art*, ima nekih desetak znanstvenih članaka na tu temu, no broj naglo raste; mi smo tu među pionirima.

Realizacija takvih sklopova, ustvari digitalnih sklopova, nema u suštini nikakve veze sa samim mozgom, mi gledamo kako mi mislimo da se te operacije događaju u mozgu, i onda pokušavamo napraviti slične sklopove.

Budući da se o mozgu zna vrlo malo, mi u biti dosta toga radimo na pretpostavkama, pazimo da ulazni i izlazni parametri sliče onima u mozgu.

Nas malo zanima način kako mozak biološki radi, jer nam se čini da je to presloženo. No, čitajući o onome što se dokučilo o prirodi signala koji putuju linijama koje povezuju neurone - aksonima - i načinima kako impulsi mogu djelovati na neurone, vrstama neurona itd., a ponekad i maštovitom interpretacijom onoga što mi smatramo da su biolozi pogrešno shvatili, mi dolazimo na ideje o tome kako bi mogli raditi naši

sklopovi. Primjerice, jedno vrijeme se činjenica da ima jako puno ulaza u neuron ignorirala, odnosno, biolozi su govorili kako je svega od 50 do 100 tih linija (aksona) aktivno, dok su ostale linije neaktivne, a sada se čini da su došli do zaključka kako to nije točno. Zašto je izgledalo da su neaktivne? To je nama zanimljivo pitanje, i smatramo da se tu nalazi potencijal za rješenje nekih svojstava za kojima mi tragamo u našim sklopovima.

SLIČNO NEURONIMA

Sklopovi koje mi konstruiramo sliče na neurone, ali ne rade isto kao dobro poznate i razvikane neuronske mreže. One rade na potpuno drugom principu. Kod neuronskih mreža neuroni rade tako da ako imate dovoljan broj impulsa na svim ulazima, onda ćete proizvesti jedan impuls na izlazu. Ovo što mi radimo sasvim je drugačije: naši sklopovi vrše konkretne matematičke operacije, mi frekvencije ulaznih impulsa možemo zbrajati, oduzimati, dijeliti, množiti itd. Znači, imamo različite operacije za različite tipove "neurona". Pa i u biološkoj stvarnosti moglo bi se dogoditi da je svaki neuron programabilan, samo da mi to još nismo shvatili.

Osim što nam se čini da bi neuron mogao pridonijeti umjetnoj inteligenciji, on zapravo pokušava odgovoriti na jedno pitanje koje si malo tko postavlja.

Prije nekog vremena Google je napravio kompjutorski program AlphaGo koji je pobijedio prvaka svijeta u igri go Lee Sedolija.To je predstavljeno kao veliki uspjeh. To su uspjeli jer su uprogramirali razne partije te igre, kao što je prije toga slično s igranjem šaha radio IBM, međutim, ustanovili su da kompjutor tako sporo uči. Nakon toga su kompjutoru uprogramirali pravila i pustili ga da igra sâm sa sobom. Kako kompjutor to može vrlo brzo raditi, odigravao je milijune partija sam sa sobom i stvorio je svoje strategije pobjeđivanja, koje nitko ne zna jer su pohranjene u memoriji računala. I tako je uspio pobijediti svjetskog prvaka.

Tvrdilo se kako je to velika pobjeda umjetne inteligencije, međutim ja smatram kako je to dokaz da je cijelo istraživanje umjetne inteligencije pogrešno usmjereno. Zbog čega?

Program AlphaGo pokretao je superkompjutor s nekoliko tisuća procesorskih jezgri i nekoliko stotina GPU-ova koji su imali dodatne procesorske jezgre, i koji je trošio struje kao mali grad. I sada je pitanje kako ljudski mozak, koji troši otprilike 2 W, može igrati jednako dobro kao takav superkompjutor. To ukazuje na to da se nikakva tehnologija ne može usporedivati s ljudskim mozgom. Pri tome, prema mojem mišljenju, još je važnija činjenica da u neuron u ljudskom mozgu ne može doći više od 200 impulsa u sekundi jer svaki impuls traje oko 5 milisekundi. Dakle, taj neuron svojom sporošću uspijeva čak i pobijediti superkompjutor koji u svakom svom procesoru ima tri milijarde impulsa svake sekunde. Ukupni broj impulsa u ljudskom mozgu zanemariv je prema onome što je taj superkompjutor morao izračunati da dođe do istog rezultata.

KRATKI CV

Mario Stipčević znanstveni je savjetnik na Institutu Ruđer Bošković (IRB) i voditelj znanstvenog centra izvrsnosti CEMS-Fotonika. Doktorirao je 1994. godine na Université de Savoie, Chambéry, Francuska, s temom iz fizike visokih energija, radeći na CERN-ovom eksperimentu Atlas, nakon čega je nastavio raditi na fizici neutrina na CERN-ovim eksperimentima NOMAD i OPERA.
Od 2004. godine vodio je na IRB-u istraživanje eksperimentalnih tehnika kvantne komunikacije i kvantne informacije s interesima koji uključuju: detektore fotona s lavinskim fotodiodama, kvantnu komunikaciju, dvofotonsko kvantno sprezanje, kvantni generator slučajnih brojeva i digitalnu holografiju s malim brojem fotona.
U razdoblju 2010./2012. bio je Fulbrightov stipendist u SAD-u na University of California Santa Barbara (UCSB).
U suradnji s grupama s UCSB-a, Sveučilišta Duke u Sjevernoj Karolini (SAD) i IQOQI-a iz Beča radio je na temama ultrabrze kvantne kriptografije, novih detektora fotona i kvantne slučajnosti.
Objavio je preko 90 znanstvenih radova u CC časopisima, citiranih preko 3.500 puta, usmeno je izlagao na brojnim konferencijama, napisao 17 stručno-popularnih članaka iz područja elektronike, ima tri prijave patenta i jedan odobreni patent. ◂

Prema tome zaključujem da je ono što se sada radi u istraživanju umjetne inteligencije potpuno pogrešno. Bio sam na jednom predavanju 2016. godine, na konferenciji SPIE u Baltimoreu u SAD-u, gdje su znanstvenici tumačili kako umjetna inteligencija (artificial intelligence, AI) ne uči brzo. Dakle, možete naučiti AI da, primjerice, prepoznaje pištolj dovoljno dobro, ali joj za to treba dugotrajno učenje od oko tri milijuna situacija. To znači da, kada se pojavi neka radikalno nova situacija, umjetna se inteligencija teško može naučiti što je to, i ne može reagirati.

BRŽE UČENJE

Za razliku od umjetne inteligencije, ljudi uče neusporedivo brže: dovoljno je svega nekoliko situacija. Znači, ljudska brzina učenja nešto je što se sadašnjim algoritmima umjetne inteligencije ni približno ne može ostvariti.

Sada se nadamo da načinom koji zovemo bio-inspirirani kompjutor, odnosno kompjutor sa slučajnim impulsima, što je, mislim, točniji naziv, možemo proizvesti nešto što bi bilo puno djelotvornije u odnosu snage i količine resursa u odnosu na klasični kompjutor. Besmisleno je imati sklop kompjutora veličine grada kako bi radili nešto što može raditi nekoliko ljudi.

Još jedna važna razlika između kompjutora, odnosno cijele serije povezanih kompjutora, koji troše silne MW struje, i svjetskog šampiona u igri go je u tome što je ta računalna struktura napravljena specifično da igra samo go, a svjetski šampion je odmah nakon završetka partije mogao, primjerice, odigrati partiju šaha, mogao je veslati, plivati, razgovarati i shvaćati viceve.... Pitanje je koliko bi kompjutor trebao biti velik da sve to može. Broj tranzistora u tom kompjutoru koji je pobijedio svjetskog prvaka u igri go znatno je veći nego broj neurona u ljudskom mozgu; ljudski mozak može napraviti mnogo više s osjetno manje snage nego što to može kompjutor. Da ponovim, mi nešto potpuno pogrešno radimo u sadašnjoj tehnologiji umjetne tehnologije, ono što radimo nije učinkovito.

Očekujemo da će se za pet godina postići značajni rezultati u području kvantnog Interneta te kako bi se on onda mogao početi nuditi kao komercijalna usluga

Za razliku od komunikacije laserima, iz fotona se ne može uzeti dio svijetla jer je to najmanja količina; morate ga uzeti cijeloga, a ako ga uzmete cijeloga, napravit ćete neizbježno neku statističku pogrešku zbog zakona fizike

Što je kvantna komunikacija, koliko su znanstvenici uspjeli stvoriti kvantnu komunikaciju, koliko je ta tehnologija sada primjenjiva u praksi?

Skok na kvantnu komunikaciju veliki je tehnološki i znanstveni korak. Kvantna komunikacija u stvari je stara nekih 30-ak godina. U prvom desetljeću u toj su se komunikaciji pojavljivali problemi koji su se rješavali, tako da je sada jasno kako je moguće uspostaviti potpuno siguran *link* između dvije točke.

Sve dalje veliki je tehnološki izazov, kada iz eksperimentalnog laboratorija prelazite u stvarne optičke *linkove* koji su negdje u zemlji ili na nekim stupovima. Oni mijenjaju svoja svojstva s obzirom na temperaturu, naprezanje itd., i tu ima dosta tehnoloških izazova da se prevladaju takve realne prepreke.

Inicijativa kvantne komunikacije (Quantum Communication Infrastructure, QCI) i inicijativa kvantne tehnologije (Quapital QT) dvije su velike inicijative Europske komisije kojima želi znanstvena dostignuća dovesti do proizvoda. Nema više istraživanja koja su sama sebi svrha, nego se sada – s obzirom na to da je znanost zrela i ima rezultate – ide u rješavanje tehnoloških problema da se naprave konkretni proizvodi i konkretne usluge temeljene na kvantnoj komunikaciji koja će osigurati nedodirljivu sigurnost u samoj digitalnoj komunikaciji.

KVANTNA TEHNOLOGIJA U KOMUNIKACIJAMA

Što je sa sigurnosti koju omogućuje primjena kvantne tehnologije u komunikacijama? Koliko su podaci sigurni u kvantnoj infrastrukturi?

Kvantna komunikacija je, kako sam već rekao, nešto što je EU odlučio razvijati i u to uložiti značajna sredstva. U tom smislu pokrenut je projekt kvantne komunikacijske infrastrukture QCI. Radi se o tome da se postojeća gusta mreža optičkih vlakana u Europi, koja se koristi za internetski promet, upotrijebi za jedan drugačiji, sigurniji način prijenosa podataka. Početkom ove godine potpisan je ugovor između Europske komisije i Digital Connecta, kojim se uspostavlja plan EU u razvoju kvantnih komunikacija. I to na dva načina. Jedan bi bio kroz postojeću svjetlovodnu infrastrukturu diljem Europe, a drugi preko satelita. Taj satelitski način bio bi da, primjerice, uputite laserski snop iz Zagreba na satelit, a on ga onda spusti, primjerice, u Beč. Za to nam trebaju posve novi sateliti. Za sada postoji samo jedan takav satelit u svijetu, Micius. Možda je taj kineski uspjeh bio odlučujući za EU da se uključi u takav projekt. Naime, kineski uspjeh u slanju satelitske kvantne komunikacije došao je kao rezultat znanstvenih dostignuća bečkog Instituta za kvantnu informaciju i kvantnu optiku (Institute for Quantum Optics and Quantum Information, IQOQI), gdje su se školovali kineski istraživači. Kinezi su njihova znanstvena dostignuća iskoristili za svoj satelit Micius.

Osnovna prednost kvantne komunikacije je siguran način dostavljanja podataka, koji je u našem informatičkom dobu glavni problem. Problem je, usto, i sigurnost informacija na mjestu, odnosno u podatkovnom centru. Sve češće otkriva se da netko presreće slanje podataka. To nije lako otkriti, a i kada se otkrije obično je kasno.

I sada su podaci koji se prenose kriptografski zaštićeni, sada su zaštićeniji nego što su ikad prije bili. Prije tridesetak godina, u vrijeme hladnog rata, kriptografijom su se bavili samo špijuni. No, pojavom Interneta kriptografija je postala civilna znanost kojoj je posao sigurno slanje podataka kroz nesiguran medij. Početkom 90-ih godina mobiteli su bili nekriptirani, tako da su jednostavno mogli biti prisluškivani. Sada se to ne može, čak ni sa specijalnom opremom, jer je komunikacija mobitelima kriptirana. Sve su komunikacije, bilo kroz Internet ili telefonsku vezu, zaštićene jer se razmjenjuje dosta važnih podataka. Šaljete broj svoje platne kartice preko Interneta, ne želite da netko čita vaše *mailove*, poruke...

Nije da mi nemamo zaštitu, pitanje je zašto nam treba bolja zaštita. Primjerice, banke su primijetile da im informacije cure pa često trebaju mijenjati platne kartice.

Zna se i da postoji puno prisluškivanja kojemu nije cilj pravljenje direktne jednokratne štete, nego je u pitanju industrijska špijunaža. To je najveći problem. Tu se Europa osjeća ugroženo i htjela bi napraviti svoj sigurni komunikacijski sustav koji će biti otporan na prisluškivanje, bilo da je riječ o političkoj ili komercijalnoj, odnosno gospodarskoj komunikaciji.

Kvantna komunikacija pruža odgovor na to pitanje. Kvantna fizika omogućuje potpuno sigurnu komunikaciju između dvije točke pomoću takozvane kvantne kriptografije, koja se, pak, ostvaruje preko kvantne komunikacije, odnosno izmjenom najmanjih količina (kvanata) svjetlosti koje nazivamo foton.

Sadašnje kriptirane komunikacije sigurne su samo ako onaj tko vas prisluškuje nema dovoljno jak kompjutor da razbije vašu kriptografiju niti nakon duljeg vremena. Za neke je podatke važno da se ne otkriju ni za deset ili više godina, kao, primjerice, za neke strateške državne podatke. Za druge, pak, nije važno; ako ste danas nešto platili, sutra to više nije važan podatak, plaćanje je izvršeno.

Dakle, postoje razne razine potreba sigurnosti. Sadašnja kriptografija sigurna je protiv napadača koji su ograničeni u komputacijskoj moći. Međutim, kvantna komunikacija omogućuje naprosto beskonačnu sigurnost. Ne može se nikako dekriptirati. Nisu joj problem nikakvi snažni kompjutori.

VEĆA SIGURNOST

Kako kvantna komunikacija omogućuje znatno veću sigurnost od klasičnih tehnologija komunikacije?

U klasičnoj komunikaciji šalje se signal, dakle, znamenke 0 i 1 enkodirane u vrlo snažne laserske impulse. Ako laser svijetli to je 1, a ako ne svijetli onda je 0. Takva komunikacija lako se prisluškuje tako da odvojite malo svjetla – time ne ometate komunikaciju, a sebi napravite kopiju podataka.

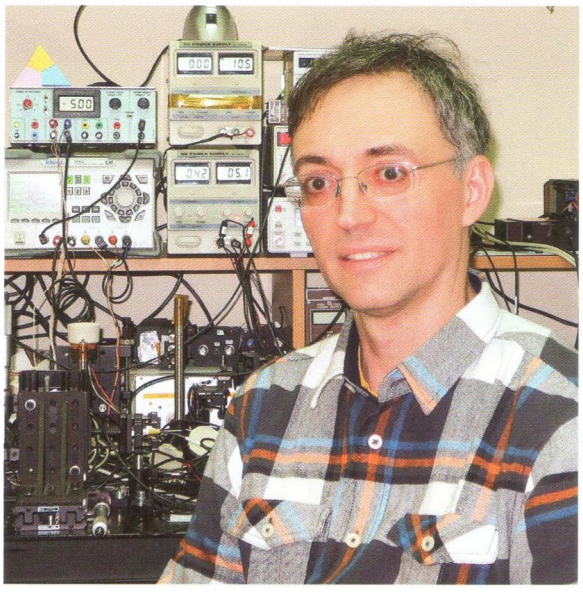
U kvantnoj komunikaciji šalje se najmanja količina svjetla koja može biti, a to je foton. On prenosi najmanju količinu informacije, jedan bit, dakle 0 ili 1, pomoću svojstva svjetlosti koje zovemo polarizacija. Polarizacija se javlja, primjerice, kada se svjetlost odbija od prozirnog medija pod malim kutom, primjerice, s površine vode, vrućeg zraka na cesti ili prozora automobila. Poznato nam je da se takvo polarizirano svjetlo može zaustaviti (tj. odbiti) polarizirajućim naočalama, ali može se i propustiti ako glavu (zapravo naočale) zakrenemo za 90 stupnjeva. Na tom principu propuštanja/odbijanja rade enkodiranje i prijenos informacije pomoću fotona.

Međutim, za razliku od komunikacije laserima, iz fotona se ne može uzeti dio svijetla jer je to najmanja količina; morate ga uzeti cijeloga, a ako ga uzmete cijeloga, napravit ćete neizbježno neku statističku pogrešku zbog zakona fizike.

Naime, rezultati određivanja polarizacije fotona ovise o tome kako smo okrenuli polarizator (naočale): foton može samo proći ili se odbiti od polarizatora, a pri tome mu se polarizacija nepovratno promijeni. Zbog toga, prisluškivač ne može kopirati ukradeni foton kako bi kopiju

Program AlphaGo pokretao je superkompjutor s nekoliko tisuća procesorskih jezgri i nekoliko stotina GPU-ova koji su imali dodatne procesorske jezgre, i koji je trošio struje kao mali grad. I sada je pitanje kako ljudski mozak, koji troši otprilike 2 W, može igrati jednako dobro kao takav superkompjutor

CEMS je jedan od deset znanstvenih centara izvrsnosti Europske unije formiranih na poziv prijava centara izvrsnosti u listopadu 2014. godine



neprimjetno vratio nazad, već on tu unosi pogrešku koja se očituje kao povećanje šuma u kanalu, i to se može detektirati. To je ključna razlika između obične i kvantne komunikacije. U kvantnoj komunikaciji odmah se može primijetiti prisluškivanje jer se poveća šum. To je jedinstvena karakteristika kvantne kriptografije i još jedan razlog zašto bi ona bila nezamjenjiva kao sigurnosna mjera.

A zašto je to važno? Pa, primjerice, zna se dogoditi da dobijete nekakav trojanski virus i da vam stoji deset godina na vašem računalu ili serveru i krade podatke, a vi ne znate za njega. U kvantnoj komunikaciji to je nemoguće jer se mjerenjem razine pogrešaka u komunikaciji odmah može uvidjeti da je netko nešto mijenjao, bilo prisluškivanjem, bilo ubacivanjem informacije.

VANJSKA SURADNJA

Što obuhvaća suradnja vaše Jedinice sa Sveučilištem u Bristolu i IQOQI?

Mi smo zapravo prvo počeli surađivati s Institutom za kvantnu informaciju i kvantnu optiku IQOQI (Institute for Quantum Information and Quantum Optics), to je institut Bečke akademije znanosti, koji je zapravo centralno mjesto u svijetu za kvantne tehnologije, oni su najbolji, i svi voditelji u svijetu nekada su bili studenti tog centra, kao i voda kineskog tima koji su napravili Micius.

Mi smo imali sreću da smo se s IQOQI uspjeli povezati 2014. godine i početi s istraživanjima kvantne informacije i kvantne optike, a sredinom prošle godine zajedno smo ušli u dva projekta.

Prvi je projekt Quapital projekt koji nastoji povezati glavne europske gradove kvantnom komunikacijom. To je projekt koji obuhvaća, za sada, 10-ak zemalja Europe, ustvari srednje i istočne Europe te se preko Beča, koji je najzapadniji grad u projektu i apsolutno najjači u kvantnoj tehnologiji, želi skrenuti pozornost institucijama EU da se sigurna internetska komunikacija treba razviti po cijeloj Europi, a ne samo u zemljama zapadne Europe.

Inače, problem s kvantnom komunikacijom je to da je iz tehnoloških razloga - koji će se teško moći riješiti u budućnosti - kvantno osigurana komunikacija kroz optička vlakna moguća za najviše 200 km; dakle svakih 200 km morate imati nekakav centar gdje ćete dekriptirati signal, ponovno ga kriptirati i poslati dalje. To su zapravo ranjive točke jer tu poruke postoje u nekriptiranom obliku.

Jedan od načina da se izbjegne taj problem jest to da se kvantna veza prema dalekim gradovima odvija tako da ju prvo pošaljete do satelita i onda signal spustite blizu tog udaljenog grada, u neku mrežu koja je udaljena unutar 200 km. Zbog toga kvantna infrastruktura zahtijeva suradnju s Europskom svemirskom agencijom (European Space Agency, ESA). Ona će biti uključena u sigurne protokole.

Taj je projekt na samim začecima i sada radimo samo eksperimente u laboratorijima te pokušavamo smisliti zajedničke projekte koje bismo prijavili kako bismo dobili novac za njihovo ostvarenje. Sada nemamo dostatno financiranje za Quapital.

Druga suradnja koja nam je sada mnogo aktivnija je sa Sveučilištem u Bristolu, gdje je jedan od bivših postdoktoranada iz Beča osnovao svoju znanstveno-istraživačku grupu. S njima radimo jedan eksperiment gdje pokušavamo napraviti kvantnu komunikaciju između više od dvije točke, dakle, jednu malu kvantnu mrežu od *n* komunikacijskih točaka.

Naime, ono što je dosad rađeno u znanstvenim laboratorijima gotovo jedino je kvantna komunikacija između samo dvije točke. No Internet, u ovom slučaju kvantni Internet, zahtijeva da možete komunicirati bilo s kim iz mreže. Odnosno, komunicirati s beskonačnim brojem točaka. Pokazuje se kako to nije jednostavno napraviti u kvantnoj komunikaciji.

Ako hoćete ići na više točaka, onda je problem to što ne možete poslati, kao u TCP protokolu (Transmission Control Protocol), nekoliko paketa i onda svatko tko ih primi pogleda jesu li adresirani na njega, a ako nisu, multiplicira ih i pošalje dalje, jer rekli smo, u kvantnoj komunikaciji ne može se napraviti kopija pa biste morali slati ogromnu količinu energije svima koji su potencijalno zainteresirani.

Tu se javlja problem nekakvog menadžmenta mreže, i to je ono što pokušavamo riješiti. Za sada postoji vrlo malo znanstvenih radova o tome, međutim, to je krucijalni problem.

OČEKIVANI REZULTATI

To je sada *on going research*. Očekujemo da će se za pet godina postići značajni rezultati u području kvantnog Interneta te kako bi se on onda mogao početi nuditi kao komercijalna usluga. Vrlo intenzivno surađujemo s kolegama iz Bristola, već smo odradili neke eksperimente u Bristolu, a ovdje u Zagrebu osmišljavamo i gradimo inovativne optičke uređaje i istražujemo druga moguća rješenja za kvantni Internet.

Područje kvantnog Interneta je mlado - zasad nitko ne zna rješenja za neka praktična pitanja, dakle, tu ima mjesta za inovacije.

Inače, što se tiče te suradnje, bitno je naglasiti da u slučajevima zemalja poput Hrvatske, kada nemate velika sredstva za istraživanja, teško možete uspjeti u područjima u kojima je znanost daleko odmakla, odnosno gdje najmanji napredak znači velika ulaganja. Prilika za nas je uvijek tamo gdje nešto nastaje i gdje su ključne nove ideje.

Govorio sam o bio-inspiriranom računalu. U tom se području počelo intenzivnije istraživati tek 2014. godine, pa za 20 godina mi tu nećemo imati što tražiti, ali sada, kada su inovativne ideje važne, tu imamo izgleda. Isto tako, u novom području istraživanja kao što su kvantna komunikacija i kvantne mreže i mi možemo konkurirati jer i mi imamo pametne ideje kao i drugi, tu ne treba previše sredstava za njihovu realizaciju. Imamo priliku te ideje, u suradnji sa Sveučilištem u Bristolu ostvariti. No treba reći i to da ta istraživanja kod nas ničim nisu posebno financirana. Financiramo ih iz tekućih projekata. S druge strane, kolege u Bristolu imaju Britanski *quantum hub*, zapravo skupinu projekata koje njihova vlada financira s 270 milijuna funti. Dakle, oni imaju sredstva za istraživanje tih tehnologija, ne samo kvantne komunikacije, nego općenito kvantnih tehnologija; oni imaju, za naše prilike, ogroman novac za to.

Koliko znam, primjerice, Njemačka je ove godine u kvantna istraživanja uložila preko 600 milijuna eura. Mi u Hrvatskoj čekamo na novi ciklus istraživačkih projekata Horizont Europe koji počinje iduće godine. To je ustvari nastavak projekta Horizon 2020, samo u novom proračunskom razdoblju EU. Zbog toga smo vrlo zainteresirani za međunarodnu suradnju, jer kada se otvore natječaji EU za znanstvena istraživanja za kvantnu komunikaciju i infrastrukturu te kvantne tehnologije, nadamo se financiranju nekih naših projekata na temelju ostvarenih rezultata iz naše međunarodne suradnje. S druge strane, Hrvatska ulaže u znanost i obrazovanje najmanje u Europi, s trendom daljnjeg opadanja, zato i ne čudi da Hrvatska gotovo nema visokotehnoloških tvrtki i da se ljudi moraju zadovoljiti slabije plaćenim poslovima. Mi smo zapravo sretni da nas dobrostojeće institucije žele kao partnere i da još uvijek imamo što ponuditi.