PRIOPĆENJE ZA MEDIJE
Petra Buljević Zdjelarević, Ured za odnose s javnošću
Institut Ruđer Bošković
T. +385 (1) 457-1269, (99) 267-95-14
E: info@irb.hr W: www.irb.hr

ZAGREB, 29 .6. 2015.

Znanstvenici razvili fizički generator slučajnih brojeva s najbržim 'refleksima'

Ruđerovac dr. sc. Mario Stipčević u suradnji s kolegom dr. sc. Rupertom Ursinom s Instituta za kvantnu optiku and kvantnu informatiku pri Austrijskoj akademiji znanosti, razvio je novi model kvantnog generatora slučajnih brojeva. Riječ je o uređaju koji na zahtjev, odnosno putem električnog impulsa, daje jedan slučajni bit u izuzetno kratkom vremenu i to uz 100 postotnu učinkovitost.

Uređaj funkcionira slično bacanju novčića s tim da bacanje i očitanje 'novčića' traje vrlo kratko i da novčić nikada ne ispadne iz ruke. **Ovaj bi se sklop, u principu, mogao postojećom tehnologijom svesti na veličinu čipa, čime bi se otvorile mogućnosti za vrlo širok spektar primjena. Rezultate istraživanja objavio je ugledan multidisciplinarni znanstveni časopis Scientific Reports (IF 5.58) kojeg objavljuje Nature Publishing Group.**

Slučajni brojevi igraju izuzetno važnu ulogu u kontekstu suvremenog društva koje se temelji na razmjeni informacija i digitalnoj obradi podataka u računalima, mobilnim uređajima, bankomatima i sl. Slučajni brojevi neizostavni su dio kriptografskih protokola koji su neophodni kako bi se osigurali sigurnost, privatnost i integritet podataka.

"Nizovi slučajnih brojeva potrebni su za cijeli niz primjena: kriptografsku zaštitu podataka, znanstvena istraživanja, simulacije, a koriste se i u stvarnim i virtualnim kockarnicama i on-line igrama, no je naša primarna motivacija bilo rješavanje fundamentalnog problema kvantnog sprezanja." – objašnjava dr. Stipčević, viši znanstveni suradnik u 'Ruđerovom' Laboratoriju za elektromagnetske i slabe interakcije te voditelj Istraživačke jedinice za fotoniku i kvantnu optiku Centra izvrsnosti za napredne materijale i senzore – CEMS.

Svatko tko se bavi programiranjem zna da su softverski generirani slučajni brojevi zapravo pseudo-slučajni, međusobno povezani matematičkom formulom i stoga predvidljivi i nesigurni za primjenu u kriptografiji te mogu dati pogrešne rezultate u znanstvenim simulacijama. Za razliku od pseudo-slučajnih softverskih generatora koji se često koriste u računalnim metodama, fizički generatori slučajnih nizova brojeva, poput ovog, ne ovise o složenim algoritmima, već o fundamentalnoj slučajnosti odabranog fizičkog procesa.

U ovom radu pod naslovom: "An On-Demand Optical Quantum Random Number Generator with In-Future Action and Ultra-Fast Response" znanstvenicima je pošlo za rukom razviti generator koji je jednostavan za primjenu, koji nudi 100 postotnu učinkovitost u proizvodnji slučajnog bita svaki puta kad ga se to traži i to u vrlo kratkom vremenu (ispod 10 nanosekundi), a da pri tome ništa u prošlosti (tj. prije 'bacanja novčića') ne utječe na rezultat.

"Kašnjenje između zahtjeva i dostupnosti slučajnog bita kod novog kvantnog generatora slučajnih brojeva je nedvojbeno najkraće moguće s postojećom tehnologijom s obzirom da ona zahtijeva minimalni logički slijed procesa potrebnih za generiranje jednog bita, odnosno samo jedan proces emisije i jedan proces detekcije fotona - najmanje količine svjetla." – objašnjava Stipčević.

Istraživanje je učinjeno u sklopu Istraživačke jedinice za fotoniku i kvantnu optiku Centra izvrsnosti za napredne materijale i senzore – CEMS.

KONTAKT PODACI SUGOVORNIKA NA TEMU:

Dr. sc. Mario Stipčević, viši znanstveni suradnik
Email: Mario.Stipcevic@irb.hr
Telefon: +385 1 457 1261
Laboratorij za elektromagnetske i slabe interakcije
Zavod za eksperimentalnu fiziku