http://physicsweb.org/article/news/10/10/2
2006/10/03

رکردِفاصله یِ جدید ی برا یِ رمزنگاری یِ کوانتمی

یک کلید ِ کوانتمی‌رمزشده را به فاصله یِ 184.6 km منتقل کرده اند، که 50% بیش از رکرد ِ قبلی (122 km) است.

این کار ِ پژوهش‌گران ی از آزمایش‌گاه ِ ملی یِ لُس آلامُس (لَنِل) [1] در نیو مِکزیکُ و مئسسه یِ ملی یِ استانداردها و فناوری (نیست) [2] در بولدِر ِ کُلُرادُ (هردو در ایالات ِ متحد) است [3]. رکرد ِ قبلی (122 km) را آوریل ِ سال ِ پیش پژوهش‌گران ی از آزمایش‌گاه ِ پژوهشی یِ تُشیبا در کِمبریج [4] برپا کرده بودند.

با انتشارِکلید ِ کوانتمی (کیوکِی‌دی) [5]، دو کاربر (که معمولاً به آن‌ها اَلیس [6] و باب [7] می‌گویند) یک کلید ِ کاتوره‌ای یِ مشترک به دست می آورند که با استفاده از آن می‌توانند اطلاعات ِشان را رمز و با امنیت مخابره کنند. این اطلاعات به شکل ِ فتون مخابره می‌شود و هر جاسوس ی (ایوْ [8]) هم که بخواهد به اطلاعات دست یابد آن را مختل می‌کند و به این ترتیب کار َش فاش می‌شود. این روش راه ی برا یِ مخابرات ِ کاملاًامن (یک هدف ِ مقدس در مخابرات) پیش می‌نهد که امنیت ِ آن با قانون‌ها یِ فیزیک ِ کوانتمی تضمین می‌شود.

دانا رُزِن‌بِرگ [9] (یک ی از این پژوهش‌گران از لَنِل) به فیزیکس‌وِب [10] گفت: " با استفاده از حس‌گرها یِ لبه‌یِ‌گذار ِ فَراکم‌نوفه کلیدِمنتشرشده ای ساخته ایم که در مسافت ِ بیش از 184.6 km در برابر ِ حمله‌ها یِ استاندارد امن است. انتقال به فاصله‌ها یِ بیش‌تر مهم است، چون به این ترتیب می‌شود فاصله یِ ایست‌گاه‌ها یِ تقویت‌کننده از هم را بیش‌تر کرد و برا یِ کاربرها یی که فاصله یِشان از هم زیاد است امکان ِ مخابره یِ امن به وجود آوْرْد."

به گفته یِ این پژوهش‌گران، فناوری یِ کلیدی یی که به این رکردشکنی انجامیده

حس‌گر ِ لبه‌یِ‌گذار (تی‌ای‌اِس) [11]ِ نیست است. تی‌ای‌اِس دراخترفیزیک هم برا یِ آشکارکردن ِ نور ِ ضعیف ِ ستاره‌ها به کار می‌رود و با آن می‌شود 65% ِ فتون‌ها یِ دریافت‌شده را آشکار کرد، درحال ی که فتودی‌یُدها یِ تجارتی یِ سنتی فقط 20% ِ این فتون‌ها را آشکار می‌کنند. این یعنی این پژوهش‌گران می‌توانستند تک‌فتون‌ها را با بازده یِ زیاد و با شمارشِ‌تاریک ِ صفر آشکار کنند. (شمارشِ‌تاریک سیگنال ی است که در نبود ِ نور ِ فرودی به آشکارگر تولید می‌شود.) رُزِن‌بِرگ گفت: " با استفاده از آشکارگرها یِ تی‌ای‌اِس برا یِ انتشارِکلید ِ کوانتمی، نسبت به آشکارگرها یِ سنتی بیت‌ها یِ امن‌تر ی در فاصله‌ها یِ بیش‌تر به دست می آید."

اما سنجه یِ موفقیت در کیوکِی‌دی فقط فاصله یِ انتشار نیست، امنیت هم مهم است. رکرد ِ 184.6 km ِ لَنِل/نیست با میان‌گین ِ بزرگ‌تر ی از تعداد ِ فتون‌ها بر تپ (نسبت به رکرد ِ قبلی یِ 122 km) به دست آمده است. به این ترتیب احتمال ِ این که یک تپ ِ لیزر بیش از یک فتون داشته باشد بیش‌تر می‌شود. وقت ی یک تپ ِ لیزر بیش از یک فتون داشته باشد، به طور ِ نظری احتمال ِ این که یک جاسوس یک فتون ِ مکرر را بگیرد بی آن که وجود َ ش آشکار شود بیش‌تر می‌شود. به این پدیده حمله یِ کاهشِ‌تعدادِفتون‌ها (پی‌اِن‌اِس) [12] می‌گویند.

گروه ِ لَنِل/نیست با همان میان‌گینِ‌تعدادِفتون‌برتپ ِ گروه ِ کِمبریج به فاصله یِ 148.7 km رسید. به علاوه، این گروه توانست کلید ی کاملاً امن نسبت به حمله‌ها یِ پی‌اِن‌اِس را به فاصله یِ 67.5 km بفرستد و رکرد ِ قبلی (50.6 km) را بشکند.

هدف ِ بعدی یِ این گروه ِ پژوهشی استفاده از کیوکِی‌دی یِ تله‌دار است، که اخیراً بار آمده. دراین فرآیند شدت ِ فتون‌ها یِ منتشرشده را تغییر می‌دهند تا تله‌ها یی درست شود که هرگونه تلاش ِ ایو برا یِ استراقِ‌سمع را آشکار و از کلید در برابر ِ حمله‌ها یِ پی‌اِن‌اِس حفاظت کند. رُزِن‌بِرگ می‌گوید: " در آزمایش‌ها یِ بعدی یِمان انتشارِکلید ِ کوانتمی یِ تله‌دار و افزایش ِ امنیت و فاصله یِ انتشار با ترکیب ِ حس‌گرها یِ لبه‌یِ‌گذار و تله را بررسی خواهیم کرد."

[1] Los Alamos National Laboratory (LANL)

[2] National Institute of Standards and Technology (NIST)

[3] New Journal of Physics **8** 193

[4] Toshiba's Cambridge Research Laboratory

[5] Quantum key distribution (QKD)

[6] Alice

[7] Bob

[8] Eve

[9] Danna Rosenberg

[10] physicsweb

[11] Transition-Edge Sensor (TES)

[12] photon-number-splitting (PNS)