http://physicsweb.org/article/news/7/6/6
2003/06/09

رمزنگاری رکرد ِ 100 km را شکست

پژوهش‌گران ی در بریتانیا، رکرد ِ فاصله برا یِ رمزنگاری یِ کوانتمی را شکستند. رمزنگاری یِ کوانتمی روش ِ اپتیکی یی برا یِ مخابرات ِ شنودناپذیر با تارها یِ اپتیکی است. اَندرو شیلدز [1] و هم‌کاران َ ش از مرکز ِ اروپایی یِ پژوهشی یِ تُشیبا [2] در بریتانیا، خبر ِ این ارتباط ِ رکردشکن (به طول ِ بیش از 100 km) را در کنفرانس ِ لیزر و الکترواپتیک [3] در بالتیمُر اعلام کردند.

مخابرات با رمزنگاری یِ کوانتمی ذاتاً امن است، چون در آن از ویژه‌گی‌ها یِ فیزیکی یِ تک‌فتون‌ها استفاده می‌شود. در این روش، هر بیت ِ یک کلید ِ رمزنگاشته رو یِ یک تک‌فتون کد می‌شود. فرستنده و گیرنده، هر کدام کلید ی برا یِ رمزگشایی یِ یک رشته فتون دارند. اما هر کوشش ی برا یِ شنود ِ پی‌غام محکوم به شکست است، چون با این کار حالت ِ کوانتمی یِ فتون‌ها یِ شنودشده تغییر می‌کند. این تغییرات را به‌ساده‌گی می‌شود آشکار کرد، و از این طریق می‌شود وجود ِ شنودگر را تشخیص داد. در عمل، وجود ِ تضعیف در تار ِ نوری و نوفه در واحد ِ آشکارگر، فاصله ای که رمزنگاری‌یِ‌کوانتمی در آن کارا است را محدود می‌کند.

گروه ِ تُشیبا، توانست با استفاده از یک آشکارگر ِ فراکم‌نوفه در آشکارگر (که تک‌فتون‌ها را آشکار می‌کند) فاصله یِ ارتباط را به‌بود دهد. این آشکارگر بر اساس ِ یک ترانزیستراِثرمیدان ِ مدولاسیون‌آلاییده [4] یِ گالیم آرسنید و آلمینیم گالیم آرسنید است، که به فرآیندها یِ بهمنی متکی نیست و به همین علت کم‌تر از ابزارها یِ معمولی به نوفه حساس است.

رکرد ِ قبلی یِ انتقال 87 km بود، که آن را نوامبر ِ گذشته پژوهش‌گران ی از شرکت ِ

ژاپنی یِ میتسوبیشی الکتریک [5] بر پا کردند. آن‌ها هم برا یِ افزایش ِ فاصله، آشکارگر ِ جدید ی بار آورده بودند که احتمالِ‌شمارش ِ حالتِ‌تاریک ِ آن کم بود.

انتظار می‌رود وقت ی سیستم‌ها یِ رمزنگاری یِ کوانتمی تجارتی شوند، اولین کاربران ِ این سیستم‌ها بانک‌ها و سازمان‌ها یِ دولتی باشند.

[1] Andrew Shields

[2] Toshiba Research Europe

[3] Conference on Lasers and Electro-Optics (CLEO)

[4] modulation doped field effect transistor (MODFET)

[5] Mitsubishi Electric