http://physicsweb.org/article/news/7/1/8
2003/01/16

خبر ِ بد برا یِ رمزشکن‌ها

رمزنگاری یِ کوانتمی، با رمزکردن ِ پیام‌ها با استفاده از حالت‌ها یِ کوانتمی یِ فتون‌ها دورنما یِ یک انتقال ِ کاملاًامن ِ داده‌ها را می‌دهد. اما فیزیک‌پیشه‌ها دریافته اند ساختن ِ چشمه‌ها یِ تک‌فتونی (که برا یِ بیش‌تر ِ شکل‌ها یِ رمزنگاری یِ کوانتمی لازم است) دشوار است. فْرِدِریک گُرُسان [1] از مئسسه یِ اپتیک ِ اُرسِی [2] در فرانسه، و هم‌کاران َش به طور ِ تجربی روش ی برا یِ رمزکردن ِ داده‌ها با استفاده از تپ‌ها یِ شامل ِ چندصد فتون نمایش داده اند. حتا اگر کیفیت ِ تپ‌ها طی ِ انتقال کاهش یابد، روش ِ آن‌ها امن می‌ماند [3].

در رمزنگاری، داده‌ها یِ پیام را با ضرب‌کردن در عدد ِ معین ی رمز می‌کنند. برا یِ بازکردن ِ رمز، گیرنده این عدد را در عدد ِ دیگر ی (به اسم ِ کلید) ضرب می‌کند، که به عدد ِ اول مربوط است. اما برا یِ این که رمزکردن کار کند، باید کلید را سری نگه داشت.

در بیش‌تر ِ شکل‌ها یِ رمزنگاری یِ کوانتمی، کلید شامل ِ یک رشته تک‌فتون است. برا یِ تعیین ِ کلید، فرستنده (که معمولاً اسم ِ اَلیس [4] را به او می‌دهند) قطبش ِ هرفتون را از بین ِ چندین جهت ِ نامتعامد انتخاب می‌کند و فتون را می‌فرستد. کوانتم‌مکانیک می‌گوید قطبش ِ فتون عوض نمی‌شود تنها اگر گیرنده (باب [5]) این قطبش را در همان دوجهت ِ متعامد ی بسنجد که اَلیس فرستاده. اگر باب قطبش را در جهت ِ دیگر ی بسنجد، فقط در حدوداً نیم ی از موارد جواب ِ درست به دست می آورد.

برا یِ تعیین ِ کلید، باب قطبش ِ هر فتون را در جهت ِ دل‌بخواه ی می‌سنجد و به اَلیس خبر می‌دهد چه سنجش‌ها یی انجام داده. سپس اَلیس به باب می‌گوید کدام یک از سنجش‌ها یِ باب در همان جهت ِ موردِنظر ِ اَلیس بوده، و این فتون‌ها به عنوان ِ کلید ِ

امن به کار می‌روند. بخش ی از این کلید را به طور ِ علنی به هم اعلام می‌کنند، و به این طریق می‌توانند بفهمند جاسوس ی (ایوْ [6]) در کار بوده یا نَه، چون هر سنجش ی که ایوْ انجام داده باشد، احتمالاً قطبش ِ بعض ی از فتون‌ها را عوض کرده. به علاوه، کوانتم‌مکانیک می‌گوید ایوْ نمی‌تواند کپی یِ کامل ی از کلید تهیه کند و آن را به باب رد کند.

گُرُسان و هم‌کاران َ ش، در سیستم ِشان به جا یِ قطبش ِ تک‌فتون‌ها، مقدار ِ میان‌گین ِ دامنه و فاز ِ میدان ِ الکتریکی یِ گروه ی از فتون‌ها را به کار می‌برند. این مقدارها هم (مثل ِ قطبش ِ تک‌فتون‌ها) قید ِ عدمِ‌قطعیت را بر می‌آورند. اما برخلاف ِ قطبش ِ تک‌فتون (که نسبت به هر دومحور ِ متعامد ی می‌تواند فقط دو مقدار می‌گیرد)، این کمیت‌ها می‌توانند گستره یِ پی‌وسته ای از مقادیر را بگیرند.

چندین گروه دارند کاربرد ِ چنین‌متغیرها یِ پی‌وسته ای در رمزنگاری یِ کوانتمی را بررسی می‌کنند. اما گُرِسان و هم‌کاران َ ش اولین‌ها یی اند که این پتانسیل را به طور ِ تجربی نمایش داده اند و قدم‌ها یی هم برا یِ تهیه یِ سخت‌افزار و نرم‌افزار ِ لازم برا یِ کار کار با کلید ِ سری بر داشته اند. سیستم ِ آن‌ها، چون متغیرها یِ پی‌وسته را می‌سنجد به این وابسته نیست که قطبش ِ همه یِ تک‌فتون ِ گسیلیده را بسنجد. در واقع این پژوهش‌گران توانستند کلید را با آهنگ ِ 75 000 بیت بر ثانیه بفرستند، هر چند بیش از نیم ی از سیگنال ِ فرستاده‌شده از بین رفته بود.

فیلیپ گُرانژیه [7] (سرپرست ِ این گروه) می‌گوید: " روش ِ ما، بالقوه بسیارسریع‌تر از شمارش ِ تک‌فتون‌ها است. به همین خاطر این روش برا یِ فرستادن ِ کلید ِ سری با آهنگِ‌بیت ِ زیاد به فاصله یِ کم (نوعاً کم‌تر از 15 km) مناسب است. اما برا یِ بررسی یِ رفتار ِ آن در فاصله‌ها یِ بیش‌تر، تحلیل ِ بیش‌تر ی لازم است."

قدم ِ بعدی یِ این پژوهش‌گران ساختن ِ دست‌گاه ی است که بتواند این فتون‌ها را با تارها یِ اپتیکی منتقل کند.

[1] Frédéric Grosshans

[2] Orsay

[3] Nature **421** 238

[4] Alice

[5] Bob

[6] Eve

[7] Philippe Grangier