

<http://physicsweb.org/article/news/9/5/5>

2005/05/10

رمزنگاری ی کوانتومی و تصویر

یک گروه فیزیک پیشه از تُشیبا [1] برای انتقال - صدا و تصویر از طریق - یک کانال - امن - تاراپتیکی رمزنگاری ی کوانتومی را به کار برده اند. این نمایش از آن نظر مهم است که نشان می دهد روش - رمزنگاری ی تک فتونی با ترافیک - واقعی ی اینترنت سازگار است و ضمناً به حد - کافی مقاوم هست که بشود آن را در شبکه ها ی تاراپتیکی ی تجارتی به کار برد. این سیستم را آندرو شیلدز [2] و هم کاران - ش از تُشیبا ریسرچ یورپ [3] در کمبریج [4]، برای نماینده ها ی دولت و مؤسسه ها ی مالی نمایش دادند.

شیلدز می گوید: ” نمایش برای ی ویدیو ی رمزنگاشته انجام شد، چون می خواستیم دو چیز را نشان بدهیم: اول این که می شود مقدار - زیاد ی داده را رمز کرد، و دوم این که می شود کلید - رمز را به طور - مرتب تغییر داد. آزمایش ها یی هم با MCI انجام داده ایم و دیده ایم که سیستم - مان می تواند حدود - یک ماه به طور - پیوسته و بدون - مشکل روی آن شبکه کار کند.“

مخابرات با رمزنگاری ی کوانتومی ذاتاً امن است، چون هر یک از بیت ها ی یک کلید - رمزنگاری روی یک تک فتون رمز شده است. کلید - رمزنگاری شامل - تعداد - زیاد ی بیت است که علی الاصول فقط برای ی گیرنده و فرستنده معلوم اند. هر کس - دیگری نخواهد این کلید را کپی کند یا تغییر دهد، فرستنده و گیرنده به سرعت می فهمند.

مولد - کلید کوانتومی ی تُشیبا می تواند تا 100 کلید - کوانتومی (تک فتون) بر ثانیه تولید کند، که برای رمز کردن - هر تک تصویر - ویدیو با یک کلید - جداگانه کافی است. این مولد در 1.55 میکرون و با تارهای اپتیکی ی استاندارد کار می کند و به طور - پیوسته مسیر - اپتیکی را می باید و کنترل می کند. به این ترتیب، این سیستم می تواند به طور - پیوسته و بی نیاز از مداخله ی کاربر کار کند.

فعالاً تُشیباً برای تولید - کلید - کوانتمی از تپ‌های لیزر - شدیداً تضعیف شده استفاده می‌کند و برای آشکار کردن - آن‌ها از آشکارگرهای نور - بهمینی بی‌تخصصی شده. اما شیلدز می‌گوید این شرکت دارد آشکارگرها و دی‌یوهای نورگسیل بی‌اساس - نقطه‌ها بی‌کوانتمی می‌سازد که می‌توانند تک‌فتون آشکار و تولید کنند. او گفت: ”نه تنها این فناوری بالقوه کم‌خرج است، بل که می‌شود آن را برای آهنگ‌داده بی‌بیش‌تر و تارهای اپتیکی بی‌بلندتر هم به کار برد. ما برای هر دو مورد ابزار - سرنمونه داریم و داریم آن‌ها را در سیستم - رمزنگاری پیمان یک‌پارچه می‌کنیم، اما 2 تا 3 سال طول می‌کشد تا بشود آن را به‌طور - روزمره به کار برد.“

پارسال رمزنگاری بی‌کوانتمی را برای اولین بار در یک مبادله بی‌تجاری به کار بردند: شهردار - وین از طریق - یک کابل - تار اپتیکی و با استفاده از یک کلید - کوانتمی، از شهرداری به بانک - آوستریا کُردیت آنشتالت [5] پول فرستاد.

- [1] Toshiba
- [2] Andrew Shields
- [3] Toshiba Research Europe
- [4] Cambridge
- [5] Austria Creditanstalt