انتقال ِ امن ِ کلید ِ کوانتمی به فاصله ی ِ زیاد

کلید ِ کوانتمی برا ی ِ رمزنگاری، در شکل ی ساده به این ترتیب ساخته میشود که فرستنده یک رشته بیت به گیرنده میفرستند که هر کدام ممکن است در یک ی از چهار حالت ِ ممکن باشند، حالت ِ 0 یا 1 (مثلَن قطبشها ی ِ عمودی-افقی)، یا حالت ِ $0'$ یا $1'$ (قطبشها یِ در راستا ی ِ نیمسازها ی ِ خطها ی ِ عمودی و افقی). اگر معلوم باشد حالت از دسته ی ِ بدون ِ پریم است یا از دسته ی ِ پریمدار، آشکارگر ِ مناسب به کار میرود و حالت ِ سیستم سنجیده میشود. گیرنده و سارق ِ احتمالی هیچ یک نمیدانند حالت ِ هر بیت از کدام دسته است. پس آشکارگرها را به تصادف انتخاب میکنند. اگر سارق ی در کار نباشد، به طُر ِ میانگین نیم ی از انتخابها ی ِ گیرنده درست بوده. گیرنده پس از سنجش انتخابها یَش (ولی نَ نتایج ِ سنجش) را به فرستنده میگوید، و فرستنده به او میگوید کدام انتخابها درست بوده. اگر سارق ی کوشیده باشد دادِها را بخاند، بعض ی از دادِها خراب شده اند، چون سارق برا ی ِ بعض ی از دادِها آشکارگر ِ نادرست به کار برده. فرستنده و گیرنده میتوانند بخش ِ کوچک ی از دادِها ی ِ متناظر با انتخابها ی ِ درست ِ گیرنده را با هم کنترل کنند و بفهمند داده ای خراب شده یا نَ.

اما اینها وقت ی ست که همه ی ِ ابزارها بینقص باشند. معلوم شده وجود ِ بعض ی نقصها در ابزارها این روش را آسیب-پذیر میکند. از جمله با فرستادن ِ باریکه ای قوی در هم ان کانال ِ انتقال- ِ-داده میشود آشکارگرها ی ِ کوانتمی را عملَن کلاسیک کرد. یک روش ِ دیگر که آسیب-پذیری یَش کمتر است، این است که فرستنده و گیرنده هردُ رشتِها یی بفرستند و بیتها ی ِ متناظر در این رشتِها جا ی ِ دیگر ی با هم تداخل کنند. از تداخل معلوم میشود کدام زُج- ِفُتُنها از یک دست و کدام از دُ دسته ی ِ مختلف َند، یی آن که در تداخلگر معلوم شود هر یک از فُتُنها یی که از فرستنده یا گیرنده آمده از کدام دسته است. اما آهنگ ِ انتقال ِ داده به این روش کم (دست- ِ-بالا 0.1 بیت بر ثانیه) بوده است. حالا توانسته اند به این روش کلید ِ کوانتمی را به فاصله ی ِ 200 km در یک تار ِ نوری منتقل کنند و آهنگ ِ انتقال ِ داده را هم 500 برابر کنند [1].

[1] Physical Review Letters **113** 190501