مجلهٔ پژوهش فیزیک ایران، جلد ۲۳، شمارهٔ ۳، پاییز ۱۴۰۲
DOI: 10.47176/ijpr.23.3.51684

توزیع کلید کوانتومی در شبکه‌های کامپیوتری

مائده عباسی[۱]، احمد شریعتی[۱]، و رضا محمدی[۲]

۱. دانشکده فیزیک، دانشگاه الزهرا، تهران، ایران

۲. دانشکده مهندسی و فناوری، دانشگاه ابوعلی سینا همدان، همدان، ایران

پست الکترونیکی: Ma.abbasi@alzahra.ac.ir

(دریافت مقاله: ۱۴۰۲/۰۲/۲۴ ؛ دریافت نسخهٔ نهایی: ۱۴۰۲/۰۵/۰۷)

چکیده

انتقال امن کلیدها بین دو طرف، یکی از مشکلات اولیه در رمزنگاری است. احتمال دستکاری یا رهگیری کلید از طریق یک استراق سمع کننده، دلیل این نگرانی است. یک راه امیدوارکننده برای حل این مشکل، توزیع کلید کوانتومی (QKD) است. توزیع امن کلیدهایی که ممکن است برای رمزگذاری و رمزگشایی پیام ها استفاده شوند، با این رویکرد امکان پذیر می‌شود، که از ایدهٔ مکانیک کوانتومی استفاده می‌کند. QKD درجه‌ای از حفاظت را ارائه می‌دهد که نمی‌تواند با استفاده از تکنیک‌های رمزنگاری کلاسیک انجام شود، و قابلیت قابل توجهی برای کاربرد در حوزه‌هایی دارد که مکاتبات ایمن در آنها بسیار مهم است. QKD یک زمینهٔ مطالعاتی است که موافقت‌نامه‌های مختلفی را در جهت توانمندسازی جایگزین ایمن کلیدهای رمزنگاری بین دو طرف، آلیس و باب، آورده است. دو دستورالعمل کلیدی در این زمینه عبارتند از BB84 که توسط بنت (Bennett) و برسارد (Brassard) طراحی شد و E91 که توسط اکرت (Ekert) پیشنهاد شد. البته دستورالعمل‌های دیگری توسعه یافته‌اند، بسیاری از این دو رویکرد اساسی الهام می‌گیرند. ما به طور خاص بر روی دستورالعمل E91 تمرکز کردیم و پتانسیل آن را برای انتقال ایمن جفت‌های درهم‌تنیده در شبکه‌های کامپیوتری بررسی کردیم. این دستورالعمل از درهم‌تنیدگی بین ذرات به عنوان وسیله‌ای برای تأیید امنیت تبادل کلید استفاده می‌کند. تحقیقات ما حول محور بررسی مبادله درهم‌تنیدگی برای دو ذره با استفاده از دستورالعمل E91 و ارائهٔ طرحی برای این منظور، با هدف توسعهٔ روشی جدید برای انتقال ایمن جفت‌های درهم‌تنیده از طریق شبکه‌های کامپیوتری بود. یافته‌های ما راه‌های امیدوارکننده‌ای را برای تحقیقات آینده در اجرای مبادلهٔ درهم‌تنیدگی ایمن در کاربردهای عملی نشان می‌دهد.

واژه‌های کلیدی: کلیدکوانتومی، مبادله درهم‌تنیدگی، رمزنگاری

مقالهٔ کامل در بخش انگلیسی همین شمارهٔ مجله به چاپ رسیده است.