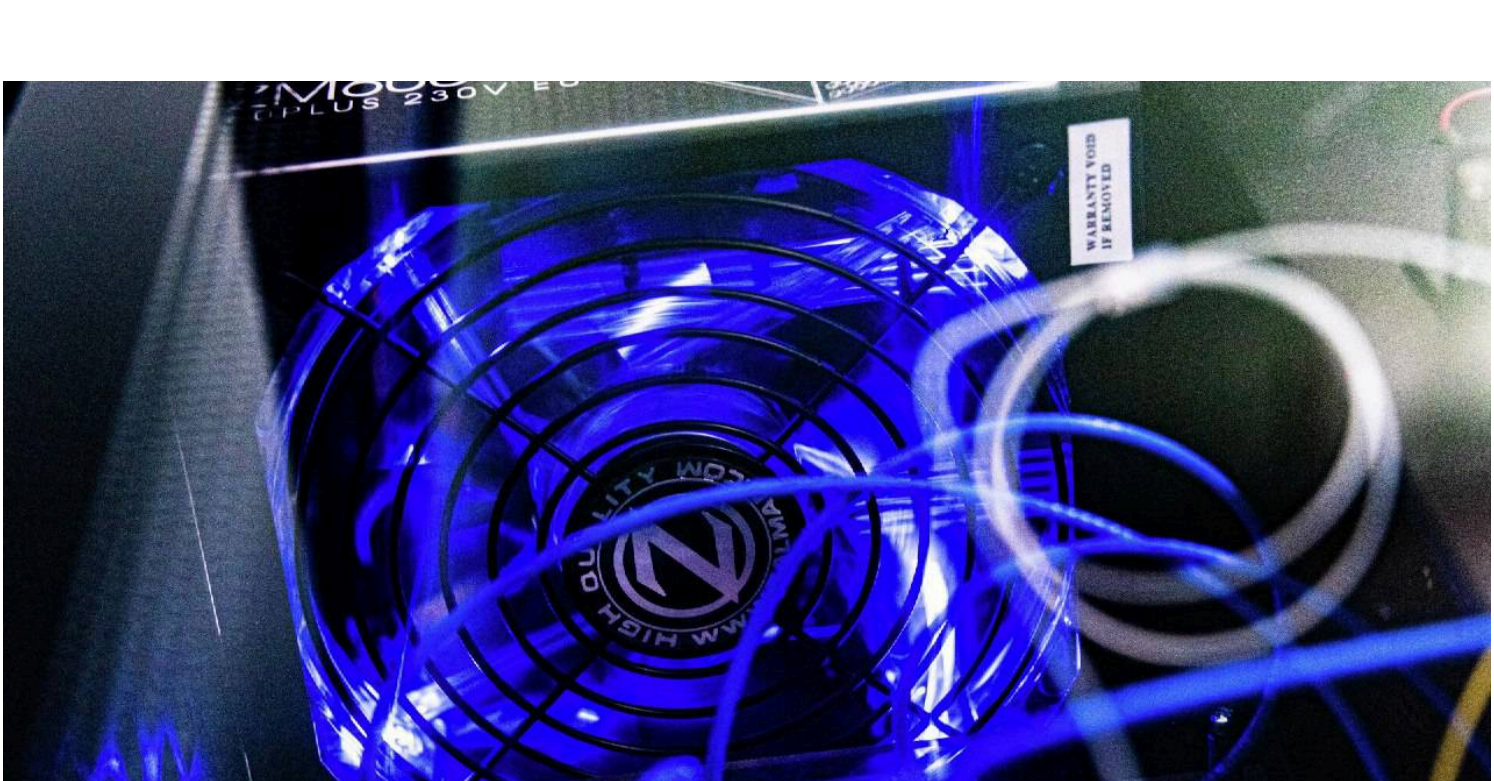
روش جدید مقابله با تهدیدات اینترنتی رایانه‌های کوانتومی در روسیه

۲۴ آبان ۱۴۰۱



محققان دانشگاه فنی ارتباطات و اطلاعات مسکو روش جدیدی برای مقابله با تهدیدهای هکری از طرف رایانه‌های کوانتومی

پیشنهاد کردند. برای این منظور می‌توان از ریزپردازنده‌های رمزنگاری‌شده (کریپتوگرافی) استفاده کرد. در حال حاضر همکاران علمی در حال تدوین طرح‌های جدید برای تهیه استانداردهای رمزنگاری ضد کوانتومی ملی روسیه هستند. به عقیده محققان دانشگاه، راه مقابله با چالش‌های ناشی از رایانه‌های کوانتومی که به راحتی رمزهای با منبع باز را می‌شکنند، استفاده از رایانه‌های ضدکوانتومی یا پست‌کوانتومی (فراکوانتومی) است. در رویکرد جدید، به جای استفاده از الگوریتم‌های قدیمی دیفی–هلمان برای تولید رمز قابل اشتراک و استاندارد امضای الکترونیکی گوست ۳۴.۱۰–۲۰۱۸، محققان برای اولین بار استفاده از سامانه‌ای از نوع کلاسیک مک‌اِلیس را پیشنهاد می‌کنند؛ سامانه‌ای که برپایه کدهای جبری–هندسی است و مولفه‌های آنها بسته به ظرفیت محاسباتی سامانه تحت حفاظت و سطح مورد نیاز تامین امنیت اطلاعات می‌تواند متفاوت باشد. نتایج تحقیقات در مجموعه مقالات همایش امسال (۲۰۲۲) سامانه‌های همگام‌سازی سیگنال‌ها، تولید و پردازش در مخابرات راه دور (سینکروانفو) منتشر شده‌است.