شناسنامه پروژه رمزنگاری کوانتومی

شناسنامه پروژه	
نام پروژه **فارسی: رمزنگاری کوانتومی** **انگلیسی: The Quantum Cryptography**	
نام زیرگروه پژوهشی: اطلاعات و ارتباطات کوانتومی	**کد پروژه:**
ارزیابی سطح آمادگی فناوری: مطالعات نظری، امکان سنجی و طراحی مفهومی ☐ طراحی تفصیلی، ساخت و آزمون نمونه اولیه در محیط آزمایشگاهی ■ ساخت و آزمون نمونه محصول در محیط عملیاتی ☐	
چکیده و نتایج پروژه: رمزنگاری کوانتومی استفاده مکانیک کوانتومی به خصوص ارتباطات کوانتومی و محاسبات کوانتومی برای اجرای عملیات رمزنگاری و شکستن سیستم‌های رمزگذاری شده را توصیف می‌کند. استفاده از رمزنگاری کلاسیک (غیر کوانتومی) برای حفاظت در برابر حمله کنندگان کوانتومی نیز به عنوان رمزنگاری کوانتومی در نظر گرفته می‌شود. نمونه‌هایی از رمزنگاری کوانتومی استفاده از ارتباطات کوانتومی برای رد و بدل کردن مخفیانه کلید (توزیع کلید کوانتومی) یا استفاده از رایانه‌های کوانتومی برای شکستن انواع گوناگون کلیدهای عمومی و امضاهای دیجیتال می‌باشد. رمزنگاری کوانتومی انجام عملیات گوناگون رمز گذاری را که با تبادلات کلاسیک غیرممکن است میسر می‌سازد که این یکی از مزیت‌های رمزنگاری کوانتومی است. مکانیک کوانتومی تضمین می‌کند که با اندازه‌گیری داده‌های کوانتومی، این اطلاعات از بین می‌روند از این ویژگی می‌توان برای تشخیص مداخله دشمن در یک پیغام استفاده کرد. برای انجام این پروژه می‌توان از چهار فناوری استفاده از لیزر پالسی ضعیف، تک فوتون‌ها، فوتون‌های درهم‌تنیده و یا متغیرهای پیوسته استفاده کرد. به نظر می‌رسد استفاده از فوتون‌های درهم‌تنیده راه مناسب‌تری باشد.	
دستاوردهای پروژه: • مخابرات امن • اینترنت امن • ارتباطات امن	