باسمه تعالی

عنوان قرارداد پژوهشی: طراحی و ساخت فرستنده-گیرنده سیستم توزیع کلید کوانتومی سازگار با شبکه

نتیجه بررسی گزارش فاز اول

تاریخ: ۹ اردیبهشت ۱۴۰۴

با تشکر و تقدیر بابت تهیه گزارش فاز اول، موارد زیر جهت اصلاح و تکمیل گزارش به استحضار می رسد:

۱- متناسب با گام ۱-۱ پروژه، لازم است بررسی دقیق سرعت انتقال کلید امن بر حسب فاصله، شدت پالس (میزان تضعیف)، سرعت کلاک فرستنده، dark count، اثر روش sifting و privacy-implification در سه پروتکل DPS، COW و BB84-decoy انجام شود. در این زمینه مراجع [23-21] مرجع اصلی می تواند مفید و راهگشا باشد (و البته سایر مقالات در این حوزه). بر اساس پارامترهای ذکر شده لازم است منحنی هایی همچون منحنی سرعت انتقال امن کلید بر حسب فاصله (مثلا مشابه شکل ۲ در مرجع [21]) با در نظر گرفتن شرایط مساله ما و پروتکل های مورد نظر ترسیم شود.

۲- طراحی ساختار بهینه برای گیرنده هنوز انجام نشده است و در گزارش نیامده است.

۳- لازم است بر اساس تجهیزات انتخاب شده و در لیست قرار گرفته، بند ۱ مورد بررسی قرار گیرد و اثر آنها مشخص شود.

۴- بخش مربوط به روش های تقویت امنیت نیاز بازخوانی و اصلاح دارد.

۵- سناریوی تست بر اساس حملات انتخاب شده مشخص شود.

۶- ساختار و تجهیزات الکترونیک و اپتیک و سرعت کلاک و قدرت AWG مورد نیاز متناسب با Rateهای ذکر شده در خروجی مورد نظر تحلیل شود و حداقل ها معین شود.

- آیا SPAD انتخاب شده برای عملکرد مورد نظر کافی است؟ چرا؟ اگر کافی نیست چه قدر با جواب فاصله دارد؟
- آیا Modulator انتخاب شده برای عملکرد مورد نظر کافی است؟ چرا؟ اگر کافی نیست چه قدر با جواب فاصله دارد؟
- این سوال برای تجهیزات حساس دیگر مورد بررسی قرار گیرد.

۷- اصلاحات ضروری در متن گزارش:

- برای پروتکل DPS با نور همدوس که در گزارش توصیف شده است، رفرنس ۲۴ اشتباه است.
- اشتباه مفهومی: پروتکل COW شکل ۲,۷ اصلاح شود. در COW تنها سه استیت ارسال میشود. مفهوم حالت دیکوی که در این پروتکل به کار میرود با آنچه برای مقابله با حمله PNS با استفاده از شدت های مختلف به کار می‌رود متفاوت است.
- اشتباهات جدید: صفحه ۴۵
- رفرنس دهی به همه‌ی اشکال و جداول که خودتان آن را تولید نکرده‌اید.
- برخی واژگان و اشکالات که در گزارش اشاره شده است. مانند صفحات ۱۲، ۱۶ و ...
- برخی اصلاحات که بعد از کامنت‌های قبلی، اعمال نشده‌اند. مانند صفحه ۳۳، ۳۹، ۴۱، ۴۲ و...

۸- سایر اصلاحات جزئی

- فاصله‌ی footnote ها از خط پایین صفحه در حد استاندارد شود. تصاویر و جداول تا حد امکان در وسط صفحه نباشد (بالا یا پایین صفحه). هم‌چنین، شماره‌گذاری بخشها از راست به چپ باشد.
- پروتکل DPS به خوبی توصیف نشده است. از آنجا که در این پروتکل انتخاب پایه نداریم و بعد از پایان مرحله کوانتومی، غربال کلید نداریم، با سایر پروتکل‌های QKD از نظر شهود امنیتی متفاوت است و لازم است توضیحات مقتضی داده شود. اگر منابع مرتبط مطالعه نشده و زمان‌بر است، برای گزارش بعدی انجام شود.

۹- سایر نکات ذکر شده در متن گزارش بررسی و اصلاح شود.

در ضمن گام ۱- ۶ پس از خرید تجهیزات بررسی، تحویل گیری و ارزیابی خواهد شد.

با تشکر

حسین بهرامگیری

ناظر قرارداد