برنامه شبیه‌سازی پروتکل‌های توزیع کلید کوانتومی

برنامه شبیه‌سازی پروتکل‌های توزیع کلید کوانتومی یک برنامه شبیه‌سازی رویداد گسسته است که به ما اجازه می‌دهد یک پروتکل توزیع کلید کوانتومی به همراه پساپردازش را با پارامترهای گوناگون شبیه‌سازی کنیم و نتایج آن در سنجه‌های گوناگون همچون نرخ کلید امن و خطای کلید بررسی کنیم.

معماری برنامه شبیه‌سازی

برنامه شبیه‌سازی دارای چند بخش است. در شکل ۱ شماتیک معماری برنامه را آورده‌ایم.

۱. بخش Simulator

در این بخش، هسته شبیه‌سازی رویداد گسسته را پیاده‌سازی کردیم و شامل دو ماژول Event و Simulation است. ماژول Event کلاس رویدادهای شبیه‌سازی و ماژول Simulation کلاس هسته‌ی شبیه‌سازی را تعریف می‌کنند. کلاس هسته‌ی شبیه‌سازی پروتکل توزیع کلید کوانتومی، کانال کوانتومی، پارامترهای فرستنده و گیرنده، نرخ جریان تاریک، نرخ کلاک، پروتکل پساپردازش و شمار سیگنال‌های ارسالی را به عنوان ورودی می‌گیرد. خروجی یک شبیه‌سازی را داده‌های آلیس و باب است و شامل کلید خصوصی آن‌دو است.

۲. بخش QDevices

در این بخش، مجموعه‌ای از ادوات کوانتومی -- فیبر، باریکه‌شکن، تداخل‌سنج ماخ-زندر و آشکارسازی فوتونی -- را پیاده‌سازی کردیم.

۳. بخش QState

در این بخش، حالت‌های کوانتومی را پیاده‌سازی کردیم. از آنجا که تا کنون تنها به حالت‌های همدوس نیاز داشتیم، این بخش ماژول حالت‌های همدوس را دارد. همچنین، ماژولی برای تعریف قطبش سیگنال‌های پیاده‌سازی کردیم.

۴. بخش QKD

در این بخش، پروتکل‌های توزیع کلید کوانتومی BB84+decoy، COW و DPS را پیاده‌سازی کردیم. به طور کلی، هر پروتکل به چهار قسمت تقسیم شده است؛ ساخت سیگنال، آشکارسازی، غربال و تخمین پارامتر. در هر قسمت، خروجی داده‌های تولید شده بدست آلیس و باب است، همچون کلیدهای خصوصی، نرخ خطا و زمان اندازه‌گیری است.

۵. بخش PostProc

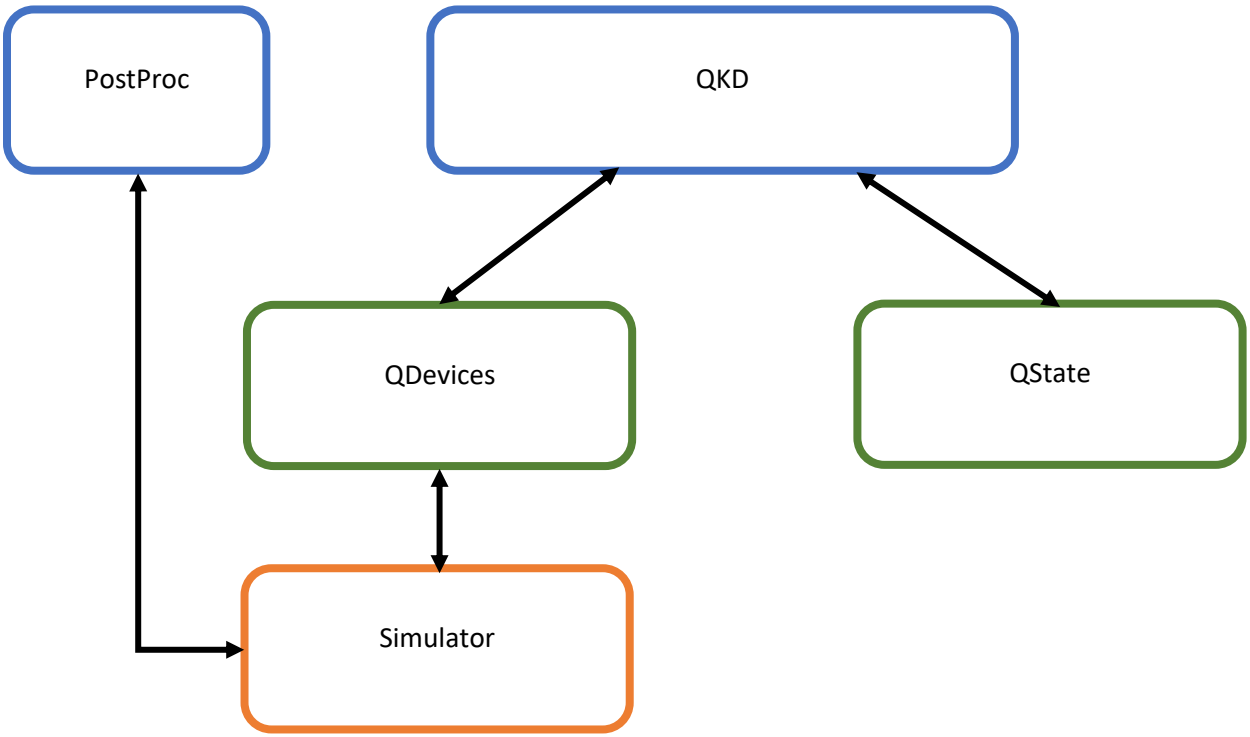
در این بخش، پروتکل‌های پساپردازش را پیاده‌سازی کردیم. این بخش شامل دو ماژول InfoRecon و PrivAmp است که به ترتیب، تطبیق‌سازی اطلاعات و تقویت حریم‌خصوصی را پیاده‌سازی می‌کنند.

نتایج شبیه‌سازی

برای نمونه چند شبیه‌سازی انجام دادیم.

نمودارهای خطا بر حسب طول فیبر

برای هر سه پروتکل COW، BB84 و DPS میزان خطا بیت کوانتومی و خطای کلید پیش از پساپردازش را بدست آوردیم. در این سه شبیه‌سازی شدت سیگنال را 0.7 و شدت سیگنال فریب را 0.1 گذاشتیم. همچنین نسبت نرخ جریان تاریک به نرخ کلاک را برابر با 10 گذاشتیم، یعنی به طور میانگین در هر کلاک، هر آشکارسازی ۱۰ جریان تاریک ثبت می‌کند.

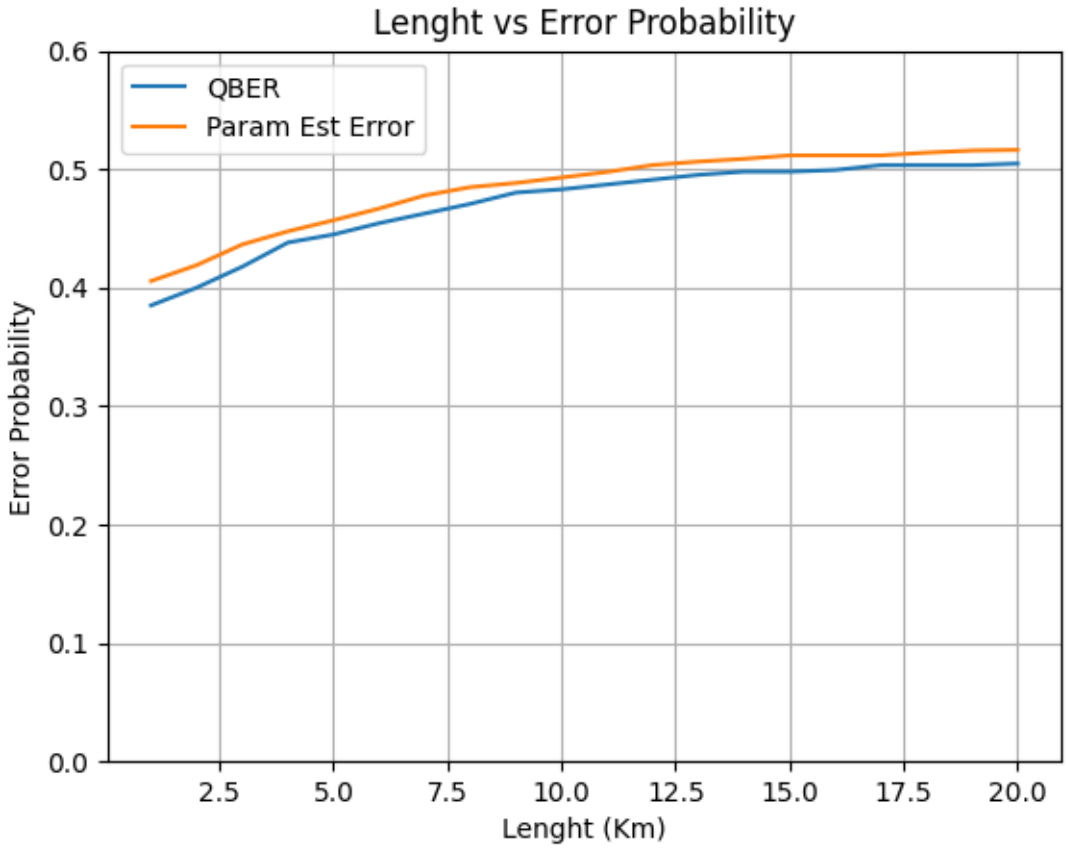


شکل ۱ معماری برنامه

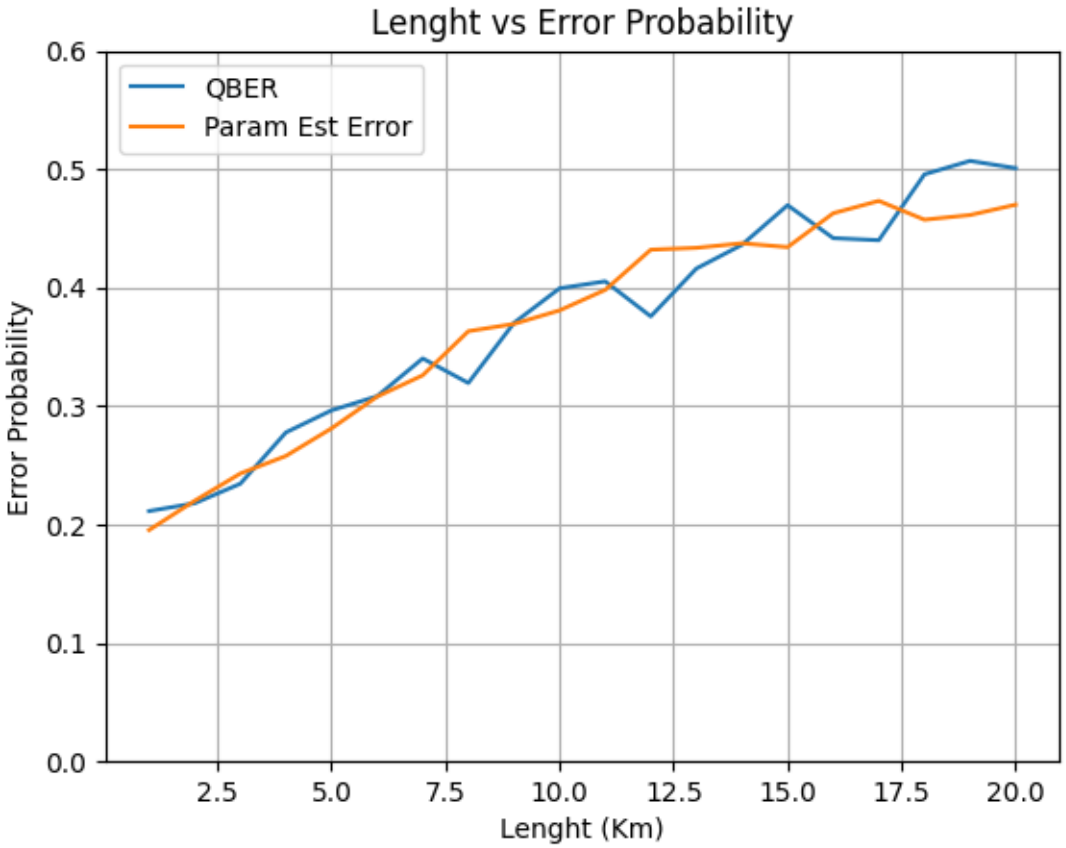
همانطور که از شکل ۲ آشکار است، از آنجا که در پروتکل BB84 اطلاعات بر روی قطبش سیگنال پیدا می‌شود، افزایش طول در نرخ خطا آنچنان ماثر نیست. در واقع، از آنجا که شدت سیگنال بسیار کم است، حتی در کمترین حالت تضعیف، سیگنال به ندرت در آشکارساز آشکار می‌شود. شکل ۳ و ۴ نیز نشان می‌دهد که میزان خطا در دو پروتکل COW و DPS وابستگی مستقیم به میزان تضعیف دارد.

نمودار میزان خطا بر حسب شدت سیگنال

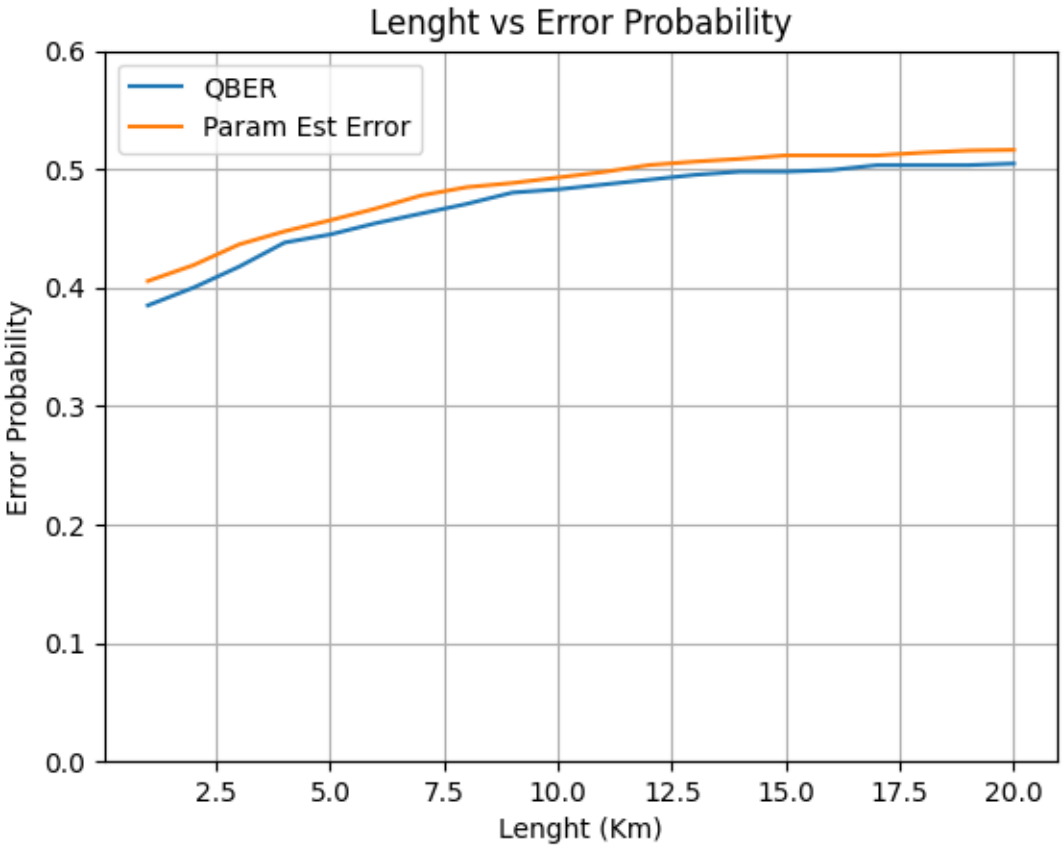
در نمودار شکل ۵ میزان خطا بیت کوانتومی، خطای پیش از پساپردازش و خطای میان دو کلید پس از انجام پساپردازش برای پروتکل BB84 بر حسب شدت سیگنال بدست آوردیم. همانطور که پیشتر گفتیم، با افزایش شدت سیگنال، احتمال آشکار شدن آن در آشکارساز افزایش می‌یابد و از این خطا کاهش می‌یابد. همچنین، دقت کنید که پس از انجام پساپردازش میزان خطای میان دو کلید آلیس و باب صفر می‌شود.



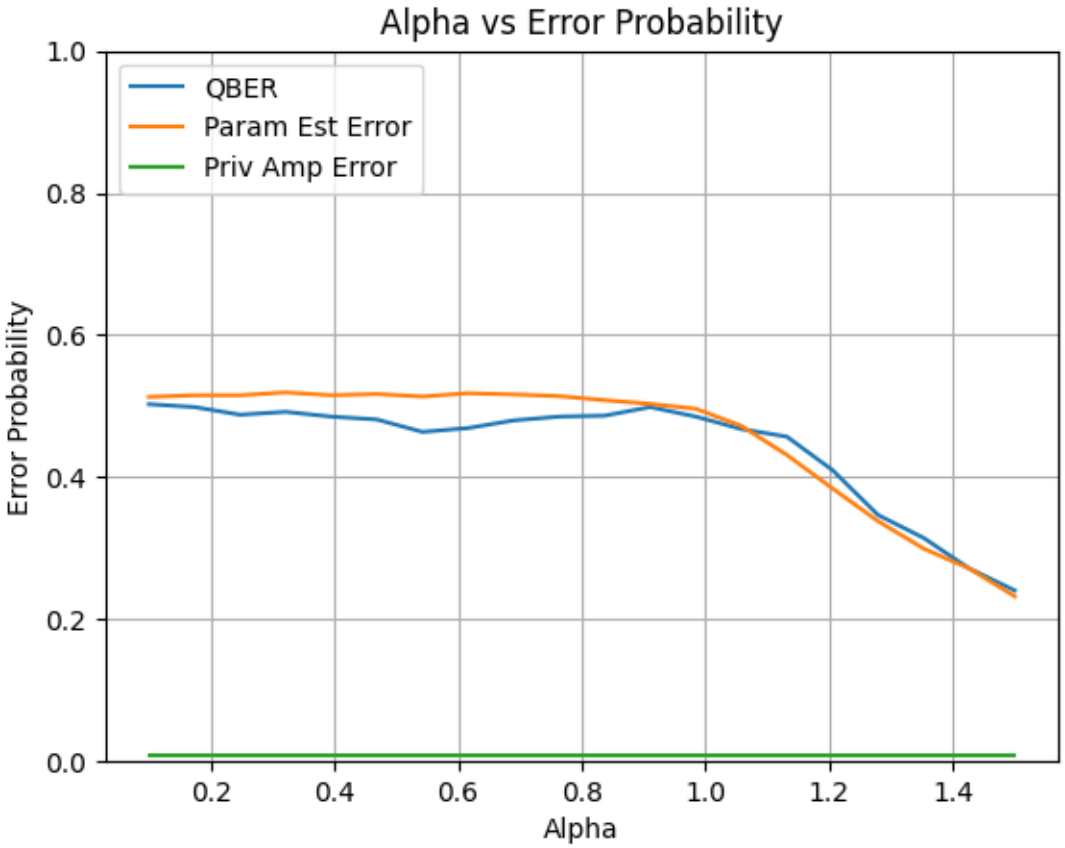
شکل ۲نمودار BB84



شکل ۳نمودار DPS



شکل ٤نمودار COW



شکل ۵ نمودار شدت