# 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.

1. 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.
2. بخش QDevices  
   در این بخش، مجموعه‌ای از ادوات کوانتومی -- فیبر، باریکه‌شکن، تداخل‌سنج ماخ-زندر و آشکارسازی فوتونی -- را پیاده‌سازی کردیم.
3. 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.
4. 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.

1. 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

شکل 1معماری برنامه

Simulator

QDevices

QState

QKD

PostProc