|  |
| --- |
| **عنوان پروژه**: **ساخت تولید کننده‌ی اعداد تصادفی(QRNG)** |
| **کاربردها**:  تولید کننده های اعداد تصادفی طیف گسترده ای از کاربردهای بالقوه در زمینه های مختلف دارد، از جمله می‌توان به موارد زیر اشاره کرد:  رمزنگاری: تولید اعداد واقعا تصادفی برای سیستم های رمزنگاری امن، مانند تولید کلید، رمزگذاری و رمزگشایی ضروری است. تولید کننده های اعداد تصادفی را می توان برای بهبود امنیت و استحکام سیستم های رمزنگاری با اطمینان از غیرقابل پیش بینی بودن و ایمن بودن کلیدهای تولید شده در برابر حملات مورد استفاده قرار داد.  شبیه سازی مونت کارلو: شبیه سازی مونت کارلو در زمینه های مختلف از جمله مالی، مهندسی و فیزیک برای شبیه سازی سیستم های پیچیده و محاسبه احتمالات استفاده می شود. از تولید کننده های اعداد تصادفی می توان برای تولید اعداد تصادفی استفاده کرد که می تواند به عنوان ورودی شبیه سازی های مونت کارلو استفاده شود و دقت و قابلیت اطمینان آنها را بهبود بخشد.  تجزیه و تحلیل آماری: اعداد تصادفی اغلب در تحلیل های آماری مانند نمونه گیری و آزمون فرضیه ها استفاده می شوند. تولید کننده های اعداد تصادفی را می توان برای تولید اعداد واقعا تصادفی استفاده کرد که می تواند دقت و قابلیت اطمینان تجزیه و تحلیل آماری را بهبود بخشد.  ارتباط امن: تولید کننده های اعداد تصادفی را می توان برای تولید کلید برای سیستم های ارتباطی ایمن، مانند SSL/TLS و VPN استفاده کرد و از محرمانه بودن و یکپارچگی ارتباطات بین طرفین اطمینان حاصل کرد. |
| **شرایط موجود در کشور**:  تا به حال چند شرکت دستگاه توزیع اعداد تصادفی با ویژگی‌های متفاوت تولید کرده‌اند. |
| **شرایط موجود در دنیا:**  چندین شرکت تولید کننده QRNG در دنیا وجود دارد که برخی از آنها عبارتند از:   * QuintessenceLabs * ID Quantique * QuantumCTek. * توشیبا * Quantis   نام برخی از محصولات هر یک از شرکت‌های بالا به شرح زیر است:  Quintessence Labs:  QL1000: یک QRNG پرسرعت که از تونل کوانتومی برای تولید اعداد تصادفی با سرعت 10 گیگابیت بر ثانیه استفاده می کند که برای استفاده در برنامه های کاربردی با امنیت بالا طراحی شده و به عنوان یک دستگاه در سطح سازمانی موجود است.  qStream: یک دستگاه فشرده QRNG که از تونل زنی کوانتومی برای تولید اعداد تصادفی با سرعت حداکثر 4 مگابیت در ثانیه استفاده می کند که برای استفاده شخصی طراحی شده و صورت USB در دسترس است.  ID Quantique:  Quantis QRNG: یک دستگاه QRNG فشرده که از تشخیص فوتون برای تولید اعداد تصادفی استفاده می کند که می تواند تا 1 گیگابیت بر ثانیه داده تصادفی تولید کند و به صورت USB یا یک دستگاه شبکه در دسترس است.  Quantis Appliance: یک دستگاه QRNG در سطح سازمانی که از تشخیص فوتون برای تولید اعداد تصادفی با سرعت حداکثر 8 گیگابیت بر ثانیه استفاده می کند که برای استفاده در برنامه های کاربردی با امنیت بالا طراحی شده و با افزونه‌های مختلف در دسترس است.  QuantumCTek:  مولد اعداد تصادفی کوانتومی: یک دستگاه فشرده QRNG که از تشخیص فوتون برای تولید اعداد تصادفی با سرعت حداکثر 16 مگابیت بر ثانیه استفاده می کند که به صورت USB یا شبکه موجود است و برای استفاده در برنامه های مختلف از جمله مالی و بازی طراحی شده است.  توشیبا:  G-Rex: یک QRNG با سرعت بالا که از تشخیص فوتون برای تولید اعداد تصادفی با سرعت حداکثر 4 گیگابیت بر ثانیه استفاده می کند و برای استفاده در برنامه های مختلف از جمله ارتباطات امن و تراکنش های مالی طراحی شده است.  QRNG مینیاتوری: دستگاه فشرده QRNG که از تشخیص فوتون برای تولید اعداد تصادفی با سرعت حداکثر 1 مگابیت بر ثانیه استفاده می کند و برای استفاده شخصی طراحی شده و به صورت USB در دسترس است.  کوانتیس:  Quantis QRNG: یک دستگاه QRNG فشرده که از تشخیص فوتون برای تولید اعداد تصادفی استفاده می کند و می تواند تا 4 مگابیت در ثانیه داده تصادفی تولید کند و به صورت USB یا شبکه در دسترس است.  Quantis Appliance: یک دستگاه QRNG است که از تشخیص فوتون برای تولید اعداد تصادفی با سرعت حداکثر 16 گیگابیت بر ثانیه استفاده می کند و برای استفاده در برنامه های کاربردی با امنیت بالا طراحی شده و با افزونه های مختلف در دسترس است. |
| **بیان و تشریح مسئله:**  انگیزه ایجاد یک QRNG پرداختن به محدودیت‌های مولد اعداد شبه تصادفی سنتی (PRNG) است، که الگوریتم‌های قطعی هستند که دنباله‌هایی از اعداد را تولید می‌کنند که به نظر تصادفی هستند اما واقعاً تصادفی نیستند. PRNG ها در برابر حملات آسیب پذیر هستند و در صورتی که الگوریتم یا مقدار ورودی اولیه مشخص باشد، می توان آنها را پیش بینی یا دستکاری کرد. از سوی دیگر، QRNG ها اعداد واقعا تصادفی تولید می کنند که قابل پیش بینی یا دستکاری نیستند و بسیار ایمن تر و قابل اعتماد تر از PRNG ها هستند.  مولد اعداد تصادفی کوانتومی (QRNG) دستگاهی است که از فرآیندهای مکانیک کوانتومی برای تولید اعداد واقعا تصادفی استفاده می کند. QRNG ها بر اصول مکانیک کوانتومی، مانند اصل عدم قطعیت و تصادفی بودن حالت کوانتومی، برای تولید اعداد واقعا تصادفی مورد استفاده قرار می گیرند.  خروجی یک QRNG دنباله ای از اعداد تصادفی است که می تواند در برنامه های مختلفی که نیاز به تصادفی بودن، امنیت و قابلیت اطمینان دارند استفاده شود و به طور فزاینده ای در زمینه هایی مانند رمزنگاری، شبیه سازی مونت کارلو، بازی، تجزیه و تحلیل آماری و ارتباطات ایمن اهمیت پیدا می کنند. |
| **اهداف پروژه:**  هدف این پروژه طراحی، توسعه و پیاده سازی یک مولد اعداد تصادفی کوانتومی (QRNG) با سطح بالایی از آنتروپی، امنیت و قابلیت اطمینان است. دستگاه باید قادر به تولید اعداد واقعا تصادفی با سرعت کافی برای برآوردن نیازهای برنامه های مختلف، با تمرکز بر برنامه های کاربردی حساس به امنیت باشد.  طراحی، توسعه و پیاده سازی: هدف این پروژه انتقال QRNG از مرحله مفهومی به یک محصول کاملاً کاربردی است که می تواند برای برنامه های مختلف استفاده شود.  سطح بالایی از آنتروپی، امنیت و قابلیت اطمینان: دستگاه باید قادر به تولید اعداد تصادفی غیرقابل پیش بینی، بدون الگو و تحت تأثیر هیچ عامل خارجی باشد. QRNG باید در برابر حملات مختلفی که می تواند تصادفی بودن خروجی را به خطر بیندازد، ایمن باشد.  سرعت کافی: QRNG باید قادر به تولید اعداد تصادفی با سرعتی باشد که نیازهای برنامه های مختلف را برآورده کند. از آنجایی که در کشور چند شرکت توانسته اند این دستگاه را بسازند، از ذکر سرعت مطلوب چشم پوشی می کنیم و با توجه به پروپوزال های ارسالی یک طرح انتخاب می شود.  QRNG باید شرایط زیر را برآورده کند:  آنتروپی: QRNG باید اعداد تصادفی با سطح بالایی از آنتروپی تولید کند. آنتروپی معیاری برای تصادفی بودن دنباله ای از اعداد است و سطح بالایی از آنتروپی برای تولید اعداد واقعا تصادفی ضروری است.  امنیت: QRNG باید در برابر حملات دشمنانی که سعی در پیش‌بینی یا دستکاری خروجی دارند، ایمن باشد.  سرعت: QRNG باید قادر به تولید اعداد تصادفی با سرعت کافی باشد.  کارایی: QRNG باید از نظر انرژی کارآمد باشد و با مصرف انرژی کم کار کند. بهره وری انرژی برای کاهش هزینه عملیاتی QRNG ضروری است و مصرف کم انرژی می تواند به کاهش اندازه و وزن دستگاه کمک کند.  استحکام: QRNG باید قوی و قابل اعتماد باشد و بتواند در شرایط محیطی مختلف بدون خرابی یا کاهش قابل توجه عملکرد کار کند. QRNG باید قادر به کنترل عوامل محیطی مختلف مانند دما، رطوبت و لرزش باشد.  اندازه: QRNG باید فشرده و قابل حمل باشد و برای استفاده در طیف وسیعی از دستگاه ها و برنامه ها مناسب باشد.  سازگاری: QRNG باید با طیف وسیعی از سیستم ها و پلتفرم ها از جمله سخت افزار، نرم افزار و پروتکل ها سازگار باشد.  انطباق: QRNG باید با استانداردها و مقررات صنعتی مربوطه، مانند NIST SP 800-90B و FIPS 140-2 و دیگر استانداردهای مرتبط مطابقت داشته باشد.  تعمیر و نگهداری: نگهداری و ارتقاء QRNG با پشتیبانی فنی و مستندات باید آسان باشد.  هزینه: هزینه تخمینی ساخت QRNG باید در پیشنهاد گنجانده شود. هزینه باید معقول و مقرون به صرفه باشد.  در نهایت از میان پیشنهاد های مطرح شده، پیشنهادی انتخاب می شود که انتظارات بیشتری را براورده کند. لازم به ذکر است که ممکن است برای بهبود دستگاه های ساخته شده، نیاز به تعریف مراحل بعدی باشد تا در نهایت بتوان به یک دستگاه که همه ی انتظارات بالا را براورده کند، دست یابیم. |
| **مرحله‌ی بعدی پروژه:** بستگی به پیشنهادهای ارسالی دارد. |