|  |
| --- |
| **عنوان پایان نامه:** بررسی مدلهای کوانتومی مناسب در رمزنگاری |
| **استاد راهنما:** جناب آقای دکتر صدیف احد پور کلخورانی |
| **مقطع تحصیلی :** کارشناسی ارشد **رشته ی :**فیزیک  **گرایش**: بنیادی(نظری)**دانشگاه :** محقق اردبیلی  **دانشکده :** علوم پایه**تاریخ فارغ التحصیلی : تعداد صفحات :** |
| **کلید واژه ها :**رمزنگاری**-**آشوبناک**-** متغیرجداگانه**-** توزیع کلید کوانتومی |
| **چکیده :**رمز گشایی سیستمهای رمزنگاری کلاسیک با توجه به تکنولوژی روز بسیار پیچیده و زمانبر میباشد ولی با ظهور کامپییوترهای کوانتومی زمان لازم یرای گشودن رمز این سیستمها بطور قابلملاحظه ای کاهش می یابد. از طرفی هیچیک از سیستمها قابلیت تشخیص جاسوس را ندارد.در این پایان نامه هدف, معرفي رمزنگاري كوانتومي و بررسی جنبه های مختلف آن میباشد.در فصل دوم مهمترین پروتکلهای پیشنهاد شده برای این نوع رمز نگاری معرفی شده و امنیت هر کدام بررسی میشود.در فصل سوم رمز نگاری با متغیر پیوسته را معرفی میکنیم, و سپس در آخر این فصلرمز نگاری با متغیر ناپیوسته را تعریف میکنیم و با تعریف یک مدل ناپیوسته هامیلتونین برای یک ذره ضربه زده شده توسط اشعه گاوسی وبا استفاده از نظریه آنتروپی واطلاعات شانون نشان میدهیم که این نوع رمز نگاری در مقابل جاسوس از امنیت زیادی برخوردار استطوریکه کوچکترین تغییر در شرایط اولیه باعث آشکار سازی جاسوس میشود. |