Sudan University of Science & Technology
College of Graduate Studies

Simulation of Quantum Cryptography Based on Ekert Protocol

A Thesis Submitted To The College Of Graduate Studies As A Fulfillment Of The Requirements For The Philosophy Degree in Physics

By

Sara Idris Babiker Mustafa

Supervised by:

Prof. Nafie Abdellateef

December2006

المستخلص

التشفير الكمى هو علم جديد يعتمد على إستخدام بروتوكلات مصممة للإستفادة من ظواهر ميكانيك الكم لضمان سرية توزيع مفاتيح التشفير . الغرض الأساسي من توزيع المفاتيح بواسطة التشفير الكمى هو أن يتفق طرفا الإتصال (الذين لا يملكون فى الأساس أى معلومات سرية مشتركة) على مفاتيح تشفير عشوائية ، بحيث تبقى سرية لكل محاولات كسر الشفرة . مهما كانت قوة هذه المحاولات التحليلية أو الحاسوبية .

تم فى هذه الأطروحة بناء برنامج محاكاة للتشفير الكمى بإستخدام بروتوكول Ekert . الذى يعتمد على متراجحة Bell . وهو بورتوكول له القدرة لكشف المتلصص من خلال إنتهاك متراجحة . Bell

تحدث الأخطاء فى الإرسال الكمى نتيجة لسببيين هما عملية التجسس (عند حدوثها) ونقاط الخلل فى منظومة الإتصال . لذلك يتم تطبيق تقنية تصحيح الأخطاء . بعد ذلك يتم إستخدام تقنية رياضية لزيادة سرية المفاتيح .

تم بناء برنامج المحاكاة بإستخدام لغة دلفى 7 البرمجية. وعرضت نتائج المحاكة بنمط تفاعلى لمستخدم البرنامج التي توضح تأثر كل من الخطأ المتوقع و قيمة متراجحة Bell ثم عدد حالات التطابق بزيادة عدد أزواج الفوتونات. كذلك نوقش تأثير معلمات زيادة السرية على معلومات المتجسس .

بالإضافة الى عرض بعض النماذج الحية التى توضح نجاح البرنامج فى تشفير وإعادة تشفير الرسائل .

Abstract

Quantum cryptography is new science that relies on the use of protocol designed to exploit quantum mechanical phenomena to achieve the secrecy of cryptographic keys. The purpose of quantum key distribution is for two correspondents, who share no secret information initially, to agree on random keys, which remain secret against attacks from more powerful analytic or computational tools.

In this thesis: simulation software for a quantum cryptography based on Ekert – protocol was built. Ekert protocol based on Bell's theorem that can expose eavesdroppers by violated Bell's inequality.

Error can occur in quantum transmission due eavesdropping and system inefficiencies. Thus, error elimination technique was implemented. After Error elimination an important mathematical technique called privacy amplification was implemented.

The simulation software was built in Borland Delphi language version 7. The simulation result was displayed in an interactive manner with respect to the software user, which explains the effect of number of EPR photons pair on number of coincidences, expected error and Bell's parameter, in case of no-eavesdropping. Also effect of point wise privacy amplification parameters on Eve's information was discussed.
In Addition, some examples of encryption and decryption of message was presented to explain the successful of software.