Ministry of Higher Education &
Scientific Research
University of Baghdad

Decoy - State Quantum Key Distribution System

A Thesis submitted to the Institute of Laser for Postgraduate Studies, University of Baghdad in partial fulfillment of requirements for the degree of Master of Science in Laser/ Electronic and Communication Engineering

By

Sura Adel Abbas

2011 AD *1432 AH*

Abstract

The goal of this work is to check the presence of Eavesdropping (PNS attack) in quantum cryptography system based on BB84 protocol, and to get a maximum secure key length as possible. This goal was achieved by using decoy states with the original signal states of the system. These decoy states with mean photon numbers of 5.38, 1.588 and 0.48 were interleaved randomly between the signal states with mean photon numbers of 2.69, 0.794 and 0.24 by a program used for operating driver circuits for the transmitter laser diodes of the system.

The readings of single photon avalanche photodiodes, working at Geiger mode at temperature T=-11°C at the detection side, were collected and BB84 protocol was applied to determine the Quantum Bit Error Rate and keys for both signal states and decoy states . Also the yields of the single photon avalanche photodiode were calculated to determine the average number of tagged photons to decide the presence of Eavesdropping. The average length for a secure key obtained from our system discarding the cases with Eavesdropping was equal to 125 with 19.583 % decoy states and 82 with 49.753% decoy states for mean photon number of 0.794 for signal states and 1.588 for decoy states.

وزارة التعليم العالي والبحث العلمي
جامعة بغداد

منظومة توزيع المفتاح الكمي ذو الحالة الزائفة

رسالة مقدمة

إلى معهد الليزر للدراسات العليا /جامعة بغداد/ لاستكمال متطلبات نيل شهادة ماجستير علوم في الليزر /الهندسة الالكترونية والاتصالات

من قبل

سرى عادل عباس

١٤٣٢هـ **٢٠١١م**

الخلاصة

الهدف من هذا العمل هو فحص وجود اختراق (فصل الفوتون) لمنظومة التجفير الكمي المعتمدة على بروتوكولBB84 وللحصول على المفتاح الاطول و الاكثر سرية قدر الامكان.

هذا الهدف حقق باستعمال حالات زائفة بالاضافة لحالات الاشارة للمنظومة هذه الحالات الزائفة كانت بمعدل عدد فوتونات = ٠,٤٨ ١,٥٨٨، ٥,٣٨ والتي تخللت عشوائيا بين حالات الاشارة والتي بمعدل عدد فوتونات = ٠,٢٤ ، ٠,٧٩٤ ، ٢,٦٩ .

قراءات كواشف الفوتون المنفرد ذات الانهيار المضاعف والتي تعمل حسب اسلوب كايكر بدرجة حرارة - ١١درجة سيليزية في جهة الكشف من المنظومة والتي تم جمعها وتم تطبيق بروتوكول BB84 لحساب م عدل خطأ الوحدة الكمية وايجاد المفاتيح لحالات الاشارة والحالات الزائفة.

كذلك حسبت نواتج كواشف الفوتون المنفرد ذات الانهيار المضاعف لايجاد عدد الفوتونات المميزة لتقرير وجود الاختراق .

معدل طول المفتاح السري لمنظومتنا الذي تم الحصول عليه باهمال حالات وجود الاختراق، يساوي ١٢٥ عند وجود معدل ٥٠٪ حالات زائفة و يساوي ٨٢ عند وجود ٢٠٪ حالات زائفة لمعدل عدد فوتونات ٠,٧٩٤ لحالات الاشارة و ١,٥٨٨ للحالات الزائفة.