Ministry of Higher Education &
Scientific Research
University of Baghdad

Experimental Realization of Quantum Cryptography System Based on the BB84 Protocol

A thesis

submitted to the Institute of Laser for Postgraduate Studies , University of Baghdad in partial fulfillment of requirements for the degree of Doctor of Philosophy in Laser .

By

Sheelan Khasraw Tawfiq

Abstract

This work is concerned with experimental realization of quantum cryptography system based on BB84 protocol.

In this work a setup was built consisting of four laser diodes at the transmitter that operate randomly emitting photons polarized at diagonal and rectilinear bases to encode the information consisting of random bits of "0"s and "1"s in order to construct the key needed for data encryption.

The receiver consists of four high speed solid state avalanche photodiodes operating in the Geiger mode each arranged with optical components that consist of a non- polarizing beam splitter , two polarizing beam splitter and half wave plate. The polarizing beam splitter splits an unpolarized light into two orthogonally polarized beams at 90^0. Using the beam splitter plus the half wave plate and the polarizing beam splitters, the received photons will be directed randomly and then polarizing beam splitters split the received beam of light according to the beam's polarization to activate the corresponding APD that is arranged to give "0" or "1" depending on which APD is activated at that time.

In addition, the receiver includes the electronic circuits required for producing suitable electrical signals, corresponding to the detectors output, that are further processed for synchronization and recording the digital signals that are sent to the PC to apply the algorithms written in MATLAB6.5 of error correction and privacy amplification.

The work concerns with designing the transmitter circuit that achieves sending minimum number of photons per emitted laser pulse and producing the signals needed for the synchronization between the transmitter and receiver during the detection process.

The parameters that affect the detectors performance involving the number of dark counts, number of blank counts and avalanche photodiodes (APD) output pulse amplitudes have been observed. It has been shown that working with low temperature for the APD, 8^oC, gave minimum number of APD detections including real counts and dark counts that are also lowered by operating the system at dark room at night time. These conditions gave a short key lengths (50 -75 bits) for encryption .Working with the same temperature in a dark room (daytime) gave longer key lengths (195 – 275) bits with high dark counts that introduce errors in the sifted key.

For both cases 30000 bits have been generated randomly with LD firing pulse width equal to 500 ns and an excess voltage varying from 2 to 7 V. The final key is obtained after applying error correction then privacy amplification algorithms. Working with higher temperatures, 28^{o}C, gave longer key lengths for both environment (350 – 780 bits) but with higher dark counts which means more errors in the sifted key.

وزارة التعليم العالي و البحث العلمي
جامعة بغداد

تحقيق تجربة لمنظومة تجفير كمي بالأعتماد على بروتوكول BB84

أطروحة مقدمة

الى معهد الليزر للدراسات العليا / جامعة بغداد لاستكمال
متطلبات نيل درجة دكتوراه فلسفة في الليزر

تقدمت بها

شيلان خسرو توفيق

1427هـ **2006م**

الخلاصة

هذا العمل يتعلق بتحقيق تجربة تجفير كمي بالأعتماد على بروتوكولBB84 . في هذا العمل تم بناء تركيب يتكون من اربعة ليزرات ثنائية عند المرسلة و التي تعمل عشوائيا" باعثة فوتونات مستقطبة بالقواعد القطرية و المستقيمة لتجفير المعلومات التي تتكون من عدد من الأصفار و الواحد العشوائية لتكوين المفتاح اللازم لعمل تجفير للمعلومات.

المستلمة تتكون من اربعة كواشف ضوئية ثنائية ذات الأنهيار المضاعف عالية السرعة و التي تعمل بنمط كايكر كل واحدة منها مرتبة مع مواد بصرية و التي تتألف من موزع ضوء غير مستقطب و موزعان للضوء مستقطبان و قاعدة نصف موجة.

موزع الضوء المستقطب يقوم بتوجيه الفوتونات غير المستقطبة الى فوتونات باتجاهين مستقطبة عموديا مع بعضها بزاوية 90 درجة. باستعمال موزع الفوتونات غير المستقطب و قاعدة نصف الموجة فان الفوتونات المستلمة سيتم توجيهها عشوائيا و من ثم تقوم موجها ت الضوء المستقطبة بتوجيه الفوتونات المستلمة طبقا الى استقطاب الفوتون لتحفيز الكاشف الضوئي الثنائي ذات الأنهيار المضاعف ذات العلاقة و الذي يكون مرتبا ليعطينا صفر أو واحد بالأعتماد على اي كاشف قد تم تحفيزه في تلك اللحظة من الزمن . بالأضافة الى ذلك توجد الدو ائر الألكترونية اللازمة لانتاج اشارات كهربائية مناسبة بالأعتماد على خرج الكاشف ، حيث ان هذا الخرج سوف يتم التعامل معه لتحقيق التزامن و لتسجيل الأشارات الرقمية التي يتم ارسالها الى الحاسوب لتنفيذ برامج تم كتابتها باستعمال برامج MATLAB6.5 لتصحيح الخطأ و تحقيق السرية.

العمل يتعلق بتصميم دوائر المرسلة التي تحقق ارسال اقل عدد من الفوتونات خلال نبضة الليزر المرسلة بطول 500 نانو ثانية و 700 نانو ثانية و تكوين الأشارات اللازمة للتزامن بين المرسلة و المستقبلة خلال عملية الكشف.

تم ملاحظة العوامل التي تؤثر على اداء الكواشف من ناحية عدد مرات الكشف المظلمة و عدد مرات الكشف الفارغة وسعة النبضة الخارجة للكواشف ذات الأنهيار المضاعف .لقد تم التوضيح ان العمل عند درجات الحرارة المنخفضة للكاشف الضوئي الثنائي ذات الأنهيار المضاعف ، 8 درجة مئوية، تعطي اقل عدد من الكشف الذي يتضمن عدد مرات الكشف الحقيقية و عدد مرات الكشف المظلمة و التي يمكن تخفيضها بان يتم تشغيل المنظومة في غرفة مظلمة ليلا ". ان العمل بهذه الشروط اعطى مفتاحا قصيرا (50 – 70) بت لتنفيذ عملية التجفير . العمل بنفس درجات الحرارة في غرفة مظلمة نهارا " أعطت مفتاحا أطو ل (195 – 275) بت مع عدد مرات كشف مظلمة عالية و التي تؤدي الى ظهور أخطاء في المفتاح المدقق.

في الحالتين تم توليد 30000 بت عشوائيا" مع الليزرات الثنائية بنبضة طولها 500 نانو ثانية (و 700 نانو ثانية) مع الفولتية الزائدة للكاشف التي تتغير من 2 فولت الى 7 فولت. المفتاح النهائي يتم الحصول عليه بعد تطبيق خوارزميات تصحيح الخطأ وتحقيق السرية. العمل مع درجات حرارة أعلى (28 درجة مئوية) أعطت مفاتيح أطول للمحيطين (350 – 780) بت و لكن مع عدد مرات كشف مظلمة أعلى و هذا يؤدي الى ظهور أخطاء أكثر في المفتاح المدقق .