الجزئية الأولى:

بسم الله الرحمن الرحيم, الحمدلله رب العالمين والصلاة والسلام على اشرف الأنبياء والمرسلين نبينا محمد وعلى اله وصحبه اجمعين,

انا عبدالعزيز التميمي ومعي نواف الحركان وبدر العتيبي , واليوم باذن الله راح نقدم لكم مشروعنا في الكوانتم كمبيوتنق بعنوان (Quantum distribution key- E91 protocol) .

في هذا المشروع راح نوضح لكم بروتوكول من البروتوكولات في الحوسبة الكمية في باب التشفير (Cryptography) وان شاء الله بنمر بكل الخطوات لتوضيح هذا البرتوكول.

هذا البروتوكول انشئه عالم بريطاني-بولندي , في عام 1991 واسمه ارتور ايكيرت , وسمي البروتوكول باسمه (E91) وهو الحرف الأول من عائلته وسنة اصدار الورقة البحثية.

قمنا في هذا المشروع بأتمتة البروتوكول وتطبيقه برمجياً وتلخيص البحث في عدة خطوات.

**Solutions tools:** استخدمنا أدوات محددة مثل ال(Qiskit) وهي سوفتووير برمجي اوبن سورس تعمل مع برمجة الحوسبة الكمية باستخدام لغة البايثون, استعملنا ايضاً ال(Composer) وهي أداة انشأتها IBM تسمح لمستخدميها ببناء وعرض وتشغيل ال(Circuits) , مما يفيدنا هذا بفهم كيف تعمل ال(Circuits) منطقياً.

**Entanglement**: مفهوم ال(Etanglement ) هو مفهوم معقد قليلاً, هو احد المعايير للحوسبة الكمية, باختصار, اذا اخذنا ذرتين من الفوتون او الالكترون, وغيرنا في قيمة أحدا الذرتين, الذرة الأخرى ستتغير قيمتها **بشكل لحظي** , حتى لو كانت الذرة الأولى موجودة في الأرض والأخرى في اخر كوكب في المجرة, من دون ايضاً فهم سبب الترابط فيما بينهم , حتى العالم الشهير البرت اينشتاين اصبح في حيرة من هذي الحالة الغربية وسماها ب (Spooky action at a distance).

لكن حتى مع عدم فهم هذي الحالة الغريبة, نستطيع استعمالها في ما يفيدنا, وهو شي تم تطبيقه فعلياً, فاصبح الكوانتم مقارنة بالكلاسيك كمبيتور اسرع واقوى بمراحل مع اخذ بالحسبان ان مفهوم الكوانتم كمبيوتر يختلف تماماً عن الكلاسيكال كمبيوتر.

الجزئية الثانية:

**Protocol E91:** في البداية وقبل شرح البروتوكول, بناخذ مثالين للتفريق بين القناة الكلاسيكية والقناة الكمية, لو اخذنا مثال شخصين يتحدثون فيما بينهم باستخدام القناة الكلاسيكية مثل (الهاتف) احتمال ان يكون فيه متنصت (Eavesdropper) احتمال عالي , لهذا وجد التشفير ليكون حتى لو تسمع الشخص للمحادثة ما يقدر يفك التشفير, لكن فك التشفير في هذه الأيام اصبح بالشي الغير صعب , مثل تشفير ال (RSA) اصبح من السهل فكه باستخدام الحوسبة الكمية, فيكون الاعتماد الأمني كلياً مبني على التشفير, لذا نستنتج ان القناة الكلاسيكية والكمبيوتر الكلاسيكي ليس امناً.

لكن في الجهة الأخرى في القناة الكمية من المحال اختراق القناة, في أسوأ الأحوال سيتم تشويش النتيجة المرسلة في القناة بسبب ان حتى في استخدام القناة الكمية يجب استخدام الاتصال الكلاسيكي للتواصل, لكن من المحال استخراج الرسالة المرسلة عن طريق القناة الكمية, لان هذا يتعارض مع مفهوم ال(Entanglement)

**مفهوم البروتوكول:** سنقسم البرتوكول الى خطوات لتتضح الصورة,

اولاً: تاتي الجزئيات (الفوتون) من طرف ثالث موثوق او من موزع للفوتون , فتقسم الجزئيات الى نصفين.

ثانياً: تكون حالة الجزئيات (entangled), لتصل الى المستخدمين (أليس و بوب).

ثالثاً: كل واحد منهم (أليس وبوب) يستخدم بوابات (Gates) بشكل عشوائي لتغيير قيمة الجزيء, وتكوم اما (X) او (Z).

رابعاً: يستخدمون الاتصال الكلاسيكي للاتفاق على أي بوابة تم استخدماها (من الكشف على النتيجة بعد التغيير).

خامساً: باستخدام البوابات المشتركة يتم استخراج المفتاح السري الذي من المحال ان يصل الى غير أليس وبوب.

**Conclusion:** في الختام, تلخيصاً للكلام, التشفير الكمي هو ثورة جديدة في عالم ال(Secure Communication) ومع استمرار الأبحاث، فإن اليوم الذي سنستخدمه فيه بنجاح ليس بعيدًا جدًا.

بروتوكول E91 يقدم المزايا المطلوبة للحفاظ على سرية المعلومات, بحيث انه يحمي خصيصاً من أي تنصت ممكن يصير على القناة.