البحث الثالث

أولا: الملخص باللغة العربية

تم فى هذا البحث تحليل السرية لمفتاح التشفير العام RSA ، و قد تبين من خلال تلك التحليل ان مفتاح التشفير العام RSA يعانى من مشكلتين أساستين:

١. تعرضه لكثير من الهجمات و أهمها:
   i. الهجوم المشفر المختار
   ii. هجوم المفتاح العام الأسى
   iii. هجوم المُعامل المشترك

٢. عملية فك التشفير بطيئة جدا ، و هذا قد أدى الى عدم إستخدام نظام RSA فى التطبيقات التى تتطلب إستهلاك طاقة و ذاكرة أقل مثل شبكات الاستشعارات اللاسلكية.

من خلال هذا البحث ، تم تقديم نظام تشفير جديد ذات المفتاح العام يسمى PQK Cryptosystem . و قد تم عمل تحليل السرية له و تبين أنه آمن ضد عمليات الهجوم التى تواجه نظام التشفير RSA .

من ناحية أخرى ، تم عمل مقارنة بين النظام المقترح و نظام التشفير RSA و تبين ان النظام الجديد أسرع فى عملية فك التشفير من النظام السابق حيث ان النظام المقترح يعتمد فى فك التشفير على حل معادلات خطية بدلاً من حل معادلات أسية معقدة.