ملخص الرسالة

الاسم الكامل:فارس فوزان العتيبي

عنوان الرسالة: مفاضلة تحليلية للنقطة العامة في الضرب القياسي للمنحنى الإهليجي

التخصص:امن المعلومات

تاريخ الدرجة العلمية:شعبان 1440هـ

تم اقتراح العديد من الاساليب لتسريع الضرب القياسي للنقطة العامة في المنحنى الإهليجي. هذه الاساليب تتضمن : اسلوب العمليات السابقة والعمليات اللاحقة. الاساليب المقترحة في الابحاث السابقة تعتمد على تقسيم مفتاح التشفير لاجزاء والتعامل معاه بشكل متوازي. ورغماً عن ذلك لم نصل الى افضل عدد من الأجزاء الذي يقودنا الى اداء افضل. وفقاً لذلك، في هذا البحث اظهرنا تحليل مفصل لكل الاساليب مع احجام مفاتيح مختلفة وعدد معالجات مختلفة وعدد من الطلبات.علاوة على ذلك،تم اقتراح اسلوب جديد وتم اختباره مع بقية الاساليب الآخرى. الاسلوب الجديد المقترح أظهر نتائج افضل وقت معالجة في اغلب الحالات.