الملخص

تزايد استعمال الأجهزة الخلوية واللاسلكية يتطلب أنظمة التشفير المفتاح العام التي تنجز مظاهر من سرية المعلومات و تتلاءم مع محدودية القوة والسعة لتلك الأجهزة مع الاحتفاظ بمستوى عالي من السرية.

تعد أنظمة التشفير على المنحنيات الإهليجية جيلا جديدا من أنظمة التشفير المفتاح العام والتي لها مفتاح أقل حجما لنفس مستوى السرية. إن العملية الأسية على المنحنيات الإهليجية أهم عملية في أنظمة التشفير على المنحنيات الإهليجية، لذلك تكمن المشكلة الرئيسية عند تطبيق تلك الأنظمة في كيفية تسريع العملية الأسية، لذا إن من أهم الاهتمامات هو تطوير طرق وخوارزميات تسمح بتنفيذ أنظمة التشفير على المنحنيات الإهليجية بفاعلية.

في هذه الرسالة، قمنا بتطوير طريقة فعالة لحساب العملية الأسية على المنحنيات الإهليجية المعرفة على الحقل المنتهي باستخدام الإحداثيات الديكارتية المتعامدة. تستطيع هذه الخوارزمية حساب $2^{م}(2^{ن}$ أ + ب) مباشرة من نقطتين أ، ب عشوائيتين على المنحنيات الإهليجية، وبدون حساب النقاط الوسطية، وبالإضافة إلى ذلك قمنا بتطبيق هذه الخوارزمية من أجل حساب العملية الأسية على المنحنيات الإهليجية وتحليل مدى الوقت المستهلك. لقد دلت النتائج عند تنفيذ هذه الخوارزمية أنها تستطيع تسريع العملية الأسية على المنحنيات الإهليجية عند أخذ مفتاح بحجم 160- بت حوالي 21.7 % .