ABSTRACT

The group of the elliptic curve points forms an *Abelian group*, that is a suitable choice for constructing a good problem similar to Discrete Logarithm Problem. This led to create cipher system based on the difficulty of solution elliptic curve discrete logarithm problem that greats a clear change in the cryptography, and open the a new windows for treatment with special group and new operations.

This thesis provides the definition and mathematical characteristics of the elliptic curves, gives the properties of constricted group with it's points. gives how it is possible to be implemented in the cryptography and analyzing the weakness for such group.

This thesis proved a new theorem that can contribute in facilitating the computational process and give method to conclude that each point in the elliptic curve -except the point at infinity- is generator point, if the order- the number of points – is prime.

Also, this thesis provides four proposed methods as a modification of ElGamal cryptosystem with the elliptic curves, as well as, design a program for implementing process of these proposed methods, compute the computational complexity of these methods compared to the original methods, compare these methods with the original methods in running time of several messages have different sizes, a great reduction in calculation time is resulted.

PDF created with pdfFactory trial version www.pdffactory.com

المستخلص

تُشكّلُ مجموعةُ نقاطِ المنحني الإهليلجيِ زمرة ابيلية (Abelian group)، و هذا اختيار مناسب لبناء مشكلة جيدة مشابهة لمشكلة اللوغارثيم المنفصل(DLP). وهذا قادَ لإنشـــاء نظـــامِ تشفير مستند على صعوبة حلِ مشكلةِ اللوغاريتم المنفصل في المنحني الإهليلجـــي (ECDLP). وهـــذا تغيير عظيمِ وواضح في أنظمة التشفير، ويَفْتحُ نوافذ جديدة للمعالجةِ بزمرِ خاصّةِ وعملياتِ جديدةِ.

و تقدم هذه الأطروحة التعريفَ والخصائصَ الرياضيةَ للمنحنيات الإهليلجيةِ، و تعطـــي خواص الزمرةِ المكونةِ من نقاط المنحني، و تعطي إمكانية تطبيقَها في أنظمة التشفيرِ وتحلّلُ نقاط الضعفَ لهذه الزمرة.

وأثبتت هذه الأطروحة نظرية جديدة يُمْكِنُ أنْ تُساهمَ في تَسهيل العمليةِ الحسابيةِ وتَعطـــي طـــريقةَ لاســـتنتاج بـــان كُلّ نقطة في المنحنى الإهليلجي- عدا النقطة غير المنتهية- هي نقطة مولّدَة، إذا كان رقم رتبة المنحني -عدد نقاطه- اوليا.

أيضاً، تقدمُ هذه الأطروحة أربعة طرق مُقتَرَحة محورة من نظام تشفير الجمال (ElGamal cryptosystem) باســـتخدام المنحنيات الإهليلجية، بالإضافة إلى، تصميم برنامج لتَطبيق عمل هذه الطرقِ المُقتَرَحةِ، وَحساب التعقيدَ الحسابيَ لهذه الطرقِ مقَارنة إلـــى الطرقِ الأصليةِ، مقارنة الوقت التنفيذي لهذه الطرقِ بالطرقِ الأصلية لعِدّة رسائل لَها حجوم مختلفةُ ووجدنا تخفيضا في وقتِ الحسابِ قد نتج.

PDF created with pdfFactory trial version www.pdffactory.com