http://uobabylon.edu.iq/media/press.aspx?mid=49660

دراسة في كلية التربية للعلوم الصرفة تبحث طريقة التحليل الجزئي

بحثت دراسة في كلية التربية للعلوم الصرفة (طريقة التحليل الجزئي المعرفة على منحنيات Koblitz المعرفة على الحقول الثنائية الموسعة)، أعدتها الأستاذ المساعد الدكتورة رومى كريم خضير التدريسية في الكلية. اقترحت الدراسة تطبيق طريقة التحليل الجزئي على نوع أخر من أنواع المنحنيات الاهليجية التي تسمى بمنحنيات Koblitz المعرفة على الحقول الثنائية الموسعة.وبينت الدراسة أن طريقة التحليل الجزئي المعرفة على منحنيات Koblitz سرعت حسابات عملية الضرب، مقارنة مع الحسابات التي طبقت نفس الطريقة على الحقول الاولية Fp، وإن الأعداد k11,k12,k21 and k22 تم تمثيلها بشكل أعداد عقدية تقع ضمن الحلقة Z[?] باستخدام (adic non-adjacent form TNAF-?)، وكذلك endomorphisms عرفت على أنها Frobenious maps ضمن الحلقة Z[?] المغمورة ضمن الحقول التربيعية الخيالية (Q?D) حيث&7? = D . وأعطت الخصائص ضمن هذه الحقول إمكانية الحساب لعملية الضرب على E بدون الحاجة إلى أي عملية مضاعفة, وهذه الخاصية تحديدا اعتبرت فائدة أساسية في تسريع الحساب إلى عملية الضرب العقدي kP .

مرتضى علي