http://uobabylon.edu.iq/media/press.aspx?mid=49638

دراسة في كلية التربية للعلوم الصرفة تبحث التحليل الجزئي لتحسين أنظمة التواقيع

بحثت دراسة في كلية التربية للعلوم الصرفة (طريقة التحليل الجزئي لتحسين أنظمة التواقيع الرقمية الكمال المطبقة على المنحنيات الاهليجية)، أعدتها الأستاذ المساعد الدكتورة رومى كريم خضير. تضمنت الدراسة اقتراح تحسين EEDSA)) من خلال حساب عملية الضرب على المنحنيات الاهليجية، باستخدام طريقة التحليل الجزئي ISD للعدد الصحيح بدلاً من استخدام قوانين الجمع والمضاعفة للمنحني الاهليجي E المعرف على الحقول الأولية Fp.وبينت الطريقة المقترحة خوارزمية (EEDSA-ISD) واستفادت من سرعة الحسابات المتحققة باستخدام طريقة ISD, وتعتمد طريقة EEDSA-ISD)) أيضًا على سرعة حسابات الـ (endomorphism s) المعرفة على المنحنيات الإهليجية E, ومن ناحية أخرى يتم تحديد مستوى الأمنية للخوارزمية المقترحة (ECDSA-ISD) بناء على صعوبة حل مسألة اللوغاريتم المنفصل المعرف على المنحنيات الاهليجية (ECDLP).وأظهرت الدراسة أن الخوارزمية المقترحة (EEDSA-ISD) أسرع وأكثر أمنا لمقاومة هجمات ECDLP)، لذلك فهو أكثر كفاءة مقارنة بنظام EEDSA)) الأصلي.

مرتضى علي