http://uobabylon.edu.iq/media/press.aspx?mid=49499

رسالة ماجستير في كلية التربية للعلوم الصرفة تناقش طريقة التحليل الجزئي لتحسين نظام الكمال

ناقشت رسالة ماجستير في كلية التربية للعلوم الصرفة (طريقة التحليل الجزئي لتحسين نظام الكمال (،nbsp&; للباحثة سارة جبار يعقوب، بإشراف الدكتورة رومى كريم خضر.تضمنت الرسالة دراسة خوارزمية التوقيع الرقمية الكمال المعرفة على المنحنيات الاهليجية&EEDSA) ;nbsp)، التي شكلت اعتمادا على نظام تشفير المفتاح المعلن الكمال (EPKC) وخوارزمية التوقيع الرقمي المعرفة على المنحني الإهليجي .

;nbsp;   &

وألقت الدراسة الضوء بشكل رئيسي على التعقيد الحسابي إلى خوارزميات EEDSA-GLV و EEDSA-ISD، التي تحدد بواسطة حساب الكلفة إلى العمليات، وتتضمن هذه العمليات عمليات المنحنيات الإهليجية وعمليات الحقول المنتهية، وقورنت الطرق المقترحة اعتمادا على أساس التعقيد الحسابي لكل تقنية في عملية دورة واحدة.وأظهرت النتائج التجريبية أن طريقة EEDSA-ISD هي أسرع من طريقة EEDSA-GLV، وعليه فأن طريقة EEDSA-ISD اعتبرت كخوارزمية كفوءة بالمقارنة مع الخوارزمية الأصلية&EEDSA ;nbsp والخوارزمية EEDSA-GLV للاستخدامات التشفيرية.

مرتضى علي