|  |  |
| --- | --- |
| abstract | المستخلص |
| **A proxy blind signature scheme**A proxy blind signature scheme is a special form of blind signature which allows a designated person called proxy signer to sign on behalf of two or more original signers without knowing the content of the message or document. It combines the advantages of proxy signature, blindsignature and multi-signature scheme and satisfies the security properties of both proxy and blind signature scheme. Most of the exiting proxy blind signature schemes were developed based on the mathematical hard problems integer factorization (IFP) and simple discrete logarithm (DLP) which take sub-exponential time to solve. This paper describes an secure simple proxy blind signature scheme based on Elliptic Curve Discrete Logarithm Problem(ECDLP) takes fully-exponential time. This can be implemented in low power and small processor mobile devices such as smart card, PDA etc. Here also we describes implementation issues of various scalar multiplication for ECDLP  | **نظام توقيع وسيط معتمد على خاصية التعمية**يعتبر النظام الوسيط المعتمد على خاصية التعمية شكلاً خاصاً من أنظمة التواقيع العمياء التي تسمح للشخص المخول بالتوقيع والمسمى الموقع الوسيط بأن يوقع بالنيابة عن اثنين أو أكثر من الموقعين الأصليين وبدون الإطلاع على محتوى الرسالة أو الوثيقة. يجمع هذا النظام بين ايجابيات التواقيع الوسيطة ، والتواقيع العمياء، وأنظمة التواقيع المتعددة ويضمن توفر خاصية الأمان لكلاً من أنظمة الوسيط وأنظمة التعمية.لقد تم تطوير أنظمة الوسيط ذات التواقيع العمياء الحالية بالإعتماد على المسائل الرياضية المعقدة والمسماه ب(مسأئل التفكيك إلى جداء عوامل أولية) وعلى (الخوارزميات المتقطعة البسيطة) والتي تأخذ وقتاً تحت أسي لحلها.تقدم هذه الورقة العلمية وصفاً لنظام تعمية وسيط بسيط ويعتمد على (مسألة الخوارزميات المتقطعة ذات المنحى البيضاوي) التي يأخذ وقتاً أسياً كاملا.يمكن تنفيذ هذا النظام على أجهزة الموبايل صغيرة المعالج ومنخفضة الطاقة مثل البطاقات الذكية والمساعدات الكفية. وسنقوم أيضا بوصف تنفيذ عملية الضرب غير الموجهة لـ(مسألة التفكيك إلى جداء عوامل أولية ذات المنحنى البيضاوي). |