ABSTRACT
Since Taiwan entered into the World Trade Organization in 2002, government procurement issues are in the spotlight around the world. As we know, there were many problems under the government procurement operations before, such as the difficulty of obtaining the procurement information, the complicated procurement process, the inconvenience of the bidding, the corruption of personal procurement, etc. If the government procurement operations can be done through the Internet, then it can not only save huge manpower, but also prevent personal corruption. Therefore, online government procurement can greatly improve our government image. As the Internet is a public environment, the security of the procurement information is very important to us. If we cannot take some security schemes to protect the procurement information, people can change or delete data easily and further influence the fairness of procurement. Thus, in this thesis we adopt Elliptic Curve Cryptosystems that can use few bits to reach the same security level as other public key cryptosystems, and also get a better efficiency during message transmission. On the other hand, using self-certified public key cryptosystems can verify efficiently the validity of public keys. Hence, in this thesis we first combine Elliptic Curve Cryptosystems with self-certified public key cryptosystems to develop a mutual authentication scheme, signcryption scheme, multi-signcryption scheme, blind signature scheme and fair document exchange scheme. Then, in the procedure of electronic procurement we can increase the security level, reduce the storage cost, and improve the efficiency of data transmission based on the schemes proposed above. Additionally, this thesis is to concentrate the study on the validity of bid bond and electronic contracting which had never been discussed before. The government organizations and bidders can process all procurement procedure by employing our proposed schemes to implement a complete electronic system. Therefore, this thesis is to provide a secure and efficient environment of government procurement.

Keywords: Elliptic Curve Cryptosystems, Self-certified Public key System, Information Security, Sealed-bid in Network, Government Procurement Law.
3.1.5 盲簽章機制
3.1.6 公平文件交換機制

3.2 領標階段

3.3 投標階段

3.4 開標階段

3.5 簽約階段

第四章 安全性及效能分析

4.1 安全性分析

4.1.1 系統建置階段

4.1.1.1 註冊機制

4.1.1.2 双向認證機制

4.1.1.3 簽章加密機制

4.1.1.4 多重簽章加密機制

4.1.1.5 盲簽章機制

4.1.1.6 公平文件交換機制

4.1.2 領標階段

4.1.3 投標階段

4.1.4 開標階段

4.1.5 簽約階段

4.2 效能分析

4.2.1 計算複雜度

4.2.2 通訊傳輸量

4.3 討論

第五章 結論

第六章 參考文獻

作者簡介


