Abstract

Reham M. Mahmoud Kouta

A NEW REMOTE SECURE E- VOTING MODEL BASED ON BLIND SIGNATURE

Electronic voting is an emerging social application of cryptographic protocols. A vast amount of literature on electronic voting has been developed over the last two decades. Voting is one of the most important activities in a democratic society. In a traditional voting environment voting process sometimes becomes quite inconvenient due to the reluctance of certain voters to visit a polling booth to cast votes besides involving huge social and human resources. The development of computer networks and elaboration of cryptographic techniques facilitate the implementation of electronic voting. In this work we propose a secure electronic voting protocol that is suitable for large scale voting over the Internet. Electronic voting can increase security of voter and ballot and increase the participation in the election. This thesis aimed to propose new e-voting model that achieves the security requirements which are authentication, privacy, integrity and non-reputation. The e-voting model is based on blind signatures and has the properties of eligibility, mobility, uniqueness, robustness, correctness, universal Verifiability, privacy, flexibility, individual verifiability, Receipt-Freeness and Walk-away. The model depends on these main entities that are involved within the voting processes voters registration, voting, counting, audit), these entities are: certificate authority, ministry of interior, voter, high committee of elections (administrator) and counter. The voter can vote from any remote where with secured data transfer (ballot) by using the blind signature to blinded ballot and then sign and encrypt it, when it sent to the high committee of elections (administrator) for checking the voter eligibility, there is encrypting random value r that attached with the blind ballot, using for removing blind the ballot which is encrypted by counter's public key. The high committee of elections checks the signature of voter and checks that if he is eligible voter not. Then remove the voter's digital signature and put his digital signature and then sends to counter party. The counter party checks the signature of high committee of election and extracts the random value r by decrypting with his private key and removing blind the ballot and counts the vote. This thesis compares the proposed model against two other models that are more effective for large scale voting over the internet and explain in details how this model is the best whether in the performance and in the properties of e-voting. Also the authors of the model development the model and show in step by step the voting process. The voter creates his key pair, issues his digital certificate from certificate authority, cast the vote and sends to the administrator. The administrator checks the voter and sends to the counter. The counter un-blinds the ballot and counts the vote.