Kabarak University International Conference on Emerging Trends and Issues in Education

Contribution ID: **41** Type: **Research Paper**

Advances in Democracy

Abstract– Democracy is founded on the principle of elections and opinion expression capabilities. Voting is an information transfer model that requires public audit and significant amount of secrecy but cannot be transferred through trust. A cryptographic voting scheme with secure protocols is an alternative measure that can offer provable security with stronger audit trail. Trust in the correct functioning of the electronic voting system is the key to democracy. Identification and verification of voters lie in the design to accurately detect fraud and audit elections. Practical implementation on a bulletin board in a secure way is feasible provided certain deficiencies like accuracy (correctness), information theoretic privacy, universal verifiability, incoercibility (receipt-freeness) and tally is addressed using cryptographic techniques. One time signature schemes ensure one man, one vote principle that can be converted to non-interactive proofs via zero knowledge proofs in identifying voters using bit commitments for distributed computation after casting votes have been exploited to achieve this objective. In this paper, real time tabulation of results in associated race has been achieved. Simulated interfaces are in the appendix section.

Primary author: Mr ACHOLA, Daniel (Kabarak)

Session Classification: Application of Emerging Innovations and Technologies in Education:

Track Classification: Application of Emerging Innovations and Technologies in Education