An E-voting Protocol Using Elliptic Curve Cryptosystem

Hamed Mousavi

March 29, 2019

Abstract

One of the most important methods of remote e-voting is based on the ElGamal homomorphic cryptosystems. These systems are secure enough provided that the discrete logarithm problem is secure. We begin this talk by mentioning the general properties of these protocols as well as proposing one of their main challenges, which is the limitation on number of voters. Finally we briefly explain how we can address this limitation by designing parallel voting subprotocols. Simulations show that the number of covering voters in this protocol is 10 times more than that of the original one. In the meanwhile, the necessary memory space is reasonable, the communication complexity is of standard level and the security is acceptable.