Topic :DEVELOPING AND MODELING A NEW E-LOTTERY SYSTEM USING ANONYMOUS SIGNATURES

Abstract: In traditional lottery systems, the players choose some numbers on a ticket, enroll it to the lottery organizer and pay an amount of money for it. But this perspective offers no guarantee to the players that the lottery organizer doesn’t manipulate the number selection in order to pay the least. This suspicion could be avoided if the lottery organizer didn’t know the numbers selected by the players before the draw. Such a system is possible to be realized by using anonymous signatures, but the design should also guarantee that forging lottery tickets after the moment of the draw or claim of a different ticket is not possible. This paper will propose and analyze a model in order to fulfill all requirement described before, using several cryptographic primitives