Abstract

Identity Cards or Kartu Tanda Penduduk (KTP) are essential for Indonesian people. KTP contains personal information, such as National Identity Number (NIK), Name, Address, Gender, etc. Since KTP has essential data and is still printed conventionally, there is a vulnerability if the KTP is lost, and the owner's data is disclosed so that if an irresponsible person finds it, the data can be used for impersonating the owner. In the previous method proposed by Haque et al., [1], the data was stored in a QR Code. However, there was no verification method to legitimize the original owner, and the system did not have a login feature. To overcome the weakness of Haque et al., method [1], the owner's NIK is encrypted using the Elliptic Curve El-Gamal (ECEG) and further signed using ECDSA by the owners before storing it in the QR Code. For obtaining the owner's data in the database, the verification process should be done after the QR Code is scanned. Using the proposed method, the probability of success for a guessing attack is 1 / (*n* - 1). Meanwhile, the probability of success for an impersonation attack is 1 / (*q1 * q2 * l*).

Keywords: qr code, card identity, KTP, ECDSA, elliptic curve el-gamal