Digital Signature Scheme

A. Ebrahimi, S. Shirmardi

September 23, 2021

1 Introduction

In cryptography, the Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography. ECDSA is a cryptographic algorithm to ensure that funds can only be spent by their rightful owners. It is dependent on the curve order and hash function used.

2 Scheme details

Let I and O be the inputs and outputs of an arbitrary transaction, Tr, respectively. The function D concatanates these variables and is used in the signature scheme:

$$D(Tr) = I + O$$

Suppose that H is an arbitrary hashing function (it can also be a combination of multiple hashing functions). In this scheme, the hash of $D(Tr)$ is calculated and used:

$$h = H(D(Tr))$$

Let $Sign$ be the signing function of the curve. Suppose that PR_k is the private key of the transaction owner. The signing process is done using PR_k and h.

$$signature = Sign\ (PR_k, h)$$