Abstract

COMPUTER IMPLEMENTED SYSTEM AND METHOD FOR DISTRIBUTING SHARES OF DIGITALLY SIGNED DATA

A computer-implemented method of distributing a shared secret, such as a transaction on the Bitcoin blockchain among a plurality of participants is disclosed. The method comprise a mapping step wherein a plurality of inputs to the mapping step are mapped to respective elliptic curve points of an elliptic curve of an elliptic curve cryptography system common to the participants. In a first encryption step, a plurality of said elliptic curve points are encrypted by means of a public key of a public-private key pair of the elliptic curve cryptography system to provide an output adapted to be decrypted by means of the corresponding private key of the public-private key pair, and in a second encryption step wherein a plurality of parts of at least one input to said second encryption step are multiplied by respective terms of a series known to said participants. In a secret sharing step a plurality of shares of an input to said secret sharing step are distributed to a plurality of said participants such that said input is accessible to a threshold number of said shares and is inaccessible to less than said threshold number of said shares.

Figure 1