

ABSTRACT

SYSTEM AND METHOD FOR INFORMATION PROTECTION

A computer-implemented method for information protection comprises: committing a transaction amount of a transaction with a first commitment scheme to obtain a transaction commitment value, committing a change of the transaction with a second commitment scheme to obtain a change commitment value, the first commitment scheme comprising a transaction blinding factor, and the second commitment scheme comprising a change blinding factor; encrypting a first combination of the change blinding factor and the change with a first key; transmitting the transaction blinding factor, the transaction amount, and the transaction commitment value to a recipient node associated with a recipient for the recipient node to verify the transaction; in response to that the recipient successfully verifies the transaction, obtaining an encrypted second combination of the transaction blinding factor and the transaction amount encrypted with a second key.

FIG. 3