

ABSTRACT

SYSTEM AND METHOD FOR INFORMATION PROTECTION

A computer-implemented method comprises: committing a transaction amount t of a transaction with a commitment scheme to obtain a transaction commitment value T , the commitment scheme comprising at least a transaction blinding factor r_t ; encrypting a combination of the transaction blinding factor r_t and the transaction amount t with a public key PK_B of a recipient of the transaction; and transmitting the transaction commitment value T and the encrypted combination to a recipient node associated with the recipient for the recipient node to verify the transaction.

FIG. 3A