ABSTRACT OF THE DISCLOSURE

Systems, methods, and computing device readable media for implementing fast oblivious transfer between two computing devices may improve data security and computational efficiency. The various aspects may use random oracles with or without key agreements to improve the security of oblivious transfer key exchanges. Some techniques may include public/private key strategies for oblivious transfer, while other techniques may use key agreements to achieve simultaneous and efficient cryptographic key exchange.

FIG. 2