

ABSTRACT OF THE DISCLOSURE
MESSAGE TRANSMITTING SYSTEM WITH HARDWARE
SECURITY MODULE

In a message transmitting system, a first user device installed therein a hardware security module and a second user device are in communication with a message exchange center. The first user device generates a first public-private key pair including a first private key only stored in the hardware security module, and a first public key sent to the message exchange center. The second user device establishes a shared key, uses the shared key to encrypt a message, and transmits the encrypted message to the first user device via the message exchange center. The hardware security module uses a specific information to derive the shared key, and uses the shared key to recover the message.

[FIG 1]