

Abstract

Each of a transmitter (1) and a receiver (2) divides temporarily-shared data into one or more purification blocks and one or more disposable blocks, and mixes each purification
5 block so as to enlarge a Hamming distance between corresponding purification blocks being held by the transmitter (1) and the receiver (2) by using a Hamming distance amplification effect. The transmitter (1) Vernam-encrypts the mixed data with the disposable data and transmits the mixed data to the receiver
10 (2), and the receiver (2) decrypts the received Vernam-encrypted data by using a disposable block owned thereby, and compares the Hamming distance between the purification block owned thereby with the mixed data with a predetermined value so as to judge whether each purification block can be
15 shared between the transmitter (1) and the receiver (2).



162162



G00002