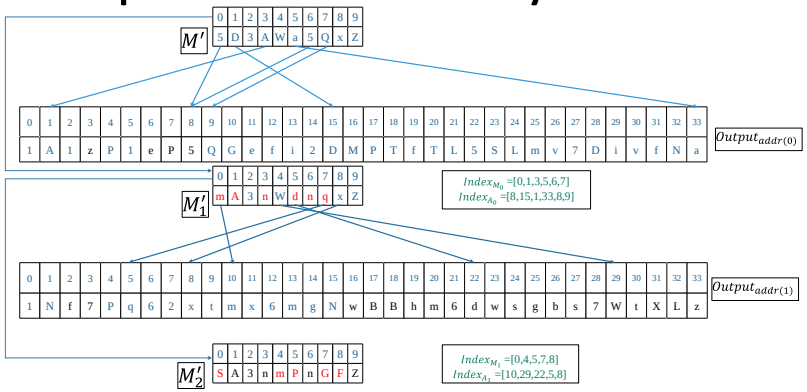
A Blockchain-Oriented Covert Communication Technology With Controlled Security Level Based on Addressing Confusion Ciphertext

Lejun ZHANG, Bo ZHANG, Ran GUO, Zhujun WANG, Guopeng WANG, Jing QIU, Shen SU, Yuan LIU, Guangxia XU, Zhihong TIAN, Sergey Gataullin

Frontiers of Computer Science, DOI: 10.1007/s01704-024-2775-2

Problems & Ideas

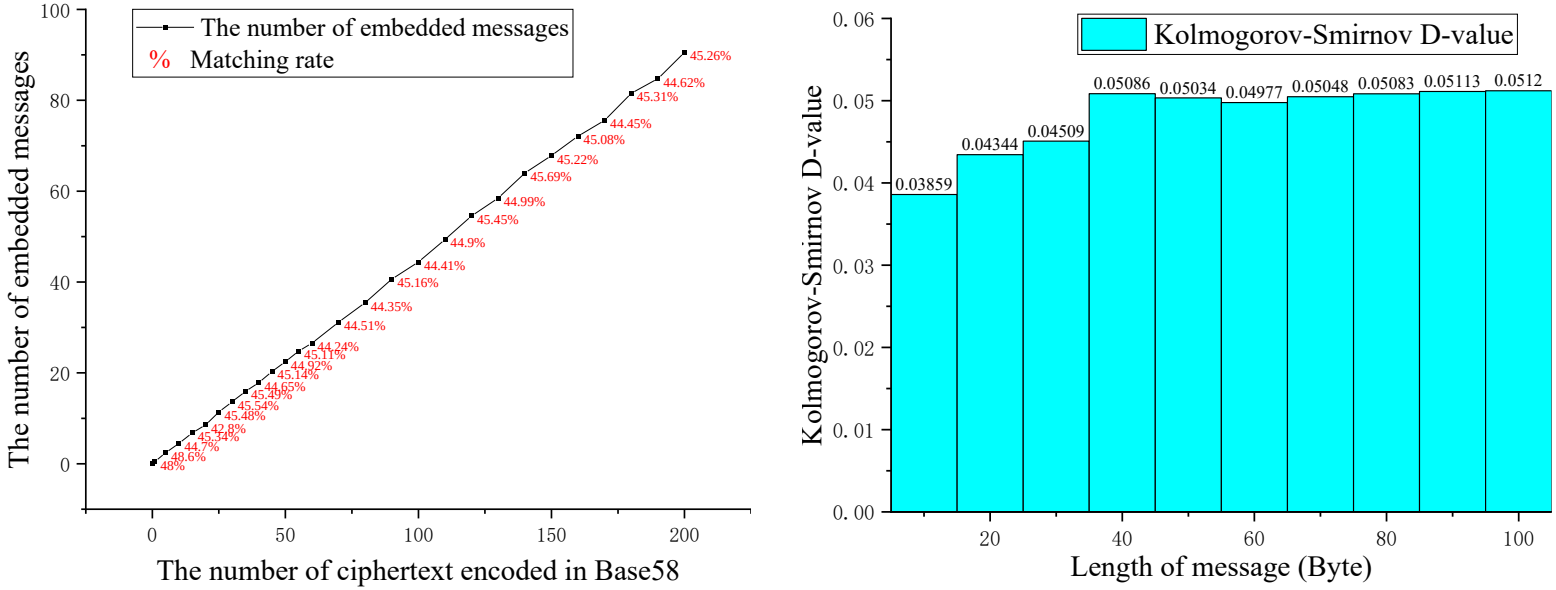
- Problems with using blockchain to achieve covert communication:
  - Some research has utilized the storage fields of blockchain transactions to hide information, which is efficient to transmit, but security is harder to control and relationships are vulnerable to exposure.
  - Some research has utilized addresses and amounts in blockchain transactions to hide information. While this method is highly secure, it is less efficient in transmission.
- Ideas: A combination of address and storage field covert communication improves security through address confusion, and field transfer improves efficiency.



In the example, if the ciphertext does not reach the set number of confusion rounds s, it will continue to be confused with the new address. The confusion process is done by iterating through each character in the address and comparing it with the character at the same position in the ciphertext. If a match is found, the corresponding character in the ciphertext is replaced with a randomly generated Base58 encoded character. After s rounds of confusion, the address index set, the ciphertext index set and the confused ciphertext m are obtained.

Main Contributions

- Contributions:
  - A controlled security level covert communication scheme (CSLCCB) where the sender sets the security level of the message transmission by controlling the number of output addresses in the transaction;
  - A novel ciphertext confusion scheme that embeds ciphertext characters in addresses and replaces the embedded locations with characters to improve the security of communication;
  - A method for chaining the generation of addresses of the parties to a transaction to facilitate the reduction of hidden information.



Left: Matching rate of ciphertext messages; Right: D-value of KS test for different lengths of ciphertext.