

ABSTRACT

Present application discloses ciphertext database query method and system based on searchable encryption. Plaintext source data, wherein said data comprises data file names and data content, is acquired; keyword is extracted from the data content obtaining a keyword list, a ciphertext index library is obtained based on an index generation key according to data file name, and ciphertext data content and ciphertext index library are stored into a ciphertext database correspondingly; a target query keyword is acquired, and processed through a trapdoor generation key generating a query ciphertext; ciphertext index library is queried based on query ciphertext obtaining a ciphertext query result and corresponding ciphertext data content; ciphertext data content is decrypted based on data decryption key obtaining a plaintext data content. The algorithms are designed with symmetric cryptographic primitives, which ensures efficiency of algorithm execution; and inverted index technology is adopted with keywords as key values, improving search efficiency.

Fig. 1