**Dual-Server Public-Key Authenticated Encryption with Keyword Search**

**ABSTRACT**

—In cloud storage, how to search sensitive data efficiently and securely is a challenging problem. The searchable encryption technique provides a secure storage method without loss of data confidentiality and usability. As an important branch of searchable encryption, public-key encryption with keyword search (PEKS) is widely studied by scholars. However, most of the traditional PEKS schemes are vulnerable to the inside keyword guessing attack (IKGA). Resisting the inside keyword guessing attack is likely to become an essential property of all new PEKS schemes. For a long time, mitigating IKGA has been inefficient and difficult, and most existing PEKS schemes fail in achieving their security goals. To address the above problems, we define the notion of Dual-server Public-key Authenticated Encryption with Keyword Search (DPAEKS), which protects against IKGA by leveraging two servers that do not cooperate, and supports the authentication property. Then, we provide a construction of DPAEKS without bilinear pairings. Experimental results obtained using a real-world dataset show that our scheme is highly efficient and provides strong security, making it suitable for deployment in practical applications.