Abstract

Suppose a database containing M records is replicated across N servers, and a user wants to privately retrieve one record by accessing the servers such that identity of the retrieved record is secret against any up to T servers. A scheme designed for this purpose is called a T-private information retrieval (T-PIR) scheme. In this work, we design a linear capacity-achieving T-PIR scheme with sub-packetization dn^{M-1} over a finite field GF(q), q>=N. The sub-packetization dn^{M-1}, where d=gcd(N,T) and n=N/d, has been proved to be optimal in our previous work. The field size of all existing capacity-achieving T-PIR schemes must be larger than Nt^{M-2} where t=T/d, while our scheme reduces the field size by an exponential factor.