

ABSTRACT

PROBABILISTIC ENCRYPTION METHOD FOR QUERYING DATABASE

A method for querying a database is described comprising the steps: composing a composite group having a first subgroup, a second subgroup and a third subgroup, each subgroup having a plurality of elements, producing an encrypted data record value by mapping a data record value to a first element of the first subgroup and mapping a first random factor to an element of the second subgroup, producing an encrypted query value by mapping a query value to a second element of the first subgroup and mapping a second random factor to an element of the third subgroup, and performing a matching operation wherein the element of the second subgroup from the encrypted data record value is removed, and element of the third subgroup from the encrypted query value is removed to obtain a function which contains a random multiple of the difference between the data record value and the query value, and using the public key to identify when the data record value is equal to the query value in the function.

[Figure 1]