Abstract of the Disclosure

PRIVATE RETRIEVAL OF DIGITAL OBJECTS

A database (104) maintains one or more groups (106) of digital objects (202). A user (102) wishes to retrieve one or more digital objects (202) from the database (104), without the database (104) being able to determine which particular digital objects (202) have been retrieved. In addition, the database (104) should not allow the user (102) to retrieve any digital objects (202) to which the user (102) has not been granted access. The user (102) requests the groups (106) containing the digital objects (202) the user (102) wishes to download, but does not identify the digital objects (202) within each group (106) that the user (102) is interested in. Using a symmetric key cryptosystem, the database (104) generates a key (204) for and encrypts each digital object (202) in the requested group (106) into ciphertext (206), and additionally encrypts each key (204). The database (104) transmits the ciphertexts (206) and encrypted keys (208) to the user (102). The user (102) identifies the keys (208) associated with the digital objects (202) of interest, and further encrypts the keys (208), returning the changed keys (506) to the database (104). The database (104) reverses its encryption of the keys (506), and transmits the partially decrypted keys (510) back to the user (102). The user (102) then applies the user's (102) own decryption algorithm to the keys (510), and then uses the decrypted keys (204) to decrypt the digital objects (202) of interest.

Figure 3.