

2 receiving a request to update the decrypted data with new data;
3 sending the new data to an encryption engine;
4 receiving, from the encryption engine, an encrypted new data; and
5 replacing the encrypted data with the encrypted new data.

1 6. The method of claim 1, further comprising:

2 searching at least one second table of the computer database system
3 using at least one second search string to identify at least one second matching
4 string, wherein the second table includes a second encrypted foreign key for each
5 field;

6 obtaining at least one second encrypted foreign key corresponding to
7 the second matching string identified using the second search string;

8 sending the at least one second encrypted foreign key to the
9 decryption engine; and

10 receiving, from the decryption engine, at least one second decrypted
11 foreign key corresponding to the at least one second encrypted foreign key, wherein
12 searching a second table of the computer database system comprises identifying
13 encrypted data for which the at least one decrypted foreign key matches the at least
14 one second decrypted foreign key.

1 7. The method of claim 1, wherein the first table of the computer

2 database system comprises a first column of encrypted foreign keys and a second
3 column of plaintext data, wherein searching the first table of the computer database
4 system using the search string to identify the matching string comprises searching
5 the column of plaintext data for one or more values that match the search string, and
6 wherein the at least one encrypted foreign key includes an encrypted foreign key for
7 each of the one or more values that match the search string.

1 8. A system comprising:

2 one or more processors and

3 a memory including instructions that, when executed by the one or
4 more processors, cause the one or more processors to:

5 receive a query that includes an indication of at least one search
6 column of a source table and a search string;
7 identify at least one searchable table based on the at least one
8 search column;
9 identify a set of encrypted identifiers in the at least one
10 searchable table associated with the search string, each of the set of
11 encrypted identifiers being associated with a value in the searchable table that
12 matches the search string;
13 generate a set of decrypted identifiers from the set of encrypted
14 identifiers;
15 identify a set of encrypted source data in the source table based
16 at least in part on the set of decrypted identifiers; and
17 generate a decrypted set of source data by decrypting each of
18 the encrypted source data in the set of encrypted source data; and
19 return the decrypted set of source data.

1 9. The system of claim 8, wherein the at least one searchable table
2 is identified from a plurality of searchable tables based on the at least one search
3 column indicated in the query, and wherein each searchable table of the plurality of
4 searchable tables is associated with a different search column.

1 10. The system of claim 8, wherein the set of encrypted identifiers is
2 decrypted using a decryption key associated with the at least one searchable table.

1 11. The system of claim 8, wherein the query is included in an
2 update request that includes new data, and wherein the instructions further cause
3 the one or more processors to:

4 update the decrypted set of source data to include the new data;
5 encrypt the updated set of source data; and
6 replace the set of encrypted source data with the encrypted updated
7 set of source data in the source table.