CLAIMS

1. A server computer system configured to engage in domain name service (DNS) transactions with a plurality of clients, the server computer system characterized by having at least one hardware processor configured to:

receive a private query from a client of the plurality of clients, the private query comprising an encryption of a hash index, the hash index indicative of a location of a record within a domain name database, the hash index encrypted according to a homomorphic encryption procedure, and wherein the hash index is determined according to a domain name;

in response to receiving the private query, perform an encrypted lookup into the domain name database according to the encrypted hash index, the encrypted lookup producing an encryption of the record without decrypting the hash index; and

transmit a private reply comprising the encryption of the record to the client.

2. The server computer system of claim 1, wherein the record comprises an internet protocol (IP) address.

3. The server computer system of claim 1, wherein the record comprises a security indicator indicative of whether accessing a domain represented by the domain name exposes a user to a computer security threat.

4. The server computer system of claim 1, further characterized by:

having the private query further comprise a version indicator indicative of a hash function used in calculating the hash index; and

having the at least one hardware processor further configured to, in response to receiving the private query, determine according to the version indicator whether the domain name database is currently indexed according to the hash function, and if not, transmit an error message to the client.

5. The server computer system of claim 1, further characterized by having the private query include a plurality of encrypted hash indices including the encrypted hash index, each of the encrypted hash indices computed according to the domain name by an application of a

distinct hash function and indicating an alternative location of the record within the domain name database.

6. A computer-implemented method of engaging in domain name service (DNS) transactions with a plurality of clients, the method characterized by having at least one hardware processor of a server computer system configured to:

receive a private query from a client of the plurality of clients, the private query comprising an encryption of a hash index, the hash index indicative of a location of a record within a domain name database, the hash index encrypted according to a homomorphic encryption procedure, and wherein the hash index is determined according to a domain name;

in response to receiving the private query, perform an encrypted lookup into the domain name database according to the encrypted hash index, the encrypted lookup producing an encryption of the record without decrypting the hash index; and

transmit a private reply comprising the encryption of the record to the client.

7. The method of claim 6, wherein the record comprises an internet protocol (IP) address.

8. The method of claim 6, wherein the record comprises a security indicator indicative of whether accessing a domain represented by the domain name exposes a user to a computer security threat.

9. The method of claim 6, further characterized by:

having the private query further comprise a version indicator indicative of a hash function used in calculating the hash index; and

having the at least one hardware processor further configured to, in response to receiving the private query, determine according to the version indicator whether the domain name database is currently indexed according to the hash function, and if not, transmit an error message to the client.

10. The method of claim 6, further characterized by having the private query include a plurality of encrypted hash indices including the encrypted hash index, each of the encrypted hash indices computed according to the domain name by an application of a

distinct hash function and indicating an alternative location of the record within the domain name database.

11. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a server computer system, cause the server computer system to engage in domain name service (DNS) transactions with a plurality of clients, the computer-readable medium characterized by storing instructions causing the server computer system to:

receive a private query from a client of the plurality of clients, the private query comprising an encryption of a hash index, the hash index indicative of a location of a record within a domain name database, the hash index encrypted according to a homomorphic encryption procedure, and wherein the hash index is determined according to a domain name; in response to receiving the private query, perform an encrypted lookup into the domain name database according to the encrypted hash index, the encrypted lookup producing an encryption of the record without decrypting the hash index; and

transmit a private reply comprising the encryption of the record to the client.