CLAIMS

1. A homomorphic encryption method using at least one processor, the homomorphic encryption method comprising:

receiving an input data; and

homomorphically encrypting the input data to obtain a homomorphically encrypted data, including multiplying a first polynomial and a second polynomial associated with the input data,

wherein said multiplying comprises:

providing a prime number p;

determining a first discrete Galois transform based on the first polynomial and the prime number;

determining a second discrete Galois transform based on the second polynomial and the prime number;

determining a point-wise product of the first discrete Galois transform and the second discrete Galois transform;

determining an inverse discrete Galois transform based on the point-wise product; and

determining a polynomial product of the first polynomial and the second polynomial based on the inverse discrete Galois transform.

2. The homomorphic encryption method of claim 1,

wherein said multiplying is performed in $\mathbb{Z}_q/\langle x^n + 1\rangle$, where $n = 2^k$ and $k \in \mathbb{Z}$.

3. The homomorphic encryption method of claim 1,

wherein p is a prime number for which p ≡ 3 (mod 4).

4. The homomorphic encryption method of claim 1,

wherein p is a prime number for which p ≡ 1 (mod 4).

5. The homomorphic encryption method of claim 1, further comprising:

determining a folding of the first polynomial;

determining a folding of the second polynomial,

wherein the first discrete Galois transform is determined based on the folding of the first polynomial, and

wherein the second discrete Galois transform is determined based on the folding of the second polynomial.

6. The homomorphic encryption method of claim 5, further comprising:

determining a twist of the folding of the first polynomial based on the prime number;

determining a twist of the folding of the second polynomial based on the prime number,

wherein the first discrete Galois transform is determined based on the twist of the folding of the first polynomial, and

wherein the second discrete Galois transform is determined based on the twist of the folding of the second polynomial.

7. The homomorphic encryption method of claim 1, further comprising:

removing twisting from the point-wise product after the inverse discrete Galois transform.

8. The homomorphic encryption method of claim 7, further comprising:

unfolding the point-wise product after the inverse discrete Galois transform with the twisting removed.

9. The homomorphic encryption method of claim 1, further comprising:

determining a Galois field $GF(p^2)$ based on the prime number p.

10. The homomorphic encryption method of claim 9, further comprising:

determining a plurality of roots in the Galois field (p^2),

wherein the first discrete Galois transform and the second discrete Galois transform are determined based on the plurality of roots.

11. The homomorphic encryption method of claim 10,

wherein the plurality of roots comprise a root of unity and a root of an imaginary unit.

12. The homomorphic encryption method of claim 10,

wherein the plurality of roots comprise an n/2-th primitive root of unity and an n/2-th primitive root of an imaginary unit.

13. A non-transitory computer-readable medium, comprising instructions which, when executed by a processor, make the processor perform a homomorphic encryption method comprising:

receiving an input data; and

homomorphically encrypting the input data to obtain a homomorphically encrypted data, including multiplying a first polynomial and a second polynomial associated with the input data,

wherein said multiplying comprises:

providing a prime number p;

determining a first discrete Galois transform based on the first polynomial and the prime number;

determining a second discrete Galois transform based on the second polynomial and the prime number;

determining a point-wise product of the first discrete Galois transform and the second discrete Galois transform;

determining an inverse discrete Galois transform based on the point-wise product; and

determining a polynomial product of the first polynomial and the second polynomial based on the inverse discrete Galois transform.

14. A homomorphic encryption device comprising:

a memory; and

at least one processor communicatively coupled to the memory and configured to:

receive an input data; and

homomorphically encrypt the input data to obtain a homomorphically encrypted data, including multiplying a first polynomial and a second polynomial associated with the input data,

wherein said multiplying comprises:

providing a prime number p;

determining a first discrete Galois transform based on the first polynomial and the prime number;

determining a second discrete Galois transform based on the second polynomial and the prime number;

determining a point-wise product of the first discrete Galois transform and the second discrete Galois transform;

determining an inverse discrete Galois transform based on the point-wise product; and

determining a polynomial product of the first polynomial and the second polynomial based on the inverse discrete Galois transform.

15. The homomorphic encryption device of claim 14,

wherein p is a prime number for which for which $p \equiv 3 \pmod 4$.

16. The homomorphic encryption device of claim 14, wherein said multiplying further comprises:

determining a folding of the first polynomial and a folding of the second polynomial,

wherein said determining the first discrete Galois transform is based on the folding of the first polynomial, and

wherein said determining the second discrete Galois transform is based on the folding of the second polynomial.

17. The homomorphic encryption device of claim 16, wherein said multiplying further comprises:

determining a twist of the folding of the first polynomial based on the prime number and a twist of the folding of the second polynomial based on the prime number,

wherein said determining the first discrete Galois transform is based on the twist of the folding of the first polynomial, and

wherein said determining the second discrete Galois transform is based on the twist of the folding of the second polynomial.

18. The homomorphic encryption device of claim 14, wherein said multiplying further comprises:

removing twisting from the point-wise product after the inverse discrete Galois transform.

19. The homomorphic encryption device of claim 18, wherein said multiplying further comprises:

unfolding the point-wise product after the inverse discrete Galois transform with the twisting removed.

20. The homomorphic encryption device of claim 19, wherein said multiplying further comprises:

determining a plurality of roots in a Galois field (p^2);

wherein the first discrete Galois transform and the second discrete Galois transform are determined based on the plurality of roots.