CLAIMS

1. An encryption method comprising:

receiving at least one plain text;

converting the at least one plain text to at least one pre-encryption integer (M_1,…,M_n);

using the at least one pre-encryption integer (M_1,…,M_n) and at least one variable solution set (v_1,…,v_n) derived from at least one symmetric key, generating at least one Diophantine equation solvable by the at least one variable solution set (v_1,…,v_n), including:

using a first subset of the at least one variable solution set (v_1,…,v_n), generating at least one initial Diophantine equation; and

using a concealment variable derived from a second subset of the at least one variable solution set (v_1,…,v_n), modifying the at least one initial Diophantine equation to generate the at least one Diophantine equation;

predicting, using a trained AI model, insolvability or solvability of the at least one Diophantine equation; and

providing the at least one Diophantine equation as at least one cipher text if the at least one Diophantine equation is predicted, by the trained AI model, as insolvable.

2. The encryption method of claim 1, further comprising:

providing at least one replacement Diophantine equation and a subset of the at least one Diophantine equation as a cipher text if any one of the at least one Diophantine equation, which is other than the subset of the at least one Diophantine equation, is predicted as solvable by the trained AI model and if the at least one replacement Diophantine equation is predicted as insolvable by the trained AI model, including:

generating the at least one replacement Diophantine equation, and

predicting, using the trained AI model, insolvability or solvability of the at least one replacement Diophantine equation.

3. The encryption method of any one of claim 1 to claim 2, further comprising:

using the at least one variable solution set (v_1,…,v_n), generating at least one faux Diophantine equation; and

ascertaining a solution of the at least one faux Diophantine equation as a non-integer,

wherein predicting, using the trained AI model, insolvability or solvability of the at least one Diophantine equation includes:

predicting, using the trained AI model, insolvability or solvability of the at least one faux Diophantine equation,

wherein providing the at least one Diophantine equation as the at least one cipher text if the at least one Diophantine equation is predicted, by the trained AI model, as insolvable includes:

providing the at least one faux Diophantine equation as a faux cipher text of the at least one cipher text if the at least one faux Diophantine equation is predicted, by the trained AI model, as insolvable.

4. The encryption method of any one of claim 1 to claim 3, wherein each variable of the at least one variable solution set is further derived from a cipher text dependent variable.

5. The encryption method of claim 4, wherein the cipher text dependent variable is based on a coefficient of a variable in a Diophantine equation of a previous cipher text, wherein the variable in the Diophantine equation of the previous cipher text includes a polynomial degree based on a previous cipher text dependent variable.

6. The encryption method of claim 1, wherein using the concealment variable derived from the second subset of the at least one variable solution set ($v_1,\ldots,v_n$), modifying the at least one initial Diophantine equation to generate the at least one Diophantine equation includes:

performing addition, subtraction, multiplication, and/or division on the at least one initial Diophantine equation with the concealment variable.

7. The encryption method of any one of claim 1 to claim 6,

wherein using the at least one pre-encryption integer ($M_1,\ldots,M_n$) and at least one variable solution set ($v_1,\ldots,v_n$) derived from at least one symmetric key, generating at least one Diophantine equation solvable by the at least one variable solution set ($v_1, \ldots,v_n$) includes:

using a plurality of relatively prime integers, partitioning the at least one pre-encryption integer (M_1,…,M_n) into a plurality of partitioned integers; and

using the partitioned integers, generating a plurality of Diophantine equations of the at least one Diophantine equation, wherein a count of the relatively prime integers, a count of the partitioned integers, and a count of the Diophantine equations are equivalent.

8. The encryption method of claim 7, wherein partitioning the at least one pre-encryption integer (M_1,…,M_n) into the partitioned integers includes:

performing a plurality of modulo operations using the at least one pre-encryption integer (M_1,…,M_n) and the relatively prime integers being a plurality of divisors, and deriving therefrom the partitioned integers being a plurality of remainders.

9. An encryption apparatus comprising:

at least one memory unit for storing computer-executable instructions; and

at least one processor communicably coupled to the at least memory unit and configured to: execute the computer-executable instructions to perform the method according to any one of claim 1 to claim 8.

10. A non-transitory, computer readable medium comprising computer-executable instructions configured to direct at least one computer processor to perform the method according to any one of claim 1 to claim 8.

11. An encryption apparatus comprising:

a plain text input unit configured to receive at least one plain text;

a symmetric key input unit configured to receive at least one symmetric key;

a plain text to integer unit communicably coupled to the plain text input unit and configured to: receive the at least one plain text from the plain text input unit and convert the at least one plain text to at least one pre-encryption integer (M_1,…,M_n);

a polynomial generation unit communicably coupled to the symmetric key unit and configured to: receive the at least one symmetric key from the symmetric key unit and derive at least one variable solution set (v_1,…,v_n) using the at least one symmetric key;

an encryption unit communicably coupled to the plain text to integer unit, the polynomial generation unit, wherein the encryption unit is configured to: receive the at least one variable solution set ($v_1,\ldots,v_n$) from the polynomial generation unit, and generate at least one Diophantine equation solvable by the at least one variable solution set ($v_1,\ldots,v_n$) using the at least one pre-encryption integer ($M_1,\ldots,M_n$) and the at least one variable solution set ($v_1,\ldots,v_n$) by being configured to: generate at least one initial Diophantine equation using a first subset of the at least one variable solution set ($v_1,\ldots,v_n$), and modify the at least one initial Diophantine equation using a concealment variable which is derived from a second subset of the at least one variable solution set ($v_1,\ldots,v_n$); and

an AI unit communicably coupled to the encryption unit and configured to: receive the at least one Diophantine equation, the AI unit having a trained AI model configured to: predict insolvability or solvability of the at least one Diophantine equation,

wherein the encryption unit is further communicably coupled to a cipher text output unit and configured to: provide the at least one Diophantine equation as at least one cipher text to the cipher text output unit if the at least one Diophantine equation is predicted as insolvable by the AI model.

12. The encryption apparatus of claim 11, wherein

the encryption unit is configured to: generate the at least one replacement Diophantine equation if any one of the at least one Diophantine equation is predicted as solvable by the trained AI model;

the AI unit is configured to: predict insolvability or solvability of the at least one replacement Diophantine equation; and

the encryption unit is configured to: provide the at least one replacement Diophantine equation and a subset of the at least one Diophantine equation, which is other than the any one of the at least one Diophantine equation which is predicted as solvable by the trained AI model, as at least one cipher text to the cipher text output unit.

13. The encryption apparatus of any one of claim 11 to claim 12, wherein

the encryption unit is configured to: generate at least one faux Diophantine equation using the at least one variable solution set ($v_1,\ldots,v_n$); and

ascertain a solution of the at least one faux Diophantine equation as a non-integer,

wherein the AI unit is configured to: receive the at least one faux Diophantine equation, and the AI model is configured to: predict insolvability or solvability of the at least one faux Diophantine equation, and

wherein the encryption unit is configured to: provide the at least one faux Diophantine equation as a faux cipher text to the cipher text output unit if the solution of the at least one faux Diophantine equation is a non-integer.

14. The encryption apparatus of any one of claim 11 to claim 13, further comprising: a cipher text dependent variable unit communicably coupled to the encryption unit, wherein

the cipher text dependent variable unit is configured to: provide a cipher text dependent variable to the polynomial generation unit; and

the polynomial generation unit is configured to: derive the at least one variable solution set ($v_1,\ldots,v_n$) using the at least one symmetric key by being configured to: further derive the at least one variable solution set ($v_1,\ldots,v_n$) using the cipher text dependent variable.

15. The encryption apparatus of claim 14, wherein

the cipher text dependent variable unit is configured to: ascertain the cipher text dependent variable based on a coefficient of a variable in a Diophantine equation of a previous cipher text, wherein the variable in the Diophantine equation of the previous cipher text includes a polynomial degree based on a previous cipher text dependent variable.

16. The encryption apparatus of claim 11, wherein

the encryption unit is configured to: modify the at least one initial Diophantine equation using the concealment variable which is derived from the second subset of the at least one variable solution set ($v_1,\ldots,v_n$) by being configured to: perform addition, subtraction, multiplication, and/or division on the at least one initial Diophantine equation with the concealment variable.

17. The encryption apparatus of any one of claim 11 to claim 16, wherein

the plain text to integer unit includes an integer de-partitioning unit configured to: partition the at least one pre-encryption integer ($M_1,\ldots,M_n$) into a plurality of partitioned integers using a plurality of relatively prime integers;

the encryption unit is configured to: generate the at least one Diophantine equation solvable by the at least one variable solution set ($v_1,\ldots,v_n$) using the at least one pre-encryption integer ($M_1,\ldots,M_n$) and the at least one variable solution set ($v_1,\ldots,v_n$) by being configured to: generate a plurality of Diophantine equations of the at least one Diophantine equation using the at least one pre-encryption integer ($M_1,\ldots,M_n$), the at least one variable solution set ($v_1,\ldots,v_n$), and the partitioned integers,

wherein a count of the relatively prime integers, a count of the partitioned integers, and a count of the Diophantine equations are equivalent.

18. The encryption apparatus of claim 17, wherein

the integer de-partitioning unit is configured to: partition the at least one pre-encryption integer ($M_1,\ldots,M_n$) into the partitioned integers based on the relatively prime integers by being configured to: perform a plurality of modulo operations using the at least one pre-encryption integer ($M_1,\ldots,M_n$), the relatively prime integers as a plurality of divisors, and deriving therefrom the partitioned integers being a plurality of remainders.

19. A decryption method comprising:

receiving at least one cipher text which includes at least one Diophantine equation;

using a symmetric key, deriving at least one variable solution set ($v_1,\ldots,v_n$) for solving the at least one Diophantine equation;

using the at least one variable solution set ($v_1,\ldots,v_n$), solving the at least one Diophantine equation to ascertain at least one pre-encryption integer ($M_1,\ldots,M_n$), including:

using a first subset of the at least one variable solution set ($v_1,\ldots,v_n$), ascertaining the at least one initial integer; and

using a concealment variable derived from a second subset of the at least one variable solution set ($v_1,\ldots,v_n$), modifying the at least one initial integer to ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$); and

converting the at least one pre-encryption integer ($M_1,\ldots,M_n$) to at least one plain text.

20. The decryption method of claim 19, wherein using the at least one variable solution set ($v_1,\ldots,v_n$), solving the at least one Diophantine equation to ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$) includes:

ascertaining the at least one integer ($M_1,\ldots,M_n$) and at least one non-integer from different Diophantine equations of the at least one Diophantine equation to ascertain one of the different Diophantine equations corresponding to the at least one non-integer as a faux Diophantine equation.

21. The decryption method of any one of claim 19 to claim 20, wherein using the symmetric key, deriving the at least one variable solution set ($v_1,\ldots,v_n$) for solving the at least one Diophantine equation includes:

using the symmetric key and a cipher text dependent variable, deriving the at least one variable solution set ($v_1,\ldots,v_n$).

22. The decryption method of claim 21, wherein the cipher text dependent variable is based on a coefficient of a variable in a Diophantine equation of a previous cipher text, wherein the variable in the Diophantine equation of the previous cipher text includes a polynomial degree based on a previous cipher text dependent variable.

23. The decryption method of claim 19, wherein using the concealment variable derived from the second subset of the at least one variable solution set ($v_1,\ldots,v_n$), modifying the at least one initial integer to ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$) includes:

performing addition, subtraction, multiplication, and/or division on the at least one Diophantine equation with the concealment variable.

24. The decryption method of any one of claim 19 to claim 23, wherein using the at least one variable solution set ($v_1,\ldots,v_n$), solving the at least one Diophantine equation to ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$) includes:

using the at least one variable solution set ($v_1,\ldots,v_n$), solving a plurality of Diophantine equations of the at least one Diophantine equation to ascertain a plurality of partitioned integers; and

using a plurality of relatively prime integers and the partitioned integers, ascertaining the at least one pre-encryption integer ($M_1,\ldots,M_n$),
wherein a count of the relatively prime integers, a count of the partitioned integers, and a count of the Diophantine equations are equivalent.

25. The decryption method of claim 24, wherein using the relatively prime integers and the partitioned integers, ascertaining the at least one pre-encryption integer ($M_1,\ldots,M_n$) includes:

de-partitioning the partitioned integers by performing a plurality of Euclidean algorithm operations using the partitioned integers as a plurality of remainders and the relatively prime integers as a plurality of quotients, and deriving therefrom at least one pre-encryption integer ($M_1,\ldots,M_n$).

26. A decryption apparatus comprising:

at least one memory unit for storing computer-executable instructions; and

at least one processor communicably coupled to the at least memory unit and configured to: execute the computer-executable instructions to perform the method according to any one of claim 19 to claim 25.

27. A non-transitory, computer readable medium comprising computer-executable instructions configured to direct at least one computer processor to perform the method according to any one of claim 19 to claim 25.

28. A decryption apparatus comprising:

a cipher text input unit configured to receive at least one cipher text which includes at least one Diophantine equation;

a symmetric key input unit configured to receive at least one symmetric key;

a decryption unit communicably coupled to the cipher text input unit and the symmetric key input unit, and configured to:

receive the symmetric key from the symmetric key input unit and the at least one Diophantine equation from the cipher text input unit;

using the symmetric key, derive at least one variable solution set ($v_1,\ldots,v_n$) for solving the at least one Diophantine equation;

using the at least one variable solution set ($v_1,\ldots,v_n$), solve the at least one Diophantine equation to ascertain at least one pre-encryption integer ($M_1,\ldots,M_n$) by being configured to:

using a first subset of the at least one variable solution set ($v_1,\ldots,v_n$), ascertain at least one initial integer;

using a concealment variable derived from a second subset of the at least one variable solution set ($v_1,\ldots,v_n$), modify the at least one initial integer to ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$); and

an integer to plain text unit communicably coupled to the decryption unit and configured to:

receive the at least one pre-encryption integer ($M_1,\ldots,M_n$) from the decryption unit, and convert the at least one pre-encryption integer ($M_1,\ldots,M_n$) to at least one plain text.

29. The decryption apparatus of claim 28, wherein

the decryption unit is configured to: using the at least one variable solution set ($v_1,\ldots,v_n$), solve the at least one Diophantine equation to ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$) by being configured to: ascertain the at least one integer ($M_1,\ldots,M_n$) and at least one non-integer from different Diophantine equations of the at least one Diophantine equation to ascertain one of the different Diophantine equations as a faux Diophantine equation.

30. The decryption apparatus of any one of claim 28 to claim 29, wherein

the decryption unit is configured to: using the symmetric key, derive the at least one variable solution set ($v_1,\ldots,v_n$) for solving the at least one Diophantine equation by being configured to: using the symmetric key and a cipher text dependent variable, derive the at least one variable solution set ($v_1,\ldots,v_n$).

31. The decryption apparatus of claim 30, wherein the cipher text dependent variable is based on a coefficient of a variable in a Diophantine equation of a previous cipher text, wherein the variable in the Diophantine equation of the previous cipher text includes a polynomial degree based on a previous cipher text dependent variable.

32. The decryption apparatus of claim 28, wherein

the decryption unit is configured to: using the concealment variable derived from the second subset of the at least one variable solution set ($v_1,\ldots,v_n$), modify the at least one initial integer to ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$) by being configured to:

perform addition, subtraction, multiplication, and/or division on the at least one Diophantine equation with the concealment variable.

33. The decryption apparatus of any one of claim 28 to claim 32, wherein

the decryption unit is configured to: using the at least one variable solution set ($v_1,\ldots,v_n$), solve the at least one Diophantine equation to ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$) by being configured to:

using the at least one variable solution set ($v_1,\ldots,v_n$), solve a plurality of Diophantine equations of the at least one Diophantine equation to ascertain a plurality of partitioned integers; and

using a plurality of relatively prime integers and the partitioned integers, ascertain the at least one pre-encryption integer ($M_1,\ldots,M_n$),
wherein a count of the relatively prime integers, a count of the partitioned integers, and a count of the Diophantine equations are equivalent.

34. The decryption apparatus of claim 33, wherein the integer to plain text unit includes an integer de-partitioning unit, wherein

the integer de-partitioning unit is configured to:

receive the partitioned integers from the decryption unit, and de-partition the partitioned integers by performing a plurality of Euclidean algorithm operations using the partitioned integers as a plurality of remainders and the relatively prime integers as a plurality of quotients, and deriving therefrom at least one pre-encryption integer ($M_1,\ldots,M_n$).