CLAIMS

[Claim 1] An apparatus comprising:
a hardware processor configured to execute:
a seed value generator configured to generate a seed value;
a divider configured to divide the seed value into a plurality of divided blocks;
an extractor configured to extract a plurality of second parameter values from a second parameter candidate value set comprising a plurality of second parameter candidate values generated by using each of a plurality of first parameter candidate values, each of the plurality of second parameter values respectively corresponding to one of the plurality of divided blocks; and
a calculator configured to generate a random number based on the plurality of second parameter values,
wherein the hardware processor is further configured to encrypt data or generate a digital signature for the data based on the random number,
wherein each of the plurality of first parameter candidate values is a random value.

[Claim 2] The apparatus of claim 1, wherein each of the plurality of second parameter candidate values included in the second parameter candidate value set is generated by performing an exponentiation operation using a corresponding one of the plurality of first parameter candidate values as an exponent or by performing a scalar multiplication operation of a point using a corresponding one of the plurality of first parameter candidate values as a scalar multiplier.

[Claim 3] The apparatus of claim 1, wherein the extractor is further configured to extract the plurality of second parameter values respectively corresponding to bit strings in the plurality of divided blocks and positions of the divided blocks in the seed value, from the second parameter candidate value set.

[Claim 4] The apparatus of claim 2, wherein
the extractor comprises:
a first extractor configured to extract a plurality of first parameter values respectively corresponding to the plurality of divided blocks from a first parameter candidate value set including the plurality of first parameter candidate values used to generate the plurality of second parameter candidate values included in the second parameter candidate value set; and
a second extractor configured to extract the plurality of second parameter respectively corresponding to the plurality of divided blocks from the second parameter candidate value set,

wherein the calculator is further configured to generate a first random number based on the plurality of first parameter values and generate a second random number based on the plurality of second parameter values.

[Claim 5] The apparatus of claim 4, wherein
the first extractor is further configured to extract the plurality of first parameter values respectively corresponding to bit strings of the plurality of divided blocks and positions of the divided blocks in the seed value from the first parameter candidate value set, and
the second extractor is further configured to extract the plurality of second parameter values respectively corresponding to bit strings in the plurality of divided blocks and positions of the divided blocks in the seed value from the second parameter candidate value set.

[Claim 6] The apparatus of claim 4, wherein the calculator generates the first random number by adding the plurality of first parameter values to each other.

[Claim 7] The apparatus of claim 4, wherein the second random number is equal to a value obtainable by performing an exponentiation operation using the first random number as an exponent or by performing a scalar multiplication operation of a point using the first random number as a scalar multiplier and using the plurality of second parameter values.

[Claim 8] The apparatus of claim 7, wherein the hardware processor is further configured to encrypt the data or generate the digital signature for the data based on the first random number and the second random number.

[Claim 9] The apparatus of claim 1, wherein the seed value comprises a random bit string.

[Claim 10] A method, comprising:
generating a seed value;
dividing the seed value into a plurality of divided blocks;
extracting a plurality of second parameter values from a second parameter candidate value set comprising a plurality of second parameter candidate values generated by using each of a plurality of first parameter candidate values, each of the plurality of second parameter values respectively corresponding to one of the plurality of divided blocks;
generating a random number based on the plurality of second parameter values; and
applying the random number to encrypt data or generate a digital signature for the data,

wherein each of the plurality of first parameter candidate values is a random value.

[Claim 11] The method of claim 10, wherein each of the plurality of second parameter candidate values included in the second parameter candidate value set is generated by performing an exponentiation operation using a corresponding one of the plurality of first parameter candidate values as an exponent or by performing a scalar multiplication operation of a point using a corresponding one of the plurality of first parameter candidate values as a scalar multiplier.

[Claim 12] The method of claim 10, wherein the extracting of the plurality of second parameter values extracts the plurality of second parameter values respectively corresponding to bit strings in the plurality of divided blocks and positions of the block in the seed value, from the second parameter candidate value set.

[Claim 13] The method of claim 11, wherein
the extracting of the plurality of second parameter values comprises:
extracting a plurality of first parameter values respectively corresponding to the plurality of divided blocks from a first parameter candidate value set including the plurality of first parameter candidate values used to generate the plurality of second parameter candidate values included in the second parameter candidate value set; and
extracting the plurality of second parameter values respectively corresponding to the plurality of divided blocks from the second parameter candidate value set, and
the generating of the random number comprises:
generating a first random number based on the plurality of first parameter values; and
generating a second random number based on the plurality of second parameter values.

[Claim 14] The method of claim 13, wherein
the extracting of the plurality of first parameter values extracts the plurality of first parameter values respectively corresponding to bit strings of the plurality of divided blocks and positions of the divided blocks in the seed value, from the first parameter candidate value set, and
the extracting of the plurality of second parameter values extracts the plurality of second parameter values respectively corresponding to bit strings in the plurality of divided blocks and positions of the divided blocks in the seed value, from the second parameter candidate value set.

[Claim 15] The method of claim 13, wherein the generating of the first random number generates the first random number by adding the plurality of first parameter values to each other.

[Claim 16] The method of claim 13, wherein the generating of the second random number generates the second random number equal to a value obtainable through an exponentiation operation using the first random number as an exponent or through a scalar multiplication of a point operation using the first random number as a scalar multiplier using the plurality of second parameter values.

[Claim 17] The method of claim 16, further comprising generating a digital signature using the first random number and the second random number.

[Claim 18] The method of claim 10, wherein the seed value comprises a random bit string.

[Claim 19] A non-transitory computer readable medium having stored thereon a program for causing a computer to execute a method of claim 10.

[Claim 20] An apparatus comprising:
a hardware processor configured to execute:
receive a seed value;
divide the seed value into a plurality of blocks;
extract, for each of the plurality of blocks, a second parameter value from a second parameter candidate value set comprising a plurality of second parameter candidate values generated by using a plurality of first parameter candidate values, by using a number of the respective block and a value in the respective block as a first index; and
generate a random number based on the second parameter values for each of the plurality of blocks; and
apply the random number to encrypt data or generate a digital signature for the data based on the random number,
wherein each of the plurality of first parameter candidate values is a random value generated.

[Claim 21] The apparatus of claim 20, wherein a number of the second parameter candidate values included in the second parameter candidate value set changes according to a length of the seed value and a total number of the plurality of blocks.