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 blocks;
a first extractor configured to extract a plurality of first parameter values from a first parameter candidate value set including a plurality of first parameter candidate values, each of the plurality of first parameter values respectively corresponding to one of the plurality of divided blocks;
a second extractor configured to extract a plurality of second parameter values from a second parameter candidate value set including a plurality of second parameter candidate values generated by using each of the plurality of first parameter candidate values included in the first parameter candidate value set, each of the plurality of second parameter values respectively corresponding to one of the plurality of divided blocks;
a third extractor configured to extract a plurality of third parameter values from a third parameter candidate value set including a plurality of third parameter candidate values generated by using each of the plurality of second parameter candidate values included in the second parameter candidate value set, each of the plurality of third parameter values respectively corresponding to one of the plurality of divided blocks; and
a calculator configured to generate a first random number based on the plurality of first parameter values, generate a second random number based on the plurality of second parameter values, and generate a third random number based on the plurality of third parameter values,
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 included in the first parameter candidate value set 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 included in the first parameter candidate value set as a scalar multiplier,
wherein the hardware processor is further configured to encrypt data or generate a digital signature for the data based on at least one of the first random number, the second random number and the third random number.

[Claim 2] The apparatus of claim 1, 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 blocks in the seed value, from the first parameter candidate value set,
the second extractor is further configured to extract the plurality of second parameter values respectively corresponding to bit strings of the plurality of divided blocks and positions of the blocks in the seed value, from the second parameter candidate value set, and
the third extractor is further configured to extract the plurality of third parameter values respectively corresponding to bit strings of the plurality of divided blocks and positions of the blocks in the seed value, from the third parameter candidate value set.

[Claim 3] The apparatus of claim 1, wherein the calculator generates the first random number by adding the plurality of first parameter values to each other.

[Claim 4] The apparatus of claim 1, 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 5] The apparatus of claim 4, wherein at least one of the plurality of third parameter candidate values included in the third parameter candidate value set are obtained by multiplying at least one of the second parameter candidate values included in the second parameter candidate value set by a secret key.

[Claim 6] The apparatus of claim 5, wherein the third random number is equal to a product of the second random number and the secret key.

[Claim 7] The apparatus of claim 6, 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, the second random number, and the third random number.

[Claim 8] The apparatus of claim 1, wherein the seed value comprises a random bit string.

[Claim 9] A method, comprising:
generating a seed value;
dividing the seed value into a plurality of blocks;
extracting a plurality of first parameter values from a first parameter candidate value set including a plurality of first parameter candidate values, each of the

plurality of first parameter values respectively corresponding to one of the plurality of divided blocks;
extracting a plurality of second parameter values from a second parameter candidate value set including a plurality of second parameter candidate values generated by using each of the plurality of first parameter candidate values included in the first parameter candidate value set, each of the plurality of second parameter values respectively corresponding to one of the plurality of divided blocks;
extracting a plurality of third parameter values from a third parameter candidate value set including a plurality of third parameter candidate values generated by using each of the plurality of second parameter candidate values included in the second parameter candidate value set, each of the plurality of third parameter values respectively corresponding to one of the plurality of divided blocks;
generating a first random number based on the plurality of first parameter values;
generating a second random number based on the plurality of second parameter values;
generating a third random number based on the plurality of third parameter values; and
applying at least one of the first random number, the second random number and the third random number to encrypt data or generate a digital signature for the data,
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 included in the first parameter candidate value set 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 included in the first parameter candidate value set as a scalar multiplier.

[Claim 10] The method of claim 9, wherein
the extracting of the extracted 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 blocks in the seed value, from the first parameter candidate value set,
the extracting of the extracted plurality of second parameter values extracts the plurality of second parameter values respectively corresponding to bit strings of the plurality of divided blocks and positions of the blocks in the seed value, from the second parameter candidate value set, and
the extracting of the extracted plurality of third parameter values extracts the plurality of third parameter values respectively corresponding to bit strings of

the plurality of divided blocks and positions of the blocks in the seed value, from the third parameter candidate value set.

[Claim 11] The method of claim 9, 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 12] The method of claim 9, 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 13] The method of claim 12, wherein at least one of the plurality of third parameter candidate values included in the third parameter candidate value set are values obtained by multiplying at least one of the second parameter candidate values included in the second parameter candidate value set by a secret key.

[Claim 14] The method of claim 13, wherein the third random number is equal to a product of the second random number and the secret key.

[Claim 15] The method of claim 14, wherein the encrypting the data or the generating the digital signature is based on the first random number, the second random number, and the third random number.

[Claim 16] The method of claim 9, wherein the seed value comprises a random bit string.

[Claim 17] A non-transitory computer readable medium having stored thereon a program for causing a computer to execute a method of claim 9.

[Claim 18] 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 first parameter value from a first parameter candidate value set comprising 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;
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 the plurality of first parameter candidate

values, by using a number of the respective block and a value in the respective block as a second index;
extract, for each of the plurality of blocks, a third parameter value from a third parameter candidate value set comprising a plurality of third parameter candidate values generated by using the plurality of second parameter candidate values, by using a number of the respective block and a value in the respective block as a first third;
generate a first random number based on the first parameter values for each of the plurality of blocks;
generate a second random number based on the second parameter values for each of the plurality of blocks;
generate a third random number based on the third parameter values for each of the plurality of blocks; and
apply at least one of the first random number, the second random number and the third random number to encrypt data or generate a digital signature for the data,
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 included in the first parameter candidate value set 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 included in the first parameter candidate value set as a scalar multiplier.

[Claim 19] The apparatus of claim 18, wherein at least one of a number of the first parameter candidate values included in the first parameter candidate value set, a number of the second parameter candidate values included in the second parameter candidate value set, and a number of the third parameter candidate values included in the third parameter candidate value set, changes according to a length of the seed value and a total number of the plurality of blocks.