CIPHERTEXT HYBRID OPERATION METHOD AND DEVICE

[0001] The present application claims priority to Chinese Patent Application No. 202210252212.3, filed with the China Patent Office on March 15, 2022 and titled "CIPHERTEXT HYBRID OPERATION METHOD AND DEVICE", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] This specification relates to the field of ciphertext operation, and, in particular, to a ciphertext hybrid operation method and apparatus.

BACKGROUND

[0003] Modern computer systems often need to use different types of data to process different kinds of information. When facing a certain operation using different types of data, a hybrid operation way may be used to obtain an operation result that meets the requirements of this certain operation.

[0004] In related technologies, there has been a series of mature solutions for hybrid operation of plaintext data, but the research on hybrid operation of ciphertext data is still in an early stage, and no unified, efficient and clear solution has been formed.

SUMMARY

[0005] In view of the above, this specification provides a ciphertext hybrid operation method and apparatus to solve the deficiencies in the related technologies.

[0006] Specifically, this specification is implemented through the following technical solutions.

[0007] According to a first aspect of embodiments of this specification, there is provided a ciphertext hybrid operation method, which is used for performing a hybrid operation on ciphertexts of a plurality of preset ciphertext types, wherein unidirectional

ciphertext conversion relationships pointing to destination ciphertext types from original ciphertext types are set among the plurality of preset ciphertext types, and a multi-level ciphertext conversion relationship is formed based on the unidirectional ciphertext conversion relationships, wherein each preset ciphertext type corresponds to a unique level in the multi-level ciphertext conversion relationship, and at least one path constituted by the unidirectional ciphertext conversion relationships exists between each preset ciphertext type and a highest-level preset ciphertext type, the method including:

[0008] receiving a target function signature and a corresponding operand set, the operand set including ciphertext operands corresponding to at least two preset ciphertext types;

[0009] determining a target ciphertext type corresponding to the at least two preset ciphertext types, wherein the target ciphertext type is simultaneously located in paths formed between each of the at least two preset ciphertext types and the highest-level preset ciphertext type; and

[0010] decrypting, in a case where the target ciphertext type supports an operation function specified by the target function signature, all the ciphertext operands in the operand set, converting the decrypted ciphertext operands to use the target ciphertext type for representation, and performing operation on the converted ciphertext operands according to the operation function specified by the target function signature.

[0011] According to a second aspect of the embodiments of this specification, there is provided a ciphertext hybrid operation apparatus, which is used for performing hybrid operation on ciphertexts of a plurality of preset ciphertext types, wherein unidirectional ciphertext conversion relationships pointing to destination ciphertext types from original ciphertext types are set among the plurality of preset ciphertext types, and a multi-level ciphertext conversion relationship is formed based on the unidirectional ciphertext conversion relationships, wherein each preset ciphertext type corresponds to a unique level in the multi-level ciphertext conversion relationship, and at least one path constituted by the unidirectional ciphertext conversion relationships exists between each preset ciphertext type and a highest-level preset ciphertext type, the apparatus including:

CLAIMS

What is claimed is:

1. A ciphertext hybrid operation method, which is used for performing a hybrid operation on ciphertexts of a plurality of preset ciphertext types, wherein unidirectional ciphertext conversion relationships pointing to destination ciphertext types from original ciphertext types are set among the plurality of preset ciphertext types, and a multi-level ciphertext conversion relationship is formed based on the unidirectional ciphertext conversion relationships, wherein each preset ciphertext type corresponds to a unique level in the multi-level ciphertext conversion relationship, and at least one path constituted by the unidirectional ciphertext conversion relationships exists between each preset ciphertext type and a highest-level preset ciphertext type, the method comprises:

receiving a target function signature and a corresponding operand set, the operand set comprising ciphertext operands corresponding to at least two preset ciphertext types;

determining a target ciphertext type corresponding to the at least two preset ciphertext types, wherein the target ciphertext type is simultaneously located in paths formed between each of the at least two preset ciphertext types and the highest-level preset ciphertext type; and

decrypting, in a case where the target ciphertext type supports an operation function specified by the target function signature, all the ciphertext operands in the operand set, converting the decrypted ciphertext operands to use the target ciphertext type for representation, and performing operation on the converted ciphertext operands according to the operation function specified by the target function signature.

2. The method according to claim 1, further comprising:

in a case where there are a plurality of preset ciphertext types being simultaneously located in the paths formed between each of the at least two preset ciphertext types and the highest-level preset ciphertext type, the target ciphertext type is a preset ciphertext type at a lowest level.

3. The method according to claim 1, wherein decrypting all the ciphertext operands in the operand set, converting the decrypted ciphertext operands to use the target ciphertext type for representation, and performing the operation on the converted ciphertext operands according to the operation function specified by the target function signature comprises:

decrypting the ciphertext operands corresponding to the at least two preset ciphertext types and a ciphertext operand corresponding to a literal type, then converting the decrypted ciphertext operands respectively to use the target ciphertext type for representation, and performing the operation on the converted ciphertext operands according to the operation function specified by the target function signature.

4. The method according to claim 1, wherein the plurality of preset ciphertext types belong to elements in a lattice-based partially-ordered set, and determining the target ciphertext type corresponding to the at least two preset ciphertext types comprises:

determining a suprema in the partially-ordered set corresponding to the at least two preset ciphertext types corresponding to the ciphertext operands in the operand set, using the suprema as the target ciphertext type.

5. The method according to claim 4, wherein the partially-ordered set is represented based on a topological sequence, edges of respective elements in the topological sequence correspond to the unidirectional ciphertext conversion relationships, and a sequence number in the topological sequence corresponding to an original ciphertext type in each unidirectional ciphertext conversion relationship is smaller than a sequence number in the topological sequence corresponding to a corresponding destination ciphertext type; and determining the target ciphertext type corresponding to the at least two preset ciphertext types comprises:

comparing sequence numbers in the topological sequence corresponding to N preset ciphertext types of the at least two preset ciphertext types, and respectively updating, in a case where the sequence numbers corresponding to the N preset ciphertext types are not completely consistent, preset ciphertext types of the N preset

ciphertext types, which correspond to non-maximum sequence numbers, to preset ciphertext types corresponding to edges thereof in the topological sequence, until the sequence numbers corresponding to the N preset ciphertext types are consistent, wherein N is the number of kinds of preset ciphertext types in the at least two preset ciphertext types; and

determining a preset ciphertext type in the topological sequence corresponding to the sequence numbers of the N preset ciphertext types as the target ciphertext type.

6. The method according to claim 1, wherein the unidirectional ciphertext conversion relationships pointing to the destination ciphertext types from the original ciphertext types being set among the plurality of preset ciphertext types comprises:

in a case where the unidirectional ciphertext conversion relationships exist between a first preset ciphertext type and a second preset ciphertext type from each other, the plurality of preset ciphertext types comprise a virtual ciphertext type having a ciphertext type the same as the first preset ciphertext type, and a unidirectional ciphertext conversion relationship in which the second preset ciphertext type points to the first preset ciphertext type is replaced with a unidirectional ciphertext conversion relationship in which the second preset ciphertext type points to the virtual ciphertext type.

7. The method according to claim 1, further comprising:

selecting, in a case where the target ciphertext type does not support a function corresponding to the target function signature, another preset ciphertext type in a path formed between the target ciphertext type and the highest-level preset ciphertext type to update the target ciphertext type, wherein the other preset ciphertext type supports the function corresponding to the target function signature.

8. The method according to claim 1, further comprising:

adjusting, according to a received adjustment instruction, the preset ciphertext types comprised in the plurality of preset ciphertext types and/or any unidirectional ciphertext conversion relationship in the multi-level ciphertext conversion relationship.

9. A ciphertext hybrid operation apparatus, which is used for performing a hybrid operation on ciphertexts of a plurality of preset ciphertext types, wherein unidirectional ciphertext conversion relationships pointing to destination ciphertext types from original ciphertext types are set among the plurality of preset ciphertext types, and a multi-level ciphertext conversion relationship is formed based on the unidirectional ciphertext conversion relationships, wherein each preset ciphertext type corresponds to a unique level in the multi-level ciphertext conversion relationship, and at least one path constituted by the unidirectional ciphertext conversion relationships exists between each preset ciphertext type and a highest-level preset ciphertext type, the apparatus comprises:

a data receiving unit for receiving a target function signature and a corresponding operand set, the operand set comprising ciphertext operands corresponding to at least two preset ciphertext types;

a target ciphertext type determination unit for determining a target ciphertext type corresponding to the at least two preset ciphertext types, wherein the target ciphertext type is simultaneously located in paths formed between each of the at least two preset ciphertext types and the highest-level preset ciphertext type; and

a data operation unit for decrypting, in a case where the target ciphertext type supports an operation function specified by the target function signature, all the ciphertext operands in the operand set, converting the decrypted ciphertext operands to use the target ciphertext type for representation, and performing operation on the converted ciphertext operands according to the operation function specified by the target function signature.

10. A computer-readable storage medium having a computer program stored thereon, wherein when the program is executed by a processor, steps of the method of any one of claims 1 to 8 are implemented.

11. An electronic device comprising a memory, a processor, and a computer program stored in the memory and runnable on the processor, wherein when the

processor executes the program, steps of the method of any one of claims 1 to 8 are implemented.