

CLAIMS

What is claimed is:

1. A method operating on a first processor comprising:
receiving first data indicating a sequence of reversible q -bit gates including a first segment for decrypting permutation encrypted data to produce decrypted data, a second segment for operating on the decrypted data to produce one or more resulting decrypted data, and a third segment for encrypting the resulting decrypted data using permutation encryption to produce permutation encrypted resulting data;
storing on a computer-readable medium second data that indicates rules for replacing a first sequence of two q -bit gates operating on at least one shared bit of an input N -bit word with a different second sequence of one or more q -bit gates that produce the same output N -bit word;
using the second data to propagate at least one q -bit gate from the first segment to a number J of gates distance into the q -bit gates for the second segment or beyond and at least one q -bit gate from the third segment to a number K of gates distance into the q -bit gates for the second segment or before to produce an obfuscated sequence of reversible q -bit gates;
sending obfuscated instructions based on the obfuscated sequence of reversible q -bit gates to a second processor for execution.
2. The method as recited in claim 1, further comprising:
storing on a computer-readable medium third data relating each code instruction in a form executable by the different second processor to one or more reversible q -bit gates operating on an N -bit word; and
using the third data to convert the obfuscated sequence of reversible q -bit gates to obfuscated code instructions in a form executable by the second processor,
wherein sending obfuscated instructions further comprises sending obfuscated code instructions in a form executable by the second processor.

3. The method as recited in claim 1, wherein:
the method further comprises storing on a computer-readable medium third data relating each code instruction in a form executable by the second processor to one or more reversible q -bit gates operating on an N-bit word; and,
said receiving first data further comprises:
receiving code instructions in a form executable by the second processor for operating on the encrypted data to produce one or more resulting decrypted data; and,
using the third data to convert the code instructions in a form executable by the second processor for operating on the encrypted data to produce one or more resulting decrypted data to the sequence of reversible q -bit gates for operating on the encrypted data to produce one or more resulting decrypted data.
4. The method as recited in claim 1, further comprising:
storing on a computer-readable medium fusion data that indicates rules for replacing each of one or more sequences reversible q -bit gates operating on an input N-bit word to produce an output N-bit word, with one or more reversible k-bit gates (wherein $3 < k \leq N$) that produce a same output N-bit word; and
using the fusion data to replace a particular sequence of one or more reversible q -bit gates of the obfuscated sequence of reversible q -bit gates with a k-bit gate that can replace the particular sequence.

5. The method as recited in claim 4, further comprising:
- storing on a computer-readable medium third data relating each code instruction in a form executable by the different second processor to one or more reversible q -bit gates operating on an N -bit word;
 - storing on a computer-readable medium fusion code data relating each of the one or more k -bit gates with one or more code instructions for the different second processor;
 - using the fusion code data to convert the k -bit gate to at least part of obfuscated code instructions; and
 - using the third data to convert any remaining reversible q -bit gates of the obfuscated sequence of reversible q -bit gates to any remaining part of the obfuscated code instructions,
- wherein sending obfuscated instructions further comprises sending obfuscated code instructions in a form executable by the second processor.

6. The method as recited in claim 1, wherein $J > N$ and $K > N$.
7. The method as recited in claim 1, wherein each reversible q -bit gate is a control gate comprising a single target bit and $q-1$ control bits that determine a value for the single target bit based on values at the $q-1$ control bits and values input to the $q-1$ control bits.
8. The method as recited in claim 1, wherein $q \in \{1, 2, 3\}$.
9. The method as recited in claim 1, wherein the second processor is different from the first processor.
10. The method as recited in claim 1, wherein access to the second processor is different from access to the first processor.
11. A non-transitory computer-readable medium carrying one or more sequences of instructions, wherein execution of the one or more sequences of instructions by a first set of one or more processors causes the first set of one or more processors to perform the steps of:
 - receiving first data indicating a sequence of reversible q -bit gates including a first segment for decrypting permutation encrypted data to produce decrypted data, a second segment for operating on the decrypted data to produce one or more resulting decrypted data, and a third segment for encrypting the resulting decrypted data using permutation encryption to produce permutation encrypted resulting data;
 - storing second data that indicates rules for replacing a first sequence of two reversible q -bit gates operating on at least one shared bit of an input N -bit word with a different second sequence of one or more reversible q -bit gates that produce the same output N -bit word;

using the second data to propagate at least one q -bit gate from the first segment to a number J of gates distance into the q -bit gates for the second segment or beyond and at least one q -bit gate from the third segment to a number K of gates distance into the q -bit gates for the second segment or before to produce an obfuscated sequence of reversible q -bit gates;
sending obfuscated instructions based on the obfuscated sequence of reversible q -bit gates to a second set of one or more processors for execution.

12. The non-transitory computer-readable medium as recited in claim 11, further comprising:

storing on a computer-readable medium third data relating each code instruction in a form executable by the different second processor to one or more reversible q -bit gates operating on an N-bit word; and
using the third data to convert the obfuscated sequence of reversible q -bit gates to obfuscated code instructions in a form executable by the second processor,
wherein sending obfuscated instructions further comprises sending obfuscated code instructions in a form executable by the second set of one or more processors.

13. The non-transitory computer-readable medium as recited in claim 11, wherein:
the method further comprises storing on a computer-readable medium third data relating each code instruction in a form executable by the second set of one or more processors to one or more reversible q -bit gates operating on an N -bit word;
and,
said receiving first data further comprises:
receiving code instructions in a form executable by the second set of one or more processors for operating on the encrypted data to produce one or more resulting decrypted data; and,
using the third data to convert the code instructions in a form executable by the second set of one or more processors for operating on the encrypted data to produce one or more resulting decrypted data to the sequence of reversible q -bit gates for operating on the encrypted data to produce one or more resulting decrypted data.
14. The non-transitory computer-readable medium as recited in claim 11, further comprising:
storing on a computer-readable medium fusion data that indicates rules for replacing each of one or more sequences of reversible q -bit gates operating on an input N -bit word to produce an output N -bit word, with one or more k -bit gates (wherein $3 < k \leq N$) that produce a same output N -bit word; and
using the fusion data to replace a particular sequence of one or more reversible q -bit gates of the obfuscated sequence of reversible q -bit gates with a k -bit gate that can replace the particular sequence.

15. The non-transitory computer-readable medium as recited in claim 14, further comprising:

storing on a computer-readable medium third data relating each code instruction in a form executable by the second set of one or more processors to one or more reversible q -bit gates operating on an N -bit word;

storing on a computer-readable medium fusion code data relating each of the one or more k -bit gates with one or more code instructions for the different second set of one or more processors;

using the fusion code data to convert the k -bit gate to at least part of obfuscated code instructions; and

using the third data to convert any remaining reversible q -bit gates of the obfuscated sequence of reversible q -bit gates to any remaining part of the obfuscated code instructions,

wherein sending obfuscated instructions further comprises sending obfuscated code instructions in a form executable by the second set of one or more processors.

16. The non-transitory computer-readable medium as recited in claim 11, wherein $J > N$ and $K > N$.
17. The non-transitory computer-readable medium as recited in claim 11, wherein each reversible q -bit gate is a control gate comprising a single target bit and $q-1$ control bits that determine a value for the single target bit based on values at the $q-1$ control bits and values input to the $q-1$ control bits.
18. The non-transitory computer-readable medium as recited in claim 11, wherein $q \in \{1, 2, 3\}$.
19. The non-transitory computer-readable medium as recited in claim 11, wherein the second set of one or more processors is different from the first set of one or more processors.
20. The non-transitory computer-readable medium as recited in claim 11, wherein access to the second set of one or more processors is different from access to the first set of one or more processors.
21. A system comprising:
 - a first set of at least one processor; and
 - at least one memory including one or more sequences of instructions,the at least one memory and the one or more sequences of instructions configured to, with the at least one processor, cause an apparatus to perform at least the following, receiving first data indicating a sequence of reversible q -bit gates including a first segment for decrypting permutation encrypted data to produce decrypted data, a second segment for operating on the decrypted data to produce one or more resulting decrypted data, and a third segment for encrypting the resulting decrypted data using permutation encryption to produce permutation encrypted resulting data;

storing on the computer-readable medium second data that indicates rules for replacing a first sequence of two q -bit gates operating on at least one shared bit of an input N -bit word with a different second sequence of one or more q -bit gates that produce the same output N -bit word;

using the second data to propagate at least one q -bit gate from the first segment to a number J of gates distance into the q -bit gates for the second segment or beyond and at least one q -bit gate from the third segment to a number K of gates distance into the q -bit gates for the second segment or before to produce an obfuscated sequence of reversible q -bit gates;

sending obfuscated instructions based on the obfuscated sequence of reversible q -bit gates to a second set of at least one processor for execution.

22. The system as recited in claim 21, further comprising:
- storing on a computer-readable medium third data relating each code instruction in a form executable by the second set of at least one processor to one or more reversible q -bit gates operating on an N -bit word; and
- using the third data to convert the obfuscated sequence of reversible q -bit gates to obfuscated code instructions in a form executable by the second set of at least one processor,
- wherein sending obfuscated instructions further comprises sending obfuscated code instructions in a form executable by the second set of at least one processor.

23. The system as recited in claim 21, wherein:
the method further comprises storing on a computer-readable medium third data relating each code instruction in a form executable by the second set of at least one processor to one or more reversible q -bit gates operating on an N-bit word; and,
said receiving first data further comprises:
receiving code instructions in a form executable by the second set of at least one processor for operating on the encrypted data to produce one or more resulting decrypted data; and,
using the third data to convert the code instructions in a form executable by the second set of at least one processor for operating on the encrypted data to produce one or more resulting decrypted data to the sequence of reversible q -bit gates for operating on the encrypted data to produce one or more resulting decrypted data.
24. The system as recited in claim 21, further comprising:
storing on a computer-readable medium fusion data that indicates rules for replacing each of one or more sequences of reversible q -bit gates operating on an input N-bit word to produce an output N-bit word, with one or more k-bit gates (wherein $3 < k \leq N$) that produce a same output N-bit word; and
using the fusion data to replace a particular sequence of one or more q -bit gates of the obfuscated sequence of q -bit gates with a k-bit gate that can replace the particular sequence.

25. The system as recited in claim 24, further comprising:
storing on a computer-readable medium third data relating each code instruction in a form executable by the second set of at least one processor to one or more reversible q -bit gates operating on an N -bit word;
storing on a computer-readable medium fusion code data relating each of the one or more k -bit gates with one or more code instructions for the second set of at least one processor;
using the fusion code data to convert the k -bit gate to at least part of obfuscated code instructions; and
using the third data to convert any remaining reversible q -bit gates of the obfuscated sequence of reversible q -bit gates to any remaining part of the obfuscated code instructions,
wherein sending obfuscated instructions further comprises sending obfuscated code instructions in a form executable by the second set of at least one processor.
26. The system as recited in claim 21, wherein $J > N$ and $K > N$.
27. The system as recited in claim 21, wherein each reversible q -bit gate is a control gate comprising a single target bit and $q-1$ control bits that determine a value for the single target bit based on values at the $q-1$ control bits and values input to the $q-1$ control bits.
28. The system as recited in claim 21, wherein $q \in \{1, 2, 3\}$.
29. The system as recited in claim 21, wherein the second set of at least one processor is different from the first set of at least one processor.
30. The system as recited in claim 21, wherein access to the second set of at least one processor is different from access to the first set of at least one processor.