

**[0055]** In a third tie-breaking technique, a pair of basis vectors is selected who has the greatest value for a square of the Euclidean norm minus the difference between the largest two elements of the distance vector.

**[0056]** In a fourth tie-breaking technique, if a pair of basis vectors induces a Euclidean norm larger than a previous pair of basis vectors, then one of the pairs is randomly chosen (with a probability of  $1/2$ ).

**[0057]** Although the methods **200** and **300** have been described as applied to separate sets of formulas, it is understood that they could be applied to a single circuit or set of formulas. For example, method **200** could be applied to first with the aim of reducing non-linear components of a circuit while possibly extending linear components. Then method **300** could be applied to optimize the linear components. Also, it is understood that if the circuit contained multiple linear portions and multiple non-linear portions, the methods **200** and **300** could be applied to each of those portions to attempt to reduce the total number of gates in the circuit.

**[0058]** FIG. 4 schematically illustrates a system **90** operable to implement the methods **100**, **200** and **300**. A computer **91** includes a microprocessor **92**, memory **93**, and an input/output device **94**. The computer is operable to receive one or more formulas **95** representing a combinational circuit, is operable to apply the methods **100**, **200**, and **300** to the formulas **95**, and is operable to output one or more simplified formulas **96** that calculate a same target signal as the formulas **95** using fewer gates.

**[0059]** FIGS. 5-7 schematically illustrate a Substitution-Box ("S-Box") for the Advanced Encryption Standard ("AES") after the method **100** has been applied to the S-Box to simplify it. The simplified S-Box of FIGS. 5-7 includes only 115 Boolean logic gates. FIG. 5 schematically illustrates a first, input portion **97** that includes 23 XOR gates (circles). FIG. 6 schematically illustrates a second portion **98** coupled to the first, input portion **97**. The second portion **98** includes 30 XOR gates (circles) and 32 AND gates (squares). Also, 11 of the 30 XOR gates and 5 of the 32 AND gates (double circles and double squares) are operable to perform inversion in GF(16). FIG. 7 schematically illustrates a third, output portion **99** coupled to the second portion **98**. The third, output portion **99** includes 26 XOR gates (circles) and 4 XNOR gates (triangles). Also, the second portion **98** corresponds to a non-linear core of inversion in GF(256). The second portion **98** represents a core of inversion in GF(256) that could be combined with various linear subcircuits to achieve inversion in GF(256).

**[0060]** Although a preferred embodiment of this invention has been disclosed, a worker of ordinary skill in this art would recognize that certain modifications would come within the scope of this invention. For that reason, the following claims should be studied to determine the true scope and content of this invention.

What is claimed is:

1. A method of simplifying a combinational circuit, comprising:

establishing an initial combinational circuit operable to calculate at least one target signal, the initial combinational circuit including multiplication operations and addition operations;

reducing a quantity of multiplication operations performed in a first portion of the initial combinational circuit to

create a first, simplified combinational circuit, the first portion including only multiplication operations and addition operations; and

reducing a quantity of addition operations performed in a second portion of the first, simplified combinational circuit to create a second, simplified combinational circuit, the second portion including only addition operations, wherein the second, simplified combinational circuit is operable to calculate the at least one target signal using fewer multiplication and fewer addition operations than the initial combinational circuit.

2. The method of claim 1, wherein said initial combinational circuit corresponds to a subcircuit of a larger combinational circuit, and wherein said steps of reducing a quantity of multiplication operations and reducing a quantity of addition operations steps are selectively repeated to further simplify the larger combinational circuit.

3. The method of claim 1, wherein said reducing a quantity of multiplication operations comprises:

a) identifying the first portion of the combinational circuit, the first portion being operable to calculate a first target signal, and the first portion including only a plurality of multiplication and addition operations;

b) establishing a set of signals including a plurality of input signals;

c) adding randomly, through use of a computer, at least one pair of the input signals together to determine at least one sum;

d) expanding the set of signals to include the at least one sum;

e) multiplying randomly, through use of the computer, at least two signals in the set of signals to determine at least one product;

f) expanding the set of signals to include the at least one product; and

g) selectively repeating steps C-F until the first target signal is found or until a quantity of multiplication operations performed in step E reaches a maximum number of desired multiplication operations.

4. The method of claim 3, further comprising:

generating a circuit specification including each addition performed in step C and including each multiplication performed in step E in response to finding the first target signal in step G, wherein a sum of the quantity of addition operations and multiplication operations performed in the circuit specification is less than a quantity of operations performed in the first portion.

5. The method of claim 4, wherein the circuit specification corresponds to at least one of a straight line program or Verilog code.

6. The method of claim 4, further comprising: constructing a combinational circuit corresponding to the circuit specification.

7. The method of claim 3, further comprising:

selectively repeating steps A and C-G until the desired target signal is found for each of a plurality of first portions of the combinational circuit.

8. A computer-implemented method of simplifying a plurality of formulas, comprising:

a) establishing a plurality of formulas including only addition operations, wherein each of the plurality of formulas corresponds to a portion of a combinational circuit including only addition operations;

b) defining a basis set including a plurality of input signals;