

[0056] 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.

[0057] 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 $\frac{1}{2}$).

[0058] 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.

[0059] 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.

[0060] 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).

[0061] 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 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 formu-

- las corresponds to a portion of a combinational circuit including only addition operations;
 - b) defining a basis set including a plurality of input signals;
 - c) determining, through use of a computer, a distance vector that includes one value for each of the plurality of formulas, the one value corresponding to a number of addition operations necessary to calculate a corresponding formula using signals from the basis set;
 - d) determining, through use of the computer, two basis vectors whose sum, when added to the distance vector, reduces at least one value in the distance vector;
 - e) adding the sum to the basis set; and
 - f) selectively repeating steps C-E until the basis set includes sums corresponding to each of the plurality of formulas.
- 2.** The method of claim **1**, further comprising: generating a circuit specification including the each sum of said two basis vectors from step D.
- 3.** The method of claim **2**, wherein the circuit specification corresponds to at least one of a straight line program or Verilog code.
- 4.** The method of claim **2**, further comprising: constructing a combinational circuit corresponding to the circuit specification.
- 5.** The method of claim **1**, wherein each of the input signals corresponds to a row from an identify matrix.
- 6.** The method of claim **1**, wherein said step D selects two basis vectors whose sum achieve a maximum reduction in the distance vector.
- 7.** The method of claim **6**, wherein if two different sums achieve the same maximum reduction in the distance vector, the sum is chosen who includes the largest Euclidean norm.
- 8.** The method of claim **6**, wherein if two different sums achieve the same maximum reduction in the distance vector, the sum is chosen who has the greatest value of the Euclidean norm minus the largest element in the distance vector.
- 9.** The method of claim **6**, wherein if two different sums achieve the same maximum reduction in the distance vector, the sum is chosen who induces the greatest value for a square of the Euclidean norm minus a difference between the largest two elements of the distance vector.
- 10.** The method of claim **6**, wherein if two different sums achieve the same maximum reduction in the distance vector and the two sums each induce different Euclidean norms, one of the two different sums is randomly chosen.
- 11.** A combinational circuit for a Substitution-Box for the Advanced Encryption Standard having a total of 115 Boolean gates, comprising:
- a first, input portion having 23 XOR gates;
 - a second portion coupled to the first, input portion having 30 XOR gate and 32 AND gates, wherein 11 of the 30 XOR gates and 5 of the 32 AND gates are operable to perform inversion in GF(16); and
 - a third, output portion coupled to the second portion having 26 XOR gates and 4 XNOR gates.
- 12.** The circuit of claim **11**, wherein the second portion corresponds to a non-linear core of inversion in GF(256).

* * * * *