

- 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.
- 9.** The method of claim **8**, further comprising: generating a circuit specification including the each sum of said two basis vectors from step D.
- 10.** The method of claim **9**, wherein the circuit specification corresponds to at least one of a straight line program or Verilog code.
- 11.** The method of claim **9**, further comprising: constructing a combinational circuit corresponding to the circuit specification.
- 12.** The method of claim **8**, wherein each of the input signals corresponds to a row from an identify matrix.
- 13.** The method of claim **8**, wherein said step D selects two basis vectors whose sum achieve a maximum reduction in the distance vector.
- 14.** The method of claim **13**, wherein if two different sums achieve the same maximum reduction in the distance vector, the sum is chosen who includes the largest Euclidean norm.
- 15.** The method of claim **13**, 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.
- 16.** The method of claim **13**, 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.
- 17.** The method of claim **13**, 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.
- 18.** 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.
- 19.** The circuit of claim **18**, wherein the second portion corresponds to a non-linear core of inversion in GF(256).

\* \* \* \* \*