METHOD OF OPTIMIZING COMBINATIONAL CIRCUITS

REFERENCE TO RELATED APPLICATIONS

[0001] This application is a divisional of U.S. application Ser. No. 12/367,660 filed on Feb. 9, 2009.

BACKGROUND OF THE INVENTION

[0002] This disclosure relates to combinational circuits, and more specifically to a method of optimizing combinational circuits.

[0003] Combinational circuits have many possible applications. One such application is computing an inverse in a Galois Field, which is a field containing a finite number of elements. A combinational circuit is a circuit having an output value determined by the values of its inputs. Combinational circuits can be represented as circuit schematics using Boolean logic gates (such as AND gates and XOR gates), or can be represented mathematically using formulas having operations corresponding to logic gates. For example, an AND gate corresponds to a field multiplication operation, and an XOR gate corresponds to a field addition operation. Logic gates can be arranged to calculate functions, and binary string output of a function may be referred to as a "target signal." In a typical truth table for a function, the target signal corresponding to the function is the last column of the truth table.

[0004] A combinational circuit may have both linear and non-linear portions, where the "non-linear" portions contain AND gates and XOR gates, and the "linear" portions contain only XOR gates. A quantity of AND gates of a combinational circuit may be referred to as the "multiplicative complexity" of the circuit. Combinational circuits and their associated formulas can be extremely large and complex in certain applications, such as microprocessors.

SUMMARY OF THE INVENTION

[0005] A method of simplifying a combinational circuit establishes an initial combinational circuit operable to calculate a target signal. A quantity of multiplication operations performed in a first portion of the initial combinational circuit is reduced to create a first, simplified combinational circuit. The first portion includes only multiplication operations and addition operations. A quantity of addition operations performed in a second portion of the first, simplified combinational circuit is reduced to create a second, simplified combinational circuit. The second portion includes only addition operations. Also, the second, simplified combinational circuit is operable to calculate the target signal using fewer operations than the initial combinational circuit.

[0006] A computer-implemented method of simplifying a plurality of formulas establishes a plurality of formulas. The formulas include only addition operations, and the formulas correspond to a portion of a combinational circuit including only addition operations. A basis set including a plurality of input signals is defined. Using a computer, a distance vector is determined 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. Using the computer, two basis vectors are determined whose sum, when added to the distance vector, reduces at least one value in the distance vector, and the sum is added to the basis set. The steps of determining two basis vectors whose sum, when added to the basis set, reduces at least one value in the distance vector, and adding the sum to the basis set may be selectively repeated until the basis set includes sums corresponding to each of the plurality of formulas.

[0007] A combinational circuit for a Substitution-Box for the Advanced Encryption Standard having a total of 115 Boolean gates comprises a first, input portion, a second portion coupled to the first, input portion, and a third, output portion coupled to the second portion. The first, input portion has 23 XOR gates. The second portion has 30 XOR gate and 32 AND gates, and computes the non-linear component of inversion in GF(256). Also, in the second portion **11** of the 30 XOR gates and 5 of the 32 AND gates are operable to perform inversion in GF(16). The third, output portion has 26 XOR gates and 4 XNOR gates.

[0008] These and other features of the present invention can be best understood from the following specification and drawings, of which the following is a brief description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. **1** schematically illustrates a method of optimizing a combinational circuit.

[0010] FIG. **2** schematically illustrates a method of reducing a quantity of AND gates in a combinational circuit.

[0011] FIG. **3** schematically illustrates a method of reducing a quantity of XOR gates in a combinational circuit.

[0012] FIG. **4** schematically illustrates a system operable to implement the methods of FIGS. **2-3**.

[0013] FIG. **5** schematically illustrates a first, input component of a S-Box for AES.

[0014] FIG. **6** schematically illustrates a second component of the S-Box for AES.

[0015] FIG. **7** schematically illustrates a third, output component of the S-Box for AES.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0016] FIG. **1** schematically illustrates a method **100** of optimizing a combinational circuit. A non-linear combinational circuit operable to calculate a target signal is identified (step **102**). As described above, the term "non-linear" refers to a circuit that includes multiplication operations (AND gates) and addition operations (XOR gates). The non-linear combinational circuit includes linear portions that include only addition operations (XOR gates). It is known that the set comprised of an AND gate, an XOR gate, and a constant "1" is functionally complete. That is, any other logic gate (such as an OR gate or a NAND gate) can be represented using only AND gates, XOR gates, and the constant "1". In one example step **102** includes converting a circuit including gates other than AND gates and XOR gates into AND gates and XOR gates. One of ordinary skill in the art would be able to perform such a conversion. In one example step **102** includes extracting a combinational circuit from a function.

[0017] A first, non-linear portion of the combinational circuit is identified (step **104**). A method **200** (see FIG. **2**) of reducing a quantity of multiplication operations is performed (step **106**), and the combinational circuit is updated (step **108**). Steps **104-108** may be selectively repeated to simplify multiple portions of the combinational circuit.

[0018] A second, linear portion of the combinational circuit is identified (step **110**) that includes only addition operations (XOR gates). A method **300** (see FIG. **3**) of reducing a quan-