fied combinational circuit that is operable to calculate the same target signal as the original combinational circuit using fewer operations.

[0018] FIG. **2** schematically illustrates the method **200** of reducing a quantity of multiplication operations (AND gates) in greater detail. The method **200** will be illustrated using formulas 1-4 below which are derived from a $GF(2^4)$ Galois Field representation from Canright (D. Canright. *A Very Compact Rijndael S-box.* Technical Report NPS-MA-05-001, Naval Postgraduate School, 2005). Thus, for this example we will assume that formulas 1-4 correspond to the first portion of a combinational circuit. However, it is understood that method **200** may also be applied to formulas other than formulas 1-4, including formulas having a greater or lesser quantity of variables and operations.

$$y_1=x_2x_3x_4+x_1x_3+x_2x_3+x_3+x_4 \quad \text{formula \#1}$$

$$y_2=x_1x_3x_4+x_1x_3+x_2x_3+x_2x_4+x_4 \quad \text{formula \#2}$$

$$y_3=x_1x_2x_4+x_1x_3+x_1x_4+x_1+x_2 \quad \text{formula \#3}$$

$$y_4=x_1x_2x_3+x_1x_3+x_1x_4+x_2x_4+x_2 \quad \text{formula \#4}$$

[0019] Formulas 5-8, shown below, show four example inputs x_1-x_4 that may be used with formulas 1-4.

$$x_1=0000000011111111 \quad \text{formula \#5}$$

$$x_2=0000111100001111 \quad \text{formula \#6}$$

$$x_3=0011001100110011 \quad \text{formula \#7}$$

$$x_4=0101010101010101 \quad \text{formula\#8}$$

[0020] Inputting the values for x_1-x_4 shown in formulas 5-8 into formulas 1-4 yields the values for signals y_1-y_4 shown in formulas 9-12 below.

$$y_1=0110010001010111 \quad \text{formula \#9}$$

$$y_2=0101001101110001 \quad \text{formula \#10}$$

$$y_3=0000111110010011 \quad \text{formula \#11}$$

$$y_4=0000101001101111 \quad \text{formula \#12}$$

[0021] If one calculated formulas 1-4 separately, starting from scratch each time, 18 multiplications (AND operations) and 16 additions (XOR operations) would be required. This would be inefficient because certain terms such as x_1x_3 and x_1x_4 appear more than once, and recalculating those terms would be a waste of resources, whether those resources were computer processor calculations or wasted space occupied by excess logic gates in a circuit.

[0022] The method **200** may be used to simplify formulas 1-4 and reduce a quantity of multiplications (AND operations) performed in formulas 1-4. In one example, the method **200** could be first applied to formula 4 for y_4. The initial formula 4 for y_4 (reproduced below) uses 5 multiplications and 4 additions. However it can be seen that formula 4 can be simplified by factoring out x_1x_3 from the first two terms as shown in formula 13 below, which only requires 3 multiplications and 4 additions (a reduction of 1 multiplication). The question then becomes whether y_4 can be processed using less than 3 multiplications.

$$y_4=x_1x_2x_3+x_1x_3+x_1x_4+x_2x_4+x_2 \quad \text{formula \#4}$$

$$y_4=(x_1x_3)(x_2+1)+(x_1+x_2)x_4+x_2 \quad \text{formula \#13}$$

[0023] To apply the method **200** to y_4, a polynomial (formula) to be simplified is obtained (step **202**), which in this case will be formula 4 for y_4. The formula is representative of one output of a non-linear portion of the combinational circuit.

[0024] A set K of known input signals x_1-x_4 is obtained (step **204**). Pairs of the input signals x_1-x_4 are added together to determine at least one sum using a computer (step **206**), and K is expanded to include the sums (step **208**) forming an expanded set K'. Because step **108** involves randomly chosen sums, the signals in K' at this point do not require any additional multiplications. Signals in the set K' are then multiplied to determine at least one product using the computer (step **210**), and K' is expanded to include the at least one product (step **212**). Steps **210-212** yield signals that require at most one more multiplication than the original set of known signals. Steps **206-212** are then selectively repeated (step **214**) until either a desired target signal is found, or a maximum number of multiplications is reached (which in the case of formula 4 this is 3 multiplications). A new formula may then be obtained (step **216**) and steps **206-214** may be selectively repeated for the new formula.

[0025] For y_4 the method **200** can yield the following simplified formula:

$$y_4=(x_1+x_2)(x_4+x_1x_3)+x_2 \quad \text{formula \#14}$$

[0026] A circuit specification is then generated (step **218**) including each addition performed in step **206** and each multiplication performed in step **210**, as shown above in formula 14. In one example, step **218** may include creating a set of short equations, or "straight line program," as shown in formulas 15-19 shown below. Although the term "straight line program" is used throughout this application, it is understood that a straight line program is just one type of a circuit specification. It is understood that other types of circuit specifications could be used, such as Verilog code.

$$t_1=x_1+x_2 \quad \text{formula \#15}$$

$$t_2=x_1 \cdot x_3 \quad \text{formula \#16}$$

$$t_3=x_4+t_2 \quad \text{formula \#17}$$

$$t_4=t_1 \cdot t_3 \quad \text{formula \#18}$$

$$y_4=x_2+t_4 \quad \text{formula \#19}$$

[0027] The improved formula 14 for y_4 requires only 2 multiplications and 3 additions, instead of 3 multiplications and 4 additions as shown in formula 13. Thus, although inputting the values of inputs x_1-x_4 into formula 4, formula 13 or formula 30 will yield the same result for y_4, formula 14 is the most efficient way to achieve this result. As described above, we know that it is not possible to compute y_4 using fewer than 2 multiplications, so once formula 30 is determined (which uses two multiplications) step **116** is complete with regards to y_4.

[0028] The method **200** may then be applied to formula 2 for y_2. Looking at formula 2 for y_2 (reproduced below) we see that formula 2 has a degree, or δ, of 3 (step **104**). So if we can compute y_2 using two multiplications the method **100** has succeeded.

$$y_2=x_1x_3x_4+x_1x_3+x_2x_3+x_2x_4+x_4 \quad \text{formula \#2}$$