

LOGIC OPERATION CIRCUIT, DIFFERENTIAL AMPLIFIER CIRCUIT, AND ELECTRONIC DEVICE

TECHNICAL FIELD

[0001] The application relates to the field of integrated circuits, and in particular to a logic operation circuit, a differential amplifier circuit, and an electronic device.

BACKGROUND

[0002] In recent years, with the rapid development of side-channel attacks, the security issues caused by vulnerabilities in integrated circuits have become increasingly significant. Edge-channel attacks, also known as side channel attacks, the core idea of the side-channel attacks is to analyze plaintext and key information by obtaining various leaked information generated during hardware operation. During hardware operation, there generates various leakage data mainly including variables such as power consumption, electromagnetic radiation, and temperature based on internal electrical level fluctuations within the chips. By analyzing these variables, data information inside the chip can be captured. With the development of mobile payments, more and more sensitive data is built on substrate chips. Although these sensitive data have been protected using encryption algorithms, the attackers can still perform side-channel analysis on the chip to obtain internal plaintext, keys, and other information. In addition, the side-channel attacks can also bring significant security risks to various electronic devices, especially AES (Advanced Encryption Standard) cryptographic devices.

[0003] In existing technology, an individual signal line is used for signal transmission, and the signal changes between 0/1, that the transmitted voltage on the signal line switches between high and low electrical levels. The changes of the level requires absorbing or releasing a large amount of charge, resulting in different physical data such as circuit power consumption, electromagnetic radiation, or temperatures. By analyzing these features, data information inside the chip can be obtained and vulnerable to side-channel attacks to side-channel attacks.

TECHNICAL PROBLEM

[0004] The application provides a logic operation circuit, a differential amplifier circuit, and an electronic device which can solve problems of side-channel attacks when using existing individual signal lines for signal transmission.

TECHNICAL SOLUTION

[0005] A logic operation circuit provided by the application includes at least one differential logic operation circuit, the differential logic operation circuit, includes a first logic network unit and a second logic network unit with functions complementarity to each other; a differential signal is composed of input signals of the first logic network unit and the second logic network unit, and is configured to implemented a preset logic function according to the input signals and output an operation result. The differential amplifier module, includes a first input end, a second input end, a first output end and a second output end, the first input end and the second input end are connected to an output ends of the first logic network and the second logic network respectively; the first output end and the second output end forms a differential output end to amplify the logic operation result and output a logic operation result.

[0006] Optionally, the differential amplifier module includes a differential amplifier unit electronically connected to the output end of the logical network module, and configured to amplify the operation result and output the logic operation result; a pre-charging unit connected to the differential amplifier unit, and configured to pre-charge the differential amplifier module for controlling a voltage of the differential output end to be a supply voltage during a pre-charging period, and a current source unit, connected to the differential amplified unit, and configured to establish a current path for the differential amplified unit during a evaluation period.

[0007] Optionally, the differential amplifier module further includes a storage unit, connected with output ends of the first logic network unit and a second network, and configured to store information.

[0008] Optionally, the differential amplifier module further Includes an absorbing unit connected to the storage unit, and configured to absorb excess electric charges

generated by the storage unit when a switch is switched.

[0009] Optionally, the storage unit further includes a first transistor, and a second transistor; gate ends of the first transistor and the second transistor are connected with a clock signal, drain ends of the first transistor and the second transistor are respectively connected with the output ends of the first logical network unit and the second logical network unit, and source ends of the first transistor and the second transistor are respectively connected with the first input end and the second input end.

[0010] Optionally, the absorbing unit includes a third transistor and a fourth transistor, when the third transistor and the fourth transistor are N-channel type transistors, a gate end of the third transistor is connected with a source end of the fourth transistor, a drain end of the third transistor is connected with the power supply voltage, a source end of the third transistor is connected with the first input end, a gate end of the fourth transistor is connected with the source end of the third transistor, a drain end of the fourth transistor is connected with a power supply voltage, a source end of the fourth transistor is connected with the second input end; when the third transistor and the fourth transistor are P-channel type transistors, the gate end of the third transistor is connected with the drain end of the fourth transistor, the source end the third transistor is connected with the power supply voltage, and the drain the third transistor is connected with the first input end; the gate end of the fourth transistor is connected with the drain end of the third transistor, the source end is connected with the power supply voltage, and the drain end of the fourth transistor is connected with the second end.

[0011] Optionally, the differential amplifier module includes at least one switch capacitance unit, connected with the current source unit, and configured to broaden output drive voltage ranges.

[0012] Optionally, the logic operation circuit has more than two differential logic operation circuits; an input end of one differential logic operation circuit is connected to an output end of the other differential logic operation circuit adjacent to the one differential logic operation circuit.

[0013] Optionally, the logic operation circuit further includes a clock buffer module connected between the differential logic operation circuits, and configured to control timing sequence s of the differential logic operation circuits.

[0014] A differential amplifier circuit includes at least one differential module, the at least one differential module includes a sub storage module with a differential input end, configured to receive and store input differential signals; a sub differential amplifier module with a differential output end connected with the sub storage module, and configured to output differential results based on the input differential signals; a sub pre-charging unit, connected to the sub differential amplifier module, and configured to pre-charge the sub differential amplifier module for controlling a voltage of the differential output end to be a supply voltage during a pre-charging period; a sub current source unit, connected to the sub differential amplifier module, and configured to establish a current path for the sub differential amplifier module during an evaluation period.

[0015] Optionally, the differential amplifier circuit includes an absorbing unit, connected to the sub storage module, and configured to absorb excess electric charges generated by the sub storage module when a switch is switched.

[0016] Optionally, the differential amplifier circuit further includes a first differential module, a first input end of the first differential module connected to a second output end of the second differential module, a second input of the first differential module connected to a first end of the second differential module, a first output end of the first differential module connected to a second input end of the second differential module, a second output end of the first differential module connected to a first input end of the second differential module.

[0017] A circuit for resisting side-channel attacks, includes the above described logic operation circuit.

[0018] An electronic device, includes the above described logic operation circuit.

[0019] Optionally, the differential amplifier module further includes the above described differential amplifier circuit .

[0020] In a third aspect, an electronic device provided includes a logic operation circuit, the logic operation circuit includes at least one differential logic operation circuit. The at least one differential logic operation circuit includes a logic network module, a differential amplifier module, and a differential amplifier module. The logic network module includes a first logic network unit and a second logic network unit with functions complementarity to each other; a differential signal generated based on input signals of the first logic network unit and the second logic network unit, the first logic network and the second logic network performs a pre-set logic function to output an operation result based on the input signals. The differential amplifier module includes a first input end, a second input end, and a first output end, and a second output end, the first input end and the second input end are connected to an output of the first logic network and the second logic network respectively; the first output end and the second output end forming a differential output end to amplify the logic operation result to obtain and output a logic operation result.

[0021] The logic operation circuit of the present invention comprises at least one differential logic operation circuit, wherein the differential logic operation circuit comprises: a logic network module and a differential amplifier module, wherein the logic network module comprises a first logic network unit and a second logic network unit with complementary logic functions. The input signals of the first logic network unit and the second logic network unit form a differential signal, and various preset logic functions can be achieved through the logic network module. Due to the weak output signal of the logic network module, the output result of the logic network module needs to be connected to a differential amplifier module for signal amplification and output the differential form of logic operation results. As the logic network module uses differential signals for signal transmission, the differential signal adopts positive and negative voltage differences between levels. To represent 0 and 1, the amplitude of the electrical level change is small, which makes changes of physical data such as circuit power consumption, electromagnetic radiation, or temperature be not obvious. That is, regardless of whether the transmitted information is 0 or 1, the physical quantities that

can be captured by the outside world are the same, making it difficult to obtain internal data information of the chip and preventing side-channel attacks, Improved data security. In addition, the use of logic network modules can achieve various logic functions, improving the logical complexity of the circuit. Due to the fact that logic network modules can use lower power supply voltages, the power consumption of the circuit is reduced; In addition, compared to using discrete devices to achieve logic functions, using dedicated logic network modules can reduce the number of components and optimize the chip area.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] In order to provide a clearer explanation of the technical solution in the embodiments of this disclosure, a brief introduction will be made to the accompanying drawings required in the description of the embodiments. It is evident that the accompanying drawings are only some embodiments of this disclosure. For those skilled in the art, other accompanying drawings can be obtained based on these drawings without creative labor.

[0023] FIG. 1 is a schematic diagram of a structure of a logic operation circuit in an embodiment of the present invention;

[0024] FIG. 2 is a schematic diagram of a structure of a differential logic operation circuit in an embodiment of the present invention;

[0025] FIG. 3 is a schematic diagram of a circuit structure of a logic operation circuit in an embodiment of the present invention;

[0026] FIG. 4 is a schematic diagram of a circuit structure of a logic operation circuit in an embodiment of the present invention;

[0027] FIG. 5 shows a two input XOR gate transmission calculation circuit of an embodiment of the present invention;

[0028] FIG. 6 shows a logic operation circuit with a switched capacitor unit in an embodiment of the present invention;

[0029] FIG. 7 is a circuit diagram of a cascaded differential logic operation circuit in an embodiment of the present invention;

[0030] FIG. 8 is a circuit diagram of a clock buffer module in an embodiment of the present invention;

[0031] FIG. 9 is a schematic diagram of a structure of a 16 bit carry ahead adder assembly in an embodiment of the present invention;

[0032] FIG. 10 is a schematic diagram of the structure of a differential amplification circuit in an embodiment of the present invention;

[0033] FIG. 11 is a schematic diagram of the circuit structure of a differential amplification circuit in an embodiment of the present invention;

[0034] FIG. 12 is a circuit diagram of an embodiment of the present invention that utilizes a differential amplification circuit to generate a differential clock signal.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0035] The following, combined with the accompanying drawings, provides a clear and complete description of the technical solution in the embodiments of this application. Obviously, the described embodiments are only a part of the embodiments of this application, not all of them. Based on the embodiments in this application, all other embodiments obtained by those skilled in the art without creative labor fall within the scope of protection in this application. Without conflict, the following embodiments and their technical features can be combined with each other.

[0036] Referring to FIG. 1, a schematic function module diagram of a logic operation circuit.

[0037] A logic operation circuit 200 includes at least one differential logic operation circuit 100. As shown in FIG. 2, the differential logic operation circuit 100 includes a logic network module 1 and a differential amplifier module 2.

[0038] The logic network module 1 includes a first logic network unit 11 and a second logic network unit 12 with functions complementarity to each other. An input signals IN of the first logic network unit 11 and an input signal $\overline{IN}$ of the second logic network unit 12 form a differential signal. A combination of transistors is applied as internal structures of the first logic network unit 11 and the second logic network unit 12, and different combinations of the transistors can be used to achieve different logic functions, such as “XOR” calculation, “AND not” calculation, “1-bit full” adder, “1-bit half” adder, or any other logic calculations capable of achieving different preset logic functions. The first logic network unit 11 and the second logic network unit 12 are located on both sides of the differential amplifier module 2. The circuit connection method is different from the Dynamic Current Mode Logic (DYCML) circuit with a logic circuit inside a charging and discharging unit, which can increase the complexity of the circuit.

[0039] The differential amplifier module 2 includes a first input end, a second input end, a first output end OUT, and a second output end $\overline{OUT}$. The first input end of differential amplifier module 2 and the second input end of differential amplifier module 2 are respectively connected to the output ends of the first logic network unit 11 and the second logic network unit 12. The first output end OUT and the second output end $\overline{OUT}$ constitute the differential output end, Differential amplifier module 2 is used to amplify the output operation results of the first logic network unit 11 and the second logic network unit 12, and output the logic operation results of the logic operation circuit 200.

[0040] Referring to FIG. 3, a schematic circuit diagram of the logic operation circuit.. The differential amplifier module 2 includes a current source unit 21, a pre-charging unit 22, and a differential amplification unit 23. The differential amplification unit 23 is connected to the output ends of the first logic network unit 11 and the second logic network unit 12 to amplify the operation result and outputting an amplifier logic operation result. The pre-charging unit 22 is connected to the differential amplification unit 23, to pre charge the differential amplification unit 23 for controlling voltage of the first output end OUT and the second output end $\overline{OUT}$ to be a power supply voltage VDD during a pre-charging period. The current source unit 21 is connected to the differential amplification unit 23 to establish a current path for the differential amplification unit 23 during an evaluation period. Specifically, the current source unit 21 includes a transistor M1, a transistor M2, and a capacitor C form the current source unit 21. The transistor M1 and the transistor M2 are N-channel MOSFETs, with a gate end of transistor M1 connected to a clock signal CLK, a source end connected to a drain end of the transistor M2 and one end of capacitor C, a gate end of the transistor M2 connected to the clock signal, and the phase of the clock signal is opposite to that of CLK. A source end of the transistor M2 and the other end of capacitor C are grounded, connected to GND. The pre-charging unit 22 includes a transistor M3 and a transistor M4. The transistor M3 and the transistor M4 are P-channel MOSFETs, and the clock

signal CLK is input to the gate of transistor M3. The source of transistor M3 is connected to the power supply voltage VDD, and the drain is connected to the first output end OUT; the clock signal CLK is input to the gate of transistor M4. The source of transistor M4 is connected to the power supply voltage VDD, and the drain is connected to the second output end. The pre-charging unit 22 is used to control the output voltage VDD of the first output end OUT and the second output end during the pre-charging period. Transistor M7 and transistor M8 form a differential amplification unit 23, which is used to amplify the operation results output by the first logic network unit 11 and the second logic network unit 12, and output the logic operation results. Transistor M7 and transistor M8 are N-channel MOSFETs. A gate terminal of the transistor M7 is connected to the output end of the first logic network unit 11, a drain end of the transistor M7 is connected to the drain of transistor M3, a source end of the transistor M7 is connected to the drain of the transistor M1, a gate end of the transistor M8 is connected to the output end of the second logic network unit 12, a drain end of the transistor M8 is connected to the drain end of transistor M4, and a source end of the transistor M8 is connected to the drain of the transistor M1. At the same time, the transistor M7 and transistor M8 also form a PDN (pull-down network) for transmitting and amplifying the voltage at the first output end OUT and the second output end $\overline{OUT}$.

[0041] The logic operation circuit in above embodiments includes at least one differential logic operation circuit, the differential logic operation circuit include the logic network module and the differential amplifier module, the logic network module includes the first logic network unit and a second logic network unit with logic functions complementary to each other, and the input signals of the first logic network unit and the second logic network unit form a differential signal, The various preset logic functions can be achieved through the logic network module. Due to the weak output signal of the logic network module, it is necessary to transmit the output result of the logic network module to the differential amplifier module for amplifying, and the differential logic operation results can be strong enough. As the logic network module uses differential signals for signal transmission, the differential signal uses

value 0 and 1 to present difference between positive and negative voltages of the electrical levels that a small amplitude changes of the electrical levels makes an inconspicuous changes of the physical data, such as, circuit power consumption, electromagnetic radiation, or temperatures, that further makes it difficult to obtain internal data information of the chip. Therefore, it prevents side-channel attacks and improves data security. In addition, compared to existing technologies that use circuits to implement simple logic functions inside differential circuits, the differential logic operation circuit sets the logic network module outside the differential amplifier module, separates various complex logic function logic network modules separately, and connects the various complex logic function logic network modules to the differential input of the differential amplifier module to achieve the logic function of the logic network module, which can perform more complex logical operations. Due to a common source and common gate structure composed of the internal logic operation network and PDN in typical differential circuits requiring higher power supply voltage to operate, the power consumption of the circuit is increased. However, in this embodiment, the logic network modules and differential amplifier module are separated, and the logic network module uses a voltage swing lower than the power supply voltage to reduce the power consumption of the circuit.

[0042] The calculation results of the logic network module in the logic operation circuit in the above embodiments are directly output and are not stored. Due to the requirement of storing intermediate information in the logic operation circuit to form a pipeline for improving computing power, in order to solve the problem of information storage, the differential amplification module 2 further includes a storage unit, which is connected to the output ends of the first logic network unit 11 and the second logic network unit 12 for information storage. In order to further minimize the channel charge injection effect, improve circuit speed, and reduce circuit power consumption, the differential amplification module 2 further includes an absorption unit, which is connected to the storage unit to absorb excess charges generated by the storage unit during switch switching. In order to stabilize the differential voltage output of the logic

operation circuit, the differential amplification module 2 of further includes a latch unit.

[0043] Referring to FIG. 4, a schematic circuit diagram of a logic operation circuit in accordance with a second embodiment is illustrated.

[0044] On the basis of FIG 3, the differential amplification module 2 of this embodiment further includes a latch unit, a storage unit, and an absorption unit.

[0045] As shown in Figure 4, a transistor M5 and a transistor M6 are P-channel MOSFETs, a first transistor M9, a second transistor M10, a third transistor M11, and a fourth transistor M12 are N-channel MOSFETs. The first transistor M9 and the second transistor M10 form the storage unit, and the third transistor M11 and the fourth transistor M12 form the absorption unit. The Transistor M5 and the transistor M6 form a latch. A gate end of the transistor M5 is connected to drain ends of the transistor M4 and transistor M6, a source end of the transistor M5 is connected to the power supply voltage VDD, a drain end of the transistor M5 is connected to the drain end of transistor M3 and a gate end of the transistor M6, and a source end of the transistor M6 is connected to the power supply voltage VDD. The latch unit is used to control the differential voltage between the first output end OUT and the second output end $\overline{OUT}$ during an evaluation period. At this point, a gate end of the transistor M7 is connected to a source end of the transistor M9, a drain end of the transistor M7 is connected to the drain end of the transistor M5, the source end of the transistor M7 is connected to the drain end of the transistor M1. A gate of the transistor M8 is connected to a source end of the transistor M10, a drain teminal of the transistor M8 is connected to the drain end of transistor M6, and a drain end source is connected to the drain end of the transistor M1. Gate ends of the first transistor M9 and the second transistor M10 are connected to the clock signal, a drain end is connected to the output ends of the first logic network unit 11 and the second logic network unit 12, and the source ends of the first transistor M9 and the second transistor M10 connected to the gate ends of the transistors M7 and M8, respectively. The first transistor M9 and the second transistor M10 control charges in the gate end of the transistor M7 and the transistor M8, achieving storing information

in the gates ends of the transistor M7 and the transistor M8. A gate end of the third transistor M11 is connected to a source end of the fourth transistor M12 and the source end of the second transistor M10, a drain end of the third transistor M11 connected to the power supply voltage VDD. A gate end of the fourth transistor M12 is connected to a source end of the third transistor M11 and a source end of the first transistor M9, a drain end of the fourth transistor M12 is connected to the power supply voltage VDD. The third transistor M11 and the fourth transistor M12 are respectively configured to absorb excess charges generated by the first transistor M9 and the second transistor M10 during switch switching. Using the third transistor M11 and the fourth transistor M12 to form the latch connection to optimize the charge injection effect of the first transistor M9 and the second transistor M10 channels. The channel charge injection refers to a phenomenon where the charges in the channel region flows into or out of the MOS switch at the moment when the MOS (metal oxide semiconductor) device is turned on or off, changing a voltage of a corresponding node and introducing errors. The optimization of channel charge injection effects in the first transistor M9 and the second transistor M10 can improve circuit speed and reduce circuit power consumption. The third transistor M11 and the fourth transistor M12 can be N-type transistors or P-type transistors. When the third transistor M11 and the fourth transistor M12 are P-type transistors, the gate end of the third transistor M11 is connected to the drain end of the fourth transistor M12, the source end of the third transistor M11 is connected to the power supply voltage, and the drain end of the third transistor M11 is connected to the gate of transistor M7. The gate end of the fourth transistor M12 is connected to the drain end of the third transistor M11, the source end of fourth transistor M12 is connected to the power supply voltage, and the drain of the fourth transistor M12 is connected to the gate of transistor M8.

[0046] The operation of the logic operation circuit in FIG. 4 is divided into a pre-charging period and an evaluation period. The process is as follows: during the pre-charging period, the clock signal CLK is at a low level, the clock signal is at a high level, the transistor M3 and the transistor M4 are conducting in the pre-charging unit,

the first output end OUT and the second output end $\overline{OUT}$ output power voltage VDD, and the first transistor M9 and the second transistor M10 are conducting, the output results of the first logic network unit 11 and the second logic network unit 12 are stored at the gate ends of transistor M7 and transistor M8, respectively. The third transistor M11 or the fourth transistor M12 conduct and absorb the excess charge generated by the switch of the first transistor M9 or the second transistor M10. At this point, the transistor M2 conducts, causing the charge on capacitor C to be released to ground GND. Meanwhile, the transistor M1 is turned off, and a current path between the power supply voltage VDD and ground GND is turned off. In the evaluation period, the clock signal CLK is at a high level and the clock signal is at a low level. In the pre-charging unit, the transistor M3 and the transistor M4, the first transistor M9, the second transistor M10, the third transistor M11, and the fourth transistor M12 are turned off. In the current source unit, the transistor M1 conducts, the capacitor C forms a virtual ground, the transistor M7 or the transistor M8 also conducts, and the first output end OUT and the second output end $\overline{OUT}$ to ground GND form a current path. Due to different impedances in the current paths of the first output end OUT and the second output end $\overline{OUT}$, there may be a situation that one output voltage drops faster than the other. At this point, the transistor M5 and the transistor M6 in the latch unit will help balance the circuit. When the output voltage drops to a certain extent, the transistor M5 or the transistor M6 will conduct to allow the output voltage to return to the power supply voltage VDD.

[0047] It can be understood that the logic operation circuit of this embodiment is divided into the pre-charging period and the evaluation period. The first transistor M9 and the second transistor M10 are configured to control the storage of information to the gate ends of the transistors M7 and M8. In the evaluation period, the function of the third transistor M11 and the fourth transistor M12 is to eliminate the harmful effects of the channel charge injection in the first transistor M9 and the second transistor M10, and utilize the beneficial effects. Due to the elimination of the channel charge injection

effect of the first transistor M9 by the third transistor M11, and the elimination of the channel charge injection effect of the second transistor M10 by the fourth transistor M12, the first transistor M9 and the second transistor M10 need to store one low level and the other high level. The benefits of the channel charge injection effect are retained at the gate ends with low levels, the defect of channel charge injection effect is eliminated by the third transistor M11 or the fourth transistor M12, so the transconductance difference of the PDN network is retained, which affects the output result. The function of transistor M3 and the transistor M4 is to control the output level back to VDD during the pre-charging period. The function of the transistor M1 and the transistor M2 is to perform logical operations by flowing electrons from the capacitor C into the logic network module during the evaluation period. During the pre-charging period, the capacitor C is discharged to release electrons to the ground. The main function of the transistor M5 and the transistor M6 is to maintain the output state during the evaluation period. In addition, the first output end OUT and the second output end $\overline{OUT}$ of the logic operation circuit in this embodiment will not have full swing, resulting in lower circuit power consumption and wider applicability.

[0048] The transistors in FIG. 4 can be partially or entirely P-type or N-type transistors. In addition, the current source unit 21 is a charge pump or any circuit that can achieve charge transfer function. Due to the fact that the transistor M1, the transistor M2, and the capacitor C are configured to provide a charge transport pathway, the charge pump in the field of integrated circuits can achieve the same function. Therefore, the capacitor C itself can be replaced by MOS commonly used in the field of integrated circuits, or implemented using MIM (metal capacitors), or special processes can be used to implement capacitors inside the chip, or capacitors can be specifically placed on another chip, and connect to the current source unit 21 by through-holes or other bonding wires on the chip to replace the capacitor C. In order to achieve two input XOR gate transmission calculation, a new technical solution is proposed based on the above embodiments.

[0049] Referring to FIG. 5, another embodiment of the present invention's two-input XOR gate transmission calculation circuit is shown.

[0050] The two-input XOR gate transmission calculation circuit of this embodiment is an instantiation formed by replacing the first logical network unit 11 and the second logical network unit 12 in FIG. 4 with the preset XOR logic function, which can complete the two input XOR function. In FIG. 5, the transistor M13 and the transistor M15 form the first XOR unit 110, the transistor M14 and the transistor M16 form the second XOR unit 120. The transistor M13, the transistor M14, the transistor M15, and the transistor M16 are all N-channel MOSFETs. A gate end of the transistor M13 is connected to the input signal, a drain end of the transistor M13 is connected to an input signal B, a source end of the transistor M13 is connected to the drain end of the first transistor M9, A gate end of the transistor M14 is connected to an input signal A, and a drain end of the transistor M14 is connected to an input signal $\overline{B}$, a source end of the transistor M14 is connected to the drain end of the first transistor M9, the gate end of the transistor M14 is connected to an input signal $\overline{A}$, the drain end of the transistor M14 is connected to the input signal $\overline{B}$, the source end of the transistor M14 is connected to the drain end of the second transistor M10, a gate end of the transistor M16 is connected to the input signal A, the drain end of the transistor M16 is connected to the input signal B, and the source end of the transistor M16 is connected to the drain end of the second transistor M10. The input signals A and B are the two input signals of the XOR gate. This embodiment can achieve the operation function of A XOR and B, and can store and complete the operation together. The logic operation circuit can preferably omit the first transistor M9 and the second transistor M10 to achieve a differential calculation circuit without storage function. It should be noted that by replacing the logical network module with any network capable of completing calculations, different logical calculation functions can be achieved.

[0051] The logic operation circuit of the above embodiment can achieve the calculation of logic functions and information storage, but when cascaded with other

circuits, the range of driving voltage provided by the current source unit is narrow. In order to increase the range of driving voltage of the next level circuit when cascading logical operation circuits, the present invention provides a new technical solution.

[0052] Referring to FIG. 6, another embodiment of the present invention's logic operation circuit with a switched capacitor unit is shown.

[0053] The differential amplification module in the logic operation circuit with a switched capacitor unit in this embodiment further includes at least one switched capacitor unit connected to the current source unit for increasing the range of output driving voltage. As shown in FIG. 6, the switch capacitor unit includes a transistor M17 and a transistor M18, which are N-channel transistors. At this point, one end of the capacitor C in the current source unit is connected to the drain end of the transistor M2, the other end of the capacitor C is connected to a drain end of the transistor M18, a gate end of the transistor M17 is connected to the clock signal, the drain end of the transistor M17 is connected to the power supply voltage VDD, a source end of the transistor M17 is connected to a drain end of the transistor M18, a gate end of the transistor M18 is connected to the clock signal CLK, and a source end of the transistor M18 is connected to ground GND. By adding switch capacitor units, a capacity of capacitor C can be reduced, an area of capacitor C can be reduced, and a range of driving voltage output from the source of transistor M1 can be wider.

[0054] The logic operation circuit of the above embodiments is only a separate circuit, and the logic functions implemented by the logic operation circuit are relatively simple. In order to achieve more complex circuit logic functions, a new technical solution is further proposed based on the above embodiments. The new technical solution can solve cascading problems of logic operation circuits, increase the complexity of the logic operation circuit, and meet the timing requirements between two logic operation circuits.

[0055] Referring to FIG. 7, a circuit diagram of a cascaded differential logic operation circuit in another embodiment of the present invention is shown.

[0056] The logic operation circuit of this embodiment includes two or more

differential logic operation circuits; in adjacent differential logic operation circuits, an output end of one differential logic operation circuit is connected to an input end of the other differential logic operation circuit to achieve cascading and increase the complexity of the circuit. Due to the high requirements for timing between logic circuits, in order to ensure that a timing sequence between cascaded logic operation circuits meets the requirements, the logic operation circuit in this embodiment further includes a clock buffer module connected between the differential logic operation circuits for controlling the timing sequential relationship between different differential logic operation circuits.

[0057] Specifically, as shown in FIG. 7, the logic operation circuit includes two differential logic operation circuits of a differential logic operation circuit 101 and a differential logic operation circuit 102. A first output end OUT and a second output end $\overline{OUT}$ of differential logic operation circuit 101 are respectively connected to the input end IN and $\overline{IN}$ corresponding to the differential logic operation circuit 102 to achieve cascading of the differential logic operation circuit 101 and the differential logic operation circuit 102. The logical network modules are connected based on the calculation relationship between the front and back stages of the logical network modules. According to timing requirements, they can be connected to the next stage through clock buffer module 103.

[0058] The clock buffer module 103 in FIG. 7 is shown in FIG. 8. A transistor M21, a transistor M24 are P-channel transistors, the transistor M22, the transistor M23, and the transistor M25 are all N-channel MOSFETs. A gate end of transistor M21 is connected to the clock signal CLK, a source end of transistor M21 is connected to the power supply voltage VDD, the drain end of transistor M21 is connected to a drain end of transistor M22, a gate of transistor M22 is connected to the signal EOE (evaluation end signal), and the source end of transistor M22 is connected to a drain end of transistor M23, The gate end of of the transistor M23 is connected to the clock signal CLK, the source end of the transistor M23 is grounded, a gate end of the transistor M24 is

connected to the drain end of transistor M21, a source end of the transistor M24 is connected to the power supply voltage VDD, a drain end of the transistor M24 is connected to a drain end of the transistor M25, a gate end of the transistor M25 is connected to the clock signal, a source end of the transistor M25 is grounded, and the drain end of the transistor M25 outputs signal SE(starting evaluation), and is connected to the gate end of transistor M19 in the differential logic operation circuit 102. In the pre-charging period, a EOE node voltage of clock buffer module 103 is 0. At the beginning of the evaluation period, the capacitor C begins to charge, and the EOE node outputs a high level to drive the differential logic operation circuit 102.

[0059] A core technical point of a connection method of the differential logic operation circuit in FIG.7 is to form the logic calculation module by N-type transistors. When the logic network module is used to calculation, using N-type transistors will improve the power consumption delay product, which is more advantageous than typical CMOS or complementary logic. In other embodiments, the logic network module may also use P-type transistors or transfer gate logic. The logical network module can be divided, arranged, and combined according to specific calculations to achieve various functions. It should be noted that CLK signals are required between the differential logic operation circuits in FIG. 7 to control the timing sequential relationship. A time of beginning evaluating and pre-charging is determined by an exact order of arrivals of the clock signals. If a phase difference between CLKs can ensure that the timing sequence meets the design requirements, the clock buffer module 103 in FIG. 7 can be omitted. If the differential logic operation circuit between the upper and lower stages needs close timing coordination and there is a close timing sequential relationship between the logics, the clock buffer module 103 in FIG. 8 needs to be used to meet the timing requirements. The differential logic operation circuits 101 can also be directly connected from the clock source to the differential logic operation circuit 102. In other optional implementations, the timing sequential relationship between different differential logic operation circuits can be controlled, and different phase-difference clocks can be connected between the differential logic operation circuit 101

and the differential logic operation circuit 102 to achieve correct timing sequence between the differential logic operation circuit 101 and the differential logic operation circuit 102. The differential logic operation circuit 101 and differential logic operation circuit 102 can cooperate with each other to produce correct calculation results, improved the accuracy of the calculation results.

[0060] The above embodiments can achieve cascading of logical operation circuits and improve the logical complexity of the circuit. The present invention provides an embodiment of implementing an adder using the above embodiments.

[0061] Referring to FIG. 9, another embodiment of a 16 bit carry look ahead adder assembly of the present invention is shown.

[0062] The 16 bit carry ahead adder assembly in this embodiment consists of four sets of 4 bit carry ahead adders, which are implemented using the differential logic operation circuits. The logic network module of the 16 bit carry ahead adder assembly is determined by logics of a specific carry generation signal G and a specific carry transmission signal P. The specific calculation logic is:

[0063] $G = G_3 + P_3G_2 + P_3P_2G_1 + P_3P_2P_1G_0$

[0064] Wherein, G_0 , G_1 , G_2 , and G_3 are the carry generation signals of the 4-bit carry ahead adders from low to high, P_0 , P_1 , P_2 , and P_3 are the carry transmission signals of the 4-bit carry ahead adders from low to high, respectively, and G is a bit generation signal of the 16 bit carry ahead adder assembly.

[0065] This embodiment can use a plurality of the differential logic operation circuits to implement an adder with more bits, but is not limited to the above examples.

[0066] The present invention also provides a differential amplification circuit, which includes at least one differential module. The differential amplification circuit of this embodiment includes a differential module, as shown in FIG. 10. The differential module includes a sub storage module 31, a sub differential amplifier module 32, a sub pre-charged electronic module 33, and a sub current source module 34.

[0067] The sub storage module 31 includes a differential input end to store the input differential signal during the pre-charging period, and to input the differential signal to

the sub differential amplifier module 32; the sub differential amplification module 32 includes a differential output end, connected to the sub storage module 31 to output the differential results based on the differential signal; the sub pre -charging electronic module 33 is connected to the sub differential amplifier module 32, to pre-charge the sub differential amplifier module to control a voltage of the differential output end to be the power supply voltage during the pre-charging period; the sub current source module 34 is connected to the sub differential amplifier module 32 to establish a current path for the differential amplifier unit during the evaluation period.

[0068] The differential amplification circuit of this embodiment can achieve information storage by adding a sub storage module 31. This differential module is connected to other circuit modules and can achieve differential transmission of signals, making changes of the physical data, such as, circuit power consumption, electromagnetic radiation, or temperatures, be not significant., and making it difficult to obtain data information inside the chip, preventing the side-channel attacks, and improving data security. In addition, as the functions of integrated circuits become increasingly complex and module integration increases, various complex logic functions can be achieved by adding storage functions to facilitate connection with other modules.

[0069] The differential amplification circuit of the above embodiment can achieve information storage. In order to further improve circuit speed and reduce circuit power consumption, the present invention provides a new technical solution to optimize the sub storage module 31.

[0070] Specifically, as shown in FIG. 11, the differential amplification circuit of this embodiment include a capacitor C1, a transistor M41, a transistor M42, a transistor M43, a transistor M44, a transistor M45, a transistor M46, a transistor M47, a transistor M48, a transistor M49, a transistor M50, a transistor M51, a transistor M52, a power supply voltage VDD, and ground GND. Wherein, the transistor M41, the transistor M42, the transistor M47, the transistor M48, the transistor M49, the transistor M50, the transistor M51, and the transistor M52 are N-channel MOS transistors, the transistor

M43, the transistor M44, the transistor M45, and the transistor M46 are P-channel MOS transistors, the transistor M49 and the transistor M50 form a sub storage module. Gate ends of the transistor M49 and the transistor M50 are connected to the clock signal $\overline{CLK}$, drain ends of the transistor M49 and the transistor M50 are connected to the differential input signal IN and $\overline{IN}$, and source ends of the transistor M49 and the transistor M50 are connected to gate ends of the transistor M47 and the transistor M48, respectively. The transistors M49 and M50 control the charges stored in gate ends of the transistors M47 and M48, enabling information to be stored in the gate ends of transistors M47 and M48.

[0071] The transistor M47 and transistor M48 form the sub differential amplifier module 32, which is configured to amplify the input differential signal IN and $\overline{IN}$. A gate end of the transistor M47 is connected to the source of the transistor M49, a drain end of the transistor M47 is connected to the drain of the transistor M45, a source end of the transistor M47 is connected to a drain end of the transistor M41, a gate end of the transistor M48 is connected to a source end of the transistor M50, a drain end of the transistor M48 is connected to a drain end of a transistor M46, and a source end of the transistor M48 is connected to a drain end of the transistor M41. At the same time, the transistor M47 and the transistor M48 also form the PDN, which are used for transmitting and amplifying voltages of output nodes, respectively.

[0072] The transistor M43 and transistor M44 form a sub pre-charged module 33. The clock signal CLK is input to a gate end of the transistor M43, a source end of the transistor M43 is connected to the power supply voltage VDD , and a drain end is connected to the first output end OUT ; the clock signal CLK is input to a gate end of the transistor M44. A source end of transistor M44 is connected to the power supply voltage VDD , and a drain end of the the transistor M44 is connected to the second output end. The pre-charging unit is configured to control the first output end OUT and the second output end to output the power supply voltage during the pre-charging period.

[0073] The transistor M41, the transistor M42, and the capacitor C1 form the sub

current source module 34. A gate end of the transistor M41 is connected to the clock signal CLK, and a source end is connected to a drain end of the transistor M42 and one end of the capacitor C1. A gate end of the transistor M42 is connected to the clock signal $\overline{CLK}$, and the clock signal $\overline{CLK}$ forms the opposite signal to CLK. A source end of the transistor M42 and the other end of capacitor C1 are grounded to GND.

[0074] The transistor M45 and the transistor M46 form a sub latch module 35. A gate end of the transistor M45 is connected to drain ends of the transistor M44 and transistor M46, a source end of the transistor M45 is connected to the power supply voltage VDD, a drain end of the transistor M45 is connected to the drain end of the transistor M43 and a gate of the transistor M46, and a source end of the transistor M46 is connected to the power supply voltage VDD. The sub latch module is configured to control the differential voltage between the first output end OUT and the second output end $\overline{OUT}$ during the evaluation period.

[0075] The operation of the differential amplification circuit in FIG. 11 is divided into the pre-charging period and the evaluation period. The principle and working process are similar to the differential logic operation circuit in FIG. 4, and will not be repeated here.

[0076] Referring to FIG. 12, a circuit diagram of another embodiment of the present invention that utilizes a differential amplification circuit to generate a differential clock signal.

[0077] The circuit diagram of this embodiment shows using a differential amplification circuit to generate a differential clock signal, the differential amplification circuit includes a first differential module 321 and a second differential module 322. The first input end IN1 of the first differential module 321 is connected to the second output end $\overline{OUT2}$ of the second differential module 322, the second input end $\overline{IN1}$ is connected to the first output end OUT2 of the second differential module 322, and the first output end OUT1 is connected to the second input end $\overline{IN1}$ of the second differential module 322, the second output end $\overline{OUT1}$ is connected to the first input

end IN2 of the second differential module 322, which is used to implement a differential clock signal.

[0078] The present invention also provides a circuit for resisting side-channel attacks, including the aforementioned logic operation circuit. By using the above logic operation circuit, changes of the physical data, such as, circuit power consumption, electromagnetic radiation, or temperature are not significant, making it difficult to obtain internal data information of the chip, preventing side-channel attacks, and improving data security. In addition, the use of logic network modules can achieve various logic functions, improving the logical complexity of the circuit. Due to the fact that logic network modules can use lower power supply voltages, the power consumption of the circuit is reduced.

[0079] The present invention also provides an electronic device including the aforementioned logic operation circuit or differential amplification circuit, such as a mobile phone, a tablet computer, a power amplifier, etc. By using the aforementioned logic operation circuit or differential amplification circuit, the physical data such as circuit power consumption, electromagnetic radiation, or temperature changes are not obvious, making it difficult to obtain internal data information of the chip, preventing side-channel attacks, and improving data security. In addition, the use of logic network modules can achieve various logic functions, which can be used to achieve more complex logic operations. Due to the fact that logic network modules can be driven by lower voltage, circuit power consumption is reduced.

[0080] That is to say, the above is only an embodiment of the present application and does not limit the scope of the patent of the present application. Any equivalent structure or equivalent process transformation made using the description and drawings of the present application, such as the combination of technical features between various embodiments, or direct or indirect application in other related technical fields, are equally included in the scope of patent protection of the present application.

CLAIMS

1. A logic operation circuit, comprising at least one differential logic operation circuit, the differential logic operation circuit comprising:

a logic network module, comprising a first logic network unit and a second logic network unit with functions complementarity to each other; a differential signal being composed of input signals of the first logic network unit and the second logic network unit, and configured to implement a preset logic function according to the input signals and output an operation result;

a differential amplification module comprising a first input end, a second input end, a first output end and a second output end, the first input end and the second input end being respectively connected to output ends of the first logic network unit and the second logic network unit, and a differential output end being composed of the first output end and the second output end and being configured to amplify the operation result and outputting a logic operation result.

2. The logic operation circuit of claim 1, wherein the differential amplifier module comprises:

a differential amplifier unit electronically connected to the output end of the logic network module, and configured to amplify the operation result and output the logic operation result;

a pre-charging unit connected to the differential amplifier unit, and configured to pre-charge the differential amplifier module for controlling a voltage of the differential output end to be a supply voltage during a pre-charging period, and

a current source unit, connected to the differential amplified unit, and configured to establish a current path for the differential amplified unit during an evaluation period.

3. The logic operation circuit of claim 2, wherein the differential amplifier module further comprises a storage unit, connected with output ends of the first logic network unit and a second network, and configured to store information.

4. The logic operation circuit of claim 3, wherein the differential amplifier module further comprises;

an absorbing unit connected to the storage unit, and configured to absorb excess electric charges generated by the storage unit when a switch is switched.

5. The logic operation circuit of claim 3, wherein the storage unit further comprises:

a first transistor, and a second transistor;

gate ends of the first transistor and the second transistor are connected with a clock signal, drain ends of the first transistor and the second transistor are respectively connected with the output ends of the first logical network unit and the second logical network unit, and source ends of the first transistor and the second transistor are respectively connected with the first input end and the second input end.

6. The logic operation circuit of claim 4, wherein the absorbing unit comprises:

a third transistor and a fourth transistor,

when the third transistor and the fourth transistor are N-channel type transistors, a gate end of the third transistor is connected with a source end of the fourth transistor, a drain end of the third transistor is connected with the power supply voltage, a source end of the third transistor is connected with the first input end, a gate end of the fourth transistor is connected with the source end of the third transistor, a drain end of the fourth transistor is connected with a power supply voltage, a source end of the fourth transistor is connected with the second input end;

when the third transistor and the fourth transistor are P-channel type transistors, the gate end of the third transistor is connected with the drain end of the fourth transistor, the source end the third transistor is connected with the power supply voltage, and the

drain the third transistor is connected with the first input end; the gate end of the fourth transistor is connected with the drain end of the third transistor, the source end is connected with the power supply voltage, and the drain end of the fourth transistor is connected with the second input end.

7. The logic operation circuit of claim 2, wherein the differential amplifier module further comprises:

at least one switch capacitance unit, connected with the current source unit, and configured to broaden output drive voltage range.

8. The logic operation circuit of claim 1, wherein the logic operation circuit has more than two differential logic operation circuits;

an input end of one differential logic operation circuit is connected to an output end of the other differential logic operation circuit adjacent to the one differential logic operation circuit.

9. The logic operation circuit of claim 1, further comprising:

a clock buffer module connected between the differential logic operation circuits, and configured to control timing sequence s of the differential logic operation circuits.

10. A differential amplifier circuit, comprising at least one differential module, the at least one differential module comprising:

a sub storage module with a differential input end, configured to receive and store input differential signals;

a sub differential amplifier module with a differential output end connected with the sub storage module, and configured to output differential results based on the input differential signals;

a sub pre-charging unit, connected to the sub differential amplifier module, and configured to pre-charge the sub differential amplifier module for controlling a voltage

of the differential output end to be a supply voltage during a pre-charging period, and
a sub current source unit, connected to the sub differential amplifier module, and
configured to establish a current path for the sub differential amplifier module during
an evaluation period.

11. The differential amplifier circuit of claim 10, further comprising:

an absorbing unit, connected to the sub storage module, and configured to absorb
excess electric charges generated by the sub storage module when a switch is switched.

12. The differential amplifier circuit of claim 10, further comprising a first differential
module, a first input end of the first differential module connected to a second output
end of the second differential module, a second input of the first differential module
connected to a first end of the second differential module, a first output end of the first
differential module connected to a second input end of the second differential module,
a second output end of the first differential module connected to a first input end of the
second differential module.

13. An electronic device, comprising a logic operation circuit of claim 6.

14. The electronic device of claim 13, further comprising a differential amplifier
circuit of claim 11.