Encrypt ECG signals based on the optimized 4-bit absolute value comparator

Lixuan Xu *

Electronic Engineering School, Hangzhou Dianzi University, Hangzhou, 310018, China

* Corresponding Author Email: 21158134@hdu.edu.cn

Abstract. As people become more conscious of private information security and advancements in Electrocardiogram (ECG) identity identification technology, the need to encrypt private data intensifies. New wearable medical devices continuously gather vast amounts of personal health data, underscoring the urgency of safeguarding privacy. This paper focuses on encrypting and decrypting rich characteristic signals like ECG. It delves into the core aspects, including the logic circuit diagram of a four-bit digit absolute comparator using Complementary Metal Oxide Semiconductor (CMOS) technology and optimizing delay through logic effort to reduce power consumption. XOR gates and other gate circuits, as well as complement subtraction principles, are employed in building logic gates. Calculating delay involves selecting the longest critical path and determining the specific parameters (g, h, and p) for each logic gate. Subsequently, energy consumption is computed using a formula, revealing a trade-off between energy and delay. After optimization, the circuit's energy consumption is 184.832, and the delay is 34.13. In summary, the 4-bit absolute value detector plays a crucial role in encryption, addressing the growing concern for privacy and data security.

Keywords: ECG; logic effort; CMOS, energy consumption; delay.

1. Introduction

With the improvement of social medical level and the gradual improvement of modern people's awareness of personal privacy, the accuracy and confidentiality of ECG signal measurement indicators are increasing day by day. ECG signals are rich in practical reference data and feature-rich data [1]. These feature-rich data make encryption more necessary and the encryption characteristics are more recognizable, which is convenient for fast decoding in the future. And because once the ECG distribution or the slope of the wave line be known, it is equivalent to roughly knowing the specific situation of a person's ECG [2]. These ECG characteristics can be a biometric for identifying people [3].

Based on the comparison principle of absolute threshold comparator, this paper encrypts a positive or negative number and splits and decrypts the dichotomy of a given range. It uses logic gate circuits to build three types of logic circuits, such as full adder, half adder and comparator. The core is a positive or negative four-bit binary subtracter. The core idea is to compare the highest digit of the last four digits of the binary number to determine whether the final output is greater than 1 or 0. It is worth noting that all four bits entered here are entered in the form of a complement. Finally, they are integrated together to get a complete circuit diagram with only the gate circuit, and then the logic effort constant g and parasitic constant p, branch constant b of all the logic gates in the circuit diagram are calculated one by one, and then pick a longest line to calculate the delay of the whole circuit, and calculate the corresponding Vdd through the shortest delay and the delay after sizing. Then the corresponding energy consumption is obtained, and the one-to-one correspondence between each kind of energy and each kind of delay is compared, and the difference between each kind of delay or energy is obtained. In other words, because of the high characteristics of the ECG, in today's identity identification, identifying a person's identity information through the ECG principle has become more and more common. Therefore, encrypting highly characteristic signals such as ECG can effectively protect user privacy.

2. Working principle of ECG signal and its application

2.1. The definition of the ECG signal

Electrocardiography is a type of Bio-electrical signal that was previously invented and widely used in clinical medicine. To a certain extent, it can present information about the running state of the human heart and stable internal properties, and it has been widely employed and mature in the diagnosis of bedside cardiovascular disorders [2]. Not only can the ECG signal be diagnosed for the medical use but also it has many characteristics which can be used for encryption and decoding.

2.2. The main characteristic of the ECG signal

The electrocardiograph is a powerful measuring tool and the essential component of its verification. As a tool, for example, the diagnostic process for patients with suspected AMI frequently includes an ECG.ST elevation, ST depression, and T-wave alterations are the more typical ECG signs of AMI [4]. Although the graphic of the ECG signals are complex, there are numerous characteristic waveform, but in the analysis of ECG signals, only the ECG waveform is required, which can be accomplished well by taking several fundamental characteristic waveform [5]. Furthermore, this distinct waveform has a set time alignment. This greatly simplifies the study and calculation of ECG waveform. Once the graphic of someone's ECG graphic is gained. The methods of Subpixel edge positioning can be used to extract the original picture to a higher resolution picture which greatly enhance the accuracy of parameter calculation [5]. The so-called Subpixel edge positioning is a method which greatly simplify the calculation and the graphic and derive more reliable data. Once the main characteristic data is gained. The Encryption and decryption of the ECG signal procession can be started. For example the most noticeable characteristic of the ECG signal supposed to be the QRS complex. The most crucial step in automatic ECG data analysis is the detection of the QRS complex. After the QRS complex has been located, the ECG signal can be examined in greater depth to look at the heart rate, ST segment, and other details [6]. The signal properties of the QRS complex, such as amplitude, breadth, QRS energy, can be extracted and to be enciphered or decoded [7]. The slope of a QRS wave can be negative and the amplitude of the QRS can be positive. So from this point on, the logic of the absolute value detector can be applied to manage the encryption process. The primary feature of the ECG signal is displayed below in Fig. 1.

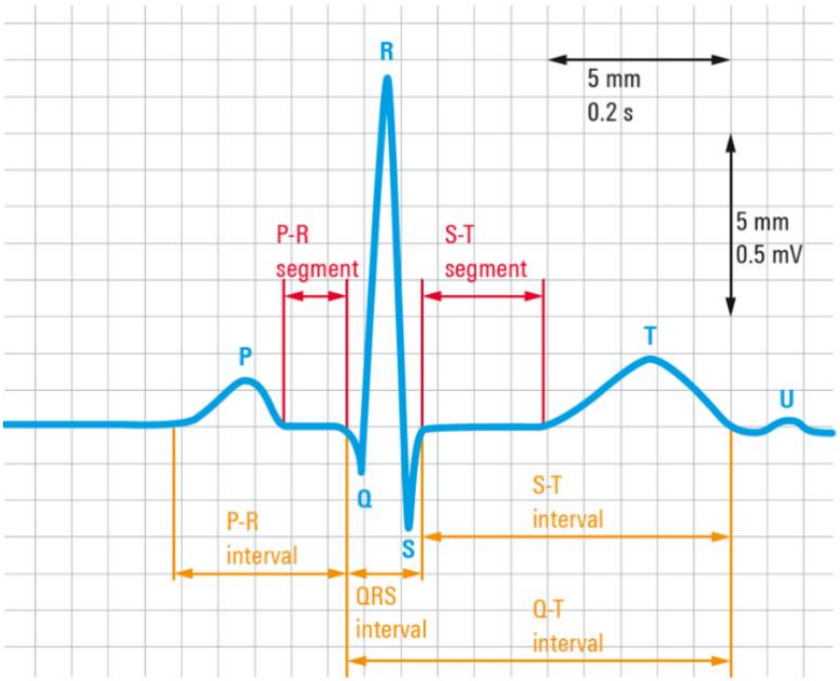


Fig 1. The ECG signal's main feature.

2.3. Absolute value Encryption transmission and decoding of the ECG signal

For absolute value encryptors, the principle must be about absolute value encryption, such as an integer, which is a certain indicator or parameter describing the electrocardiogram, such as the QRS parameter, absolute value encryption can be used to encrypt this parameter, give an interval, for example, the parameter is 68, and then constantly set a threshold. And then to divide 100,50,25, to keep approaching this number, 1 is greater than the threshold, 0 is less than the threshold, the threshold can be understood as a given binary fraction, transmission is the shortest path mentioned later, so as to obtain the least energy and relatively short delay. The final decoding is the inverse process of encryption, and the final value can be obtained by backward inference given an interval.To be more specific, if a range of 1-100 is given, and then divide this range into 1-50 and 50-100, output 1 if the integer is greater than 50, output 0 if it is less than 50, for example 68, the first number is 1, and so on, the second number is 50-75 and 75-100, and obviously the second number is 0. The third number is 50-62 and 63-75, which becomes 1 again, and then 63-69, which is 0, and then 63-66 and 67-69, and obviously 68 fits into the 67-69 interval so it's 1, and finally when 68 and 68 coincide the output becomes 0 and the encryption ends and gets 101010.

3. The principle of the absolute value detector and application

3.1. Definition of 4-Bit absolute value detector

The four-bit absolute value threshold comparator can be used to encrypt and decrypt ECG signals, which is the core of logical comparison in ECG encryption. With the logic that the absolute value is 1 when it is greater than the threshold value, and 0 when it is less than the threshold value, specific integers can be encoded to achieve an encryption effect. For example, if the input of the threshold is 0001 which means 0001 is the number which refers to 1. And if the input is 1011,it’s undoubted that the absolute value of the -3 is 3 which is much more bigger than 1.So the output is 1 which means -3’s absolute value is bigger than 1.

3.2. The composition and top-level logic of a four-bit absolute value comparator

Due to the removal of many cumbersome and unnecessary functions, it saves a lot of power consumption and reduces the delay. Finally, the effect that 1 is greater than the threshold value and 0 is smaller than the threshold value. But it is worth noting that behind the simplification is actually a completely different idea, in the design of the circuit shown in the following figure, the use is a completely different from the previous shunt processing idea, but cleverly integrated. The circuit can also be divided into three parts: the input side, the high level comparator (using the principle of subtracter to achieve) and the full adder part when the input number is positive or negative. The settings of the full adder of one-bit are placed at the very beginning, consisting of an IS-OR gate and an and-gate and an XOR gate, as shown in the Fig.2 below.

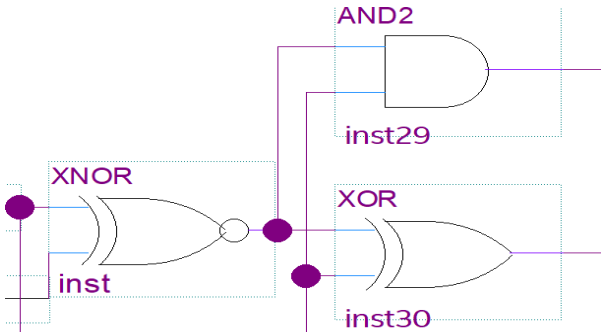


Fig 2. The full adder of one-bit.

The whole idea of this circuit is the subtracter, because the subtracter can achieve the ratio of two numbers, so it is often used to compare the size. When the input value is positive or negative, A-B is equivalent to A+B '+1, when the reduction is negative, the highest digit 0/1 is extracted, and then the

remaining three digits, if it is positive, it is directly taking the inverse and add one, if it is negative, take the last three digits as his complement (the complement of negative number is the inverse code +1). In the final analysis, the inverse code or complement adds one, and the complement of positive and negative numbers needs to be the inverse code plus one at the end, and then the result 1/0 is obtained in the comparator shown in Fig.3.

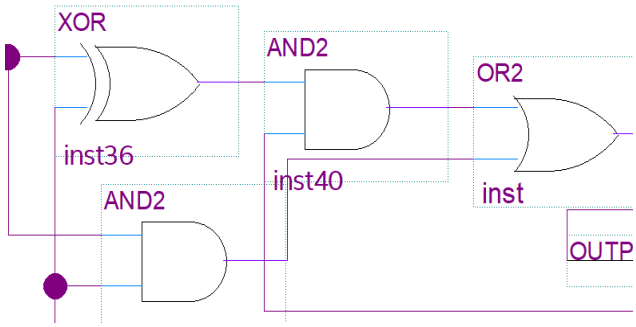


Fig 3. The comparator based on the subtractor.

The final comparison is to add the subtraction and the subtraction to get the highest digit. If the highest digit, that is, the sign bit of the fourth digit, is 1, then the inverse code can be obtained as the positive number? Positive numbers need to be reversed and then added one, and negative numbers do not need to be, because the input of negative numbers is already a complement (except the complement of the sign bit) is already added 1 based on the inverse code, so there is no need to add 1 again, and positive numbers have not been added one, so finally 1 will be added. Finally, the complete absolute value threshold comparator is obtained, and the logic key of this circuit lies in the idea of subtracter. The layout of this circuit in Fig.4 is shown below.

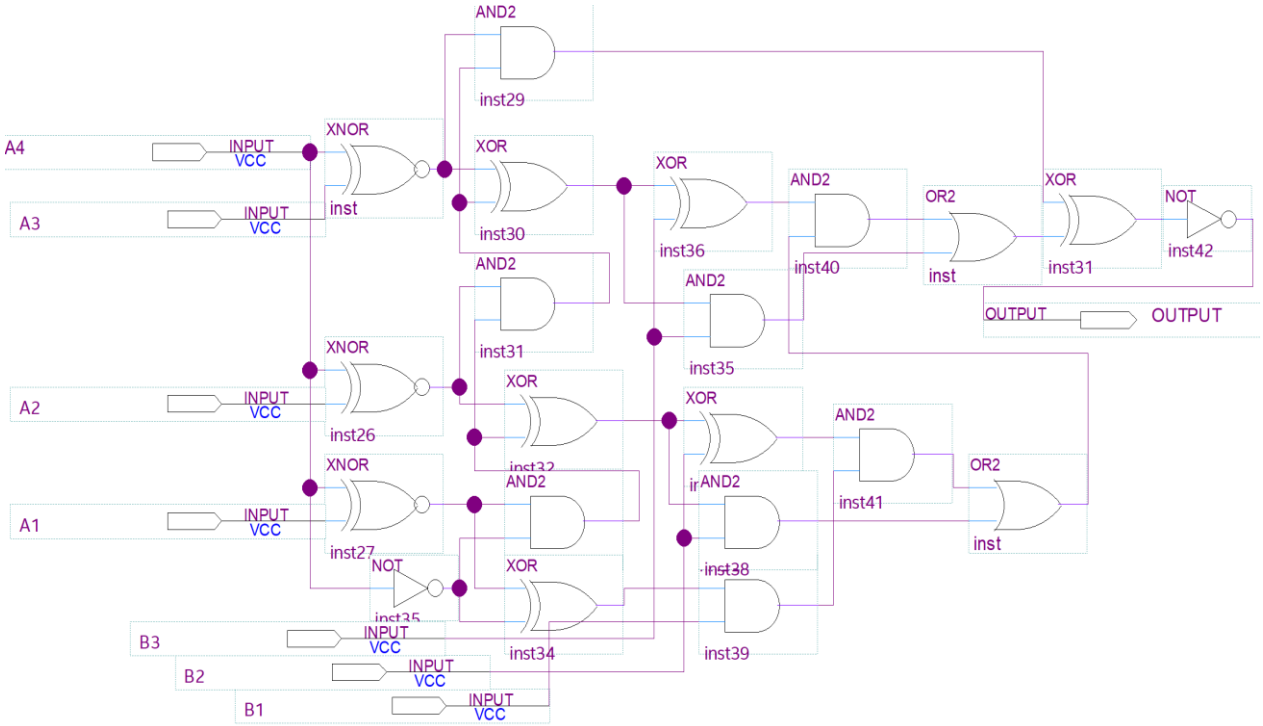


Fig 4. The layout of the top circuit.

3.3. The optimization of the delay of the absolute value detector

Process variation is thought to be a significant issue when designing circuits. Environmental and process-induced variation are frequently the sources of variances [8]. The delay is the variation which caused by interconnects of the circuit. In order to achieve the evaluation of delay, the longest path in the whole circuit should be selected, that is, the so-called critical path, as seen in the following Fig.5.

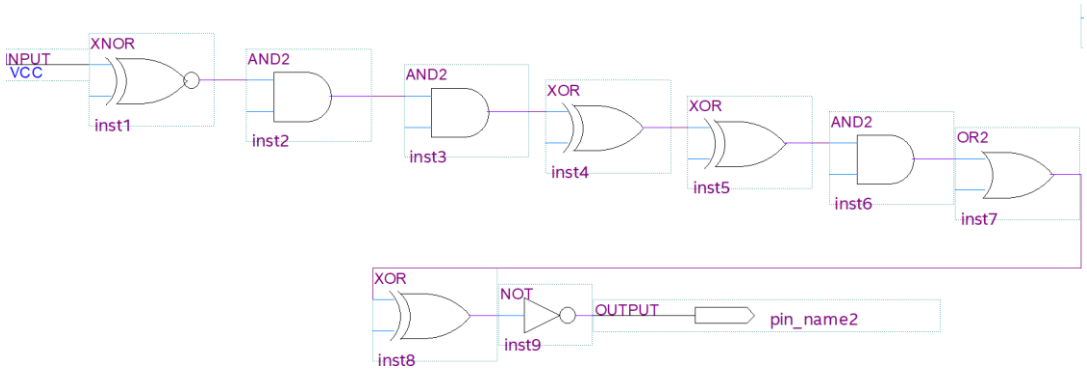


Fig 5. The critical path.

Characteristics of CMOS and the formula of each parameter, the G parameters, H parameters and B parameters of each device composed of CMOS can be calculated. The following is the formula for the path's logical effort (G), electrical effort (H), and parasitic effort (P).

$$G_{path} = g_1 \cdot g_2 ... g_n \tag{1}$$

$$H_{path} = h_1 \cdot h_2 ... h_n \tag{2}$$

$$B_{path} = b_1 \cdot b_2 ... b_n \tag{3}$$

The first formula G represents the multiplicative of g, and H represents the multiplicative of h in the same way, but H is equal to Cout/Cin, which means that there is no need to calculate the multiplicative of h, and B is equal to the multiplicative of each small branch b, and b is equivalent to the capacitance of the input on the main road plus the branch's input capacitance divided by the main road's input capacitance, which is easily obtained by the following formula.

$$\mathrm{b} = \frac{C_{on-path} + C_{off-path}}{C_{on-path}} \tag{4}$$

In order to calculate these parameters above, g, h and b and p are the parameters which should be gained. One gate's total delay, d, is made up of two components: the effort delay, f, which is equal to g times h while driving the capacitive load, and the intrinsic parasitic delay, p.

$$\mathrm{d} = gh + p \tag{5}$$

Wider transistors that supply more current have bigger diffusion capacitances, therefore the parasitic delay is generally independent of the transistor sizes in the gate. The ratio of the transistor sizes in the gate to the load capacitance and the gate's complexity determine the effort delay in turn. Electrical effort (h) is the term for the former, and logical effort (g) is the term for the latter. The following is the formula for the logical effort (g), electrical effort (h), and parasitic effort (p).

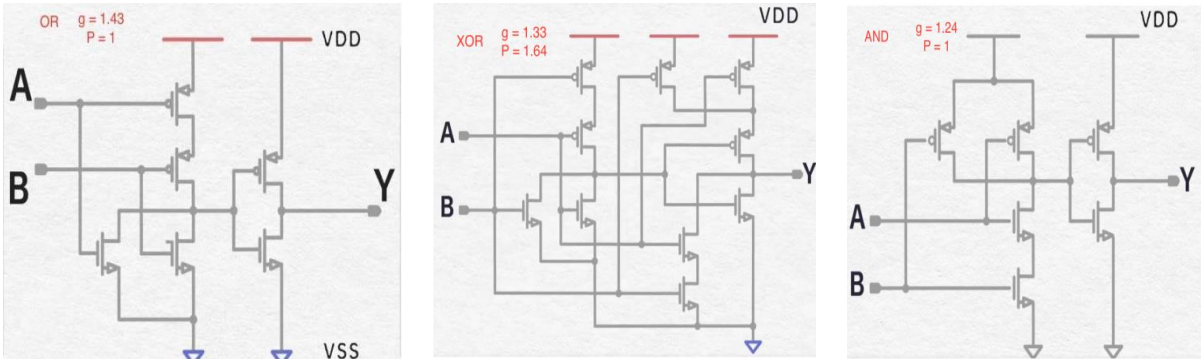
$$g = \frac{R_{gate} \cdot C_{in,gate}}{R_{INV} \cdot C_{in,INV}} \tag{6}$$

$$h = \frac{C_{out}}{C_{in,gate}} \tag{7}$$

$$p = \frac{C_{par,gate}}{C_{par,INV}} \tag{8}$$

The gate complexity is characterized by the logical effort, g. Only the ratio of the input gate capacitance to the input reference inverter capacitance remains after the gate resistance to inverter resistance can be immediately decreased to 1 [9]. The output capacitance divided by the input gate

circuit's resistance is equal to the parameter h. The ratio of the parasitic gate circuit's capacitance to the parasitic inverter's capacitance, or parameter p, is p. additionally, the g and p of the gate that are displayed below are presented in Fig. 6.



(a) (b). (c).

Fig 6. The g and p of the gate.

The ratio of the input capacitance to the input capacitance of an inverter providing the same output current is known as the logical effort. Assumed unit-sized inverter values in Fig. 6(a) are, for instance, Wp = 650 nm, Wn = 430 nm, and Lp = Ln = 100 nm (drawn L). Since the nmos tubes in the Fig.6 (a) are in series, and since the parameter of nmos is 430nm, from the input end, for example, port a, port a points to an nmos and pmos. So the reference capacitance of the nmos is (1/430) + (1/430) =2/430, which is equal to 430/2. Similarly, the equivalent pmos of the above pmos is equal to 650. And because the reference input is the sum of the reference nmos and the reference pmos at the input. So the formula (650+430)/(430/2)+650 is equal to 1.24.Y is the output, is the output of nmos and pmos, and the reference Y points to the addition of the reference nmos and pmos. So it's not hard to see that the ratio is 1. The same can be said for XOR gates as shown in the Fig.6 (b) and OR gates Fig.6 (c).

$$Pathdelay\ (D) = \sum_{i=1}^{n} (GHB + P_i) \tag{9}$$

Thus, the path effort delay and the path parasitic delay, P, make up the path delay, D, which is the total of the delays of each of the path's gate stages, di. The path effort delay can be computed by multiplying the G, H, and B parameters to obtain the final F [9]. (f) Is the ideal delay per device in the absence of p. (F stands for stage effort without parasitic delay p). Gate sizing for Power Delay product minimization when considering the link with its Power and Delay while employing the Unified Logical Effort method [10]. Finally, the stage effort is calculated by the formula shown below and the minimum delay if referred to the formula above.

$$f = \sqrt[n]{F} = \sqrt[n]{GHB} \tag{10}$$

Since the H parameter is equal to Cout/Cin, and Cin is a buffer of two inverters at the input side, H is equal to 32/2, which is equal to 16 is shown in figure 7.

Critical path (gama=1)										
H=32/2=16	Stage	1	2	3	4	5	6	7	8	9	10
	Cin	2	1	1	1	1	1	1	1	1	1
	g	1.33	1	1.24	1.24	1.33	1.33	1.24	1.43	1.33	1
	b	1	1	2	2	2	2	1	1	1	1
	p	1.64	1	1	1	1.64	1.64	1	1	1.64	1
	K=21.169										
	F:path effort:2183.68										
	f:2.157										
	VDD:0.76										
	mini delay:34.13										
	τopt(1.5*mini delay):34.13=51.20										

Fig 7. The calculation of each CMOS.

3.4. The energy consumption of this absolute value detector

As for the energy calculation of the four-digit absolute value comparator, the formula (11) can be directly applied to obtain the total power consumption.

$$E = C_L \cdot V_{dd}^{\ 2} \tag{11}$$

At this time, the highest power consumption can be obtained in exchange for the least delay from the following figure, but the high power consumption is not recommended. Therefore, the most original VDD can be substituted into the formula (12) to get the smallest delay, but when the longest delay is calculated, it will be brought back to the formula to get a lowest power consumption, so power consumption and delay are not both fish and bear's feet.

$$\tau = k \cdot \frac{V_{dd}}{(V_{dd} - 0.2)^2} \tag{12}$$

Finally, after sizing the device, the resulting delay, that is, the minimum path effort per CMOS after local optimization, can meet the power consumption is slightly lower and meet the appropriate delay. And the k is equal to Cl over beta. As is mentioned above, the Fig. 8 is the relationship between energy and delay is shown below.

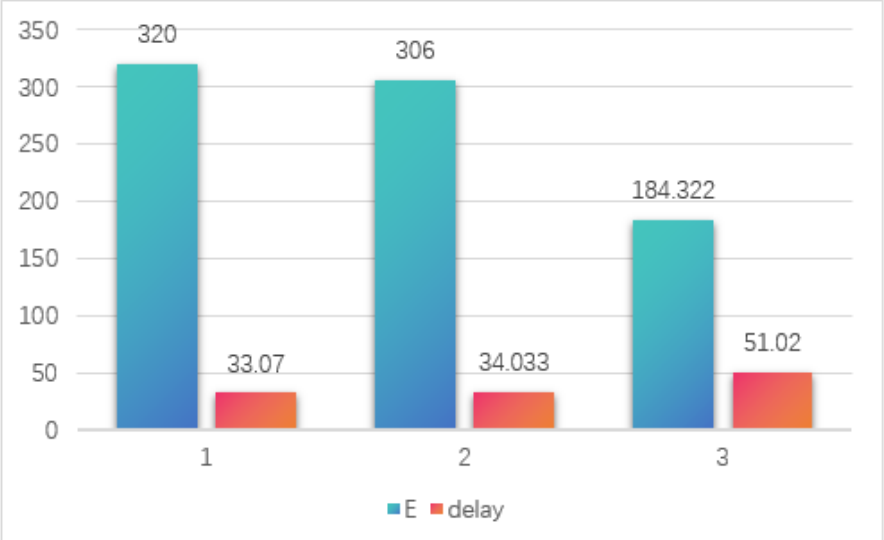


Fig 8. The relationship between energy and delay.

4. Conclusion

Encryption is an important means to protect privacy, and the more rigorous the encryption method, the less easy it is to be cracked. Create a comparator with a four-bit absolute value threshold. This 4-bit "absolute value detector" has a minimum energy of 50% and a delay that is 1.5 times greater than the minimum delay. Here, "energy" refers to the total energy probability distribution derived from the VDD for a specific input, while "delay" refers to the worst-case propagation delay. Make use of supply voltage scaling and gate size as variables. For delay modeling, assume gamma (c parasite/Cgate) = 1. After calculation, the delay of the absolute threshold comparator is 34.13, and the power consumption is 184.832.

However, after encrypting the ECG signal through the absolute value comparator principle, the parameters can be changed by changing the width of the CMOS channel, such as g and h and p, etc., by changing the structure of the channel to change the delay of the comparator encryption, in the future, with the emergence of more new materials, will gradually replace the original metal oxide materials such as CMOS. Under the continuous iteration of the final material, technology, etc., the delay will be shorter, the power consumption will be lower, and the material will be more energy-

saving. In addition to ECG signals, the idea of this comparison can be applied to other signals similar to ECG signals with high characteristics and high privacy in the future to achieve universal privacy encryption.

References

[1] Arin G, Jianwei Z, Hesham E, et al. Increased Risks of Re-identification For Patients Posed by Deep Learning-Based ECG Identification Algorithms. Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual International Conference, 2021.

[2] Zeng Jixin. Development of identity recognition system based on finger ECG signal. Hangzhou Dianzi University, 2015.

[3] Chiu C C, Chuang C M, Hsu C Y. A novel personal identity verification approach using a discrete wavelet transform of the ECG signal. 2008 International Conference on Multimedia and Ubiquitous Engineering (mue 2008). IEEE, 2008: 201-206.

[4] Aranda A, Karel J, Bonizzi P, et al. Acute MI Detection Derived From ECG Parameters Distribution. IEEE, 2019.

[5] Li Zhiqiang, Ren Xiaohong, Lin Yongwu. Research on key techniques of image-based ECG waveform detection. Chinese Journal of Metrology, 2023, (02):110-113+121.

[6] Li C, Zheng C, Tai C. Detection of ECG characteristic points using wavelet transforms. IEEE Transactions on biomedical Engineering, 1995, 42(1): 21-28.

[7] Pan J, Tompkins W J. A real-time QRS detection algorithm. IEEE transactions on biomedical engineering, 1985 (3): 230-236.

[8] Verma K G, Singh R, Kaushik B K, et al. Monte Carlo analysis of propagation delay due to process induced line parasitic variations in VLSI interconnects. 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC). IEEE, 2011: 6-10.

[9] Celinski P, Al-Sarawi S, Abbott D, et al. Logical effort based design exploration of 64-bit adders using a mixed dynamic-cmos/threshold-logic approach. IEEE Computer Society Annual Symposium on VLSI. IEEE, 2004: 127-132.

[10] Saravanakumar S, Srinivasan K, Rukkumani V, et al. Delay Minimization and Evaluation in Logic Paths of RC Interconnects by Unified Logical Effort. 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). IEEE, 2021: 1-6.