

Implementation of an 8-bit bit-slice AES *S*-box with rapid single flux quantum circuits

Ruo-Ting Yang(杨若婷), Xin-Yi Xue(薛新伊), Shu-Cheng Yang(杨树澄), Xiao-Ping Gao(高小平), Jie Ren(任洁), Wei Yan(严伟), and Zhen Wang(王镇)

Citation: Chin. Phys. B, 2022, 31 (**9**): 098501. DOI: 10.1088/1674-1056/ac70b9
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Characterization of topological phase of superlattices in superconducting circuits

Jianfei Chen(陈健菲), Chaohua Wu(吴超华), Jingtao Fan(樊景涛), and Gang Chen(陈刚)
Chin. Phys. B, 2022, 31 (**8**): 088501. DOI: 10.1088/1674-1056/ac5612

Shortcut-based quantum gates on superconducting qubits in circuit QED

Zheng-Yin Zhao(赵正印), Run-Ying Yan(闫润瑛), and Zhi-Bo Feng(冯志波)
Chin. Phys. B, 2021, 30 (**8**): 088501. DOI: 10.1088/1674-1056/abea96

Design of sextuple-mode triple-ring HTS UWB filter using two-round interpolation

Ming-En Tian(田明恩), Zhi-He Long(龙之河), You Lan(蓝友), Lei-Lei He(贺磊磊), and Tian-Liang Zhang(张天良)
Chin. Phys. B, 2021, 30 (**5**): 058503. DOI: 10.1088/1674-1056/abd7e1

Compact ultra-narrowband superconducting filter using N-spiral resonator with open-loop secondary coupling structure

Lin Tao(陶琳), Bin Wei(魏斌), Xubo Guo(郭旭波), Hongcheng Li(李宏成), Chenjie Luo(骆晨杰), Bisong Cao(曹必松), Linan Jiang(姜立楠)
Chin. Phys. B, 2020, 29 (**6**): 068502. DOI: 10.1088/1674-1056/ab888d

Compact high-order quint-band superconducting band-pass filter

Di Wu(吴荻), Bin Wei(魏斌), Xi-Long Lu(陆喜龙), Xin-Xiang Lu(卢新祥), Xu-Bo Guo(郭旭波), Bi-Song Cao(曹必松)
Chin. Phys. B, 2018, 27 (**6**): 068503. DOI: 10.1088/1674-1056/27/6/068503

Implementation of an 8-bit bit-slice AES *S*-box with rapid single flux quantum circuits

Ruo-Ting Yang(杨若婷)[1,2,3], Xin-Yi Xue(薛新伊)[4], Shu-Cheng Yang(杨树澄)[1,2], Xiao-Ping Gao(高小平)[1,2], Jie Ren(任洁)[1,2,3,†], Wei Yan(严伟)[4,‡], and Zhen Wang(王镇)[1,2,3]

[1] *State Key Laboratory of Functional Material for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai* 200050, *China*

[2] *CAS Center for Excellence in Superconducting Electronics (CENSE), Shanghai* 200050, *China*

[3] *University of Chinese Academy of Sciences, Beijing* 100049, *China*

[4] *School of Software and Microelectronics, Peking University, Beijing* 100871, *China*

(Received 26 January 2022; revised manuscript received 13 May 2022; accepted manuscript online 18 May 2022)

Rapid single flux quantum (RSFQ) circuits are a kind of superconducting digital circuits, having properties of a natural gate-level pipelining synchronous sequential circuit, which demonstrates high energy efficiency and high throughput advantage. We find that the high-throughput and high-speed performance of RSFQ circuits can take the advantage of a hardware implementation of the encryption algorithm, whereas these are rarely applied to this field. Among the available encryption algorithms, the advanced encryption standard (AES) algorithm is an advanced encryption standard algorithm. It is currently the most widely used symmetric cryptography algorithm. In this work, we aim to demonstrate the SubByte operation of an AES-128 algorithm using RSFQ circuits based on the SIMIT Nb03 process. We design an AES *S*-box circuit in the RSFQ logic, and compare its operational frequency, power dissipation, and throughput with those of the CMOS-based circuit post-simulated in the same structure. The complete RSFQ *S*-box circuit costs a total of 42237 Josephson junctions with nearly 130 Gbps throughput under the maximum simulated frequency of 16.28 GHz. Our analysis shows that the frequency and throughput of the RSFQ-based *S*-box are about four times higher than those of the CMOS-based *S*-box. Further, we design and fabricate a few typical modules of the *S*-box. Subsequent measurements demonstrate the correct functioning of the modules in both low and high frequencies up to 28.8 GHz.

Keywords: RSFQ, AES, *S*-box, hardware implementation

PACS: 85.25.–j, 85.25.Cp, 85.25.Hv **DOI:** 10.1088/1674-1056/ac70b9

1. Introduction

Rapid single flux quantum (RSFQ) circuits[1] are the first members of the SFQ families. They are a kind of the superconducting digital circuits that can work in an ultra-low temperature (typically at 4.2 K) environment. It is known that RSFQ circuits have significant advantages in reducing crosstalk and power consumption (nearly nW/gate). The picosecond switching time of Josephson junctions (JJs) makes them operate much faster than common CMOS circuits, e.g., the fastest RSFQ devices were tested working in 770 GHz at 4.2 K.[2] Another unique feature of RSFQ circuits is that most logic cells (AND, OR, etc.) are driven by the clock signal, i.e., RSFQ circuits are natural gate-level pipelining synchronous sequential circuits. Such a feature makes RSFQ circuits both high-throughput and high-frequency clocking.

RSFQ circuits are suitable for their applications that may require intensive computing resources, low power consumption, or high throughput. In the past few years, they were found in many applications, such as the analog-to-digital converter (ADC),[3] fast Fourier transform (FFT) processors,[4] and CPU processors.[5] We observed that the high-throughput and high-speed performance of the RSFQ circuits could take the advantage of a hardware implementation of the encryption algorithm. The advanced encryption standard (AES)[6] algorithm is one of the most popular encryption algorithms in symmetric key encryption. It is widely used in the field of information security. The AES algorithm has been studied widely by using CMOS circuits.[7–10] Still, only one research team could be found, which implemented a 128-bit AES algorithm in the RSFQ logic[11] with logic simulation results only.

In this paper, we demonstrate the key operation of the AES-128 algorithm, i.e., SubBytes operation, using the RSFQ circuits based on the SIMIT Nb03 process including its cell library. Simulated performance of the RSFQ circuits, such as the throughput, clock frequency, and power consumption, are presented and compared with those of the same structure in the CMOS logic. Moreover, we fabricate the individual modules of the *S*-box in chips and test them under both high- and low-frequency clocks. The measurement results show the correctness of the function. To our best knowledge, it is the first demonstration of the working of the RSFQ-based AES modules.

The rest of this paper is organized as follows. Section 2 briefly introduces the basic concepts of the AES algorithm

†Corresponding author. E-mail: jieren@mail.sim.ac.cn

‡Corresponding author. E-mail: yanwei@ss.pku.edu.cn

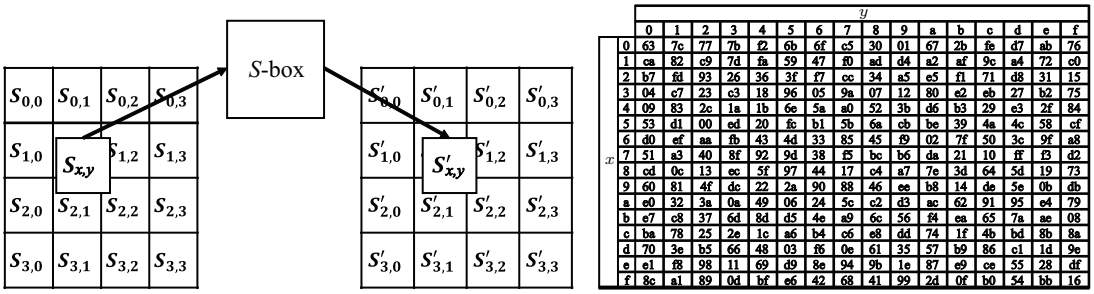
© 2022 Chinese Physical Society and IOP Publishing Ltd

and implementation of the *S*-box circuit. Section 3 proposes our AES *S*-box hardware implementation structure and design in the RSFQ logic as well as presents a comparison with the circuit of the same structure in the CMOS logic. The design and test results of individual modules of the *S*-box are presented in Section 4. In Section 5, we present conclusions and propose an outlook.

2. AES algorithm and *S*-box circuit

The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. It is declared as an advanced encryption standard algorithm by the National Institute of Standards and Technology (NIST) in 2001. The Rijindael algorithm[12] is adopted in AES as a cryptographic algorithm, which is widely used in many fields.[13–16] The essence of the AES algorithm is to convert polynomial multiplication and modular operation into shift calculation and bit XOR operation, which greatly simplifies the hardware implementation.

The four individual transformations in the cipher are SubBytes( ), ShiftRows( ), MixColumns( ), and AddRoundKey( ). In the SubBytes( ) transformation, each byte of a state is non-linear substituted independently using a substitution table, which is known as an *S*-box. The ShiftRows( ) transformation is a shift operation, where the bytes in the last three rows of the state, excluding its first row, are cyclically shifted over different numbers of bytes. In the MixColumns( ) transformation, each column is treated as a four-term polynomial and it operates on the state column-by-column. The AddRoundKey( ) transformation is a simple bitwise XOR operation, where a Round Key is added to the state.



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Fig. 1. SubBytes( ) mapping process (left) and the *S*-box table (right).

The SubBytes( ) transformation is a mapping process, whose operation and hexadecimal form are presented in Fig. 1. For example, if S1.1 equals $\{64\}$, the result of transformation becomes $S'1.1 = \{43\}$.

The design of the *S*-box implementation circuit is the core to the implementation of the SubBytes( ) transformation, as well as vital challenge in designing compact implementations of AES. In the CMOS circuits, the look-up table (LUT) is a common method to complete the circuit design.[17] The state matrix greatly simplifies the difficulty in designing, and it is very easy to realize in the CMOS circuits. It can also effectively improve the rate of data throughput. The concept is also adopted in Ref. [11] where they realize *S*-box in the RSFQ logic. There are some other methods to design the *S*-box, e.g., the order-reduced method.[16] A multiplier is used in this method. However, larger costs in hardware resources for an RSFQ multiplier will reduce the advantages of a high multiplexing rate with a larger delay in the critical path.

In this paper, we choose to implement the *S*-box of a masked and bit-sliced AES-128 algorithm.[18] The whole circuit is designed in a full-combinational way. The idea of linear and non-linear mappings is adopted in the design.[19] There are two reasons why we choose this design method:

(i) The RSFQ circuits take the advantage of high throughput and frequency, but calculations like multiplication cost enormous resources. In this method, addition and multiplication in a single-bit calculation are realized, respectively, through XOR gate for linear mapping and AND gate for non-linear mapping, which is ideal for the RSFQ circuits.

(ii) The full-combinational design method is the most basic design method in the CMOS logic. Compared to a multiplier or LUT design in the RSFQ logic, a full-combinational structure is more hardware resource-efficient with higher reliability.

3. Hardware structure and implementation

The whole *S*-box implementation circuit is shown in Fig. 2. It consists of 14 modules, named as the linear map number (lm) or non-linear map number (nlm) or input/output map. The input map is the input module that processes and calculates the input signal. It is a linear mapping module, where the input data is put through XOR calculation and then passed to the next few modules after the processing is completed. The non-linear map number (number=0–5) works as the non-linear mapping module and consists of AND gate, while the linear map number (number=0–5) works as the linear mapping module and consists of XOR gate. The output map is an output mapping module composed of NOT gate, which combines and adjusts the data from previous modules.

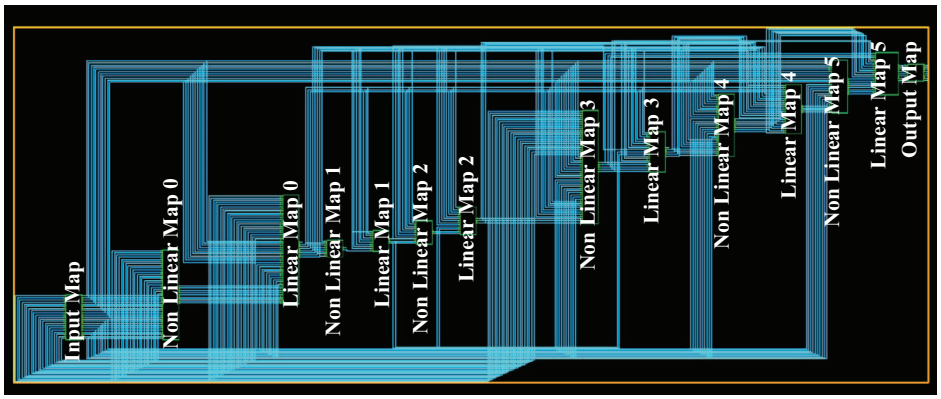


Fig. 2. Structure of *S*-box implementation in bit-sliced AES-128.

We build the same pre-simulation structure in our simulator environment, as shown in Fig. 3. Besides the main function module of the *S*-box, we use the D-flip-flop (DFF) as a buffer to reach the path balancing for the gate-level pipelining character of RSFQ. We ran the pre-simulation under the SIMIT-Nb03 Verilog cell library. The gate-level Verilog simulation result is shown in Fig. 4, where TI is the input clock signal, TO is the output clock signal, and aesout_0 to aesout_7 are the outputs of the circuit. Every square wave of picosecond width stands for an RSFQ logic signal. There are a total of 32 pipeline stages. Hence, the first result comes out after the 33rd clock arrives. The simulation results are consistent with the *S*-box table, e.g., the 8th output is {30} with input {08}, confirming the correctness of our design.

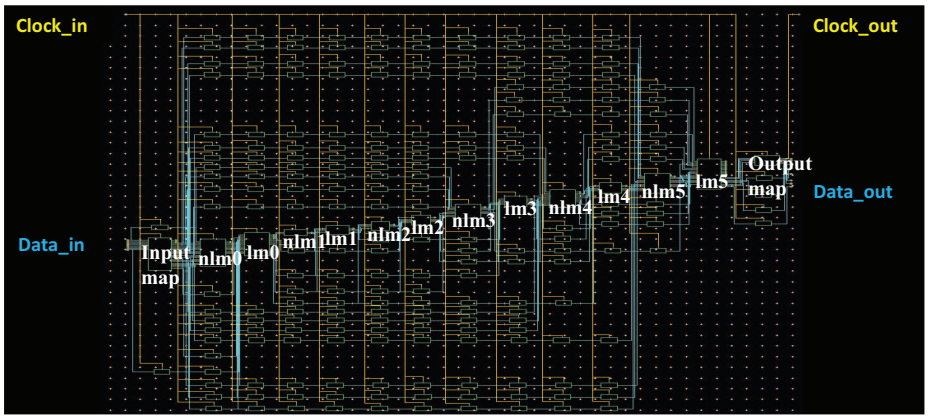


Fig. 3. Pre-simulation structure of *S*-box in RSFQ logic circuit.

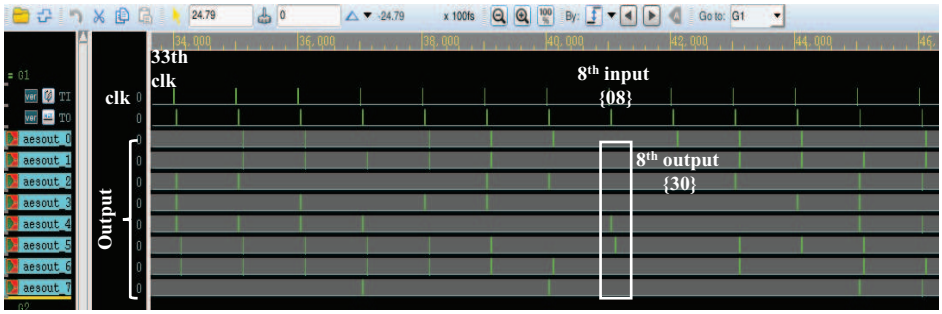


Fig. 4. Simulation results of *S*-box implementation circuit in RSFQ logic.

The layout and post-simulation results of the circuit are carried out based on the JSIC complier, which is an EDA tool for logic synthesis, placement, and routing of single-flux-quantum (RSFQ) logic circuits developed by our EDA groups. It contains 42237 JJs and 117 logic cells. The maximum frequency of the *S*-box implementation circuit after layout (Fig. 5) is 16.28 GHz.

For the same *S*-box implementation circuit structure, comparative results between the CMOS logic and RSFQ logic are listed in Table 1. For comparison, the results of the CMOS circuit are obtained under TSMC 7 nm CMOS logic 1P15M process by flattening the whole circuit. Two parts indicate the

advantages of the RSFQ-based circuit of the *S*-box. Firstly, the working frequency of the RSFQ-based circuit is much higher than that of the CMOS-based circuit. The maximum working frequency of the RSFQ-based *S*-box is 16.28 GHz, while it is 4 GHz in the CMOS circuits of the same structure. Secondly, due to the unique gate-level pipelining character of the RSFQ circuits, the higher the clock frequency, the higher the throughput. The throughput of the whole *S*-box is 130.24 Gbps under 16.28 GHz of the main frequency, which is much higher than that of the CMOS logic-based circuits. Although it is hard to estimate the power consumption of the whole RSFQ-based *S*-box with limitation of our EDA tool, the power consumption of the RSFQ-based single module still shows at least two orders of magnitude lower than that of the CMOS-based circuits. It is to be mentioned that the minimum line width of our SIMIT-Nb03 process is 1.4 μm. The successfully tested modules play a cornerstone role for our follow-up work in building the whole system and offer good test suggestions.

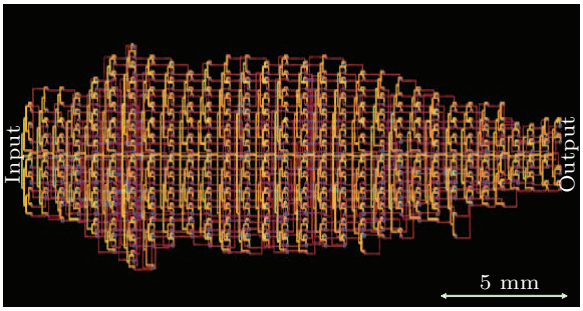


Fig. 5. Layout of *S*-box implementation circuit.

Table 1. The performance of same *S*-box implementation structure in different logic circuits.

	Frequency (GHz)	Throughput (Gbps)	Power (W)	Area (μm^2)
CMOS	4	32	0.069*/0.022†	59
S-box	16.28	130.24	–	21465×6300

*Input activity 1. †Input activity 0.1

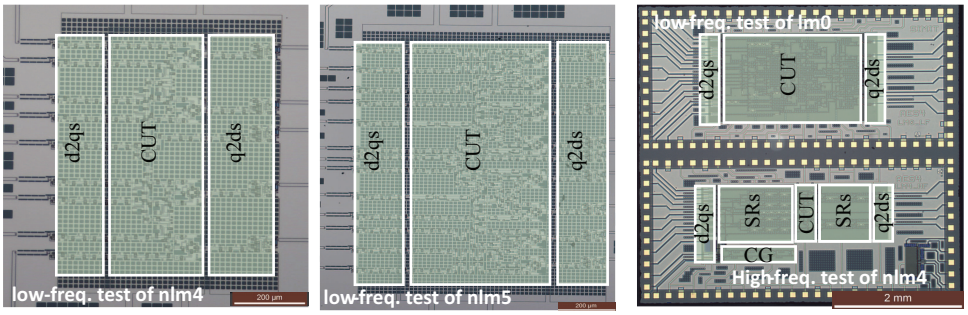
4. Fabrication and testing

4.1. Module design and information

In the previous section, we designed the whole circuit with correct simulation results. Tape-out verification of the design is needed in the next step. Here, we select several modules to tape out, by considering the limitation of the current integration of the RSFQ circuits. The selected modules are linear lm0, nlm4, and nlm5, covering both linear mapping and non-linear mapping modules with JJ varying from several hundreds to thousands. We believe that these three modules are sufficient for demonstration. We adopt the concurrent-flow clocking[20] to design fully pipelined synchronous RSFQ circuits in each module.

The simulation results are obtained in pscan[21] after conducting global optimization. The widest margin of the module is up to 51.06%, while the narrowest one still reaches 26% of a module with JJs of more than two thousands. The wider margin indicates less impact of deviation caused by the fabrication, i.e., better performance of the circuits.

The modules of nlm4, nlm5, and lm0 are taped out in different batches by using our self-developed SIMIT Nb03 6-kA/cm2 process.[22,23] The circuits are tested by using the OCTOPUX[24] test system for superconducting integrated circuits. Figure 6 shows the microphotographs of the low-frequency and high-frequency test circuits of nlm4, and the low-frequency test circuits of lm0 and nlm5. Table 2 presents the integration, power consumption, area, and the designed frequency of each module taped out. The largest module is lm0 with 2271 JJs and the smallest module is nlm4 with 128 JJs. Three modules are designed and optimized under the main frequency of 17.5 GHz.



(a) (b) (c)

Fig. 6. Microphotographs of test modules of *S*-box circuits: (a) nlm4 in low frequency, (b) nlm5 in low frequency, (c) lm0 in low frequency and nlm4 in high frequency.

Table 2. The related parameters of each module.

Name of circuits	Number of JJs	Power (μW)*	Area (μm^2)	Main frequency (GHz)	Max frequency (GHz)
Nlm4	128	53.47	270×720	17.5	27.85
Nlm5	354	141.37	510×1020	17.5	25.06
Lm0	2271	1003.37	2250×1350	17.5	20.17

*The results was calculated under the main frequency of 17.5 GHz.

4.2. Low-frequency test results

As shown in Figs. 6(a) and 6(b), each low-frequency test circuit consists of D2Qs (digital-to-SFQ pulse converter), CUT (circuit under test), and Q2Ds (SFQ pulse-to-digital converter). D2Q and Q2D work as interfacing units between the digital level signal and SFQ pulse signal.

The obtained test results are shown in Fig. 7. Each square signal in the blue line stands for an SFQ signal input pulse, while each transition edge of the red line stands for an SFQ signal output pulse. As shown in Fig. 7(a), the first 12 lines in blue color stand for input signals A1-A3, B1-B3, C1-C3, and D1-D3. The bottom blue line stands for the clock signal. The output signal XO1 (X = A or B or C or D) and XO2 are expected to be (X1*X2) and (X2*X3), respectively. The output values of each module are matched with our expectations, and the results indicate the correctness in design and fabrication. The widest margins of nlm4/nlm5/lm0 are 68%, 32%, and 2%, respectively.

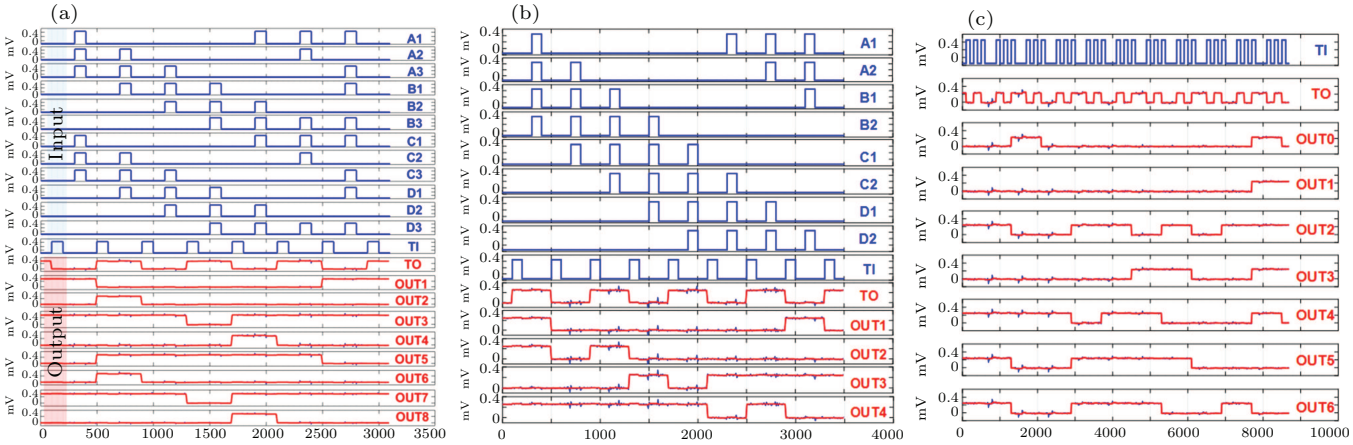


Fig. 7. Low-frequency test results of each module: (a) nlm5, (b) nlm4, (c) lm0.

From the test results, we find that the test margins of lm0 is significantly lower than the simulation. The first reason is due to the instability of different batches of our developing fabrication process. According to the data of PCM (process control monitor) of this batch of process detection chips, the critical current density J_C, which is the key process parameter of the Josephson junction, is different from the designed value under two test methods, one is 8.47% higher and the other is 10.56% lower. The shift in J_C results in a shift in the critical current I_C of the Josephson junction in the circuit, which changes the timing information of cells, making the timing on the critical path more stringent, especially for large-scale circuits. By analyzing the test data and structure of lm0, we find that the critical path made of two complex IP exists in the data path of two output ports, and the test results of these two ports show extremely small margins, which limit the margins of the whole circuit. Tested margins can be improved by optimizing the critical path timing in design. In addition to process parameter shift, the deviation also comes from the gap between the simulation model and the actual model of the device. The ideal RCSJ model commonly used in the SFQ circuit simulation has not yet taken into account the effects of parasitic parameters in actual devices.

4.3. High-frequency test results

Since our current superconducting test system can offer and receive only low-frequency signals, an on-chip high-frequency test structure is adopted. In the lower part in Fig. 6, a clock generator (CG) is used as the high-frequency clock input, and a shift register (SR) is used to store the test patterns. The test patterns are read into SR at a low-frequency clock, and the results are also read out from SR at that low-frequency clock. However, with the flag signal of a trigger, the test patterns pass through the CUT at a high-frequency clock.

The test results of nlm4 are shown in Fig. 8(a) and they are matched with the expected ones. The margins of nlm4 at different frequencies are also shown in Fig. 8(b). The widest margin of this circuit is 56%, which is very close to that in simulation. The maximum tested clock frequency is 28.84 GHz.

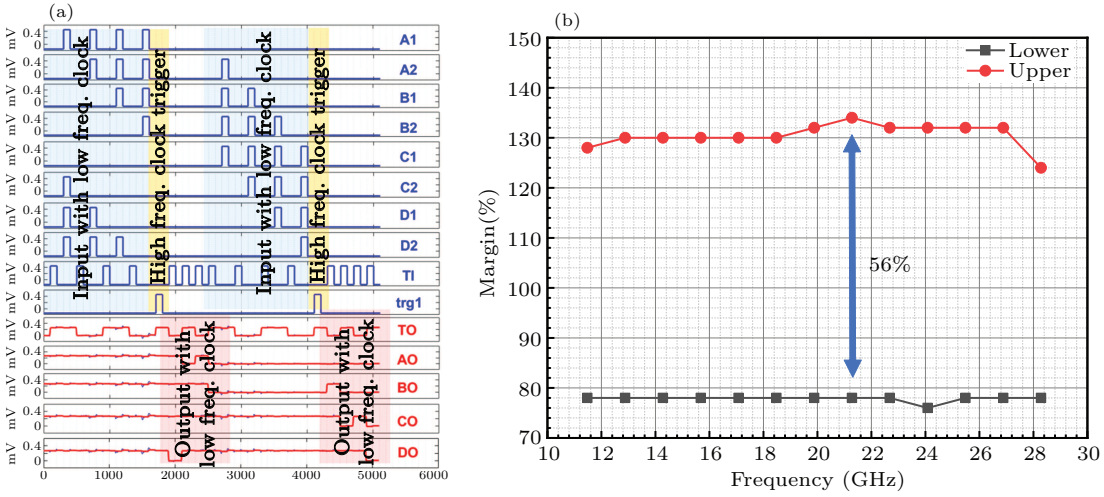


Fig. 8. High-frequency test results of nlm4 (a) and margins of nlm4 at different frequencies (b).

5. Conclusions

We have demonstrated one of the most important operations, i.e., SubBytes( ) operation of the AES-128 algorithm, using RSFQ circuits based on the SIMIT-Nb03 cell library, and successfully fabricated and tested some of the modules in *S*-box. The whole *S*-box consists of 32 pipeline stages with 42237 JJs, out of which the tested nlm4, nlm5, and lm0 modules consist of 128 JJs, 354 JJs, and 2271 JJs, respectively. The maximum working frequency of the *S*-box is 16.28 GHz, and the maximum testing working frequency of a single module of the *S*-box is 28.84 GHz. The comparative results between the CMOS-based circuits and RSFQ-based circuits indicate that the RSFQ-based *S*-box modules get advantages in frequency and throughput, while it is still being competitive in power consumption under our backward fabrication process.

Despite the limitation of the current integration of the RSFQ circuit and immature EDA tools, we did not fabricate the whole *S*-box implementation circuit, but several feature modules were tested with correct functions and margins, which indicate some reliability of our design. Compared with the mature commercial CMOS process, our process is still under development, so the stability is not enough, which also limits the large-scale circuit test margin. We are planning to find some effective optimization methods to improve the optimization efficiency of our EDA tools and further reduce the scale of the designed circuit. With the steady development of the fab-process and integration, *S*-box, as well as the complete AES algorithm with higher performance, can be implemented in near future.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 92164101), the National Natural Science Foundation of China (Grant No. 62171437), the Strategic Priority Research Program of the Chinese Academy of Sciences (Grant No. XDA18000000), Shanghai Science and Technology Committee (Grant No. 21DZ1101000), and the National Key R&D Program of China (Grant No. 2021YFB0300400). The authors would like to thank Ya-Jun Ha, Bin-Han Liu and Ling Xin for the valuable discussion and help. The fabrication was performed in the Superconducting Electronics Facility (SELF) of SIMIT.

References

[1] Likharev K K and Semenov V K 1991 *IEEE Trans. Appl. Supercond.* **1** 3
[2] Chen W, Rylyakov A V, Patel V, Lukens J E and Likharev K K 1999 *IEEE Trans. Appl. Supercond.* **9** 3212
[3] Radparvar M 1994 *IEEE Trans. Appl. Supercond.* **4** 92
[4] Sakashita Y, Yamanashi Y and Yoshikawa N 2015 *IEEE Trans. Appl. Supercond.* **25** 1301205
[5] Fujimaki A, Tanaka M, Yamada T, Yamanashi Y, Park H and Yoshikawa N 2008 *IEICE Trans. Electron.* **E91.C** 342
[6] Dworkin M, Barker E, Nechvatal J, Foti J, Bassham L, Roback E and Dray J 2001 *Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197*, (NIST FIPS) National Institute of Standards and Technology, Gaithersburg, MD
[7] Kim H, Hong S and Lim J 2011 *International Workshop on Cryptographic Hardware and Embedded Systems—CHES 2011*, *Lecture Notes in Computer Science* Vol. 6917 Springer, Berlin, Heidelberg, pp. 95–107
[8] Wang Y and Ha Y 2013 *IEEE Transactions on Circuits and Systems* Ⅱ, *Express Briefs* **60** 36
[9] Masoumi M 2020 *IEEE Transactions on Circuits and Systems* Ⅱ, *Express Briefs* **67** 1314
[10] Sawataishi S, Ueno R and Homma N 2020 *IEEE Transactions on Circuits and Systems* Ⅱ, *Express Briefs* **67** 1604
[11] Zhou Y, Tang G M, Yang J H, Yu P S and Peng C G 2021 *IEEE Trans. Appl. Supercond.* **31** 1302911
[12] Daemen J, Rijmen V and Leuven K U *AES Proposal: Rijndael Version2* [Online] Available: http://www.nist.gov/cryptotoolkit
[13] 2004 *IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements*, *IEEE Std 802.11i-2004*, 24 July 2004, pp.1–190
[14] Li L and Kuai J H 2020 *2020 International Conference on Wireless Communications and Smart Grid (ICWCSG)*, June 12–14, 2020, Qingdao, China, pp. 1–4
[15] Briliyant O C and Baihaqi A 2017 *11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, October 26–27, 2017, Lombok, Indonesia, pp. 1–5

[16] Huy D Q, Duc N M, Khai L D and Lung V D 2019 *IEEE-RIVF International Conference on Computing and Communication Technologies*, March 20–22, 2019, Danang, Vietnam, pp. 1–6
[17] Mcloone M and Mccanny J V 2003 *J. VLSI. Sig. Proc. Syst.* **34** 261
[18] Riou S [Online] available: https://github.com/sebastien-riou/masked-bit-sliced-aes-128
[19] Peralta R [Online] available: http://cs-www.cs.yale.edu/homes/peralta/CircuitStuff/SLP_AES_113.txt
[20] Gaj K, Friedman E G and Feldman M J 1997 *J. VLSI. Sig. Proc. Syst.* **16** 247
[21] Polonsky S, Shevchenko P, Kirichenko A, Zinoviev D and Rylyakov A 1997 *IEEE Trans. Appl. Supercond.* **7** 2685
[22] Gao X, Qiao Q, Wang M, Niu M, Liu H, Maezawa M, Ren J and Wang Z 2021 *IEEE Trans. Appl. Supercond.* **31** 1101105
[23] Ying L, Zhang X, Niu M, Ren J, Peng W, Meazawa M and Wang Z 2021 *IEEE Trans. Appl. Supercond.* **31** 1301504
[24] Zinoviev D Y and Polyakov Y A 1997 *IEEE Trans. Appl. Supercond.* **7** 3240