Overview of large-scale AQFP efforts and FSDL plans at Yokohama National University

Christopher L. Ayala

Yokohama National University – Institute of Advanced Sciences, Yokohama, Japan email: ayala-christopher-pz@ynu.ac.jp • chris.ayala@ieee.org

Supported by Army Research Office Grant Number W911NF-24-1-0153



Yoshikawa Group @ YNU

Institute of Advanced Sciences (IAS) Quantum Information Research Center



Quantum Information Research Center

Advancec Sciences

Institute o

FSDL Members



Prof. Nobuyuki Yoshikawa



Prof. Christopher

Ayala



Prof. Yuki Prof. Zongyuan Hironaka Ιi

Haruya Ikeda (student)



Prof. Prof. Wenhui Luo Hongxiang Shen



Dr. Hideo Dr. Naoki Takeuchi Suzuki (now @ AIST)



Prof. Olivia Prof. Yuxing Chen (now @ TCU) (now @ SWJTU)

He





横浜国立大学

先端科学高等研究院

Dr. Taiki Yamae (now @ AIST)









Prof. Yuki Yamanashi

Motivation

3

Trend of rising electricity demand of information and communications technology (ICT).

Currently 10% of the total electric power worldwide.

9,000 terawatt hours (TWh)



N. Jones, Nature, vol. 561, no. 7722, pp. 163-166, Sep. 2018.

Worst-case scenario: ICT could use as much as 50% of global electricity by 2030.

A. S. G. Andrae and T. Edler, Challenges, vol. 6, no. 1, pp. 117–157, Jun. 2015.



TechNavio, Data Center Market by Component and Geography - Forecast and Analysis 2022-2026 **SKU:** IRTNTR40958

Global market for data centers growing rapidly – <u>Cybersecurity is a key major challenge.</u>

Motivation



Motivation – Bitcoin (BTC) example



Energy-efficient superconductor electronics (SCE) potentially address power problem in largescale computing, data centers and cybersecurity.

University of Cambridge Bitcoin Electricity Consumption Index: <u>https://ccaf.io/cbeci/index/comparisons</u> (2023)



MANA AQFP microprocessor

AQFP logic for computing

1

- Adiabatic quantum-flux-parametron (AQFP) logic
 - Composed of a pair of Josephson junction (JJ) superconductor devices
 - **•** Extremely small bit energy $<< I_c \Phi_0$
 - Very small switching energy due to adiabatic operation
 - 1.4 zJ per JJ at 4.2 K in experiment [1]
 - High gain
 - 10-50x gain from µA's of input current
 - High robustness
 - Clock speeds on par with state-of-the-art CMOS logic (5-10GHz)



After cooling overhead [2], ~80x more efficient than 7nm FinFET with V_{DD} = 0.8V [3]

[1] N. Takeuchi et al., Appl. Phys. Lett., vol. 114, no. 4, p. 042602 (2019)
[2] D.S. Holmes et al., IEEE TAS, 23, no.3, (2013)
[3] A. Stillmaker et al., Integration. 58, pp. 74-81 (2017)

AQFP logic a promising candidate for energy-efficient computing.

Cell library: minimalist design

8

L_{in} = 1.13 pH L_x = 5.67 pH L_d = 6.16 pH L₁, L₂ = 1.53 pH L_q = 7.88 pH L_{out} = 31.9 pH k_{d1}, k_{d2} = -0.154 k_{x1}, k_{x2} = -0.209 kout = -0.515 J₁, J₂ = 50 μ A

Excitation/clock lines are 50Ω microstriplines

Interconnect are shielded striplines





N. Takeuchi *et al., Supercond. Sci. Technol.*, vol. 30, no. 3, p. 035002, Mar. 2017. C. L. Ayala *et al., Supercond. Sci. Technol.*, vol. 33, no. 5, p. 054006, Mar. 2020.



Data propagation in AQFP logic

9



[1] N. Takeuchi et al., Appl. Phys. Lett., vol. 114, no. 4, p. 042602, Jan. 2019.

Semi-custom AQFP design flow





Towards AQFP microprocessors: MANA



MANA – Monolithic Adiabatic iNtegration Architecture

- **Goal:** Demonstrate AQFP can do both logic and memory
- RISC-like datapath + dataflow-like control

11

21,460 JJs in 1 x 1 cm² chip; 30 fJ/op at RT @ 5 GHz

IEEE **SPECTRUM** Superconducting Microprocessors?

Turns Out They're Ultra-Efficient

The 2.5 GHz prototype uses 80 times less energy than its semiconductor counterpart, even accounting for cooling



The AQFP-based MANA microprocessor sealed on a chip holder. The microprocesso die contains over 20,000 superconductor Josephson junctions. It is the first ever adiabatic superconducting microprocessor.

Hot New

電力を1/2000に

WERT RETOXE. 5/RETURNES

投票適用的の影響するクロプロセッキ 14111 を開発すナ (開1)

ロチョンビューターの制限にも利用







Cryptography: hashing

12

In what application can we leverage SCE technology today?

- □ How about cryptography hashing?
 - □ h: $\{0, 1\}^* \rightarrow \{0, 1\}^n$
 - □ Input: "message" arbitrarily long binary input
 - Output: "digest" fixed length (*n*) binary output
 - Ideally a unique signature for the input message
 - **\square** Similar inputs \Rightarrow dissimilar outputs
 - Ideally difficult to reverse engineer input using output

Uses:

- □ O(1) data structure in programs (Hash Table)
- Digital signatures
- Encryption/cybersecurity
- Cryptocurrency

Architecture implementation properties:

- Data feedback is typically well-controlled
- Control is simple, usally defined as fixed rounds/iterations (counters)
- Usually, no need for centralized memory during hashing



Secure Hashing Algorithms (SHA)

13

Algorithm	Year	Output Size	State Size	Operations	Collisions Found?		
SHA-0	1993	160-bit	160-bit	AND, XOR, OR, ROT, <mark>ADD32</mark>	Yes ($\leq 2^{34}$ evaluations)		
SHA-1	1995	160-bit	160-bit	AND, XOR, OR, ROT, <mark>ADD32</mark>	Yes (< 2 ⁶³ evaluations)		
SHA-2 (Bitcoin mining)	2001	256-bit	512-bit	AND, XOR, OR, ROT, SHR, <mark>ADD32</mark>	No (2 ¹²⁸ evaluations)		
SHA-3 (SHA3-256)	2015	256-bit	1600-bit*	AND, XOR, ROT, NOT	No (2 ¹²⁸ evaluations)		

SHA3/Keccak ("Ket-chak") algorithm won the NIST hash function competition in 2012

SHA-3 is paramterizable*, simple, and modern – good candidate for implementation.



16-bit AQFP Kogge-Stone adder component [1]

[1] T. Tanaka et al, "A 16-bit parallel prefix carry look-ahead Kogge-Stone adder implemented in adiabatic quantum-flux-parametron logic," IEICE Transactions on Electronics, vol. E105–C, no. 6, Jun. 2022.

Measurement of SHA-3 permutation block

C. L. Ayala et al., "Multi-GHz zeptojoule computing using emerging adiabatic superconductor circuits," DOI: 10.1109/isvlsi61997.2024.00106





1	+16 / -12	7	10^{-4}	10^{-18}	
2	+12 / -12	4.5	10^{-3}	10^{-17}	
3	+14 / -12	5	10^{-4}	10^{-18}	
4	+12 / -10	4	10^{-2}	10^{-17}	

(l=0 b=25 r=16 c=9 n=12)

JJ count: 13,008 JJs (state size=25 bits) Chip: 7 mm x 7 mm, 48 pad Active circuit area: 5.0 mm x 5.6 mm Maximum operation: 7 GHz AC margins: +16% / -12%



- Complex test PyVISA used to help automate experiment
- □ First +10k JJ AQFP chip at GHz speeds 4 / 6 chips
- BER rather high on the permutation outputs (10⁻⁴) at 7 GHz
- □ BER on debug shift-registers (SR) reasonable (10⁻¹⁸) at 7 GHz

Limitations of SHA-3 demo

15

- □ State size *b* is only 25-bits
- □ Increasing state size and performance requires...

Are	ea efficiency	Latency / clock distribution	Flux trapping					
	Advanced process such as MIT LL SFQ5ee [1] Directly coupled QFP (DQFP) + π-	 Low latency clocking [3,4] Power-clock H-tree distribution 	 Detailed analysis and better systematic moat designs [5, 6] 					
	JJs [2] Novel compact memory MAJ5+ logic gates	Interconnect drivability Boosters for long interconnect Impedance matched lines						

Y. He *et al.*, *Supercond. Sci. Technol.*, vol. 33, no. 3, p. 035010, Feb. 2020.
 N. Takeuchi *et al.*, *Supercond. Sci. Technol.*, vol. 33, no. 6, p. 065002, May 2020.
 N. Takeuchi *et al.*, *Appl. Phys. Lett.*, vol. 115, no. 7, p. 072601, Aug. 2019.
 Y. He *et al.*, *Appl. Phys. Lett.*, vol. 116, no. 18, p. 182602, May 2020.

[5] C. J. Fourie *et al.*, *IEEE Trans. on Appl. Supercond.*, vol. 30, no. 6, pp. 1–9, Sep. 2020.
[6] L. Schindler *et al.*, *IEEE Trans. on Appl. Supercond.*, 2024, accepted.
[7] IARPA SuperTools research program

Foundations of Superconducting Logic (FSDL)

DEVCOM Army Research Laboratory, in collaboration with the Laboratory for Physical Sciences (LPS), is soliciting proposals for foundational research in superconducting electronics (SCE). SCE is a promising technology for high-speed and energy-efficient digital circuits, but scaling towards denser and more reliable systems has been slow. The goal of the Foundations of Superconducting Digital Logic (FSDL) program is to uncover foundational issues limiting the progress of this technology and to pursue innovative research into overcoming these issues across topics such as materials, Josephson junctions, flux trapping, and architecture. FSDL aims to provide the foundation to enable breakthroughs in circuit density and reliability for future SCE-based systems.

URL: <u>https://arl.devcom.army.mil/collaborate-with-us/opportunity/foundations-of-superconducting-digital-logic-fsdl/</u>

- □ Kicked off: May 2024
- □ 4-year program with several performer teams
- YNU is on a performer team led by UC Riverside (Prof. Shane Cybart) along with partners at University of Maryland (Prof. Steven Anlage) and Stanford University (Prof. Kent Irwin, Prof. Kathryn Moler)

YNU's FSDL Plans

17

Flux trapping investigation

- Design and fabrication of SQUID, AQFP/RSFQ and PTL test structures featuring various moat configurations to investigate the vortex trapping effects.
- Distribute design samples to RF near-field nonlinear microwave microscope (NLMM, UMD) and Scanning SQUID Microscopy (Stanford) groups.
- Measure flux trapping effects in design samples and correlate with microscopy data.

Circuit editing

- Design and fabrication of aforementioned circuits suitable for focused ion beam (FIB) circuit editing.
- Distribute design design samples to FIB group (UCR).
 - Description Modify critical currents, improve symmetry, repair lines, add new nano-moats/pinning sites
- □ Measure changes (improved margins, reduced offsets, etc.) due to FIB.

Putting it all together

Leverage microscopy data, electrical measurement data, and FIB-based circuit improvements to establish new design guidelines to be implemented in next generation standard cells.

Flux trapping in an AQFP register file

18

Block diagram and chip photo: a 16-word by 4-bit AQFP register file



- With three input and two output ports
- Circuit size: 6.8 mm x 6.8 mm
- Total junction number: 6,438 JJs

Examples of low-speed test results

Test results after the initial cool-down



Test result after the second cool-down

	HSTPA004 No.2		Address number														Corrects	
G4		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	/Addresses
	D _{a1}	W	С	0	С	С	С	0	С	С	С	С	С	W	W	С	С	11/16
Data	D _{a2}	W	С	0	С	С	С	С	С	С	С	С	С	W	W	С	С	12/16
output A	D _{a3}	W	С	0	С	С	С	0	С	С	С	W	0	W	W	С	С	9/16
	D _{a4}	W	С	0	С	С	С	С	С	С	С	0	0	W	W	С	0	9/16
	D _{b1}	W	С	С	С	С	С	U	U	W	W	W	U	W	W	U	U	5/16
Data	D _{b2}	W	С	С	С	С	С	С	С	W	W	W	W	W	W	W	W	7/16
output B	D _{b3}	С	С	0	С	0	С	0	С	С	W	W	W	С	W	С	W	8/16
	D _{b4}	W	С	С	С	С	С	С	С	W	W	W	W	W	W	W	W	7/16

C: correct operation, W: wrong operation, U: unstable operation

Flux trapping substantially affects the circuit operation.

Moat analysis of AQFP OR cell using InductEx



Standard moat arrangement







- Move junctions away from moats
- Redesigned transformer with internal moat

Only simulation – experimental validation in progress

Operating margins of the OR cells with standard and redesigned moat arrangements



x-axis represents the 4096 possible trapped fluxon configurations in terms of a 12-bit binary sequence to represent fluxons trapped in moats F1 to F12.

L. Schindler et al., IEEE Trans. Appl. Supercond., 2024

FIB Circuit Edit Examples





Design error in ac network of AQFP circuit – FIB-based circuit edit used to repair disconnected line



Typical logic test circuit with MUX to select which logic output to observe on single output pad – FIB-based circuit edit used to troubleshoot logic errors from MUX failure.

Microscopy used to pinpoint if failure is possibly due to flux trapping. FIB used to create additional post-fabrication moats to improve operation.

Current progress: SQUID design for flux trap measurements



Nb wiring thickness SiO₂ insulator thickness 400 nm CTL 400 nm CC SiO₂ 300 nm] COU BC 1300 nm BC SiO2 AlOx BC SiO₂ 300 nm 1 BAS BAS RES **1**300 nm GC GC 300 nm⁺ Ground plane (GP) Si Substrate

Cross section of AIST process

HSTP ($J_c = 10 \text{ kA/cm}^2$) 1KP ($J_c = 1 \text{ kA/cm}^2$)

Schematic and layout of 1KP SQUID design



• $I_c = 100 \ \mu A$

symmetric DC-SQUID



Current progress: SQUID design for flux trap measurements

22

22 types of SQUIDs with different moat structures



1. Pre-moat 2. No moat 3. w+//4.w++ 5. d+//6d++

8. Point moat



12. in-moat





14. Only in-moat 15.Only in-moat2 16.in-moat point

21. JJ moat





9. 2-layer point moat 10. 2-layer W+ 11.Point moat y

13. inmoat2

17. U-moat 18. U-moat d-19. U-moat in 20. U-moatin 2

22. JC moat

1KP Chip design with 220 SQUIDs



Resistors for creating a temperature gradient

Current progress: SQUID measurement results



Current progress: AQFP shift registers for flux trap measurements



Layout of 10 AQFP shift registers for HSTP



AQFP shift registers with different moat structures





No moat around JJ

> Center moat and far-JJ moat

Current progress: AQFP shift register for individual flux trap measurements



Measured similarly for all buffers

25



Current progress: AQFP shift register for individual flux trap measurements



Circuit simulation results

26





Current progress: SFQ shift register design for flux trap measurements





SFQ-DFF with 6 different moat structures



HSTP cell library



Reduced distance



Increase width

No-moat



Storage-loop moat



in/out port Moat

Similar circuits will be done for MIT LL 8-Nb layer SFQ5ee process

And if we solve (or meaningfully mitigate) foundational challenges in superconducting digital logic?

28

Hybrid RSFQ-AQFP Transport Triggered Architecture (TTA)

29



AQFP circuits: TTA execution units and distributed registers

SFQ<->AQFP interfaces: Interface between SFQ/AQFP circuits, SerDes [2]

SFQ circuits: Long distance interconnect network and routing [3]

 Leverage strengths of RSFQ & AQFP [1]

- Globally asynchronous, locally synchronous
- TTA [4] shown to have performance and power advantage in postquantum cryptography applications over RISC-V

More investigation needed for hybrid design of large-scale RSFQ-AQFP systems.

[1] C. L. Ayala, in Superconducting SFQ VLSI (SSV), 2015/2019 [2] Y. Hironaka et al., IEEE Access, vol. 10, 2022. [3] A. Fujimaki et al., IEICE trans. electron., vol. E97.C, no. 3, 2014. [4] H. Corporaal and P. van der Arend Microprocessing and Microprogramming, vol. 38, no. 1, pp. 53 –60, 1993. [5] L. Akçay and S. B. Ö. Yalçin, 2021, DOI: 10.3906/elk-2003-27

Towards practical applications

[4] C. L. Ayala, ISVLSI 2024, doi: 10.1109/isvlsi61997.2024.00106

[5] O. Chen, IEEE Transactions on Emerging Topics in Computing, doi: 10.1109/TETC.2023.3330979

30



Large-scale SHA3 AQFP crypto chip (1 cm x 1 cm) Fully homomorphic encryption

Thank You

ACKNOWLEDGMENTS

Research was sponsored by the Army Research Office and was accomplished under Grant Number W911NF-24-1-0153. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

This work was also supported by the Grant-in-Aid for Scientific Research (S) No. 19H05614 and the Grant-in-Aid for Scientific Research (C) No. 21K04191 from the Japan Society for the Promotion of Science (JSPS).

This work was also supported by the VLSI Design and Education Center (VDEC) of the University of Tokyo in collaboration with Cadence Design Systems, Inc.

The circuits were fabricated in the Clean Room for Analog-digital superconductiVITY (now Qufab, Superconducting Quantum Circuit Fabrication Facility) of the National Institute of Advanced Industrial Science and Technology (AIST) using the high-speed standard process (HSTP) and low-Jc process (1KP).