Rethinking Most-significant Digit-first Arithmetic for Quantum Computing in NISQ Era

Dr. He Li

helix@seu.edu.cn / heli@ieee.org

16 Feb. 2023

Department of Electronics Science and Engineering

Southeast University, China

Outline

Part I – Experience in Quantum Information Processing

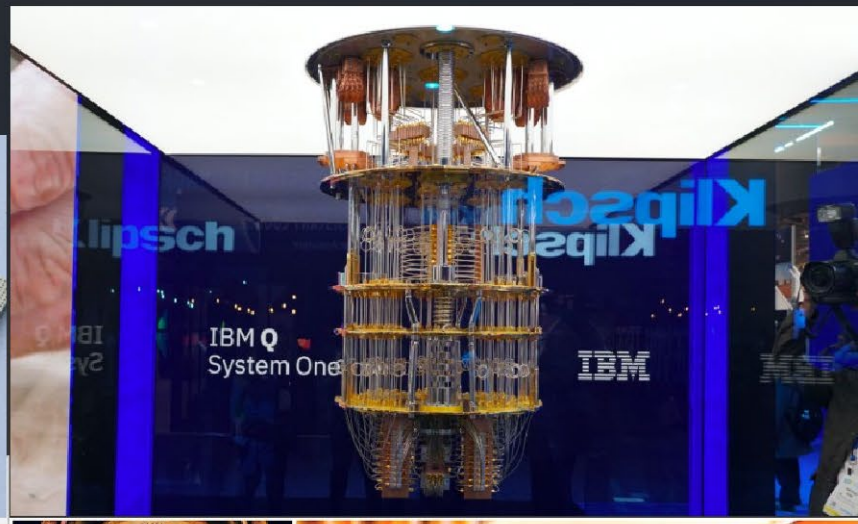
Part II – Quantum Arithmetic and MSDF Arithmetic

Part III – Quantum Most-Significant Digit-First Arithmetic

Part I – Experience is Quantum Information Processing

Industry – Tech Giants

- IBM
  - IBM Q System One Computer Center
  - 53, 65-qubit processor for IBM Q Network
- Google AI
  - 54-qubit processor "Sycamore"
  - 72-qubit processor "Bristlecone"
- Microsoft
  - Quantum Development Kit
  - Q# Programming Language
  - Azure Quantum – cloud service
- intel
  - 49-qubit processor



nature

Explore our content | Journal information

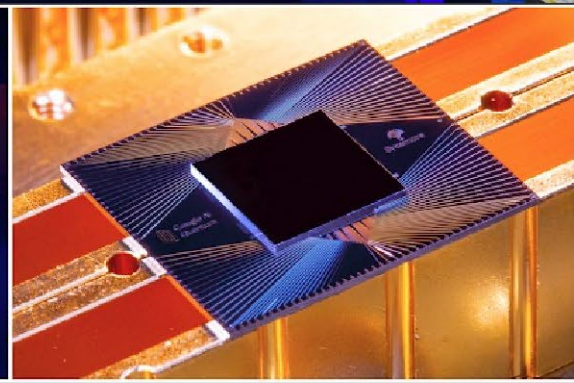
nature > articles > article

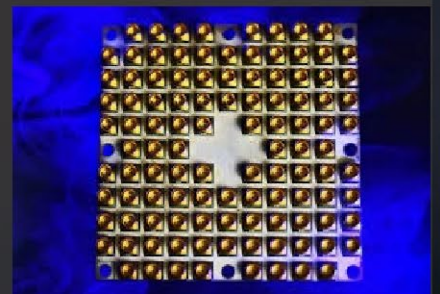
Article | Published: 23 October 2019

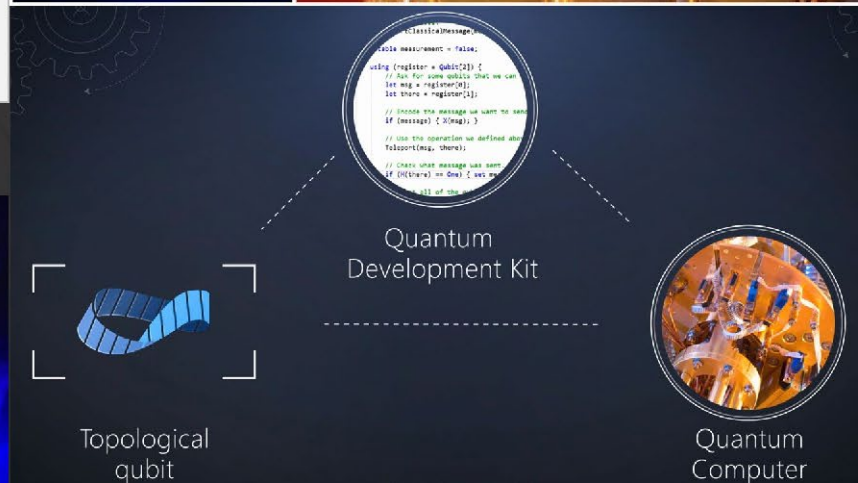
Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

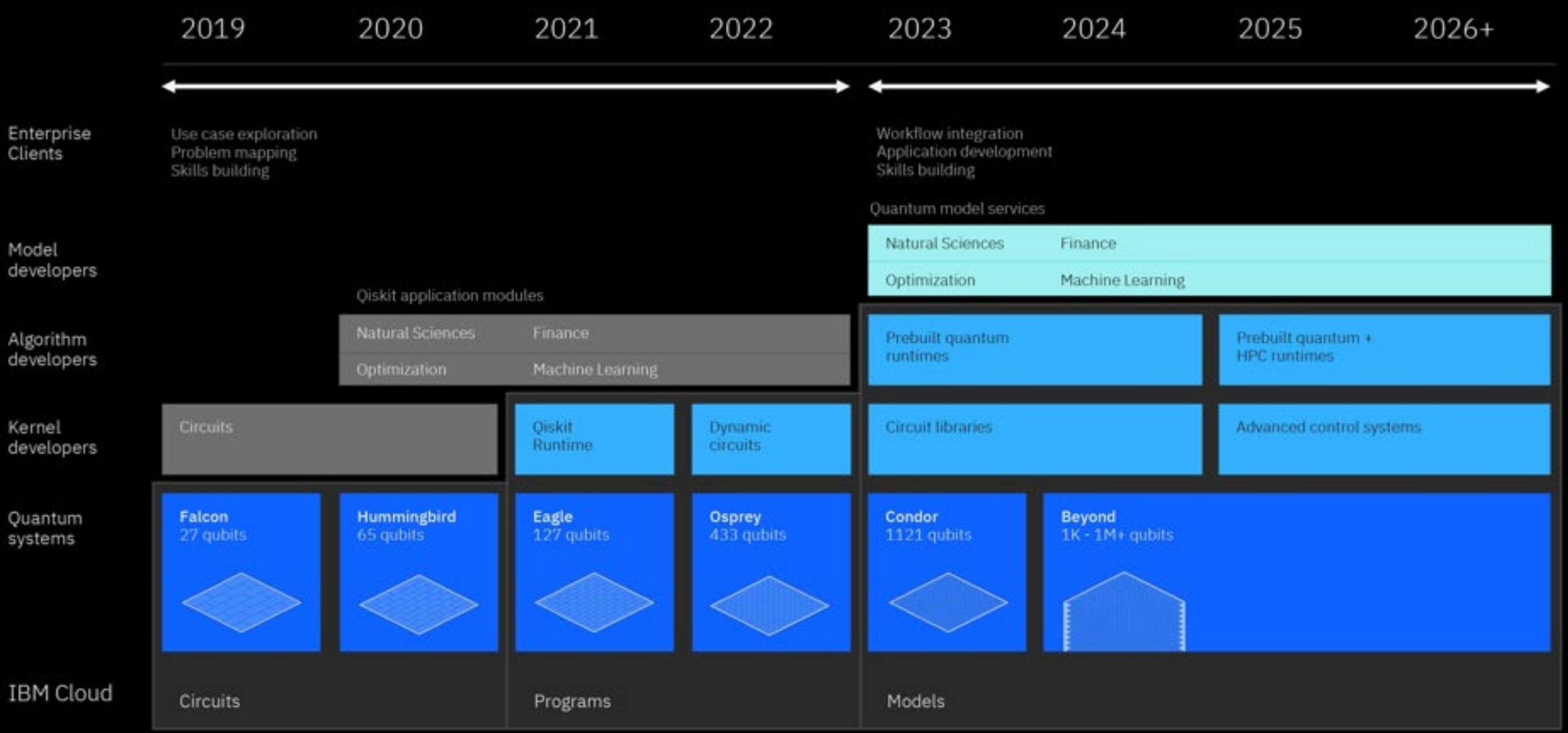






Development Roadmap

IBM **Quantum**

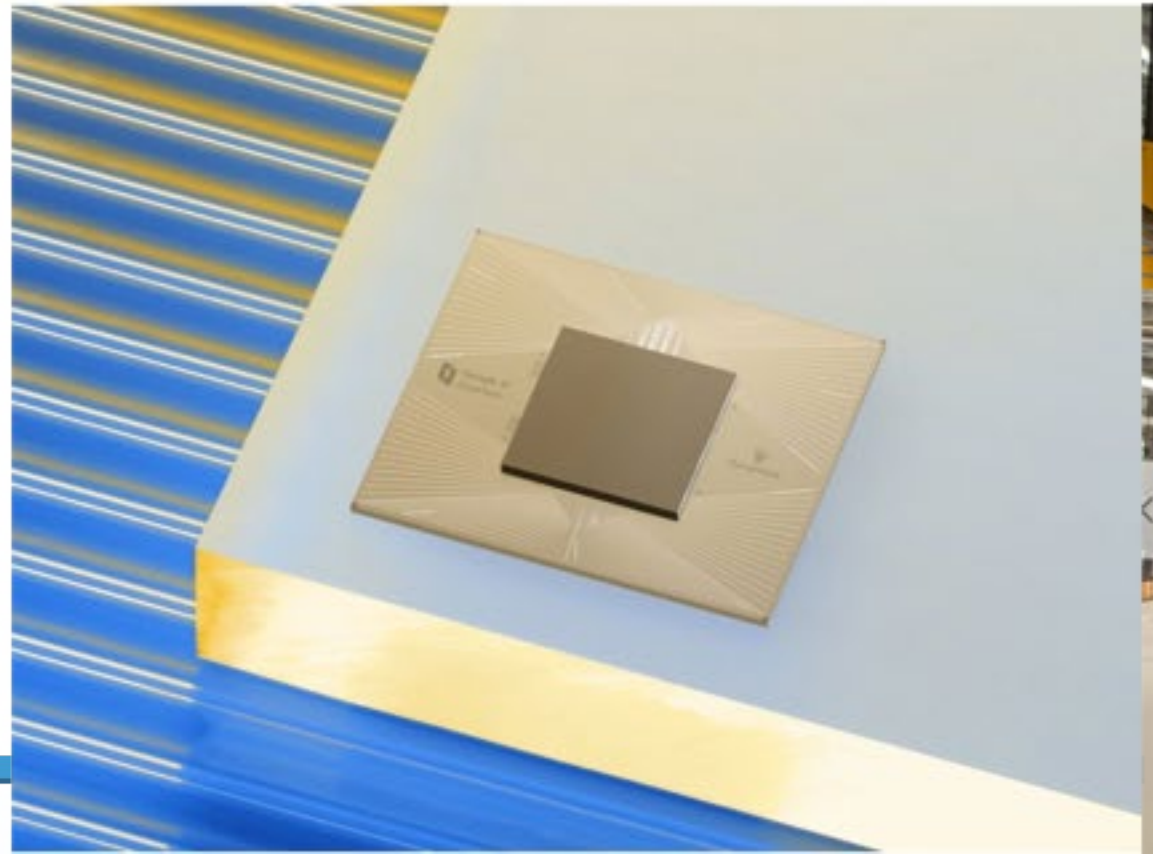


THE WALL STREET JOURNAL.

CIO JOURNAL

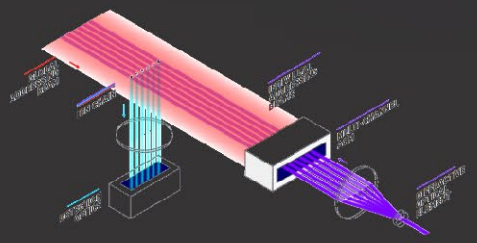
Google Aims for Commercial-Grade Quantum Computer by 2029

Tech giant is one of many companies racing to build a business around the nascent technology

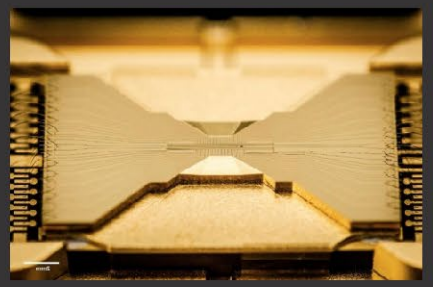


Other Quantum Processors

Trapped Ion



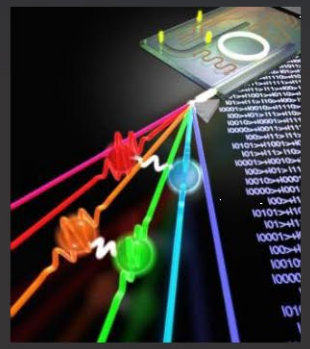
IONQ



(32 qubits)

Honeywell

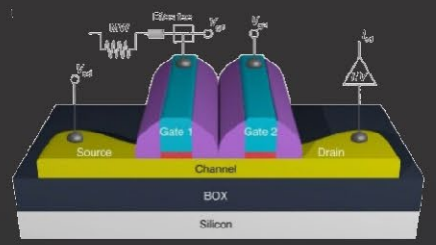
Photonics



XANADU

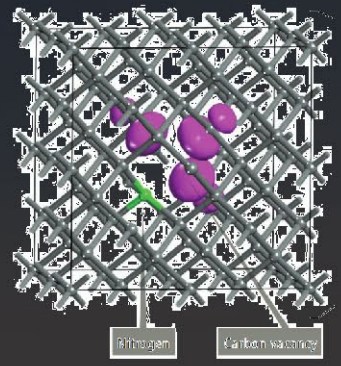
PsiQuantum

Silicon-Based Spin



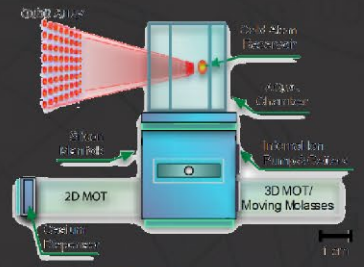
Silicon Quantum Computing

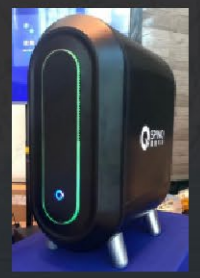
NV Center-in-Diamond



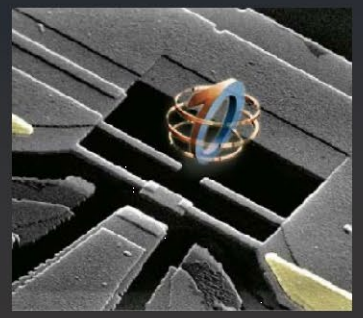
QUANTUM BRILLIANCE

NMR

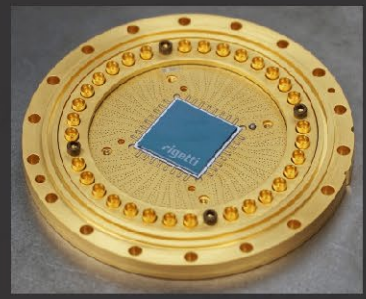




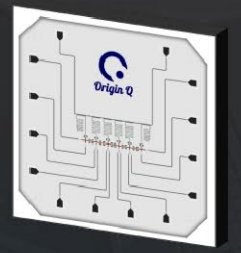
Superconducting



rigetti



本源量子 Origin Quantum



Quantum Information Processing (QIP)

- *Quantum information science* have demonstrated advantages in several fields:
  - Computing: speed-ups certain computational tasks where no classical methods can do.
  - Communication: entanglement-assisted communication increases channel capacity.
  - Cryptography: extending classical key with information-theoretic security.
  - Sensing: more accurate estimation, positioning, and synchronization.
  - Simulation: simulating complex reactions that are formidable for classical computers.
- Any other applications/advantages of quantum information technologies?
- Artificial intelligence and machine learning tasks are essentially implemented on a physical device. How about doing the job on a quantum computational device?
- Can quantum information science revolutionize the way of learning from data?

An Invited Blog Article in OpenFPGA Foundation

Naveed Sherwani • 2nd
Chairman at Silicon Federation
1d •

+ Follow ···

FPGAs and Quantum computing.

As McKinsey consulting estimated, quantum computing industry was worth $507.1 million in 2019, and may exceed $65 billion by 2030. Quantum key distribution (QKD) market was estimated to be $89 million in 2020 and projected to reach $214 million by 2025. FPGAs' customised design methodology and pipeline parallelism features allow us to design quantum computing emulators involving physically representing qubit structure and displaying actual quantum behavior. On the other hand, FPGAs' flexible fabric and adaptable interfaces facilitate the construction of classical-quantum signal co-processing in QKD systems, thereby increasing the secure key rates.

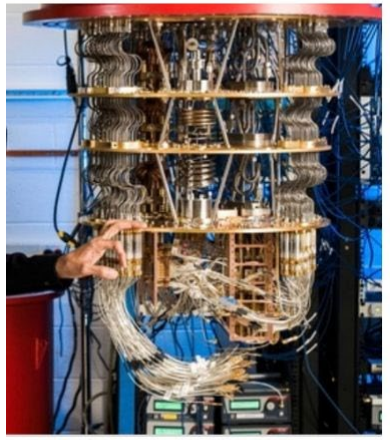
A recent IEEE MICRO article (https://lnkd.in/gszrEeZ)
from Dr. He Li presented a detailed review of state-of-the-art development of quantum computing emulators and quantum key distillation accelerators on FPGAs, with a balance between theoretical, implementational and technological results.

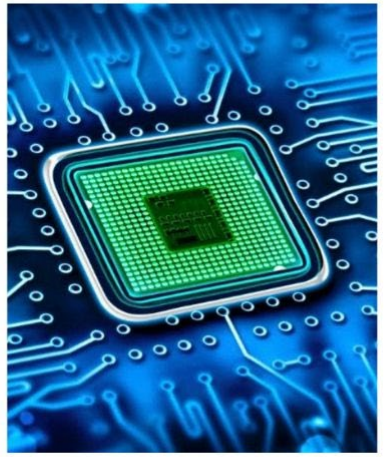
See details in https://lnkd.in/gYSpsdU

#fpgas #osfpga #quantumcomputing

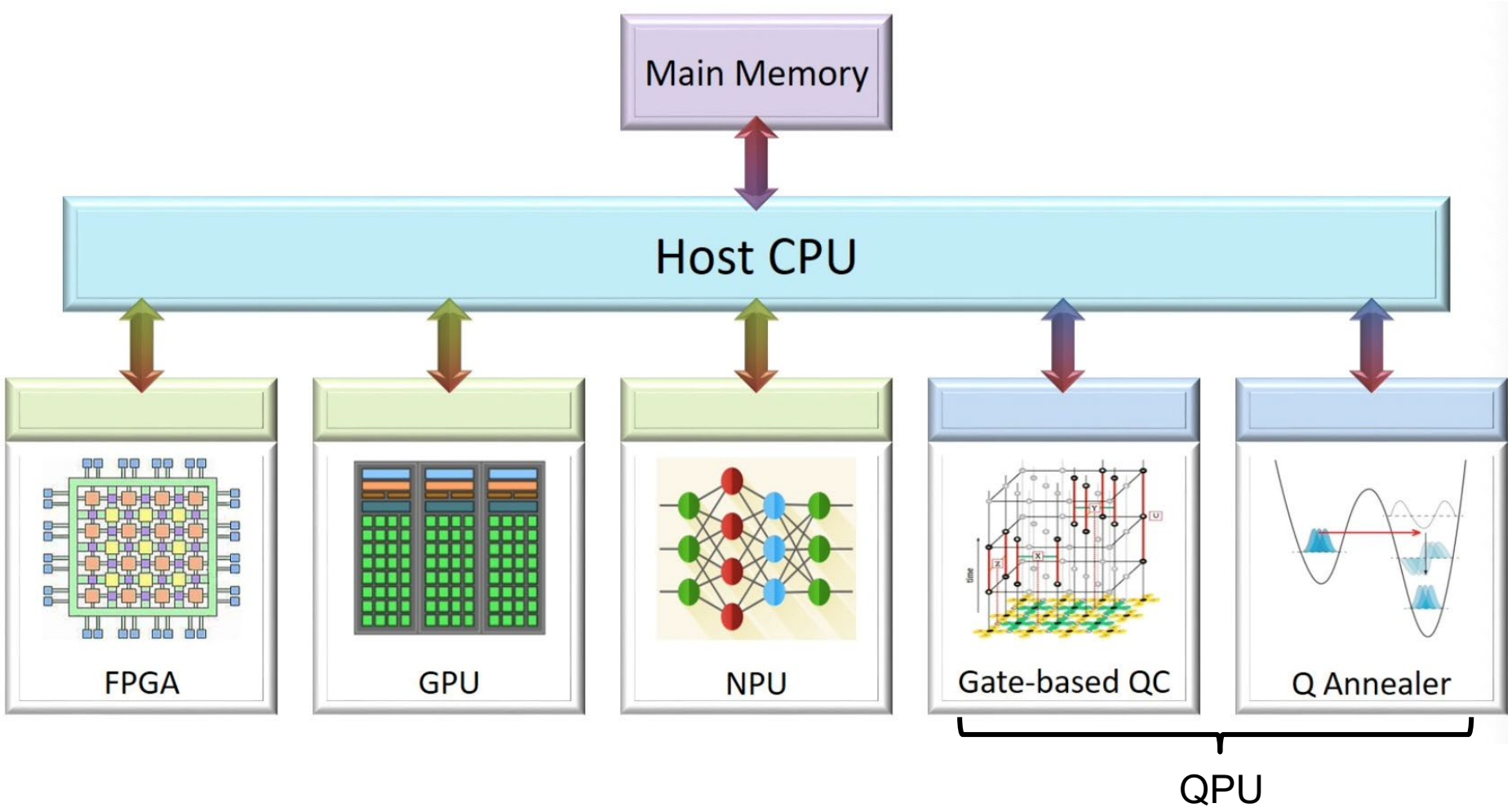
Dr. He Li

When FPGAs meet Quantum Information





Classical-Quantum Co-design System



Source: https://arxiv.org/abs/2102.02035

Case study: Experimental demonstration of practical, high-speed CV-QKD System

- Designing and implementing practical, field deployable, high speed CV-QKD system: Investigating the viability of low cost and commercially available analogue to digital converters (ADC) and digital to analogue converters (DAC).

- Demonstrating fully operational CV-QKD systems that can monitor parameters in real-time and distil secret keys in real time.

Ref: Weerasinghe A, Alhussein M, Li H, Wonfor A, Penty R. Experimental demonstration of practical high-speed Gaussian coherent state continuous-variable quantum key distribution with real-time parameter monitoring and key distillation. SPIE Photonex, 2023.

CV-QKD hardware system

- Our system operates at a symbol rate of 40 MHz and housed in 19-inch rack mounting boxes at Alice and Bob.
- DAC module: modulation signal generation at Alice, ADC module: recording data at Bob

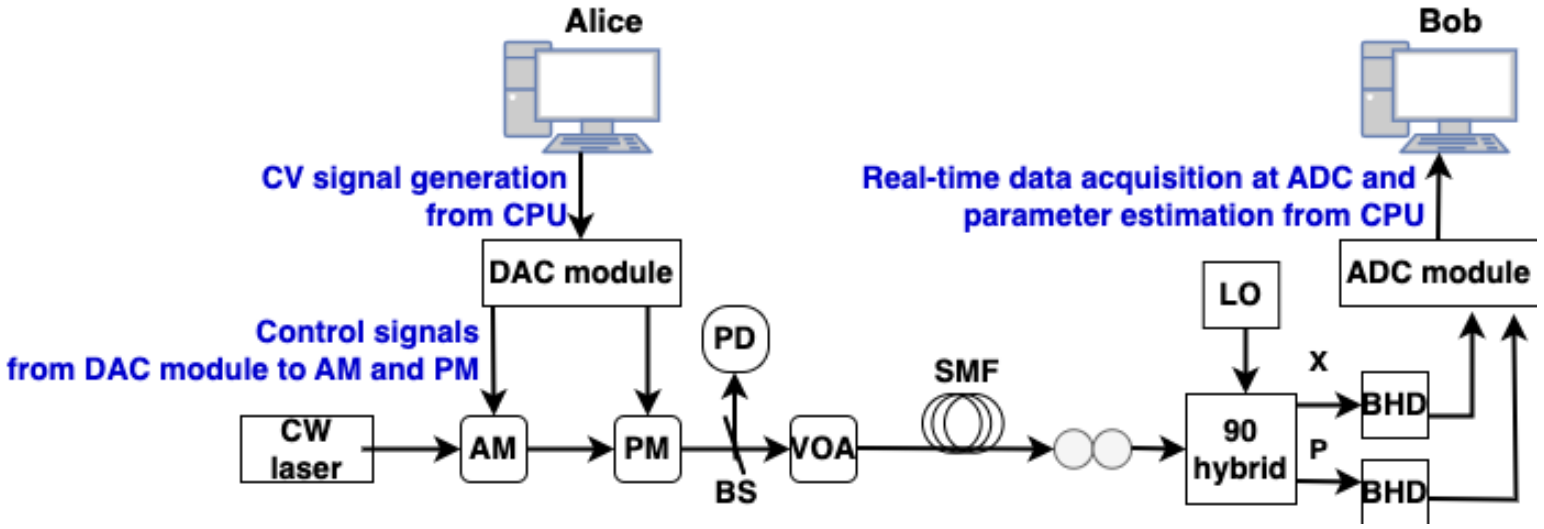


Fig.1. Optical hardware of our CV-QKD system: CW- continuous wavelength, AM- amplitude modulator, PM- phase modulator, BS- beam splitter, PD- photodiode, VOA- variable optical attenuator, SMF- single mode fibre, LO- local oscillator, BHD- balanced homodyne detector

Table 1. System parameters of our CV-QKD system

Parameter	Value
Repetition frequency	40 MHz
Detector efficiency	0.50
Detector bandwidth	400 MHz
Electrical noise	0.10 (Shot noise units)
Modulation variance	2.2
Reconciliation efficiency	0.95
Laser wavelength	1550 nm
Laser linewidth	100 kHz

Ref: Weerasinghe A, Alhussein M, Li H, Wonfor A, Penty R. Experimental demonstration of practical high-speed Gaussian coherent state continuous-variable quantum key distribution with real-time parameter monitoring and key distillation. SPIE Photonex, 2023.

Real-time parameter monitoring and post processing toolchain

- Parameters monitored in real-time at Bob: **excess noise**, **phase noise**, **shot noise**, and **bit error rates (BER)** after slice reconciliation. 10% of data in a block is used to monitor these parameters.

- Can detect faulty operations of the system immediately.

- Post processing toolchain run on a GPU will achieve real time key distillation (currently run offline on a CPU):
  - Phase drift compensation using LO and reference pulses.
  - Slice reconciliation for converting to binary data.
  - Error reconciliation with low density parity check codes with adaptive code rates.
  - Privacy amplification to distil secret keys.

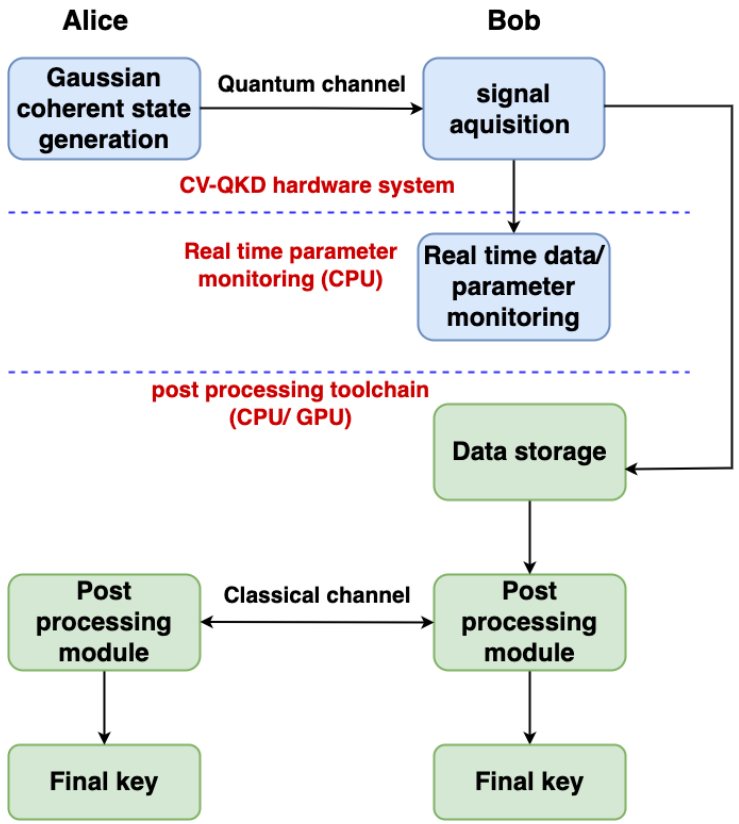


Fig. 2. Schematic of the front-end optical hardware system, real-time parameter monitoring and back-end post processing toolchain of our GMCS CV-QKD system: Central processing unit (CPU), graphical processing unit (GPU).

Ref: Weerasinghe A, Alhussein M, Li H, Wonfor A, Penty R. Experimental demonstration of practical high-speed Gaussian coherent state continuous-variable quantum key distribution with real-time parameter monitoring and key distillation. SPIE Photonex, 2023.

Results

- Asymptotic key rates estimated from average parameters measured over several hours: **4.6 Mb/s (20 km), 3.2 Mb/s (25 km), 0.8 Mb/s (50 km)**
- Secret key rates with finite size effects: **3.1 Mb/s (20 km), 2.3 Mb/s (25 km), 0.5 Mb/s (50 km)**

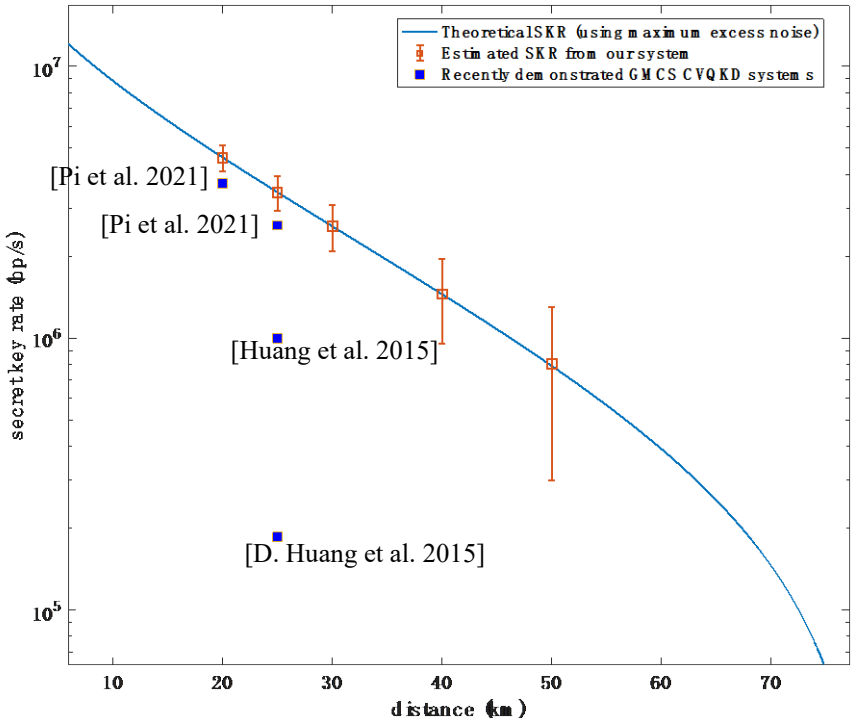


Fig. 3. Secret key rate vs. transmission distances for our CV-QKD system: Red points with error bars show the range of secret key rates estimated from measured excess noise from the system. The blue points represent the secret key rate values from the corresponding references.

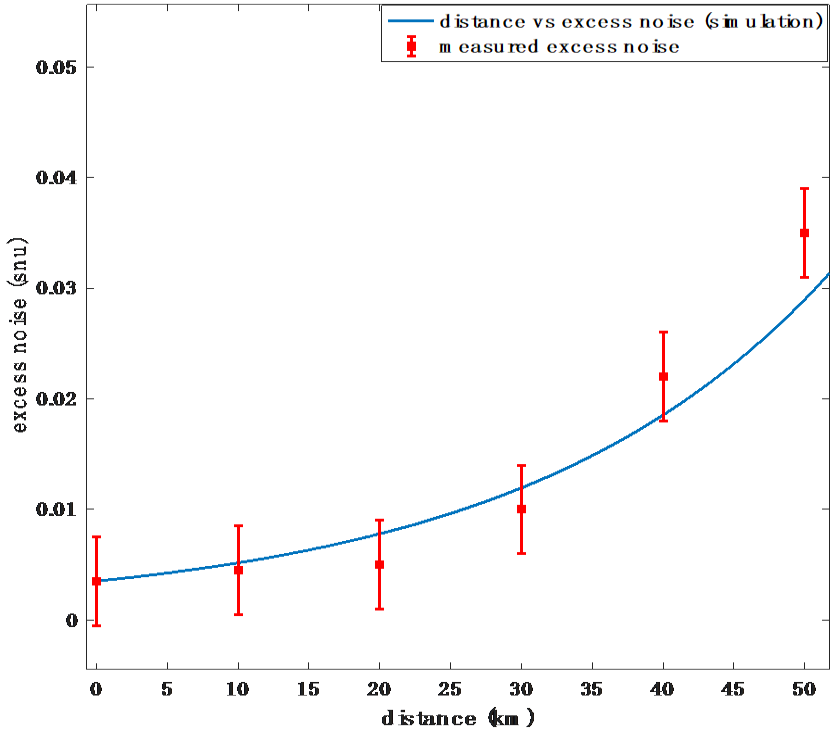


Fig. 4. Excess noise measured from our real-time parameter monitoring system is shown by red markers with error bars. The blue curve shows the expected excess noise levels from our CV-QKD system using a simulation.

Ref: Weerasinghe A, Alhussein M, Li H, Wonfor A, Penty R. Experimental demonstration of practical high-speed Gaussian coherent state continuous-variable quantum key distribution with real-time parameter monitoring and key distillation. SPIE Photonex, 2023.

Summary

- We have demonstrated a practical, field deployable, high-speed GMCS CV-QKD system at 40 MHz symbol rate.
- Our system consists of front-end optical hardware system and back-end real-time parameter monitoring and post processing toolchain. We distil secret keys offline from collected data.
- We have achieved a secret key rate of 2.3 Mb/s (with finite size effects) at 25 km transmission distance.
- We are currently working on a higher symbol rate real-time system and field trial.

Ref: Weerasinghe A, Alhussein M, Li H, Wonfor A, Penty R. Experimental demonstration of practical high-speed Gaussian coherent state continuous-variable quantum key distribution with real-time parameter monitoring and key distillation. SPIE Photonex, 2023.

Part II – Quantum Arithmetic and MSDF Arithmetic

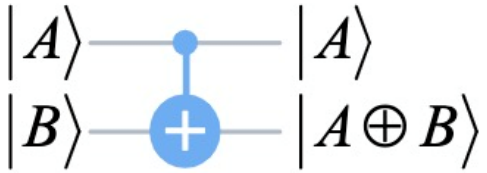
Motivations:

- Quantum Computing (QC) or Quantum Machine Learning (QML) has become more and more popular…
- Before we run actual quantum computing algorithm, can we think about the fundamental elements to build quantum circuits for quantum algorithms?
- What arithmetic algorithm and arithmetic circuits can be used for generic QC & QML?

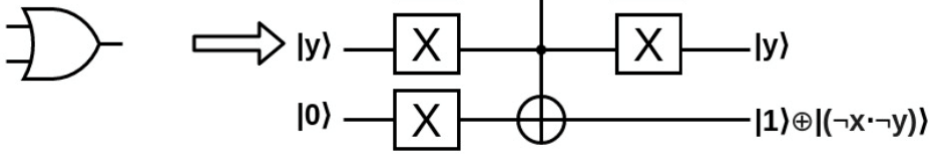
Gate-based Quantum Computation

NOT gate

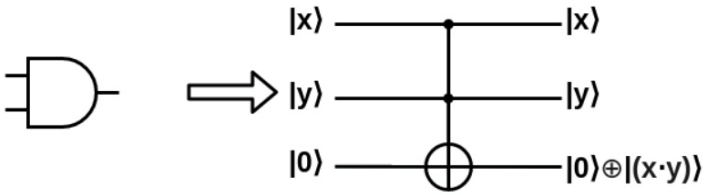
CNOT gate



OR gate



AND gate



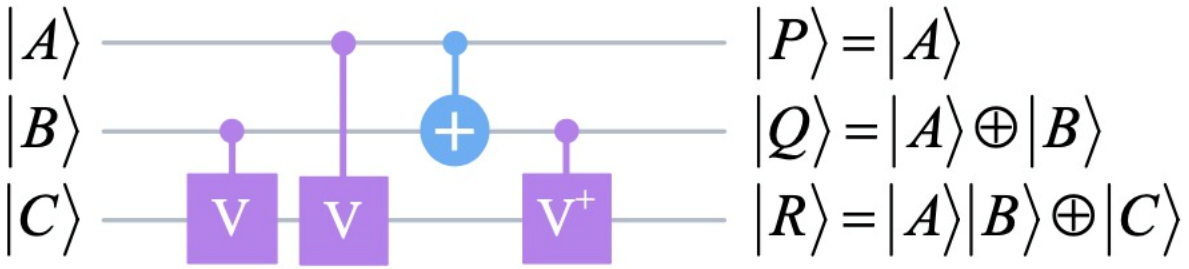
H gate

Y gate

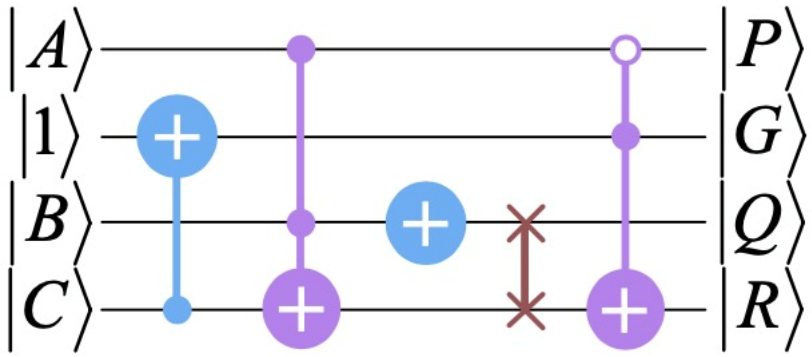
S gate

T gate

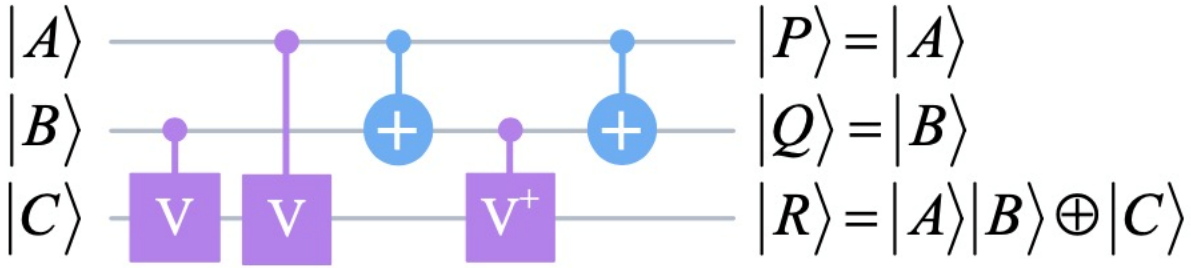
Gate-based Quantum Computation



Toffoli gate

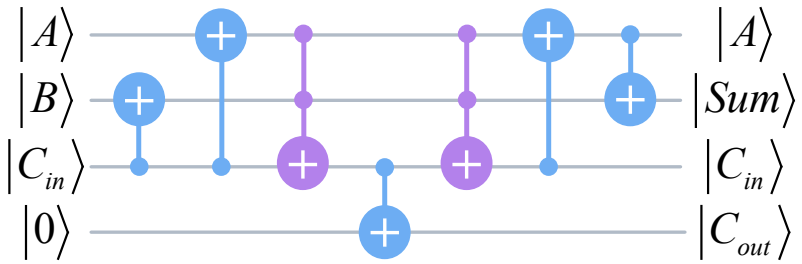


Khan (NG) gate

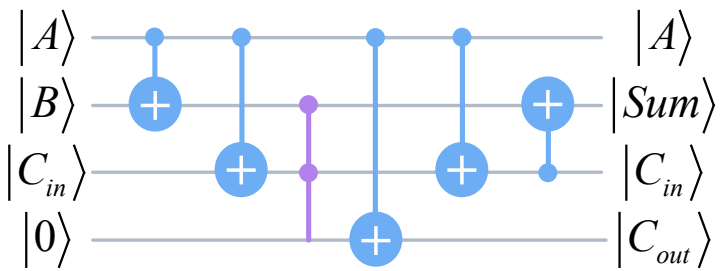


Peres gate

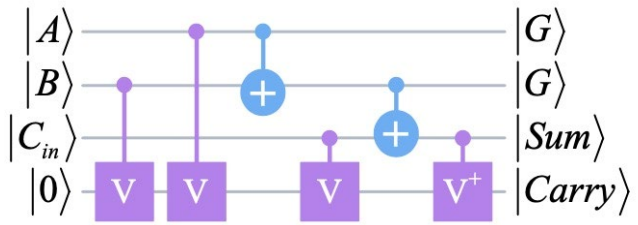
Case Study: Binary Quantum Full Adder (BQFA)



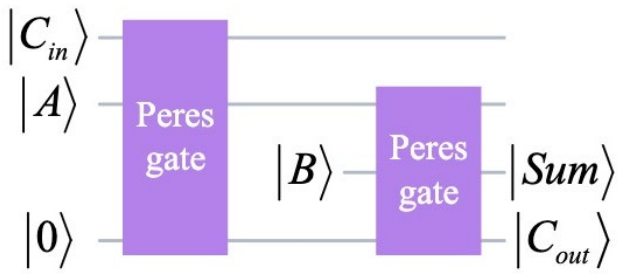
BQFA with 4 qubits [1]



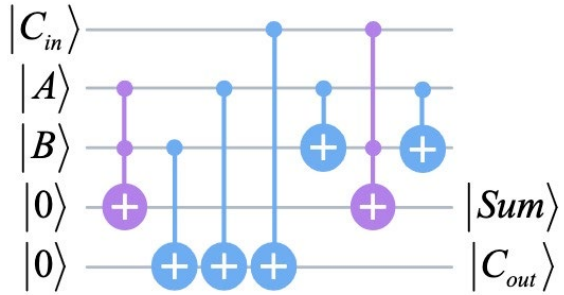
BQFA with 4 qubits [2]



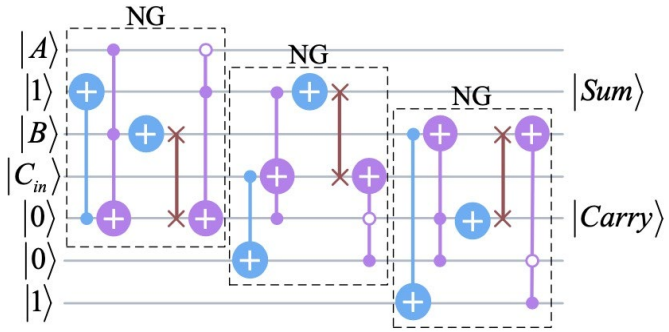
BQFA with 4 qubits [3]



BQFA with 4 qubits [4]



BQFA with 5 qubits [5]



BQFA with 7 qubits [6]

REF:
[1] S. A. Cuccaro, T. G. Draper, S. A. Kutin, and D. P. Moulton, “A new quantum ripple-carry addition circuit,” arXiv preprint quant-ph/0410184, 2004
[2] C. Gidney, “Halving the cost of quantum addition,” Quantum, vol. 2, p. 74, 2018.
[3] A. K. Biswas et al., “Efficient approaches for designing reversible binary coded decimal adders,” Microelectronics journal, vol. 39, no. 12, 2008.
[4] M. Islam et al., “A novel quantum cost efficient reversible full addergate in nanotechnology,” arXiv preprint arXiv:1008.3533, 2010.
[5] M. A. Sohel et al., “Quantum computing based implementation of fulladder,” IEEE International Conference for Innovation in Technology,2020
[6] M. Mazumder, “Synthesis of quantum circuit for full adder using khan gate,” International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 6, no. 6, 2017.

Comparison of Binary Quantum Full Adder

Design methods	# qubits	# gates						# garbage qubits	Circuit depth					
		NOT	CNOT	Toffoli	Peres	V	Logical AND		NOT	CNOT	Toffoli	Peres	V	Logical AND
Mazumder *et al.* [5]	7	3	3	6	0	0	0	5	3	3	6	0	0	0
Sohel *et al.* [6]	5	0	5	2	0	0	0	3	0	4	2	0	0	0
Islam [7]	4	0	0	0	2	0	0	2	0	0	0	2	0	0
Biswas *et al.* [8]	4	0	2	0	0	4	0	2	0	2	0	0	4	0
Cuccaro *et al.* [9]	4	0	5	2	0	0	0	2	0	4	2	0	0	0
Gidney [26]	4	0	5	0	0	0	1	2	0	3	0	0	0	1

less non-Clifford gates

Left-to-Right Computing

Miloš D. Ercegovac

Cycle	-2	-1	0	1	2	$\cdots$
Input	x_1	x_2	x_3	x_4	x_5	$\cdots$
Compute			z_1	z_2	z_3	$\cdots$
Output				z_1	z_2	$\cdots$

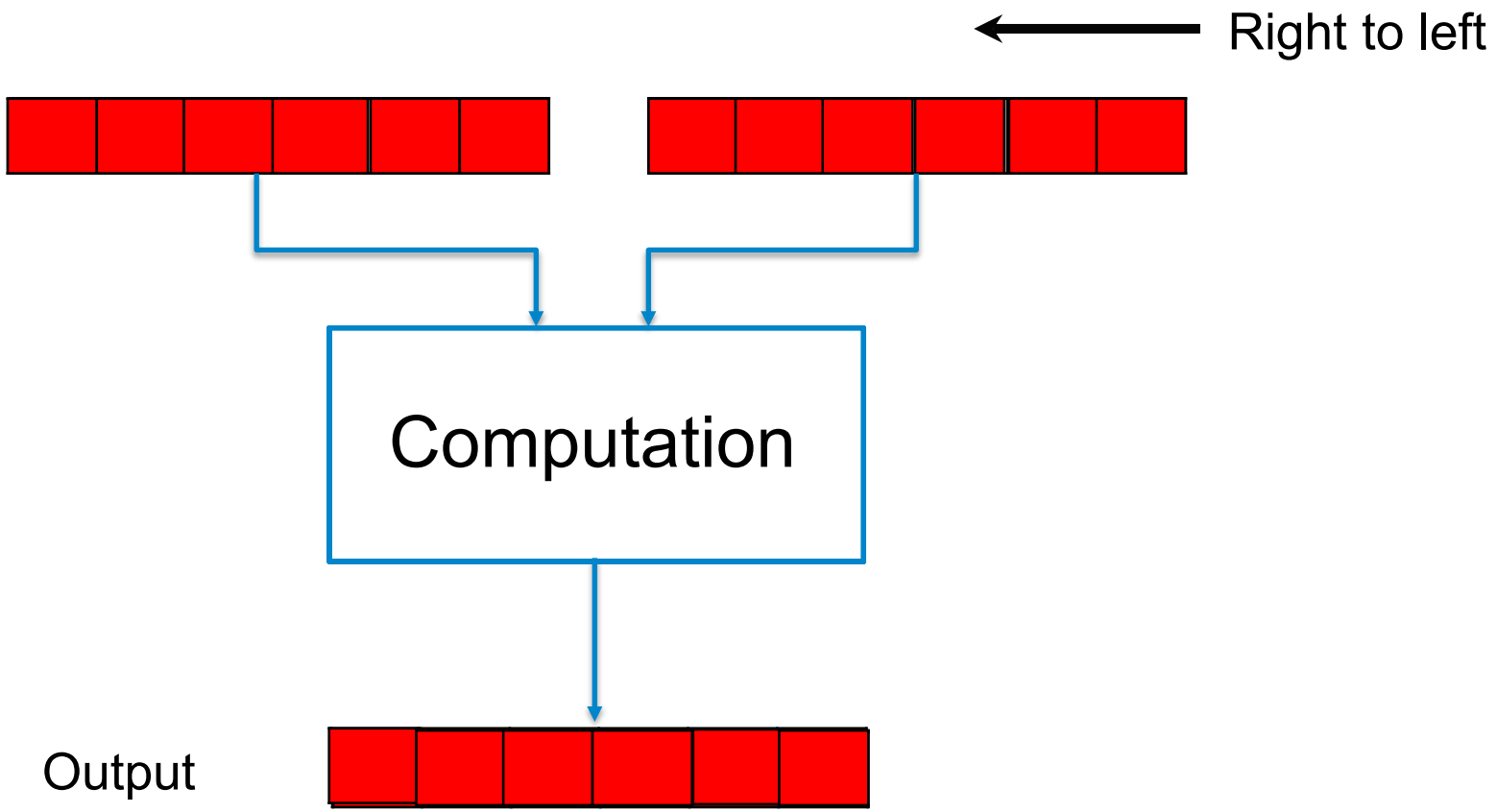
$\delta = 2$

Left-to-Right: online arithmetic

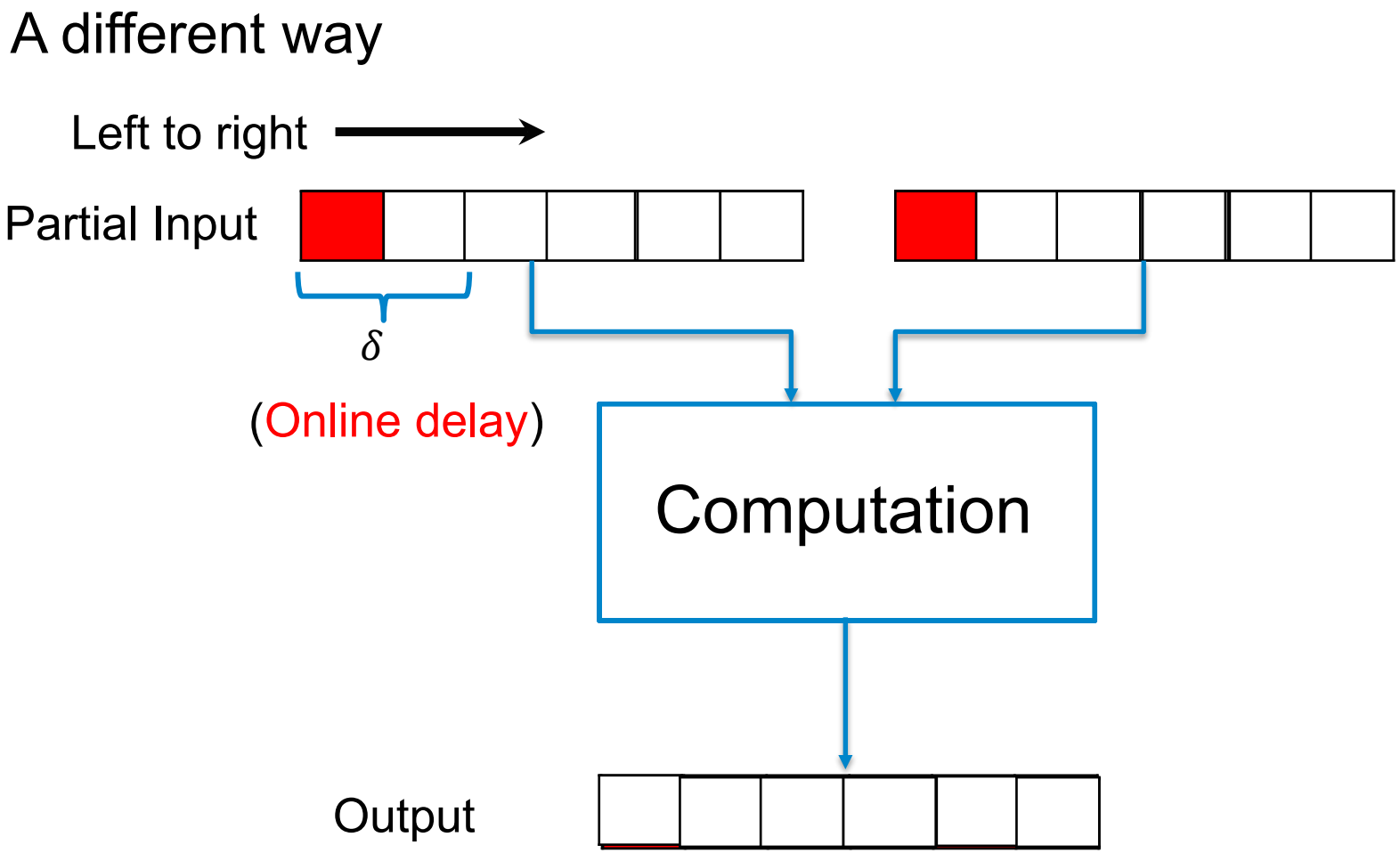
- Online arithmetic algorithms operate in a digit-serial most-significant digit mode
- To compute the first digit of the result, δ+ 1 digits of the input operands
- Thereafter, for each new digit of the operands, an extra digit of the result obtained
- The online delay δ typically a small integer, *e.g.*, 1 to 4.

Calculations with Different Arithmetic Paradigms

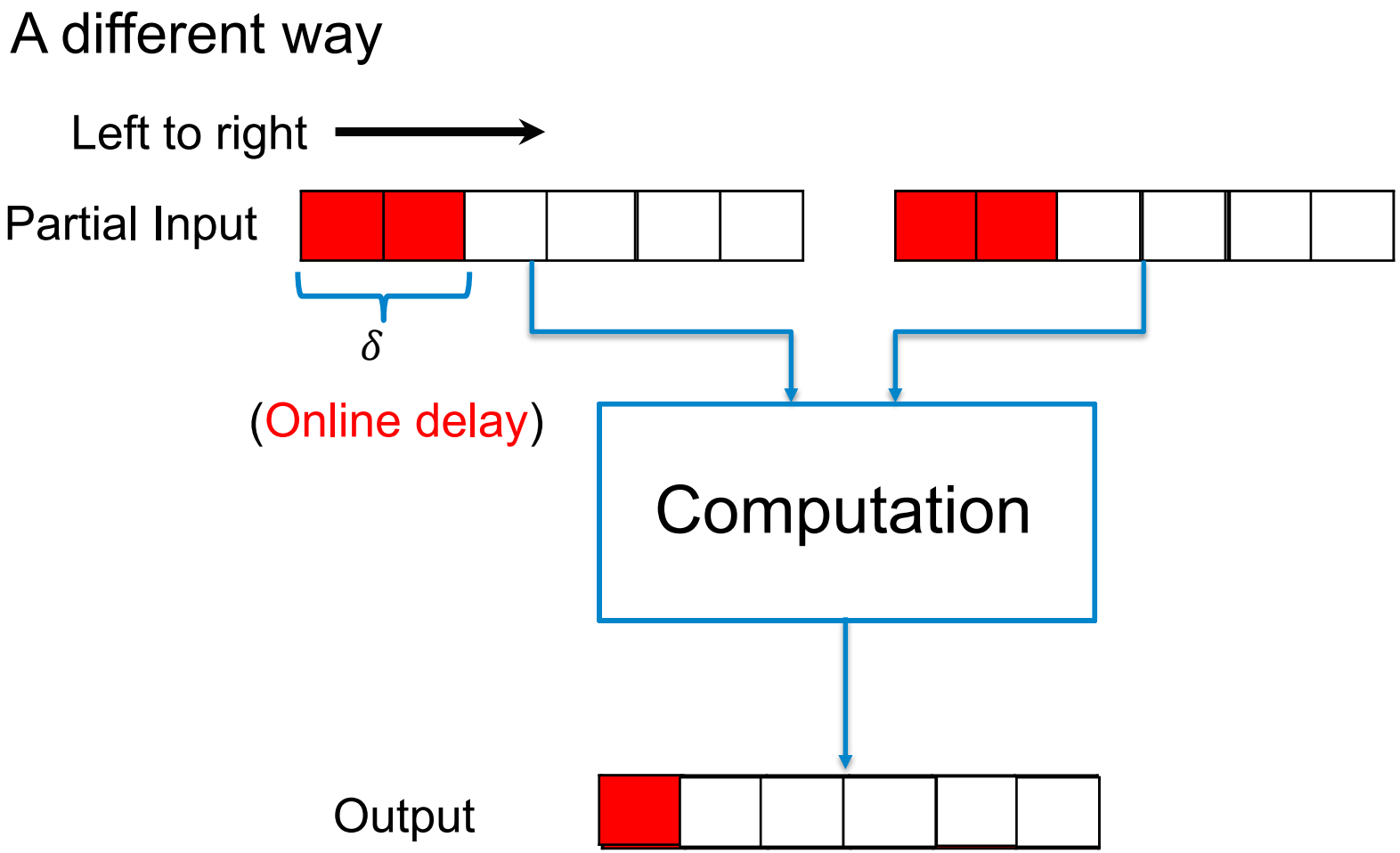
The normal way



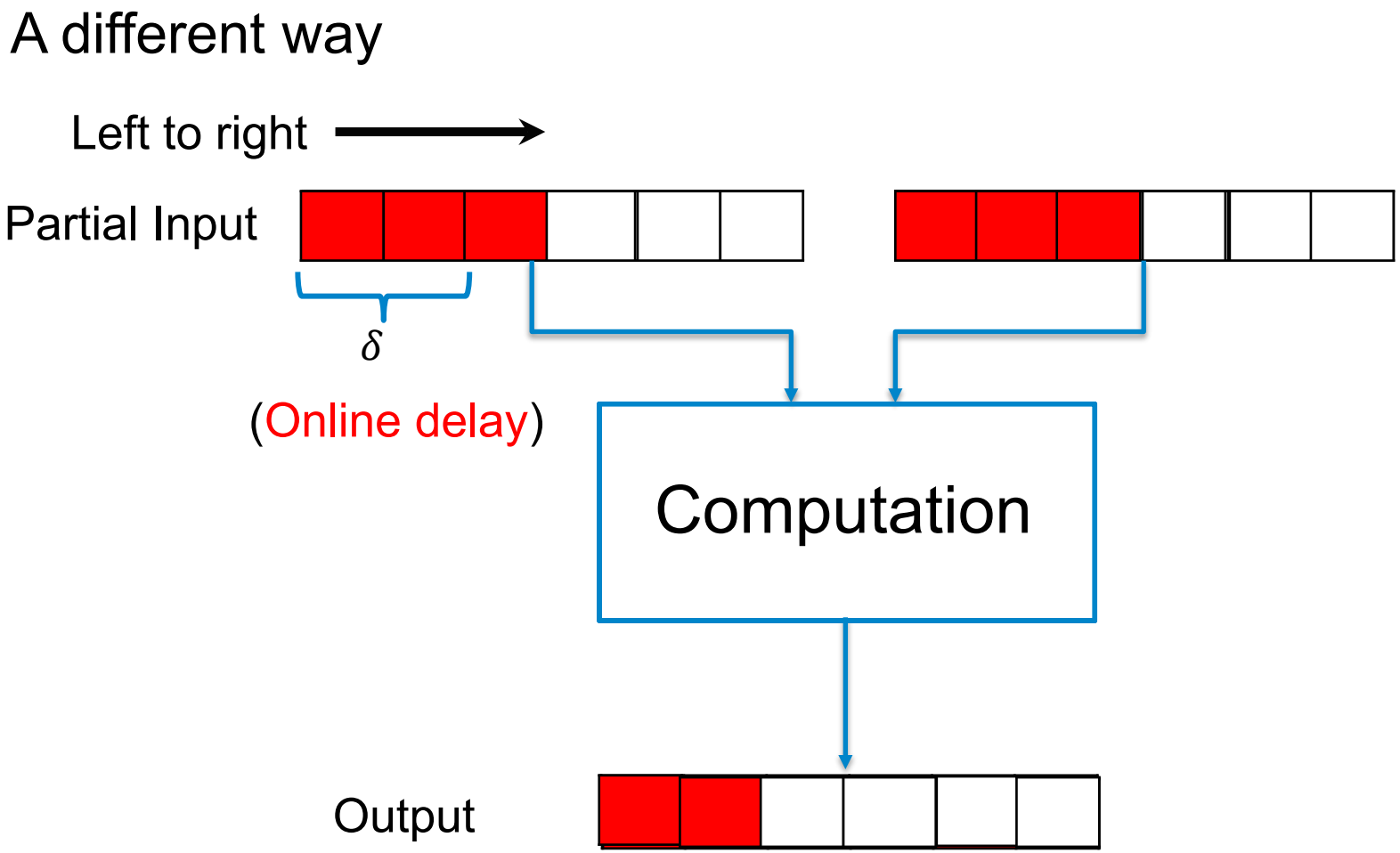
Arithmetic Paradigms



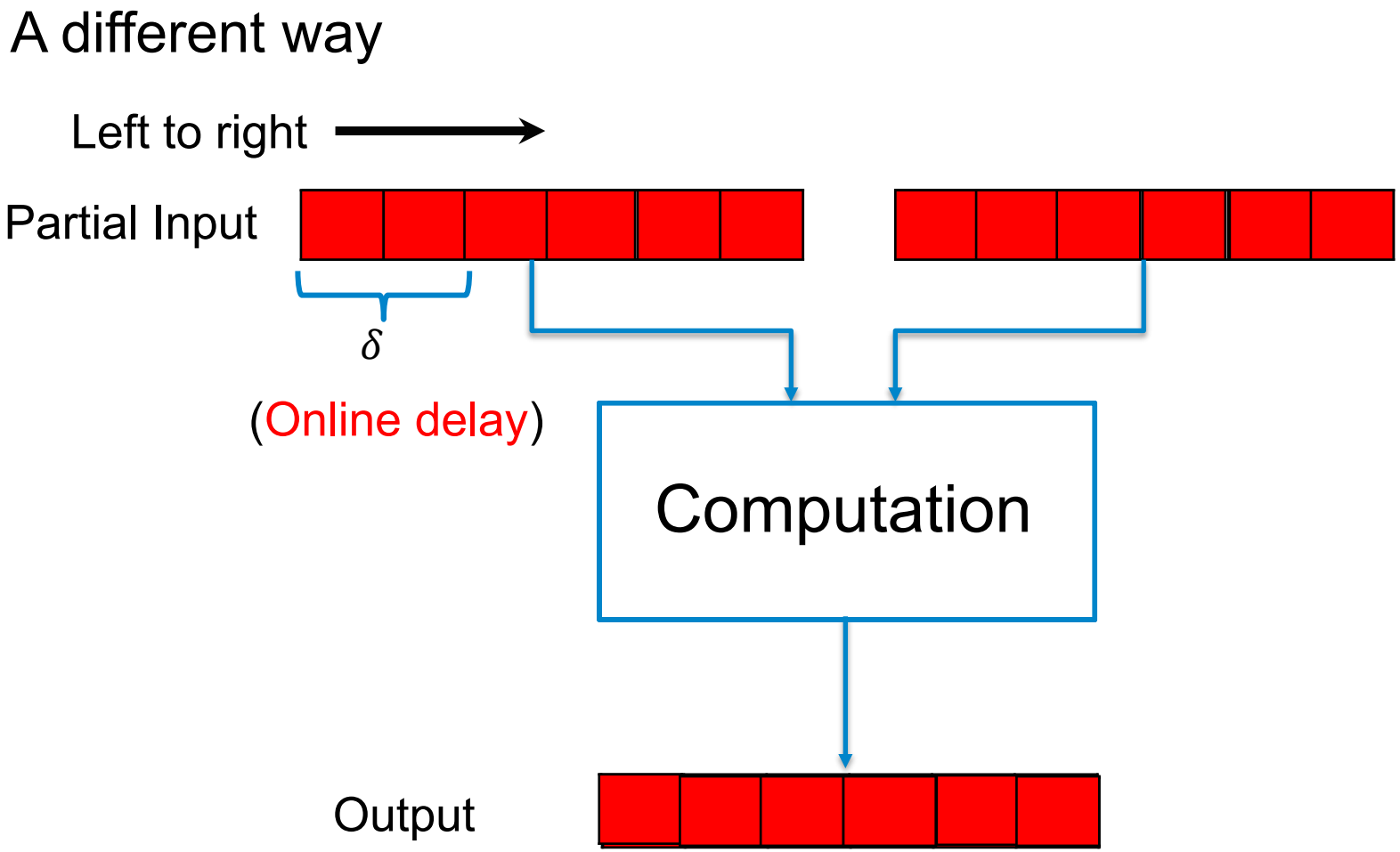
Arithmetic Paradigms



Arithmetic Paradigms



Arithmetic Paradigms



Application: Anytime Control

One-shot Control Algorithms

Fixed Precision:
specify a target precision in advance and only return one result.

Non-incremental:
start optimisation from scratch every time.

VS.

Anytime Control Algorithms

Increasing Precision:
return results of increasing precision over time.

Incremental:
generate results in stages which can be refined in variable precision.

Iterative Algorithms

- In numerical analysis

$$x^{(k+1)} = f\left(x^{(k)}\right)$$

$$x^* = \lim_{k\to\infty} x^{(k)}$$

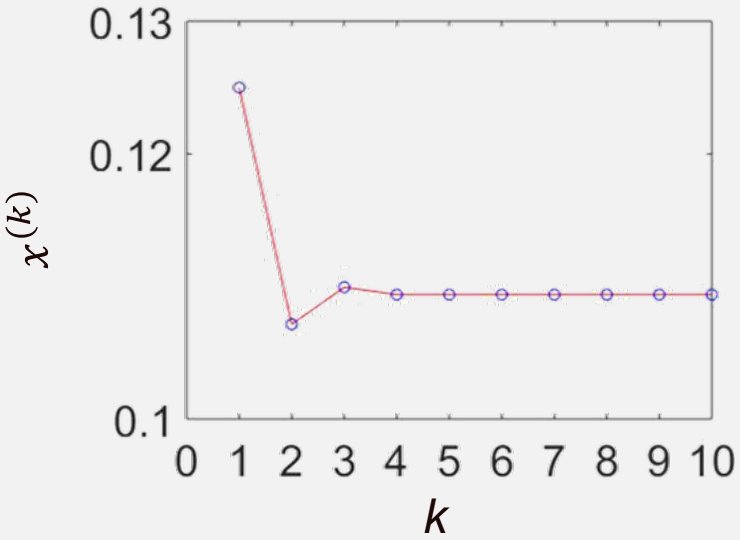
$$\left\|x^{(k)} - x^*\right\| < \eta$$

- Examples of this template:
  - Classic iterative methods:

    Jacobi & Newton's
  - Gradient descent method

Example (Jacobi)

$$x^{(k+1)} = {}^{1}/_{8} - {}^{1}/_{7}\,x^{(k)}$$



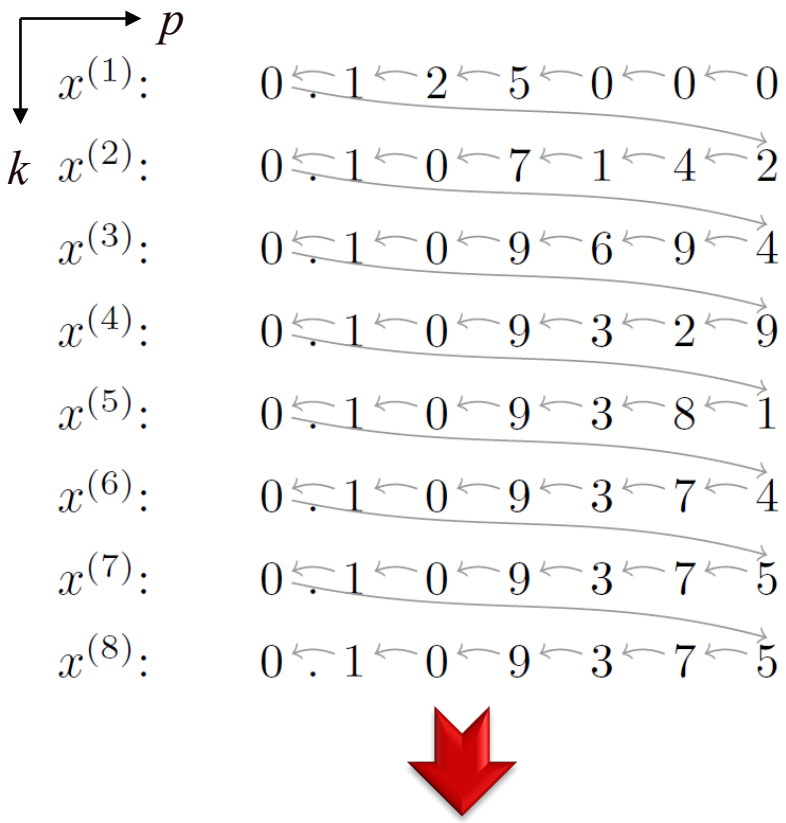
Iterating via LSDF

Jacobi: $x^{(k+1)} = {}^{1}/_{8} - {}^{1}/_{7}\, x^{(k)}$ using conventional arithmetic.

Question: If the result has not converged…

a) Run for more iterations *K*?

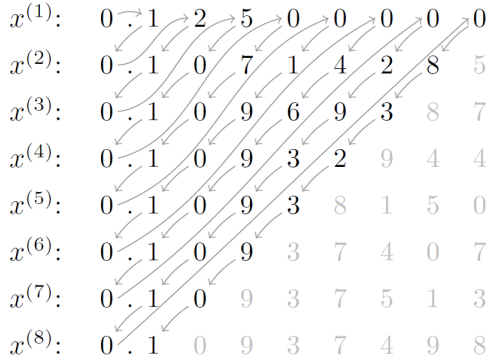
b) Restart with higher precision *P*?



ARCHITECT: Iterating via MSDF

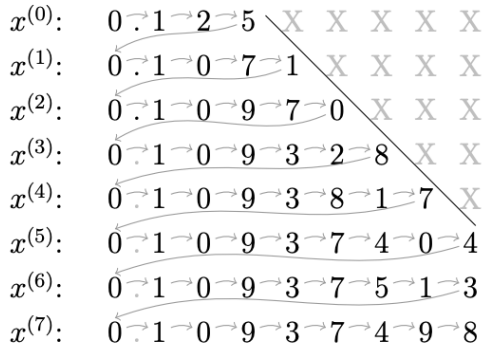
FPT'17 (Best paper)

Iterating exactly



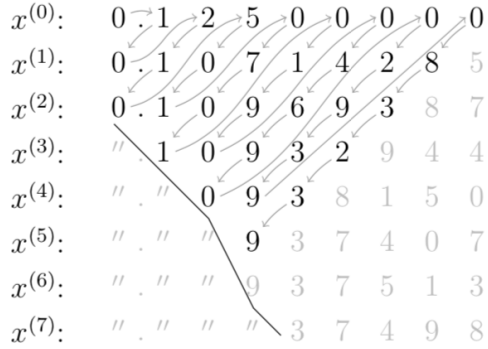
ARITH'18

Don't-care digit elision



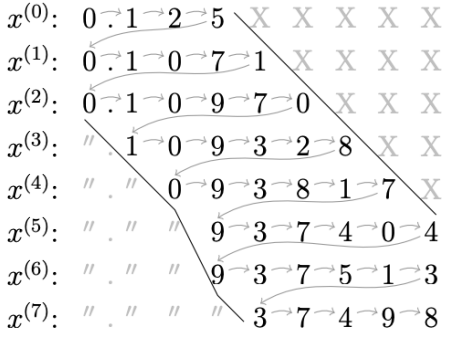
TVLSI'19

Don't-change digit elision



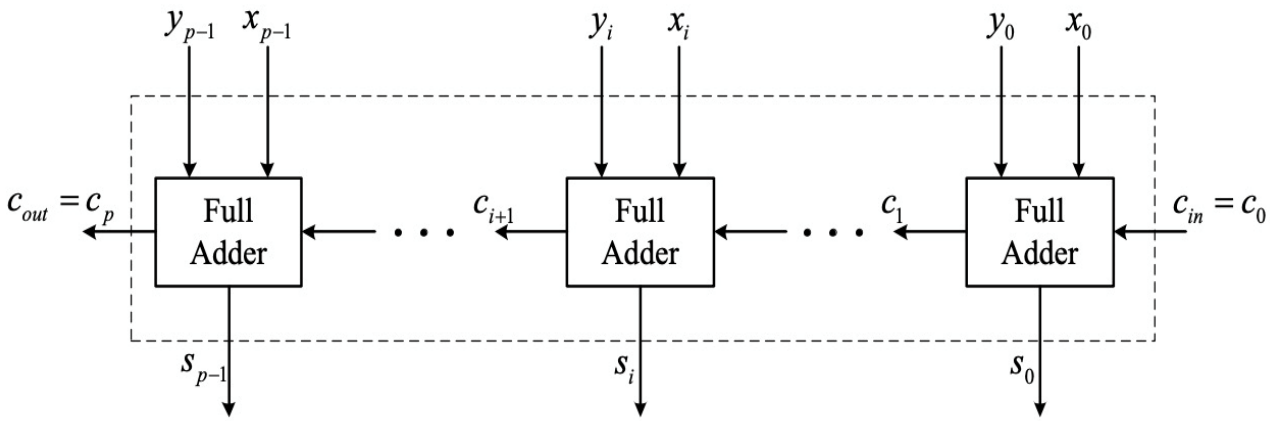
TC'20

Combined elision approach

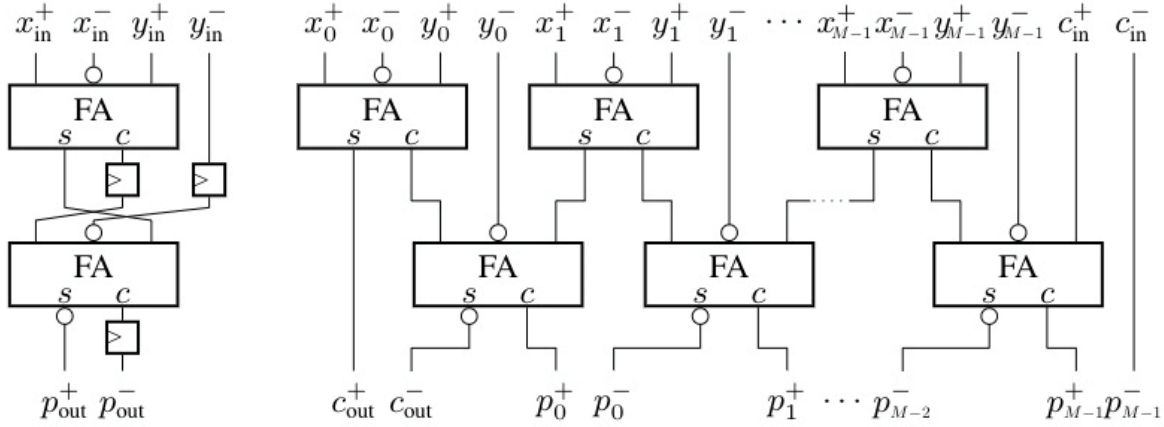


Part III – Quantum Most-Significant Digit-First Arithmetic

Carry-ripple Adder



MSDF Adder



Some Trials:

To address current problems

- ✓ Lack of consistent metrics used to evaluate each design.
- ✓ Lack of detailed design parameters discussion and comparison.

In this work,

1. Most-significant digit-first arithmetic and least-significant digit-first operators have been implemented, and will be further investigated.
2. Qubit-efficient arithmetic
3. Low-depth arithmetic
4. Low quantum gates

} Design space exploration

5. A library of benchmarking and generic metrics for comparison are also interesting directions.

Comparison of QLSDF and QMSDF Adders

TABLE II
COMPARISON OF BINARY QUANTUM FULL ADDER

Benckmark	Design methods	# qubits	# gates				Circuit depth			
			CX gate	Toffoli	Temporary logical-AND	T-count	CX gate	Toffoli	Temporary logical-AND	T-depth
QFA-1	Carry-first [21]	4	5	2	0	14	4	2	0	8
QFA-2	Sum-first	4	5	1	0	7	5	1	0	4
QFA-3	Gidney [13]	4	5	0	1	4	3	0	1	2

x p

TABLE III
COMPARISON OF DIFFERENT STRUCTURES OF QUANTUM MSDF ADDER.

Benckmark	Optimization strategy	Qubits	Implementation cost					Circuit depth				
			X gate	CX gate	Toffoli gate	Temporary logical-AND	T-count	X depth	CX depth	Toffoli depth	Temporary logical-AND	T-depth
QMDA-1	Use of QFA-1 (no strategy)	$6p+2$	$3p$	$10p$	$4p$	0	$28p$	2	8	4	0	16
QMDA-2	Fig. 6	$5p+2$	$3p$	$9p$	$4p$	0	$28p$	1	$6p+1$	$3p+1$	0	$12p+4$
QMDA-3	Fig. 7	$5p+3$	$3p$	$9p$	p	p	$11p$	1	$5p+2$	p	p	$6p$
QMDA-4	Fig. 8	$5p+2$	$3p$	$9p$	$p+1$	p	$11p+7$	1	$4p+1$	$p+1$	p	$6p+4$
QMDA-5	Fig. 9	$6p+2$	$3p$	$10p$	0	$2p$	$8p$	2	6	0	2	4

Quantum LSDF Full Adder: Carry-first & Sum-first

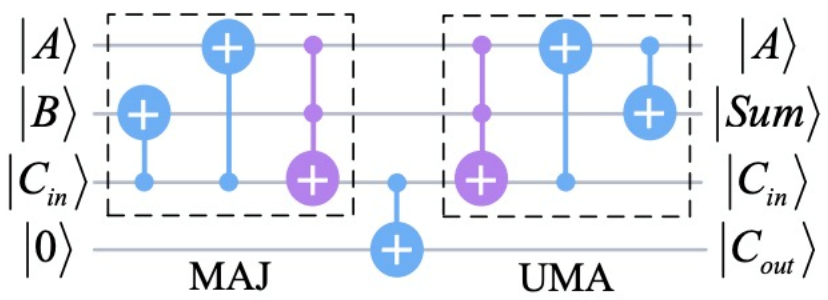


Fig. 2. Design of 4-qubit quantum full adder based on qubit state reuse [21], where MAJ ("majority") indicates the core calculation of a quantum addition, while UMA ("UnMajority and Add") is the additional calculation required.

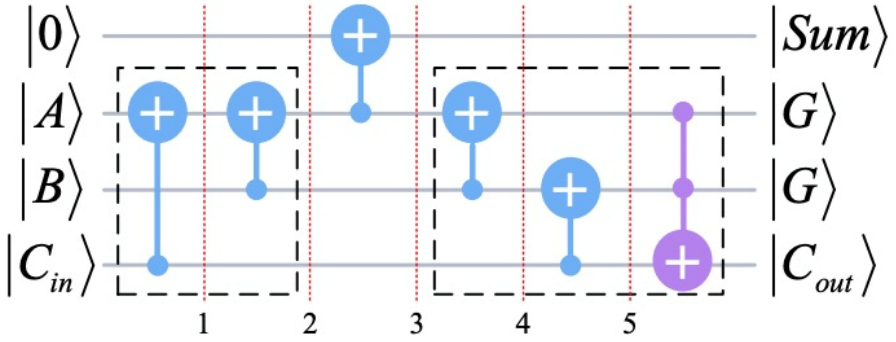
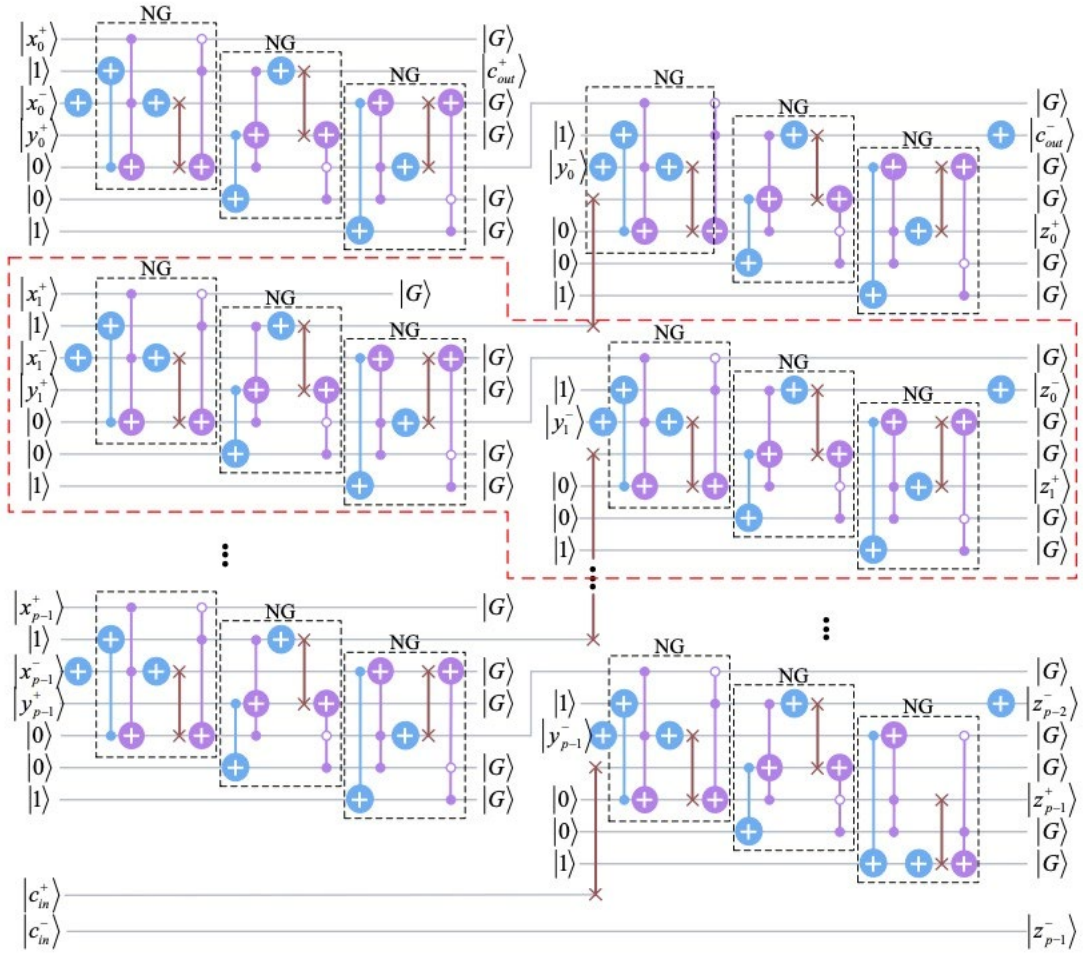


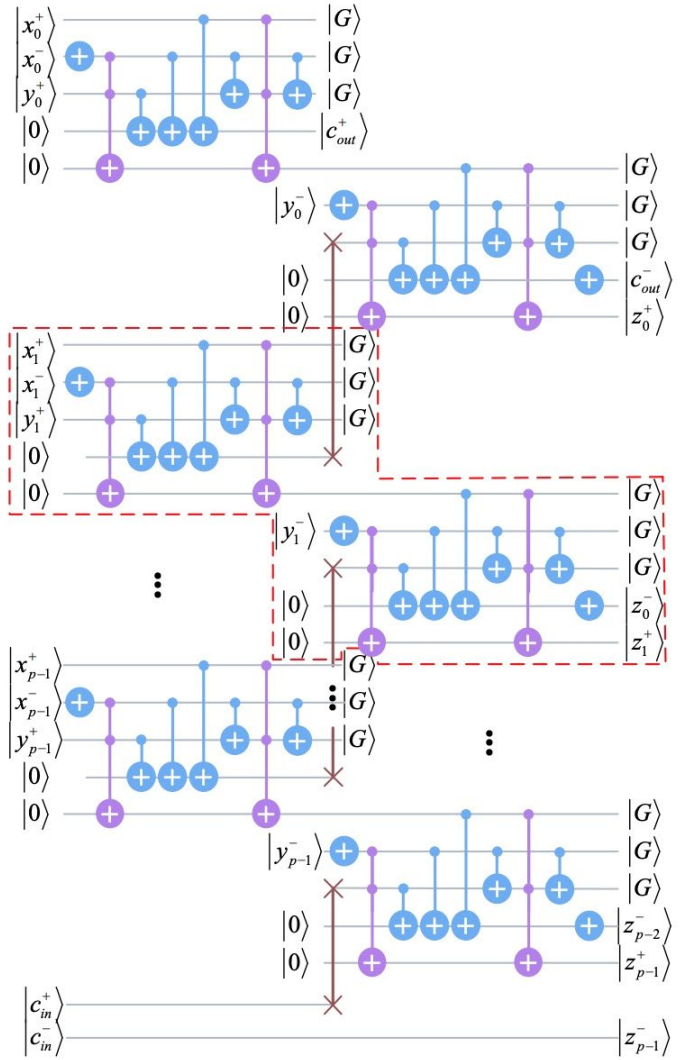
Fig. 5. Design of sum-first QFA, where the leftmost part generates the sum state, the middle gate duplicates the sum state to an inserted quantum circuit, and the rightmost part generates the carry state. The output states of four qubits are derived in Table I.

Generally Speaking…

Quantum MSDF Adders – #Qubits Reduction

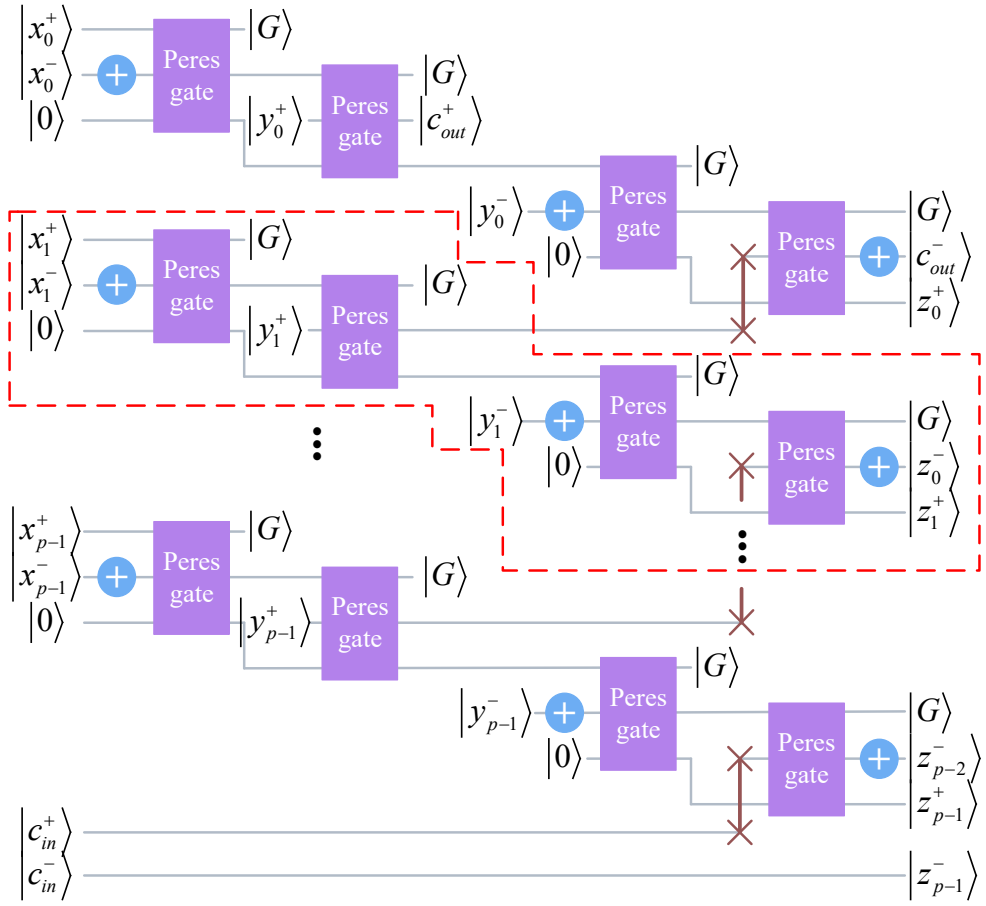


Based on 7-qubit BQFAs

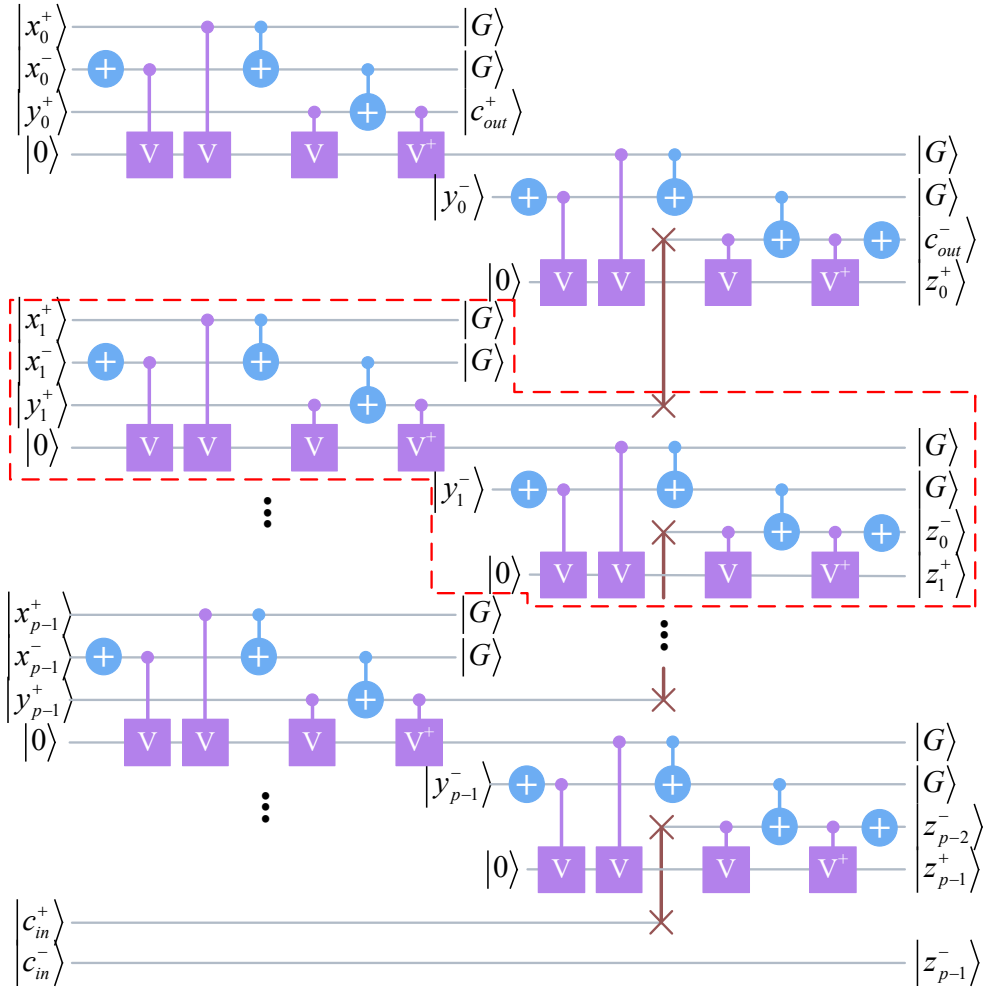


Based on 5-qubit BQFAs

Quantum MSDF Adders – #Qubits Reduction

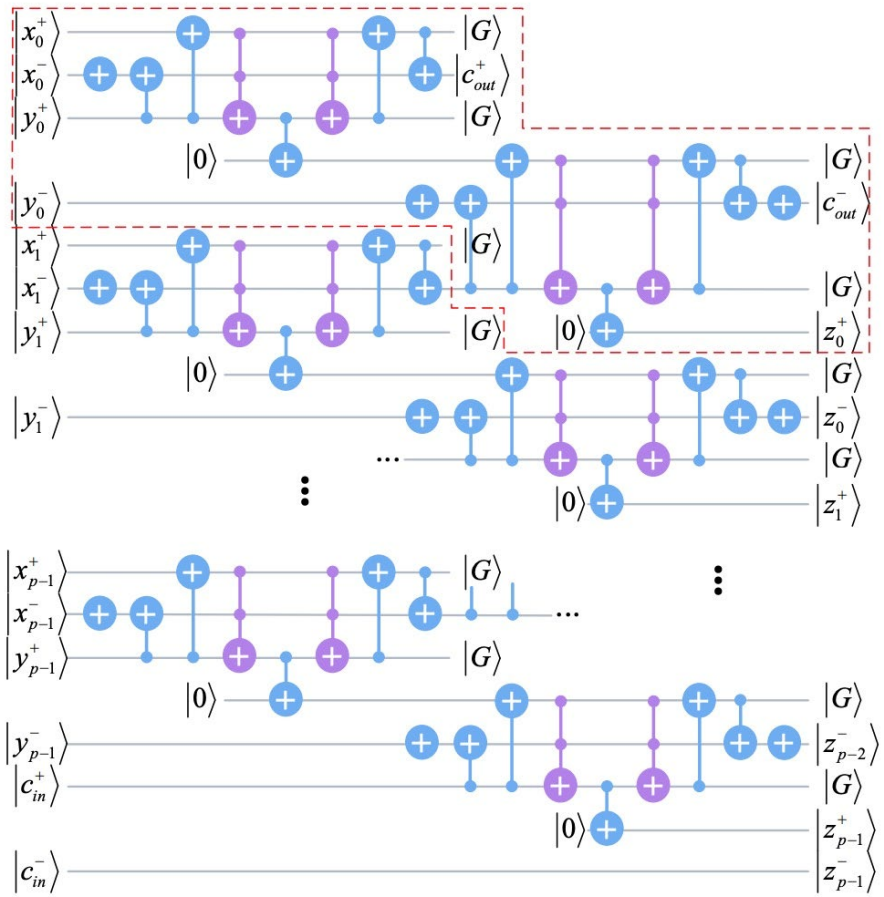


Based on 4-qubit BQFAs with Peres gate

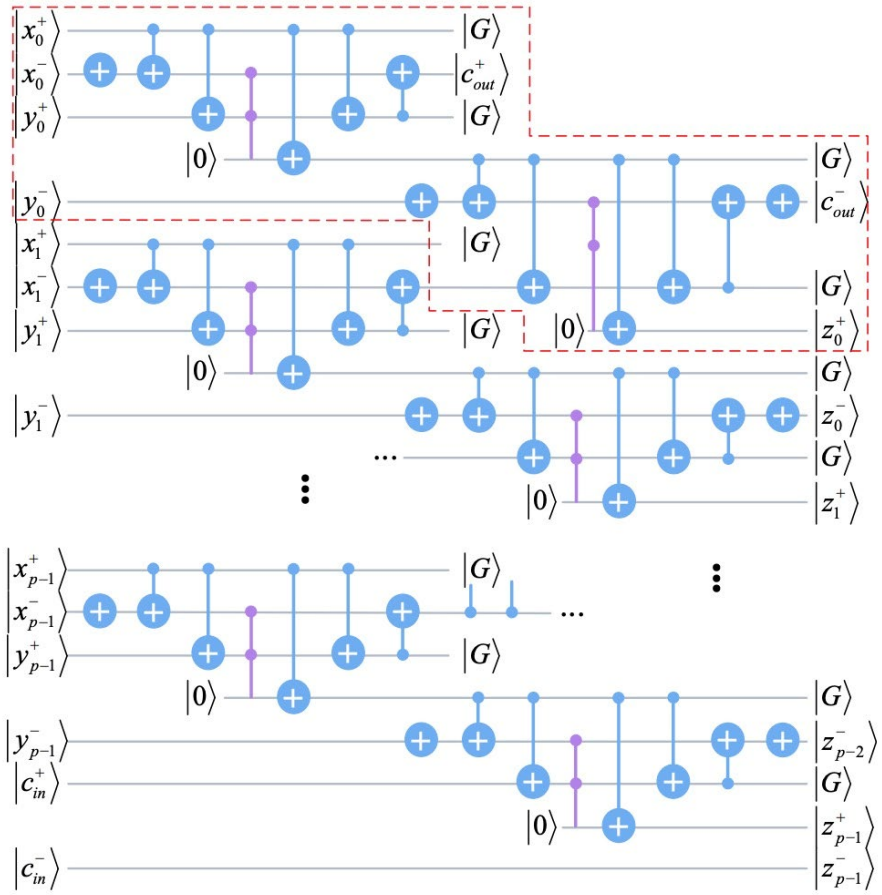


Based on 4-qubit BQFAs with V gate

Quantum MSDF Adders – Qubit-state Reuse



With qubit state reuse



With less non-Clifford gates

Specifically Speaking…

Qubit-efficient QMDA

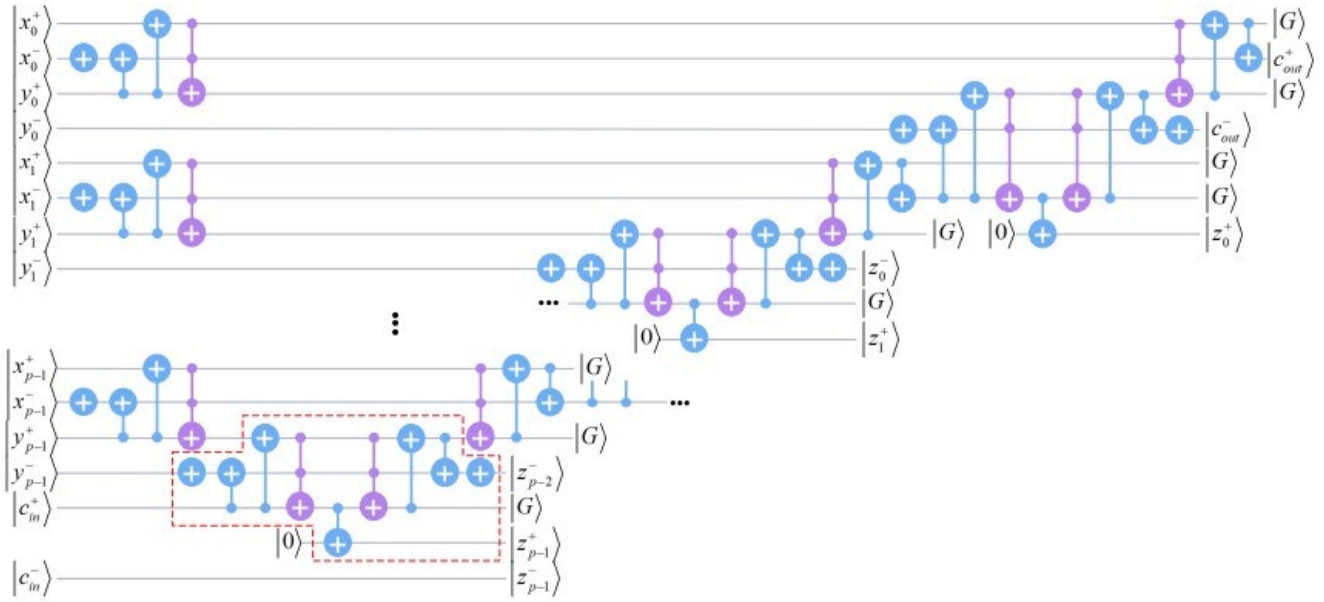


Fig. 6. Qubit-efficient QMDA with carry-first QFAs. The quantum circuit in the red box is a carry-first QFA sharing the qubit y_{p-1}^{+} with other parts of this QMDA.

Qubit-efficient & low T-count QMDA & Sum-first

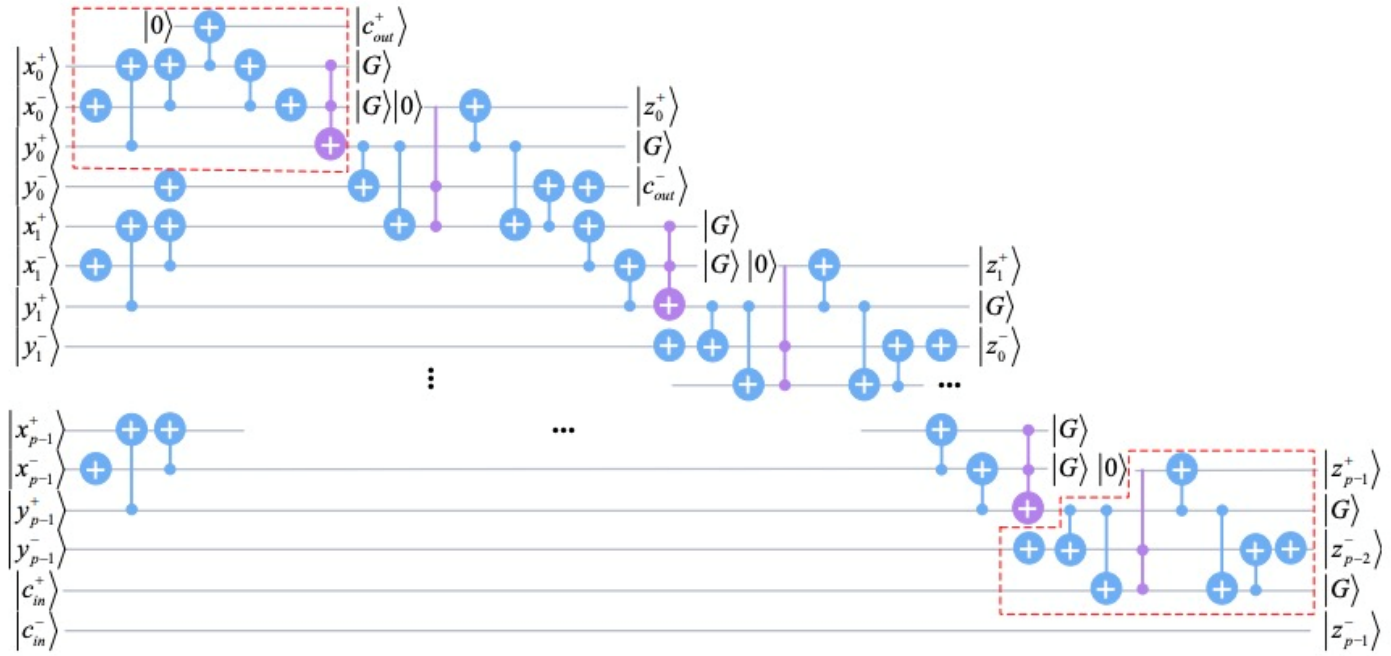


Fig. 7. QMDA with qubit-efficient and low T-count optimisations by using sum-first QFAs (top-left box) and temporary logical-AND (bottom right box) [13].

Qubit-efficient & low T-count QMDA & Sum-first & Carry-first

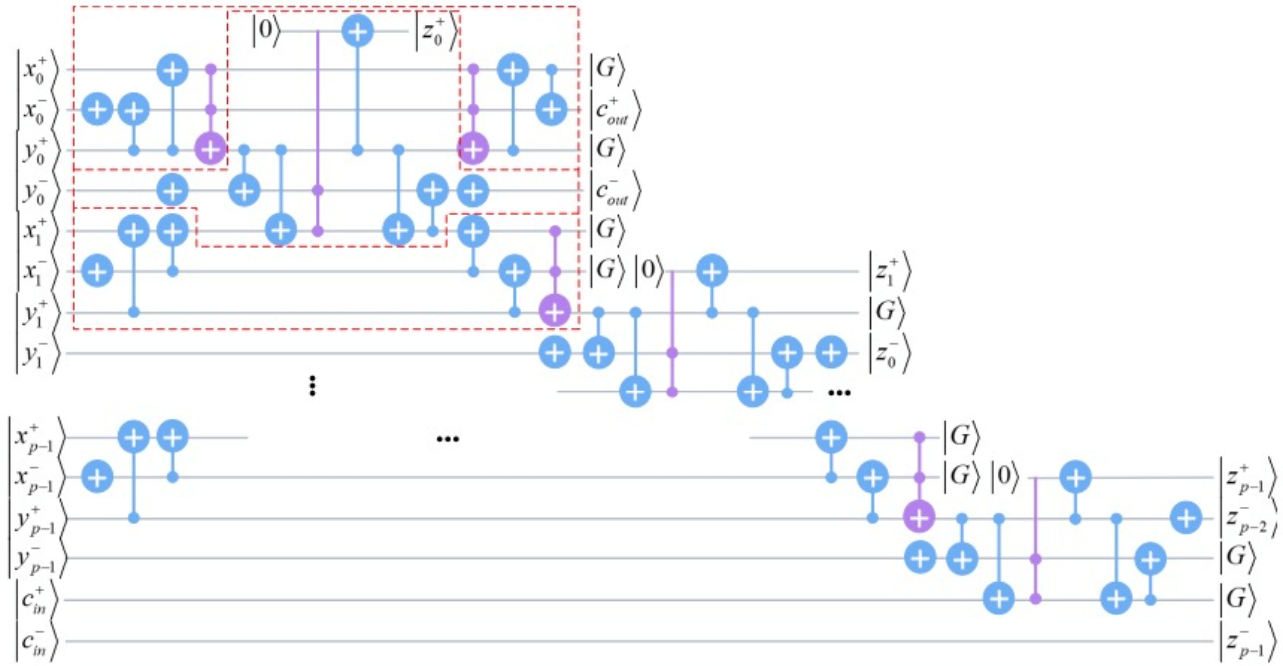


Fig. 8. QMDA with qubit-efficient and low T-count optimisations by using temporary logical-AND [13], carry- and sum-first QFAs. The quantum circuit in the box shows a carry-first QFA (top), temporary logical-AND [13] (middle) and sum-first QFA (botton), respectively.

Low-depth & low T-count QMDA

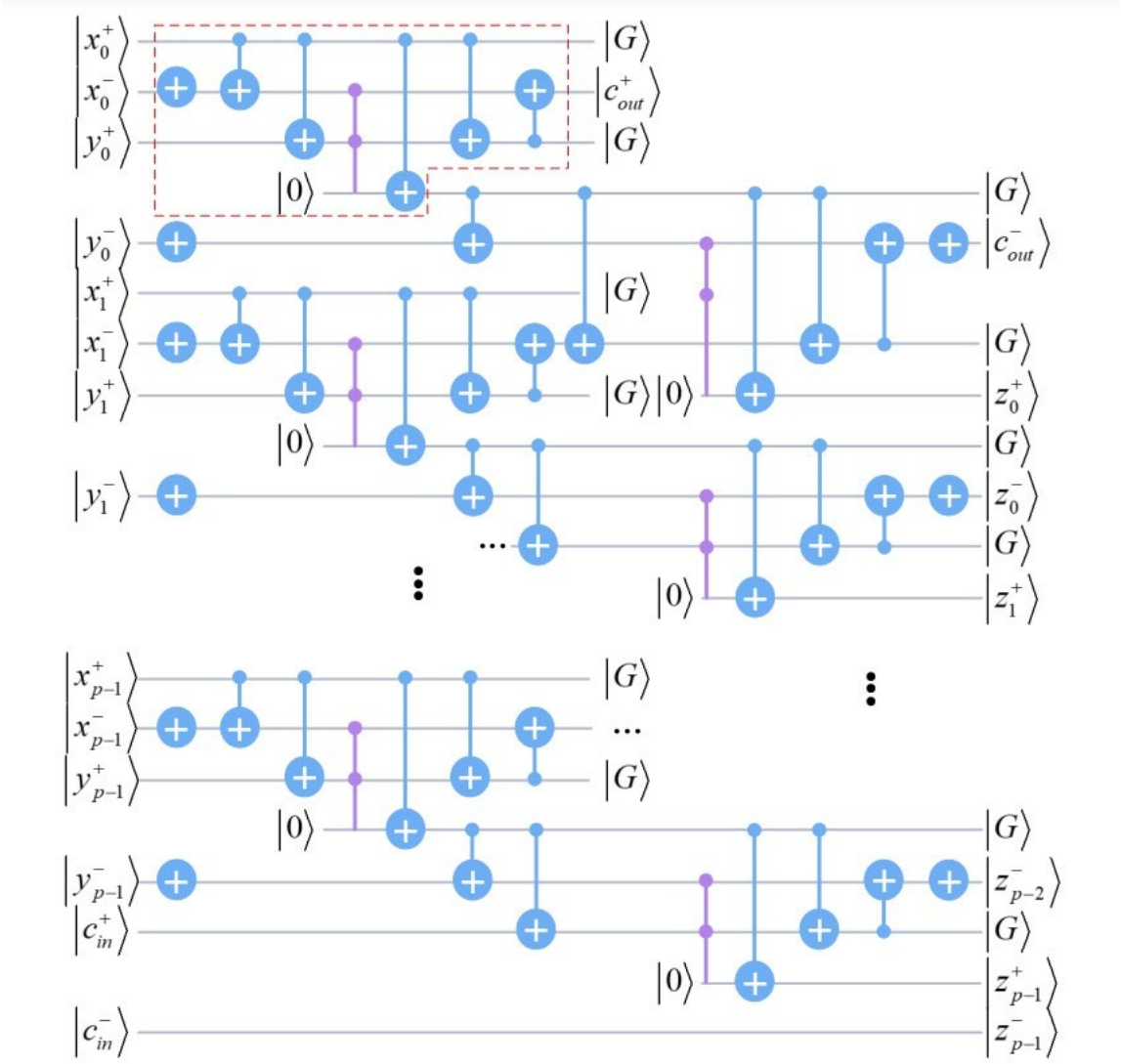


Fig. 9. QMDA with low-depth and low T-count optimisations by using temporary logical-AND based QFAs (red box).

Evaluation: Adder Trees

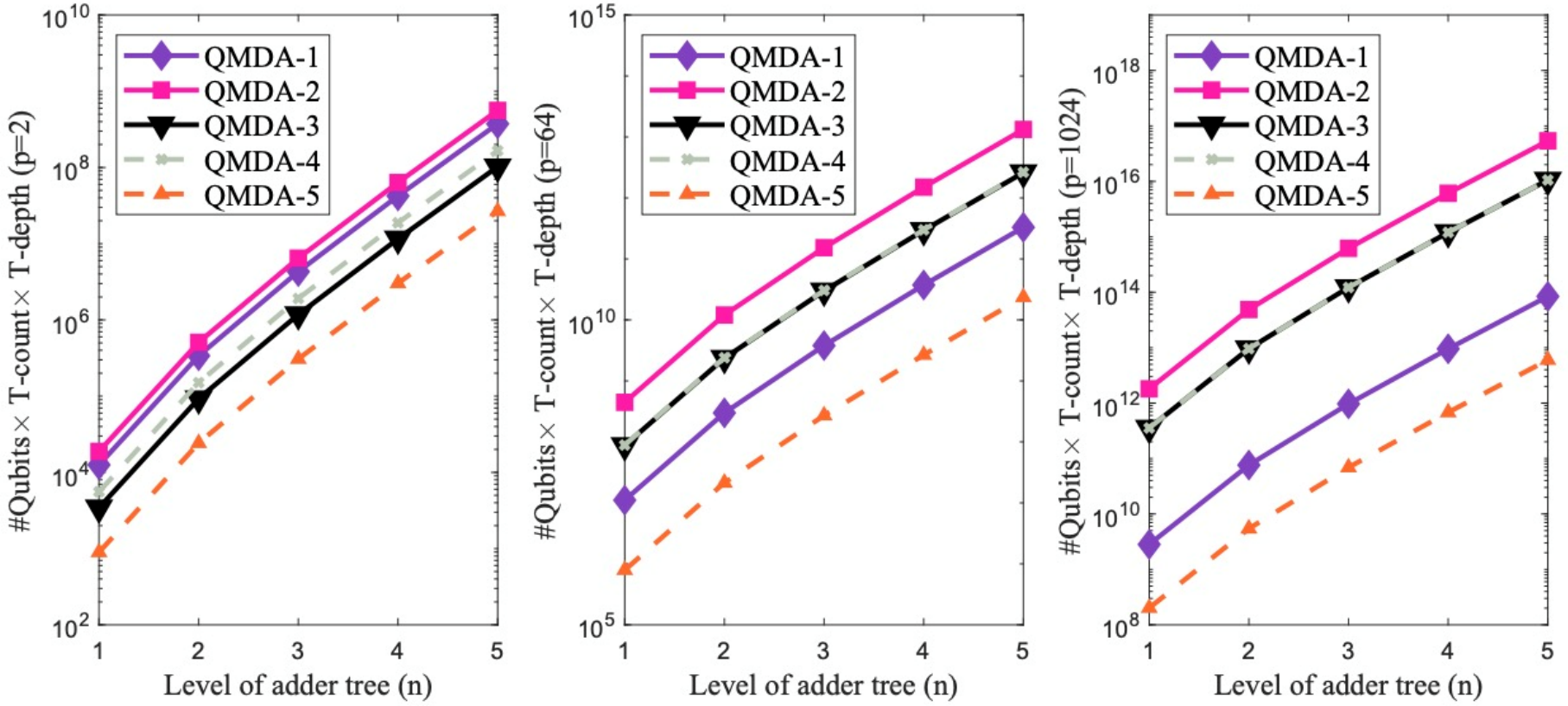
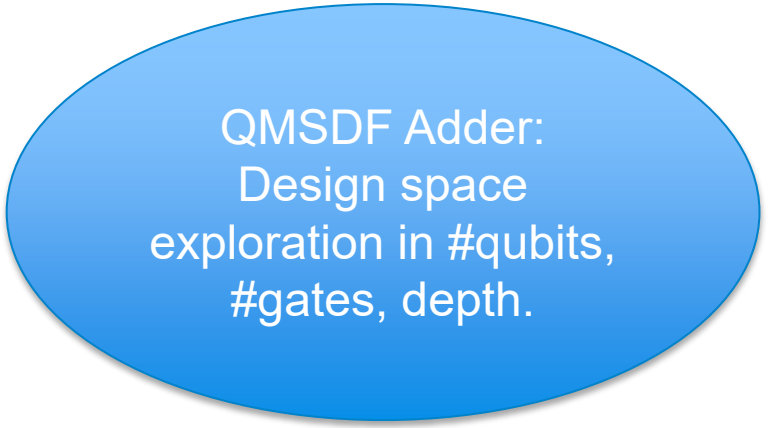


Fig. 14. Analysis of the product of qubits usage, T-count and T-depth in different adder tree levels n, when p is 2, 64 and 1024, respectively.

Comparisons with STOAs



T-depth:
Quantum carry-lookahead adders O(log *p*)
Quantum ripple-carry adders O(*p*)

T-depth:
QMDA is independent of the word length *p*

Conclusion

1. We propose the first design-space exploration method for quantum MSDF adder circuits in terms #qubits, #gates and circuit depth.
2. A library of quantum circuit implementations for quantum LSDF and MSDF addition.
3. 4.0x T-depth decreases, 3.5x T-count decline, and 1.2x qubit usage reduction.

Thank you very much.

helix@seu.edu.cn / heli@ieee.org