SHANDONG UNIVERSITY

Improved Quantum Circuits for AES: Reducing the Depth and the Number of Qubits

Qun Liu[1,3] Bart Preneel[4] Zheng Zhao[1,3]
Meiqin Wang(✉)[1,2,3]

[1]School of Cyber Science and Technology, Shandong University, Qingdao, China

[2]Quan Cheng Laboratory, Jinan, China

[3]Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China

[4]imec-COSIC, KU Leuven, Belgium

December 5, 2023

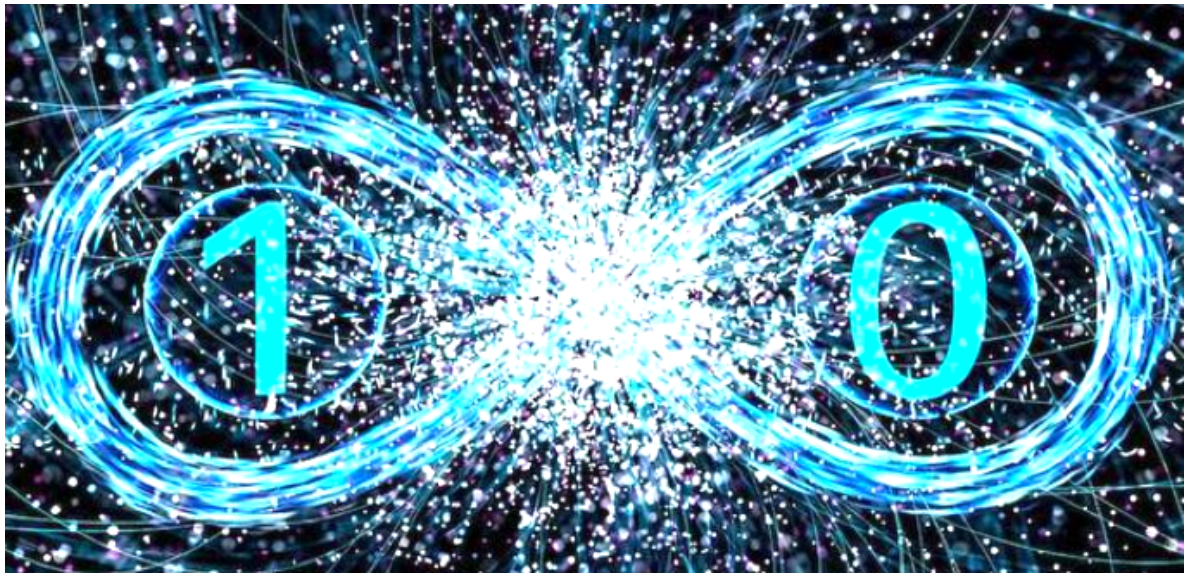
Outline

Outline

Motivation

Overview

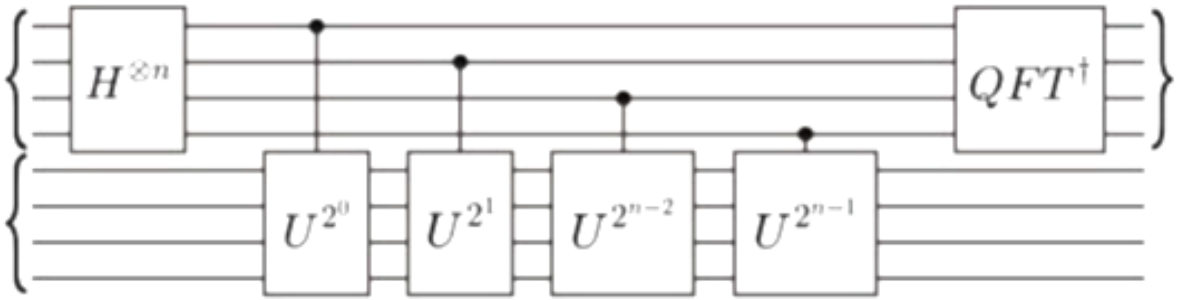
- Quantum computing presents both challenges and opportunities for the field of cryptography.
- It has become crucial to investigate the security of cryptographic primitives against quantum attacks.



Motivation

Shor's Algorithm

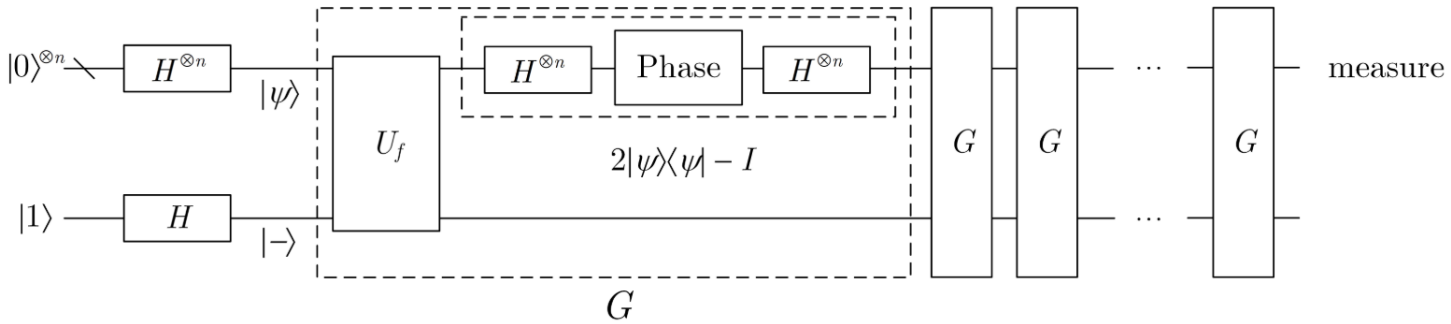
- Shor's algorithm threatens widely-used cryptographic protocols, such as RSA and ECC, by efficiently factoring large numbers.



Motivation

Grover's Algorithm

- Grover's algorithm is the main threat for the **symmetric ciphers**.
- It accelerates the search of an **unsorted database**, impacting **hash functions** and **symmetric ciphers**.



Motivation

Symmetric Ciphers

- **Grover's algorithm**.
- **Simon's algorithm**. Its primary application is in solving a specific type of problem, **finding a hidden relation between two sets of binary strings**.
- **CNS algorithm** (Chailloux et al., ASIACRYPT 2017).
  - It is an efficient quantum collision search algorithm **without large qRAM**.
  - It seeks to achieve an efficient quantum search while minimizing the amount of quantum memory needed for the computation.
- Others.

Motivation

Symmetric Ciphers

- **Grover's algorithm**.
- **Simon's algorithm**. Its primary application is in solving a specific type of problem, **finding a hidden relation between two sets of binary strings**.
- **CNS algorithm** (Chailloux et al., ASIACRYPT 2017).
  - It is an efficient quantum collision search algorithm **without large qRAM**.
  - It seeks to achieve an efficient quantum search while minimizing the amount of quantum memory needed for the computation.
- Others.

Motivation

NIST's Call for PQC

- In 2016, NIST initiated an effort known as the **Post-Quantum Cryptography Standardization Project**.
- The primary goal was to standardize cryptographic algorithms that could **resist attacks from both classical and quantum computers**.

Motivation

NIST's Call for PQC

- It involved the strategic use of **AES circuit resource estimation**.
- Specifically, **security categories 1, 3, and 5** correspond to key recovery attacks against AES-128, -192, and -256, respectively.

Category	Cipher	Bound of gate counts
Level-1	AES-128	$2^{170}/\texttt{MAXDEPTH}$
Level-3	AES-192	$2^{233}/\texttt{MAXDEPTH}$
Level-5	AES-256	$2^{298}/\texttt{MAXDEPTH}$

- In addition to the gate count, another important parameter known as **MAXDEPTH** has been introduced. NIST limits quantum attacks to a fixed running time or **circuit depth**.

Motivation

NIST's Call for PQC

- It involved the strategic use of **AES circuit resource estimation**.
- Specifically, **security categories 1, 3, and 5** correspond to key recovery attacks against AES-128, -192, and -256, respectively.

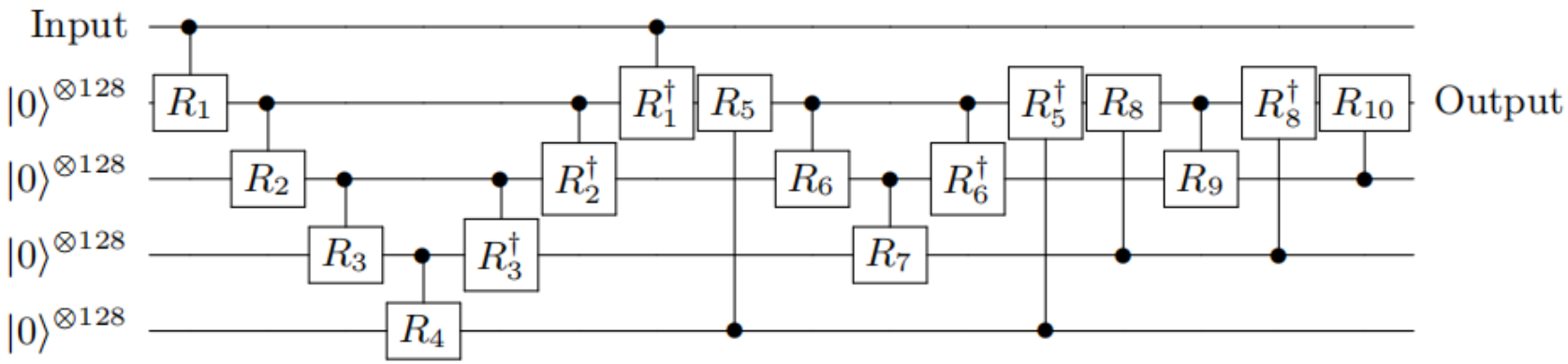
Category	Cipher	Bound of gate counts
Level-1	AES-128	$2^{170}/\texttt{MAXDEPTH}$
Level-3	AES-192	$2^{233}/\texttt{MAXDEPTH}$
Level-5	AES-256	$2^{298}/\texttt{MAXDEPTH}$

- In addition to the gate count, another important parameter known as **MAXDEPTH** has been introduced. NIST limits quantum attacks to a fixed running time or **circuit depth**.

Related Work

Grassl et al. - PQCrypto 2016:

- The **foundational work** initiated by Grassl et al. introduced a novel **zig-zag architecture**.
- It aimed to **minimize the qubit count** required for implementing AES circuits.



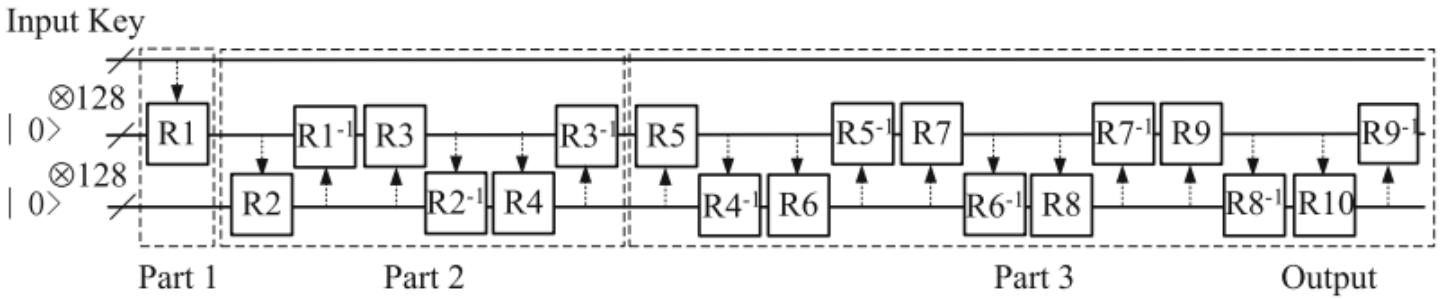
Related Work

Langenberg et al. - 2019:

- Langenberg et al. in 2019 presented a new circuit for the AES S-box and key expansion, reducing the qubit count.

Zou et al. - ASIACRYPT 2020:

- Zou et al. in their paper at ASIACRYPT 2020, further **refined the zig-zag architecture**.
- Introducing novel AES S-box circuits.
- Reflecting a continuous pursuit of optimizing quantum circuits for improved performance and resource utilization.



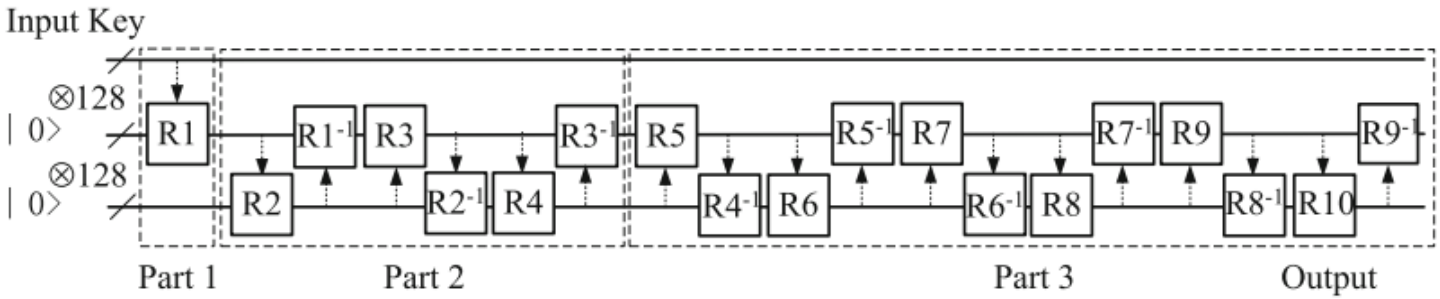
Related Work

Langenberg et al. - 2019:

- Langenberg et al. in 2019 presented a new circuit for the AES S-box and key expansion, reducing the qubit count.

Zou et al. - ASIACRYPT 2020:

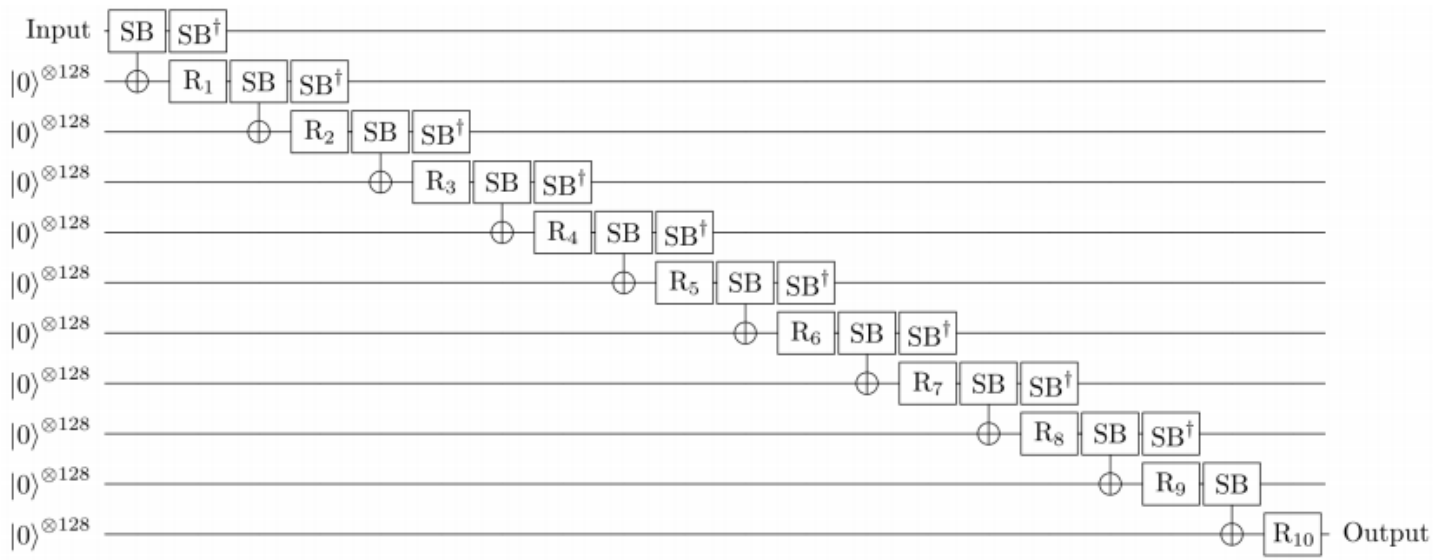
- Zou et al. in their paper at ASIACRYPT 2020, further **refined the zig-zag architecture**.
- Introducing novel AES S-box circuits.
- Reflecting a continuous pursuit of optimizing quantum circuits for improved performance and resource utilization.



Related Work

Jaques et al. - EUROCRYPT 2020:

- Jaques et al. proposed several innovative methods to reduce both **quantum depth and qubit count**.
- Original **pipeline architecture**.



(from Jang et al.)

Related Work

Huang et al. - ASIACRYPT 2022:

- Huang et al., presented at ASIACRYPT 2022, introduced S-boxes characterized by low T-depth.
- This strategic approach effectively led to reductions in T-depth
- Further advancing the state-of-the-art in quantum circuit optimization for AES.

Ongoing Contributions - Li, Lin, Jang, et al.:

- These efforts show the dynamic nature of the field.
- They explore various avenues to improve the performance and security of AES in quantum computing.

Related Work

Huang et al. - ASIACRYPT 2022:

- Huang et al., presented at ASIACRYPT 2022, introduced S-boxes characterized by low T-depth.
- This strategic approach effectively led to reductions in T-depth
- Further advancing the state-of-the-art in quantum circuit optimization for AES.

Ongoing Contributions - Li, Lin, Jang, et al.:

- These efforts show the dynamic nature of the field.
- They explore various avenues to improve the performance and security of AES in quantum computing.

Outline

Quantum Circuit

- Construction of quantum circuits involves a universal fault-tolerant gate set: Hadamard (H), Phase Shift (S), CNOT, and T gate.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad \text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Quantum Circuit

Optimization Goals

1. **Width**. The **space complexity** corresponds to the number of logical qubits needed for the entire quantum computation.
2. T-**depth**. The **time complexity** refers to the time required to execute non-parallelizable logical T gates.
3. **DW-cost**. The **circuit complexity** is determined by the product of the time and space complexity.
4. **Full depth**. A **forward-looking perspective** suggests that each gate has a depth equal to one, with the T gate incurring a cost similar to other gates.
5. **Gate count**. All the gates used in the circuit.

Quantum Circuit

Optimization Goals

1. **Width**. The **space complexity** corresponds to the number of logical qubits needed for the entire quantum computation.
2. T-**depth**. The **time complexity** refers to the time required to execute non-parallelizable logical T gates.
3. **DW-cost**. The **circuit complexity** is determined by the product of the time and space complexity.
4. **Full depth**. A **forward-looking perspective** suggests that each gate has a depth equal to one, with the T gate incurring a cost similar to other gates.
5. **Gate count**. All the gates used in the circuit.

The AND Operation

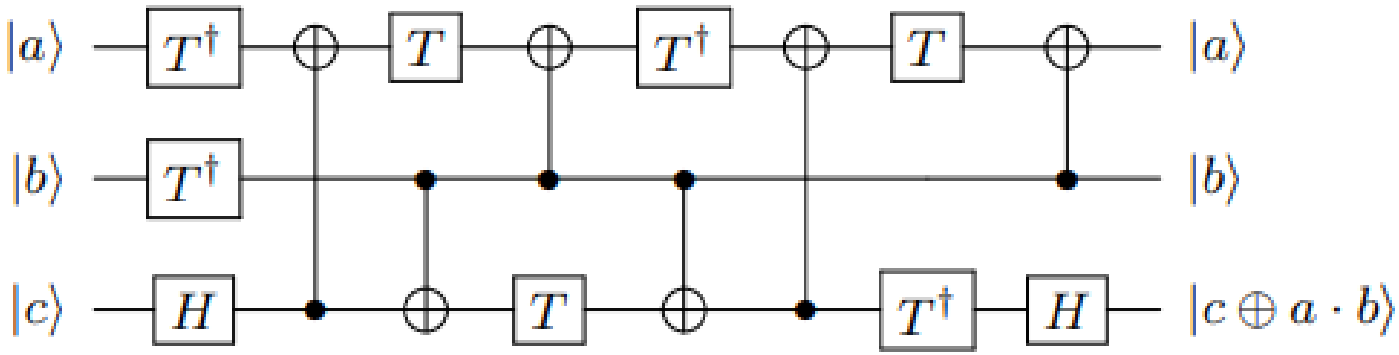
- The Clifford gates are **much cheaper** than the T gate.
- In our quantum circuit, the AND operation $a \cdot b$ is the only source of T-depth.
- Currently, there exist **multiple approaches** for implementing the AND operations:
  - the **Toffoli gate** with T-depth 1, or 4, achieving $|a\rangle |b\rangle |c\rangle \rightarrow |a\rangle |b\rangle |c \oplus a \cdot b\rangle$.
  - the **quantum** AND **gate** using one ancilla qubit with T-depth 1, achieving $|a\rangle |b\rangle |0\rangle \rightarrow |a\rangle |b\rangle |a \cdot b\rangle$.

The AND Operation

- The Clifford gates are **much cheaper** than the T gate.
- In our quantum circuit, the AND operation $a \cdot b$ is the only source of T-depth.
- Currently, there exist **multiple approaches** for implementing the AND operations:
  - the **Toffoli gate** with T-depth 1, or 4, achieving $|a\rangle |b\rangle |c\rangle \rightarrow |a\rangle |b\rangle |c \oplus a \cdot b\rangle$.
  - the **quantum** AND **gate** using one ancilla qubit with T-depth 1, achieving $|a\rangle |b\rangle |0\rangle \rightarrow |a\rangle |b\rangle |a \cdot b\rangle$.

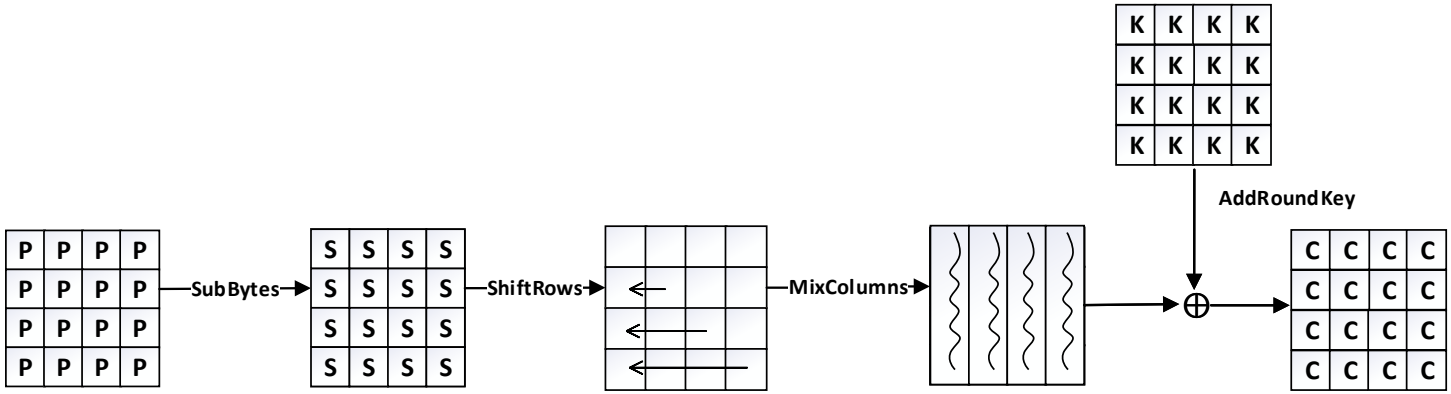
Quantum Circuit

- Treat them as a unified operation
- Use $|a\rangle |b\rangle |0\rangle \rightarrow |a\rangle |b\rangle |a \cdot b\rangle$
- Set $c = 0$



Outline

Description of AES Family



- AddRoundKey.
- ShiftRows.
- SubBytes.
- MixColumns.

$$M = \begin{pmatrix} 0x02 & 0x03 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x03 & 0x01 \\ 0x01 & 0x01 & 0x02 & 0x03 \\ 0x03 & 0x01 & 0x01 & 0x02 \end{pmatrix}.$$

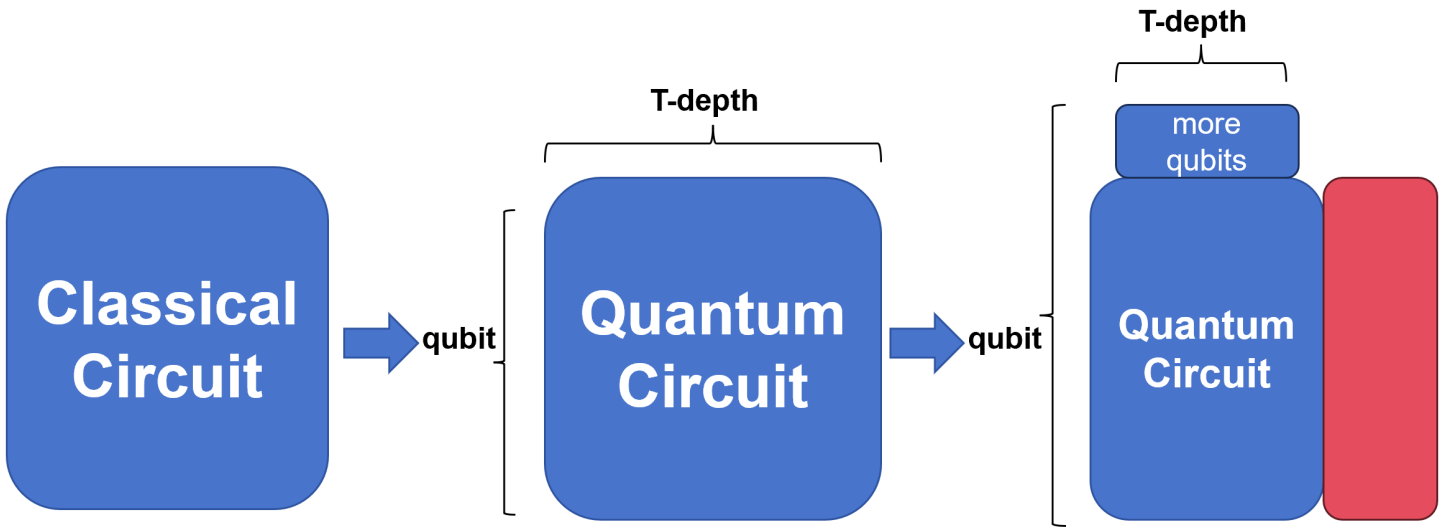
Optimization

- S-box: width, depth, T-depth, gate count.
- MixColumns: width, depth, gate count.

Optimization of S-box

From Classical Circuit to Quantum Circuit

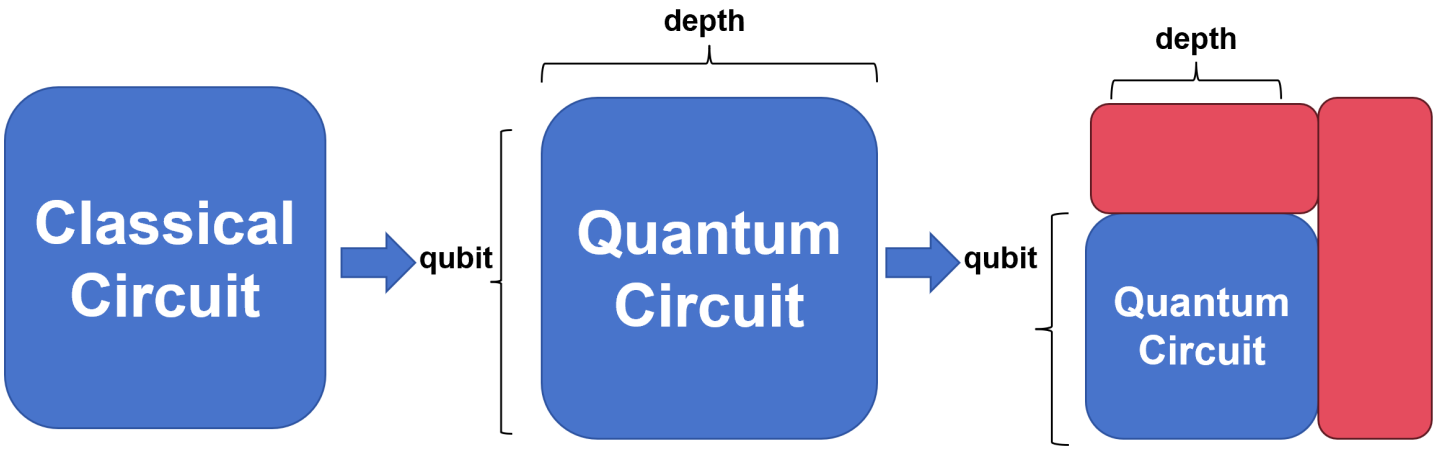
- The S-box circuit constructed by Jaques et al. for AES requires 120 ancilla qubits with T-depth 6. (EUROCRYPT 2020)
- Subsequently, Huang et al. reduced the T-depth to 4 while keeping the number of qubits at 120 or T-depth 3 with more qubits. (ASIACRYPT 2022)



Optimization of S-box

m-XOR Technique

- Construct a new quantum circuit from the classical circuit.
- **qubit, gates, full depth**.



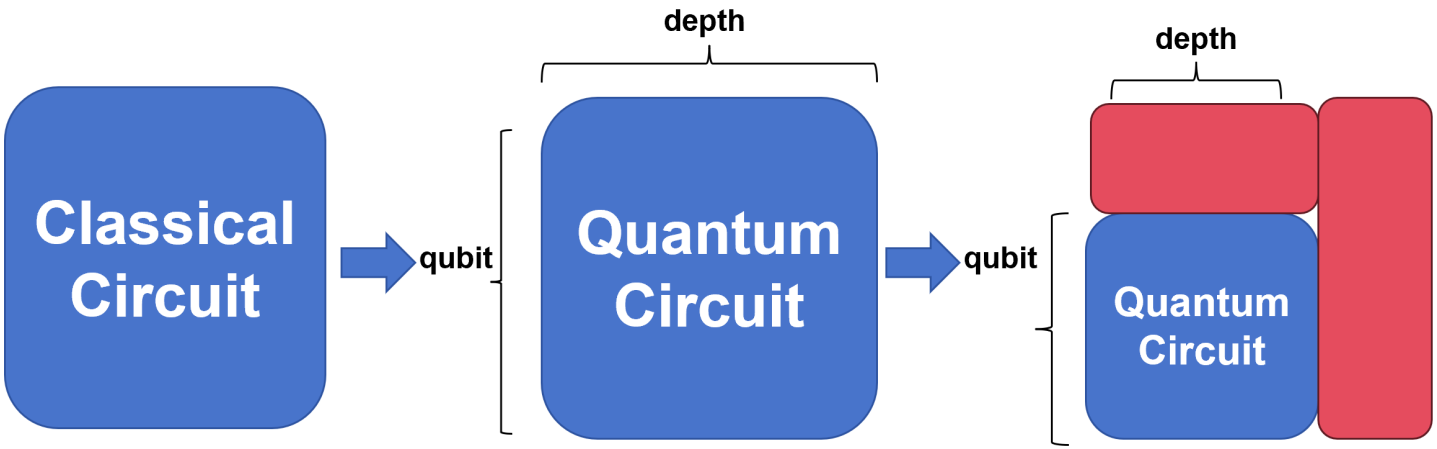
Further application

- If the S-box circuit used for improvements is updated, our approach can still be employed to reduce these three metrics.

Optimization of S-box

m-XOR Technique

- Construct a new quantum circuit from the classical circuit.
- qubit, gates, full depth.



Further application

- If the S-box circuit used for improvements is updated, our approach can still be employed to reduce these three metrics.

Optimization of S-box

Classical Operation

- s-XOR: $a = a \oplus b$.
- g-XOR: $c = a \oplus b$.

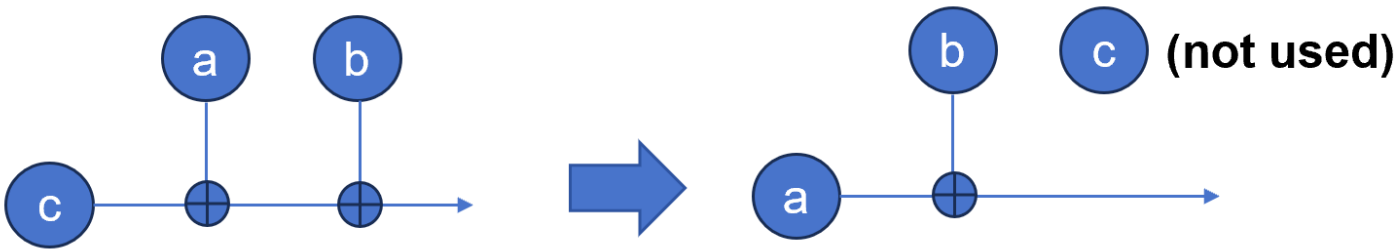
Quantum Operation

- The *updating* operation is $\mathit{in\text{-}place}$ and can be implemented by a CNOT gate $|a\rangle|b\rangle \rightarrow |a\rangle|a \oplus b\rangle$, defined as $\mathrm{CNOT}(a, b)$.
- The *creating* operation is $\mathit{out\text{-}of\text{-}place}$, requiring two CNOT gates $|a\rangle|b\rangle|c\rangle \rightarrow |a\rangle|b\rangle|c \oplus a\rangle$ and $|a\rangle|b\rangle|c \oplus a\rangle \rightarrow |a\rangle|b\rangle|c \oplus a \oplus b\rangle$, defined as $\mathrm{CNOT2}(a, b, c)$.

Optimization of S-box

Observation

Given a quantum circuit with **creating operations**, some qubits can be reused by transforming creating operations into **updating operations**.



Optimization of S-box

Proposition

In a **sequentially written quantum circuit**, the conversion from a creating operation $t_c = t_c \oplus (t_a \oplus t_b)$ to an updating operation $t_a = t_a \oplus t_b$ requires the fulfillment of the following conditions:

- t_a should not be utilized in the subsequent circuit.
- t_c does not appear in the previous circuit.

- To successfully perform the conversion, **both conditions must be satisfied**.
- Failing to meet either condition can compromise the **correctness of the circuit**.

Comparisons of Resource Estimations of the AES S-box

There are various implementations of S-box quantum circuits. Some circuits use Toffoli gates, while others use AND gates. We show the comparison of different Toffoli-based circuits.

Source	Width	#Toffoli	#CNOT	#1qCliff	Toffoli depth
[23]	16+16	55	314	4	40
[34]	6+16	52	326	4	41
[34]	7+16	48	330	4	39
[34]	8+16	46	332	4	37
[26]	5+16	57	193	4	24
[26]	6+16	57	195	4	22
[19]	120+16	34	186	4	6
[16]	120+16	34	214	4	4
This paper	**74**+16	34	**168**	4	4

- Ancilla qubit count: $120 \rightarrow 74$
- CNOT gate count: $214 \rightarrow 168$

Comparisons of Resource Estimations of the AES S-box

Next, we compare the S-box circuits utilizing AND gates. We estimated both the S-box and S-box† using Q#.

Source	Width	#CNOT	#1qCliff	$\#T$	#M	$\#TD$	$\#FD$
[19]	136	664	205	136	34	6	117
[16]	136	718	208	136	34	4	109
This paper	**99**	**624**	**204**	136	34	4	**101**

- Qubit count: $136 \rightarrow 99$
- CNOT gate count: $718 \rightarrow 624$
- Depth: $109 \rightarrow 101$

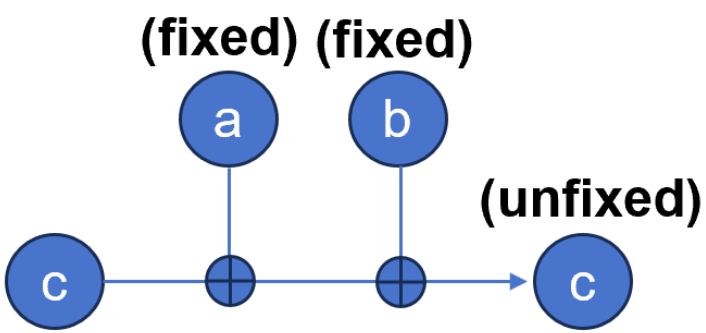
Optimization of MixColumns

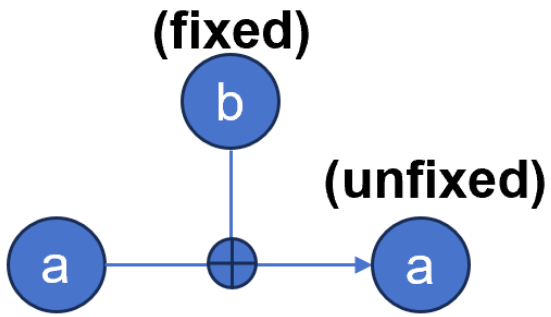
Property

We use $|t\rangle = g(|a_0\rangle, |a_1\rangle)$ to represent a quantum gate. Every qubit has two states:

- **Unfixed**. The value of unfixed $|t\rangle$ is **updated** by the gate.
- **Fixed**. The values of fixed $|a_0\rangle$ and $|a_1\rangle$ are **not changed**.

Each unfixed qubit $|t\rangle$ must be put at depth d, where $|t\rangle$ is not used at depth d' $(d' \geq d)$.
Each fixed qubit $|a_i\rangle$, $i = 0$ or 1, it must be put at depth d, where $|a_i\rangle$ is not updated at depth d' $(d' \geq d)$.





Comparisons of MixColumns

The implementation of MixColumns has been widely studied.
Usually, we can use optimized classical circuits to reduce the cost.
However, the depth in classical circuits and quantum circuits is different.

Source	#CNOT	Width	$\#FD$
[3,28]	206	135	13
[24]	210	137	**11**
[19]	277	32	111
[13,34]	277	32	39
[33]	92	32	30
This Paper	98	32	**16**

- In-place circuit, depth 30 $\rightarrow$ 16.
- For the out-of-place circuit, we show the forward depth.
- Because we can execute *uncomputation* operation in next round.

Comparisons of MixColumns

The implementation of MixColumns has been widely studied.
Usually, we can use optimized classical circuits to reduce the cost.
However, the depth in classical circuits and quantum circuits is different.

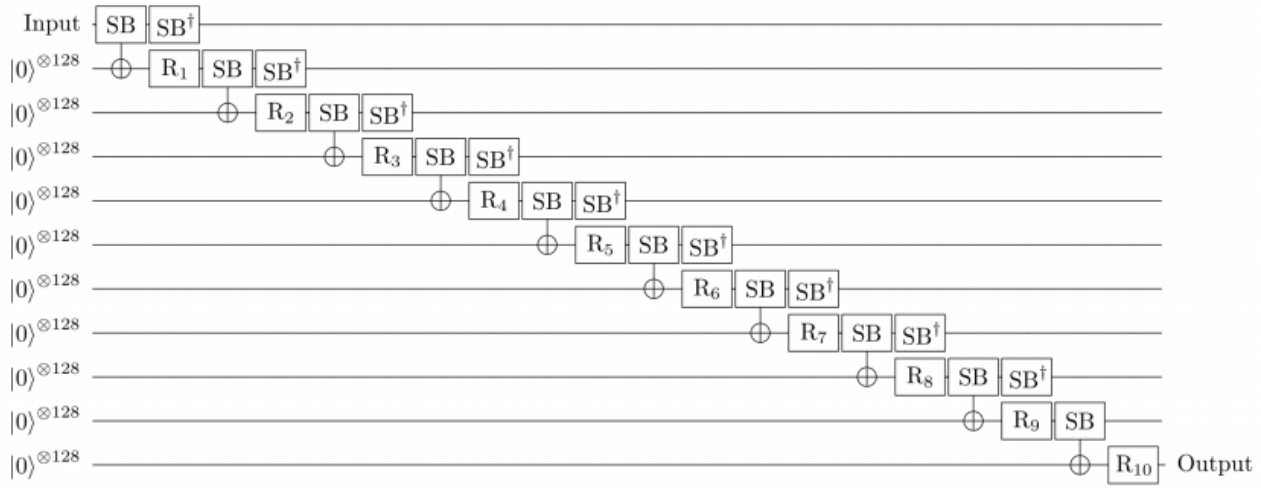
Source	#CNOT	Width	$\#FD$
[3,28]	206	135	13
[24]	210	137	**11**
[19]	277	32	111
[13,34]	277	32	39
[33]	92	32	30
This Paper	98	32	**16**

- In-place circuit, depth $30 \rightarrow 16$.
- For the out-of-place circuit, we show the forward depth.
- Because we can execute *uncomputation* operation in next round.

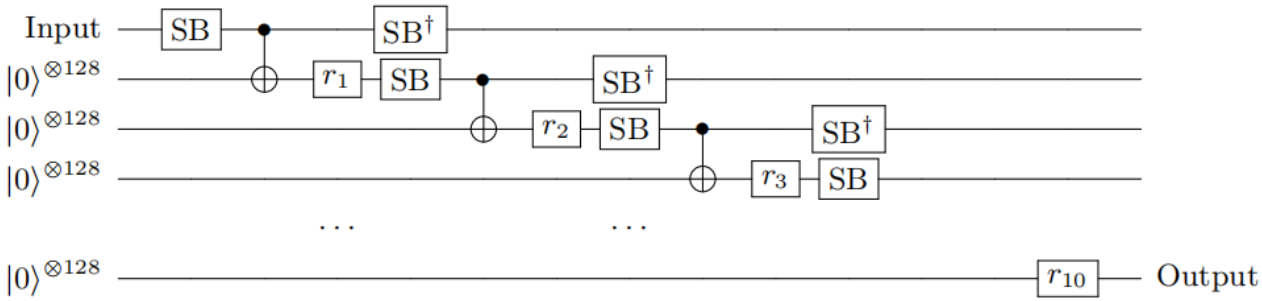
Outline

Pipeline Architecture for AES

In Jang et al.'s work:

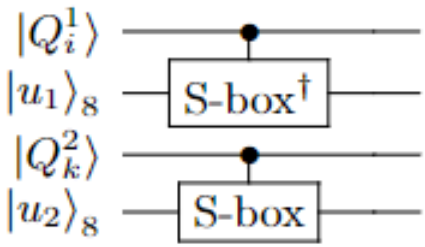


more depth



more qubits

Improved Pipeline Architecture for AES



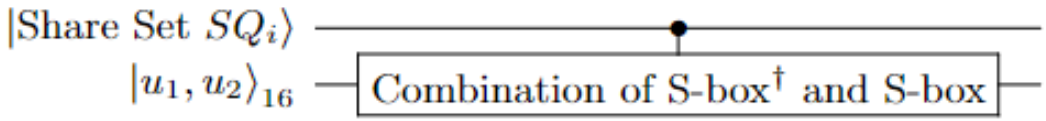
Example

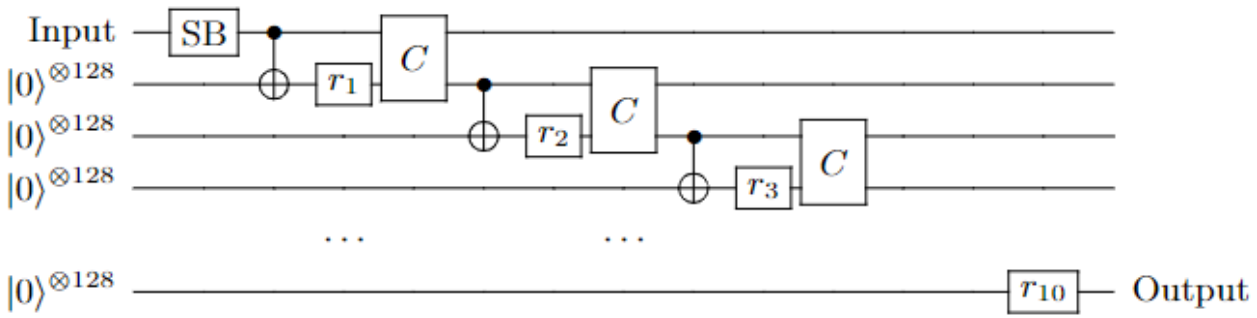
- In R_1, SB uses 16 Q_i^1 $(0 \leq i \leq 15)$.
- In R_2, SB uses 16 Q_k^2 $(0 \leq k \leq 15)$ and SB† cleans up the qubits in 16 Q_i^1 $(0 \leq i \leq 15)$.
- Then, in round R_3, SB uses the 16 Q_i^1 $(0 \leq i \leq 15)$ sets, and SB† clears the qubits in the 16 Q_k^2 $(0 \leq k \leq 15)$ sets.
- These two sets of ancilla qubits are alternated in the remaining rounds.
- The total count of ancilla qubits is $2 \times 16 \times 120 = 3840$.

Improved Pipeline Architecture for AES

Observation

- In the independent structure of S-box and S-box†, during the execution of S-box†, the qubits are consistently cleaned up, and these qubits are not utilized in the S-box operation.
- Conversely, S-box employs a fresh qubit set to select the available qubits.





Discussion on Different Pipeline Architectures

Simple Structure

- An r-**round cipher** ($r \geq 1$) consists of only **two components**.
- **SB and MixColumns**: depth d_s and d_m.
- SB and MixColumns requires q_s and q_m ancilla qubits.
- Each round requires q_r ($q_r \geq 1$) qubits.

Architecture	Width	$\#FD$
Original architecture[19]	$(r+1) \cdot q_r + q_s + q_m$	$d_s + \max(d_s, d_m)$
Shallowed architecture[18]	$(r+1) \cdot q_r + \max(2q_s, q_m)$	$d_s + d_m$
Combined architecture	$(r+1) \cdot q_r + \max((1+\epsilon) \cdot q_s, q_m)$	$d_s + d_m$

Observation

- If $d_s > d_m$, the shallowed and combined pipeline architectures have the lowest circuit depth.
- If $q_m > \epsilon \cdot q_s$, the combined pipeline architecture has the lowest width.

Share Technique: Reducing Qubit Count

Definition

- $q^{old}_{private}$ is the set of qubits that will be cleaned up by S-box†.
- q^{old}_{public} is the set of unallocated qubits for S-box†.
- $q^{new}_{private}$ is the set of qubits used by S-box.
- q^{new}_{public} is the set of qubits that are not used by S-box.

Property

- $SQ_i = q^{old}_{private} \cup q^{old}_{public} = q^{new}_{private} \cup q^{new}_{public}$

Proposition

After completing the combination of S-box and S-box†, the sizes of the five qubit sets remain constant.

Share Technique: Reducing Qubit Count

Definition

- $q^{old}_{private}$ is the set of qubits that will be cleaned up by S-box†.
- q^{old}_{public} is the set of unallocated qubits for S-box†.
- $q^{new}_{private}$ is the set of qubits used by S-box.
- q^{new}_{public} is the set of qubits that are not used by S-box.

Property

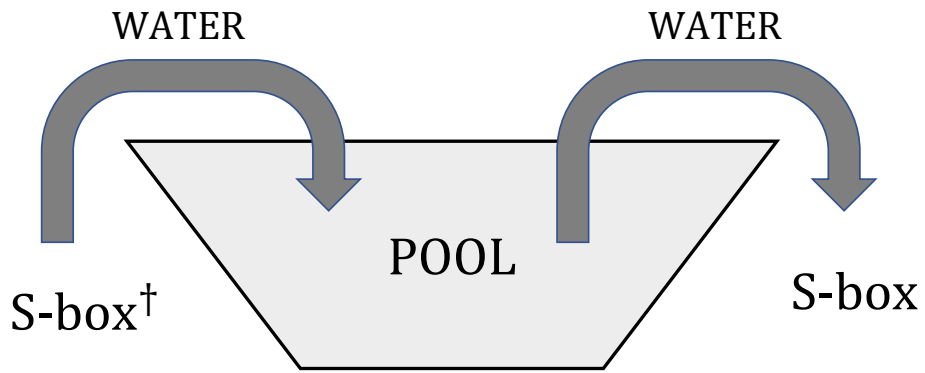
- $SQ_i = q^{old}_{private} \cup q^{old}_{public} = q^{new}_{private} \cup q^{new}_{public}$

Proposition

After completing the combination of S-box and S-box†, the sizes of the five qubit sets remain constant.

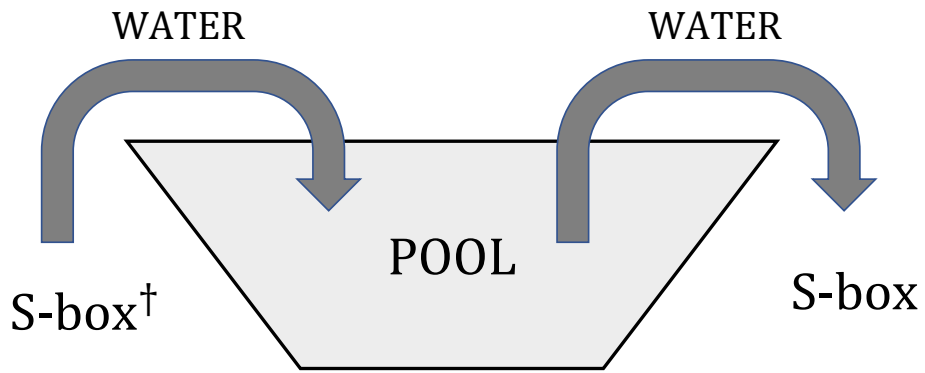
Share Technique

- During the combination process, we set $|SQ_i| = a$ and $|q^{old}_{private}| = u$.
- $|q^{old}_{public}|$ is $z = a - u$.
- S-box† cleans up all the qubits in $q^{old}_{private}$ and adds them to q^{old}_{public}. This results in a total of $u + z = a$ qubits in q^{old}_{public}.
- $|q^{old}_{public}|$ remains $a - u = z$.
- In conclusion, as long as q^{old}_{public} contains a sufficient number of qubits, the sizes of the qubit sets remain unchanged.



Share Technique

- During the combination process, we set $|SQ_i| = a$ and $|q^{old}_{private}| = u$.
- $|q^{old}_{public}|$ is $z = a - u$.
- S-box† cleans up all the qubits in $q^{old}_{private}$ and adds them to q^{old}_{public}. This results in a total of $u + z = a$ qubits in q^{old}_{public}.
- $|q^{old}_{public}|$ remains $a - u = z$.
- In conclusion, as long as q^{old}_{public} contains a sufficient number of qubits, the sizes of the qubit sets remain unchanged.



Share Technique

We propose the algorithm to apply the share technique.

Algorithm 2 Combination of S-box and S-box†

Input: Public qubit set SQ_i, used qubit set $q^{old}_{private}$, and unallocated qubit set q^{old}_{public}
Output: New used qubit set $q^{new}_{private}$, and new unallocated qubit set q^{new}_{public}

1: The depth d_{max} is the maximum of depth of S-box and S-box†
2: **for** the current depth d from 1 to d_{max} **do**
3: **if** $|q^{old}_{public}| = 0$ **then**
4: **return Error**
5: **end if**
6: Choose $q \in q^{old}_{public}$, execute S-box under depth d, and put q into $q^{new}_{private}$
7: Execute S-box† under depth d. If one qubit q' is cleaned up, put q' into q^{old}_{public}
8: **end for**
9: $q^{new}_{public} = SQ_i / q^{new}_{private}$
10: **return** q^{new}_{public} and $q^{new}_{private}$

We optimize the AES S-box. (24 qubits are enough)

Layer	Previous pool	Need	Preset qubits	Cleaning	New pool
L_1	0	16	16	1	1
L_2	1	9	8	18	18
L_3	18	3	0	14	29
L_4	29	3	0	4	30
L_5	30	6	0	6	30
L_6	30	4	0	3	29
L_7	29	14	0	3	18
L_8	18	18	0	9	9
L_9	9	1	0	16	24

Comparisons of Different Structures

Source	Method	Width	#CNOT	#Toffoli(AND)	Toffoli(AND) depth
[18]	Independence	$120+120+32=240+32$	428	68	4
This paper	**Combination**	$\mathbf{74+24+32=98+32}$	**312**	68	4

- Prior to executing the combination, 74 ancilla qubits are utilized, and then we allocate 24 qubits with an initial state of $|0\rangle$ in $\mathrm{q}_{\mathrm{public}}^{\mathrm{old}}$.
- The number of ancilla qubits: $240 \rightarrow 98$

Outline

Improved Quantum Circuits for AES

24 Different Quantum Circuits for AES

- AES-128/-192/-256
- Different AND operations:
  - the circuit without decomposing the Toffoli gates;
  - the circuit with T-depth 1 and 4 ancilla qubits (Toffoli gate);
  - the circuit with T-depth 4 and 0 ancilla qubits (Toffoli gate);
  - the AND-based decomposition to construct AES quantum circuit.
- Two implementations for the linear layer:
  - in-place circuit, which utilizes the circuit found by us with depth 16.
  - out-of-place circuit with depth 11.

- Using ProjectQ

Using Toffoli Gate

Cipher	Source	#CNOT	#NOT	#Toffoli	Toffoli depth	Width	Toffoli depth × Width
AES-128	[13]	166,548	1,456	151,552	12,672	984	12,469,248
	[1]	192,832	1,370	150,528	-	976	-
	[25]	53,360	1,072	16,688	12,168	264	3,212,352
	[23]	107,960	1,570	16,940	1,880	864	1,624,320
	[34]	128,517	4,528	19,788	2,016	512	1,032,192
	[16]($p = 9$)	126,016	2,528	17,888	1,558	374	582,692
	[25]	53,496	1,072	16,664	1,472	328	482,816
	[16]($p = 18$)	126,016	2,528	17,888	820	492	403,440
	[18]	81,312	800	12,240	40	6,368	254,720
	[26]($m = 16$)	77,984	2,224	19,608	476	474	225,624
	This paper(out-of-place)	75,024	800	12,920	40	**4,823**	**192,920**
	This paper(in-place)	65,736	800	12,920	40	**3,667**	**146,680**
AES-192	[13]	189,432	1,608	172,032	11,088	1,112	12,329,856
	[25]	70,736	1,160	19,328	14,496	328	4,754,688
	[23]	125,580	1,692	19,580	1,640	896	1,469,440
	[34]	152,378	5,128	22,380	2,022	640	1,294,080
	[18]	92,856	896	14,008	48	6,688	321,024
	[26]($m = 16$)	90,832	2,568	22,800	572	538	307,736
	This paper(out-of-place)	85,808	896	14,552	48	**5,356**	**257,088**
	This paper(in-place)	74,456	896	14,552	48	**3,935**	**188,880**
AES-256	[13]	233,836	1,943	215,040	14,976	1,336	20,007,936
	[25]	74,472	1,367	23,480	17,412	392	6,825,504
	[23]	151,011	1,992	23,760	2,160	1,232	2,661,120
	[34]	177,645	6,103	26,774	2,292	768	1,760,256
	[18]	113,744	1,103	17,408	56	6,976	390,656
	[26]($m = 16$)	110,688	3,069	27,816	646	502	388,892
	This paper(out-of-place)	106,704	1,119	18,360	56	**6,097**	**341,432**
	This paper(in-place)	93,288	1,119	18,360	56	**4,429**	**248,024**

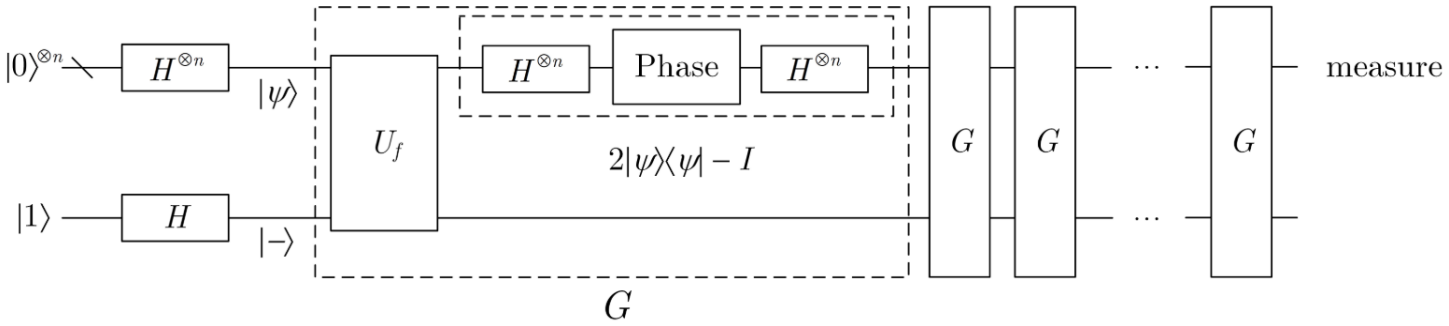
- In conclusion, compared with the previous lowest results, the product of our implementations achieved a reduction of 35%, 38%, 36% for AES-128, -192, and -256, respectively.
- Qubit count: $6368 \rightarrow 3667$

Using AND Gate

Cipher	Source	#CNOT	#1qCliff	$\#T$	$\#M$	T-depth	Width	DW-cost	$\#FD$
AES-128	[18](out-of-place)	152,496	39,952	27,200	5,440	40	7,524	300,960	749
	This paper(out-of-place)	141,664	51,800	27,200	6,120	40	**4,844**	**193,760**	**730**
	[18](in-place)	142,992	37,520	27,200	5,440	40	6,372	254,880	928
	This paper(in-place)	132,376	51,800	27,200	6,120	40	**3,689**	**147,560**	**800**
AES-192	[18](out-of-place)	174,152	46,232	30,464	6,392	48	8,100	388,800	895
	This paper(out-of-place)	160,608	58,424	30,464	6,936	48	**5,356**	**257,088**	**876**
	[18](in-place)	162,536	43,192	30,464	6,392	48	6,692	321,216	1,114
	This paper(in-place)	149,256	58,424	30,464	6,936	48	**3,945**	**189,360**	**962**
AES-256	[18](out-of-place)	213,624	56,975	37,536	8,024	56	8,644	484,064	1,048
	This paper(out-of-place)	200,544	73,879	38,080	8,840	56	**6,124**	**342,944**	**1,018**
	[18](in-place)	199,896	53,327	37,536	8,024	56	6,980	390,880	1,307
	This paper(in-place)	187,128	73,879	38,080	8,840	56	**4,457**	**249,592**	**1,120**

- For the in-place version, the circuit depth achieves a reduction of 13.8%, 13.6%, and 14.3%, respectively.
- It is worth noting that the circuits with the AND gate and out-of-place linear layer have a lower depth.
- For AES-128, -192, and -256, we only require the depth of 730, 876, and 1,018, respectively.

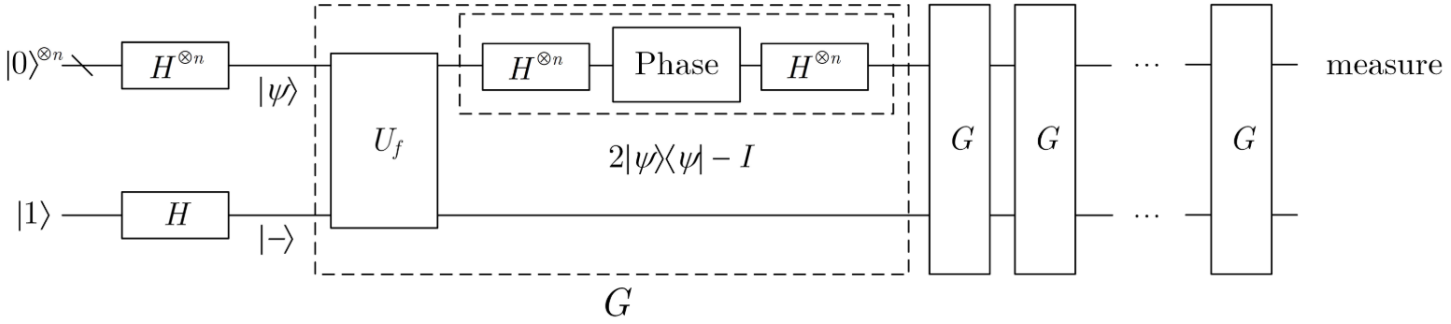
Grover's Algorithm



- For a given m and c, we use an operator U_f for evaluating a Boolean function $f : \{0,1\}^k \rightarrow \{0,1\}$, where

$$f(x) = \begin{cases} 1, & \text{if } Enc_x(m) = c\,, \\ 0, & \text{if } Enc_x(m) \neq c\,. \end{cases}$$

Grover's Algorithm



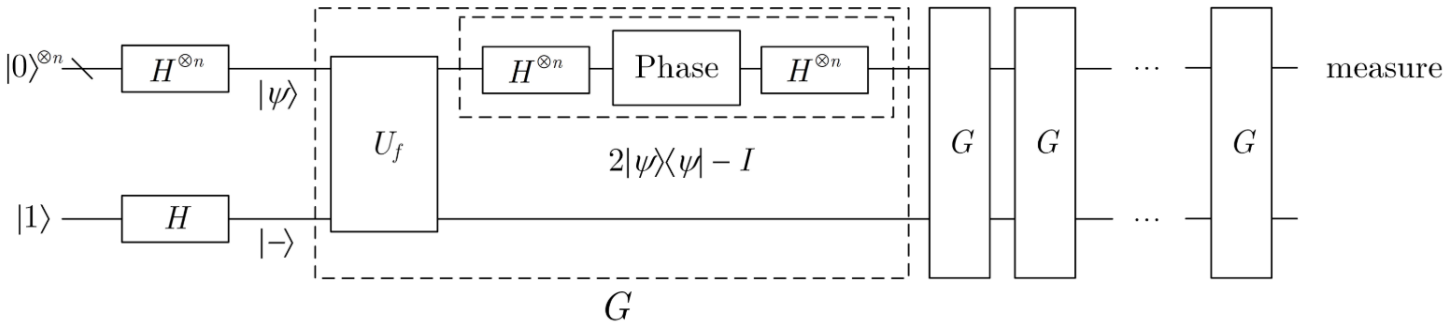
- Grover's algorithm searches a space of 2^k elements, working with a superposition:

$$|\psi\rangle = H^{\otimes k}|0\rangle^{\otimes k} = \frac{1}{2^{k/2}}\Sigma_{x\in\{0,1\}^k}|x\rangle$$

and a single qubit:

$$|\varphi\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\,.$$

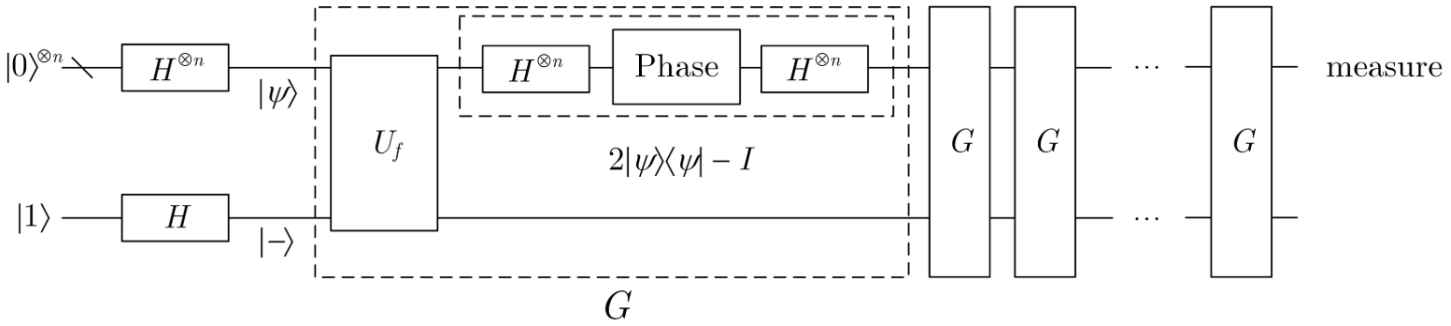
Grover's Algorithm



- When we apply the Grover Oracle U_f to a state $|x\rangle|y\rangle$, where $|y\rangle$ is a single qubit, the oracle maps $|x\rangle|y \oplus f(x)\rangle$. If we set $|y\rangle = |\varphi\rangle$, the transformation is

$$|x\rangle|\varphi\rangle \rightarrow (-1)^{f(x)}|x\rangle|\varphi\rangle \ .$$

Grover's Algorithm



- Following the above process, Grover's algorithm prepares the state $|\psi\rangle|\varphi\rangle$. Then, it repeatedly applies the Grover iteration,

$$\mathrm{G} = (2|\psi\rangle\langle\psi| - \mathrm{I})\mathrm{U_f}.$$

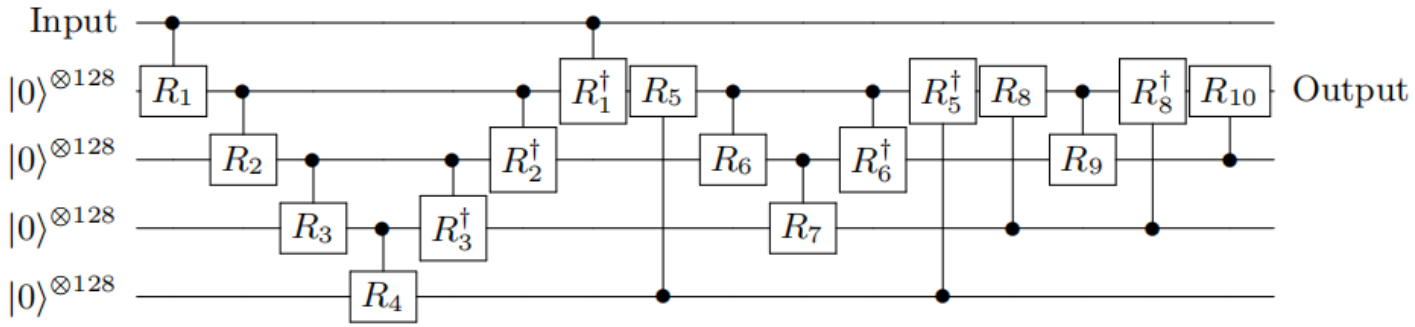
Applying Grover's Algorithm for AES

Cipher	r	Source	Width (W)	Gates (G)	$\#FD$	$FD \times G$	$FD \times W$	$FD^2 \times G$	$FD^2 \times W$
AES-128	1	[19]	1.92×2^{11}	1.33×2^{82}	1.08×2^{75}	1.436×2^{157}	1.038×2^{87}	1.551×2^{232}	1.120×2^{162}
		[18]	1.84×2^{12}	1.36×2^{82}	1.15×2^{74}	1.564×2^{156}	1.055×2^{87}	1.797×2^{230}	1.212×2^{161}
		This paper	1.18×2^{12}	1.37×2^{82}	1.12×2^{74}	$\mathbf{1.535 \times 2^{156}}$	$\mathbf{1.325 \times 2^{86}}$	$\mathbf{1.719 \times 2^{230}}$	$\mathbf{1.480 \times 2^{160}}$
AES-192	2	[19]	1.02×2^{13}	1.50×2^{115}	1.14×2^{107}	1.710×2^{222}	1.163×2^{120}	1.949×2^{239}	1.326×2^{227}
		[18]	1.84×2^{13}	1.45×2^{115}	1.37×2^{106}	1.988×2^{221}	1.261×2^{120}	1.365×2^{328}	1.731×2^{226}
		This paper	1.24×2^{13}	1.44×2^{115}	1.35×2^{106}	$\mathbf{1.944 \times 2^{221}}$	$\mathbf{1.679 \times 2^{119}}$	$\mathbf{1.312 \times 2^{328}}$	$\mathbf{1.130 \times 2^{226}}$
AES-256	2	[19]	1.09×2^{13}	1.84×2^{147}	1.29×2^{139}	1.187×2^{287}	1.401×2^{152}	1.531×2^{426}	1.814×2^{291}
		[18]	1.96×2^{13}	1.74×2^{147}	1.61×2^{138}	1.398×2^{286}	1.576×2^{152}	1.123×2^{425}	1.266×2^{291}
		This paper	1.43×2^{13}	1.76×2^{147}	1.56×2^{138}	$\mathbf{1.373 \times 2^{286}}$	$\mathbf{1.117 \times 2^{152}}$	$\mathbf{1.071 \times 2^{425}}$	$\mathbf{1.740 \times 2^{290}}$

- It implies that we need to use two plaintext-ciphertext pairs to determine the key.
- In terms of resources corresponding to Grover's algorithm, one key expansion algorithm corresponds to two round functions.

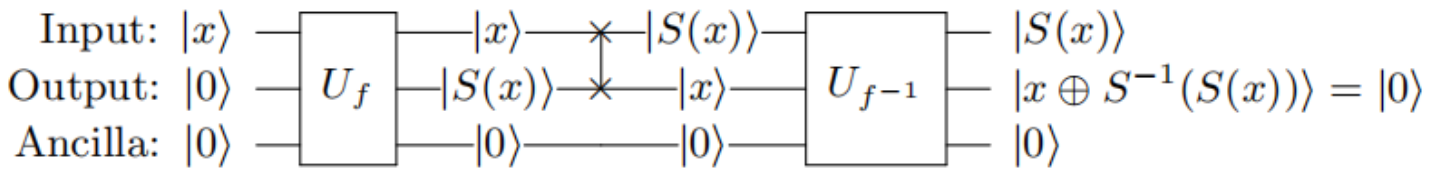
Outline

Zig-Zag Architecture

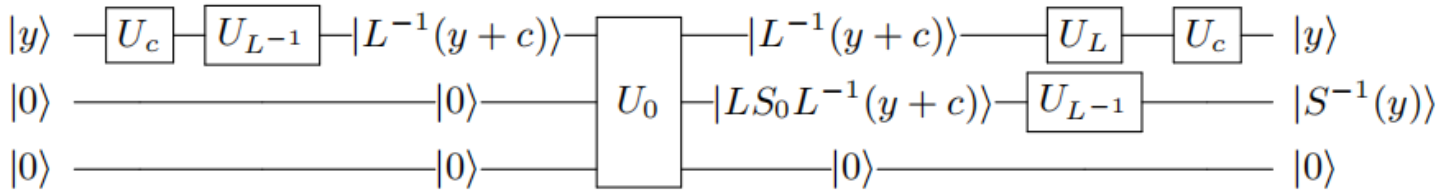


- The zig-zag architecture is proposed by performing reverse operations in each round.
- Subsequently, at ASIACRYPT 2020, Zou et al. improved the zig-zag architecture and implemented AES-128 with 512 qubits and Toffoli depth 2016.
- At ASIACRYPT 2022, Huang et al. proposed the round-in-place architecture to improve the results.

Round-in-Place S-box Circuit

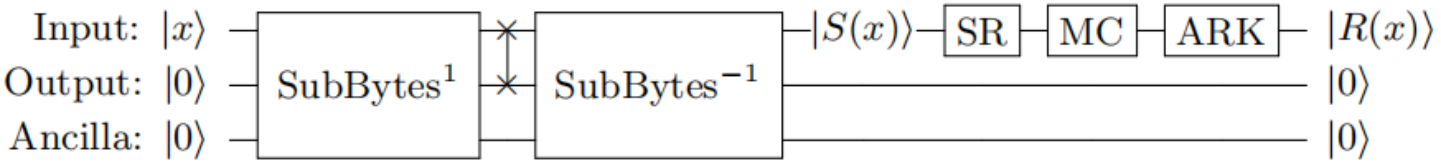


- If we also have the inverse circuit $U_{f^{-1}}$, we can achieve the *in-place* circuit by swapping $|x\rangle$ and $|S(x)\rangle$.

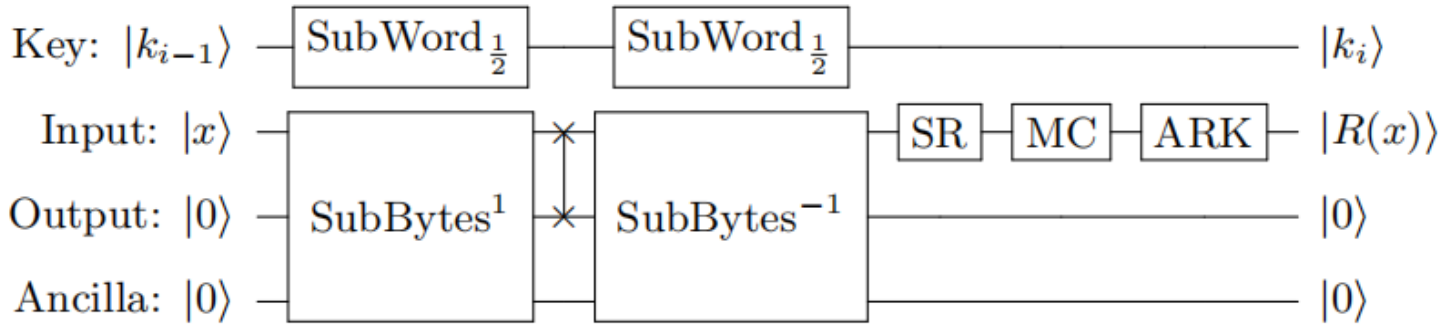


- Huang et al. provided a method to convert U_f into $U_{f^{-1}}$.
- They provided an SAT-based method and implement U_L or $U_{L^{-1}}$ by 14 CNOT gates.
- adding 42 CNOT gates and 4 X gates.

Round-in-Place S-box Circuit



- Based on the *round-in-place* S-box circuit, one can construct the *round-in-place* round function $\mathrm{R_i}$ easily.



- For $\mathrm{i} = 1, 2$, the key schedule can be split.
- For $\mathrm{i} = 4, 8, 16$, the structure is similar.

Constructing a Low-Width S-box Circuit

- 8 input qubits $u_0, \ldots, u_7$, and 8 output qubits $s_0, \ldots, s_7$.
- There are 9, 3, 4, and 18 target qubits in T-depth 1, 2, 3, and 4.
- Because the layer in T-depth 4 contains the most AND gates, we must satisfy its parallelism first.
- In other layers, AND gates do not require any more ancilla qubits.
- Apart from 8 output qubits, we need to allocate 10 ancilla qubits.
- The final number of ancilla qubits of the S-box is 70.

Width	#CNOT	#1qCliff	#T	#M	T-depth	Full depth
60+10+16	688	220	136	34	4	132

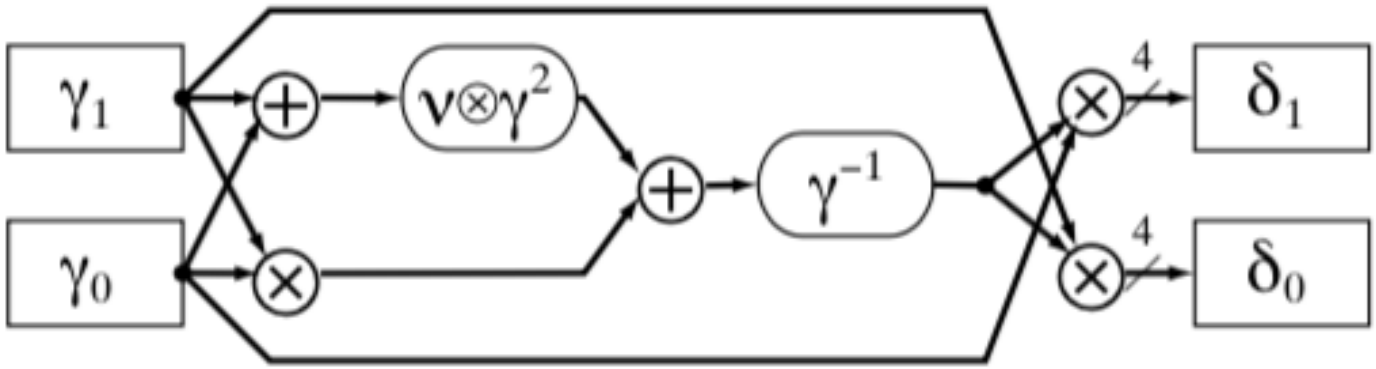
Applying New S-box Circuit into Round-in-place Architecture

AES-128	Width	T-depth	DW-cost
$i = 1$	$256 + 128 + 156 + 1120 = 1660$	$80 \times 1 = 80$	**132,800**
$i = 2$	$256 + 64 + 78 + 560 = 958$	$80 \times 2 = 160$	153,280
$i = 4$	$256 + 32 + 78 + 280 = 646$	$80 \times 4 = 320$	206,720
$i = 8$	$256 + 16 + 78 + 140 = 490$	$80 \times 8 = 640$	313,600
$i = 16$	$256 + 8 + 78 + 70 = 412$	$80 \times 16 = 1280$	527,360

- AES-128 can be implemented by the *round-in-place* round function with the lower DW-cost 132,800, while the previous best result is 204,800.
- For AES-192, we achieve a circuit with DW-cost (width $\times$ T-depth) $1,724 \times 96 = 165,504$.
- For AES-256, we achieve a circuit with DW-cost (width $\times$ T-depth) $1,788 \times 112 = 200,256$.

Future Work

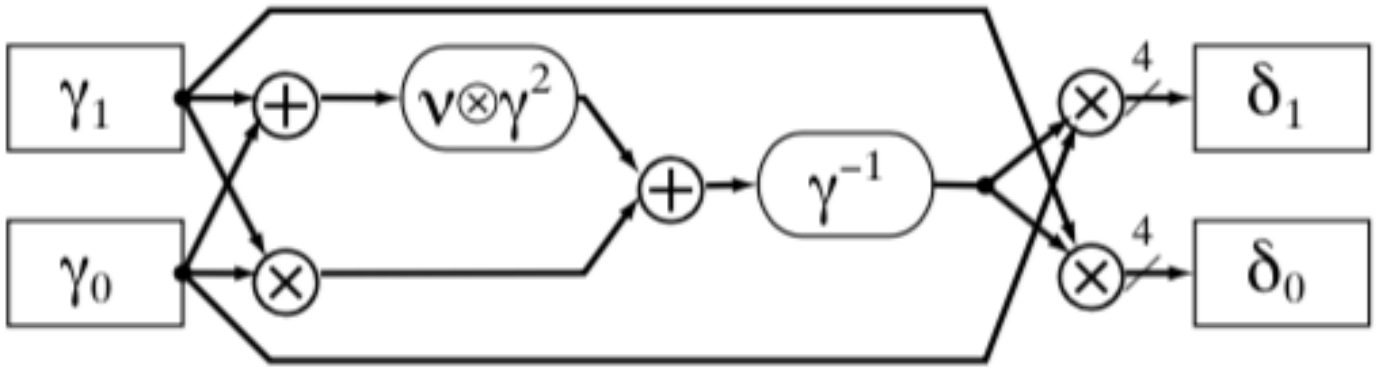
- In the future, we can improve the quantum circuit for AES.
- Our method can be used to transform the classical circuit into the quantum circuit.
- Thus, how to improve the classical circuit is a question.



- If the classical circuit used for improvements is updated, our approach can still be employed to reduce these three metrics.

Future Work

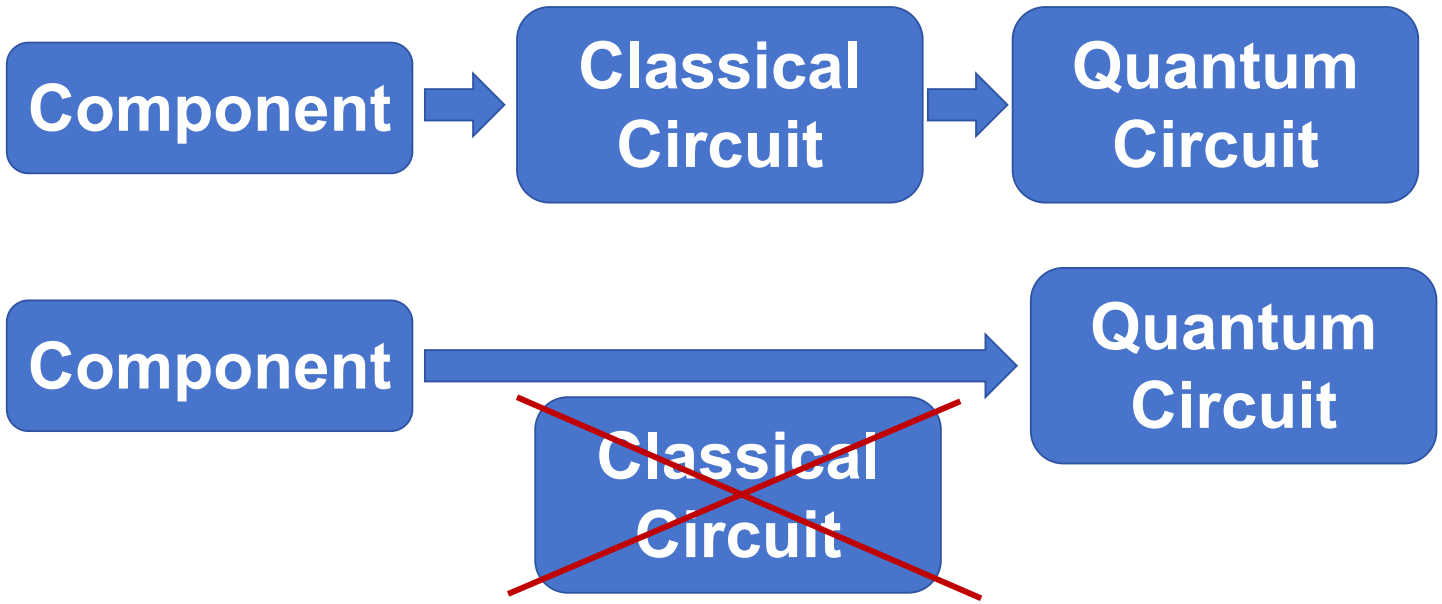
- In the future, we can improve the quantum circuit for AES.
- Our method can be used to transform the classical circuit into the quantum circuit.
- Thus, how to improve the classical circuit is a question.



- If the classical circuit used for improvements is updated, our approach can still be employed to reduce these three metrics.

Future Work

- How to construct the quantum circuit directly is still a problem.



- In previous work, many circuits are constructed by classical circuits.
- Thus, we should consider how to construct the quantum circuit.

Future Work

- In classical computing, searching an unsorted database typically requires examining each element one by one, resulting in a linear time complexity.
- Grover's algorithm, on the other hand, achieves a quadratic speedup by exploiting quantum parallelism.
- This quantum parallelism is a key factor in Grover's algorithm's efficiency, allowing it to perform the search with a square root speedup.

Thanks for Your Attention!