Post-rebuttal Improvements

No Author Given

No Institute Given

1 More efficient quantum circuits of AES

Thanks for the comments! We find that we can reduce the Toffoli depth and the number of Toffoli gates in our Algorithm 3. Based on our new Algorithm 3, we can construct more efficient quantum circuits for AES. The results of the new quantum circuits of AES are listed in Table 1. Note that the $T \cdot M$ for our new circuit of AES-192 is 1441280, which is better than 1469440 in the circuit proposed by Langenberg. The implementation of AES S-box and S-box^{-1} are available at

`https://github.com/Asiacrypt2020submission370/aes/`.

The details of the new quantum circuits of AES are described in Section 2.

Table 1. Summary of the new results

Cipher	# qubits	Toffoli Depth	# Toffoli	# CNOT	# NOT	$T \cdot M$	Source
AES-128	512	2452	21332	143400	4528	1255424	our previous submission
	512	2284	19788	136408	4528	1169408	see Sect. 2.1
AES-192	640	2395	23940	168664	5128	1532800	our previous submission
	640	2252	22380	162120	5128	1441280	see Sect. 2.2
AES-256	768	2769	29452	202104	6103	2126592	our previous submission
	768	2594	26774	189013	6103	1992192	see Sect. 2.3

1.1 More efficient implementation of Algorithm 3

As shown in `https://github.com/Asiacrypt2020submission370/aes/blob/master/S-box/Algorithm_4.c`, our new Algorithm 3 can be constructed with 6 ancilla qubit, 17 Tofoli gates, and 93 CNOT gates, while our previous Algorithm 3 required 6 ancilla qubits, 21 Toffoli gates, and 109 CNOT gates. In detail, the new Algorithm 3 can reduce the Toffoli gate and the Toffoli depth simultaneously.

We also find that the Toffoli depth of our new Algorithm 3 is the same as Algorithm 6 in our previous submission. We think it reflects the structure of S-box. That is, S-box (or S-box^{-1}) needs the same Toffoli gates to compute

the intermediate values t_{29}, t_{33}, t_{37}, t_{40} in Observation 2 (or t'_{29}, t'_{33}, t'_{37}, t'_{40} in Observation 4).

Since our new Algorithm 3 needs to recompute t_{36} and t_2, we can obtain a new depth-qubit tradeoff of Algorithm 3 as follows. First, we observe that our new Algorithm 3 shall compute t_{36} three times. If we introduce a new ancilla qubit to store t_{36}, we do not need to recompute t_{36}. That is, we can save two Toffoli gates and two Toffoli depth by storing t_{36} in a new ancilla qubit. Second, our new Algorithm 3 needs to compute t_2 twice. If we introduce a new ancilla qubit to store t_2, we can save one Toffoli gates and one Toffoli depth. That is, we can obtain a new depth-qubit tradeoff i of our new Algorithm 3 with $17-(i+1)$ Toffoli depth, $6+i$ ancilla qubits, $17-(i+1)$ Toffoli gates, and $93+(i+1)$ CNOT gates (for $1 \leq i \leq 2$).

1.2 More efficient implementations of Algorithm 4 and Algorithm 5

Since Algorithm 4 (or Algorithm 5) shall call Algorithm 3 twice to compute S-box, we can obtain improved Algorithm 4 (or Algorithm 5) with the new Algorithm 3. That is, we can obtain a new depth-qubit trade-off i of Algorithm 4 as follows.

1. When $i = 0$, Algorithm 4 can compute the output of S-box with 6 ancilla qubits, 52 Toffoli gates, 325 CNOT gates, and 4 NOT gates. The Toffoli depth of Algorithm 4 in this case is 52.
2. When $1 \leq i \leq 2$, Algorithm 4 can compute the output of S-box with $6+i$ ancilla qubits, $52\text{-}2(i+1)$ Toffoli gates, $325+2(i+1)$ CNOT gates, 4 NOT gates. The Toffoli depth of Algorithm 4 in this case is $52\text{-}2(i+1)$.

In addition, we can also obtain a new depth-qubit trade-off i of Algorithm 5 as follows.

1. When $i = 0$, Algorithm 5 can compute the output of S-box with 7 ancilla qubits, 68 Toffoli gates, 348 CNOT gates, 4 NOT gates, and 68 Toffoli depth.
2. When $1 \leq i \leq 2$, Algorithm 5 can compute S-box with $7+i$ ancilla qubits, $68\text{-}2(i+1)$ Toffoli gates, $348+2(i+1)$ CNOT gates, 4 NOT gates, and $68\text{-}2(i+1)$ Toffoli depth.

1.3 Cost of our quantum circuits of S-box and S-box^{-1}

Because Algorithm 5 (or Algorithm 7) is designed to compute the output of S-box (or S-box^{-1}) for the case the output qubits are not zero. It is interesting to compare the number of Toffoli gates used in Algorithm 5 with Algorithm 7. We observe the Toffoli gate in Algorithm 5 is 68, while the number of Toffoli gates in Algorithm 7 is 69. We can explain the reason as follows.

According to the Observation 2 in our previous submission, we can store z_{11} (or z_{17}) in S_5 (or S_2) without affecting the other output qubits. In other words, we do not need to store z_{11} and z_{17} in Z in Algorithm 5. However, Algorithm 7 contains only one z_7, which only appears in S_3 (see in Observation 4). That is,

we need to store 17 z_i (for $0 \leq i \leq 17$, and $i \neq 7$) in Z in Algorithm 7, while Algorithm 5 just store 16 z_j in Z (for $0 \leq j \leq 17$, $j \neq 11$ and 17). Since we need one Toffoli gate to clean up Z, Algorithm 7 requires one more Toffoli gates than Algorithm 5.

2 Quantum Circuits of AES

2.1 Our Improved Quantum Circuit Implementations of AES-128

After denoting r_i^j and s_i^{j+1} as the i-th byte of Round j and the S-box operations in Round $j+1$ (for $0 \leq j \leq 9$ and $0 \leq i \leq 15$), the time and memory cost of each parts can be computed as follows.

The time and space cost of Part 1. We just compute Round 1 and remove Round 0 in Part 1 (see in Fig. 1).

1. We can obtain Round 0 by implementing at most 128 Pauli-X gates (or called NOT gate) on the input keys W_0, W_1, W_2, W_3.
2. We can adopt Algorithm 4 in parallel to compute s_i^1 (for $0 \leq i \leq 15$), because we have 384 zero qubits (from the 128 to 511 qubits in initial state in Fig. 1). Since we need 128 qubits to store these 16 bytes s_i^1 (for $0 \leq i \leq 15$), we have $384 - 128 = 256$ qubits left for ancilla qubits. In other words, we can obtain a depth-qubit trade-off $i = 2$ for these 16 S-box operations. That is, we can implement these 16 S-box operations with 128 ancilla qubits, 736 Toffoli gates and 5296 CNOT gates. The Toffoli depth of these 16 S-box operations is 46, because we can implement the 16 S-box in parallel.
3. After obtaining s_i^1 (for $0 \leq i \leq 15$), we can apply at most 128 NOT gates to Round 0 so as to obtain W_0, W_1, W_2, W_3 again. Then we can compute the round-key W_4, W_5, W_6, W_7 for Round 1 with the knowledge of W_0, W_1, W_2, W_3. Similar to step 2, we can obtain a depth-qubit trade-off $i = 2$ for these 4 S-box operations for W_4, because we have 224 ancilla qubits left. That is, we need 184 Toffoli gates and 1324 CNOT gates to implement these 4 S-box operations. The Toffoli depth of this operation is 46, because we can implement these 4 S-box in parallel.
4. We not only require $3 \times 32 = 96$ CNOT gates and 1 NOT gate to produce W_4, W_5, W_6, W_7, but also need 128 CNOT gates to implement the AddRoundKey operation. In addition, we still need $277 \times 4 = 1108$ CNOT gates to implement 4 times MixColumns operations.

To sum up, we can implement Part 1 with 920 Toffoli gates, 7952 CNOT gates, and 337 NOT gates. Since the 16 S-box in Round 1 and W_4 cannot be implemented in parallel, the Toffoli depth of the above operation is 92.

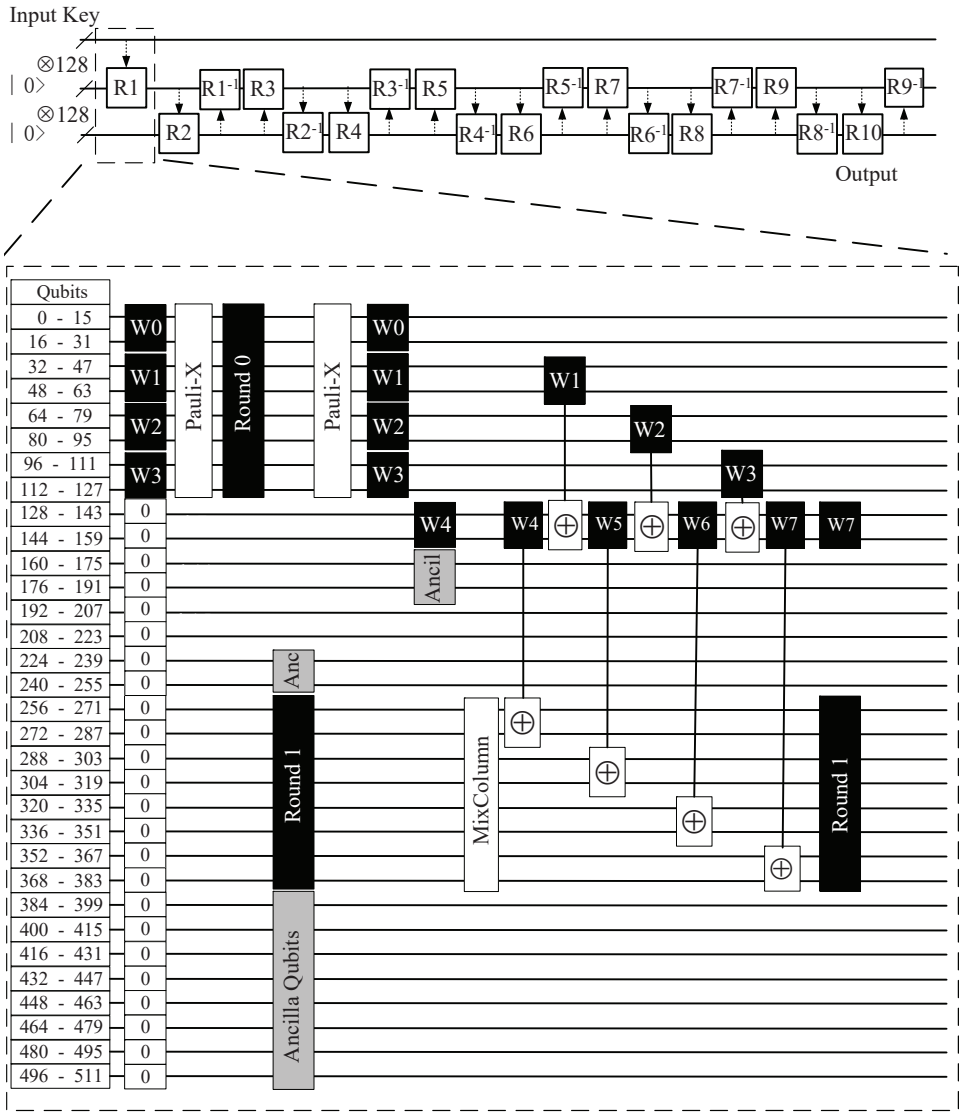

Fig. 1. Our method for computing Round 1.

The time and space cost of Part 2. Part 2 contains three similar rounds from Round 2 to Round 4. In the following, we show the time and memory cost of computing Round 4 and removing Round 3, which can be divided into 5 phases (see in Fig. 2).

1. We can compute $s_0^4, \cdots, s_7^4$ in Round 4 and the first two bytes S-box operations of W_{16}, which requires 80 qubits to store these 10 bytes output of S-box. Since we have 160 zero qubits (the 224-255 and 384-511 qubits in state0 in Fig. 2), we have $160 - 80 = 80$ qubits left for ancilla qubits. As a result, we can obtain a depth-qubit trade-off $i = 2$ for these 10 S-box operations. That is, we can implement these 10 S-box operations with 80 ancilla qubits, 460 Toffoli gates, 3310 CNOT gates and 40 NOT gates. The Toffoli depth of these 10 S-box operations is 46, because we can implement these 10 S-box operations in parallel.
2. We can remove $r_0^3, \cdots, r_7^3$ in Round 3 by adopting Algorithm 7. Since we have 80 zero qubits (the 240-255 and 448-511 qubits in state1 in Fig. 2), we can obtain a depth-qubit trade-off $i = 3$ for these 8 S-box^{-1} operations. That is, we can implement these 8 S-box^{-1} operations with 80 ancilla qubits, 504 Toffoli gates, 3176 CNOT gates and 192 NOT gates. The Toffoli depth of the 8 S-box^{-1} operations is 63, because we can implement these 8 S-box^{-1} in parallel.
3. We can compute $s_8^4 \cdots, s_{15}^4$ in Round 4 and the last two bytes of W_{16}, which requires 80 qubits to store these 10 bytes output of S-box. Since we have 144 zero qubits (the 240-319 and 448-511 qubits in state2 in Fig. 2), we have $144 - 80 = 64$ qubits left for ancilla qubits. In other words, we can obtain the depth-qubit trade-off $i = 1$ (and $i = 0$) for the first 4 S-box (the left 6 S-box) operations. That is, we can implement the first 4 S-box operations with $4 * 7$ =28 ancilla qubits, 192 Toffoli gates, 1316 CNOT gates and 16 NOT gates, while the left 6 S-box operations can be implemented with 36 ancilla qubits, 312 Toffoli gates, 1950 CNOT gates and 24 NOT gates. To sum up, we can implement these 10 S-box operations with 64 ancilla qubits, 504 Toffoli gates, 3266 CNOT gates and 40 NOT gates. The Toffoli depth of these 10 S-box operations is 52, because we can implement these 10 S-box operations in parallel.
4. We can remove the $r_8^3, \cdots, r_{15}^3$ in Round 3 by adopting Algorithm 7. Since we have 64 zero qubits here (the 256-319 qubits in state3 in Fig. 2), we can obtain a depth-qubit trade-off $i = 1$ for these 8 S-box^{-1} operations. That is, we can implement these 8 S-box^{-1} operations with 64 ancilla qubits, 544 Toffoli gates, 3136 CNOT gates and 192 NOT gates. The Toffoli depth of the 8 S-box^{-1} operations is 67, because we can implement the 8 S-box in parallel.
5. We shall implement the MixColumns and AddRoundKey operations so as to obtain Round 4. The MixColumns operation for 128-bit state requires $277 \times 4 = 1108$ CNOT operations. According to the round-key algorithm of AES-128, after the SubWord operation, we still need $32 \times 8 = 256$ CNOT gates and 1 NOT gate to compute W_{16}, W_{17}, W_{18}, W_{19}. As a result, we can

implement the AddRoundKey operation with 256+128=384 CNOT gates and 1 NOT gate.

To sum up, we need 2012 Toffoli gates, 14380 CNOT gates and 465 NOT gates to obtain Round 4 and remove Round 3. The Toffoli depth of the above five steps is 228.

Similar to the above operation, we can compute the time and memory cost of the left rounds in Part 2 as follows. The depth and qubits of obtaining Round 3 and removing Round 2 can be computed as follows.

1. We can compute the $s_0^3, \cdots, s_7^3$ in Round 3 and the first 2 S-box operations of W_{12}. Since we have 112 zero qubits here, we can obtain a depth-qubit trade-off $i = 2$ for these 10 S-box operations. That is, we can implement these 10 S-box operations with 80 ancilla qubits, 460 Toffoli gates, 3310 CNOT gates and 40 NOT gates. The Toffoli depth of these 10 S-box operations is 46.
2. We can remove the $r_0^2, \cdots, r_7^2$ in Round 2. Since we have 112 zero qubits, we can obtain a new depth-qubit trade-off $i = 3$ for these 8 S-box^{-1} operations. That is, we can implement these 8 S-box^{-1} operations with 80 ancilla qubits, 504 Toffoli gates, 3176 CNOT gates and 192 NOT gates. The Toffoli depth of the 8 S-box^{-1} operations is 63.
3. We can compute the $s_8^3, \cdots, s_{15}^3$ in Round 3 and the last 2 S-box of W_{12}. Since we have 96 zero qubits, we can obtain a new depth-qubit trade-off $i = 2$ for these 10 S-box operations. That is, we can implement these 10 S-box operations with 80 ancilla qubits, 460 Toffoli gates, 3310 CNOT gates and 40 NOT gates. The Toffoli depth of these 10 S-box operations is 46.
4. We can remove the $r_8^2, \cdots, r_{15}^2$ in Round 2. Since we have 96 zero qubits, we can obtain a new depth-qubit trade-off $i = 3$ for these 8 S-box^{-1} operations. That is, we can implement these 8 S-box^{-1} operations with 80 ancilla qubits, 504 Toffoli gates, 3176 CNOT gates and 192 NOT gates. The Toffoli depth of the 8 S-box^{-1} operations is 63.
5. We need $277 \times 4 + 128 + 7 \times 32 = 1460$ CNOT gates and 1 NOT gate to implement the MixColumns and AddRoundKey operations.

To sum up, we require 1928 Toffoli gates, 14432 CNOT gates and 465 NOT gates to obtain Round 3 and remove Round 2. The Toffoli depth of this transformation is 218.

The time and memory of obtaining Round 2 and removing Round 1 can be computed as follows.

1. We point out that we can gain more ancilla qubits in the above operation, because we have not computed the round-key W_7 (or W_{11}) for Round 2 (or Round 3) yet.
2. We can compute the first 12 S-box operations $s_0^2, \cdots, s_{11}^2$ in Round 2. Since we have 224 zero qubits here, we can obtain a new depth-qubit trade-off $i = 2$ for the 12 S-box operations. That is, we can implement these 12 S-box operations with 96 ancilla qubits, 552 Toffoli gates, 3972 CNOT gates and 48 NOT gates. The Toffoli depth of these 12 S-box operations is 46, because we can implement these 12 S-box operations in parallel.

3. We can remove the first 8 bytes $r_0^1, \cdots, r_7^1$ in Round 1, and obtain the last 4 bytes of S-box operations $s_{12}^2, \cdots, s_{15}^2$ in Round 2. Since we have 96 zero qubits, we can obtain a depth-qubit trade-off $i = 2$ for the 8 S-box^{-1} operations, while the 4 S-box operation are implemented with a depth-qubit trade-off $i = 0$. That is, we can implement these 8 S-box^{-1} operations with 72 ancilla qubits, 520 Toffoli gates, 3160 CNOT gates and 192 NOT gates. The 4 S-box operations can be implemented with 24 ancilla qubits, 208 Toffoli gates, 1300 CNOT gates and 16 NOT gates. The Toffoli depth of these 8 S-box^{-1} and 4 S-box operations is 65.
4. We can remove the last 8 bytes of Round 1 and obtain the 4 bytes S-box of W_8. Since we have 128 zero qubits, we can obtain a depth-qubit trade-off $i = 3$ for the 8 S-box^{-1} operations, and a depth-qubit trade-off $i = 2$ for the 4 S-box operations. That is, we can implement these 8 S-box^{-1} operations with 80 ancilla qubits, 504 Toffoli gates, 3176 CNOT gates and 192 NOT gates. The 4 S-box operations can be implemented with 32 ancilla qubits, 184 Toffoli gates, 1308 CNOT gates and 16 NOT gates. The Toffoli depth of these 8 S-box^{-1} and 4 S-box operations is 63.
5. We need $277 \times 4 + 128 + 8 \times 32 = 1492$ CNOT gates and 1 NOT gate to implement the MixColumns and AddRoundKey operations.

To sum up, we require 1968 Toffoli gates, 14424 CNOT gates and 465 NOT gates to obtain Round 2 and remove Round 1. The Toffoli depth of this operation is 174.

The time and space cost of Part 3. Part 3 contains 6 similar rounds operations. In the following, we will show the time and memory cost of obtaining Round 5 and removing Round 4. Then we can compute the time and memory cost of the other rounds in Part 3 in a similar way. As shown in Fig. 3, we can divide the above transformation into 5 phases.

1. We can compute the $s_0^5, \cdots, s_7^5$ in Round 5 and the first two S-box operations of W_{20}. Since we have 128 zero bits (from the 256 to 383 qubits in state0 in Fig. 3), we have 128-64=64 qubits left for ancilla qubits, because we need $|0\rangle^{\otimes 64}$ qubits to store $s_0^5, \cdots, s_7^5$. Since Algorithm 4 and Algorithm 5 require 6 qubits and 7 qubits respectively. We need at least $6 \times 8 + 2 \times 7 = 62$ qubits to run Algorithm 4 eight times and Algorithm 5 twice in parallel. As a result, we have $64 - 48 - 14 = 2$ ancilla qubits left, which can introduce one more ancilla qubit for the first 2 S-box of W_{20}. That is, we can implement the first 2 S-box of W_{20} with 16 ancilla qubits, 128 Toffoli gates, 704 CNOT gates and 8 NOT gates, while the 8 S-box of Round 5 can be implemented with 48 ancilla qubits, 416 Toffoli gates, 2600 CNOT gates and 32 NOT gates. To sum up, we can implement these 10 S-box operations with 64 ancilla qubits, 544 Toffoli gates, 3304 CNOT gates and 40 NOT gates. The Toffoli depth of these 10 S-box operations is 64, which is determined by the Toffoli depth of Algorithm 5.

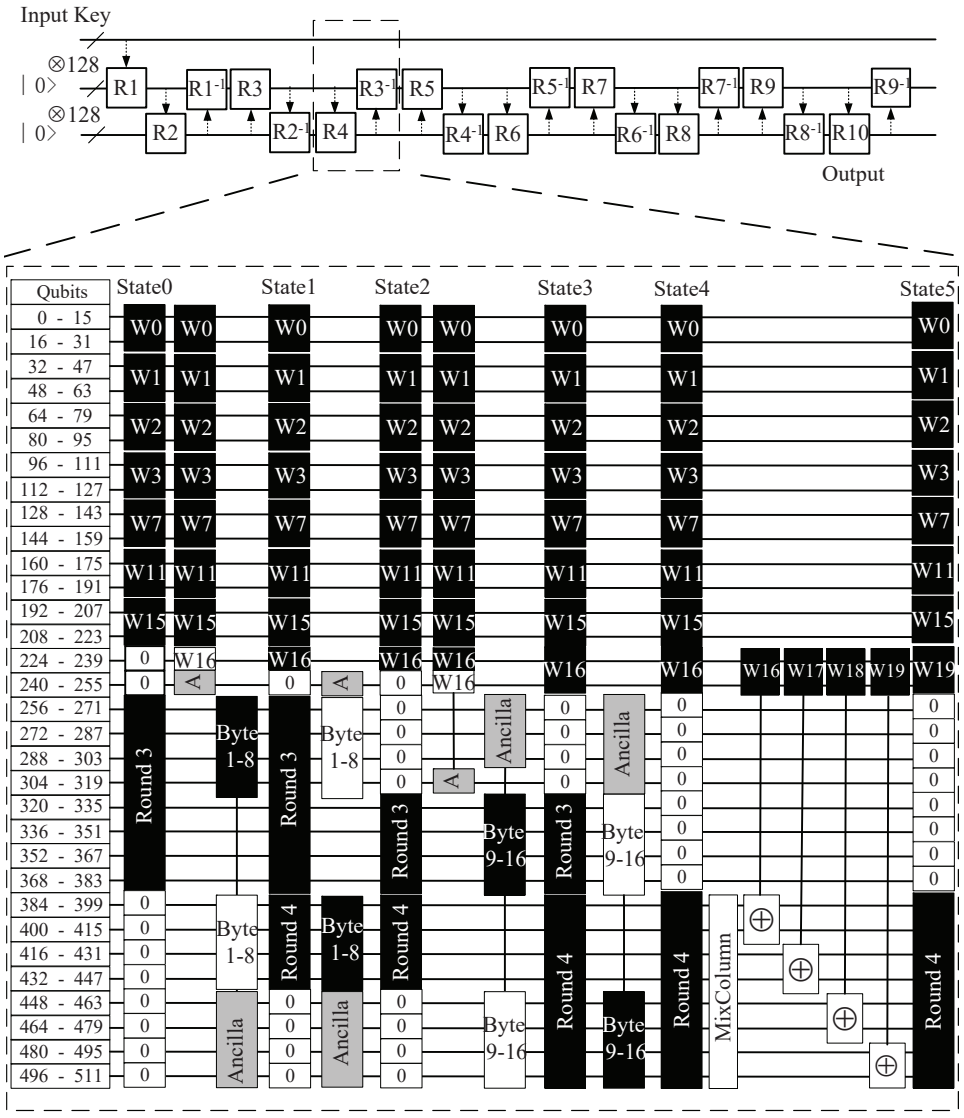

Fig. 2. Our method for computing Round 4 and removing Round 3 of AES-128.

2. We can remove the $r_0^4, \cdots, r_7^4$ in Round 4 by computing eight times S-box^{-1} operations with Algorithm 7. Since we have 64 qubits left for ancilla qubits (see in state1 in Fig. 3), we can obtain a depth-qubit trade-off $i = 1$ for these 8 S-box^{-1} operations. That is, we can implement these 8 S-box^{-1} operations with 64 ancilla qubits, 536 Toffoli gates, 3144 CNOT gates and 192 NOT gates. The Toffoli depth of these 8 S-box^{-1} operations is 67, because we can implement these 8 S-box^{-1} in parallel.
3. We can compute the $s_8^5, \cdots, s_{15}^5$ in Round 5 and the last two bytes of W_{20}. Similar to Step 1, we also have 2 ancilla qubits left, which can obtain a depth-qubit trade-off $i = 1$ for the last 2 S-box operations in W_{20}. Similar to step 1, we can implement these 10 S-box operations with 64 ancilla qubits, 544 Toffoli gates, 3304 CNOT gates and 40 NOT gates. The Toffoli depth of these 10 S-box operations is 64.
4. We shall remove the $r_8^4, \cdots, r_{15}^4$ of Round 4 in state3 by implementing eight times S-box^{-1} operations with Algorithm 7. Since we have 64 ancilla qubits here, we can implement these 8 S-box^{-1} operations with 64 ancilla qubits, 536 Toffoli gates, 3144 CNOT gates and 192 NOT gates. The Toffoli depth of the 8 S-box^{-1} operation is 67.
5. We shall implement the MixColumns and AddRoundKey operations so as to obtain Round 5. The 4 times MixColumns operation requires $277 \times 4 = 1108$ CNOT operations. According to the key algorithm of AES-128, after the **SubWord** operation, we still need $32 \times 8 = 256$ CNOT gates and 1 NOT gate to compute W_{20}, W_{21}, W_{22}, W_{23}. As a result, we can implement the AddRoundKey operation with 256+128=384 CNOT gates and 1 NOT gate.

That is, we need 2160 Toffoli gates, 14388 CNOT gates, 465 NOT gates to obtain Round 5 and remove Round 4, while the Toffoli depth is 262. We can compute the time and space cost of the left 5 rounds in Part 3 in a similar way. However, different rounds of AES-128 require different cost in the AddRoundKey operation. According to the key schedule of AES-128, we need $256 \times 3 = 768$ CNOT gates and $1 \times 3 = 3$ NOT gate to generate the 3 round-keys of Round 6, Round 7 and Round 8, while the round-key of Round 9 and Round 10 require $256 \times 2 = 512$ CNOT gates and $4 \times 2 = 8$ NOT gates.

The time and space cost of our quantum circuit of AES-128. The time and memory cost of our quantum circuit of AES-128 can be obtained by summing Part 1, Part 2 and Part 3. **All in all,** our quantum circuit of AES-128 needs 512 qubits, 19788 Toffoli gates, 136408 CNOT gates and 4528 NOT gates. The Toffoli depth of our quantum circuit implementation of AES-128 is 2284 (see in Table 2).

2.2 Our Improved Quantum Circuit Implementations of AES-192

Since our quantum circuit implementation of AES-192 is similar to AES-128, we just show the conclusions and omit the details. As shown in Table 3, our quantum

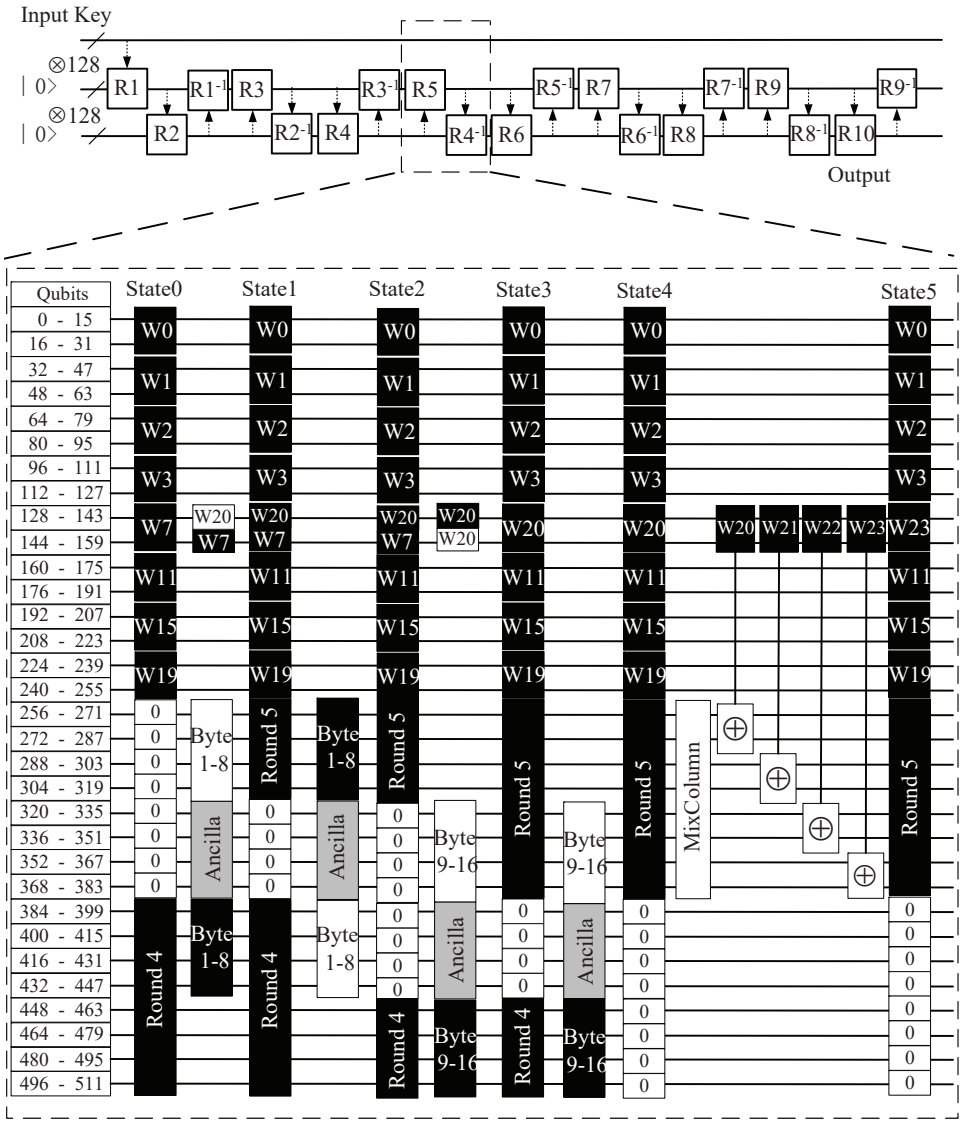

Fig. 3. Our method for computing Round 5 and removing Round 4 of AES-128.

Table 2. The number of quantum gates to implement each round of AES-128

	Operation	Toffoli Depth	# Toffoli	# CNOT	# NOT
Part 1	Obtain Round 1 and Remove Round 0	92	920	7952	337
Part 2	Obtain Round 2 and Remove Round 1	174	1968	14424	465
	Obtain Round 3 and Remove Round 2	218	1928	14432	465
	Obtain Round 4 and Remove Round 3	228	2012	14380	465
Part 3	Obtain Round 5 and Remove Round 4	262	2160	14388	465
	Obtain Round 6 and Remove Round 5	262	2160	14388	465
	Obtain Round 7 and Remove Round 6	262	2160	14388	465
	Obtain Round 8 and Remove Round 7	262	2160	14388	465
	Obtain Round 9 and Remove Round 8	262	2160	14388	468
	Obtain Round 10 and Remove Round 9	262	2160	13280	468
Sum	10 rounds	2284	19788	136408	4528

circuit of AES-192 requires 640 qubits, 22380 Toffoli gates, 162120 CNOT gates and 5128 NOT gates. The Toffoli depth of our quantum circuit implementation of AES-192 is 2252.

Table 3. The number of quantum gates to implement each round of AES-192

Operation	Toffoli Depth	# Toffoli	# CNOT	# NOT
Obtain Round 1 and Remove Round 0	92	920	7920	81
Obtain Round 2 and Remove Round 1	109	1744	13012	448
Obtain Round 3 and Remove Round 2	119	2080	14784	465
Obtain Round 4 and Remove Round 3	172	1928	14496	465
Obtain Round 5 and Remove Round 4	172	1744	13140	448
Obtain Round 6 and Remove Round 5	174	1968	14562	465
Obtain Round 7 and Remove Round 6	218	1928	14405	465
Obtain Round 8 and Remove Round 7	218	1928	14453	448
Obtain Round 9 and Remove Round 8	228	2012	14348	465
Obtain Round 10 and Remove Round 9	262	2160	14260	465
Obtain Round 11 and Remove Round 10	226	1808	13108	448
Obtain Round 12 and Remove Round 11	262	2160	13632	465
Sum of 12 rounds	2252	22380	162120	5128

2.3 Our Improved Quantum Circuit Implementations of AES-256

Since our quantum circuit implementation of AES-256 is similar to AES-128, we just show the result and omit the details. As shown in Table 4, our quantum circuit of AES-256 requires 768 qubits, 26774 Toffoli gates, 189013 CNOT gates and 6103 NOT gates. The Toffoli depth of our quantum circuit implementation of AES-256 is 2594.

Table 4. The number of quantum gates to implement each round of AES-256

Operation	Toffoli Depth	# Toffoli	# CNOT	# NOT
Obtain Round 1 and Remove Round 0	46	736	6468	64
Obtain Round 2 and Remove Round 1	109	1774	13028	465
Obtain Round 3 and Remove Round 2	109	1774	13028	464
Obtain Round 4 and Remove Round 3	109	1774	13220	465
Obtain Round 5 and Remove Round 4	119	2080	14560	464
Obtain Round 6 and Remove Round 5	172	1928	14464	465
Obtain Round 7 and Remove Round 6	174	1968	14424	464
Obtain Round 8 and Remove Round 7	218	1928	14437	465
Obtain Round 9 and Remove Round 8	228	2012	14412	464
Obtain Round 10 and Remove Round 9	262	2160	14420	465
Obtain Round 11 and Remove Round 10	262	2160	14420	464
Obtain Round 12 and Remove Round 11	262	2160	14420	465
Obtain Round 13 and Remove Round 12	262	2160	14420	464
Obtain Round 14 and Remove Round 13	262	2160	13312	465
Sum of 14 rounds	2594	26774	189013	6103