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

https://youtu.be/PneTVFnJ_oU

정보컴퓨터공학과 송경주

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Contribution

- Improved structure of S-box
  - 120개의 ancilla qubit과 T-depth 4로 S-box를 구현한 Huang et al.[1]의 연구결과를 개선함
  - mixing-XOR 기법을 사용하여 linear transformation 내에서 idle qubit를 식별하여 중간값 저장에 사용함
  - 해당 기법을 통해 depth와 qubit을 줄여 83개의 ancilla qubit와 T-depth 4로 AES S-box을 구현함

- Combination of S-box and S-box† (reverse of S-box)
  - 240개의 ancilla qubit을 사용한 shallowed pipeline 구조의 Jang et al.[2]의 연구결과를 개선함
  - combined pipeline 구조를 사용하여 ancilla qubit를 98개로 59% 감소시킴

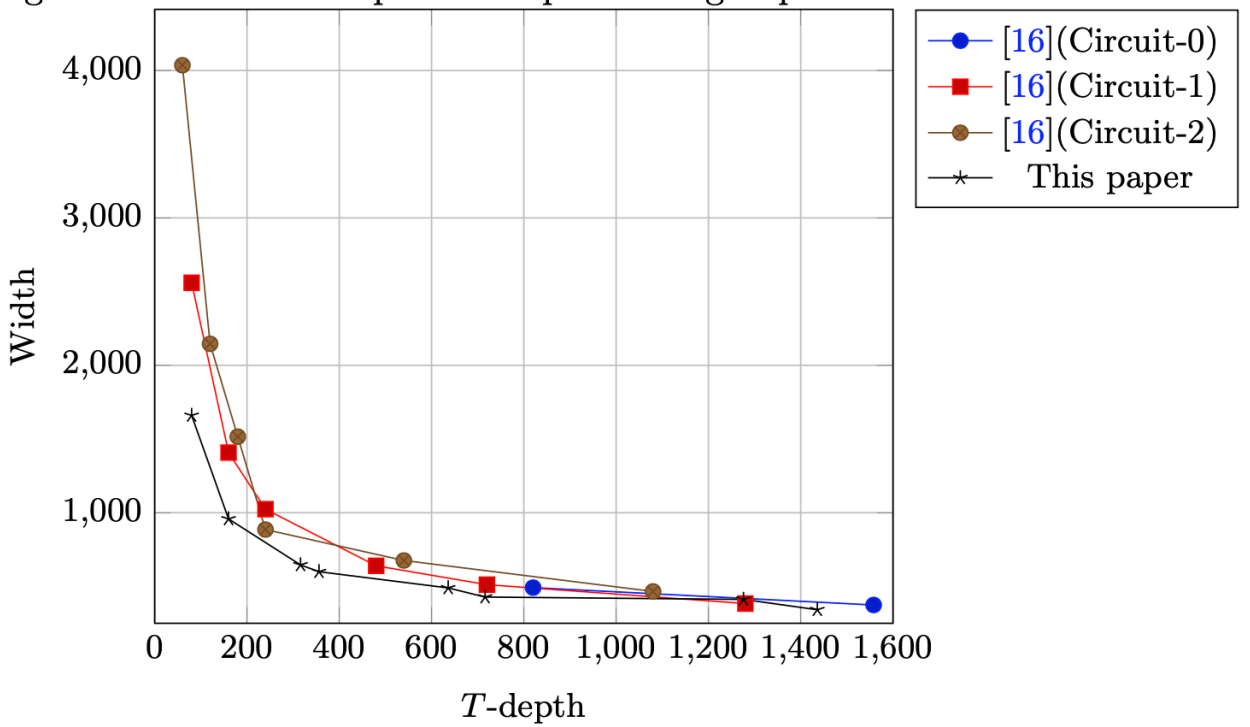
- Improved quantum circuit for reduced circuit complexity.
  - AES-128, AES-192, AES-256에 대해 깊이 730, 876, 1018 만을 가짐
  - Jang et al[2] 결과와 비교하여 큐비트 수 및 DW-cost가 AES-128, AES-192, AES-256에서 각각 42.4%, 41.2%, 36.5% 감소했다.

[1] Huang, Z., Sun, S.: Synthesizing quantum circuits of AES with lower T-depth and less qubits. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13793, pp. 614–644. Springer (2022), https://doi.org/10.1007/978-3-031-22969-5_21
[2] Jang, K., Baksi, A., Song, G., Kim, H., Seo, H., Chattopadhyay, A.: Quantum analysis of AES. IACR Cryptol. ePrint Arch. p. 683 (2022)

Contribution

- Introducing AND gates into the zig-zag architecture.
  - Huang et al.[1]이 ASIACRYPT 2022에서 소개한 양자회로를 수정함
  - 개선된 회로를 통해 양자회로 depth가 증가함에 따라 큐비트 수의 상당한 감소를 이룸
  - round-in-place zig-zag 구조를 적용하므로써 Huang et al 연구결과와 비교했을 때 DW-cost가 204,800에서 132,800으로 감소하였다.

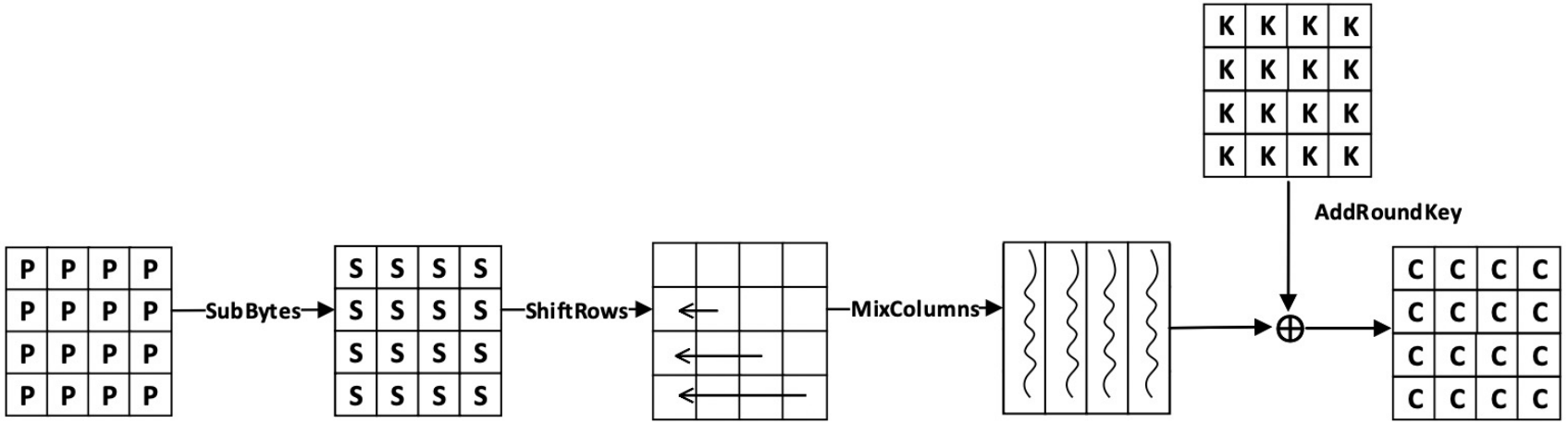
Fig. 1: Width and T-depth for implementing a quantum circuit for AES-128.



[1] Huang, Z., Sun, S.: Synthesizing quantum circuits of AES with lower T-depth and less qubits. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13793, pp. 614–644. Springer (2022), https://doi.org/10.1007/978-3-031-22969-5_21

AES (Advanced Encryption Standard)

- AES는 NIST에서 표준화 한 128-bit (16 bytes) state 의 블록암호
- AES family: AES-128(10 round, 128-bit key), AES-192(12 rounds, 192-bit key), AES-256 (14 rounds, 256-bit key)
- 연산: AddRoundKey ∘ MixColumns ∘ ShiftRows ∘ SubBytes



AES (Advanced Encryption Standard)

- **AddRoundKey**: 각 state에 대해 round key를 XOR함
- **ShiftRows**: i-th row ($i = 0,1,2,3$)에 대해 i만큼 왼쪽으로 shift 시킴
- **SubBytes**: 각 byte 크기의 state에 대해 8-bit S-box를 병렬로 수행함 (128bit의 state는 16개의 S-box lookup을 통해 변환됨)
- **MixColumns**: 특정 행렬을 사용하여 각 column에 대해 linear transformation 수행

(4×4 byte 상태의 state 행렬과 특정 행렬의 각 column에 대해 갈루아 필드 $GF(2^8)$ 상에서 곱셈 진행)

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

- **Key Schedule**: mater key: W_0, W_1 ... W_{s-1} (s: AES-128(4), AES-192(6), AES-256(8))
  - RotWord: 4byte에 대해 주기적으로 한 위치씩 왼쪽으로 회전
  - Rcon: word의 각 byte와 상수 XOR
  - SubWord: word의 4byte에 대해 4개의 S-box를 병렬로 적용

AES S-box quantum circuit

<AES S-box quantum circuit>

- Jaques et al.[1]가 제안한 S-box 는 120개의 ancilla qubit와 T-depth 6을 가진다.
- Huang et al.[2]에서 이를 개선하여 120개의 ancilla qubit와 T-depth 4를 가진다.

→ 위의 논문들의 결과를 개선하기 위해 mixing-XOR(m-XOR) 기술을 사용함

[1]Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing Grover oracles for quantum key search on AES and LowMC. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 280–310. Springer (2020)

AES S-box quantum circuit

<m-XOR Technique>

- creating operation이 포함된 양자회로를 updating operation으로 변환하여 일부 큐비트를 재사용
  - creating: a⊕b 결과를 큐비트 c에 저장(out-of-place)
  - updating: a⊕b 결과를 큐비트 b에 저장(in-place)

- m-XOR: 최소한의 큐비트 사용을 위해 updating operation과 creating operation mix

Ex) 두개의 큐비트 q_a, q_b에 대해 sub-operation이 creating operation: $q_c = q_c \oplus (q_a \oplus q_b)$일 때,
만약 q_a가 재사용되지 않는다면 updating operation: $q_a = q_a \oplus q_b$을 통해 q_a로 대체해서 사용할 수 있다.
: 다음과 같이 연산하기 위해서는 해당 조건을 만족해야 함.

1) q_a가 subsequent circuit 에서 사용되지 않아야 함
2) q_c가 이전 회로에서 사용되지 않아야 함 (0 상태여야 하므로)

→ idle qubit detection이 해당 기술의 핵심

Algorithm 1 Transformation from *creating* operations into *updating* operations

Input: A sequentially written quantum circuit $\mathcal{C}$ in sequence
Output: The optimized quantum circuit with a reduced number of qubits and gates, as well as less quantum depth

```
for each gate g ∈ C do
    if g is creating operation t_c = t_c ⊕ (t_a ⊕ t_b) then
        if t_c appears in the previous circuit then
            Continue
        end if
        Check the subsequent circuit and count the number n_a that t_a is used
        Check the subsequent circuit and count the number n_b that t_b is used
        if n_i = 0 (i = a or b) then
            Replace t_c with t_i in g and in the subsequent circuit
        end if
    end if
end for
return C
```

AES S-box quantum circuit

<AES S-box에 m-XOR Technique 적용>

[이전 AES S-box: m-XOR 적용 전]

- 연산: AND operation: 34개, creating operation: 120개, X gate: 4개
- 8-bit input $u_0, \dots, u_7$에 대해 8-bit output $s_0, \dots, s_7$
- S-box에서 120개의 ancilla qubit 사용: $t_0, \dots, t_{26}, m_0, \dots, m_{62}, l_0, \dots, l_{29}$

[이전 AES S-box에 m-XOR 적용]

- 46개의 필요 없는 큐비트 발견
- 74 ancilla qubits을 통해 S-box 최적화: $q_0, q_1 \dots, q_{73}$.
- 오른쪽 표: 74 ancilla qubits로 구현된 AES S-box
- Ex) line 2: 이전의 CNOT2(u_7, u_1, t_2)연산에 대해 CNOT(u_1, u_7)로 변경
  - ■u_7이 이후에 사용되지 않음

ancilla + input qubit

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

<Toffoli gate를 사용하여 구현한 S-box 자원 비교>

No.	Gate	No.	Gate	No.	Gate
0	CNOT2(u_7, u_4, q_0)	53	AND(q_{15}, q_9, q_{26})	106	CNOT(q_{25}, q_{63})
1	CNOT2(u_7, u_2, q_1)	54	AND(q_{61}, q_{21}, q_{32})	107	CNOT(q_{40}, q_{64})
2	CNOT(u_1, u_7)	55	AND(q_{16}, q_{60}, q_{35})	108	CNOT(q_{36}, q_{65})
3	CNOT2(u_4, u_2, q_2)	56	CNOT(q_{25}, q_{63})	109	CNOT(q_{21}, q_{66})
4	CNOT(u_1, u_3)	57	CNOT2(q_{16}, q_{26}, q_{27})	110	CNOT(q_{39}, q_{67})
5	CNOT2(q_0, u_3, q_3)	58	CNOT2(q_9, q_{16}, q_{28})	111	CNOT(q_{33}, q_{68})
6	CNOT2(u_6, u_5, q_4)	59	CNOT(q_{28}, q_{62})	112	CNOT(q_{16}, q_{69})
7	CNOT2(u_0, q_3, q_5)	60	CNOT2(q_{21}, q_{26}, q_{29})	113	CNOT(q_{38}, q_{70})
8	CNOT2(u_0, q_4, q_6)	61	CNOT2(q_{28}, q_{26}, q_{34})	114	CNOT(q_{41}, q_{71})
9	CNOT2(q_3, q_4, q_7)	62	AND(q_{29}, q_{28}, q_{30})	115	CNOT(q_{37}, q_{72})
10	CNOT(u_2, u_6)	63	AND(q_{27}, q_{25}, q_{31})	116	CNOT2(q_{57}, q_{58}, q_{60})
11	CNOT(u_2, u_5)	64	AND(q_{62}, q_{32}, q_{33})	117	CNOT2(q_{46}, q_{52}, q_{61})
12	CNOT2(u_7, q_2, q_8)	65	AND(q_{63}, q_{35}, q_{36})	118	CNOT2(q_{42}, q_{44}, q_{62})
13	CNOT2(q_3, u_6, q_9)	66	CNOT(q_{25}, q_{26})	119	CNOT2(q_{43}, q_{51}, q_{63})
14	CNOT(u_3, u_6)	67	CNOT(q_{30}, q_{16})	120	CNOT2(q_{50}, q_{54}, q_{64})
15	CNOT(u_5, u_3)	68	CNOT(q_{34}, q_{33})	121	CNOT2(q_{45}, q_{57}, q_{65})
16	CNOT2(q_6, u_3, q_{10})	69	CNOT(q_{31}, q_{21})	122	CNOT2(q_{58}, q_{65}, q_{66})
17	CNOT(u_0, u_4)	70	CNOT(q_{26}, q_{36})	123	CNOT2(q_{42}, q_{63}, q_{67})
18	CNOT(q_4, u_4)	71	CNOT2(q_{33}, q_{36}, q_{37})	124	CNOT2(q_{47}, q_{55}, q_{68})
19	CNOT2(q_0, u_4, q_{11})	72	CNOT2(q_{16}, q_{21}, q_{38})	125	CNOT2(q_{48}, q_{49}, q_{69})
20	CNOT(u_0, u_1)	73	CNOT2(q_{16}, q_{33}, q_{39})	126	CNOT2(q_{49}, q_{64}, q_{70})
21	CNOT(u_1, q_4)	74	CNOT2(q_{21}, q_{36}, q_{40})	127	CNOT2(q_{56}, q_{62}, q_{71})
22	CNOT2(q_1, q_4, q_{12})	75	CNOT2(q_{38}, q_{37}, q_{41})	128	CNOT2(q_{44}, q_{47}, q_{72})
23	CNOT2(q_1, q_7, q_{13})	76	CNOT(q_{40}, q_{64})	129	CNOT2(q_{66}, q_{70}, q_{73})
24	CNOT2(q_{11}, q_{10}, q_{14})	77	CNOT(q_{36}, q_{65})	130	CNOT(q_{60}, q_{46})
25	CNOT2(u_7, u_3, q_{15})	78	CNOT(q_{21}, q_{66})	131	CNOT(q_{57}, q_{48})
26	CNOT(q_0, u_5)	79	CNOT(q_{39}, q_{67})	132	CNOT(q_{61}, q_{51})
27	AND(q_8, q_3, q_{16})	80	CNOT(q_{33}, q_{68})	133	CNOT(q_{60}, q_{52})
28	AND(q_{12}, q_5, q_{17})	81	CNOT(q_{16}, q_{69})	134	CNOT(q_{61}, q_{53})
29	AND(u_4, u_0, q_{18})	82	CNOT(q_{38}, q_{70})	135	CNOT(q_{68}, q_{54})
30	AND(u_7, u_3, q_{19})	83	CNOT(q_{41}, q_{71})	136	CNOT(q_{64}, q_{59})
31	AND(q_4, q_6, q_{20})	84	CNOT(q_{37}, q_{72})	137	CNOT(q_{61}, q_{60})
32	AND(q_{11}, q_{10}, q_{21})	85	AND(q_{40}, q_3, q_{42})	138	CNOT2(q_{61}, q_{67}, s_4)
33	AND(q_0, u_6, q_{22})	86	AND(q_{36}, q_5, q_{43})	139	CNOT2(q_{63}, q_{72}, s_3)
34	AND(q_2, u_5, q_{23})	87	AND(q_{21}, u_0, q_{44})	140	CNOT2(q_{54}, q_{62}, s_0)
35	AND(q_1, q_7, q_{24})	88	AND(q_{39}, u_3, q_{45})	141	CNOT2(q_{51}, q_{69}, s_7)
36	CNOT(q_{16}, q_9)	89	AND(q_{33}, q_6, q_{46})	142	CNOT2(q_{67}, q_{69}, s_6)
37	CNOT(q_{18}, q_{16})	90	AND(q_{16}, q_{10}, q_{47})	143	CNOT2(q_{68}, q_{70}, s_1)
38	CNOT(q_{19}, q_{15})	91	AND(q_{38}, u_6, q_{48})	144	CNOT2(q_{71}, q_{48}, s_5)
39	CNOT(q_{19}, q_{21})	92	AND(q_{41}, u_5, q_{49})	145	CNOT2(q_{71}, q_{53}, s_2)
40	CNOT(q_{22}, q_{23})	93	AND(q_{37}, q_7, q_{50})	146	CNOT(q_{66}, s_7)
41	CNOT(q_{22}, q_{24})	94	AND(q_{64}, q_8, q_{51})	147	CNOT(q_{52}, s_6)
42	CNOT(q_{17}, q_9)	95	AND(q_{65}, q_{12}, q_{52})	148	CNOT(q_{59}, s_5)
43	CNOT(q_{13}, q_{16})	96	AND(q_{66}, u_4, q_{53})	149	X(s_6)
44	CNOT(q_{20}, q_{15})	97	AND(q_{67}, u_7, q_{54})	150	X(s_5)
45	CNOT(q_{24}, q_{21})	98	AND(q_{68}, q_4, q_{55})	151	CNOT(q_{66}, s_4)
46	CNOT(q_{23}, q_9)	99	AND(q_{69}, q_{11}, q_{56})	152	CNOT(q_{60}, s_3)
47	CNOT(q_{24}, q_{16})	100	AND(q_{70}, q_0, q_{57})	153	CNOT(q_{73}, s_2)
48	CNOT(q_{23}, q_{15})	101	AND(q_{71}, q_2, q_{58})	154	CNOT(q_{46}, s_1)
49	CNOT(q_{14}, q_{21})	102	AND(q_{72}, q_1, q_{59})	155	CNOT(q_{66}, s_0)
50	CNOT2(q_{15}, q_{21}, q_{25})	103	CNOT(q_{15}, q_{60})	156	X(s_1)
51	CNOT(q_{15}, q_{60})	104	CNOT(q_9, q_{61})	157	X(s_0)
52	CNOT(q_9, q_{61})	105	CNOT(q_{28}, q_{62})		

[16] Huang, Z., Sun, S.: Synthesizing quantum circuits of AES with lower T-depth and less qubits. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13793, pp. 614–644. Springer (2022), https://doi.org/10.1007/978-3-031-22969-5_21

[19] Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing Grover oracles for quantum key search on AES and LowMC. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 280–310. Springer (2

AES S-box quantum circuit

85 $\mathrm{AND}(q_{40}, q_3, q_{42})$
86 $\mathrm{AND}(q_{36}, q_5, q_{43})$
87 $\mathrm{AND}(q_{21}, u_0, q_{44})$
88 $\mathrm{AND}(q_{39}, u_3, q_{45})$
89 $\mathrm{AND}(q_{33}, q_6, q_{46})$
90 $\mathrm{AND}(q_{16}, q_{10}, q_{47})$
91 $\mathrm{AND}(q_{38}, u_6, q_{48})$
92 $\mathrm{AND}(q_{41}, u_5, q_{49})$
93 $\mathrm{AND}(q_{37}, q_7, q_{50})$
94 $\mathrm{AND}(q_{64}, q_8, q_{51})$
95 $\mathrm{AND}(q_{65}, q_{12}, q_{52})$
96 $\mathrm{AND}(q_{66}, u_4, q_{53})$
97 $\mathrm{AND}(q_{67}, u_7, q_{54})$
98 $\mathrm{AND}(q_{68}, q_4, q_{55})$
99 $\mathrm{AND}(q_{69}, q_{11}, q_{56})$
100 $\mathrm{AND}(q_{70}, q_0, q_{57})$
101 $\mathrm{AND}(q_{71}, q_2, q_{58})$
102 $\mathrm{AND}(q_{72}, q_1, q_{59})$

- 기존: 18개의 ancilla qubit 사용했음
- 16개의 parallel AND 게이트 후 → $q_{73}, s_0, s_1 \ldots s_7$ (9개) 큐비트가 0으로 설정됨을 발견
- 따라서 9개의 ancilla qubit만 사용 가능

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**

<AND gate를 사용하여 구현한 S-box 자원 비교>

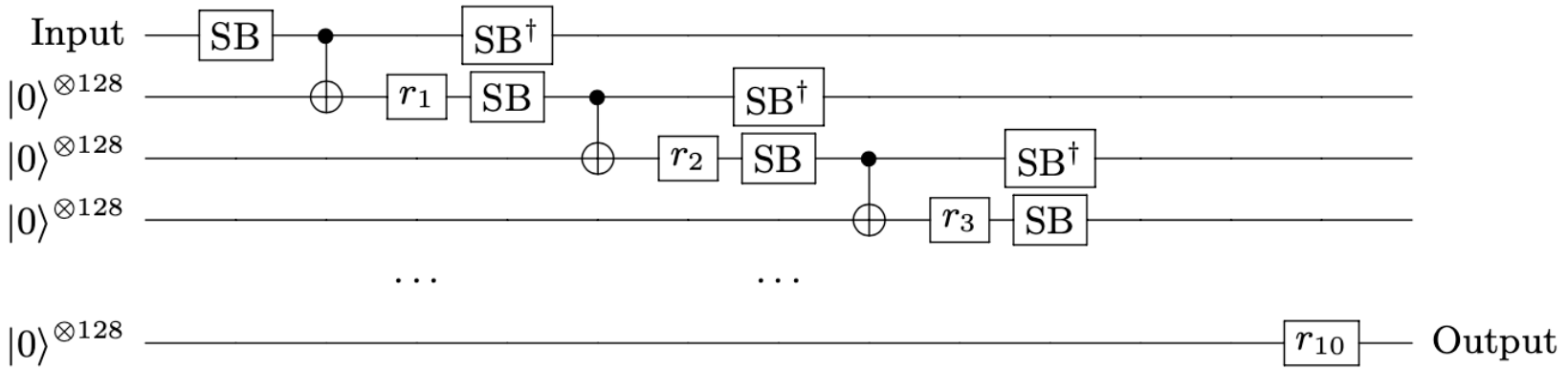
[19] Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing Grover oracles for quantum key search on AES and LowMC. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 280–310. Springer (2020)
[16] Huang, Z., Sun, S.: Synthesizing quantum circuits of AES with lower T-depth and less qubits. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology - ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5-9, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13793, pp. 614–644. Springer (2022), https://doi.org/10.1007/978-3-031-22969-5_21

AES S-box quantum circuit

- Improved Combination of S-box and S-box†
  - Jaques et al. : pipeline architecture AES
  - Jang et al. : shallowed pipeline architecture [120+120=240 ancilla qubit]
  - This paper: combined architecture [74+24=98 ancilla qubit] (combined pipeline architecture with share technique to combine the S-box and S-box†)

AES S-box quantum circuit

- Pipeline Architecture for AES



<Shallowed pipeline architecture>

- 첫번째 SB에서 사용한 120개의 ancilla qubit를 두번째 SB 동작과 동시에 첫번째 SB를 inverse하여 Depth를 증가시키지 않음과 동시에 사용한 ancilla qubit을 리셋 시켜 세번째 SB에서 사용할 수 있도록 하여 총 사용 큐비트 수를 줄임
- 즉, 홀수 S-box/ 짝수 S-box 는 같은 ancilla qubit을 clean up 해서 사용함 (2세트*120개의 ancilla qubit 사용)

AES S-box quantum circuit

- Combined pipeline S-box
  - 기존 기법에서는 S-box* 실행 중에 큐비트가 clean up 되며 이러한 큐비트는 S-box에서 바로 사용x → clean up 된 큐비트를 바로 사용할 수 있는 기법 **“share technique”**

  - **Original pipeline: S-box / S-box*+MixColumns**
  - **Shallowed pipeline: S-box+S-box* / MixColumns**
  - **Combined : S-box+S-box* (Combined) / MixColumn**

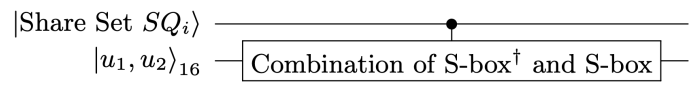


Fig. 5: Combined structure to execute S-box and S-box† simultaneously.

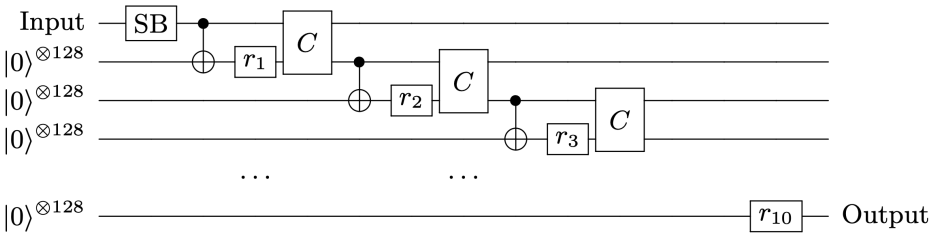


Fig. 6: The combined pipeline architecture, where C is the combined S-box and S-box†.

Table 5: Comparison of different pipeline architectures.

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	$(r+1)\cdot q_r + \max((1+\epsilon)\cdot q_s, q_m)$	$d_s + d_m$

Q & A