‘Optimized Quantum Implementation of AES’ 논문 리뷰

장경배

https://youtu.be/ZjJjR69UuXs

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Paper

Optimized Quantum Implementation of AES

Da Lin, Zejun Xiang*, Runqing Xu, Shasha Zhang
and Xiangyong Zeng

Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan, 430062, China.

- **23년, 2월 15일**

Contribution

- **AES 양자 회로 최적화** 논문
- **큐비트 수**를 줄이는 데 초점을 둠
- **새로운 S-box 구현** 제시 (Asiacrypt'20의 S-box 개선)
- **Toffoli depth X 큐비트 수** 비용이 가장 낮음

Overall

Table 1 The quantum resource of different NCT-based circuits for AES-128.

Source		#Qubits	Toffoli Depth	#Toffoli	#CNOT	#Pauli-X	$T \cdot M$
[10]		984	12672	151552	166548	1456	12469248
[1]		976	not reported	150528	192832	1370	not reported
[18]		864	1880	16940	107960	1570	1624320
[32]		512	2016	19788	128517	4528	1032192
[28]		656	not reported	18040	101174	1976	not reported
		400	not reported	19064	118980	4528	not reported
[13]*		492	820	17888	126016	2528	403440
		374	1558				582692
[14]◇		3936	76	12920	84120	800	299136
		6368	40	12240	81312		254720
This work	$m = 1$	269	7396	19608	77408	2224	1989524
	$m = 1^\dagger$	274	6480		78448		1775520
	$m = 2$	282	3720		77408		1049040
	$m = 2^\dagger$	287	3306		78416		948822
	$m = 3$	295	2622		77444		773490
	$m = 4$	308	1970		77408		606760
	$m = 4^\dagger$	313	1700		78272		532100
	$m = 5$	321	1736		77444		557256
	$m = 6$	334	1304		77552		435536
	$m = 7$	347	1304		77480		452488
	$m = 8$	360	1106		77408		398160
	$m = 8^\dagger$	365	908		77984		331420
	$m = 9$	373	872		77660		325256
	$m = 10$	386	872		77624		336592
	$m = 11$	399	872		77588		347928
	$m = 12$	412	872		77552		359264
	$m = 13$	425	872		77516		370600
	$m = 14$	438	872		77480		381936
	$m = 15$	451	872		77444		393272
	$m = 16$	464	674		77408		312736
	$m = 16^\dagger$	474	476		77984		225624

[32] Asiacrypt'20

[13] Asiacrypt'22

[14] 한성대

- m은 S-box 병렬화 개수

Overall

Table 1 The quantum resource of different NCT-based circuits for AES-128.

Source		#Qubits	Toffoli Depth	#Toffoli	#CNOT	#Pauli-X	$T \cdot M$
[10]		984	12672	151552	166548	1456	12469248
[1]		976	not reported	150528	192832	1370	not reported
[18]		864	1880	16940	107960	1570	1624320
[32]		512	2016	19788	128517	4528	1032192
[28]		656	not reported	18040	101174	1976	not reported
		400	not reported	19064	118980	4528	not reported
[13]*		492	820	17888	126016	2528	403440
		374	1558				582692
[14]◇		3936	76	12920	84120	800	299136
		6368	40	12240	81312		254720
This work	$m = 1$	269	7396	19608	77408	2224	1989524
	$m = 1^\dagger$	274	6480		78448		1775520
	$m = 2$	282	3720		77408		1049040
	$m = 2^\dagger$	287	3306		78416		948822
	$m = 3$	295	2622		77444		773490
	$m = 4$	308	1970		77408		606760
	$m = 4^\dagger$	313	1700		78272		532100
	$m = 5$	321	1736		77444		557256
	$m = 6$	334	1304		77552		435536
	$m = 7$	347	1304		77480		452488
	$m = 8$	360	1106		77408		398160
	$m = 8^\dagger$	365	908		77984		331420
	$m = 9$	373	872		77660		325256
	$m = 10$	386	872		77624		336592
	$m = 11$	399	872		77588		347928
	$m = 12$	412	872		77552		359264
	$m = 13$	425	872		77516		370600
	$m = 14$	438	872		77480		381936
	$m = 15$	451	872		77444		393272
	$m = 16$	464	674		77408		312736
	$m = 16^\dagger$	474	476		77984		225624

- Asiacrypt'22와 이번 논문 둘 다 **큐비트 수를 적게 사용**
- 하지만 이번 논문에서 **Toffoli depth**를 더 줄임
  → **S-box 변경의 영향이 큼**

Overall

Table 1 The quantum resource of different NCT-based circuits for AES-128.

Source		#Qubits	Toffoli Depth	#Toffoli	#CNOT	#Pauli-X	$T \cdot M$
[10]		984	12672	151552	166548	1456	12469248
[1]		976	not reported	150528	192832	1370	not reported
[18]		864	1880	16940	107960	1570	1624320
[32]		512	2016	19788	128517	4528	1032192
[28]		656	not reported	18040	101174	1976	not reported
		400	not reported	19064	118980	4528	not reported
[13]*		492	820	17888	126016	2528	403440
		374	1558				582692
[14]◇		3936	76	12920	84120	800	299136
		6368	40	12240	81312		254720
This work	$m = 1$	269	7396	19608	77408	2224	1989524
	$m = 1^\dagger$	274	6480		78448		1775520
	$m = 2$	282	3720		77408		1049040
	$m = 2^\dagger$	287	3306		78416		948822
	$m = 3$	295	2622		77444		773490
	$m = 4$	308	1970		77408		606760
	$m = 4^\dagger$	313	1700		78272		532100
	$m = 5$	321	1736		77444		557256
	$m = 6$	334	1304		77552		435536
	$m = 7$	347	1304		77480		452488
	$m = 8$	360	1106		77408		398160
	$m = 8^\dagger$	365	908		77984		331420
	$m = 9$	373	872		77660		325256
	$m = 10$	386	872		77624		336592
	$m = 11$	399	872		77588		347928
	$m = 12$	412	872		77552		359264
	$m = 13$	425	872		77516		370600
	$m = 14$	438	872		77480		381936
	$m = 15$	451	872		77444		393272
	$m = 16$	464	674		77408		312736
	$m = 16^\dagger$	474	476		77984		225624

- **Toffoli, Full depth 최소화,**
  대신 **많은 큐비트 수 허용**

Quantum circuits for S-box

- S-box 양자 회로 구현들에 대한 성능 비교

Table 7 The comparison of different NCT-based circuits for outputs are $|0\rangle^{\otimes 8}$.

Operation	Source	#Qubits	#Toffoli	#CNOT	#Pauli-X	Toffoli Depth
S-box	[18]	16	55	314	4	40
	[28]	16	55	322	4	40
	[15]	120	34	186	4	6
	[32]	6	52	326	4	41
		7	48	330	4	39
		8	46	332	4	37
	[13]	120	34	212	4	4
		202	78	355	4	3
	This work	5	57	193	4	24
		6	57	195	4	22
S-box^{-1}	[13]	6	52	368	8	41
	This work	5	58	187	10	26*
		5	57	205	8	24†
		6	57	207	8	22†

- Asiacrypto'20의 S-box 구현을 개선
  → **큐비트 수를 적게 사용**, 하지만 **Toffoli depth 감소**

Quantum circuits for S-box

- S-box 양자 회로 구현들에 대한 성능 비교

Table 7 The comparison of different NCT-based circuits for outputs are $|0\rangle^{\otimes 8}$.

Operation	Source	#Qubits	#Toffoli	#CNOT	#Pauli-X	Toffoli Depth
S-box	[18]	16	55	314	4	40
	[28]	16	55	322	4	40
	[15]	120	34	186	4	6
	[32]	6	52	326	4	41
		7	48	330	4	39
		8	46	332	4	37
	[13]	120	34	212	4	4
		202	78	355	4	3
	This work	5	57	193	4	24
		6	57	195	4	22
S-box^{-1}	[13]	6	52	368	8	41
	This work	5	58	187	10	26*
		5	57	205	8	24†
		6	57	207	8	22†

- Asiacrypt'22 [13] 의 S-box보다 무조건 좋다고 평가할 수는 없음
  - 하지만 Toffoli depth X 큐비트 수 성능이 많이 차이나는 이유는
    회로 아키텍처 선택의 차이 → [13]의 S-box 특성 상, **Zig-zag 아키텍처는 적합하지 않음.**

Proposed Quantum Circuit of AES

- **S-box^{-1}**를 활용한 **큐비트 수 감소** (Aisacrypt'20, 21과 동일)

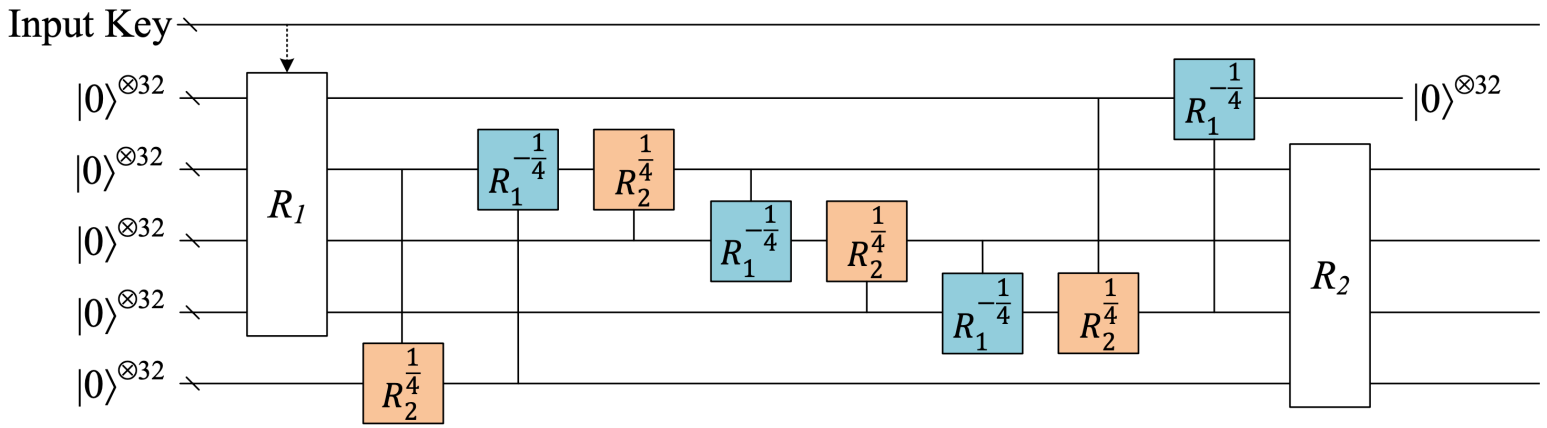

Fig. 3 The procedure for the **SubBytes** when $m = 4$.

Proposed Quantum Circuit of AES

- AES 양자 회로 첫 번째 라운드 : **Key Whitening 최적화**
  → Known-plaintext에 대한 **128-qubit 절약**

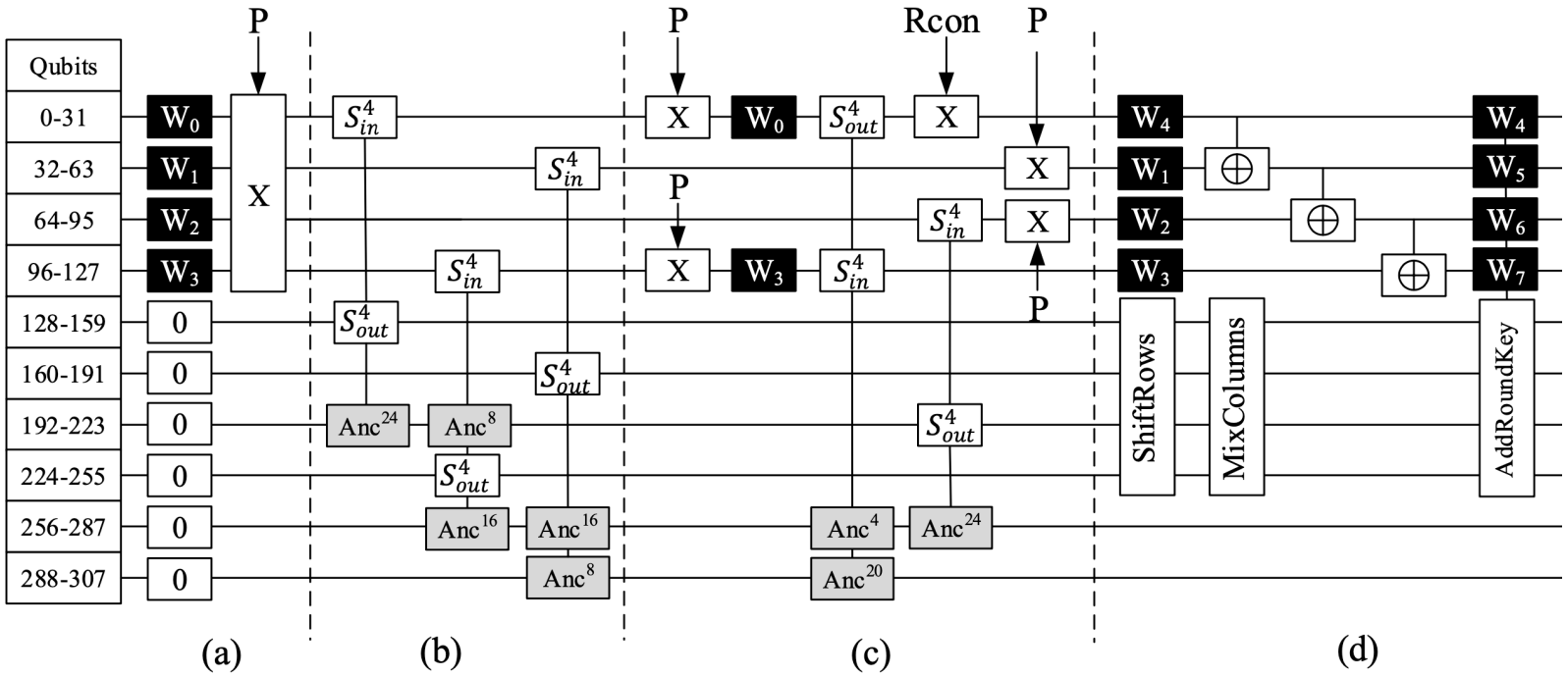

Fig. 5 The quantum circuit for the first round of AES-128. $(m = 4)$

Proposed Quantum Circuit of AES

- 이후 라운드들에 대한 AES 양자 회로

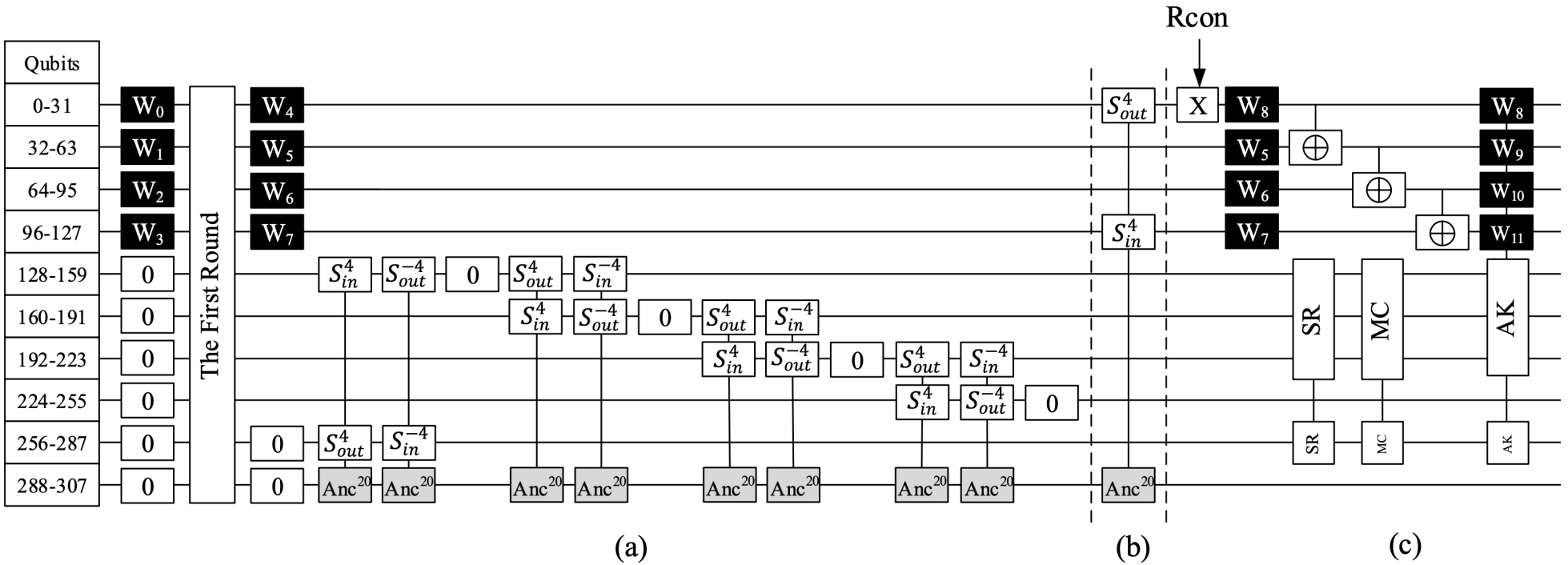

Fig. 6 The quantum circuit for the second round of AES-128. $(m = 4)$

Conclusion

- 최적화 metric
  - 큐비트 X Full depth
  - 큐비트 X Toffoli depth
    - 390656 (한성대)
    - 388892 (리뷰 논문)
  - 양자 게이트 수 X Full depth (양자 공격 비용)

- 큐비트 X Toffoli depth^2
  - 21876736 (한성대)
  - 251224232 (리뷰 논문)

							Toffoli depth		큐비트 X Toffoli depth ^{2}
256	GLRS [24]		233836	1943	215040	14976	1336	20007936	130929	299638849536
	LPS [39]		151011	1992	23760	2160	1232	2661120	33525	5748019200
	ZWSLW [57]		177645	6103	26774	2292	768	1760256	·	4034506752
	☆		117704	1103	18088	108	4576	494208	1907	53374464
	◎	✿	113744	1103	17408	56	6976	390656	1377	21876736
	◈		127472	1103	17408	56	8640	483840	1118	27095040
	☆		193248	1103	41496	81	5816	471096	1826	38158776
	◎	❀	186448	1103	39936	42	9456	397152	1335	16680384
	◈		200176	1103	39936	42	11120	467040	1076	19615680

- 큐비트 X Full depth^2

Table 3 The quantum resource of different NCT-based circuits for AES-256.

Source		#Qubits	Toffoli Depth	#Toffoli	#CNOT	#Pauli-X	$T \cdot M$
[10]		1336	14976	215040	233836	1943	20007936
[18]		1232	2160	23760	151011	1992	2661120
[32]		768	2292	26774	177645	6103	1760256
[14]$^\diamond$		4576	108	18088	117704	1103	494208
		6976	56	17408	113744		390656
This work	$m = 1$	397	10622	27816	109856	3069	4216934
	$m = 1^\dagger$	402	9322		111416		3747444
	$m = 2$	410	5324		109830		2182840
	$m = 2^\dagger$	415	4724		111312		1960460
	$m = 3$	423	3736		109908		1580328
	$m = 4$	436	2826		109856		1232136
	$m = 4^\dagger$	441	2436		111104		1074276
	$m = 5$	449	2488		109908		1117112
	$m = 6$	462	1864		110064		861168
	$m = 7$	475	1844		109920		875900
	$m = 8$	488	1556		109856		759328
	$m = 8^\dagger$	493	1270		110688		626110
	$m = 9$	501	1218		110220		610218
	$m = 10$	514	1218		110168		626052
	$m = 11$	527	1218		110116		641886
	$m = 12$	540	1218		110064		657720
	$m = 13$	553	1218		110012		673554
	$m = 14$	566	1218		109960		689388
	$m = 15$	579	1218		109908		705222
	$m = 16$	592	932		109856		551744
	$m = 16^\dagger$	602	646		110688		388892

Thank you!