Eurocrypt 구현 버그 수정

장경배

https://youtu.be/M2M-9twOg3k

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Eurocrypt AES Implementation

- **Eurocrypt 논문에서 추정한 자원들과 구현 기법, Q# 소스 코드에 대한 분석**을 **상호 비교**

operation	#CNOT	#1qCliff	#T	#M	T-depth	full depth	width
[GLRS16] S-box	8683	1028	3584	0	217	1692	44
[BP10] S-box	818	264	164	41	35	497	41
[BP12] S-box	654	184	136	34	6	101	137

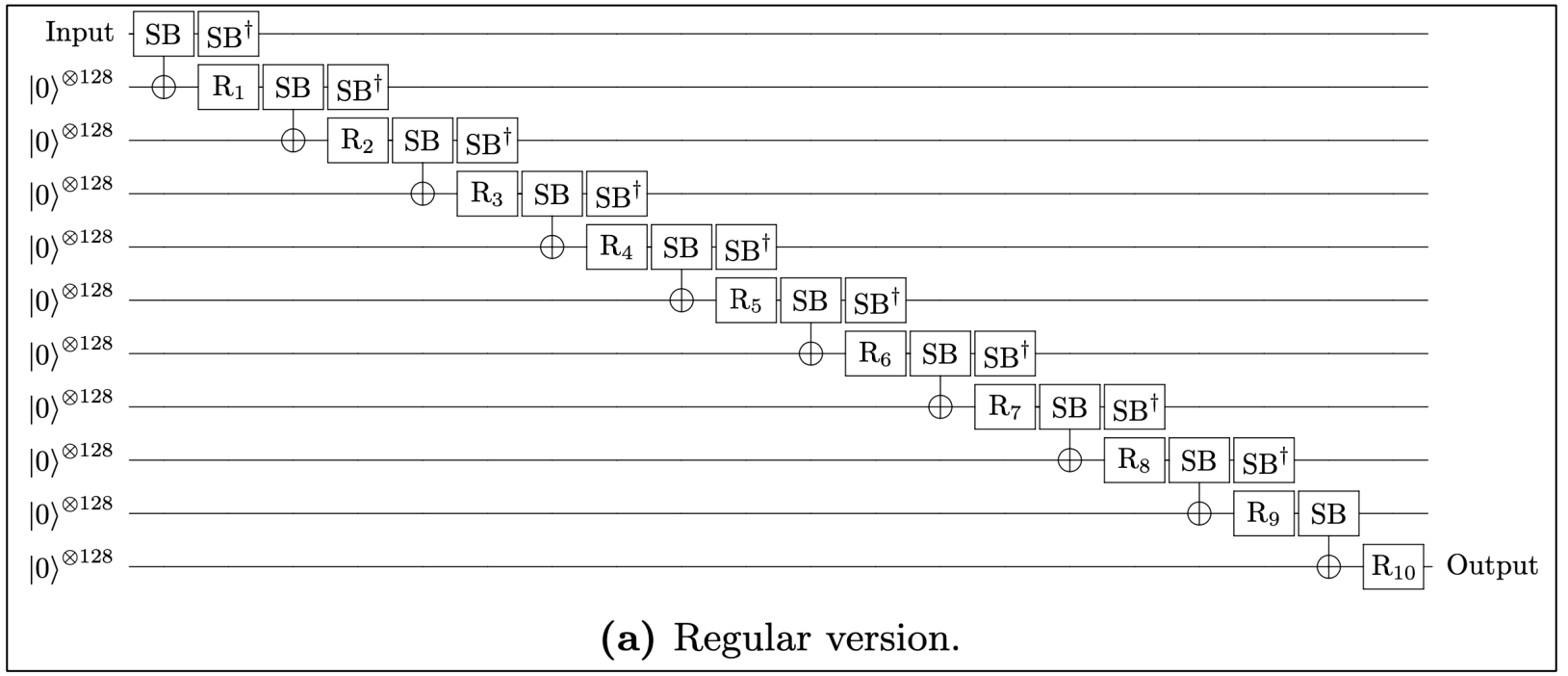
< S-box에 사용되는 양자 자원들(Eurocrypt) >

operation	#CNOT	#1qCliff	#T	#M	T-depth	full depth	width
AES-128 oracle (IP MC, $r = 1$)	292313	84428	54908	13727	121	2816	1665
AES-192 oracle (IP MC, $r = 1$)	329697	94316	61436	15359	120	2978	1985
AES-256 oracle (IP MC, $r = 1$)	404139	116286	75580	18895	126	3353	2305

< AES 양자 회로 oracle 비용 (Eurocrypt) >

Non-parallelizable SubBytes

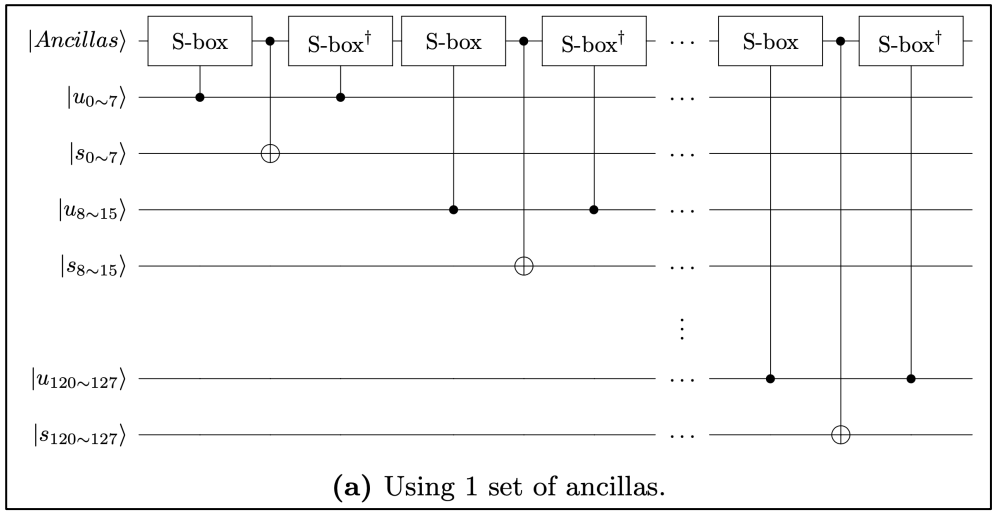
- **Plaintext & Key** : 256 Qubits
- **SubBytes 출력** : 1280 Qubits
- **SBox Ancilla Qubits** : 120 Qubits
- **현재 까지, 총 1,656 Qubits**
- **SubBytes에 대한 Ancilla Qubits 한 세트만을 사용**



(a) Regular version.

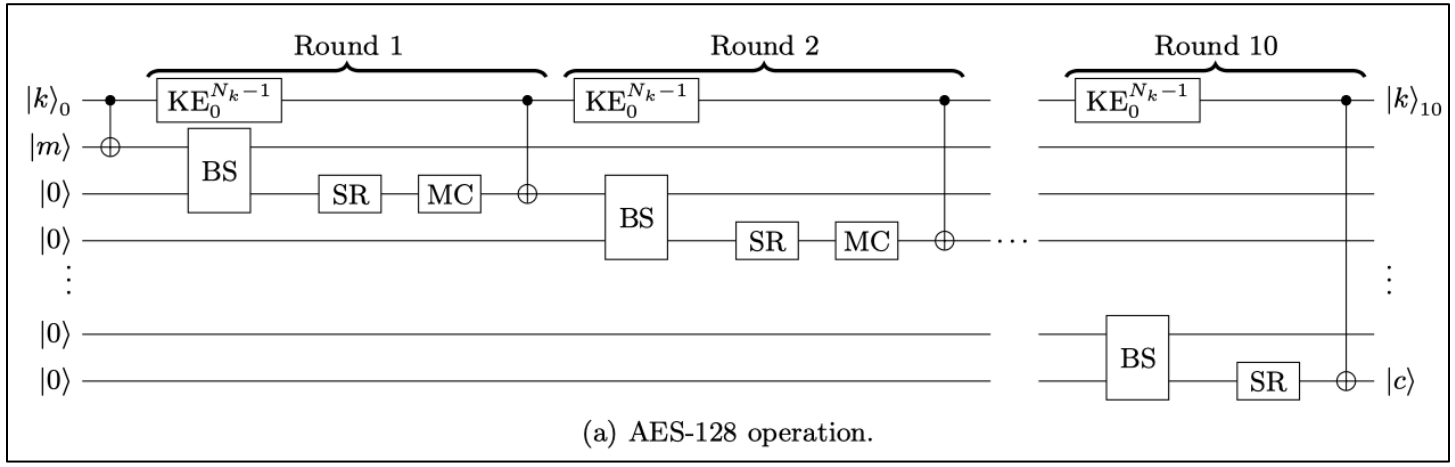
Non-parallelizable SubBytes

- **하나의 Ancilla 세트(120 Qubits)만을 사용하는 방식의 회로 구조**
  - 순차적인 Sbox 실행이 강요되지만, **모든 Sbox들이 병렬로 동작하는 Full Depth가 추정**되고 있음.



(a) Using 1 set of ancillas.

Non-parallelizable SubBytes



(a) AES-128 operation.

2,816

operation	#CNOT	#1qCliff	#T	#M	T-depth	full depth	width
AES-128 oracle (IP MC, $r = 1$)	292313	84428	54908	13727	121	2816	1665

101 X 10 = 1,010

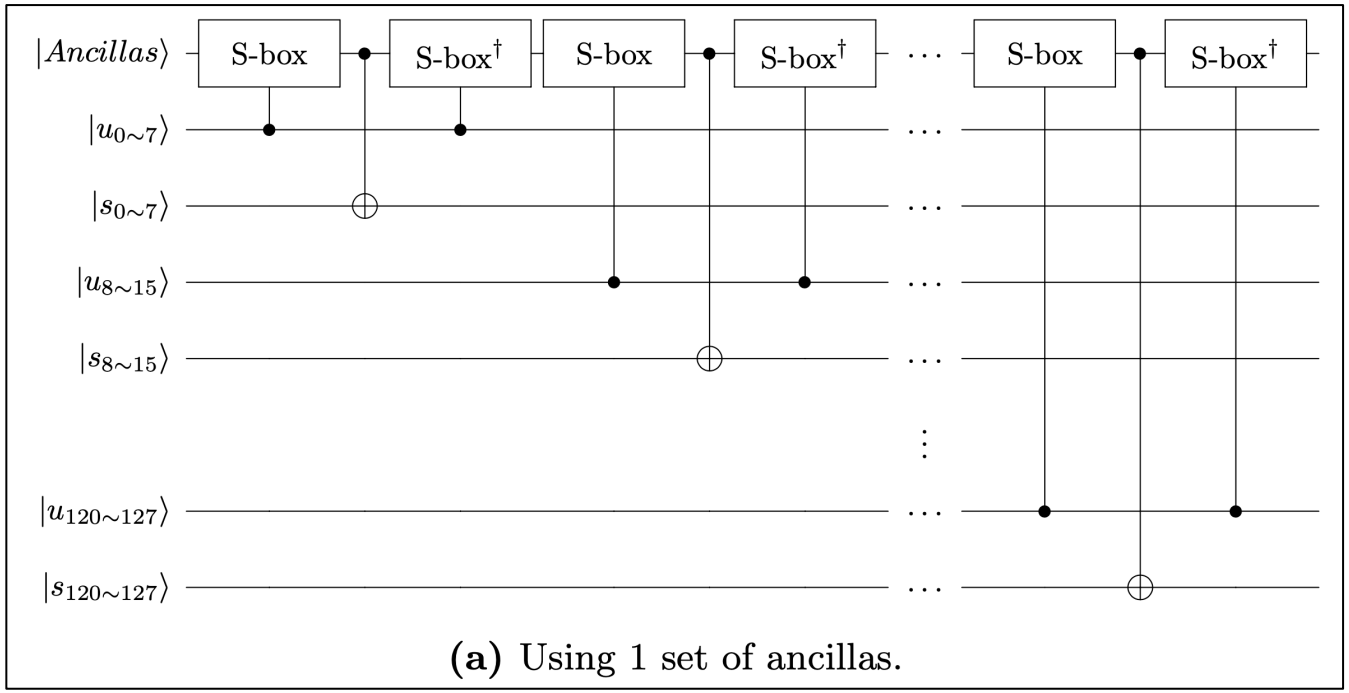
operation	#CNOT	#1qCliff	#T	#M	T-depth	full depth	width
[GLRS16] S-box	8683	1028	3584	0	217	1692	44
[BP10] S-box	818	264	164	41	35	497	41
[BP12] S-box	654	184	136	34	6	101	137

111 X 10 = 1,110

operation	#CNOT	#1qCliff	#T	#M	T-depth	full depth	width
In-place MixColumn	1108	0	0	0	0	111	128
[Max19] MixColumn	1248	0	0	0	0	22	318

Uninitialized Ancilla Qubits in SubBytes

- **Ancilla 세트를 초기화 (Clean qubits) 하는 reverse 연산 생략**
  - Ancilla Qubits은 S-box 동작 후, **여전히 output을 생성하는데 계산된 temp 값들을 가지고 있는 상태**임
  - Ancilla 세트를 **재사용**하기 위해서는, **reverse 연산을 수행하여 0 상태의 Qubits으로 만들어주어야 함**
  - **Eurocrypt에서는 reverse 연산(Clean Qubits)를 생략하고 Ancilla set을 재사용**
    - reverse 연산을 생략하고 **0xffffffff** 에 대한 Output을 생성해 본 결과, **0x6a4e6216** 생성
    - **첫번째 Sbox를 제외하고 잘못된 Output 생성**



(a) Using 1 set of ancillas.

Corrected Report

- **배치된 Qubits에 따른 올바른 Output를 생성하도록** 수정, **이 때의 Depth를 추정**
  - **Reverse 연산 추가, 순차적인 Sbox 실행에 대한 Depth**를 **ProejctQ**에서 추정

Table 3: Quantum resources required for SubBytes implementation.

Method	#CNOT	#1qCliff	#T	Toffoli depth	#qubits	Full depth
SubBytes	12,000	2,240	7,328	12	2,176	167

Table 6: Corrected..

Method	#CNOT	#1qCliff	#T	Toffoli depth	#qubits	Full depth
SubBytes	12,000	1,220	7,328	192	376	2,672
SubWord						
Key schedule						
MixColumns						
One round						

Corrected Report

- **조금 더 분석해 본 결과, AES Full 회로에 대한 자원 추정이 이상함**
  - **병렬화를 감안하고 계산을 해도 이해할 수 없는 depth가 보고됨**

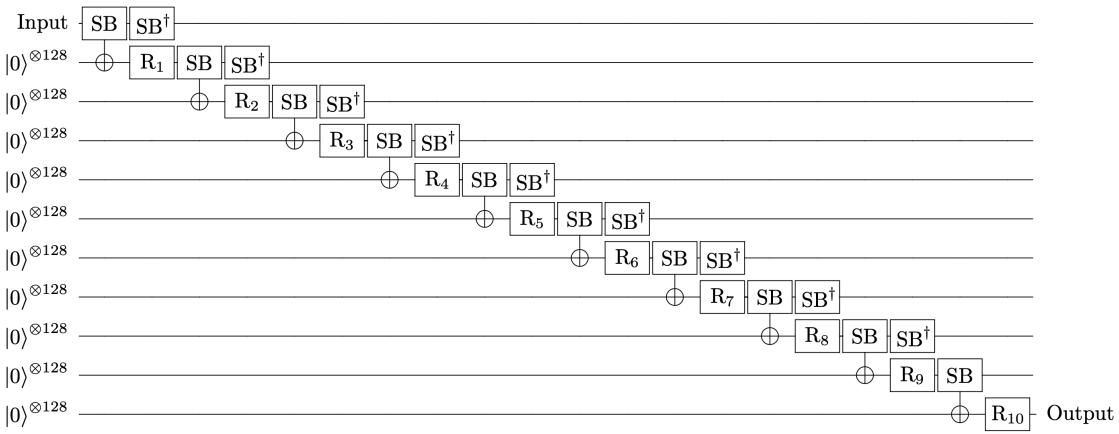


Table 1. Summary of the quantum resources to implement AES

Algorithm	# qubits	Toffoli depth	# Toffoli	# CNOT	# NOT	$T \cdot M$	Source
AES-128	984	12672	151552	166548	1456	12469248	[11]
	976	not reported	150528	192832	1370	not reported	[3]
	864	1880	16940	107960	1570	1624320	[18]
	512	2016	19788	128517	4528	1032192	Sect. 6.1
AES-192	1112	11088	172032	189432	1608	12329856	[11]
	896	1640	19580	125580	1692	1469440	[18]
	640	2022	22380	152378	5128	1294080	Sect. 6.2
AES-256	1336	14976	215040	233836	1943	20007936	[11]
	1232	2160	23760	151011	1992	2661120	[18]
	768	2292	26774	177645	6103	1760256	Sect. 6.2

operation	#CNOT	#1qCliff	#T	#M	T-depth	full depth	width
AES-128 (in-place MC)	291150	83116	54400	13600	120	2827	1785
AES-192 (in-place MC)	328612	93160	60928	15232	120	2987	2105
AES-256 (in-place MC)	402878	114778	75072	18768	126	3353	2425
AES-128 (Maximov's MC)	293730	83236	54400	13600	120	2094	2937
AES-192 (Maximov's MC)	331752	93280	60928	15232	120	1879	3513
AES-256 (Maximov's MC)	406288	114318	75072	18768	126	1955	4089

operation	#CNOT	#1qCliff	#T	#M	T-depth	full depth	width
[GLRS16] S-box	8683	1028	3584	0	217	1692	44
[BP10] S-box	818	264	164	41	35	497	41
[BP12] S-box	654	184	136	34	6	101	137

operation	#CNOT	#1qCliff	#T	#M	T-depth	full depth	width
In-place MixColumn	1108	0	0	0	0	111	128
[Max19] MixColumn	1248	0	0	0	0	22	318

AES-192 → (101 x 12 Rounds) x 2 = 2,424

AES-192 → (101 x 14 Rounds) x 2 = 2,828

Corrected Report

Table 6: Corrected..

Method	#CNOT	#1qCliff	#T	Toffoli depth	#qubits	Full depth
SubBytes	12,000	1,220	7,328	192	376	2,672
SubWord						
Key schedule						
MixColumns						
One round						

Table 7: Corrected..

Method	#CNOT	#1qCliff	#T	Toffoli depth	#qubits	Full depth
AES-128						
AES-192						
AES-256						

감사합니다