ARIA 양자회로 구현

https://youtu.be/PcI97yxT-IU

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

S-box

$$S_1(\alpha) := \mathbf{A}.\alpha^{-1} + \mathbf{a}$$

$$\mathbf{A} = \begin{bmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{bmatrix} \text{ and } \mathbf{a} = \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix}$$

$$S_1^{-1}(\alpha) := (\mathbf{A}^{-1}.(\alpha + \mathbf{a}))^{-1}$$

$$\mathbf{A}^{-1} = \begin{bmatrix} 0&0&1&0&0&1&0&1\\ 1&0&0&1&0&0&1&0\\ 0&1&0&0&1&0&0&1\\ 1&0&1&0&0&1&0&0\\ 0&1&0&1&0&0&1&0\\ 0&0&1&0&1&0&0&1\\ 1&0&0&1&0&1&0&0\\ 0&1&0&0&1&0&1&0 \end{bmatrix} \text{ and } \mathbf{a} = \begin{bmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{bmatrix}$$

AES와 동일

$$S_2(\alpha) := \mathbf{B}.\alpha^{247} + \mathbf{b}$$

$$S_2(\alpha) := \mathbf{B}.(\alpha^{-1})^8 + \mathbf{b} = \mathbf{B}.\mathbf{C}.\alpha^{-1} + \mathbf{b}$$

$$= \mathbf{D}.\alpha^{-1} + \mathbf{b}$$

$$\mathbf{D} = \begin{bmatrix} 0&1&0&1&0&1&1&1\\ 0&0&1&1&1&1&1&1\\ 1&1&1&0&1&1&0&1\\ 1&1&0&0&0&0&1&1\\ 0&1&0&0&0&0&1&1\\ 1&1&0&0&1&1&1&0\\ 0&1&1&0&0&0&1&1\\ 1&1&1&1&0&1&1&0 \end{bmatrix} \text{ and } \mathbf{b} = \begin{bmatrix} 0\\1\\0\\0\\0\\1\\1\\1 \end{bmatrix}$$

$$S_2^{-1}(\alpha) = (\mathbf{D}^{-1}.(\alpha + \mathbf{b}))^{-1}$$

$$\mathbf{D}^{-1} = \begin{bmatrix} 0&0&0&1&1&0&0&0\\ 0&0&1&0&0&1&1&0\\ 0&0&0&0&1&0&1&0\\ 1&1&1&0&0&0&1&1\\ 1&1&1&0&1&1&0&0\\ 0&1&1&0&1&0&1&1\\ 1&0&1&1&1&1&0&1\\ 1&0&0&1&0&0&1&1 \end{bmatrix} \text{ and } \mathbf{b} = \begin{bmatrix} 0\\1\\0\\0\\0\\1\\1\\1 \end{bmatrix}$$

S-box

- S-box (S_1)
  - Boyar and Peralta
    - Bit-slicing 기법을 AES S-box에 적용
    - $S(x) = A \cdot x^{-1} + [11000110]^T = B \cdot F(U \cdot x) + [11000110]^T$
    - 3단계로 구성 → **Top linear Layer (U), a middle non–linear Layer, bottom linear layer (B)**

Top Linear Part:

$T_1 = U_0 + U_3$	$T_2 = U_0 + U_5$	$T_3 = U_0 + U_6$	$T_4 = U_3 + U_5$	$T_5 = U_4 + U_6$
$T_6 = T_1 + T_5$	$T_7 = U_1 + U_2$	$T_8 = U_7 + T_6$	$T_9 = U_7 + T_7$	$T_{10} = T_6 + T_7$
$T_{11} = U_1 + U_5$	$T_{12} = U_2 + U_5$	$T_{13} = T_3 + T_4$	$T_{14} = T_6 + T_{11}$	$T_{15} = T_5 + T_{11}$
$T_{16} = T_5 + T_{12}$	$T_{17} = T_9 + T_{16}$	$T_{18} = U_3 + U_7$	$T_{19} = T_7 + T_{18}$	$T_{20} = T_1 + T_{19}$
$T_{21} = U_6 + U_7$	$T_{22} = T_7 + T_{21}$	$T_{23} = T_2 + T_{22}$	$T_{24} = T_2 + T_{10}$	$T_{25} = T_{20} + T_{17}$
$T_{26} = T_3 + T_{16}$	$T_{27} = T_1 + T_{12}$			

Nonlinear Part:

$M_1 = T_{13} \cdot T_6$	$M_2 = T_{23} \cdot T_8$	$M_3 = T_{14} + M_1$	$M_4 = T_{19} \cdot U_7$	$M_5 = M_4 + M_1$
$M_6 = T_3 \cdot T_{16}$	$M_7 = T_{22} \cdot T_9$	$M_8 = T_{26} + M_6$	$M_9 = T_{20} \cdot T_{17}$	$M_{10} = M_9 + M_6$
$M_{11} = T_1 \cdot T_{15}$	$M_{12} = T_4 \cdot T_{27}$	$M_{13} = M_{12} + M_{11}$	$M_{14} = T_2 \cdot T_{10}$	$M_{15} = M_{14} + M_{11}$
$M_{16} = M_3 + M_2$	$M_{17} = M_5 + T_{24}$	$M_{18} = M_8 + M_7$	$M_{19} = M_{10} + M_{15}$	$M_{20} = M_{16} + M_{13}$
$M_{21} = M_{17} + M_{15}$	$M_{22} = M_{18} + M_{13}$	$M_{23} = M_{19} + T_{25}$	$M_{24} = M_{22} + M_{23}$	$M_{25} = M_{22} \cdot M_{20}$
$M_{26} = M_{21} + M_{25}$	$M_{27} = M_{20} + M_{21}$	$M_{28} = M_{23} + M_{25}$	$M_{29} = M_{28} \cdot M_{27}$	$M_{30} = M_{26} \cdot M_{24}$
$M_{31} = M_{20} \cdot M_{23}$	$M_{32} = M_{27} \cdot M_{31}$	$M_{33} = M_{27} + M_{25}$	$M_{34} = M_{21} \cdot M_{22}$	$M_{35} = M_{24} \cdot M_{34}$
$M_{36} = M_{24} + M_{25}$	$M_{37} = M_{21} + M_{29}$	$M_{38} = M_{32} + M_{33}$	$M_{39} = M_{23} + M_{30}$	$M_{40} = M_{35} + M_{36}$
$M_{41} = M_{38} + M_{40}$	$M_{42} = M_{37} + M_{39}$	$M_{43} = M_{37} + M_{38}$	$M_{44} = M_{39} + M_{40}$	$M_{45} = M_{42} + M_{41}$
$M_{46} = M_{44} \cdot T_6$	$M_{47} = M_{40} \cdot T_8$	$M_{48} = M_{39} \cdot U_7$	$M_{49} = M_{43} \cdot T_{16}$	$M_{50} = M_{38} \cdot T_9$
$M_{51} = M_{37} \cdot T_{17}$	$M_{52} = M_{42} \cdot T_{15}$	$M_{53} = M_{45} \cdot T_{27}$	$M_{54} = M_{41} \cdot T_{10}$	$M_{55} = M_{44} \cdot T_{13}$
$M_{56} = M_{40} \cdot T_{23}$	$M_{57} = M_{39} \cdot T_{19}$	$M_{58} = M_{43} \cdot T_3$	$M_{59} = M_{38} \cdot T_{22}$	$M_{60} = M_{37} \cdot T_{20}$
$M_{61} = M_{42} \cdot T_1$	$M_{62} = M_{45} \cdot T_4$	$M_{63} = M_{41} \cdot T_2$		

Bottom Linear Part:

$L_0 = M_{61} \oplus M_{62}$	$L_1 = M_{50} \oplus M_{56}$	$L_2 = M_{46} \oplus M_{48}$	$L_3 = M_{47} \oplus M_{55}$	$L_4 = M_{54} \oplus M_{58}$
$L_5 = M_{49} \oplus M_{61}$	$L_6 = M_{62} \oplus L_5$	$L_7 = M_{46} \oplus L_3$	$L_8 = M_{51} \oplus M_{59}$	$L_9 = M_{52} \oplus M_{53}$
$L_{10} = M_{53} \oplus L_4$	$L_{11} = M_{60} \oplus L_2$	$L_{12} = M_{48} \oplus M_{51}$	$L_{13} = M_{50} \oplus L_0$	$L_{14} = M_{52} \oplus M_{61}$
$L_{15} = M_{55} \oplus L_1$	$L_{16} = M_{56} \oplus L_0$	$L_{17} = M_{57} \oplus L_1$	$L_{18} = M_{58} \oplus L_8$	$L_{19} = M_{63} \oplus L_4$
$L_{20} = L_0 \oplus L_1$	$L_{21} = L_1 \oplus L_7$	$L_{22} = L_3 \oplus L_{12}$	$L_{23} = L_{18} \oplus L_2$	$L_{24} = L_{15} \oplus L_9$
$L_{25} = L_6 \oplus L_{10}$	$L_{26} = L_7 \oplus L_9$	$L_{27} = L_8 \oplus L_{10}$	$L_{28} = L_{11} \oplus L_{14}$	$L_{29} = L_{11} \oplus L_{17}$
$S_0 = L_6 \oplus L_{24}$	$S_1 = L_{16} \oplus L_{26} \oplus 1$	$S_2 = L_{19} \oplus L_{28} \oplus 1$	$S_3 = L_6 \oplus L_{21}$	$S_4 = L_{20} \oplus L_{22}$
$S_5 = L_{25} \oplus L_{29}$	$S_6 = L_{13} \oplus L_{27} \oplus 1$	$S_7 = L_6 \oplus L_{23} \oplus 1$		

$$U = \begin{bmatrix} 0&0&0&0&0&0&0&1 \\ 0&1&1&0&0&0&0&1 \\ 1&1&1&0&0&0&0&1 \\ 1&1&1&0&0&1&1&1 \\ 0&1&1&1&0&0&0&1 \\ 0&1&1&0&0&0&1&1 \\ 1&0&0&1&1&0&1&1 \\ 0&1&0&0&1&1&1&1 \\ 1&0&0&0&0&1&0&0 \\ 1&0&0&1&0&0&0&0 \\ 1&1&1&1&1&0&1&0 \\ 0&1&0&0&1&1&1&0 \\ 1&0&0&1&0&1&1&0 \\ 1&0&0&0&0&0&1&0 \\ 0&0&0&1&0&1&0&0 \\ 1&0&0&1&1&0&1&0 \\ 0&0&1&0&1&1&1&0 \\ 1&0&1&1&0&1&0&0 \\ 1&0&1&0&1&1&1&0 \\ 0&1&1&1&1&1&1&0 \\ 1&1&0&1&1&1&1&0 \\ 1&0&1&0&1&1&0&0 \end{bmatrix}$$

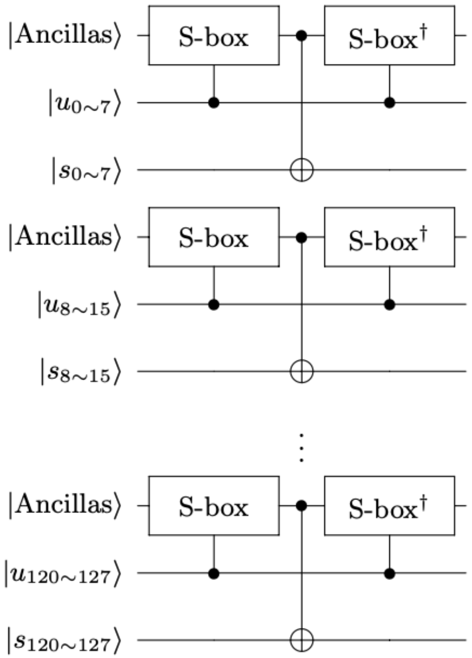
$$B = \begin{bmatrix} 0&0&0&1&1&0&1&1&0&1&1&0&0&0&0&1&1&0 \\ 1&1&0&0&0&0&1&1&0&1&1&0&0&0&0&1&1&0 \\ 1&0&1&0&0&0&1&0&1&0&0&0&1&0&1&1&0&1 \\ 1&1&0&1&1&0&0&0&0&1&1&0&0&0&0&1&1&0 \\ 0&1&1&0&1&1&0&0&0&1&1&0&0&0&0&1&1&0 \\ 1&0&1&1&1&0&0&1&1&0&1&1&1&0&1&1&1&0 \\ 0&0&0&0&1&1&0&1&1&0&0&0&1&1&0&1&1&0 \\ 1&0&1&1&0&1&0&0&0&0&0&0&1&1&0&1&1&0 \end{bmatrix}$$

S-box

- S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "**Implementing Grover Oracles for quantum key search on AES and LowMC**," in *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, ser. Lecture Notes in Computer Science, A. Canteaut and Y. Ishai, Eds., vol. 12106. Springer, 2020, pp. 280–310. [Online]. Available: https://doi.org/10.1007/978-3-030-45724-2 10
- K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, and A. Chattopadhyay, "**Quantum analysis of AES**," Cryptology ePrint Archive, Paper 2022/683, 2022, https://eprint.iacr.org/2022/683.
- B. Langenberg, H. Pham, and R. Steinwandt, "**Reducing the cost of implementing the advanced encryption standard as a quantum circuit**," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–12, 01 2020.
- J. Zou, Z. Wei, S. Sun, X. Liu, and W. Wu, "**Quantum circuit implementations of aes with fewer qubits**," in *Advances in Cryptology – ASIACRYPT 2020*, S. Moriai and H. Wang, Eds. Cham: Springer,International Publishing, 2020, pp. 697–726.
- Z. Huang and S. Sun, "**Synthesizing quantum circuits of AES with lower T-depth and less qubits**," Cryptology ePrint Archive, Report 2022/620, 2022, https://eprint.iacr.org/2022/620.

S-box

- S-box (S_1)
  - “Quantum analysis of AES” 논문에서 사용한 기법 적용
  - S–box† 사용 X
  - 매번 S-box에 ancilla qubits(68개) 할당



(b) Using multiple ancilla sets.

Table 3: Comparison of quantum implementations of AES S-box.

Method		#CNOT	#1qCliff	#T	TD	M	Full depth
S-box [32]		1818	124	1792	88	40	951
S-box [16]		358	68	224	8	123	104
S-box [17]	✤	392	72	238	6	136	85
S-box [49]		628	98	367	40	32	514
S-box [77]		437	72	245	55	22	339
S-box [21, 22]	391 lines	1470	670	1218	66	399	640
	406 lines	1507	548	1245	74	414	709
	413 lines	1484	561	1169	62	421	591
	409 lines	1483	574	1190	74	416	693
	400 lines	2244	1006	2254	111	408	998
S-box [36]		418	72	238	4	136	72
		824	160	546	3	198	69
S-box [51]		·	·	·	32	20	·
S-box [52]		·	·	·	24	21	·
		·	·	·	22	22	·
S-box [54]		372	72	238	4	90	69
S-box		418	72	238	4	136	61
	✿	366	72	238	4	84	58
	❀	781	160	546	3	152	56

✤: Reused in this work to fix [44] ❉.
✿: Used in this work (Toffoli depth 4).
❀: Used in this work (Toffoli depth 3).

K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, and A. Chattopadhyay, “Quantum analysis of AES,” Cryptology ePrint Archive, Paper 2022/683, 2022, https://eprint.iacr.org/2022/683

S-box

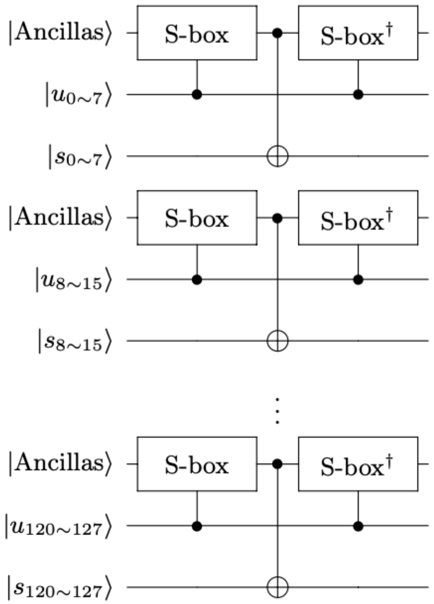
- S-box (S_1)
  - “Quantum analysis of AES” 논문에서 사용한 기법 적용
  - S−box† 사용 X , 매번 S-box에 ancilla qubits(68개) 할당

    → 이전 연구에 비해 큐비트 측면에서도 최적화

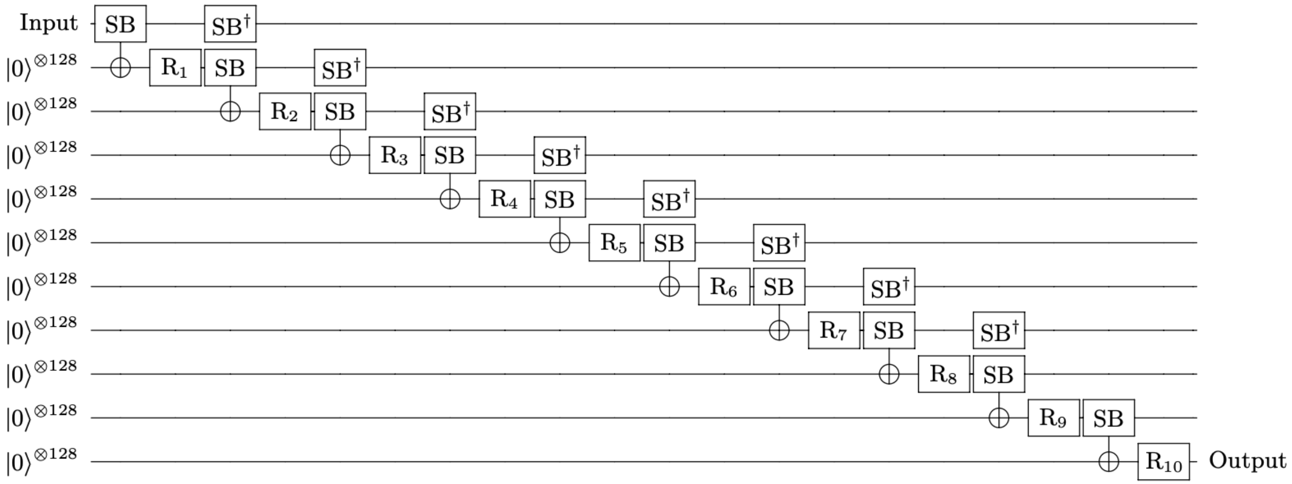
    → S−box† 비용이 들지 않는 pipeline 구조로 구현하기 복잡

Method	Source	#CNOT	#X	#Toffoli	Toffoli depth	#Qubit	depth
	[11]	569	4	448	196	40	-
Itoh-Tsujii	[13]	1114	4	108	4	$\boxed{162}$	151
	Ours	1106	4	108	4	170	137
Boyar-Peralta	**Ours**	162	4	34	4	$\boxed{84}$	33

38개의 ancilla qubit 재사용
garbage = 재사용 큐비트,Input, output 뺀 나머지108개



(b) Using multiple ancilla sets.



(b) Shallow and shallow/low depth versions (Ours).

K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, and A. Chattopadhyay, “Quantum analysis of AES,” Cryptology ePrint Archive, Paper 2022/683, 2022, https://eprint.iacr.org/2022/683

S-box

- S−box^{-1} (S_1^{-1})
  - "Quantum analysis of AES" + "Synthesizing quantum circuits of AES with lower T-depth and less qubits"
  - "Synthesizing quantum circuits of AES with lower T-depth and less qubits" 해당 논문에서 S−box^{-1} 사용
  - S−box^{-1} 내의 S-box는 "Quantum analysis of AES" 기법 사용
  - S−box = $\boldsymbol{LS_0(x)} + c = \boldsymbol{B \cdot F(U \cdot x)} + [11000110]^T,$

    $(L = linear\ function, S_0(x) = inversion)$
  - $x = S_0^{-1}L^{-1}(y+c) = S_0L^{-1}(y+c) = \boldsymbol{L^{-1}(LS_0)L^{-1}(y+c)}$

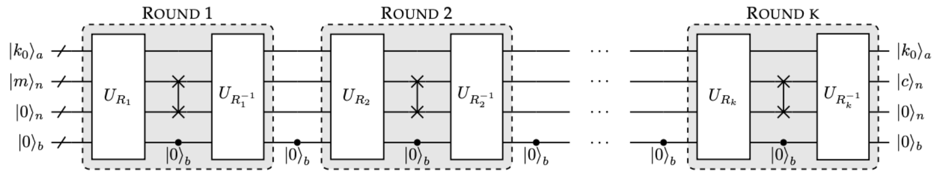


Fig. 5. The OP-based round-in-place structure

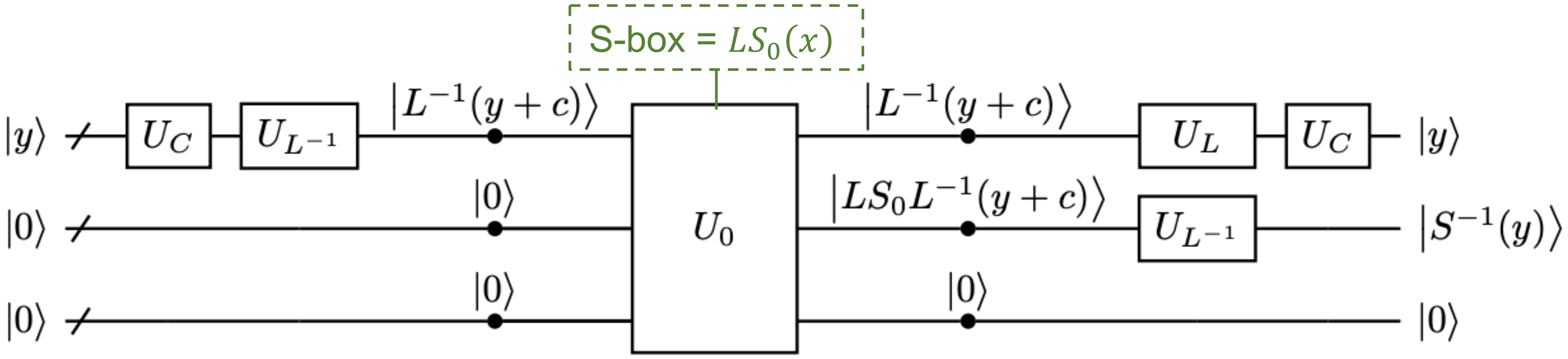


Fig. 15. The circuit for implementing the S-box^{-1} of AES

K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, and A. Chattopadhyay, "Quantum analysis of AES," Cryptology ePrint Archive, Paper 2022/683, 2022, https://eprint.iacr.org/2022/683

Z. Huang and S. Sun, "Synthesizing quantum circuits of AES with lower T-depth and less qubits," Cryptology ePrint Archive, Report 2022/620, 2022, https://eprint.iacr.org/2022/620.

S-box

- S-box (S_2)
  - Itoh-Tsujii algorithm
    - 곱셈과 제곱으로 이루어진 연산

$$\alpha^{-1} = \alpha^{254} = ((\alpha.\alpha^2).(\alpha.\alpha^2)^4.(\alpha.\alpha^2)^{16}.\alpha^{64})^2$$

  - Squaring (제곱기)
    - **XZLBZ 사용**

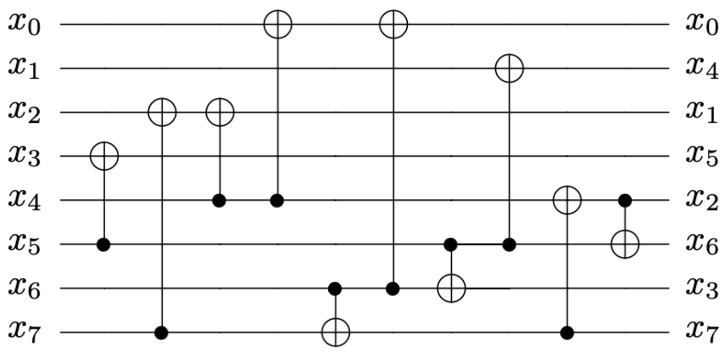


Fig. 4: Squaring in $\mathbb{F}_{2^8}/(x^8+x^4+x^3+x+1)$ using XZLBZ

CNOT gate: 10

Depth : 7

    - PLU 사용

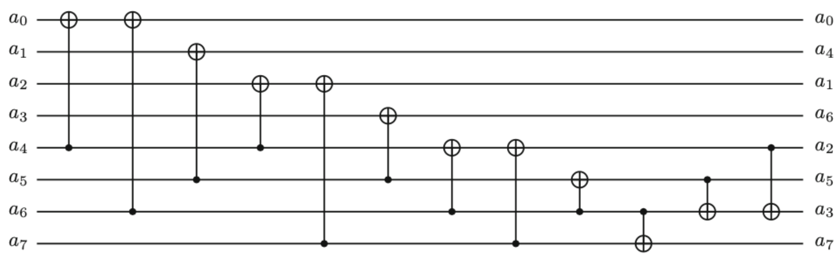


Fig. 1. Circuit for squaring in $\mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$.

CNOT gate: 12

Depth : 7

S-box

- S-box (S_2)
  - Multiplication (곱셈기)
    - Karatsuba Multiplication (Jang.et.al)
      - 카라추바 알고리즘을 재귀적으로 사용하여 Toffoli depth가 1인 곱셈 (81개 중 38개의 ancilla qubit 재사용)

Table 1: Quantum resources required for multiplication.

Source	#Clifford	#T	Toffoli depth	Full depth
CMMP [2]	435	448	28	195
J++ [11]	390	189	1	28

※: The multiplication size n is 8.

  - Affine function
    - 결과 큐비트를 할당하여 **out-of-place** 연산

$$S_2(\alpha) := \mathbf{B}.(\alpha^{-1})^8 + \mathbf{b} = \mathbf{B}.\mathbf{C}.\alpha^{-1} + \mathbf{b}$$
$$= \mathbf{D}.\alpha^{-1} + \mathbf{b}$$

$$\mathbf{D} = \begin{bmatrix} 0&1&0&1&0&1&1&1 \\ 0&0&1&1&1&1&1&1 \\ 1&1&1&0&1&1&0&1 \\ 1&1&0&0&0&0&1&1 \\ 0&1&0&0&0&0&1&1 \\ 1&1&0&0&1&1&1&0 \\ 0&1&1&0&0&0&1&1 \\ 1&1&1&1&0&1&1&0 \end{bmatrix} \text{ and } \mathbf{b} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

S-box

- S-box 양자 자원 비교
  - S_1 ← Boyar-Peralta, S_2 ← Itoh-Tsujii
  - 다만, 비교를 위해 Itoh-Tsujii 기법을 S_1에 적용하여 비교

Method	Source	#CNOT	#X	#Toffoli	Toffoli depth	#Qubit	depth
Itoh-Tsujii	[11]	569	4	448	196	40	-
	[13]	1114	4	108	4	162	151
	Ours	1106	4	108	4	170	137
Boyar-Peralta	**Ours**	162	4	34	4	84	33

Itoh-Tsujii	XZLBZ	1080	4	108	4	162	141
Boyar-Peralta	Inversion	190	4	34	4	84	55

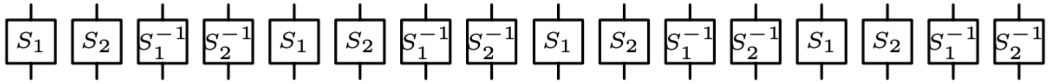
Substitution Layer

- Substitution Layer
  - 총 16개의 S-box가 병렬적으로 사용 → 순차 연산에 비해 depth 감소
  - [13] → 초기에 608 (38 x 16) ancilla qubit (재사용 가능) 할당
  - 초기에 **304 (38 x 8)** ancilla qubit (재사용 가능) 할당

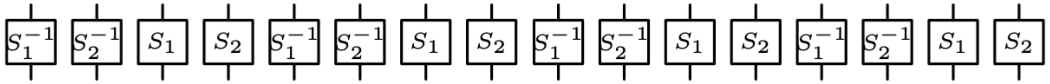
    → S_2, S_2^{-1} 에만 필요
  - S_1 에 적용한 기술(Boyar-Peralta)은 큐비트 수는 감소하지만

    병렬처리로 인해 depth 측면에서는 이득이 없음

    → S_2의 depth가 S_1에 비해 높아 **depth가 S_2에 의해 측정**



(a) S-box layer type 1



(b) S-box layer type 2

Diffusion Layer

- Diffusion Layer

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} = \begin{pmatrix} 0&0&0&1&1&0&1&0&1&1&0&0&0&1&1&0 \\ 0&0&1&0&0&1&0&1&1&1&0&0&1&1&0&1 \\ 0&1&0&0&1&0&1&0&0&0&1&1&1&0&0&1 \\ 1&0&0&0&0&1&0&1&0&0&1&1&0&1&1&0 \\ 1&0&1&0&0&1&0&0&1&0&0&1&0&0&1&1 \\ 0&1&0&1&1&0&0&0&0&1&1&0&0&0&1&1 \\ 1&0&1&0&0&0&0&1&0&1&1&0&1&1&0&0 \\ 0&1&0&1&0&0&1&0&1&0&0&1&1&1&0&0 \\ 1&1&0&0&1&0&0&1&0&0&1&0&0&1&0&1 \\ 1&1&0&0&0&1&1&0&0&0&0&1&1&0&1&0 \\ 0&0&1&1&0&1&1&0&1&0&0&0&0&1&0&1 \\ 0&0&1&1&1&0&0&1&0&1&0&0&1&0&1&0 \\ 0&1&1&0&0&0&1&1&0&1&0&1&1&0&0&0 \\ 1&0&0&1&0&0&1&1&1&0&1&0&0&1&0&0 \\ 1&0&0&1&1&1&0&0&0&1&0&1&0&0&1&0 \\ 0&1&1&0&1&1&0&0&1&0&1&0&0&0&0&1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix}$$

Algorithm 1: Quantum circuit implementation of ARIA Diffusion Layer using out-of-place.

Input: x, M
Output: $result$

0: Allocate result qubit $\rightarrow result[16][8]$
0: **for** $0 \leq i \leq 16$ **do**
0:     **for** $0 \leq j \leq 16$ **do**
0:         **if** $M[16 + j]$==1 **then**
0:             CNOT8bit(x, j, $result$, i)
0: return result =0

- 16 x 16 이진 행렬 곱셈
- 128 개의 결과 큐비트를 매 라운드마다 할당하여 **out-of-place** 연산 → **depth 최적화**

Method	#CNOT	#Qubit	depth
PLU	768	128	31
XZLBZ	376	128	17
Out-of-place	896	256	**7**

Quantum resource estimation

- ARIA 양자 자원 추정
  - [11]에 비해 **Depth** 측면에서 최적화
  - [13]에 비해 **Depth, Qubit** 측면에서 모두 최적화

    ※ [13]에서 잘못된 추정 결과 발견

NCT Level

Cipher	Source	#X	#CNOT	#Toffoli	Toffoli depth	#Qubit	Depth
ARIA-128	[11]	1,595	231,124	157,696	4,312	1,560	9,260
	[13]	1,408	285,784	25,920	60	29,216	3,500
	This work	1,408	173,652	17,040	60	26,864	**2,187**
ARIA-192	[11]	1,851	273,264	183,368	5,096	1,560	10,948
	[13]	1,624	324,136	29,376	68	32,928	3,978
	This work	1,624	197,036	19,312	68	30,320	**2,480**
ARIA-256	[11]	2,171	325,352	222,208	6,076	1,688	13,054
	[13]	1,856	362,488	32,832	76	36,640	4,455
	This work	1,856	220,420	21,584	76	33,776	**2,772**

Clifford + T Level

Cipher	Source	#Clifford	#T	T-depth	#Qubit	Full depth
ARIA-128	[11]	1,494,287	1,103,872	17,248	1,560	37,882
	[13]	494,552	181,440	240	29,216	4,650
	This work	311,380	119,280	240	26,864	**2,952**
ARIA-192	[11]	1,742,059	1,283,576	20,376	1,560	44,774
	[13]	560,768	205,632	272	32,928	5,285
	This work	353,156	135,184	272	30,320	**3,347**
ARIA-256	[11]	2,105,187	1,555,456	24,304	1,688	51,666
	[13]	627,000	229,824	304	36,640	5,919
	This work	394,948	151,088	304	33,776	**3,741**

[11]A. K. Chauhan and S. K. Sanadhya, "Quantum resource estimates of grover's key search on aria," in *Security, Privacy, and Applied Cryptography Engineering: 10th International Conference, SPACE 2020, Kolkata, India, December 17–21, 2020, Proceedings 10*. Springer, 2020, pp. 238–258.
[13] Y. Yang, K. Jang, Y. Oh, and H. Seo, "Depth-optimized quantum implementation of aria," *Cryptology ePrint Archive*, 2023.

Quantum resource estimation

- ARIA 양자 자원 추정 (추가, 논문 x)
  - [11]에 비해 **Depth** 측면에서 최적화
  - [13]에 비해 **Depth, Qubit** 측면에서 모두 최적화

    ※ [13]에서 잘못된 추정 결과 발견

	CNOT	1qClifford	T	T-depth	Qubit	Full depth
[11]	1,494,287		1,103,872	17,248	1,560	37,882
e_print [13]	441,560	53,248	181,440	240	29,216	4,650 (3,545)
ICISC	427,912	53,248	181,440	240	29,216	4,241 (3,158)
S-box만 변환	266,152	35,488	119,280	240	24,112	3,158
DL 변환(out-of_place)	273,432	35,488	119,280	240	25,904	3,028
This work	275,892	35,488	119,280	240	26,864	2,952

[11]A. K. Chauhan and S. K. Sanadhya, "Quantum resource estimates of grover's key search on aria," in *Security, Privacy, and Applied Cryptography Engineering: 10th International Conference, SPACE 2020, Kolkata, India, December 17–21, 2020, Proceedings 10*. Springer, 2020, pp. 238–258.
[13] Y. Yang, K. Jang, Y. Oh, and H. Seo, "Depth-optimized quantum implementation of aria," *Cryptology ePrint Archive*, 2023.

Grover's key search

- ARIA Grover 공격 비용 추정
  - Grover 공격 최적 iteration $[\frac{\pi}{4}\sqrt{2^k}]$
  - Oracle에는 2개의 회로 필요 → 2 x $[\frac{\pi}{4}\sqrt{2^k}]$ x quantum resources
  - $r = [key\ size/\ block\ size]$개의 평문-암호문 쌍을 얻는 것이 고유한 키를 식별할 수 있음.

  → Grover 공격 비용 : 2 x r x $[\frac{\pi}{4}\sqrt{2^k}]$ x quantum resource

  - **ARIA 는 NIST Level 1, 3, 5를 달성**

Cipher	Source	Total gates	Total depth	Cost (complexity)	#Qubit	NIST security
ARIA-128	[11]	$1.998 \cdot 2^{85}$	$1.816 \cdot 2^{79}$	$1.814 \cdot 2^{165}$	1,561	Level 1
	[13]	$1.117 \cdot 2^{84}$	$1.783 \cdot 2^{76}$	$1.991 \cdot 2^{160}$	29,217	
	This work	$\mathbf{1.296 \cdot 2^{83}}$	$\mathbf{1.132 \cdot 2^{76}}$	$\mathbf{1.468 \cdot 2^{159}}$	**26,865**	
ARIA-192	[11]	$1.146 \cdot 2^{119}$	$1.073 \cdot 2^{112}$	$1.23 \cdot 2^{231}$	3,121	Level 3
	[13]	$1.2 \cdot 2^{117}$	$1.013 \cdot 2^{109}$	$1.216 \cdot 2^{226}$	65,857	
	This work	$\mathbf{1.469 \cdot 2^{116}}$	$\mathbf{1.284 \cdot 2^{108}}$	$\mathbf{1.886 \cdot 2^{224}}$	**60,449**	
ARIA-256	[11]	$1.384 \cdot 2^{151}$	$1.238 \cdot 2^{144}$	$1.714 \cdot 2^{295}$	3,377	Level 5
	[13]	$1.336 \cdot 2^{149}$	$1.135 \cdot 2^{141}$	$1.516 \cdot 2^{290}$	72,081	
	This work	$\mathbf{1.642 \cdot 2^{148}}$	$\mathbf{1.435 \cdot 2^{140}}$	$\mathbf{1.178 \cdot 2^{289}}$	**67,553**	

Conclusion

- 이전 연구에 비해 depth, qubit 측면에서 모두 최적화
- ARIA-128, 192, 256 은 각각 NIST Level 1, 3, 5를 달성
- S-box에서 depth를 줄인 것은 전체 depth에 영향을 미치지 못함.
- 이후, 모든 S-box에 Boyar-Peralta 기법을 찾아서 구현할 예정

Q & A