Quantum Implementation and Analysis of ARIA

Yujin Oh, Kyungbae Jang, Yujin Yang, Hwajeong Seo
Hansung University

Introduction & Contribution

Background

Proposed Method

Performance & Evaluation

Conclusion

Introduction & Contribution

- **Grover's algorithm** reduce in the complexity of symmetric key cryptographic attacks to the square root.

  → This raises increasing challenges in considering symmetric key cryptography as secure.

- Establish secure **post-quantum** cryptographic systems.

  → There is a need for quantum **post-quantum security** evaluations of cryptographic algorithms.

- In this paper, we propose an optimized quantum circuits for **ARIA**.

  → We assess the **post-quantum security** strength of ARIA in accordance with NIST criteria.

Introduction & Contribution

1. Depth optimized quantum implementation.

→We focus on optimizing the **ARIA** quantum circuit **in terms of depth**.

→ As a result, it exhibits **the lowest depth** compared to previous studies.

2. Applying various techniques for each part

→ We apply various techniques in each part.

→ Additionally, we compare the estimated resource to highlight the most efficient techniques for each part.

3. Post-quantum Security Assessment of ARIA

→ We estimate **the cost of Grover's key search** using an our implemented quantum circuit

→ We compare the estimated cost of Grover's key search for ARIA with the **security levels** defined by NIST.

Background : ARIA

- ARIA is a Korean symmetric key cipher included in the validation subjects of the KCMVP(Korean Cryptographic Module Validation Program)

- ARIA adopts an SPN (Substitution- Permutation Network) structure and shares similarities with the AES (Advanced Encryption Standard) due to the considerati on of AES design principles during its development.

- The main components of ARIA are the substitution layer, diffusion layer, and key schedule.

Background : Quantum gates

- **Quantum gates** commonly used for implementing quantum circuits of block ciphers

  → This is not an exhaustive list of all possible gates that can be used.

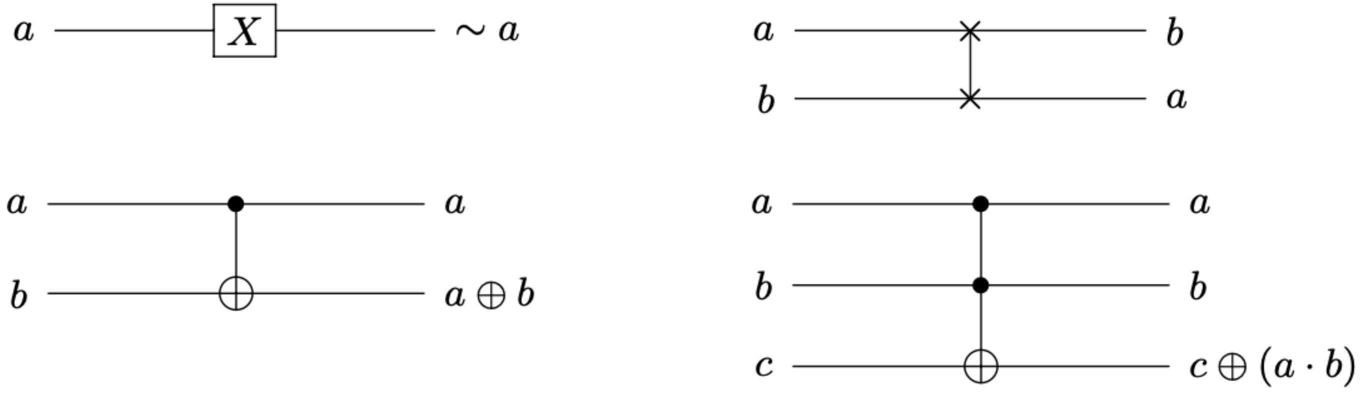
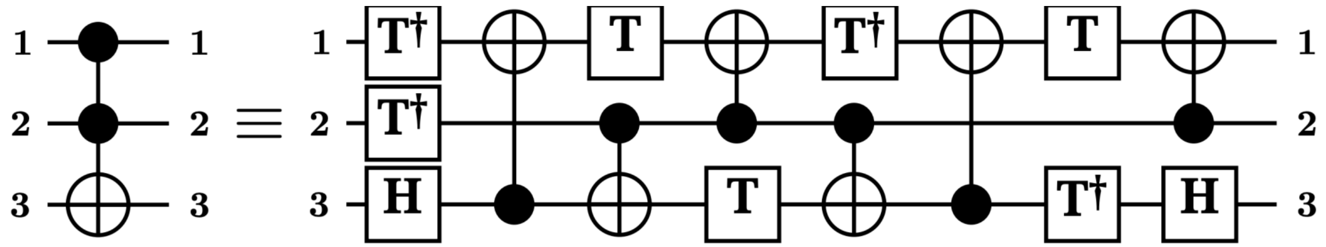


Fig. 5: Quantum gates: X (left top), Swap (right top), CNOT (left bottom) and Toffoli (right bottom) gates.



Toffoli gate decomposition (T- depth 4, total depth 8)

Background : Grover's key search

- **Key search using Grover's Algorithm**

1. Prepare a k-qubit key in a **superposition state** using **Hadamard gates**.

$$H^{\otimes k} |0\rangle^{\otimes k} = |\psi\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2^{k/2}} \sum_{x=0}^{2^k-1} |x\rangle$$

2. This circuit encrypts a known plaintext(p) in a **superposition state** using a pre-prepared key, producing ciphertexts for every possible key value.

If the ciphertext matches the expected ciphertext, the sign of the desired key state to be recovered is **negated**.

$$f(x) = \begin{cases} 1 \text{ if } Enc_{key}(p) = c \\ 0 \text{ if } Enc_{key}(p) \neq c \end{cases}$$

$$U_f(|\psi\rangle |-\rangle) = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle |-\rangle$$

3. The Diffusion Operator serves to **amplify the amplitude** of the target key state indicated by the oracle, identifying it by flipping the sign of said amplitude to negative.

Proposed Method : S-box

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

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

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

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

Same as AES

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

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

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

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

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

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

Proposed Method : S-box

- **S-box (S_1)**
  - Boyar and Peralta
    - $S(x) = A \cdot x^{-1} + [11000110]^T = B \cdot F(U \cdot x) + [11000110]^T$
    - → **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:				
$L_0 = M_{61} \oplus M_{62}$	$L_1 = M_{50} \oplus M_{56}$	$L_2 = M_{46} \oplus M_{48}$	$L_3 = M_{47} \oplus M_{55}$	$L_4 = M_{54} \oplus M_{58}$
$L_5 = M_{49} \oplus M_{61}$	$L_6 = M_{62} \oplus L_5$	$L_7 = M_{46} \oplus L_3$	$L_8 = M_{51} \oplus M_{59}$	$L_9 = M_{52} \oplus M_{53}$
$L_{10} = M_{53} \oplus L_4$	$L_{11} = M_{60} \oplus L_2$	$L_{12} = M_{48} \oplus M_{51}$	$L_{13} = M_{50} \oplus L_0$	$L_{14} = M_{52} \oplus M_{61}$
$L_{15} = M_{55} \oplus L_1$	$L_{16} = M_{56} \oplus L_0$	$L_{17} = M_{57} \oplus L_1$	$L_{18} = M_{58} \oplus L_8$	$L_{19} = M_{63} \oplus L_4$
$L_{20} = L_0 \oplus L_1$	$L_{21} = L_1 \oplus L_7$	$L_{22} = L_3 \oplus L_{12}$	$L_{23} = L_{18} \oplus L_2$	$L_{24} = L_{15} \oplus L_9$
$L_{25} = L_6 \oplus L_{10}$	$L_{26} = L_7 \oplus L_9$	$L_{27} = L_8 \oplus L_{10}$	$L_{28} = L_{11} \oplus L_{14}$	$L_{29} = L_{11} \oplus L_{17}$
$S_0 = L_6 \oplus L_{24}$	$S_1 = L_{16} \oplus L_{26} \oplus 1$	$S_2 = L_{19} \oplus L_{28} \oplus 1$	$S_3 = L_6 \oplus L_{21}$	$S_4 = L_{20} \oplus L_{22}$
$S_5 = L_{25} \oplus L_{29}$	$S_6 = L_{13} \oplus L_{27} \oplus 1$	$S_7 = L_6 \oplus L_{23} \oplus 1$		

$$U = \begin{bmatrix} 00000001 \\ 01100001 \\ 11100001 \\ 11100111 \\ 01110001 \\ 01100011 \\ 10011011 \\ 01001111 \\ 10000100 \\ 10010000 \\ 11111010 \\ 01001110 \\ 10010110 \\ 10000010 \\ 00010100 \\ 10011010 \\ 00101110 \\ 10110100 \\ 10101110 \\ 01111110 \\ 11011110 \\ 10101100 \end{bmatrix}$$

$$B = \begin{bmatrix} 000110110110000110 \\ 110000110110000110 \\ 101000101000101101 \\ 110110000110000110 \\ 011011000110000110 \\ 101110011011101110 \\ 000011011000110110 \\ 101101000000110110 \end{bmatrix}$$

Proposed Method : S-box

- **S-box (S_1)**
  - We apply the implementation by Jang et al. [9], which achieved the **best depth reduction** (while using a reasonable number of qubits), to the ARIA S-box.
  - By applying this method, we can significantly reduce both **the depth and the number of qubits and gates** compared to previous research.

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

Proposed Method : S-box

- **S−box^{-1} (S_1^{-1})**
  - "Quantum analysis of AES" + "Synthesizing quantum circuits of AES with lower T-depth and less qubits"
  - According to Huang et al, implementing the inverse of S1 requires the S1 circuit.

    → replacing only the S1 circuit part with the circuit in Jang et al.
  - S−box = $\boldsymbol{LS_0(x)} + c = \boldsymbol{B \cdot F(U \cdot x)} + [11000110]^T$,

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

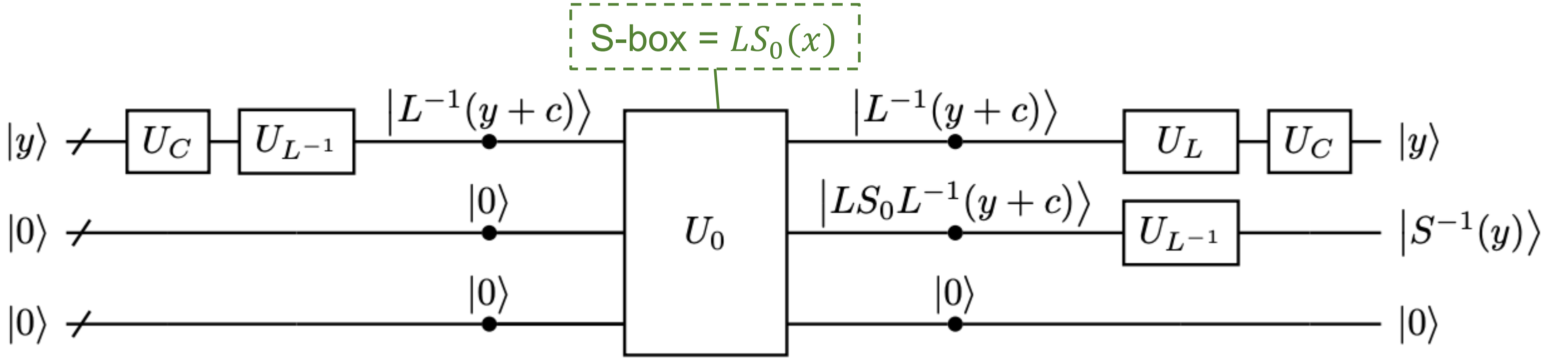


Fig. 15. The circuit for implementing the S-box^{-1} of AES

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.

Proposed Method : S-box

- **S-box (S_2)**
  - We use **Itoh-Tsujii algorithm** to compute a^{-1}

    → **Squaring and multiplication**

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

  - Squaring
    - In squaring, modular reduction can be employed **XZLBZ** because it is a linear operation.

      → Without allocating additional ancilla qubits (i.e., **in-place**), **using only CNOT gates**.

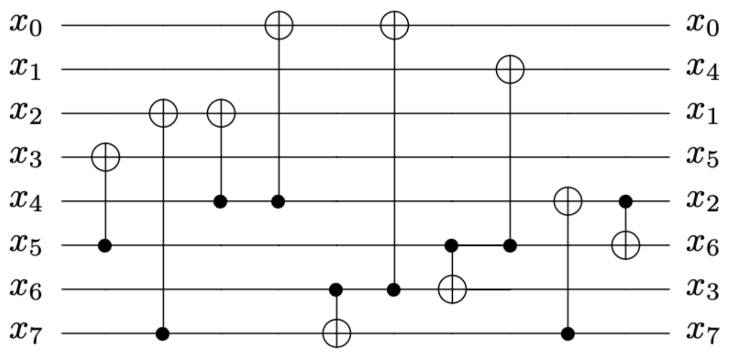


Fig. 4: Squaring in $\mathbb{F}_{2^8}/(x^8 + x^4 + x^3 + x + 1)$ using XZLBZ

CNOT gate: 10

Depth : 7

Proposed Method : S-box

- **Multiplication in a S-box(S_2)**
  - We apply **WISA’22 [Jang et al.] multiplication**

    → optimized with a **Toffoli depth of one** for any field size.

  - WISA’22[Jang et al.] multiplication
    - Using the **Karatsuba algorithm recursively** and allocating additional ancilla qubits.

      → All the AND operations become independent and the operations of **all Toffoli gates in parallel.**

      → The allocated ancilla qubits can be **reused** through **reverse operations**.

[Jang et al.] K. Jang, W. Kim, S. Lim, Y. Kang, Y. Yang, and J. Hwa, “Optimized implementation of quantum binary field multiplication with toffoli depth one,” in International Conference on Information Security Applications.

Proposed Method : S-box

- **Quantum resources required for implementations of a S-box**
  - S_1 ← Boyar-Peralta, S_2 ← Itoh-Tsujii
    - For comparison, note that quantum resources applied to S_1 are presented.

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

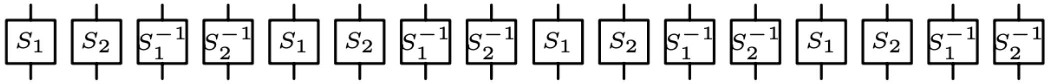
Proposed Method : Substitution Layer

- **Substitution Layer**
  - We reduce the depth by parallelizing the processing of all S-boxes(16) in each substitution layer
  - We initially allocate a total **of 304 (38×8)** ancilla qubits

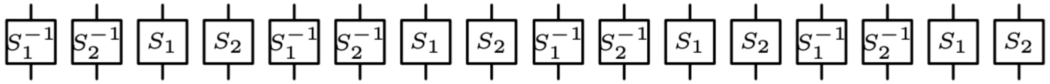
    → Only need S_2, S_2^{-1}
  - Due to parallel processing, the technique applied to S_1 has been beneficial in reducing the number of q ubits, **but there is no corresponding gain in terms of depth**.

    → This is because the depth cost of S_2 is higher than that of S_1,

    resulting in the depth of a substitution layer being measured by S_2.



(a) S-box layer type 1



(b) S-box layer type 2

Proposed Method : 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** $0 \le i \le 16$ **do**
0:     **for** $0 \le j \le 16$ **do**
0:         **if** $M[16 + j]$==1 **then**
0:             CNOT8bit(x, j, $result$, i)
0: return result =0

- 16 x 16 binary matrix multiplication
- 128 ancilla qubits are allocated for each round (i.e., out-of-place) to store the output of the diffusion layer. → **optimizing the depth**

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

Performance & Evaluation

- **Estimation of the quantum resources required for ARIA**
  - Our implementation of the ARIA quantum circuit achieves over **92.5%** improvement in **full depth** and over **98.7%** improvement in **Toffoli depth** compared to the implementation proposed in Chauhan et al.
  - Compared to Yang et al, our implementation is improved the **full depth** by **36.7%** and **the number of qubits** by **8%.**

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.

Performance & Evaluation

- **Grover's key search**
  - Grover's key search cost: the quantum resources x 2 x $\left\lfloor \frac{\pi}{4}\sqrt{2^k} \right\rfloor$

→ ARIA-128,192,256 can be evaluated as achieving post-quantum security Level 1,3 and 5,respectively.

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

- This paper presents the **implementation** of a quantum circuit for **ARIA**.
- We focus on optimizing **Toffoli and full depths**
- Our ARIA quantum circuit achieves over **92.5%** improvement in full depth and o ver **98.7%** improvement in Toffoli depth compared to the implementation propo sed in Chauhan et al.
- Compared to [13], our implementation is improved the full depth by **36.7%** and the number of qubits by **8%**.
- We analyze **the cost of Grover's key search attack**.

  →We can conclude that ARIA-128, 192, and 256 achieve quantum security level 1, 3 an d 5, respectively
- In future work, we plan to explore the **Boyar- Peralta** technique for all S-boxes and integrate it.

Q & A