Depth-Optimized Quantum Implementation of ARIA

Yujin Yang, Kyungbae Jang, Yujin Oh, and Hwajeong Seo

한성대학교
HANSUNG UNIVERSITY

CryptoCraft LAB

Index

Our Contribution

Low depth quantum implementation of ARIA

- Toffoli-depth and Full-depth reduction for the quantum circuit of Korean cryptosystems ARIA

Various techniques for optimization

- Use of optimized multiplication(Karatsuba), linear layer optimization method(XZLBZ), and parallel processing implementation

Evaluation of post-quantum security

- Evaluation of quantum security by comparing the estimated cost of Grover key search with the security level provided by NIST

Quantum Computer (Background)

- Quantum computers are built upon the principles of quantum mechanics (superposition and entanglement)
  - Can solve specific problems at a faster rate compared to classical computers

- The advancement of large-scale quantum computers has the potential to pose a threat to the security of current cryptographic systems.
  - Symmetric-key ciphers can be compromised by general attacks using the Grover's search algorithm (reduce the data search complexity $N \rightarrow \sqrt{N}$)

- In recent years, studies have been conducted to evaluate post-quantum security in existing symmetric-key ciphers.
  - Estimation the complexity of recovering secret keys using the Grover's search algorithm
  - Evaluation security strength based on these findings

ARIA Block Cipher (Background)

- ARIA is a symmetric-key cryptography algorithm
  - optimization for ultra-light environments and hardware implementation

- ARIA holds significance as symmetric key cipher included in the validation subjects of the KCMVP (Korean Cryptographic Module Validation Program).
  - For preparedness against emerging threats, assessing the quantum security strength of ARIA is crucial.

- There is already a study that measured the quantum security strength of ARIA in 2020 by Chauhan et al.[1].
  - However, Chauhan et al.[1] primarily focuses on qubit optimization.

  → need for research that addresses the recent emphasis on optimizing depth.

[1] Chauhan, A.K., Sanadhya, S.K.: 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) 238–258

Quantum Gates (Background)

In the quantum computer environment, logic gates not available
→ Quantum gates are utilized as replacements for logic gates

- The X gate replaces classical NOT operation
- The CNOT gate replaces classical XOR operation
- The Toffoli gate replaces classical AND operation

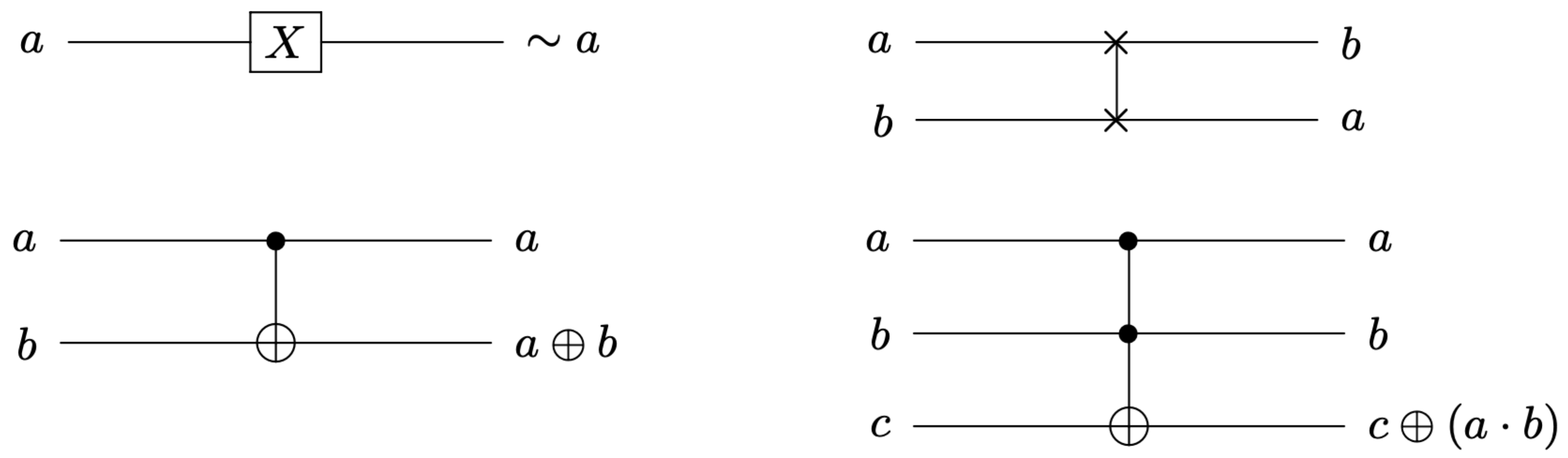
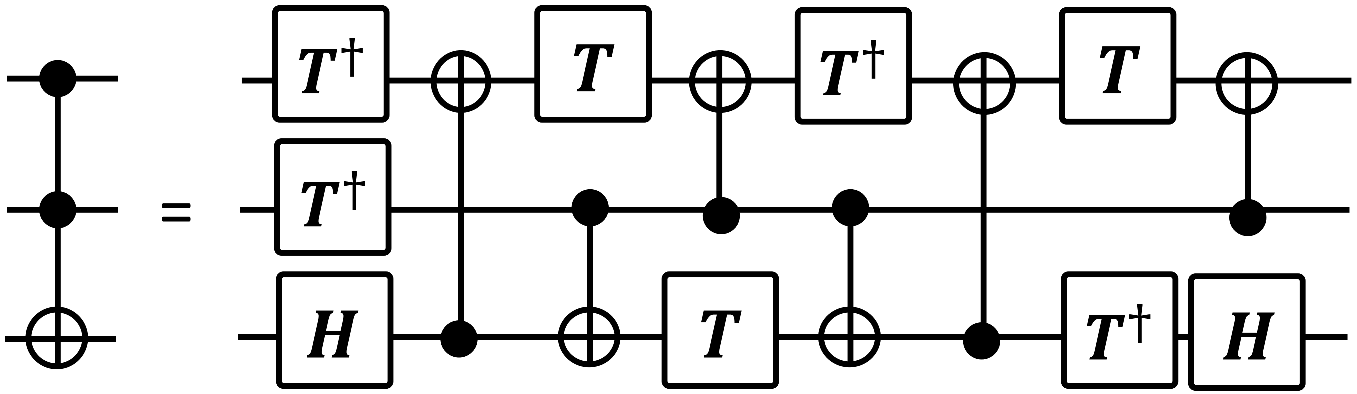


Fig. 4: Quantum gates: X (left top), Swap (right top), CNOT (left bottom) and Toffoli (right bottom) gates.

Quantum Gates (Background)

- Toffoli gates are highly complex quantum gates.
  - one Toffoli gate = 8 Clifford gates (CNOT, H) + 7 T gates
- We employ the Toffoli gate construction proposed by Amy et al.[2]



- T-depth : 4
- Full depth : 8

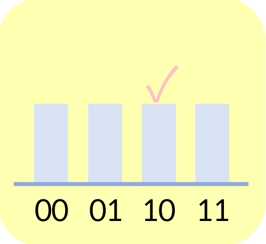
[Fig] Decomposition of Toffoli gate[1]

[2] M. Amy, D. Maslov, M. Mosca, M. Roetteler, and M. Roetteler, "A meet- in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits,"

Grover's Key Search Algorithm (Background)

1. **[Initialization]** n-qubit key has the same amplitude at all state of the qubits

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



2. **[Oracle Operator]** $f(x) = 1$, sign of the solution key is changed to negative.
Amplify the amplitude of the negative sign state.

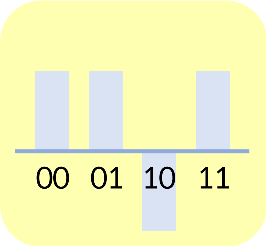
repeat $\frac{\pi}{4}\sqrt{2^k}$

prepared key

$$U_f(|\psi\rangle|-\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle|-\rangle \quad f(x) = \begin{cases} 1 \text{ if } \boxed{Enc(key)} = c \\ 0 \text{ if } \boxed{Enc(key)} \neq c \end{cases}$$

known ciphertext

ciphertext —— comparison

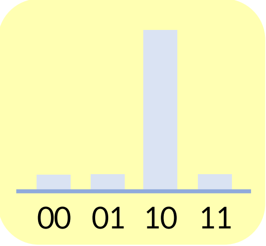


3. **[Diffusion Operator]** a key state (target key state) is transforming with a negative amplitude into a symmetric state.

each key state

$$D = 2|s\rangle\langle s| - I$$

average value



Proposed Quantum Implementation of S-box

In quantum computers, qubit states are unknown → Look-up table method can't be used
⇒ **Implement S-box circuit** based on **generation equation** using quantum gates

S-box **generation equation**

(input) 8-bit blocks

8 x 8 Matrix

8 x 1 Matrix

$$S_1(x) = A \cdot x^{-1} \oplus [1,1,0,0,0,1,1,0]^T$$

$$S_2(x) = B \cdot x^{247} \oplus [0,1,0,0,0,1,1,1]^T$$

$$x^{-1} = x^{254} \bmod m(x)$$

$$x^{247} = (x^{-1})^8 \bmod m(x)$$

irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Proposed Quantum Implementation of S-box

In quantum computers, qubit states are unknown → Look-up table method can't be used
⇒ **Implement S-box circuit** based on **generation equation** using quantum gates

S-box **generation equation**

(input) 8-bit blocks

8 x 8 Matrix

8 x 1 Matrix

$$S_1(x) = A \cdot x^{-1} \oplus [1,1,0,0,0,1,1,0]^T$$
$$S_2(x) = B \cdot x^{247} \oplus [0,1,0,0,0,1,1,1]^T$$

$$x^{-1} = x^{254} \bmod m(x)$$
$$x^{247} = (x^{-1})^8 \bmod m(x)$$

irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

process

1. Get $\boldsymbol{x^{-1}}$
2. Matrix-vector Multiplication
   (8 x 8 Matrix) $\cdot\, x^n$
3. constant(vector) Multiplication

Proposed Quantum Implementation of S-box

Get x^{-1}

(1) Itoh Tsuji Inversion Algorithm

$$x^{-1} = x^{254} = ((x \cdot x^2) \cdot (x \cdot x^2)^4 \cdot (x \cdot x^2)^{16} \cdot x^{64})^2$$

(2) Squaring – XZLBZ[3]

- XZLBZ [3] proposed a heuristic search algorithm based on factorization in binary matrices
- implement in-place structure
  → consist of CNOT gates
- 10 CNOT gates, circuit depth of 7

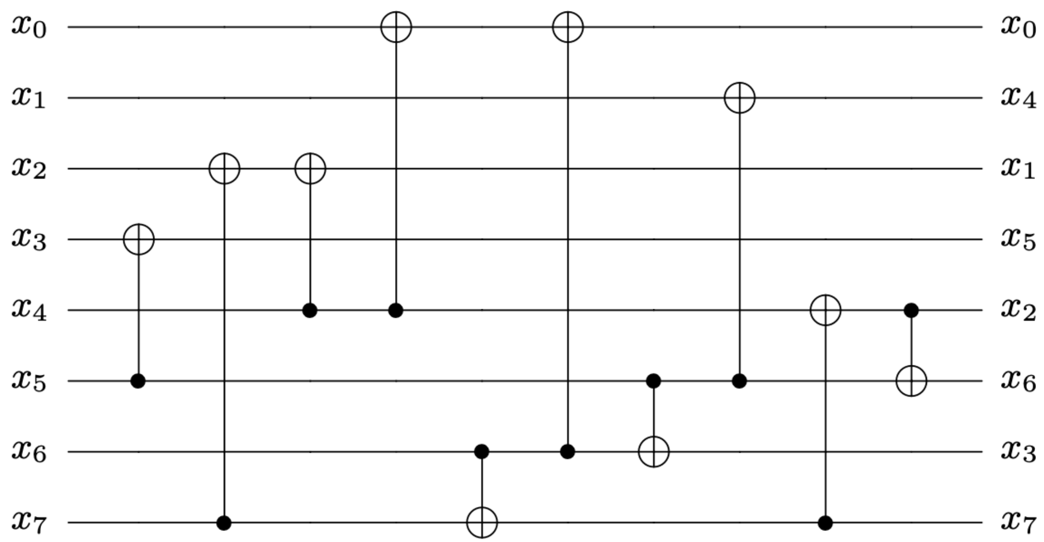


Fig. 5: Quantum circuit implementation for Squaring in $\mathbb{F}_{2^8}/(x^8 + x^4 + x^3 + x + 1)$

[3] Xiang, Z., Zeng, X., Lin, D., Bao, Z., Zhang, S.: Optimizing implementations of linear layers. IACR Transactions on Symmetric Cryptology (2020) 120–145

Proposed Quantum Implementation of S-box

Get x^{-1}

(3) Multiplication – Karatsuba multiplication optimized for Toffoli depth

(quantum-quantum multiplication)

Table 1: Quantum resources required for multiplication.

	Source	#Clifford	#T	Toffoli depth	Full depth
schoolbook	CMMP [2]	435	448	28	195
Karatsuba	J++ [13]	390	189	1	28

※: The multiplication size n is 8.

Matrix-vector Multiplication & constant(vector) Multiplication

classical-quantum multiplication → use XZLBZ

Cheung, D., Maslov, D., Mathew, J., Pradhan, D.K.: On the design and opti mization of a quantum polynomial-time attack on elliptic curve cryptography. In: Kawano, Y., Mosca, M. (eds.) TQC 2008. LNCS, vol. 5106, pp. 96–104. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-89304-2-9

Jang, K., Kim, W., Lim, S., Kang, Y., Yang, Y., Seo, H.: Optimized implementation of quantum binary field multiplication with toffoli depth one. In: International Conference on Information Security Applications, Springer (2022) 251–264

Proposed Quantum Implementation of Diff-layer

- Diffusion function A is expressed as 16 x 16 binary matrix multiplication

$$A: GF(2^8)^{16} \rightarrow GF(2^8)^{16}$$

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

1byte (8-bit)

- 0 : 8 x 8 zero matrix
- 1 : 8 x 8 identity matrix

(maintaining qubits)

- Through using XZLBZ, reduction of 51.04% (CNOT gates) and 45.16% (depth)

Table 2: Quantum resources required for Diffusion layer.

Source	#CNOT	qubit	Depth
PLU factorization	768	128	31
XZLBZ [25]	376	128	17

768 (= 96 × 8) , 376 (= 47 × 8)

Proposed Quantum Implementation of Key-Schedule

1) Key Initialization

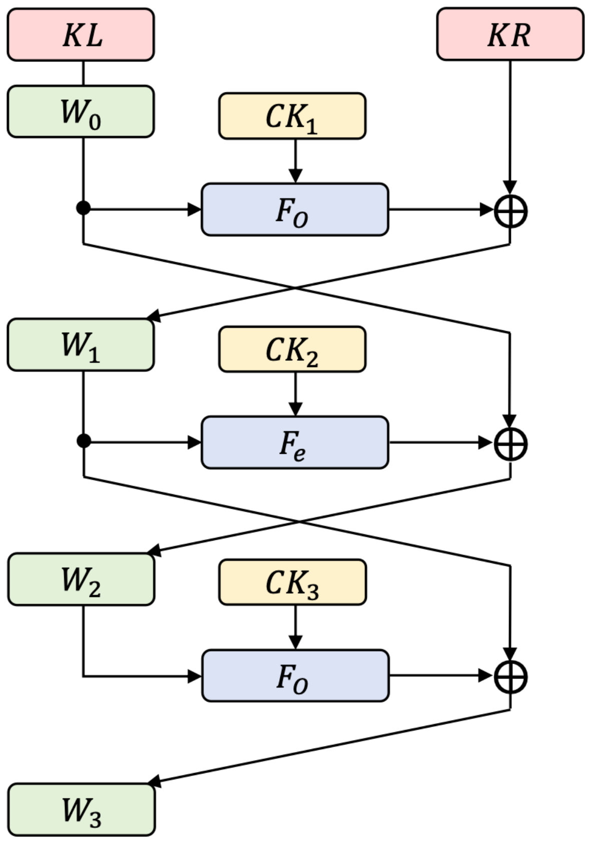


Fig. 3: Key Initialization of ARIA

Algorithm 1: Quantum circuit implementation of key schedule for ARIA.

Input: master key MK, key length l, vector a, b, ancilla qubit anc, round number r
Output: round key ek

▷ Key Initialization

K_L K_R

$W_1 \leftarrow F_o(MK[:128], a, b, anc)$ ▷ $MK[:128]$ is K_L
Constant_XOR($W_1[l-128:128]$, $MK[l-128:l]$) ▷ $MK[l-128:l]$ is K_R

$W_2 \leftarrow F_e(W_1, a, b, anc)$
$W_2 \leftarrow$ CNOT128($MK[:128], W_2$)

$W_3 \leftarrow F_o(W_2, a, b, anc)$
$W_3 \leftarrow$ CNOT128(W_1, W_3)

- K_L value is **identical** to W_0 value → instead of generating W_0, **use K_L**
⇒ **reduce** the number of **qubits**

- K_R is a **constant** → replace **CNOT gates** with **X gates**
⇒ **reduce the number of gates** and **gate cost**

Proposed Quantum Implementation of Key-Schedule

2) Key Generation

Algorithm 1: Quantum circuit implementation of key schedule for ARIA.

Input: master key MK, key length l, vector a, b, ancilla qubit anc, round number r
Output: round key ek

$\lll \rightarrow \ggg$

$num = [19, 31, 67, 97, 109]$
for $i \leftarrow 0$ to r **do**
  if $i = 0 \pmod 4$ **then** $K_L = W_0$
    Constant_XOR(ek, $MK[:128]$)
  else
    $ek \leftarrow$ CNOT128($W_{(i\%4)}, ek$)
  $ek \leftarrow$ CNOT128($W_{(i+1)\%4} \ggg num[i\%4], ek$)
return ek

$$
\begin{aligned}
&ek_1 = (W_0) \oplus (W_1 \ggg 19), && ek_2 = (W_1) \oplus (W_2 \ggg 19) \\
&ek_3 = (W_2) \oplus (W_3 \ggg 19), && ek_4 = (W_0 \ggg 19) \oplus (W_3) \\
&ek_5 = (W_0) \oplus (W_1 \ggg 31), && ek_6 = (W_1) \oplus (W_2 \ggg 31) \\
&ek_7 = (W_2) \oplus (W_3 \ggg 31), && ek_8 = (W_0 \ggg 31) \oplus (W_3) \\
&ek_9 = (W_0) \oplus (W_1 \lll 61), && ek_{10} = (W_1) \oplus (W_2 \lll 61) \\
&ek_{11} = (W_2) \oplus (W_3 \lll 61), && ek_{12} = (W_0 \lll 61) \oplus (W_3) \\
&ek_{13} = (W_0) \oplus (W_1 \lll 31), && ek_{14} = (W_1) \oplus (W_2 \lll 31) \\
&ek_{15} = (W_2) \oplus (W_3 \lll 31), && ek_{16} = (W_0 \lll 31) \oplus (W_3) \\
&ek_{17} = (W_0) \oplus (W_1 \lll 19)
\end{aligned}
\qquad (3)
$$

- When assigning W to $\boldsymbol{ek}$, since $\boldsymbol{W_0}$ is equal to K_L(constant), the CNOT gate operation can be replaced with the X gate operation

⇒ reduce the number of gates and gate cost

Evaluation

($Clifford + T$ Level)

Table 4: Required decomposed quantum resources for ARIA quantum circuit implementation

Cipher	Source	#Cliford	#T	T-depth	#Qubit (M)	Full depth	Toffoli depth (TD)	TD-M cost ($TD \times M$)
ARIA-128	CS [2]◇	1,494,287	1,103,872	17,248	1,560	37,882	4,312	6,726,720
	This work	481,160	181,440	240	29,216	4,241	60	1,752,960
ARIA-192	CS [2]◇	1,742,059	1,283,576	20,376	1,560	44,774	5,096	7,949,760
	This work	551,776	205,632	272	32,928	5,083	68	2,239,104
ARIA-256	CS [2]◇	2,105,187	1,555,456	24,304	1,688	51,666	6,076	10,256,288
	This work	616,920	229,824	304	36,640	5,693	76	2,784,640

◇ Extrapolated result

88.8% reduction (Full depth) 98.7% reduction (Toffoli depth) 72.9% reduction (TD-M cost)

- In CS's paper[1], the decomposed quantum resources were not explicitly provided.
  → the quantum resources are extrapolated based on the information provided in the paper
- Significantly reduces depth-related metrics (Full depth, Toffoli depth, TD-M cost) while considering the trade-off between qubit and depth.

[1] Chauhan, A.K., Sanadhya, S.K.: 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) 238–258

Evaluation

$$[\text{Table 5}] = [\text{Table 4}] \times \left\lceil \frac{\text{key size}}{\text{block size}} \right\rceil \times 2 \times \left\lfloor \frac{\pi}{4}\sqrt{2^k} \right\rfloor$$

Total gates X Full depth = Cost(complexity)

Table 5: Cost of the Grover's key search for ARIA

Cipher	Source	Total gates	Full depth	Cost (complexity)	#Qubit	*TD*-*M* cost	NIST Level[6,7]
ARIA-128	CS [2]	$1.946 \cdot 2^{85}$	$1.816 \cdot 2^{79}$	$1.767 \cdot 2^{165}$	1,561	$1.26 \cdot 2^{87}$	(Level 1) 2^{157}
	This work	$1.985 \cdot 2^{83}$	$1.626 \cdot 2^{76}$	$1.614 \cdot 2^{160}$	29,217	$1.313 \cdot 2^{84}$	
ARIA-192	CS [2]	$1.133 \cdot 2^{119}$	$1.073 \cdot 2^{113}$	$1.216 \cdot 2^{232}$	3,121	$1.489 \cdot 2^{121}$	(Level 3) 2^{192}, 2^{221}
	This work	$1.135 \cdot 2^{117}$	$1.949 \cdot 2^{109}$	$1.106 \cdot 2^{227}$	65,857	$1.672 \cdot 2^{119}$	
ARIA-256	CS [2]	$1.371 \cdot 2^{151}$	$1.238 \cdot 2^{145}$	$1.698 \cdot 2^{296}$	3,377	$1.921 \cdot 2^{153}$	(Level 5) 2^{274}, 2^{285}
	This work	$1.268 \cdot 2^{149}$	$1.092 \cdot 2^{142}$	$1.385 \cdot 2^{291}$	73,281	$1.04 \cdot 2^{152}$	

NIST Level Achieve

[6] Jang, K., Baksi, A., Song, G., Kim, H., Seo, H., Chattopadhyay, A.: Quantum analysis of aes. Cryptology ePrint Archive (2022)
[7] Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing grover oracles for quantum key search on aes and lowmc. Cryptology ePrint Archive, Report 2019/1146 (2019)

Evaluation

Table 5: Cost of the Grover's key search for ARIA

Cipher	Source	Total gates	Full depth	Cost (complexity)	#Qubit	TD-M cost
ARIA-128	CS [2]	$1.946 \cdot 2^{85}$	$1.816 \cdot 2^{79}$	$1.767 \cdot 2^{165}$	1,561	$1.26 \cdot 2^{87}$
	This work	$1.985 \cdot 2^{83}$	$1.626 \cdot 2^{76}$	$1.614 \cdot 2^{160}$	29,217	$1.313 \cdot 2^{84}$
ARIA-192	CS [2]	$1.133 \cdot 2^{119}$	$1.073 \cdot 2^{113}$	$1.216 \cdot 2^{232}$	3,121	$1.489 \cdot 2^{121}$
	This work	$1.135 \cdot 2^{117}$	$1.949 \cdot 2^{109}$	$1.106 \cdot 2^{227}$	65,857	$1.672 \cdot 2^{119}$
ARIA-256	CS [2]	$1.371 \cdot 2^{151}$	$1.238 \cdot 2^{145}$	$1.698 \cdot 2^{296}$	3,377	$1.921 \cdot 2^{153}$
	This work	$1.268 \cdot 2^{149}$	$1.092 \cdot 2^{142}$	$1.385 \cdot 2^{291}$	73,281	$1.04 \cdot 2^{152}$

NIST MAXDEPTH[8]

$2^{40}, 2^{64}, 2^{96}$

- ARIA-128 meets the MAXDEPTH requirement (ARIA-128 < 2^{96})
- In the case of exceeding MAXDEPTH (ARIA-192, 256), the focus should be on minimizing the costs of relevant metrics ($FD^2{\times}M, TD^2{\times}M$) instead of directly imposing a MAXDEPTH limit on the cost.

[8] NIST.: Call for additional digital signature schemes for the post-quantum cryptography standardization process (2022) https://csrc.nist.gov/csrc/media/ Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022. pdf.

Conclusion

- We propose the quantum circuit for ARIA, focusing on circuit depth optimization.
  - Our quantum circuit implementation achieves the full depth improvement of over 88.8% and Toffoli depth by more than 98.7% compared to the previous work (Chauhan et al.)

- We estimate the cost of Grover's attacks for the proposed circuit, and then evaluate the security strength based on the criteria provided by NIST.
  - ARIA achieves post-quantum security levels 1, 3, and 5 for all key sizes.
  - Only ARIA-128 satisfies the MAXDEPTH limit.

- Future work
  - Optimization of ARIA's quantum circuit further with consideration for the MAXDEPTH limit

Thank you