Depth Optimized Quantum Circuits for HIGHT and LEA

2nd Yujin Oh 3rd Minwoo Lee 5th Hwajeong Seo 1st Kyungbae Jang 4th Dukyoung Kim IT department IT department IT Department IT Department IT Department Hansung University Hansung University Hansung University Hansung University Hansung University Seoul, Korea Seoul, Korea Seoul, South Korea Seoul, South Korea Seoul, South Korea starj1023@gmail.com oyj0922@gmail.com minunejip@gmail.com dudejrdl123@gmail.com hwajeong84@gmail.com

Abstract—Quantum computers can model and solve several problems that have posed challenges for classical super computers, leveraging their natural quantum mechanical characteristics. A large-scale quantum computer is poised to significantly reduce security strength in cryptography. In this context, extensive research has been conducted on quantum cryptanalysis.

In this paper, we present optimized quantum circuits for Korean block ciphers, HIGHT and LEA. Our quantum circuits for HIGHT and LEA demonstrate the lowest circuit depth compared to previous results. Specifically, we achieve depth reductions of 48% and 74% for HIGHT and LEA, respectively. We employ multiple novel techniques that effectively reduce the quantum circuit depth with a reasonable increase in qubit count.

Based on our depth-optimized quantum circuits for HIGHT and LEA block ciphers, we estimate the lowest quantum attack complexity for Grover's key search. Our quantum circuit can be utilized for other quantum algorithms, not only for Grover's algorithm. Furthermore, the optimization methods gathered in this work can be adopted for generic quantum implementations in cryptography.

Index Terms—Quantum Computers, HIGHT, LEA, Grover's Algorithm

I. INTRODUCTION

Large-scale quantum computers, which are expected to emerge in the near future, pose a threat to the assured security of cryptography for classical computers. Two quantum algorithms are considered as major threats: Shor's algorithm [1] and Grover's algorithm [2]. Shor's algorithm can break RSA and Elliptic Curve Cryptography (ECC), which are based on the factorization and discrete logarithm problems. Grover's algorithm reduces the search complexity of N to \sqrt{N} with a speedup of square root.

As is well-known, NIST has considered the degradation of security and is constructing Post-Quantum Cryptography (PQC) to be ready for potential attacks by quantum computers. In the NIST PQC document [3], NIST introduced postquantum security levels from 1 to 5, corresponding to the difficulty of breaking AES and the SHA-2/3 family (using Grover's key search). In this context, extensive research is conducted on various ciphers [4]–[12] to evaluate their postquantum security strength.

For Grover's key search, reducing depth is more effective than reducing qubit count if parallelization of Grover's algorithm is unavoidable under a depth constraint (referred to as MAXDEPTH in [3]; related details are given in Section II-C).

In this paper, we present depth-optimized quantum circuits for HIGHT and LEA. Our quantum circuits for HIGHT and LEA achieve a depth reduction improvement of 48% and 74%, respectively, compared to the previous best result [13]. Based on our quantum circuits, we estimate the quantum complexity for Grover's key search for LEA and HIGHT and evaluate the post-quantum security level.

A. Contributions

Contributions of this paper can be summarized as follows.

- In our understanding, a depth-optimized quantum circuit is optimal for Grover's search algorithm (strictly speaking, under the depth constraint known as MAXDEPTH). We present improved quantum circuits for HIGHT and LEA in terms of circuit depth. We achieve circuit depth improvements of 48% and 74% for HIGHT and LEA, respectively.
- Multiple methods for effectively reducing circuit depth are gathered in this work. Note that the methods applied in the implementation can be adopted for generic quantum circuit implementations.
- Based on the implemented quantum circuits, which are optimal for quantum attack, the required quantum complexities for HIGHT and LEA are redefined in this work. With estimated quantum complexities, we re-evaluate the post-quantum security level for HIGHT and LEA.

B. Previous Work

In [14], quantum circuits for HIGHT and LEA were firstly presented. The aim of the authors was to reduce the number of qubits without considering circuit depth. In [13], the authors designed parallel quantum additions in the round function and key schedule for HIGHT and LEA. As a result, the circuit depth was significantly reduced compared to [14].

II. PRELIMINARIES

A. Quantum Gates

We summarize common quantum gates used for implementation of cryptographic algorithms in Figure 1. The X gate of Figure 1 operates on single qubit and inverts the input qubit; $X(a) = \sim a$. The CNOT gate of Figure 1 operates on two qubits and inverts the target qubit if the control qubit is 1; CNOT $(a, b) = (a, a \oplus b)$. The Toffoli gate of Figure 1 operates on three qubits and inverts the target qubit if both control qubits is 1; Toffoli $(a, b, c) = (a, b, a \oplus (b \cdot c))$.

B. Grover's Key Search

The process of Grover's search is divided into three steps: Input, Oracle, and Diffusion Operator. This section describes Grover's key search for ciphers.

1) *Input*: Hadamard gates are used to prepare a superposition state on a k-qubit input key, resulting in equal probabilities for all 2^k values of the unknown key.

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

2) In the *Oracle* stage, the target cipher is implemented as a quantum circuit that generates the ciphertext using the key in a superposition state. The resulting ciphertext (also in a superposition state) is compared with the known ciphertext (often omitted in resource estimation [4], [15], [16]). If a match is found (i.e., f(x) = 1), the sign of the solution key is negated.

$$f(x) = \begin{cases} 1 \text{ if } \operatorname{Enc}(x) = \operatorname{ciphertext} \\ 0 \text{ if } \operatorname{Enc}(x) \neq \operatorname{ciphertext} \end{cases}$$
$$U_f(|\psi\rangle |-\rangle) = \frac{1}{2^{k/2}} \sum_{x=0}^{2^k - 1} (-1)^{f(x)} |x\rangle |-\rangle$$

3) The *Diffusion operator* enhances the probability of the solution marked by the oracle (denoted by a negative sign). Since the complexity of the diffusion operator is negligible compared to the quantum circuit of the target cipher, it is commonly omitted in estimations [15], [16]. In Grover's key search, an extreme number of iterations of the oracle and diffusion operator are executed sequentially to measure a solution with high probability.

C. Post-Quantum Security Level and MAXDEPTH by NIST

With the beginning of NIST's standardization of postquantum cryptography, post-quantum security levels were defined (see [3]). NIST estimated the quantum attack complexities for AES-128, -192, and -256 by referring to Grassl et al's AES quantum circuit implementation, designating them as post-quantum security levels 1, 3, and 5, respectively. Recently, AES quantum circuits have been optimized through extensive research, leading NIST to adjust the quantum attack complexities of these levels based on Jaques et al's work [16]. As a result, the quantum attack complexities for these levels have decreased significantly [17].

Alongside the post-quantum security level, NIST introduced a parameter called MAXDEPTH. NIST considers the extreme depth of the quantum circuit for attacking using Grover's algorithm, as it requires a large number of iterations. Thus, if the circuit depth for Grover's key search exceeds MAXDEPTH, parallelization of Grover's search becomes unavoidable. Generally, we evaluate trade-off performance by measuring timespace complexity (the product of depth and qubit count). However, for the parallelization of Grover's algorithm, this metric changes by multiplying the depth by one more factor. The reason is the poor parallelization efficiency of Grover's algorithm. In [18], the authors analyzed the performance of parallelization for Grover's algorithm. In short, if we want to reduce the circuit depth by a factor of S, we should increase the number of instances for Grover's algorithm by a factor of S^2 . That is, the metric of time-space complexity changes to time-squared-space complexity. This is why reducing the depth is significantly important for Grover's algorithm.

III. QUANTUM CIRCUIT IMPLEMENTATION OF HIGHT

In this section, we describe our depth-optimized quantum circuit implementation of HIGHT. Compared to the previous work [13], we achieve a depth reduction of 54% with only 68 additional qubits.

A. Shallow Architecture for HIGHT

We apply the optimization technique introduced in Jang et al.'s AES quantum circuit implementation [19], namely the *shallow* architecture. The shallow architecture has an advantage for parallelization, as it can reduce depth with only a small increase in qubit count. The round function of HIGHT is defined by (where r is the round number, notation \boxplus means modular addition, and the functions F_0 and F_1 correspond to linear layers, see Equation 3):

$$\begin{split} X[i] &= X[i-1], \quad i = 1, 3, 5, 7\\ X[0] &= X[7] \oplus (F_0(X[6]) \boxplus RK[4r-3])\\ X[2] &= X[1] \boxplus (F_1(X[0]) \oplus RK[4r-0])\\ X[4] &= X[3] \oplus (F_0(X[2]) \boxplus RK[4r-1])\\ X[6] &= X[5] \boxplus (F_1(X[4]) \oplus RK[4r-2]) \end{split}$$
(1)

In the previous work [13], the subsequent round function of HIGHT is delayed until the completion of the reverse operation of the current round function. However, in the shallow architecture, the reverse operation of the current round function is performed simultaneously with the subsequent round function (i.e., in parallel). Figures 2 and 3 show the circuit diagrams for the regular and shallow architectures.

For the shallow architecture, we should divide the current and subsequent round functions in independent. In [13], the authors perform the reverse operation to reuse ancilla qubits of the current round function in the subsequent round function. That is, the current and subsequent round functions share the ancilla qubits each other (for details, see Figure 3 in [13]). In contrast, we run two sets of ancilla qubits by allocating additional ancilla qubits for the subsequent round function.

We use the CDKM adder (the same quantum adder adopted in [13]), which requires a single ancilla qubit for quantum addition. In [13], 4 ancilla qubits are allocated for quantum additions in parallel, as at most 4 additions are performed simultaneously in the round function. Note that after the



Fig. 1: Quantum gates used in this work.





Fig. 3: The shallow architecture adopted in this work.

completion of the additions, the 4 ancilla qubits are initialized to the clean state (i.e., $|0\rangle$) and reused in subsequent quantum additions. In [13], these 4 ancilla qubits are reused in the subsequent rounds. However, we allocate an additional 4 ancilla qubits to avoid sharing ancilla qubits between the current and subsequent rounds.

We should allocate additional qubits to operate key schedule of the current and subsequent rounds independently. The key schedule of HIGHT is given by (where r is the round number and θ is constant):

for
$$r = 0$$
 to 7:
for $i = 0$ to 7:
 $RK[16 \cdot r + i] = K[i - r \mod 8] \boxplus \delta_{16 \cdot r + i}$
for $i = 0$ to 7:
 $RK[16 \cdot r + i + 8] = K[(i - r \mod 8) + 8] \boxplus \delta_{16 \cdot r + i + 8}$
(2)

In [13], qubits for 4 δ s are initially allocated to operate 4 round keys simultaneously. After the use of the round keys, they are initialized to K, and 4 δ s are changed for the subsequent rounds. However, we require 8 round keys, with 4 round keys initialized in reverse order of the subsequent round and another 4 round keys generated in the subsequent round. Consequently, we allocate more ancilla qubits for the additional 4 δ s (i.e., 32 qubits).

Thanks to this, during the reverse operations of the current function, the subsequent round function can be performed in parallel.

B. Out-of-Place Implementation of linear layer

In HIGHT, linear layer operations which called F_0 and F_1 are given by:

$$F_0(x) = (x \lll 1) \oplus (x \lll 2) \oplus (x \lll 7) F_1(x) = (x \lll 3) \oplus (x \lll 4) \oplus (x \lll 6)$$
(3)

The authors in [13] adopted the same implementation method for F_0 and F_1 as in [14]. They presented an in-place

TABLE I: Quantum resources required for implementations of F_0 and F_1 .

Operation	Source	#CNOT	#Qubit (reuse)	Depth
F_0	[14] and [13]	21	8	15
F_0	Ours	24	16 (8)	3
F_1	[14] and [13]	24	8	17
F_1	[14] and [13]	24	16 (8)	3

implementation without using specific methods such as PLU decomposition.

We present an out-of-place implementation of the linear layers. In-place implementation has the advantage of reducing the number of qubits but increases circuit depth. Additionally, in the round function of HIGHT, if we use in-place implementation, the reverse operation of the linear layer (F_0 and F_1) must be performed since the input value of x is required in the subsequent round. This means that the subsequent round can only run after the completion of the reverse operation, leading to an increase in circuit depth.

Our out-of-place implementation allocates output qubits for the result. Thus, the required circuit depth is only 3, and the input value of the operations is maintained after the operation, enabling the subsequent round to run.

Additionally, the out-of-place implementation is efficient since we reuse output qubits using reverse operations. After using the output qubits as a result, we initialize them by performing the reverse operation of the linear layer. By allocating only 32 (= 8×4) output qubits for F_0 and F_1 , we effectively reduce circuit depth. Note that this reverse operation does not delay the subsequent round since we already have the input value.

C. Results

Table II shows the quantum resources required for our HIGHT quantum circuit compared with the results of [14] and [13]. Our quantum circuit implementation requires more qubits but provides the lowest depth. We achieve a 56% improvement in circuit depth compared to [13], with a reasonable increase in the number of qubits. As a result, we achieve the highest trade-off performances in terms of TD-M and FD-M, which represent time-space complexity. Unsurprisingly, for TD^2-M and FD^2-M trade-off performances (major metrics under the depth constraint), we provide much greater improvement since our circuit depth is the lowest.

TABLE II: Quantum resources required for implementations of HIGHT.

Source #CNOT #1aCliff	#1aCliff	ғ # Т	Toffoli depth	#Qubit	Full depth	$TD_{-}M$	$FD_{-}M$	$TD^2 M$	$FD^2 M$	
Source	Source #CNO1 #1qCll	πιqciiii	π1	(TD)	(M)	(FD)	1 D-M	$1^{\circ} D^{-101}$	1 D -1	$\Gamma D - M$
[14]	64,799	13,444	50,176	•	201	68,415	•	$1.639\cdot 2^{23}$		$1.711\cdot 2^{39}$
[13]	57,558	16,144	40,540	1,664	228	14,058	$1.447\cdot 2^{18}$	$1.528\cdot 2^{21}$	$1.176\cdot 2^{29}$	$1.311\cdot 2^{35}$
Ours	57,440	16,598	40,422	832	296	7,308	$1.879 \cdot \mathbf{2^{17}}$	$1.031 \cdot \mathbf{2^{21}}$	$1.527 \cdot \mathbf{2^{27}}$	$1.84\cdot\mathbf{2^{33}}$

TABLE III: Quantum resources required for implementations of LEA.

Cipher	Source	#CNOT	#1qCliff	#T	Toffoli depth (TD)	#Qubit (M)	Full depth (FD)	TD-M	FD- M	TD^2 -M	FD^2 - M
LEA-128	[14]	94,104	30,592	71,736	•	289	82,825		$1.427\cdot 2^{24}$	•	$1.803\cdot 2^{40}$
	[13]	94,104	31,588	71,736	5856	388	47,401	$1.083\cdot2^{21}$	$1.096\cdot 2^{24}$	$1.549\cdot 2^{33}$	$1.586\cdot 2^{39}$
	Ours	94,104	31,588	71,736	1,464	2,695	12,326	$1.881\cdot 2^{21}$	$1.98\cdot 2^{24}$	$1.345 \cdot \mathbf{2^{32}}$	$1.49\cdot\mathbf{2^{38}}$
LEA-192	[14]	138,852	45,758	107,604	•	353	124,181	•	$1.306\cdot 2^{25}$	•	$1.238\cdot 2^{42}$
	[13]	138,852	47,748	107,604	6832	518	55,301	$1.688\cdot 2^{21}$	$1.707\cdot 2^{24}$	$1.407\cdot 2^{34}$	$1.441\cdot 2^{40}$
	Ours	138,852	47,748	107,604	1,708	3,209	14,298	$1.307\cdot 2^{22}$	$1.367\cdot 2^{25}$	$1.09\cdot\mathbf{2^{33}}$	$1.193\cdot\mathbf{2^{39}}$
LEA-256	[14]	156,672	36,753	129,024	•	417	175,234	•	$1.089\cdot 2^{26}$	•	$1.456\cdot 2^{43}$
	[13]	158,688	54,630	122,976	7808	582	63,108	$1.083\cdot2^{22}$	$1.095\cdot 2^{25}$	$1.033\cdot 2^{35}$	$1.054\cdot 2^{41}$
	Ours	158,688	54,630	122,976	1,952	3,657	16,257	$1.702\cdot 2^{22}$	$1.772\cdot 2^{25}$	$1.622\cdot\mathbf{2^{33}}$	$1.758 \cdot \mathbf{2^{39}}$

IV. QUANTUM CIRCUIT IMPLEMENTATION OF LEA

In this section, we describe our depth-optimized quantum circuit implementation of LEA. Compared to previous work [13], we achieve a depth reduction of 74% with a reasonable number of qubits. The round function and key schedule of LEA-128 are as follows (see [20] for details of LEA-192 and LEA-256, $(0 \le i \le 23)$ and notation \ll means left rotation):

$$\begin{split} K[0] &= (K[0] \boxplus (\delta_{i \mod 4} \ll i)) \ll 1 \\ K[1] &= (K[1] \boxplus (\delta_{i \mod 4} \ll (i+1))) \ll 3 \\ K[2] &= (K[2] \boxplus (\delta_{i \mod 4} \ll (i+2))) \ll 6 \\ K[3] &= (K[3] \boxplus (\delta_{i \mod 4} \ll (i+3))) \ll 11 \\ RK_i &= (K[0], K[1], K[2], K[1], K[3], K[1]) \end{split}$$
(4)

 $\begin{aligned} X_{i+1}[0] &= \left((X_i[0] \oplus RK_i[0]) \boxplus (X_i[1] \oplus RK_i[1]) \right) \ll 9 \\ X_{i+1}[1] &= \left((X_i[1] \oplus RK_i[2]) \boxplus (X_i[2] \oplus RK_i[3]) \right) \ll 5 \\ X_{i+1}[2] &= \left((X_i[2] \oplus RK_i[4]) \boxplus (X_i[3] \oplus RK_i[5]) \right) \ll 3 \\ X_{i+1}[3] &= X_i[0] \end{aligned}$ (5)

A. Parallel Additions for Round Function

In [13], the authors achieved depth reduction compared to [14] by parallelizing quantum additions in the key schedule of LEA. However, for the round function, sequential quantum additions are performed. In contrast, we present a quantum implementation of the key schedule where quantum additions are operated in parallel.

To achieve this, we copy the inputs of the key schedule before performing the quantum additions (i.e., apply CNOT $(copy_{target}, copy_{result})$). Thus, in our implementation, additional qubits for $copy_{result}$ are allocated. After the completion of quantum additions, both inputs and $copy_{result}$ cannot be initialized, thus we cannot reuse these as we did in the quantum implementation of HIGHT. B. Simultaneous Execution of Round Function and Key Schedule

In [13], the round function is performed after the key schedule in their LEA quantum circuit implementation, leading to sequential execution of the round function and key schedule. In contrast, we present a quantum circuit implementation where the round function and key schedule are performed in parallel. To enable parallelization, we allocate additional ancilla qubits to operate quantum additions of the key schedule and round function simultaneously. Thanks to this, for LEA-128, where 4 sequential quantum additions were performed in [13], our quantum circuit runs 4 quantum additions in parallel, resulting in a reduction of circuit depth.

C. Results

Table III shows the quantum resources required for our LEA quantum circuit compared with previous work [13], [14]. Our quantum circuits for LEA require more qubits but provide the lowest depth. We achieve a 74% circuit depth reduction compared to [13], with a reasonable increase in qubit count. Although we cannot achieve the highest trade-off performances in terms of TD-M and FD-M, we achieve optimal performance in terms of TD^2-M and FD^2-M for Grover's search under the depth constraint.

V. EVALUATION

In this section, we estimate the quantum resources required for Grover's key search for HIGHT and LEA. Our depthoptimized quantum circuits for HIGHT and LEA provide the lowest quantum attack complexity. As we described in Section II-C, Grover's algorithm increases the probability of measuring a solution by iterating a set of oracle and diffusion operator. In [21], the authors analyzed the optimal number of iterations for a k-bit search space as $\lfloor \frac{4}{\pi}\sqrt{2^k} \rfloor$. The Grover oracle consists of twice the execution of the quantum circuit of the target cipher. For the diffusion operator, as we noted earlier, it is omitted in our resource estimation since the overhead is negligible (this approach is commonly adopted [16], [19]). In summary, the quantum resources required for Grover's key search are estimated as follows: Table II or III $\times 2 \times \lfloor \frac{\pi}{4}\sqrt{2^k} \rfloor$.

Table IV shows the quantum resources required for Grover's key search for HIGHT and LEA. We evaluate the postquantum security level suggested by NIST [17]. As described in Section II-C, NIST defines levels 1, 3, and 5 to correspond to the attack complexity for AES-128, -192, and -256, respectively. As observed in Table IV, HIGHT and LEA require more quantum resources than AES for the same key size. This is because the required quantum resources for HIGHT and LEA are more than AES. In our opinion, quantum additions used in HIGHT and LEA consume a lot of quantum resources (such as gates and depth). However, AES quantum circuits do not require quantum addition and have been recently optimized [16], [19]. Thus, HIGHT and LEA achieve the appropriate post-quantum security level according to the key size.

TABLE IV: Quantum resources required for Grover's key search for HIGHT and LEA.

Cipher	Total gates	Total depth	Complexity	NIST level
HIGHT	$1.372 \cdot 2^{81}$	$1.402\cdot 2^{77}$	$1.924 \cdot 2^{158}$	Level 1 (2^{157})
LEA-128	$1.183\cdot 2^{82}$	$1.182\cdot 2^{78}$	$1.398\cdot\mathbf{2^{160}}$	Level 1 (2^{157})
LEA-192	$1.763 \cdot 2^{114}$	$1.371 \cdot 2^{110}$	$1.209 \cdot \mathbf{2^{225}}$	Level 3 (2^{221})
LEA-256	$1.008\cdot 2^{147}$	$1.558 \cdot 2^{142}$	$1.57\cdot 2^{289}$	Level 5 (2^{285})

VI. CONCLUSION

We investigated previous quantum circuits of HIGHT and LEA and improved them in terms of quantum circuit depth. Multiple novel techniques are gathered in this work to effectively reduce quantum circuit depth, such as shallow architecture and copying for parallel operation. Depth-optimized quantum circuits offer optimal performance for Grover's key search. Consequently, our quantum circuits provide the lowest quantum attack complexity and the best trade-off performance for major metrics under the depth constraint. Since the quantum circuit implementation of the target block cipher is a fundamental block in quantum cryptanalysis, the presented quantum circuits in this work can be utilized for other quantum algorithms, not only for Grover's search.

VII. ACKNOWLEDGEMENT

This work was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT).(No. RS-2023-00277994, Quantum Circuit Depth Optimization for ARIA, SEED, LEA, HIGHT, and LSH of KCMVP Domestic Cryptographic Algorithms, 80%) and this work was partly supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (<Q|Crypton>, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity, 20%).

REFERENCES

- P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations* of computer science. IEEE, 1994, pp. 124–134.
- [2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium* on Theory of computing, 1996, pp. 212–219.
- [3] NIST., "Submission requirements and evaluation criteria for the post-quantum cryptography standardization process," 2016, https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.
- [4] Q. Liu, B. Preneel, Z. Zhao, and M. Wang, "Improved quantum circuits for AES: Reducing the depth and the number of qubits," Cryptology ePrint Archive, Paper 2023/1417, 2023, https://eprint.iacr.org/2023/1417. [Online]. Available: https://eprint.iacr.org/2023/1417
- [5] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck, "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3," in *Selected Areas in Cryptography – SAC 2016*, R. Avanzi and H. Heys, Eds. Cham: Springer International Publishing, 2017, pp. 317–337.
- [6] M. Rahman and G. Paul, "Grover on katan: Quantum resource estimation," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–9, 2022.
- [7] R. Anand, A. Maitra, and S. Mukhopadhyay, "Grover on SI-MON," *Quantum Information Processing*, vol. 19, no. 9, Sep 2020, http://dx.doi.org/10.1007/s11128-020-02844-w.
- [8] 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.
- [9] R. Anand, A. Maitra, S. Maitra, C. S. Mukherjee, and S. Mukhopadhyay, "Quantum resource estimation for FSR based symmetric ciphers and related Grover's attacks," in *Progress in Cryptology - INDOCRYPT* 2021 - 22nd International Conference on Cryptology in India, Jaipur, India, December 12-15, 2021, Proceedings, ser. Lecture Notes in Computer Science, A. Adhikari, R. Küsters, and B. Preneel, Eds., vol. 13143. Springer, 2021, pp. 179–198. [Online]. Available: https://doi.org/10.1007/978-3-030-92518-5_9
- [10] B. N. Bathe, R. Anand, and S. Dutta, "Evaluation of Grover's algorithm toward quantum cryptanalysis on ChaCha," *Quantum Inf. Process.*, vol. 20, no. 12, p. 394, 2021. [Online]. Available: https://doi.org/10.1007/s11128-021-03322-7
- [11] R. Anand, A. Maitra, and S. Mukhopadhyay, "Evaluation of quantum cryptanalysis on SPECK," in *Progress in Cryptology – INDOCRYPT* 2020, K. Bhargavan, E. Oswald, and M. Prabhakaran, Eds. Cham: Springer International Publishing, 2020, pp. 395–413.
- [12] M. Almazrooie, A. Samsudin, R. Abdullah, and K. N. Mutter, "Quantum reversible circuit of AES-128," *Quantum Information Processing*, vol. 17, no. 5, p. 1–30, may 2018. [Online]. Available: https://doi.org/10.1007/s11128-018-1864-3
- [13] K. Jang, G. Song, H. Kim, H. Kwon, H. Kim, and H. Seo, "Parallel quantum addition for korean block ciphers," *Quantum Information Processing*, vol. 21, no. 11, p. 373, 2022.
- [14] K. Jang, S. Choi, H. Kwon, H. Kim, J. Park, and H. Seo, "Grover on korean block ciphers," *Applied Sciences*, vol. 10, no. 18, p. 6407, 2020.
- [15] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's algorithm to AES: Quantum resource estimates," in *Post-Quantum Cryptography*, T. Takagi, Ed. Cham: Springer International Publishing, 2016, pp. 29–43.
- [16] 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
- [17] 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/callfor-proposals-dig-sig-sept-2022.pdf.
- [18] P. Kim, D. Han, and K. C. Jeong, "Time-space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2," *Quantum Information Processing*, vol. 17, pp. 1–39, 2018.

- [19] 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. [Online]. Available: https://eprint.iacr.org/2022/683
- [20] D. Hong, J.-K. Lee, D.-C. Kim, D. Kwon, K. H. Ryu, and D.-G. Lee, "Lea: A 128-bit block cipher for fast encryption on common processors," in *Information Security Applications*, Y. Kim, H. Lee, and A. Perrig, Eds. Cham: Springer International Publishing, 2014, pp. 3–27.
- In Information Security Applications, T. Kim, H. Lee, and A. Perrig, Eds. Cham: Springer International Publishing, 2014, pp. 3–27.
 [21] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik*, vol. 46, no. 4-5, p. 493–505, Jun 1998. [Online]. Available: http://dx.doi.org/10.1002/(SICI)1521-3978(199806)46:4/5₁493::AID-PROP493₆3.0.CO;2-P