IEEE Transactions on Quantum Engineering

Received June 30, 2021; revised December 20, 2021; accepted December 21, 2021; date of publication January 4, 2022; date of current version February 17, 2022.

Digital Object Identifier 10.1109/TQE.2022.3140376

Grover on KATAN: Quantum Resource Estimation

MOSTAFIZAR RAHMAN AND GOUTAM PAUL (Senior Member, IEEE)

Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata 700108, India

Corresponding author: Goutam Paul (e-mail: goutam.k.paul@gmail.com).

ABSTRACT This article presents the cost analysis of mounting Grover's key search attack on the family of KATAN block cipher. Several designs of the reversible quantum circuit of KATAN are proposed. Owing to the National Insitute of Standards and Technology's (NIST) proposal for postquantum cryptography standardization, the circuits are designed focusing on minimizing the overall depth. We observe that the reversible quantum circuits designed using AND gates and T-depth one Toffoli gate give more shallow circuits. Grover oracle for KATAN is designed based on the reversible circuits, which are used further to mount Grover's key search attack on KATAN. The designs are implemented using the software framework ProjectQ, which provides a resource estimation tool to perform an appropriate cost analysis in an automated way. While estimating the resources, NIST's depth restrictions are also respected.

INDEX TERMS Grover's algorithm, KATAN, postquantum cryptography (PQC), ProjectQ implementation, quantum cryptanalysis.

I. INTRODUCTION

Recent progress in the area of development of viable quantum computers has threatened the security of existing cryptographic schemes. Introduction of Shor's algorithm [1], [2] has put those public key schemes at risk, which were designed considering the hardness to solve the integer-factorization and discrete-logarithm problem. For symmetric-key schemes, threats due to generic attack using Grover's algorithm [3] only has been considered for a long time [4]. However, merely by doubling the key length the effect of Grover's algorithm can be nullified. Later, the introduction of quantum attacks using Simon's algorithm [5] on even-mansour cipher [6], three-round feistel cipher [7], encryption schemes [8], and HCTR-based schemes [9] has unveiled the facade of resistance of such schemes against quantum attacks. Based on computation power, quantum adversarial models have also been developed [10]. With ever-increasing chance of compromise of the security of cryptographic schemes with the progress toward the development of quantum computers and the difficulty of the transition to quantum-secure cryptographic schemes, the National Institute of Standards and Technology (NIST) put forth the proposal for standardization of postquantum cryptographic (PQC) schemes [11].

A. WHY RESOURCE ESTIMATION?

As the computing power of future quantum machines cannot be predicted accurately, the security of postquantum schemes cannot be estimated with certainty based on the current scenarios. Thus, NIST proposes to measure the security strengths in terms of computational resources rather than "bits of security" [11]. These computational resources can be measured in terms of the number of elementary operations, circuit size, etc. Resource estimation gives a quantitative measure of the complexity of the circuit. It provides a comparative filter between two competing design or attack implementations. As KATAN [12] is classically not broken, and till now, generic quantum attack using Grover's algorithm [3] is the only way to break the cipher, resource estimation of Grover's attack on KATAN shows the efficiency of the attack in the current scenario. Recently, a lot of work has explored the resource estimation of different quantum attacks on cryptographic schemes, such as resource estimation of Grover's search on symmetric-key primitives [13]–[18], resource estimation for computing discrete logarithms on binary elliptic curves [19], resource estimation of preimage attacks using Grover's search on hash functions [20], etc. In addition, study regarding the resource estimation of fault-tolerant quantum random access memory has also been conducted [21].

B. WHY KATAN?

KATAN, introduced in CHES 2009, is a family of lightweight block ciphers fulfilling the essential criteria to run in resource-constrained devices [12]. It is a hardware-oriented cipher specially designed for sensor networks, radio-frequency identification tags, and Internet of Things [12], [22]. Over the years, extensive cryptanalysis on KATAN has been done, like, differential attacks [23], conditional differential cryptanalysis [24], [25], meet-in-the-middle attacks [26]–[29], related-key boomerang attacks [30], [31], cube attack [32], subkey recovery attack [33], linear hull cryptanalysis [34], MILP-aided division property-based analysis [35], etc. All these attacks are on the round-reduced versions of KATAN. Instead of having a relatively small key length (80 bits), till now, there is no such attack using classical algorithms that penetrates all rounds of KATAN. This motivates us to analyze KATAN against the generic attack using Grover's algorithm. As a general rule of thumb, 80-bit security of KATAN against a quantum adversary can be achieved by doubling the key length. However, extending the key length of a nonlinear feedback shift register-based block cipher is not straightforward, and the results in this article might provide insights in designing an extended version of KATAN. In addition, analyzing the security of KATAN against quantum adversaries gives a notion regarding the security of ciphers, which are based on the same design principle. To the best of our knowledge, till now, no study has been conducted regarding the concrete cost analysis about Grover's key search on KATAN.

C. RELATED WORKS ON RESOURCE ESTIMATION

Grover's attack on symmetric-key schemes is mostly defined in terms of "bits of security." However, NIST's proposal has prompted redefining security in terms of computational resources. Earlier, Grassl *et al.* [13] estimated the computational resources of mounting Grover's attack on the advanced encryption standard (AES). Later, Langenberg *et al.* [14] and Almazrooie *et al.* [15] further reduced the cost of implementing AES using quantum gates and qubits. These analyses are based on reducing the number of qubits. In Eurocrypt 2020, Jaques *et al.* [36] studied the cost of implementing Grover's attack on AES by focusing on minimizing the depth of the circuit rather than the width. Apart from AES, resource estimation for Grover's attack has also been studied for feedback shift register-based schemes [16], Speck [17], and GIFT [18].

D. OUR CONTRIBUTION

In this work, we provide an estimation of computational resources for mounting Grover's attack on variants of the KATAN block cipher. Details regarding KATAN are provided in Section II-A. First, a quantum circuit for KATAN is proposed, where classical AND gates are realized using the CCNOT gate. As the CCNOT gate is not considered as a basic operation gate, an equivalent decomposition of the CCNOT gate using Clifford and T gates are considered. An alternate design of KATAN is also proposed by using a quantum AND gate.

The proposed circuits are used to design Grover's oracle of the KATAN block cipher. This oracle is then used to estimate the computational resources required for mounting Grover's key search attack. The computational resources are measured in terms of Clifford $+T$ gates, T-depth, and normal depth and width of the circuit. The circuits for Grover's oracle are implemented in ProjectQ framework [37], [38], which provides features to estimate the resources in an automated way. The quantum circuits are proposed focusing on reducing the overall depth and T-depth. No bounds on circuit width and usage of auxiliary qubits are considered as NIST has not provided any restriction on the width. Resource estimation by considering NIST's MAXDEPTH limit is also computed, and subsequent parallelization of the circuit is studied.

E. ORGANIZATION

The rest of this article is structured as follows. In Section II-A, a brief introduction regarding the KATAN block cipher is provided. In Sections II-B and II-C, a brief overview of Grover's algorithm and its impact on symmetric-key schemes are illustrated. Section III gives an overview regarding the design rationale of the quantum circuits. In Section IV, the design of quantum circuits of KATAN is proposed. Section V gives the cost of implementing Grover's oracle and mounting Grover's attack on variants of KATAN. Finally, Section VI concludes this article.

II. PRELIMINARIES

In this section, details regarding the KATAN block cipher, Grover's algorithm and its impact on symmetric-key cryptography, parallelization of Grover's algorithm, and cost estimation techniques are provided. In the rest of this article, G, D, and W denote the total gate cost, depth, and width of the quantum circuit, respectively. #CNOT, #1qCliff, #T, and #M refer to the number of CNOT gates, 1-qubit Clifford gates, T gates, and measure gates, respectively.

A. KATAN BLOCK CIPHER

KATAN is a family of lightweight hardware-oriented block ciphers proposed by Cannière *et al.* [12] in 2009. Depending on the block-length, there are the following three variants.

1) KATAN32: It has a block length of 32 bits.
2) KATAN48: It has a block length of 48 bits.
3) KATAN64: It has a block length of 64 bits.

The key size is 80 bits for all variants. Initially, the plaintext is loaded into two registers, L_1 and L_2. The lengths of L_1 and L_2 are different across the variants and given in Table 1. The least significant bit (LSB) and the most significant bit (MSB) of the plaintext are loaded to $L_2[0]$ and $L_1[|L_1|-1]$, respectively, where $L_i[p]$ denotes the pth bit in register L_i ($i \in \{1, 2\}$). In each round, the values in L_1 and L_2 are updated using two nonlinear feedback functions $f_a(\cdot)$ and $f_b(\cdot)$,

TABLE 1. Parameters of the KATAN Variants

Variant	$\|L_1\|$	$\|L_2\|$	x_1	x_2	x_3	x_4	x_5
KATAN32	13	19	12	7	8	5	3
KATAN48	19	29	18	12	15	7 6	
KATAN64	25	39	24	15	20	11	9

Variant	y_1	y_2	y_3	y_4	y_5	y_6
KATAN32	18	7	12	10	8	3
KATAN48	28	19	21	13	15	6
KATAN64	38	25	33	21	14	9

TABLE 2. Resource Estimation for Reversible Quantum Circuit of KATAN Block Cipher Using a Decomposition of Toffoli Gate With *T*-Depth 4

Variant	#CNOT	#1qCliff	$\#T$	$\#M$	T-Depth	D	W
KATAN32	13870	2032	10668	32	1654	4461	1080
KATAN48	26332	4064	21336	48	2058	6253	1620
KATAN64	38794	6096	31944	64	1836	5752	2160

TABLE 3. Resource Estimation for Reversible Quantum Circuit of KATAN Block Cipher Using a Decomposition of Toffoli Gate With *T*-Depth 3

Variant	#CNOT	#1qCliff	$\#T$	$\#M$	T-Depth	D	W
KATAN32	15394	3556	10668	32	1651	4071	1080
KATAN48	29380	7112	21336	48	1858	5825	1620
KATAN64	43366	10668	32004	64	1722	5367	2160

respectively. These two functions are defined as follows:

$$f_a(L_1) = L_1[x_1] \oplus L_1[x_2] \oplus (L_1[x_3] \cdot L_1[x_4]) \oplus (L_1[x_5] \cdot \text{IR}) \oplus k_a$$

$$f_b(L_2) = L_2[y_1] \oplus L_2[y_2] \oplus (L_2[y_3] \cdot L_2[y_4]) \oplus (L_2[y_5] \cdot L_2[y_6]) \oplus k_b$$

where k_a and k_b are two subkey bits and IR is *irregular* update rule. Let a KATAN variant use r rounds in total. Then, the 80-bit key is expanded using a key scheduling algorithm to $2r$ bits, and in round i, key bit at position $2i$ and $2i+1$ are used as k_a and k_b, respectively. The taps ($\{x_j\}$ and $\{y_j\}$) of L_1 and L_2 are different for the variants, and their values are given in Table 1. The *irregular* update rule IR controls the XORing of $L_1[x_5]$, and its values depend on another linear feedback shift register (LFSR) (for more details regarding IR and its values, refer to Table 3 in [12]). Fig. 1 shows a brief outline about the round function of KATAN.

There are in total 254 rounds for all variants. In a single round, f_a and f_b are applied one, two, and three times for KATAN32, KATAN48, and KATAN64, respectively. For KATAN48 and KATAN64, in a single round f_a and f_b are applied by using the same key bits. In each round, bit at position i moves to $i+1$ in both L_1 and L_2, and the MSBs are discarded. $L_1[0]$ and $L_2[0]$ are updated using the value of $f_b(L_2)$ and $f_a(L_1)$, respectively. Now, the details regarding the key scheduling algorithm are provided.

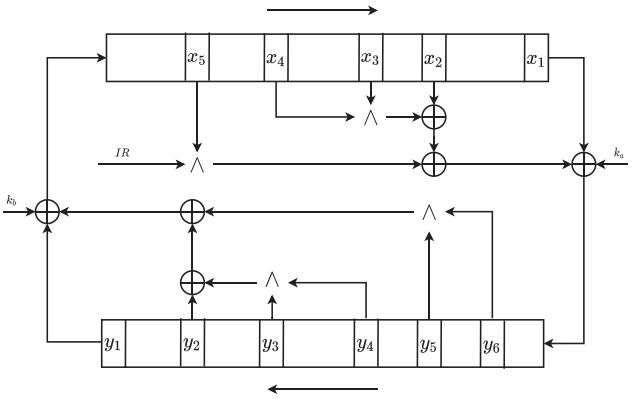

FIGURE 1. Schematic diagram of a round function of KATAN.

1) KEY SCHEDULING ALGORTIHM

Consider an 80-bit key K, and K_j denotes the jth bit of K. Initially, K is loaded to an LFSR, where the LSB of K is loaded to position 0 of the LFSR. As discussed earlier, in round i, key bits at positions $2i$ and $2i+1$ are used from the expanded round key. The 80-bit key K is expanded in the following way:

$$k_i = \begin{cases} K_i & \text{for } 0 \le i \le 79 \\ k_{i-80} \oplus k_{i-61} \oplus k_{i-50} \oplus k_{i-13} & \text{Otherwise.} \end{cases}$$

The key scheduling algorithm is same for all variants.

B. GROVER'S SEARCH ALGORITHM

Consider a list of $N = 2^n$ states indexed from 0 to $N-1$. Suppose, there is a function $f : \{0,1\}^n \to \{0,1\}$ and for a fixed a, $f(a) = 1$. The problem is to find this a by making oracle calls to f. By using classical algorithms, this problem can be solved by making $O(N)$ queries to the oracle; whereas by using a quantum computer, Grover's algorithm [3] can solve the problem by querying the oracle $O(\sqrt{N})$ times. Algorithm 1 gives the steps of Grover's search.

If operator G is applied j times, then the success probability of finding a is approximately $\sin^2((2j+1)/\sqrt{(N)})$. If, there are t states $a_0, a_1, \ldots, a_{t-1}$ such that $f(a_i) = 1$ for $0 \le i \le t-1$, then the success probability of finding one such a_i is at least $\frac{1}{2}$ when G is iterated $O(\sqrt{N/t})$ times [40]. For detail analysis on Grover's algorithm, refer to [3] and [41]. It is argued in [42], that Grover's algorithm is optimal when the number of oracle queries is less than $\frac{\pi}{4}\sqrt{N}$.

C. KEY RECOVERY ATTACK ON BLOCK CIPHER USING GROVER'S ALGORITHM

In [4], it is given that a key recovery attack can be mounted on a block cipher using Grover's algorithm. Consider a block cipher E with a block length of n bits and a key length of k bits. Let E encrypt an n-bit message m under a secret key K to obtain a ciphertext c. An adversary having the knowledge of an (m, c) pair can recover the key K using Grover's algorithm by iterating the G operator $O(2^{k/2})$ times. According to [4],

Algorithm 1: Grover's algorithm.

1) Initialize an n-qubit register Z. Hadamard transformation $H^{\otimes n}$ is applied on Z to obtain $|\Psi\rangle$, where

$$|\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle.$$

2) Consider a unitary map $U_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$. Grover operator G is defined as $U_{\Psi^\perp}U_f$, where $U_{\Psi^\perp} = H^{\otimes n}UH^{\otimes n}$ and

$$U(|x\rangle) = \begin{cases} -|x\rangle, & \text{for } x \neq 0 \\ |x\rangle, & \text{for } x = 0. \end{cases}$$

Operator G is applied $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ times to the register Z.

3) Z is measured to determine the value of x for which $f(x) = 1$. Output the result.

if G is iterated more than $\pi 2^{\frac{n}{2}-3}$ times, then the k-bit key can be recovered with an overwhelming probability.

Note that there are may be more than one key that maps m to c. All such keys, except the right one, that map m to c are known as spurious keys. Grover's algorithm that handles multiple solutions [40] retrieves a spurious key with the same probability as of retrieving the right key. If multiple plaintext–ciphertext pairs are used then the probability of retrieving a spurious key decreases significantly. If r pairs are used, then Grover's oracle should be constructed using r message blocks. Jaques *et al.* [36] argued that at least $\lceil \frac{k}{n} \rceil$ plaintext–ciphertext pairs should be used to recover the right key with an overwhelming probability.

D. COST METRICS

For cost analysis of mounting Grover's attack, two cost metrics that are proposed in [43] are considered. Consider a quantum circuit that has a depth and width of D and W, respectively, and which consists of G quantum gates. The two cost metrics are G-cost metric, which considers $\Theta(G)$ RAM operations, and DW-cost metric, which considers $\Theta(DW)$ RAM operations. It is shown by Jaques *et al.* [36] that G-cost and DW-cost are minimized by minimizing the number of parallel machines.

E. AUTOMATED RESOURCE ESTIMATION

In this work, the present circuits for Grover's oracle are designed and implemented in the ProjectQ [37], [38] framework. ProjectQ provides a module for automated estimation of required resources in terms of gate counts and circuit depth and width. In general, it is considered that for fault-tolerant quantum computation, the Clifford + T gate set forms a good universal gate [44]. Thus, the circuits are designed using a Clifford + T gate set only. Logical T gates are considered more expensive than the Clifford gates [45], and thus, along with normal depth, T-depth is also considered as a viable cost function. T-depth was first considered as a cost function by Amy *et al.* [46]. Previous works regarding the resource estimation for mounting Grover's attack on several ciphers considered T-depth as a resource constraint [13]–[16], [36]. While measuring T-depth, all gates apart from the T gates are ignored. In the case of measuring total depth, all gates are assigned a weight of 1. Like previous works, uncontrolled `SWAP` operations are regarded as free.

III. DESIGN RATIONALE

Here, the insights behind designing the circuits in this article are discussed. The designs in this work consider security strength defined in NIST's proposal for PQC standardization, the efficiency in implementing Grover's algorithm.

A. NIST PQC STANDARDIZATION

Constructing a combinatorial circuit by optimizing the depth and the number of gates is an intractable problem. Although Boyar *et al.* [47] have proposed heuristics-based methods to construct low-depth circuits, the gate cost of the circuit increases significantly when restrictions on the depth are more tightened. NIST has put a restriction on the circuit depth to match the time-boundness; however, there is no restriction on the number of qubits to be used. Owing to these factors, the quantum circuits in this work are designed to minimize the overall depth, whereas no restrictions are put in using the ancillary qubits.

B. IMPLEMENTATION ISSUES OF GROVER'S ALGORITHM

1) DEPTH CONSTRAINTS

In the standardization process of PQC [11], NIST introduces a parameter `MAXDEPTH` owing to the difficulty in running long serial computations. Thus, the resources of a quantum adversary are bounded by the maximum depth of a circuit. Once this `MAXDEPTH` is reached, multiple instances of Grover's algorithm are needed to be run in parallel. The permissible values of `MAXDEPTH` ranges from 2^{40} to 2^{96}. Jaques *et al.* [36] concluded that if the limits of resources in terms of depth, width, and gate count are fixed, then to mount an optimal attack the depth should be fully utilized and parallelization should be minimized as much as possible.

2) PARALLELIZATION

The efficiency of Grover's algorithm reduces significantly if parallelization is considered. The study regarding the parallelization of Grover's algorithm is studied in [48], [49], and [42]. Zalka [42] reported that by using S quantum machines a factor of $\sqrt{S}$ can be gained. This gain can be achieved in two ways: 1) running the full Grover's algorithm on S identical quantum machines and 2) partitioning the entire search space into S parts and assigning each part to each of the S identical machines, and the author also concluded that it is more advantageous to parallelize quantum searching algorithms by dividing the search space and assigning each space to different independent quantum machines. Kim *et al.* [50] formally

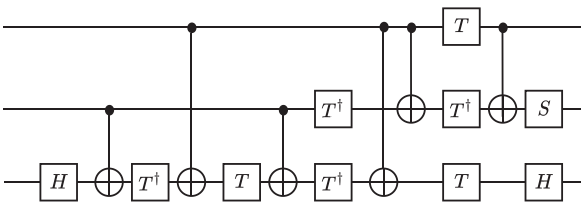

FIGURE 2. Decomposition of Toffoli gate into Clifford + T set with T-depth 4.

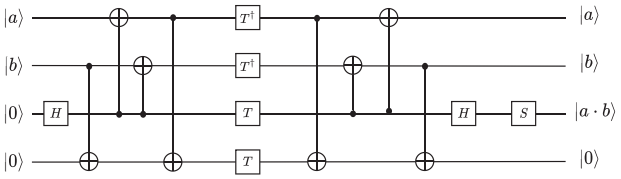

FIGURE 3. Design of and gate.

defined the notion of these two settings as outer and inner parallelization. In outer parallelization, Grover's algorithm is run on the entire search space on S identical machines, whereas in inner parallelization the search space is divided into S parts and Grover's algorithm is run on each part on S identical machines. In both cases, the required number of iterations is less than that of running only a single instance of Grover's algorithm. However, by using inner parallelization the probability of obtaining spurious keys is reduced, and thus, inner parallelization is more preferable to the outer one.

C. REALIZATION OF CLASSICAL "AND" OPERATION IN QUANTUM CIRCUITS

The AND operations in KATAN can be replaced with CCNOT gates in quantum circuits. However, the CCNOT gate is not a basic gate operation, and thus, instead of applying it directly its decomposition into a Clifford + T set is considered. Resource estimation of the proposed design is compared in terms of the cost metrics, and thus, several decompositions of CCNOT gates are considered to compare the corresponding cost metrics. As the codes for resource estimation are run on the ProjectQ framework, the default decomposition of CCNOT gates in that framework are considered initially. This decomposition has T-count 7 and T-depth 4, and is shown in Fig. 2.

There are two more decompositions of CCNOT/Toffoli gate into Clifford + T set. The decomposition proposed by Amy *et al.* [46] had T-depth 3 and does not use any ancillary qubit. Selinger proposed another decomposition, which uses four ancillary qubits and has T-depth 1. Both decompositions are considered in our design, and computational resources are estimated for the reversible quantum circuit of KATAN based on those decompositions.

Another design is considered where instead of using a CCNOT gate, an AND gate is used, which has T-depth 1. This AND gate is designed by Jaques *et al.* [36], and is based on the work of Selinger [51] and Jones [52]. Fig. 3 shows the design of the AND gate used in this article.

IV. RESOURCE ESTIMATION OF KATAN IMPLEMENTATION

Here, first, a reversible quantum circuit for KATAN using quantum gates and qubits is designed. The construction of the complete block cipher is composed of designing the round operations and designing the key scheduling operations. Then, the cost analysis for the designed circuit is estimated.

A. DESIGNING THE KEY SCHEDULE

The key scheduling algorithm of KATAN consists of XOR operations for generating a key bit, and thus, its equivalent quantum circuit can be realized easily by using CNOT gates in place of the XOR operations. All variants of KATAN have 254 rounds in total, and in each round, two key qubits are required. Therefore, in total $254 \times 2 = 508$ key qubits are required. Among these 508 key qubits, 80 qubits are initially given, and hence, $(508-80) = 428$ qubits are required to be generated. In the proposed design, four CNOT gates are required to generate a qubit, and thus, $428 \times 4 = 1712$ CNOT gates and 428 ancillary qubits are required for generating all the necessary key qubits. To construct the reversible circuit, all these operations are uncomputed after the full run of the KATAN block cipher.

B. DESIGNING THE ROUND OPERATION

Designing of the round operations mainly involves the realization of the nonlinear feedback functions $f_a(\cdot)$ and $f_b(\cdot)$ using quantum gates and qubits. Both the functions are composed of AND operations and XOR operations. The XOR operation can be realized using the CNOT gate, whereas the AND operation can be realized using the CCNOT gate. After the round operations, the new feedback qubit is stored using an ancillary qubit. In each round, $f_a(\cdot)$ and $f_b(\cdot)$ are computed once, twice, and thrice for KATAN32, KATAN48, and KATAN64, respectively. So, the number of new qubits in each round for KATAN32, KATAN48, and KATAN64 are 2, 4, and 6, respectively, and thus, the total number of ancillary qubits that are used for implementing $f_a(\cdot)$ and $f_b(\cdot)$ are 508, 1016, and 1524, respectively. After the completion of 254 rounds, the qubits corresponding to the ciphertext are fanned out to a quantum register, and the round operations are uncomputed to realize the reversible circuit. The design of the reversible quantum circuit for KATAN is given in Algorithm 2. Note that $C(a, t)$ refers to the application of the CNOT gate on target qubit t with control qubit a, and $\text{Tof}(a, b, t)$ refers to the application of CCNOT/Toffoli gate on target qubit t with control qubits a and b. The values x_i and y_i correspond to the values given in Table 1.

Table 2 gives the resource estimation for designing the KATAN cipher with the decomposition provided in ProjectQ.

Algorithm 2: Quantum circuit for round operation of KATAN.

INPUT: Message register $\mathcal{M}$, ciphertext register $\mathcal{C}$, key register $\mathcal{K}$

1) numRounds $\leftarrow$ 254 and iter $\leftarrow c$ (The value of c is 1, 2, and 3 for KATAN32, KATAN48, and KATAN64, respectively.)
2) Initialize a register $\mathcal{I}$ with the round values of the irreducible polynomial IR.
3) $\mathcal{M}$ is divided into L_1 and L_2.
4) numAQ $\leftarrow$ numRounds $\times$ iter$\cdot$ numAQ ancillary qubits are added to L_1 and L_2.
5) (2 $\times$ numRounds-80) ancillary qubits are added to $\mathcal{K}$.
6) Compute the new 428 key qubits and store them in the ancillary qubits of $\mathcal{K}$.
7) For $0 \leq j \leq$ numRounds perform the following operations-
   a) $C(L_2[\text{numAQ} - j + y1], L_1[\text{numAQ} - 1 - j])$
   b) $C(L_2[\text{numAQ} - j + y2], L_1[\text{numAQ} - 1 - j])$
   c) $\text{Tof}(L_2[\text{numAQ} - j + y3], L_2[\text{numAQ} - j + y4], L_1[\text{numAQ} - 1 - j])$
   d) $\text{Tof}(L_2[\text{numAQ} - j + y5], L_2[\text{numAQ} - j + y6], L_1[\text{numAQ} - 1 - j])$
   e) $C(\mathcal{K}[2 * j + 1], L_1[\text{numAQ} - 1 - j])$
   f) $C(L_1[\text{numAQ} - j + x1], L_2[\text{numAQ} - 1 - j])$
   g) $C(L_1[\text{numAQ} - j + x2], L_2[\text{numAQ} - 1 - j])$
   h) $\text{Tof}(L_1[\text{numAQ} - j + x3], L_1[\text{numAQ} - j + x4], L_2[\text{numAQ} - 1 - j])$
   i) if $(\mathcal{I}[j]{=}1)$
   $C(L_1[\text{numAQ} - j + x5], L_2[\text{numAQ} - 1 - j])$
   j) $C(\mathcal{K}[s2 * j], L_2[\text{numAQ} - 1 - j])$
8) Fan out the qubits corresponding to the ciphertext to $\mathcal{C}$
9) Uncompute the operations in Steps 7 and 8.

TABLE 4. Resource Estimation for Reversible Quantum Circuit of KATAN Block Cipher Using a Decomposition of Toffoli Gate With *T*-Depth 1

Variant	#CNOT	#1qCliff	#T	#M	T-Depth	D	W
KATAN32	29110	2032	10668	32	508	3055	7176
KATAN48	56812	4064	21336	48	584	4661	13812
KATAN64	84514	6096	32004	64	536	4295	20448

Resource estimation using the decomposition of Toffolli gate having T-depth 3 and T-depth 1 are given in Tables 3 and 4, respectively.

Table 5 gives the cost estimates of implementing the quantum reversible circuit using AND gate for the variants of KATAN block cipher.

TABLE 5. Resource Estimation for Reversible Quantum Circuit of KATAN Block Cipher Using an AND Gate

Variant	#CNOT	#1qCliff	#T	#M	T-Depth	D	W
KATAN32	16918	4572	6096	32	636	3315	2604
KATAN48	32428	9144	12192	48	779	4467	4668
KATAN64	47938	13716	18288	64	694	4075	6732

TABLE 6. Comparison of *G*-Cost Metric and Depth of the Designs

Design/	KATAN32		KATAN48		KATAN64	
Decomposition	G	D	G	D	G	D
T-depth 4	$2^{14.7}$	$2^{12.12}$	$2^{15.66}$	$2^{12.61}$	$2^{16.23}$	$2^{12.49}$
T-depth 3	$2^{14.86}$	$2^{11.99}$	$2^{15.82}$	$2^{12.51}$	$2^{16.39}$	$2^{12.39}$
T-depth 1	$2^{15.35}$	$2^{11.58}$	$2^{16.33}$	$2^{12.19}$	$2^{16.9}$	$2^{12.09}$
AND gate	$2^{14.75}$	$2^{11.69}$	$2^{15.72}$	$2^{12.13}$	$2^{16.29}$	$2^{11.99}$

C. COST METRICS OF THE DESIGNS

Now, the cost metrics of the several designs are compared. As NIST puts no bound on the width of the circuit, so instead of the DW-cost metric only the depth of the circuit is compared here. Table 6 compares the G cost and depth of various designs of the KATAN block cipher. From Table 6, it is evident that designs based on an AND gate and T-depth one Toffoli/CCNOT gate have comparatively lower depth. Hence, for constructing Grover's oracle, these two designs are considered.

V. QUANTUM RESOURCE ESTIMATION OF GROVER ON KATAN

Now, the resource requirement of Grover's oracle and Grover's search on KATAN is estimated. Initially, no parallelization is considered, and it is assumed that the Grover operator is running in serial. Later, NIST's MAXDEPTH is considered, and the resource requirement based on MAXDEPTH is estimated. The reversible quantum circuits based on T-depth one Tofolli gate and AND gate are used to estimate the resources for Grover's search on KATAN.

A. RESOURCE ESTIMATION OF GROVER'S ORACLE

Consider a block cipher with a block length of n bits and a key length of k bits. For such a block cipher, the probability of finding a unique key using r plaintext–ciphertext pairs is $e^{-2^{k-rn}}$ [36]. As discussed in Section III-B, the value of r should be at least $\lceil \frac{n}{k} \rceil$ to uniquely identify the correct key. These $\lceil \frac{k}{n} \rceil$ number of encryptions can be implemented in Grover's oracle in parallel. The key length for all variants of KATAN is 80 bits. Based on the value of n, the value of r and the corresponding success probabilities are determined.

For KATAN32, $n = 32$ and $k = 80$; therefore, r should be $\lceil \frac{80}{32} \rceil = 3$, and the probability of finding a unique key is approximately 0.99. Fig. 4 shows Grover's oracle for KATAN32. The value of r is set to 2 for KATAN48 and KATAN64 to recover a unique key with overwhelming probability. Grover's oracle for KATAN48/KATAN64 is shown

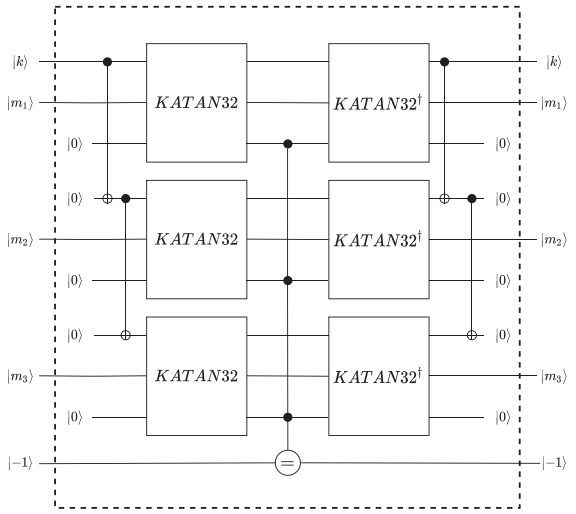

FIGURE 4. Grover's oracle of KATAN32.

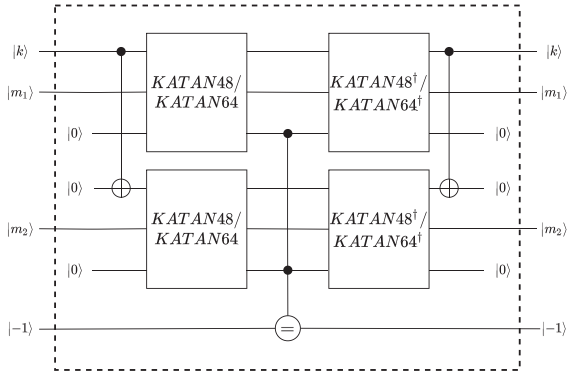

FIGURE 5. Grover's oracle of KATAN48/KATAN64.

TABLE 7. Resource Estimation for Grover's Oracle of KATAN Block Cipher

Design	Variant	#CNOT	#1qCliff	#T	T-Depth	D	W
T-depth 1 CCNOT	KATAN32	175556	12352	64630	1006	6052	42688
	KATAN48	227696	16304	85680	1160	9262	54944
	KATAN64	338600	24448	128464	1066	8548	81440
AND Gate	KATAN32	102404	27592	37248	1259	6560	15256
	KATAN48	130160	36624	49104	1546	8872	18368
	KATAN64	192296	54928	73600	1379	8104	26576

in Fig. 5. The estimated resources for implementing the Grover's oracle for KATAN block cipher are given in Table 7.

B. COST ESTIMATION OF GROVER'S SEARCH

For implementing Grover's search, the Grover operator G needs to be applied $\lfloor \frac{\pi}{4} 2^{k/2} \rfloor$ times (see Section II-B). For estimating the cost of Grover's search, cost related to U_f is considered, and the cost of $U_{\Psi^\perp}$ is ignored. It is assumed that no parallelization is used, and thus, all the resources (except width) are increased by a factor of $\lfloor \frac{\pi}{4} 2^{k/2} \rfloor$. Table 8 gives the cost estimation of implementing Grover's search on KATAN without parallelization.

TABLE 8. Resource Estimation for Grover's Search on KATAN Block Cipher

Design	Variant	#CNOT	#1qCliff	#T	T-Depth	D	W
T-depth 1 CCNOT	KATAN32	$2^{57.07}$	$2^{53.24}$	$2^{55.63}$	$2^{49.63}$	$2^{52.21}$	$2^{55.03}$
	KATAN48	$2^{57.45}$	$2^{53.64}$	$2^{56.04}$	$2^{49.83}$	$2^{52.83}$	$2^{55.4}$
	KATAN64	$2^{58.02}$	$2^{54.23}$	$2^{56.62}$	$2^{49.71}$	$2^{52.71}$	$2^{55.96}$
AND Gate	KATAN32	$2^{56.29}$	$2^{54.4}$	$2^{54.84}$	$2^{49.95}$	$2^{52.33}$	$2^{53.54}$
	KATAN48	$2^{56.64}$	$2^{54.81}$	$2^{55.23}$	$2^{50.25}$	$2^{52.77}$	$2^{53.82}$
	KATAN64	$2^{57.2}$	$2^{55.4}$	$2^{55.82}$	$2^{50.08}$	$2^{52.64}$	$2^{54.35}$

TABLE 9. Resource Estimation for Grover's Search on KATAN Block Cipher With Depth Limit

Design	Variant	GD	MAXDEPTH		
			2^{40}	2^{64}	2^{96}
T-depth 1 CCNOT	KATAN32	$2^{109.8}$	$2^{69.8}$	$2^{45.8}$	$2^{13.8}$
	KATAN48	$2^{110.81}$	$2^{70.81}$	$2^{46.81}$	$2^{14.81}$
	KATAN64	$2^{111.27}$	$2^{71.27}$	$2^{47.27}$	$2^{15.27}$
AND Gate	KATAN32	$2^{109.33}$	$2^{69.33}$	$2^{45.33}$	$2^{13.33}$
	KATAN48	$2^{110.14}$	$2^{70.14}$	$2^{46.14}$	$2^{14.14}$
	KATAN64	$2^{110.58}$	$2^{70.58}$	$2^{46.58}$	$2^{14.58}$

C. COST ESTIMATION UNDER A DEPTH LIMIT

Cost estimation in Table 8 is given without considering parallelization. However, to respect a depth limit, parallelization becomes inevitable. In the call of the proposal for PQC standardization, NIST has put a restriction on the depth limit [11]. The depth limit is referred to as MAXDEPTH, and its value can range from 2^{40} to 2^{96}. This forces to mount the attack using the parallelization of Grover's search algorithm. As discussed in Section III-B, it is assumed that inner parallelization is used to respect the depth limit.

To estimate the gate cost by considering the depth limit, a formula is provided by NIST. Consider a circuit that runs nonparallel to Grover's search with depth D and total gates G where $D = d \times$MAXDEPTH for some $d \geq 1$. Now, to mount an attack by achieving the same success probability as before while fitting the depth limit MAXDEPTH, d^2 parallel machines are required where each machine with gate cost of G/d run for $1/d$ fraction of the total time. Hence, the total gate cost is $(G/d) \times d^2 = GD/$MAXDEPTH. Based on this formula, gate costs for mounting Grover's attack under the constraint of different plausible values of MAXDEPTH are given in Table 9.

VI. CONCLUSION

Resource estimation for Grover's key search on the family of KATAN block cipher respecting NIST's MAXDEPTH depth restrictions was explored. Several designs of the reversible quantum circuit for KATAN block cipher were proposed focusing on minimizing the depth. Design based on AND gates produced relatively low depth circuits for KATAN48

and KATAN64, whereas for KATAN32 design based on T-depth one Toffoli gate produced shallow circuit. Instead of minimizing the overall depth, if minimization of T-depth is considered, then the circuits designed using T-depth one Toffoli gates produced low-depth circuits. These designs were then used to produce low-depth circuits for Grover's key search. For concrete cost analysis, the proposed circuits were implemented in ProjectQ, and the automated resource estimation tool of ProjectQ is leveraged on to count the required resources.

Typically, any new cryptanalysis work was evaluated in comparison with prior attacks on the same cipher. To the best of our knowledge, ours is the very first work on resource analysis of quantum attacks on KATAN, and hence, no such comparative study is relevant here.

The quantum resource estimation for Grover's attack on KATAN establishes that it is infeasible to mount Grover's attack on KATAN using the current available technology. Further, it would be interesting to estimate the cost of other algorithms that have an impact on cryptography.

REFERENCES

[1] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi: 10.1137/S0097539795293172.

[3] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219, doi: 10.1145/237814.237866.

[4] A. Yamamura and H. Ishizuka, "Quantum cryptanalysis of block ciphers. (Algebraic systems, formal languages and computations)," *RIMS Kokyuroku*, vol. 1166, pp. 235–243, 2000. [Online]. Available: https://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/1166-29.pdf

[5] D. R. Simon, "On the power of quantum computation," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1474–1483, Oct. 1997, doi: 10.1137/S0097539796298637.

[6] H. Kuwakado and M. Morii, "Security on the quantum-type even-mansour cipher," in *Proc. Int. Symp. Inf. Theory Appl.*, 2012, pp. 312–316. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6400943

[7] H. Kuwakado and M. Morii, "Quantum distinguisher between the 3-round feistel cipher and the random permutation," in *Proc. IEEE Int. Symp. Inf. Theory*, 2010, pp. 2682–2685, doi: 10.1109/ISIT.2010.5513654.

[8] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period finding," in *Proc. Adv. Cryptology*, 2016, pp. 207–237, doi: 10.1007/978-3-662-53008-5_8.

[9] M. Rahman and G. Paul, "Quantum attacks on HCTR and its variants," *IEEE Trans. Quantum Eng.*, vol. 1, 2020, Art. no. 3102408, doi: 10.1109/TQE.2020.3041426.

[10] M. Zhandry, "How to construct quantum random functions," in *Proc. IEEE 53rd Annu. Symp. Found. Comput. Sci.*, 2012, pp. 679–687, doi: 10.1109/FOCS.2012.37.

[11] NIST, "Submission requirements and evaluation criteria for the post-quantum cryptography standardization process," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2016. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-draft-aug-2016.pdf

[12] C. De Cannière, O. Dunkelman, and M. Knežević, "KATAN and KTANTAN - A family of small and efficient hardware-oriented block ciphers," in *Proc. Cryptographic Hardware Embedded Syst.*, 2009, pp. 272–288, doi: 10.1007/978-3-642-04138-9_20.

[13] 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, Switzerland: Springer, 2016, pp. 29–43, doi: 10.1007/978-3-319-29360-8_3.

[14] B. Langenberg, H. Pham, and R. Steinwandt, "Reducing the cost of implementing the advanced encryption standard as a quantum circuit," *IEEE Trans. Quantum Eng.*, vol. 1, 2020, Art. no. 2500112, doi: 10.1109/TQE.2020.2965697.

[15] M. Almazrooie, A. Samsudin, R. Abdullah, and K. N. Mutter, "Quantum reversible circuit of AES-128," *Quantum Inf. Process.*, vol. 17, no. 5, pp. 1–30, May 2018, doi: 10.1007/s11128-018-1864-3.

[16] R. Anand, S. Maitra, A. Maitra, C. S. Mukherjee, and S. Mukhopadhyay, "Resource estimation of grovers-kind quantum cryptanalysis against FSR based symmetric ciphers," Cryptology ePrint Archive, Rep. 2020/1438, 2020. [Online]. Available: https://eprint.iacr.org/2020/1438

[17] K. Jang, S. Choi, H. Kwon, H. Kim, J. Park, and H. Seo, "Grover on Korean block ciphers," *Appl. Sci.*, vol. 10, no. 18, 2020, Art. no. 6407. [Online]. Available: https://www.mdpi.com/2076-3417/10/18/6407

[18] K. Jang, H. Kim, S. Eum, and H. Seo, "Grover on gift," Cryptology ePrint Archive, Rep. 2020/1405, 2020. [Online]. Available: https://eprint.iacr.org/2020/1405

[19] G. Banegas, D. J. Bernstein, I. van Hoof, and T. Lange, "Concrete quantum cryptanalysis of binary elliptic curves," *IACR Trans. Cryptographic Hardware Embedded Syst.*, vol. 2021, no. 1, pp. 451–472, Dec. 2020. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8741

[20] 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*, R. Avanzi and H., Eds. Cham, Switzerland: Springer Int. Publishing, 2017, pp. 317–337, doi: 10.1007/978-3-319-69453-5_18.

[21] O. D. Matteo, V. Gheorghiu, and M. Mosca, "Fault-tolerant resource estimation of quantum random-access memories," *IEEE Trans. Quantum Eng.*, vol. 1, 2020, Art. no. 4500213, doi: 10.1109/TQE.2020.2965803.

[22] M. Appel *et al.*, "Block ciphers for the IoT-SIMON, SPECK, KATAN, LED, TEA, PRESENT, and SEA compared," 2016. [Online]. Available: https://download.hrz.tu-darmstadt.de/pub/FB20/Dekanat/Publikationen/CDC/2016-09-05_TR_SimonSpeckKatanLedTeaPresentSea.pdf

[23] M. R. Albrecht and G. Leander, "An all-in-one approach to differential cryptanalysis for small block ciphers," in *Selected Areas in Cryptography*, L. R. Knudsen and H. Wu, Eds. Berlin, Germany:Springer, 2013, pp. 1–15, doi: 10.1007/978-3-642-35999-6_1.

[24] S. Knellwolf, W. Meier, and M. Naya-Plasencia, "Conditional differential cryptanalysis of NLFSR-based cryptosystems," in *Advances in Cryptology*, M. Abe, Ed. Berlin, Germany: Springer, 2010, pp. 130–145, doi: 10.1007/978-3-642-17373-8_8.

[25] S. Knellwolf, W. Meier, and M. Naya-Plasencia, "Conditional differential cryptanalysis of TRIVIUM and KATAN," in *Selected Areas in Cryptography*, A. Miri and S. Vaudenay, Eds. Berlin, Germany: Springer, 2012, pp. 200–212, doi: 10.1007/978-3-642-28496-0_12.

[26] B. Zhu and G. Gong, "Multidimensional meet-in-the-middle attack and its applications to KATAN32/48/64," *Cryptogr. Commun.*, vol. 6, no. 4, pp. 313–333, 2014, doi: 10.1007/s12095-014-0102-9.

[27] T. Isobe and K. Shibutani, "All subkeys recovery attack on block ciphers: Extending meet-in-the-middle approach," in *Selected Areas in Cryptography*, L. R. Knudsen and H. Wu, Eds. Berlin, Germany: Springer, 2013, pp. 202–221, doi: 10.1007/978-3-642-35999-6_14.

[28] T. Fuhr and B. Minaud, "Match box meet-in-the-middle attack against KATAN," in *Fast Software Encryption*, C. Cid and C. Rechberger, Eds. Berlin, Germany: Springer, 2015, pp. 61–81, doi: 10.1007/978-3-662-46706-0_4.

[29] A. Bogdanov and C. Rechberger, "A 3-subset meet-in-the-middle attack: Cryptanalysis of the lightweight block cipher KTANTAN," in *Selected Areas in Cryptography*, A. Biryukov, G. Gong, and D. R. Stinson, Eds. Berlin, Germany: Springer, 2011, pp. 229–240, doi: 10.1007/978-3-642-19574-7_16.

[30] T. Isobe, Y. Sasaki, and J. Chen, "Related-key boomerang attacks on KATAN32/48/64," in *Information Security and Privacy*, C. Boyd and L. Simpson, Eds. Berlin, Germany: Springer, 2013, pp. 268–285, doi: 10.1007/978-3-642-39059-3_19.

[31] J. Chen, J. S. Teh, C. Su, A. Samsudin, and J. Fang, "Improved (related-key) attacks on round-reduced KATAN-32/48/64 based on the extended boomerang framework," in *Information Security and Privacy*, J. K. Liu

and R. Steinfeld, Eds. Cham, Switzerland: Springer International, 2016, pp. 333–346, doi: 10.1007/978-3-319-40367-0_21.

[32] Z. Ahmadian, S. Rasoolzadeh, M. Salmasizadeh, and M. R. Aref, "Automated dynamic cube attack on block ciphers: Cryptanalysis of SIMON and KATAN," *IACR Cryptology ePrint Arch.*, vol. 2015, 2015, Art. no. 40. [Online]. Available: https://eprint.iacr.org/2015/040

[33] T. Isobe and K. Shibutani, "Improved all-subkeys recovery attacks on FOX, KATAN and SHACAL-2 block ciphers," in *Proc. 21st Int. Workshop Fast Softw. Encryption*, (Revised Selected Papers, Lecture Notes in Computer Science Series), C. Cid and C. Rechberger, Eds. vol. 8540. Berlin, Germany: Springer, 2014, pp. 104–126, doi: 10.1007/978-3-662-46706-0_6.

[34] D. Shi, L. Hu, S. Sun, and L. Song, "Linear (hull) cryptanalysis of round-reduced versions of KATAN," in *Proc. 2nd Int. Conf. Inf. Syst. Secur. Privacy*, 2016, pp. 364–371. [Online]. Available: https://www.scitepress.org/Documents/2016/57391/

[35] L. Sun, W. Wang, R. Liu, and M. Wang, "MILP-aided bit-based division property for ARX ciphers," *Sci. China Inf. Sci.*, vol. 61, no. 11, pp. 1–3, 2018, doi: 10.1007/s11432-017-9321-7.

[36] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "Implementing Grover oracles for quantum key search on AES and LowMC," in *Advances in Cryptology*, A. Canteaut and Y. Ishai, Eds. Cham, Switzerland: Springer International, 2020, pp. 280–310, doi: 10.1007/978-3-030-45724-2_10.

[37] D. S. Steiger, T. Häner, and M. Troyer, "ProjectQ: An open source software framework for quantum computing," *Quantum*, vol. 2, p. 49, Jan. 2018, doi: 10.22331/q-2018-01-31-49.

[38] T. Häner, D. S. Steiger, K. Svore, and M. Troyer, "A software methodology for compiling quantum programs," *Quantum Sci. Technol.*, vol. 3, no. 2, Feb. 2018, Art. no. 20501, doi: 10.1088/2058-9565/aaa5cc.

[39] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, "Tight bounds on quantum searching," Univ. Southern Denmark, Odense, Denmark, Tech. Rep., 1996.

[40] P. Kaye, R. Laflamme, and M. Mosca, *An Introduction to Quantum Computing*. Oxford, U.K.: Oxford Univ. Press, Inc., 2007.

[41] C. Zalka, "Grover's quantum searching algorithm is optimal," *Phys. Rev. A*, vol. 60, no. 4, pp. 2746–2751, Oct. 1999, doi: 10.1103/PhysRevA.60.2746.

[42] S. Jaques and J. M. Schanck, "Quantum cryptanalysis in the RAM Model: Claw-finding attacks on SIKE," in *Proc. Annu. Int. Cryptology Conf.*, vol. 11692, 2019, pp. 32–61, doi: 10.1007/978-3-030-26948-7_2.

[43] H. Buhrman, R. Cleve, M. Laurent, N. Linden, A. Schrijver, and F. Unger, "New limits on fault-tolerant quantum computation," in *Proc. 47th Annu. IEEE Symp. Found. Comput. Sci.*, 2006, pp. 411–419, doi: 10.1109/FOCS.2006.50.

[44] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Phys. Rev. A*, vol. 86, no. 3, Sep. 2012, Art. no. 032324, doi: 10.1103/PhysRevA.86.032324.

[45] M. Amy, D. Maslov, M. Mosca, and M. Roetteler, "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 32, no. 6, pp. 818–830, Jun. 2013, doi: 10.1109/TCAD.2013.2244643.

[46] J. Boyar, M. Find, and R. Peralta, "Small low-depth circuits for cryptographic applications," *Cryptogr. Commun.*, vol. 11, pp. 109–127, 2019, doi: 10.1007/s12095-018-0296-3.

[47] D. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: 10.1038/nature23461.

[48] D. J. Bernstein and B. Yang, "Asymptotically faster quantum algorithms to solve multivariate quadratic equations," in *Post-Quantum Cryptography*. Lecture Notes in Computer Science, vol. 10786, T. Lange and R. Steinwandt, Eds. New York, NY, USA: Springer, 2018, pp. 487–506, doi: 10.1007/978-3-319-79063-3_23.

[49] 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 Inf. Process.*, vol. 17, no. 12, Oct. 2018, doi: 10.1007/s11128-018-2107-3.

[50] P. Selinger, "Quantum circuits of T-depth one," *Phys. Rev. A*, vol. 87, 2013, Art. no. 042302, doi: 10.1103/PhysRevA.87.042302.

[51] C. Jones, "Low-overhead constructions for the fault-tolerant Toffoli gate," *Phys. Rev. A*, vol. 87, Feb. 2013, Art. no. 022328, doi: 10.1103/PhysRevA.87.022328.