Noname manuscript No.
(will be inserted by the editor)

Grover on Present: Quantum Resource Estimation

Mostafizar Rahman · Goutam Paul

Received: date / Accepted: date

Abstract In this work, we present cost analysis for mounting Grover's key search on Present block cipher. Reversible quantum circuits for Present are designed taking into consideration several decompositions of toffoli gate. This designs are then used to produce Grover oracle for Present and their implementations cost is comapred using several metrics. Resource estimation for Grover's search is conducted by employing these Grover oracles. Finally, gate cost for these designs are estimated considering NIST's depth restrictions.

Keywords Grover's algorithm · Present · Post-Quantum Cryptography · ProjectQ Implementation · Quantum Cryptanalysis

Mathematics Subject Classification (2020) 81P94

1 Introduction

Exploting the quantum-mechanical phenomena to solve computationally hard problems is the focus of researchers in the recent time which has lead to the development of Grover's search algorithm [25], Simon's algorithm [52], Shor's algorithm [50, 51], etc. Introduction of such algorithms threatens the security of cryptographic schemes. The most notable of these is the Shor's algorithm whose ability to solve the factorization problem and compute discrete logarithms in polynomial-time has unveiled the vulnerability of several public key cryptographic schemes, like, RSA, ECDSA and ECDH. Private key schemes are vulnerable to generic key recovery attacks due to implications of Grover's search algorithm on block ciphers [63]. Recently, the vulnerabilities posed by Simon's algorithm on some

M. Rahman
Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India.
E-mail: mrahman454@gmail.com

G. Paul
Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India.
E-mail: goutam.paul@isical.ac.in

specific symmetric key schemes have been studied [33, 34, 32, 14, 48, 23]. Thus the security of cryptographic algorithms are on the verge of being compromised due to the inevitability of the introduction of quantum computers. Owing to such conditions, National Institute of Standards and Technology (NIST) has called for proposals for post-quantum cryptography standardization with goals for standardizing new cryptographic algorithms that are secure against classical as well as quantum attacks [53]. They have put restrictions on the upper bound of the depth of the quantum circuit for mounting quantum attacks and called it `MAXDEPTH`. There is no restrictions on the width of the circuit.

Resource Estimation

For recovering the key of block ciphers, Grover's search provides square root speed up over classical brute force techniques. As a general rule of thumb, it is considered that the security threats of private key schemes posed by Grover's search algorithm can be avoided by doubling the key length. However, such notions only provide a general idea regarding the post-quantum security of block ciphers as the cost estimation of Grover oracle is not considered. Thus resource estimation for mounting Grover's search on block cipher gives a concrete idea about the security of such block ciphers in post-quantum world.

Moreover, due to the unpredictability of computing power of future quantum computers, NIST has proposed to measure security in terms of elementary operations, circuit size, etc rather than "bits of security" [53], as done in the case of evaluating security in the classical model. As of now, Grover's search is the only quantum algorithm that poses a threat to Present block cipher [13], estimating the resources for mounting the attack gives an idea regarding the efficiency of the attack. Recently, evaluations of security against quantum adversaries in terms of computational resources receive a substantial attention and studies are conducted in this regard to estimate resources required for mounting Grover's key search on symmetric key schemes [24, 36, 4, 7, 28, 29, 28, 29], Grover's search on hash functions [5], computing discrete logarithm on binary elliptic curve [9], etc.

Why Present?

Present [13] is an ultra-lightweight hardware-optimized block cipher specifically designed for area-constrained and power-constrained devices. Over the years, its efficient hardware performance along with strong security has prompted researchers to perform a lot of security analysis. There are several analysis on its round-reduced version; like, linear cryptanalysis [19, 46, 20, 15, 38, 2, 18, 37, 40, 42], differential cryptanalysis [56, 57, 41, 10, 59, 60], improbable differential attack [55], related-key differential attack [47, 21], algebraic cryptanalysis [35], fault attacks [43, 8, 58], differential power analysis [65], side channel cube attacks [64, 66], biclique cryptanalysis [45, 39, 3], integral attack [62], deep learning based distinguishers [27], known-key distinguishers [12], truncated differential attack [11], etc. However, except for the known key distinguisher, full Present block cipher is still impregnable to classical attacks. This motivates us to analyze the security of Present against quantum attacks. Like all other block ciphers, Present is also susceptible

to Grover's attack; but, it does not provide any concrete idea regarding the security of Present in the post-quantum world. Hence, estimating the resources for mounting Grover's attack on Present helps us to analyze its security more appropriately against quantum adversaries.

Our Contribution

This work provides several aspects regarding the implementation of Present block cipher using quantum gates and qubits. First, the round operations of Present are designed and implemented in ProjectQ [54, 26]. These implemented round operations are unit tested for validation of its correctness. Next, these operations are combined together to produce the quantum circuit for full Present block cipher. Several decompositions of toffoli gate are used in the implementations and corresponding quantum circuits are compared using cost metrics.

Next, the full implementations of Present is used to design Grover oracle for this cipher along with resource estimation computed using the ProjectQ framework. The resource estimation for mounting Grover's attack on Present using the Grover oracle along with the corresponding success probability is also computed. We also provide an estimation of the gate cost if NIST's `MAXDEPTH` limit is respected.

Organization

The rest of the paper is organized as follows. First, a brief introduction of the Present block cipher is provided in Section 2.1. Then, details regarding Grover's search algorithm is given in Section 2.2. Section 2.3 describes the mechanism of mounting Grover's attack on a block cipher. In Section 4.1 and Section 4.2 details regarding the design of quantum circuits for round operations and key scheduling algorithm is discussed. Resource estimation for complete implementation of Present is provided in Section 4.3. Section 5.1 illustrates the design of Grover oracle of Present and corresponding resource estimates. In Section 5.2, resource estimation for mounting Grover's key search on Present is given. Finally, the paper is summarized and the concluding remarks are furnished in Section 6.

2 Preliminaries

Here, a brief discussion about Present block cipher, Grover's algorithm and Grover's attack on block cipher is provided. In the rest of the paper, the total gate cost, depth and width of the quantum circuit are denoted by G, D and W respectively. The number of CNOT gates, 1-qubit clifford gates, T gates and measure gates are referred by #CNOT, #1qCliff, #T and #M respectively.

2.1 Present Block Cipher

Present [13] is a Substitution-Permutation network [44] based block cipher which has a block length of 64 bits. In terms of key size there are two variants- 80-bit

and 128-bit. Present contains 31 rounds and the round function is comprised of adding the round key (AddRoundKey), a linear bitwise permutation (pLayer) and a non-linear substitution layer (sBoxLayer).

– **AddRoundKey.** There are in total 32 round keys are used in Present. 31 round keys are used in 31 different rounds and the last one is used for post-whitening. Consider a round key $RK^i = k^i_{63} \cdots k^i_0$ for $1 \leq i \leq 32$ and state bits $a_{63} \cdots a_0$, then the *AddRoundKey* operation is defined as

$$a_j \leftarrow a_j \oplus k^i_j,$$

where $0 \leq j \leq 63$.

– **pLayer.** In this layer bits are permutated as shown in Table 1. A bit in position i is moved to a new position $P(i)$.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Table 1: Bit Permutation of Present

– **sBoxLayer.** Present uses a 4-bit to 4-bit s-box which is applied in parallel 16 times to the Present-state. The input to the s-box is 4 consecutive bits starting from the least significant bit. The input and output to the s-box is shown in Table 2.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 2: S-box of Present

Key Scheduling Algorithm (KSA).

There are two variants of Present on the basis of key- 80-bit and 128-bit variant. The two key scheduling algorithms are quite similar. Here, the a brief description regarding the two variants are provided.

KSA of 80-bit Key. Initially the key register is loaded with 80-bit supplied key. Let us consider the contents of the key register K is $\kappa_{79}\kappa_{78}\cdots\kappa_1\kappa_0$. In each round the key register is updated in the following way-

1. The key register is left rotated by 61 bits, *i.e*, $[\kappa_{79}\kappa_{78}\cdots\kappa_1\kappa_0] = [\kappa_{18}\kappa_{17}\cdots\kappa_{20}\kappa_{19}]$.
2. S-box is applied on the leftmost 4 bits, *i.e*, $[\kappa_{79}\kappa_{78}\kappa_{77}\kappa_{76}] = S[\kappa_{79}\kappa_{78}\kappa_{77}\kappa_{76}]$.
3. Round Counter is XOR-ed with κ_{19}, κ_{18}, κ_{17}, κ_{16} and κ_{15}.

In each round, the key bits $\kappa_{79}\kappa_{78}\cdots\kappa_{16}$ are used as round key bits.

KSA of 128-bit Key. Initially the key register is loaded with 128-bit supplied key. Let us consider the contents of the key register K is $\kappa_{127}\kappa_{126}\cdots\kappa_1\kappa_0$. The key bits $\kappa_{127}\kappa_{126}\cdots\kappa_{64}$ constitutes the round key for each round. In each round, the key register is updated in the following way-

1. The key register is left rotated by 61 bits, *i.e*,
$$[\kappa_{127}\kappa_{126}\cdots\kappa_1\kappa_0] = [\kappa_{66}\kappa_{65}\cdots\kappa_{68}\kappa_{67}].$$
2. Two s-boxes are applied on the leftmost 8 bits, *i.e*,
   (a) $[\kappa_{127}\kappa_{126}\kappa_{125}\kappa_{124}] = S[\kappa_{127}\kappa_{126}\kappa_{125}\kappa_{124}]$
   (b) $[\kappa_{123}\kappa_{122}\kappa_{121}\kappa_{120}] = S[\kappa_{123}\kappa_{122}\kappa_{121}\kappa_{120}]$
3. Round Counter is XOR-ed with κ_{66}, κ_{65}, κ_{64}, κ_{63} and κ_{62}.

2.2 Grover's Search Algorithm.

Grover's algorithm [25] is used for searching in a completely unstructured dataset. Consider a function $f : \{0,1\}^n \to \{0,1\}$ ($N = 2^n$) and there exists a state w such that

$$f(x) = \begin{cases} 1, & \text{for } x = w \\ 0, & \text{for } x \neq w. \end{cases}$$

Suppose, f can be realized using a black-box reversible function B_f, where

$$B_f|x\rangle|a\rangle = |x\rangle|f(x) \oplus a\rangle,\ \forall x \in \{0,1\}^n \text{and } a \in \{0,1\}.$$

The problem is to find a x such that $f(x) = 1$. Any deterministic classical algorithm can solve the problem by querying the function $O(2^n)$ times. However, leveraging on quantum computing techniques, Grover's algorithm can solve the problem by making $O(\sqrt{2^n})$ queries; which is a significant speed-up in comparison to the classical counterpart.

Before describing Grover's algorithm, consider two unitary maps on n qubits, $U_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$ and $U : |x\rangle \mapsto (-1)^{g(x)}|x\rangle$, where the function $g : \{0,1\}^n \to \{0,1\}$ is defined as

$$g(x) = \begin{cases} 1, & \text{for } x = 0^n \\ 0, & \text{for } x \neq 0^n. \end{cases}$$

Fig. 1 shows the implementation of U_f using the black-box B_f and an ancillary qubit by employing the phase kick-back phenomenon. Classically, $g(x)$ can be realized by computing $(\overline{x}_0 \wedge \overline{x}_1 \cdots \wedge \overline{x}_{n-1})$, where x_i corresponds to $(i+1)^{\text{th}}$ bit of

x. Thus, U can be implemented by replacing B_f with a reversible quantum circuit for the following map:

$$|x\rangle|a\rangle \mapsto |x\rangle|a \oplus (\overline{x}_0 \wedge \overline{x}_1 \cdots \wedge \overline{x}_{n-1})\rangle.$$

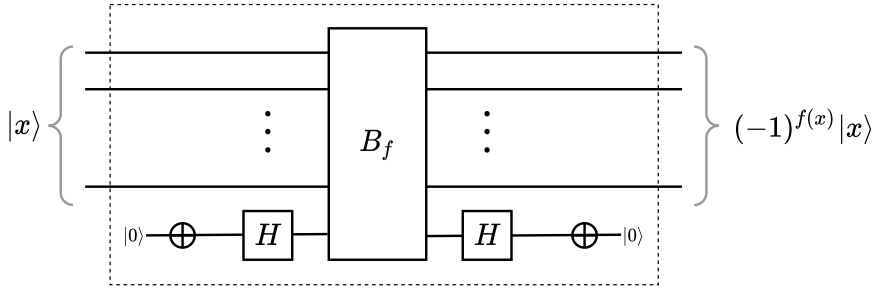


Fig. 1: Implementation of U_f using B_f

Now, Grover operator G is defined as $U_{\psi^\perp}U_f$ where $U_{\psi^\perp} = H^{\otimes n}UH^{\otimes n}$. Based on this, the steps of Grover's algorithm is shown in Algorithm 1.

Algorithm 1 Grover's Algorithm

1. An n-qubit register Z is initialized. Hadamard transformation $H^{\otimes n}$ is applied on Z.
2. Grover operator G is applied $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ times to the register Z.
3. Z is measured and the result is output.

Consider instead of iterating $\lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ times, G is iterated k times in Step 2 of Algorithm 1. Two superposition states $|U\rangle$ and $|V\rangle$ are defined as

$$|U\rangle = \frac{1}{\sqrt{u}} \sum_{x \in U} |x\rangle$$

$$|V\rangle = \frac{1}{\sqrt{v}} \sum_{x \in V} |x\rangle$$

where $U = \{x \in \{0,1\}^n : f(x) = 1\}$, $u = |U|$ and $V = \{x \in \{0,1\}^n : f(x) \neq 1\}$, $u = |V|$. Based on this, following proposition can be stated.

Proposition 1 ([25, 61]) *As hadamard operation is applied in Step 1 of Algorithm 1, the state is in the superposition* $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$. *After application of* k *iterations in Step 2, the resulting superposition of the state is*

$$sin((2k+1)\theta)|U\rangle + cos((2k+1)\theta)|V\rangle,$$

where $\theta = sin^{-1}\sqrt{\frac{u}{N}}$.

Note that, in this case $u = 1$, as it is assumed that only when $x = w$, $f(x) = 1$. However, Proposition 1 holds for any arbitary value of u. From Proposition 1, it can be concluded that after the measurement in Step 3, a right/correct state is output by Grover's algorithm with probability $|sin((2k+1)\theta)|^2$. When $k = \lfloor \frac{\pi}{4}\sqrt{N/u} \rfloor$, a state from U is measured with probability at least $\frac{1}{2}$ [25, 16]. Now, the technique of mounting key recovery attack on block ciphers using Grover's search is discussed.

2.3 Key Recovery Attack on Block Cipher using Grover's Algorithm.

Yamamura and Ishizuka have shown that Grover's algorithm can be used to mount key recovery attack on a block cipher [63]. This attacks is generic as it does not rely on the construction of the block cipher. Consider a block cipher E which uses a k-bit key $\mathcal{K}$ and its block length is n. The encryption of a message m by block cipher E using the key $\mathcal{K}$ is denoted by $E_{\mathcal{K}}(m)$. Algorithm 2 shows the steps of mounting Grover's attack on E.

Algorithm 2 Grover's Attack on Block Cipher

1. A plaintext-ciphertext pair (P, C) is prepared where $C = E_{\mathcal{K}}(P)$. The function f is defined as
$$f(x) = \begin{cases} 1 \text{ if } E_x(P) = C \\ 0 \text{ if } E_x(P) \neq C \end{cases}$$
2. A k-qubit register Z is initialized. Hadamard transformation $H^{\otimes n}$ is applied on Z to obtain
$$\frac{1}{\sqrt{2^k}} \sum_{x \in \{0,1\}^k} |x\rangle.$$
3. Grover operator G is applied $\lfloor \frac{\pi}{4}\sqrt{2^k} \rfloor$ times to the register Z.
4. Z is measured and the right key $\mathcal{K}$ is obtained with probability at least $\frac{1}{2}$.

3 Design Rationale

While designing the quantum circuits for Present, several rationales have been considered. Here, those design rationales are discussed.

3.1 Depth Constraints and Resource Estimation

A parameter `MAXDEPTH` is introduced by NIST in its call for the Post Quantum Cryptography standardization [53] to limit the run time of long serial computations. Once a circuits reaches this depth, prallelization of the circuit becomes inevitable. Here, the values of `MAXDEPTH` that are considered are 2^{40}, 2^{64} and 2^{96}. All these values conforms to NIST's `MAXDEPTH` limit.

For resource estimation, the circuits are implemented in ProjectQ [54, 26] framework and the resource estimation is carried out using the resource estimation function of ProjectQ in a fully automated way.

3.2 Cost Metrics

In [31], two cost metrics are proposed for analysing the cost of a given circuit. Consider a quantum circuit that has a depth and width of D and W and 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. In this work, these two cost metrics are used for cost analysis.

3.3 Decomposition of Toffoli Gate

For a fair comparison with other related works, the quantum circuits are required to be designed using Clifford+T gate set. However, in several occasions in this work, toffoli gates are used to realize the quantum circuits. In such cases, decomposition of the toffoli gates using Clifford+T gate set becomes necessary. For that purpose, three decompositions are followed in this work.

First, the default decomposition of toffoli gates into Clifford+T set employed in ProjectQ framework is considered. This decomposition uses seven T gates, three 1-qubit clifford gates and three qubits.

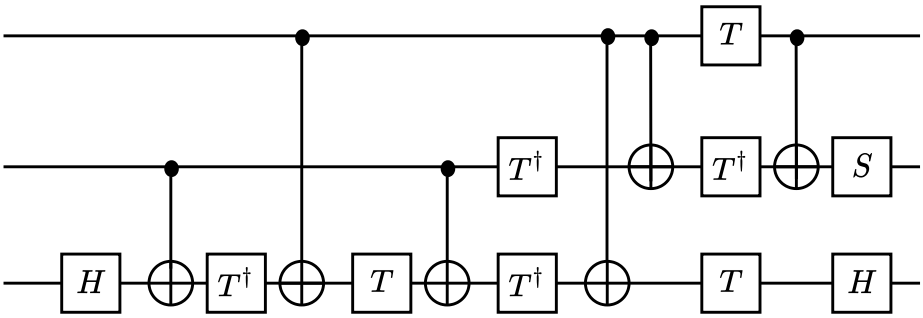


Fig. 2: Decomposition of Toffoli gate into Clifford+T Set with T-depth of 4

Next, consider the decomposition of toffoli gate into Clifford+T gate set provided by Amy *et al.* [6] shown in Fig 3. This decomposition uses 6 CNOT gates, 7 T gates, 3 clifford gates and its T-depth is 3. It is conjectured that T-depth of 3 is optimal for quantum circuits without ancillas obtained through the decomposition of toffoli gate [6].

Selinger gives a representation of toffoli gate using clifford + T gate of T-depth 1 [49] which is shown in Fig. 4. Along with lower T-depth, this representation has lower depth than the representation in Fig. 3 but it uses some ancilla qubits; hence the width is increased.

4 A Quantum Circuit on Present

The implementation of Present in ProjectQ is discussed in this section. First of all, reversible quantum circuit for round operations (AddRoundKey, pLayer,

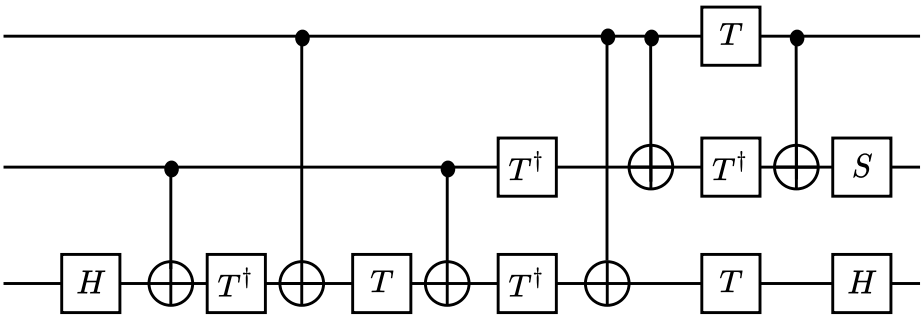


Fig. 3: Decomposition of toffoli gate into Clifford+T Set with T-depth of 3

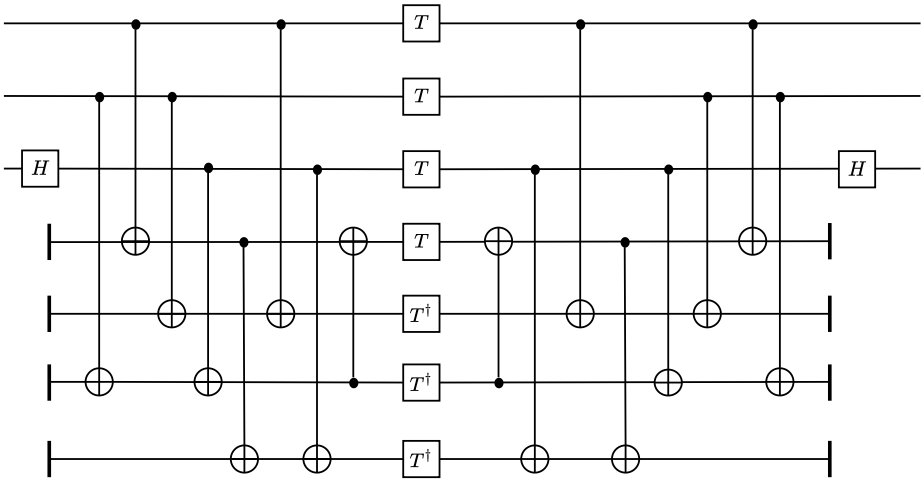


Fig. 4: Decomposition of toffoli gate into Clifford+T Set with T-depth 1

sBoxLayer) and key scheduling algorithm are designed. Then this circuits are combined together to obtain a reversible quantum circuit for Present block cipher.

4.1 Designing the Round Operations

Each round of Present is constituted of three operations, namely, AddRoundKey, pLayer and sBoxLayer and the complete Present block cipher is comprised of 31 such rounds. For both variant of Present the block length is 64 bits. Hence, same quantum circuit for operation is valid for both variants. Here, a reversible quantum circuit for each round operation is provided.

AddRoundKey.

This operation consists of XOR-ing of a 64-bit round key to the internal state of Present. This operation can be realized in the quantum circuit by using 64 CNOT gates where the key bits acts as control bits and internal state bits are target bits.

pLayer.

This operation is a linear permutation of the state bits which can be realized using SWAP gates. However, in ProjectQ, we explicitly do not use SWAP gates to implement the pLayer; instead input to each s-box is maintained based on the output of pLayer and ProjectQ internally use SWAP gates to bring inputs to each s-box to a neighborhood. Thus pLayer is implicitly realized in the implementation.

sBoxLayer.

Present uses 4×4-bit s-box. The input and output of the s-box are shown in Table 2. `Revkit` [1] is integrated into ProjectQ to find reversible logic by using automated synthesis routines. `PermutationOracle` operation of the `Revkit` library is used to synthesis a reversible circuit for a permutation. As the s-box of Present is permutation over 2^4 elements, `PermutationOracle` automatically finds a reversible circuit over 4 qubits to realize the permutation. The circuit is generated using toffoli gates, CNOT gates and NOT gates. However, instead of using toffoli gates, its equivalent decomposition using 1-qubit clifford + T set is considered. Quantum circuit of the s-box using toffoli gates is shown in Algorithm 3. Note that, $Tof(a, b, c)$ denotes the application of tofolli gate on target qubit c using the control qubit a and b; $CNOT(a, b)$ denotes application of CNOT gate on target qubit b using the control qubit a; and $X(a)$ denotes the application of NOT gate on qubit a. Fig. 5 shows the circuit of Present s-box using toffoli gates. This s-box circuit uses 19 toffoli gates, 5 CNOT gates and 2 NOT gates. However, to realize the circuits using 1-qubit clifford + T set, CNOT gates and NOT gates, several decompositions of toffoli gates (discussed in Section 3.3) are considered.

In Table 3, resource requirement for Present s-box under various decompositions are listed. It is clearly evident that by using toffoli gate of T-depth 1, T-depth as well as overall depth of the circuit decreases significantly; whereas the width of the circuit also increases significantly. As restrictions on width are not considered in NIST's call for proposal for post-quantum cryptography [53, §4.A.5], decomposition of the s-box using toffoli gate of depth 1 become interesting, in particular, for its lower depth. The quantum circuits for the s-box are unit tested in ProjectQ for its correctness.

4.2 Key Scheduling.

There are two variants of Present block cipher on the basis of key size- 80-bit key and 128-bit key. Round operation of KSA of both the variant consists of a rotation operation, XOR-ing of a 5-bit round counter and application of s-box to some bits. For the 80-bit variant, in each round a single s-box is applied; whereas two s-boxes are applied on 8 bits for the 128-bit variant. For designing the quantum

Algorithm 3 Quantum Circuit for S-box of Present

INPUT: Qubits: q_0, q_1, q_2, q_3 where q_3 is the most significant qubit and q_0 is the least sigificant qubit

1. Initialize an ancillary register ANC with 4 qubits
2. $Tof(q_0, q_1, ANC[0])$
3. $Tof(ANC[0], q_3, q_1)$
4. $Tof(q_0, q_2, ANC[0])$
5. $Tof(q_0, q_1, ANC[1])$
6. $Tof(q_2, ANC[1], q_3)$
7. $Tof(q_0, q_1, ANC[1])$
8. $CNOT(q_3, q_2)$
9. $Tof(q_0, q_3, q_1)$
10. $Tof(q_0, q_2, ANC[2])$
11. $Tof(ANC[2], q_3, q_1)$
12. $Tof(q_0, q_2, ANC[2])$
13. $Tof(q_0, q_1, ANC[3])$
14. $Tof(ANC[3], q_3, q_2)$
15. $Tof(q_0, q_1, ANC[3])$
16. $Tof(q_3, q_2, q_0)$
17. $Tof(q_3, q_2, q_1)$
18. $Tof(q_3, q_1, q_2)$
19. $Tof(q_3, q_2, q_1)$
20. $Tof(q_2, q_1, q_0)$
21. $CNOT(q_2, q_0)$
22. $CNOT(q_2, q_3)$
23. $Tof(q_0, q_1, q_2)$
24. $CNOT(q_1, q_3)$
25. $CNOT(q_0, q_3)$
26. $X(q_2)$
27. $X(q_3)$
28. Measure q_3, q_2, q_1, q_0 for the output of the s-box

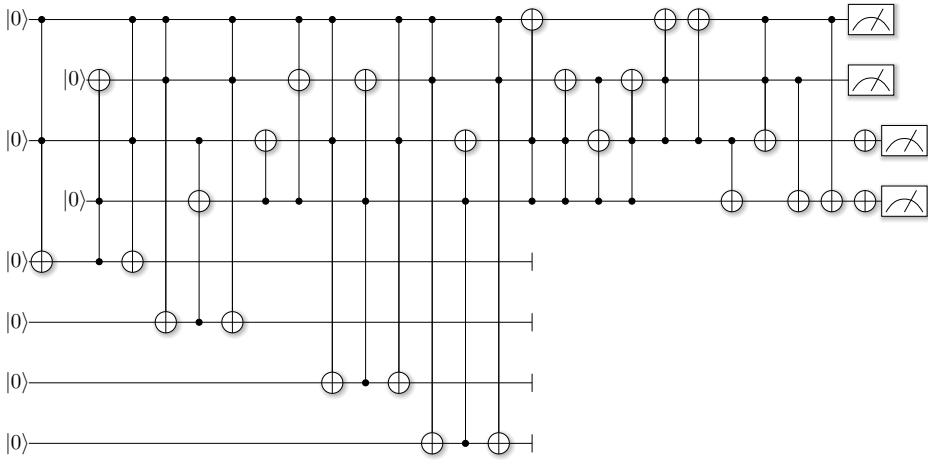


Fig. 5: Quantum Circuit for Present S-box using toffoli Gate

circuit, XOR-ing of round counter can be realized by using the CNOT gate where counter bits are the control bits and corresponding key bits acts as target. In

-

Decomposition	#CNOT	#1qCliff	#T	#M	T-Depth	Full Depth	Width
T-Depth 4	119	36	133	4	63	190	8
T-Depth 3	138	59	133	4	34	177	8
T-Depth 1	309	36	133	4	19	139	84

Table 3: Quantum Resources Required for Present S-box for Several Decompositions

ProjectQ, XOR-ing of round counter is realized by using `AddConstant` operation. The rotation operation is not explicitly implemented; rather application of s-box and XOR-ing of round counter on corresponding qubits are controlled. ProjectQ internally uses `SWAP` gate to realize the rotation operation. Fig.6 shows the quantum circuit for the KSA of 80-bit key. In terms of resource requirement, 128-bit KSA is quite similar with the 80-bit KSA; only difference is the extra usage of a s-box in each round of 128-bit KSA. Resource requirement for realisation of KSA in quantum circuit under several kind of synthesis is listed in Table 4. In quantum circuit for KSA, T gates are required only for designing the s-box. As the number of s-boxes used in 128-bit KSA is twice the number of s-boxes used in 80-bit KSA, the number of T-gates is double for 128-bit KSA with respect to 80-bit KSA when similar decomposition of toffoli gate is cosidered.

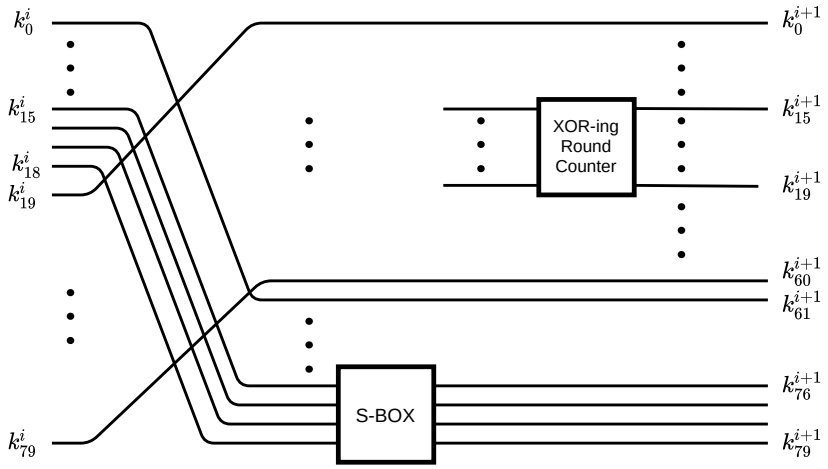


Fig. 6: Present Key Scheduling Function of 80-bit Key

Key Size	Decomposition of Toffoli Gate	#CNOT	#1qCliff	#T	T-Depth	Full Depth	Width
80-bit	T-Depth 4	119	71	133	63	189	148
	T-Depth 3	138	90	133	57	176	164
	T-Depth 1	309	71	133	19	138	224
128-bit	T-Depth 4	238	107	266	65	189	200
	T-Depth 3	276	145	266	57	176	200
	T-Depth 1	618	107	266	19	138	352

Table 4: Resource Estimation for Key Scheduling Algorithm of Present

4.3 Implementation of Full Present

Now, a reversible quantum circuit for full Present is designed. Quantum circuits for round operations and key scheduling algorithm are combined to obtain the quantum circuit for the complete Present block cipher. The resource estimation for the reversible circuit considering the different decompositions of the toffoli gate are listed in Table 5.

Key Size	Decomposition of Toffoli Gate	#CNOT	#1qCliff	#T	T-Depth	Full Depth	Width
80-bit	T-Depth 4	64761	19912	70091	2010	6004	2316
	T-Depth 3	74774	29925	70091	1818	5619	2316
	T-Depth 1	164891	19912	70091	606	4407	42368
128-bit	T-Depth 4	68450	21028	74214	2015	5833	2488
	T-Depth 3	79052	31630	74214	1767	5461	2488
	T-Depth 1	174470	21028	74214	589	4283	44896

Table 5: Resource Estimation for Reversible Quantum Circuit of Present

4.4 Comparison using Cost Metrics

The proposed designs can be compared using the cost metrics discussed in Section 3.2. Along with the G-cost and DW-cost, the full depth of all the proposed quantum circuits for Present are listed in Table 6. Although, the circuits designed using the toffoli gates of T-depth 1 have lowest depth, but their G-cost and DW-cost is the highest among all the designs. In comparison to toffoli gates of T-depth 4, the overall depth of toffoli gates of T-depth 3 is lower without using any ancillary qubits at the expense of using more quantum gates. And thus the circuits designed using toffoli gates of T-depth 3 have lowest DW-cost; whereas the circuits designed using the toffoli gates of T-depth 4 have lowest G-cost. Toffoli gates

of T-depth 1 uses more qubits and gates to reduce the depth and T-depth; and thus the G-cost and DW-cost of the corresponding quantum circuits of Present are high.

Decomposition of	Present-80			Present-128		
Toffoli Gate	D	G	DW	D	G	DW
T-depth 4	$2^{12.55}$	$2^{17.24}$	$2^{23.73}$	$2^{12.51}$	$2^{17.32}$	$2^{23.79}$
T-depth 3	$2^{12.46}$	$2^{17.42}$	$2^{23.63}$	$2^{12.41}$	$2^{17.5}$	$2^{23.7}$
T-depth 1	$2^{12.11}$	$2^{17.96}$	$2^{27.48}$	$2^{12.06}$	$2^{18.04}$	$2^{27.52}$

Table 6: Comparison of Reversible Quantum Circuit of Present using G-cost Metric and DW-cost Metric

5 Quantum Resource Estimation of Grover on Present

Now, using the proposed quantum circuit of Present, a concrete resource estimation is conducted for mounting Grover's attack on Present block cipher. First, Grover oracle is designed for Present to mount grover search. Then, based on the design of Grover oracle, resources required to perform a key recovery attack on Present is estimated. Finally, due to NIST's restriction on depth-limit, cost-estimation under depth restrictions is conducted.

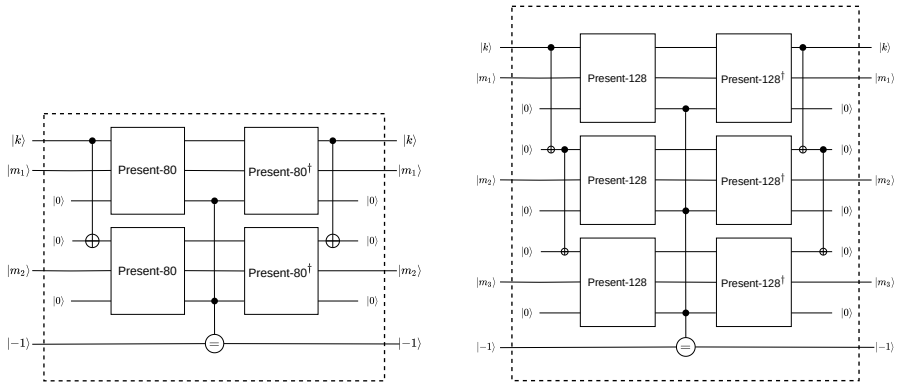
5.1 Resource Estimation of Grover Oracle

Here, quantum circuit for Grover oracle of Present is designed. While designing the Grover oracle, the number of plaintext-ciphertext pairs are required to recover the right key uniquely needs to be determined. Jaques *et al.* shows that for a block cipher with block length of n-bit and key length of k-bit, if r plaintext-ciphertext pairs are used, then $r \geq \lceil \frac{k}{n} \rceil$ [30]. In such case, then the probability of uniquely recovering the correct key is $e^{-2^{k-rn}}$ [30].

For Present-80, $n = 64$ and $k = 80$; thus $r \geq \lceil \frac{80}{64} \rceil \implies r \geq 2$ and the probability of finding a unique key is 0.99 for $r = 2$. For Present-128, $n = 64$ and $k = 128$; so, $r \geq 2$ and the success probability is 0.36 for $r = 2$. For $r = 3$, the success probability for Present-128 is 0.99. Grover oracle for Present-80 and Present-128 is shown in Fig. 7a and Fig. 7b respectively. Table 7 lists the resources required to design the Grover oracle with their corresponding success probabilities.

5.2 Resource Estimation of Grover's Search

To mount key recovery attack on a block cipher using Grover's search, $\lfloor \frac{\pi}{4} 2^{k/2} \rfloor$ iterations of Grover operator G is required. While estimating the resources, cost incurred by the operator U_f is considered only; cost imposed by the operator $U_{\psi^\perp}$



(a) Grover Oracle for Present-80 (b) Grover Oracle for Present-128

Fig. 7: Grover Oracle of Present Block Cipher

Key Size	r	p_s	Decomposition of Toffoli Gate	#CNOT	#1qCliff	$\#T$	T-Depth	Full Depth	Width
80-bit	2	0.99	T-depth 4	259588	79712	280812	4049	11999	8912
			T-depth 3	299640	99242	300838	4120	11248	8912
			T-depth 1	660108	79712	280812	1216	8824	169120
128-bit	2	0.36	T-depth 4	274248	84136	297248	3941	11673	9448
			T-depth 3	316656	105344	318448	4003	10932	9448
			T-depth 1	698392	84152	297304	1182	8576	179080
128-bit	3	0.99	T-depth 4	412020	126428	446544	3948	11694	14176
			T-depth 3	475632	158240	478344	4010	10953	14176
			T-depth 1	1048236	126452	446628	1189	8597	268624

Table 7: Resource Estimation for Grover Oracle of Present. p_s denotes the Success Probability of Recovering the Right Key Uniquely.

is ignored. In this case, no restriction on depth limit is considered and assumed that Grover operator is applied in serial. Hence, to estimate the resources of mounting Grover's search, the resources (except width) in Table 7 are multiplied by $\lfloor \frac{\pi}{4} 2^{k/2} \rfloor$. As it is assumed that no parallelization is involved, so width remains the same as in Grover oracle. Resource estimation for mounting Grover's search is listed in Table 8.

Table 9 compares between the circuits used for mounting Grover's search on Present proposed in this paper. It can be concluded from the table that using low-depth toffoli gate is a costly affair for mounting key recovery attack on Present.

Key Size	r	p_s	Decomposition of Toffoli Gate	#CNOT	#1qCliff	$\#T$	T-Depth	Full Depth	Width
80-bit	2	0.99	T-depth 4	$2^{57.64}$	$2^{55.93}$	$2^{57.75}$	$2^{51.63}$	$2^{53.2}$	$2^{13.12}$
			T-depth 3	$2^{57.84}$	$2^{56.25}$	$2^{57.85}$	$2^{51.66}$	$2^{53.11}$	$2^{13.12}$
			T-depth 1	$2^{58.98}$	$2^{55.93}$	$2^{57.75}$	$2^{49.9}$	$2^{52.76}$	$2^{17.37}$
128-bit	2	0.36	T-depth 4	$2^{81.72}$	$2^{80.01}$	$2^{81.83}$	$2^{75.6}$	$2^{77.16}$	$2^{13.21}$
			T-depth 3	$2^{81.92}$	$2^{80.34}$	$2^{81.93}$	$2^{75.62}$	$2^{77.07}$	$2^{13.21}$
			T-depth 1	$2^{83.06}$	$2^{80.01}$	$2^{81.83}$	$2^{73.86}$	$2^{76.72}$	$2^{17.45}$
128-bit	3	0.99	T-depth 4	$2^{82.3}$	$2^{80.6}$	$2^{82.42}$	$2^{75.6}$	$2^{77.16}$	$2^{13.79}$
			T-depth 3	$2^{82.51}$	$2^{80.92}$	$2^{82.52}$	$2^{75.62}$	$2^{77.07}$	$2^{13.79}$
			T-depth 1	$2^{83.65}$	$2^{80.6}$	$2^{82.42}$	$2^{73.87}$	$2^{76.72}$	$2^{18.04}$

Table 8: Resource Estimation for Grover Search on Present

Decomposition of	Present-80, r=2			Present-128, r=2			Present-128, r=3		
Toffoli Gate	D	G	DW	D	G	DW	D	G	DW
T-depth 4	$2^{53.2}$	$2^{58.89}$	$2^{66.32}$	$2^{77.16}$	$2^{82.97}$	$2^{90.37}$	$2^{77.16}$	$2^{83.56}$	$2^{90.95}$
T-depth 3	$2^{53.11}$	$2^{59.07}$	$2^{66.33}$	$2^{77.07}$	$2^{83.15}$	$2^{90.28}$	$2^{77.07}$	$2^{83.74}$	$2^{90.86}$
T-depth 1	$2^{52.76}$	$2^{59.61}$	$2^{70.13}$	$2^{76.72}$	$2^{83.69}$	$2^{94.17}$	$2^{76.72}$	$2^{84.28}$	$2^{94.76}$

Table 9: Comparison of Quantum Circuit for Grover Search on Present using G-cost Metric and DW-cost Metric

5.3 Cost Estimation under a Depth Limit

In Table 8, the values are computed without considering any restriction on the depth of the circuit. However, NIST has put restriction on the maximum depth of the circuit (`MAXDEPTH`) in its call for the proposal for post-quantum cryptography standardization [53]. The minimum and maximum plausible value of `MAXDEPTH` is 2^{40} and 2^{96} respectively. The restriction on depth-limit alters the total gate cost of mounting key search. Consider, a non-parallel circuit for Grover's search have G gate cost and D depth. If Grover's search is parallelized by restricting the depth-limit to `MAXDEPTH`, then the modified gate cost is $GD/$`MAXDEPTH` [53]. Table 10 lists the gate cost of Grover's search under the depth restriction.

6 Conclusion

In this work, resource estimates for mounting Grover's attack on Present is done in a fully automated way by using the ProjectQ framework. It is observed that using low-depth decompositions of toffoli gate may increase the overall G-cost as well as DW-cost significantly. Circuits for Grover oracle designed using toffoli gates of T-depth 4 has the lowest G-cost; whereas Grover oracle for Present-128 designed using toffoli gates of T-depth 3 have lowest DW-cost.

Decomposition of Toffoli Gate	Variant	r	GD	MAXDEPTH		
				2^{40}	2^{64}	2^{96}
T-depth 4	Present-80	2	$2^{112.09}$	$2^{72.09}$	$2^{48.09}$	$2^{16.09}$
	Present-128	2	$2^{160.13}$	$2^{120.13}$	$2^{96.13}$	$2^{64.13}$
	Present-128	3	$2^{160.72}$	$2^{120.72}$	$2^{96.72}$	$2^{64.72}$
T-depth 3	Present-80	2	$2^{112.18}$	$2^{72.18}$	$2^{48.18}$	$2^{16.18}$
	Present-128	2	$2^{160.22}$	$2^{120.22}$	$2^{96.22}$	$2^{64.22}$
	Present-128	2	$2^{160.81}$	$2^{120.81}$	$2^{96.81}$	$2^{64.81}$
T-depth 1	Present-80	2	$2^{112.37}$	$2^{72.37}$	$2^{48.37}$	$2^{16.37}$
	Present-128	2	$2^{160.41}$	$2^{120.41}$	$2^{96.41}$	$2^{64.41}$
	Present-128	2	2^{161}	2^{121}	2^{97}	2^{65}

Table 10: Gate Cost for Grover's Search on Present with Depth Limit

References

1. Revkit. https://msoeken.github.io/revkit.html
2. Abdelraheem, M.A.: Estimating the Probabilities of Low-Weight Differential and Linear Approximations on PRESENT-Like Ciphers. In: T. Kwon, M.K. Lee, D. Kwon (eds.) Information Security and Cryptology – ICISC 2012, pp. 368–382. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
3. Abed, F., Forler, C., List, E., Lucks, S., Wenzel, J.: Biclique Cryptanalysis Of PRESENT, LED, And KLEIN. Cryptology ePrint Archive, Report 2012/591 (2012). https://eprint.iacr.org/2012/591
4. Almazrooie, M., Samsudin, A., Abdullah, R., Mutter, K.N.: Quantum Reversible Circuit of AES-128. Quantum Information Processing **17**(5), 1–30 (2018). DOI 10.1007/s11128-018-1864-3. URL https://doi.org/10.1007/s11128-018-1864-3
5. Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., Schanck, J.: Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3. In: R. Avanzi, H. Heys (eds.) Selected Areas in Cryptography – SAC 2016, pp. 317–337. Springer International Publishing, Cham (2017)
6. Amy, M., Maslov, D., Mosca, M., Roetteler, M.: A Meet-in-the-Middle Algorithm for Fast Synthesis of Depth-Optimal Quantum Circuits. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **32**(6), 818–830 (2013). DOI 10.1109/tcad.2013.2244643. URL http://dx.doi.org/10.1109/TCAD.2013.2244643
7. Anand, R., Maitra, S., Maitra, A., Mukherjee, C.S., Mukhopadhyay, S.: Resource Estimation of Grovers-kind Quantum Cryptanalysis against FSR based Symmetric Ciphers. Cryptology ePrint Archive, Report 2020/1438 (2020). https://eprint.iacr.org/2020/1438
8. Bagheri, N., Ebrahimpour, R., Ghaedi, N.: New differential fault analysis on PRESENT. EURASIP Journal on Advances in Signal Processing **2013**(1), 145 (2013). DOI 10.1186/1687-6180-2013-145. URL https://doi.org/10.1186/1687-6180-2013-145
9. Banegas, G., Bernstein, D.J., van Hoof, I., Lange, T.: Concrete Quantum Cryptanalysis of Binary Elliptic Curves. IACR Transactions on Cryptographic Hardware and Embedded Systems **2021**(1), 451–472 (2020). DOI 10.46586/tches.v2021.i1.451-472. URL https://tches.iacr.org/index.php/TCHES/article/view/8741
10. Blondeau, C.: B.: Links between theoretical and effective differential probabilities: Experiments on present. In: In: TOOLS'10. (2010)
11. Blondeau, C., Nyberg, K.: Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. In: P.Q. Nguyen, E. Oswald (eds.) Advances in Cryptology – EUROCRYPT 2014, pp. 165–182. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
12. Blondeau, C., Peyrin, T., Wang, L.: Known-Key Distinguisher on Full PRESENT. In: R. Gennaro, M. Robshaw (eds.) Advances in Cryptology – CRYPTO 2015, pp. 455–474. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)

13. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, CHES '07, p. 450–466. Springer-Verlag, Berlin, Heidelberg (2007). DOI 10.1007/978-3-540-74735-2_31. URL https://doi.org/10.1007/978-3-540-74735-2_31
14. Bonnetain, X., Hosoyamada, A., Naya-Plasencia, M., Sasaki, Y., Schrottenloher, A.: Quantum Attacks Without Superposition Queries: The Offline Simon's Algorithm. In: S.D. Galbraith, S. Moriai (eds.) Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I, *Lecture Notes in Computer Science*, vol. 11921, pp. 552–583. Springer (2019). URL https://doi.org/10.1007/978-3-030-34578-5_20
15. Borghoff, J., Knudsen, L.R., Leander, G., Thomsen, S.S.: Cryptanalysis of PRESENT-Like Ciphers with Secret S-Boxes. In: A. Joux (ed.) Fast Software Encryption, pp. 270–289. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
16. Boyer, M., Brassard, G., Hoyer, P., Tapp, A.: Tight Bounds on Quantum Searching. Tech. rep. (1996)
17. Buhrman, H., Cleve, R., Laurent, M., Linden, N., Schrijver, A., Unger, F.: New Limits on Fault-Tolerant Quantum Computation. In: 2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06), pp. 411–419 (2006). DOI 10.1109/FOCS.2006.50
18. Bulygin, S.: More on linear hulls of PRESENT-like ciphers and a cryptanalysis of full-round EPCBC-96. Cryptology ePrint Archive, Report 2013/028 (2013). https://eprint.iacr.org/2013/028
19. Cho, J.Y.: Linear Cryptanalysis of Reduced-Round PRESENT. In: J. Pieprzyk (ed.) Topics in Cryptology - CT-RSA 2010, pp. 302–317. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
20. Collard, B., Standaert, F.X.: A Statistical Saturation Attack against the Block Cipher PRESENT. In: M. Fischlin (ed.) Topics in Cryptology – CT-RSA 2009, pp. 195–210. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
21. Emami, S., Ling, S., Nikolić, I., Pieprzyk, J., Wang, H.: The resistance of present-80 against related-key differential attacks. Cryptography and Communications **6**(3), 171–187 (2014). DOI 10.1007/s12095-013-0096-8. URL https://doi.org/10.1007/s12095-013-0096-8
22. Fowler, A.G., Mariantoni, M., Martinis, J.M., Cleland, A.N.: Surface codes: Towards practical large-scale quantum computation. Physical Review A **86**(3) (2012). DOI 10.1103/physreva.86.032324. URL http://dx.doi.org/10.1103/PhysRevA.86.032324
23. Ghosh, S., Sarkar, P.: Breaking Tweakable Enciphering Schemes using Simon's Algorithm. Des. Codes Cryptogr. **89**(8), 1907–1926 (2021). DOI 10.1007/s10623-021-00893-5. URL https://doi.org/10.1007/s10623-021-00893-5
24. Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R.: Applying Grover's Algorithm to AES: Quantum Resource Estimates. In: T. Takagi (ed.) Post-Quantum Cryptography, pp. 29–43. Springer International Publishing, Cham (2016). DOI 10.1007/978-3-319-29360-8_3. URL https://doi.org/10.1007/978-3-319-29360-8_3
25. Grover, L.K.: A Fast Quantum Mechanical Algorithm for Database Search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, STOC '96, p. 212–219. Association for Computing Machinery, New York, NY, USA (1996). DOI 10.1145/237814.237866. URL https://doi.org/10.1145/237814.237866
26. Häner, T., Steiger, D.S., Svore, K., Troyer, M.: A Software Methodology for Compiling Quantum Programs. Quantum Science and Technology **3**(2), 020501 (2018). DOI 10.1088/2058-9565/aaa5cc. URL http://dx.doi.org/10.1088/2058-9565/aaa5cc
27. Jain, A., Kohli, V., Mishra, G.: Deep Learning based Differential Distinguisher for Lightweight Cipher PRESENT. Cryptology ePrint Archive, Report 2020/846 (2020). https://eprint.iacr.org/2020/846
28. Jang, K., Choi, S., Kwon, H., Kim, H., Park, J., Seo, H.: Grover on Korean Block Ciphers. Applied Sciences **10**(18) (2020). DOI 10.3390/app10186407. URL https://www.mdpi.com/2076-3417/10/18/6407
29. Jang, K., Kim, H., Eum, S., Seo, H.: Grover on gift. Cryptology ePrint Archive, Report 2020/1405 (2020). https://eprint.iacr.org/2020/1405
30. Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing Grover Oracles for Quantum Key Search on AES and LowMC. In: A. Canteaut, Y. Ishai (eds.) Advances in Cryptology – EUROCRYPT 2020, pp. 280–310. Springer International Publishing, Cham (2020)

31. Jaques, S., Schanck, J.M.: Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE **11692**, 32–61 (2019). DOI 10.1007/978-3-030-26948-7_2
32. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking Symmetric Cryptosystems Using Quantum Period Finding. In: M. Robshaw, J. Katz (eds.) Advances in Cryptology – CRYPTO 2016, pp. 207–237. Springer Berlin Heidelberg, Berlin, Heidelberg (2016). DOI 10.1007/978-3-662-53008-5_8. URL https://doi.org/10.1007/978-3-662-53008-5_8
33. Kuwakado, H., Morii, M.: Quantum Distinguisher between the 3-round Feistel cipher and the Random Permutation. In: 2010 IEEE International Symposium on Information Theory, pp. 2682–2685 (2010). DOI 10.1109/ISIT.2010.5513654. URL https://doi.org/10.1109/ISIT.2010.5513654
34. Kuwakado, H., Morii, M.: Security on the quantum-type Even-Mansour cipher. In: 2012 International Symposium on Information Theory and its Applications, pp. 312–316 (2012)
35. Lacko-Bartošová, L.: Algebraic Cryptanalysis of Present Based on the Method of Syllogisms. Tatra Mountains Mathematical Publications **53**(1), 201–212 (2013). DOI doi:10.2478/v10127-012-0047-3. URL https://doi.org/10.2478/v10127-012-0047-3
36. Langenberg, B., Pham, H., Steinwandt, R.: Reducing the Cost of Implementing the Advanced Encryption Standard as a Quantum Circuit. IEEE Transactions on Quantum Engineering **1**, 1–12 (2020). DOI 10.1109/TQE.2020.2965697. URL https://doi.org/10.1109/TQE.2020.2965697
37. Lauridsen, M.M., Rechberger, C.: Linear Distinguishers in the Key-less Setting: Application to PRESENT. In: G. Leander (ed.) Fast Software Encryption, pp. 217–240. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
38. Leander, G.: On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN. In: K.G. Paterson (ed.) Advances in Cryptology – EUROCRYPT 2011, pp. 303–322. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
39. Lee, C.: Biclique Cryptanalysis of PRESENT-80 and PRESENT-128. J. Supercomput. **70**(1), 95–103 (2014). DOI 10.1007/s11227-014-1103-3. URL https://doi.org/10.1007/s11227-014-1103-3
40. Liu, G., Jin, C., Kong, Z.: Key recovery attack for present using slender-set linear cryptanalysis. Science China Information Sciences **59**(3), 32110 (2016). DOI 10.1007/s11432-015-5295-9. URL https://doi.org/10.1007/s11432-015-5295-9
41. Liu, G.Q., Jin, C.H.: Differential cryptanalysis of PRESENT-like cipher. Designs, Codes and Cryptography **76**(3), 385–408 (2015). DOI 10.1007/s10623-014-9965-1. URL https://doi.org/10.1007/s10623-014-9965-1
42. Liu, G.Q., Jin, C.H.: Linear Cryptanalysis of PRESENT-like Ciphers with Secret Permutation. The Computer Journal **59**(4), 549–558 (2015). DOI 10.1093/comjnl/bxv074. URL https://doi.org/10.1093/comjnl/bxv074
43. Luo, H., Chen, W., Ming, X., Wu, Y.: General differential fault attack on present and gift cipher with nibble. IEEE Access **9**, 37697–37706 (2021). DOI 10.1109/ACCESS.2021.3062665
44. Menezes, A.J., Vanstone, S.A., Oorschot, P.C.V.: Handbook of Applied Cryptography, 1st edn. CRC Press, Inc., USA (1996)
45. Mohammad Hossein Faghihi Sereshgi, M.D., Shakiba, M.: Biclique cryptanalysis of mibs-80 and present-80. Cryptology ePrint Archive, Report 2015/393 (2015). https://eprint.iacr.org/2015/393
46. Ohkuma, K.: Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis. In: M.J. Jacobson, V. Rijmen, R. Safavi-Naini (eds.) Selected Areas in Cryptography, pp. 249–265. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
47. Özen, O., Varıcı, K., Tezcan, C., Kocair, Ç.: Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT. In: C. Boyd, J. González Nieto (eds.) Information Security and Privacy, pp. 90–107. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
48. Rahman, M., Paul, G.: Quantum Attacks on HCTR and its Variants. IEEE Transactions on Quantum Engineering (2020). DOI 10.1109/TQE.2020.3041426
49. Selinger, P.: Quantum circuits of T-depth one. Physical Review A **87**(4) (2013). DOI 10.1103/physreva.87.042302. URL http://dx.doi.org/10.1103/PhysRevA.87.042302
50. Shor, P.: Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994). DOI 10.1109/SFCS.1994.365700

51. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. **26**(5), 1484–1509 (1997). DOI 10.1137/S0097539795293172. URL https://doi.org/10.1137/S0097539795293172
52. Simon, D.R.: On the Power of Quantum Computation. SIAM J. Comput. **26**(5), 1474–1483 (1997). DOI 10.1137/S0097539796298637. URL https://doi.org/10.1137/S0097539796298637
53. of Standards, N.I., Technology.: Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process (2016). https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)#FN3
54. Steiger, D.S., Häner, T., Troyer, M.: ProjectQ: An Open Source Software Framework for Quantum Computing. Quantum **2**, 49 (2018). DOI 10.22331/q-2018-01-31-49. URL http://dx.doi.org/10.22331/q-2018-01-31-49
55. Tezcan, C.: Improbable differential attacks on Present using undisturbed bits. J. Computational Applied Mathematics **259**, 503–511 (2014)
56. Tezcan, C.: Differential Factors Revisited: Corrected Attacks on PRESENT and SERPENT. In: T. Güneysu, G. Leander, A. Moradi (eds.) Lightweight Cryptography for Security and Privacy, pp. 21–33. Springer International Publishing, Cham (2016)
57. Tezcan, C., Okan, G.O., Şenol, A., Doğan, E., Yücebaş, F., Baykal, N.: Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited. In: A. Bogdanov (ed.) Lightweight Cryptography for Security and Privacy, pp. 18–32. Springer International Publishing, Cham (2017)
58. Wang, G., Wang, S.: Differential Fault Analysis on PRESENT Key Schedule. In: 2010 International Conference on Computational Intelligence and Security, pp. 362–366 (2010). DOI 10.1109/CIS.2010.84
59. Wang, M.: Differential Cryptanalysis of Reduced-Round PRESENT. In: S. Vaudenay (ed.) Progress in Cryptology – AFRICACRYPT 2008, pp. 40–49. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
60. Wang, M., Sun, Y., Tischhauser, E., Preneel, B.: A Model for Structure Attacks, with Applications to PRESENT and Serpent. In: A. Canteaut (ed.) Fast Software Encryption, pp. 49–68. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
61. Watrous, J.: Introduction to Quantum Computing (2005). URL https://cs.uwaterloo.ca/~watrous/QC-notes/
62. Wu, S., Wang, M.: Integral Attacks on Reduced-Round PRESENT. In: S. Qing, J. Zhou, D. Liu (eds.) Information and Communications Security, pp. 331–345. Springer International Publishing, Cham (2013)
63. Yamamura, A., Ishizuka, H.: Quantum Cryptanalysis of Block Ciphers (Algebraic Systems, Formal Languages and Computations.). Tech. rep. (2000)
64. Yang, L., Wang, M., Qiao, S.: Side Channel Cube Attack on PRESENT. In: J.A. Garay, A. Miyaji, A. Otsuka (eds.) Cryptology and Network Security, pp. 379–391. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
65. Zhang, J., Gu, D., Guo, Z., Zhang, L.: Differential power cryptanalysis attacks against PRESENT implementation. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), vol. 6, pp. V6–61–V6–65 (2010). DOI 10.1109/ICACTE.2010.5579367
66. Zhao, X., Wang, T., Guo, S.: Improved Side Channel Cube Attacks on PRESENT. Cryptology ePrint Archive, Report 2011/165 (2011). https://eprint.iacr.org/2011/165