A Practical-Quantum Differential Attack on Block Ciphers

Tarun Yadav, Manoj Kumar, Amit Kumar, S K Pal

Scientific Analysis Group, DRDO, Metcalfe House Complex, Delhi-110 054, INDIA
{tarunyadav,manojkumar,amitkumar,skpal}@sag.drdo.in

Abstract. Differential attack is a basic cryptanalysis method for block ciphers that exploits the high probability relations between the input and output differences. The existing work in quantum differential cryptanalysis of block ciphers focuses on resource estimation to recover the last round subkeys on the basis of existing relations constructed on classical computers. To find such relations using quantum computer, we propose a method to search the high probability differential and impossible differential characteristics using quantum computer. The method explores all possible input and output difference pairs simultaneously using superposition of qubits. The proposed method is used to design the quantum circuit to search the differential characteristics for a toy cipher smallGIFT. The branch-and-bound based method is used to validate differential and impossible differential characteristics obtained using proposed method.

Keywords: Block Cipher, Differential Cryptanalysis, GIFT, Quantum Cryptanalysis

1 Introduction

With the advances in development of quantum computers [11], there is a possible threat on the security of asymmetric and symmetric cryptographic algorithms. Existing asymmetric cryptosystem such as RSA and elliptic curve would become insecure due to polynomial time solution on a quantum computer using Shor's algorithm [26]. The major impact of quantum computing on the security of symmetric key cipher is the quadratic speed-up to search the key space using Grover's algorithm [13]. The classical symmetric ciphers can be attacked more efficiently using the Grover's search algorithm on quantum computers.

The block ciphers are widely deployed symmetric key cryptographic primitives in the real world applications. The development of quantum computers with sufficient qbits can pose a real threat on the security of block ciphers. The exhaustive key search is the only readily available attack that is applicable to every block cipher. Grover's algorithm can provide a quadratic speed-up in the exhaustive search of the entire key space. It can be used to reduce the

exhaustive attack complexity of n-bit block cipher to $2^{n/2}$ on a quantum computer in comparison to the complexity of 2^n on classical computers. Therefore, the complexity of 128-bit block cipher with a key size of 128 bits will be reduced to 64 bits on a quantum computer. To prevent this attack, there is recommendation [1] to increase the key size to withstand post quantum security. The existing block ciphers are expected to survive in the post quantum era but with a larger key size.

The differential cryptanalysis is the most widely used cryptanalytic technique to analyse the security of block ciphers. It was proposed by Biham and Shamir and a full round differential attack was presented against DES [7]. A lot of research work has been carried out to increase the efficiency of differential attack in the past three decades. The first requirement for a differential attack is the high probability relations between the input and output differences. To search the optimal differential relations is a tedious task and a lot of research has been carried out to improve the efficiency of search techniques. Initially, branch-and-bound based methods were used to construct these relations and various improvements in this approach has been proposed [20]. The major development in this area was application of MILP to construct the optimal differential characteristics [24] [21]. The machine learning based approach has also been used to construct the high probability differential distinguishers [30]. However, practical-quantum version of the differential attack has never been presented in the open literature. The impossible differential cryptanalysis is a variant of differential attack that uses zero probability differential characteristics to filter out the wrong keys. The miss-in-the-middle approach is used to construct the impossible differential characteristics. MILP based search technique is also used to get the zero probability differential characteristics. We present the first approach using quantum search to construct the differential and impossible differential characteristics.

Existing work in quantum cryptanalysis. Recent developments in quantum cryptanalysis of block ciphers focused on quantum resource estimation for exhaustive key search attack. For this purpose, block ciphers are implemented in quantum circuits to estimate the cost of exhaustive key search using Grover's algorithm. NIST also used the same approach for indicating the strength of a cipher in post quantum world [25]. Various authors presented the cost of exhaustive key search on a quantum computer for the block ciphers AES [5] [12] [17], Speck [2] [15], Simon [3] [22], ARIA [10], AES, GIFT [16] [4], SKINNY [4], SATURNIN [4], PIPO [18], SPEEDY [27]. Quantum version of differential, linear and impossible differential attacks have been explored in [19] [23] [29] and authors have presented key recovery attacks using the existing characteristics. The use of quantum computers to come up with the good differential characteristics for block ciphers was left an open problem.

Our Contributions. In this work, we present a quantum version of the differential attack on block ciphers. We propose a quantum computer based method to search high probability differential characteristics for the first time. We construct a quantum circuit for the S-box and diffusion layer of a toy version of lightweight

block cipher GIFT [6]. Using proposed method, we construct a quantum circuit to find the 3-round differential characteristics. We make use of the Hadamard gates to explore the all possible input and output differences. We run this circuit 10,000 times on qasm simulator and measure the qbits to get the optimal differential characteristics. In the same experiment, we get the impossible differential (zero probability) differential characteristics. We also used the branch-and-bound based method to construct the characteristics for smallGIFT and compared it with the output of proposed method.

Organisation. The remaining part of the paper is organised as follows. In Section 2, we describe an 8-bit toy cipher smallGIFT. In Section 3, we construct the quantum circuit for 4-bit S-box, diffusion layer, encryption and decryption algorithm. Quantum differential and impossible differential characteristic search for smallGIFT is described in section 4. We compare the results of quantum differential characteristics search with the branch and bound based method in Section 5. In section 6, we provide quantum resource estimation for GIFT-64. The paper is concluded in Section 7.

2 Preliminaries

2.1 Quantum Gates

Various gates are used in a quantum computer which emulate the bit operations. In this paper we have used Pauli-X, CNOT, Toffoli, Swap and Hadamard gates. These gates are chosen to emulate the S-box and permutation operations used in the cipher. Pauli-X gate is a single qubit gate and it is used to invert the state of qubit as shown in Fig. 1. CNOT gate (Fig. 2) is double qubit gate and it is used to perform the XOR operation as well as to transfer the state to another qubit. Toffoli gate is a triple qubit gate and it is used to emulate the AND THEN XOR operation as shown in Fig. 3. Toffoli gate with Pauli-X is used for the OR operation as depicted in Fig. 3c. Swap gate (Fig. 4) is a double qubit gate and it swaps the states of qubits. Permutation operation used in a cipher is emulated using the swap gates. Hadamard gate (Fig. 5) is used to bring the qubit in a superposition state. Such superposition states are required to explore all possibilities corresponding to the input qubits.

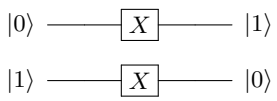


Fig. 1: Pauli-X Gate

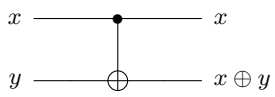
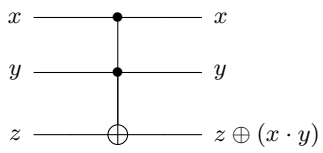
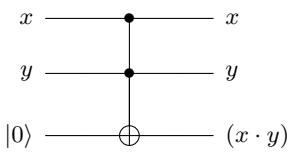


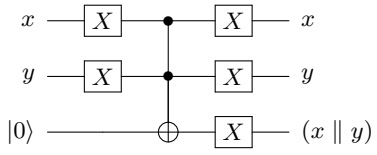
Fig. 2: CNOT Gate



(a) Toffoli Gate



(b) AND Circuit



(c) OR Circuit

Fig. 3: AND and OR operations using Toffoli Gate

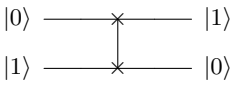


Fig. 4: Swap Gate

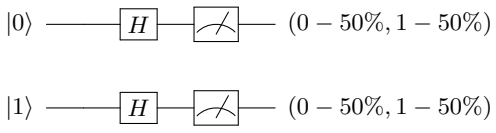


Fig. 5: Hadamard(H) Gate

2.2 Differential and Impossible Differential Cryptanalysis

An ideal block cipher is designed in such a way that an adversary can not distinguish its output from a random permutation after making sufficient (q) number of queries. In differential attack, the non-uniform relations between the input and output pairs are searched and used as a distinguisher between the cipher and random source [7]. The input pairs generated with a particular difference value Δ_i propagate to the output pairs related with some difference Δ_o with the high probability. These high probability differential characteristics ($\Delta_i \rightarrow \Delta_o$) are used to distinguish the output of a block cipher from the output of a random function. The subkeys used in the last rounds are also recovered using these differential characteristics. The main challenge is to find out such high probability relations in the input and output differences. The existing classical techniques find such relations by starting with a particular difference and search through all paths that are bounded by a probability value. The paths with optimal probability are used as the differential characteristics. MILP is the another technique which converts the differential characteristic search problem into an MILP model and solve the problem with optimization problem solver like CPLEX/Gurobi [9] [14] to get the optimal differential characteristics.

The impossible differential attack works with zero probability differential characteristics and such differential characteristics are obtained using a miss-in-the-middle like approach [8]. In this method, differential characteristics ($\Delta_i \rightarrow \Delta_m$) and ($\Delta_n \rightarrow \Delta_o$), probability one each, are connected to get an impossible differential ($\Delta_i \not\rightarrow \Delta_o$) by proving a contradiction between the probability one differentials. The MILP based method is also used to get the impossible differential characteristics [28]. The impossible differential characteristics are used as distinguisher and last round subkeys are recovered by sieving the wrong keys that suggest the impossible differential.

2.3 SmallGIFT: 8-bit Toy Cipher

We propose a smaller version of lightweight block cipher GIFT [6] for practical demonstration of quantum differential and impossible differential attack on block ciphers. The smallGIFT is a block cipher with 8-bit block size and 4-bit S-box (Table 1). The 4-bit S-box is same as used in GIFT and there are four rounds in smallGIFT. In each round, the 4-bit S-box is used two times in parallel and bit permutation (Table 2) is applied on the output from S-box layer. The key expansion algorithm divides the 16-bit master key K into four 4-bit nibbles s.t. $K = K_0||K_1||K_2||K_3$. The round key for round r will be $K_{(r\,mod 4)}$. We describe the encryption algorithm of 4-round smallGIFT using 4-bit S-box S and 8-bit permutation P_8 in Algorithm 1.

x	0 1 2 3 4 5 6 7 8 9 A B C D E F
S(x)	1 a 4 c 6 f 3 9 2 d b 7 5 0 8 e

Table 1: S-Box

i	0 1 2 3 4 5 6 7
BP_i	0 3 5 7 2 4 6 1

Table 2: 8-bit Permutation (BP)

Algorithm 1: Encryption Algorithm of smallGIFT

Input: $P(= X_0) = (x_7, x_6, \cdots, x_0)$ and $RK_r = (U, V)(0 \leq r \leq 3)$
Output: $C = X_4$
for r=0 to 3 **do**
  for j=0 to 1 **do**
    $(y'_{3+4*j}, y'_{2+4*j}, y'_{1+4*j}, y'_{0+4*j}) = S(x_{3+4*j}, x_{2+4*j}, x_{1+4*j}, x_{0+4*j})$
  end
  $(y_7, y_6, \cdots, y_0) = P_8(y'_7, y'_6, \cdots, y'_0)$
  for l=0 to 1 **do**
    $y_{4l+1} = y_{4l+1} \oplus u_l$
    $y_{4l} = y_{4l} \oplus v_l$
  end
  $X_{r+1} = (y_7, y_6, \cdots, y_0)$
end

3 Quantum Circuit for smallGIFT

The smallGIFT encryption algorithm has three major components S-box, permutation and key addition. We need quantum circuits for each component to design the circuit for the encryption algorithm. In this section, we describe quantum circuits for S-box, permutation, key addition, encryption algorithm and decryption algorithm. The quantum circuit for encryption algorithm without key addition is used to search the differential characteristics and these characteristics are used to mount key recovery attack using decryption circuit.

3.1 Quantum Circuit for S-box

Designers of GIFT have provided software and hardware optimized implementation of the S-box of GIFT-64. In-place implementation of S-box is described

using AND, OR and NOT gates (Algorithm 2). Using this implementation the quantum circuit of 4-bit S-box is presented in Fig. 6. The quantum circuit of S-box uses Pauli-X, CNOT, Toffoli and Swap gates that have been described in previous section. The order of output qubits in Algorithm 2 is different from the order of input qubits. To correct the order, we swap first and last qubits using swap gate. The quantum circuit of S-box is referred as QS throughout the paper. The quantum circuit for inverse S-box is obtained by applying the gate operations in the reverse direction. The circuit for inverse S-box (IQS) is shown in Fig. **??**.

Algorithm 2: Optimized in place implementation of S-box

Input : $x = (x[3], x[2], x[1], x[0]))$
Output : $(x[0], x[2], x[1], x[3]))$
1 $x[1] = x[1] \oplus (x[0] \cdot x[2])$
2 $x[0] = x[0] \oplus (x[1] \cdot x[3])$
3 $x[2] = x[2] \oplus (x[0] \parallel x[1])$
4 $x[3] = x[3] \oplus x[2]$
5 $x[3] = \neg x[3]$
6 $x[1] = x[1] \oplus x[3]$
7 $x[1] = \neg x[1]$
8 $x[2] = x[2] \oplus (x[0] \cdot x[1])$

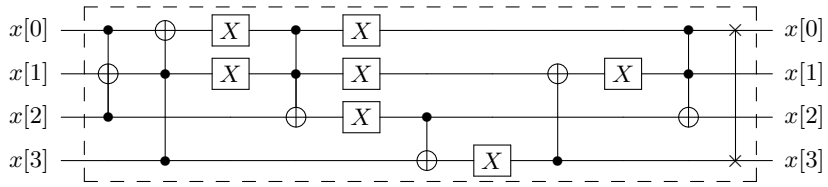


Fig. 6: Quantum Circuit for GIFT/smallGIFT S-box (QS)

3.2 Quantum Circuit for Permutation

The bit permutation operation used in the diffusion layer of block ciphers is a rearrangement of bits in a different order. This operation can be performed using multiple swap operations.The equivalent swap operations for bit permutation used in smallGIFT is described in Equation 1).The permutation described in Table 2 can be performed using four swap operations and these operations are implemented using swap gates on a quantum computer.

$$BP \equiv swap(1,3) \rightarrow swap(1,7) \rightarrow swap(2,5) \rightarrow swap(2,4) \tag{1}$$

3.3 Quantum Circuit for Key Addition

As decribed in the Algorithm 1, the round subkeys are XORed with selective bits of the current state in the key addition layer. In quantum circuit, the key addition operation is performed using CNOT gates and it is depicted in Fig. 7.

3.4 Quantum Circuit for Encryption and Decryption Algorithm of smallGIFT

The encryption algorithm of smallGIFT consists of S-box, permutation and key addition operations. Quantum circuits for these individual components have been discussed in the previous subsections. We present quantum circuit design for the encryption algorithm of smallGIFT by integrating individual circuits (Fig. 7).

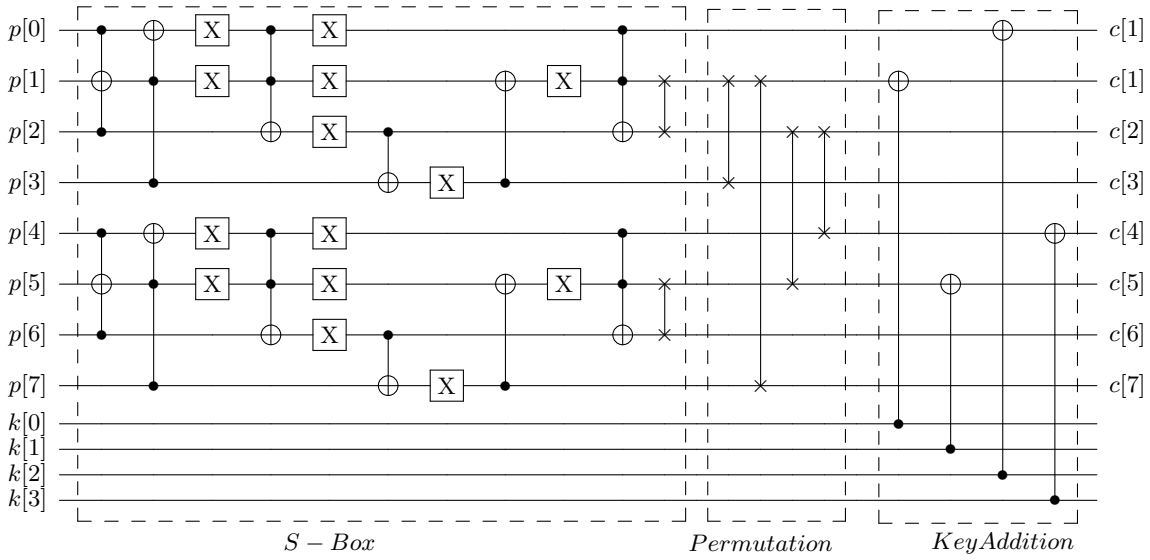


Fig. 7: Quantum Circuit for Encryption Algorithm of SmallGIFT

4 Quantum Circuit to Search Differential characteristics

Searching the high probability differential characteristics is a challenging problem. Generally, the classical approach consists of two parts, minimization of number of active S-boxes and optimization of probability of differential characteristic. The complexity to explore all possible output difference increase exponentially. Quantum computing allows us to explore the all possible output differences in each round. Therefore, a quantum circuit can explore all possible paths corresponding

to all input differences. The combined probability of these paths will be higher than any optimal differential characteristic obtained using classical approach. The quantum differential characteristics search is expected to provide better results than existing methods as the complexity of exiting method increases exponentially with each additional round. We describe the procedure to design the quantum circuit for quantum differential characteristics search for smallGIFT in Algorithm 3.

We require 24 qubits to search the differential charactertics for smallGIFT. In Algorithm 3, 16 qubits $(q_0, ..., q_{15})$ are used to explore all possibles options of 8-bit plaintext pairs $(P, P^{'})$ with the difference Δ. H gate is applied on 8 qubits($\Delta = q_{16}, ...q_{23}$) to generate all possible input differences. These differences(Δ) are transferred to $P^{'}$ using CNOT gates. H gate is applied on P to get all possible options of 8-bit plaintext. The plaintext pairs $(P, P^{'})$ with the difference Δ are obtained using CNOT gates on P and $P^{'}$. The 4-bit QS is applied on P and $P^{'}$ and the resulting differences are stored in $P^{'}$ using CNOT gates. The permutation BP is applied on $P^{'}$ using four swap gates. The procedure is repeated for r rounds and the measurement of qubit corresponding to $\Delta(q_{16}, ...q_{23})$ and $P^{'}(q_8, ...q_{15})$ provides input difference Δ_i and output difference Δ_o respectively.

The measurements are affected by errors and may not accurate. To get the accurate results, the experiment needs to be repeated sufficient number of times. Therefore, to get the high probability input and output differences, we need to repeat Algorithm 3 many times. The repeated executions give histogram corresponding to each input and output difference. The difference pair with maximum probability will be the optimal differential characteristics for r rounds.

Algorithm 3: Quantum Differential Characteristics Search for small-GIFT

Input : 24 qubits (q_0 to q_{23}), no. of rounds (r)
Output : Input and Output difference after r rounds

$P = (P[0], P[1], ..., P[7]) = (q_0, q_1, ..., q_7)$
$P^{'} = (P^{'}[0], P^{'}[1], ..., P^{'}[7]) = (q_8, q_9, ..., q_{15})$
$\Delta = (\Delta[0], \Delta[1], ..., \Delta[7]) = (q_{16}, q_{17}, ..., q_{23})$
$\Delta = H(\Delta)$
$P^{'} = CNOT(\Delta, P^{'})$
$round = 1$
repeat ▷ r times
  $P = H(P)$
  $P^{'} = CNOT(P, P^{'})$
  $P^{'}[0, 1, 2, 3] = CNOT(QS(P[0, 1, 2, 3]), QS(P^{'}[0, 1, 2, 3])$
  $P^{'}[4, 5, 6, 7] = CNOT(QS(P[4, 5, 6, 7]), QS(P^{'}[4, 5, 6, 7])$
  $SWAP(P^{'}[1], P^{'}[3])$
  $SWAP(P^{'}[1], P^{'}[7])$
  $SWAP(P^{'}[2], P^{'}[5])$
  $SWAP(P^{'}[2], P^{'}[4])$
  $round = round + 1$
until $round \leq r$;
$\Delta_i \leftarrow Measure(q_{16}, q_{17}, ..., q_{23})$
$\Delta_o \leftarrow Measure(q_8, q_9, ..., q_{15})$

5 Results

We apply the Algorithm 3 on 3 rounds of smallGIFT and search 3-round high probability differential characteristic for the input difference 0x01 (Δ). For a fix input difference, extra 8 qubits ($q_{16}, ..., q_{23}$) are not required and the difference can be fixed in $P^{'}$ itself. The qubit state corresponding to $P^{'}[0]$ is set as "1" using Pauli-X gate. We present the quantum circuit1-round differential characteristic of small GIFT(Fig. 8). The circuit for 3 rounds of smallGIFT is executed 10000 times on qasm simulator[1] to get the probability distribution of output differences. The output difference with highest probability and zero probability are obtained in the histogram. Top 5 high probability output differences listed and compared with branch and bound approach in Table 3. The impossible output differences corresponding to zero probability points in histogram are described in Table 4.

6 Conclusion

In this paper, we presented an approach for differential and impossible differential cryptanalysis of block ciphers using quantum computers. The proposed quantum

[1] https://qiskit.org/

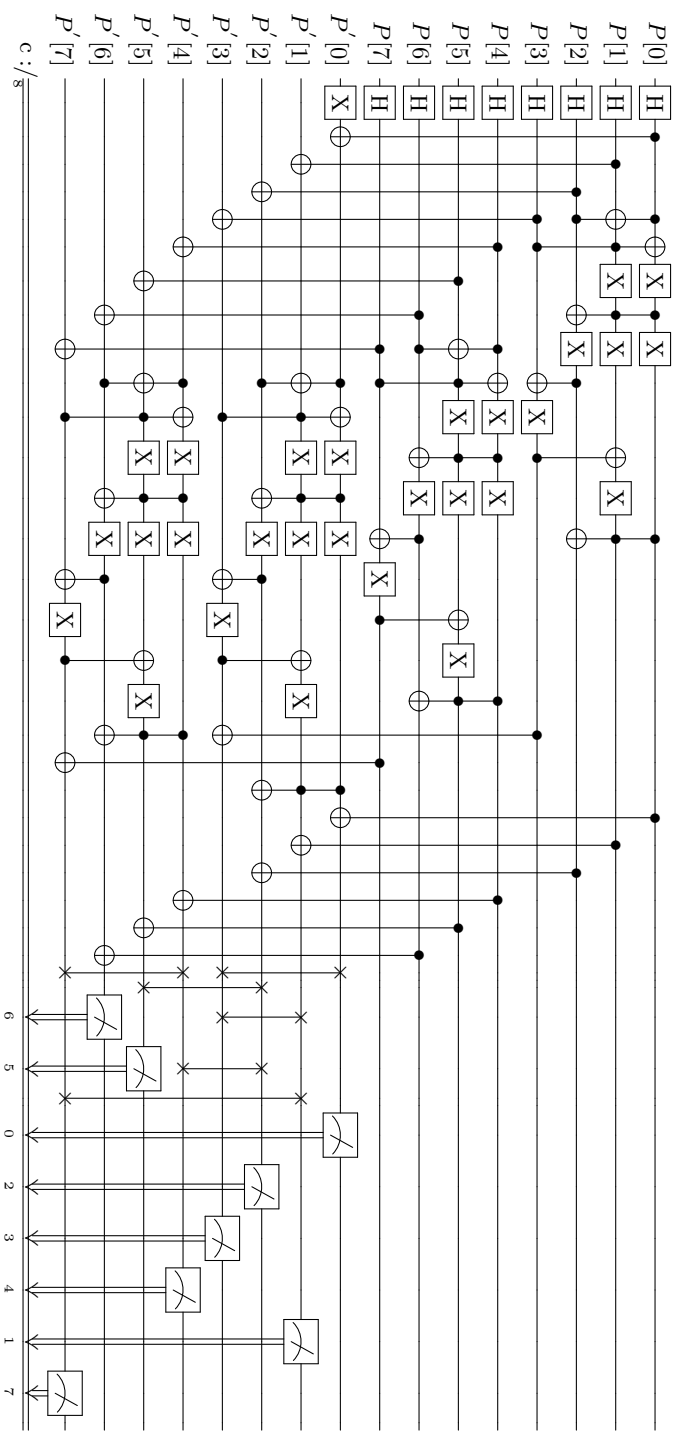


Fig. 8: Practical-Quantum Differential Characteristics Search for 1-round smallGIFT

	Branch and Bound Approach		**Algorithm 4 on Quantum Simulator**	
	Output Difference	***Probability***	***Output Difference***	***Probability***
1	41(00101001)	0.0137	41(00101001)	0.0150
2	09(00001001)	0.0098	09(00001001)	0.0109
3	86(01010110)	0.0098	33(00100001)	0.0100
4	127(01111111)	0.0089	127(01111111)	0.0094
5	95(01011111)	0.0089	95(01011111)	0.0088

Table 3: Top 5 high probability output differences for input difference 0x01(00000001)

	Impossible Differential Characteristics
1	1(00000001) $\rightarrow$ 20(00010100)
2	1(00000001) $\rightarrow$ 40(00101000)
3	1(00000001) $\rightarrow$ 80(01010000)
4	1(00000001) $\rightarrow$ 84(01010100)

Table 4: Impossible output differences for input difference 0x01

differential characteristics search is used to search high probability and zero probability differential characteristics for a toy cipher smallGIFT. We utilized the superposition in qubits to try all possible input and outputs differences. The results are compared and validated using existing methods. After the advent of a quantum computer with sufficient qubits the proposed approach can be used to mount the differential and impossible differential attack on block ciphers.

References

1. Augot, D., Batina, L., Bernstein, D.J., Bos, J.W., Buchmann, J.A., Castryck, W., Dunkelman, O., Güneysu, T., Gueron, S., Hülsing, A., Lange, T., Rechberger, C., Schwabe, P., Sendrier, N., Vercauteren, F., & Yang, B. Initial recommendations of long-term secure post-quantum systems. (2015)
2. Anand, R., Maitra, A., Mukhopadhyay, S., Evaluation of quantum cryptanalysis on speck. International Conference on Cryptology in India. (2020)
3. Anand R, Maitra A, Mukhopadhyay S Grover on simon. arXiv preprint, arXiv:200410686, (2020)
4. Bijwe, S. Chauhan, A.K., and Sanadhya, S.K., Quantum Search for Lightweight Block Ciphers: GIFT, SKINNY, SATURNIN.
5. Bonnetain X, Naya-Plasencia M, Schrottenloher A., Quantum security analysis of AES. IACR Transactions on Symmetric Cryptology, pp. 55–93. (2019)
6. Banik, S., Pandey, S.K., Peyrin, T.,Sasaki, Y., Sim, S.M., and Todo, Y., GIFT: A small present - towards reaching the limit of lightweight encryption. In Wieland Fischer and Naofumi Homma, editors, Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, volume 10529 of Lecture Notes in Computer Science, pages 321–345. Springer, 2017.

7. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, vol. 4, pp. 3–72, springer (1991)
8. Biham, E., Biryukov, A., and Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials, In J. Stern, editor, Advances in Cryptology, EUROCRYPT'99, LNCS, vol. 1592, pp. 12-23. Springer Verlag, 1999.
9. https://www.ibm.com/analytics/cplex-optimizer
10. Chauhan, A., and Sanadhya, S., Quantum Resource Estimates of Grover's Key Search on ARIA, pp. 238-258. 12 2020.
11. Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. Surface codes: Towards practical large-scale quantum computation. Phys. Rev. A, 86:032324, Sep 2012.
12. Grassl, M., Langenberg, B., Roetteler, M.,and Steinwandt, R., Applying grover's algorithm to AES: quantum resource estimates. In Tsuyoshi Takagi, editor, Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings, volume 9606 of Lecture Notes in Computer Science, pages 29–43. Springer, 2016.
13. Grover, L.K., A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996, pages 212–219. ACM, 1996.
14. https://www.gurobi.com/
15. Jang K., Choi S., Kwon H., Seo H., Grover on SPECK: Quantum Resource Estimates. Cryptology ePrint Archive, Report 2020/640. https://eprint.iacr.org/2020/640
16. Jang, K., Kim, H., Eum, S., and Seo, H., Grover on GIFT.," IACR Cryptol. ePrint Arch., vol. 2020, p. 1405, 2020.
17. Jaques, S., Naehrig, M., Roetteler, M., and Virdia, F., Implementing grover oracles for quantum key search on AES and lowmc. In Anne Canteaut and Yuval Ishai, editors, Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II, volume 12106 of Lecture Notes in Computer Science, pages 280–310. Springer, 2020.
18. Jang, K., Song, G., Kwon, H., Uhm, S., Kim, H., Lee, W.K. ,and Seo, H., Grover on PIPO," Electronics, vol. 10, no. 10, p. 1194, 2021.
19. Kaplan, M., Leurent, G., Leverrier, A. and Naya-Plasencia, M., 2015. Quantum differential and linear cryptanalysis. IACR Transactions on Symmetric Cryptology (2016): 71-94.
20. Kumar, M., Suresh, TS, Pal, S.K., Panigrahi, A.: Optimal Differential Trails in Lightweight Block Ciphers ANU and PICO. Cryptologia, vol. 44, No. 1, pp. 68-78 (2020)
21. Kumar, M., Yadav, T.,: MILP Based Differential Attack on Round Reduced WARP. In: Batina L., Picek S., Mondal M. (eds) Security, Privacy, and Applied Cryptography Engineering. SPACE 2021. Lecture Notes in Computer Science, vol. 13162, pp. 42-59. Springer, Cham. https://doi.org/10.1007/978-3-030-95085-9_3 (2022)
22. Leander, G., May, A., (2017) Grover meets simon–quantumly attacking the fxconstruction. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham. pp 161–178
23. Li, H. and Yang, L., 2015, November. Quantum differential cryptanalysis to the block ciphers. In International Conference on Applications and Techniques in Information Security (pp. 44-51). Springer, Berlin, Heidelberg.

24. Mouha, N., Wang, Q., Gu, D. and Preneel, B.: Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming. In Chuankun Wu, Moti Yung, and Dongdai Lin, editors, Inscrypt 2011, vol. 7537, LNCS, pp. 57–76. Springer (2011)
25. NIST. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process, 2016.
26. Shor, P.W., Polynominal time algorithms for discrete logarithms and factoring on a quantum computer. In Leonard M. Adleman and Ming-Deh A. Huang, editors, Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, May 6-9, 1994, Proceedings, volume 877 of Lecture Notes in Computer Science, page 289. Springer, 1994.
27. Song, G., Jang, K., Kim, H., Eum, S., Sim, M., Kim, H., Lee, W.K., and Seo, H., Grover on SPEEDY.
28. Sasaki, Y., and Todo, Y.: New Impossible Differential Search Tool from Design and Cryptanalysis Aspects - Revealing Structural Properties of Several Ciphers. In Jean-Sebastien Coron and Jesper Buus Nielsen, editors, Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III, vol. 10212 of Lecture Notes in Computer Science, pp. 185-215, Springer (2017)
29. Zhou, Q., Lu, S., Zhang, Z. and Sun, J., 2015. Quantum differential cryptanalysis. Quantum Information Processing, 14(6), pp.2101-2109.
30. Yadav, T., Kumar, M.: Differential-ML Distinguisher: Machine Learning based Generic Extension for Differential Cryptanalysis. In Longa, P., Rafols, C., editors, Progress in Cryptology- LATINCRYPT 2021