Linear Cryptanalysis Through the Lens of CHSH Game

Arpita Maitra\textsuperscript{1}, Ravi Anand\textsuperscript{2}, Suman Dutta\textsuperscript{3}

\textsuperscript{1} TCG Centre for Research and Education in Science and Technology, Kolkata-700091, West Bengal, India, \textsuperscript{2} R C Bose Centre for Cryptology and Security, Indian Statistical Institute, 203 B.T. Road, Kolkata 700108, West Bengal, India, \textsuperscript{3} Applied Statistics Unit, Indian Statistical Institute, 203 B.T. Road, Kolkata-700108, West Bengal, India

Application of CHSH game in Linear Cryptanalysis is presented. Till date, the known usage of CHSH game in Quantum Cryptology is to verify the device independence of the protocols. We observed that the classical symmetric ciphers having the bias equal to 0.25 can be improved to 0.35 exploiting the game which indicates clear improvement over existing Linear and Differential cryptanalysis. In the present initiative, we showed the application of the game in linear cryptanalysis on a lightweight cipher named SIMON. However, the approach can be extended to Differential cryptanalysis too. This observation opens a new direction of research in quantum cryptography.

I. INTRODUCTION

Bell inequality \cite{1} certifies the non-local relationship between two correlated systems. In other words, Bell inequality confirms the quantumness of the system. This inequality can be described in the form of a game, named CHSH \cite{2} game.

In CHSH game, there are one referee and two players whom we generally call Alice and Bob. Referee provides a bit $x$ to Alice and a bit $y$ to Bob. After receiving the bits, Alice and Bob each outputs a bit, say, $a$ for Alice and $b$ for Bob. The players win the game if $x \land y = a \oplus b$.

In classical domain where there is no existence of entanglement, the best strategy to win the game would be as follows.

1. Alice and Bob both output 0 irrespective of their inputs.

2. Alice and Bob both output 1 irrespective of their inputs.

In such case, they will win the game with probability 0.75. On the other hand, in quantum domain where one can take the advantage of entanglement, wins the game with better probability.

In this case, Alice and Bob share maximally entangled state prior to the game. After receiving the inputs from referee, the players measure their respective systems in some specified bases. The choice of basis depends on the input bits. It is well proven that in such strategy, Alice and Bob can improve their winning probability upto 0.85.

In quantum cryptography, CHSH game is used for testing the device independence of the protocols. Precisely, 0.85 probability certifies the existence of maximally entangled state amongst the legitimate parties \cite{3,9}. If the shared states are maximally entangled, then from the monogamy relation of entanglement \cite{10,12}, it is guaranteed that the information about the raw key extracted by an eavesdropper, generally familiar as Eve, can not be greater than the information extracted by Bob (one of the authenticated parties).

The probability is calculated from input-output statistics. For example, in case of Quantum Key Distribution (QKD) protocols, the QKD boxes are available as Black boxes to the legitimate parties. Each box can take an input bit ($x$ or $y$) and provides an output bit ($a$ or $b$). If the input-output statistics satisfies the winning condition with probability 0.85, then there must exists a non-local maximal correlation between the boxes available to the authenticated parties. This non-local correlation guarantees the absolute security of the protocol. In the present initiative, we report another application of the game in quantum cryptography.

In cryptography, cipher is the encrypted form of message. Message is encrypted in the motivation towards hiding the information from the eavesdropper. The encryption as well as the decryption function are known to all, however the secret thing is the key. The encryption function is chosen in such a way so that without any knowledge of the key it is not possible to decrypt the cipher. Even the designer of the crypto-system also can not decipher it without the knowledge of the key. Hence, extracting the key bits is the prime motivation for attacking the cipher. Formally, we name it as cryptanalysis (breaking the code).

It is expected that the ciphers are designed in such a way so that the random variables 0 and 1 come from a probability distribution \{1/2, 1/2\}. However, any shifting from this distribution may cause loopholes in the cipher. Exploiting this one can extract the key bit(s). The deviation from 1/2 is called bias. Thus, finding a bias for a given cipher is another important job in cryptanalysis.

Now, consider that there are two probability distributions \{p, 1-p\} and \{q, 1-q\}, where $q = p + \epsilon$ and $\epsilon$ is an infinitesimal small number. To distinguish these two probability distributions with 99% confidence, the number of samples required is approximately $64/p^2$. Thus, if $\epsilon$ increases, then the number of samples decreases. For
infinitesimally small ϵ, we can write $64/p\epsilon^2 \approx 1/\epsilon^2$. If $p = 1/2$, ϵ is called the bias of the random variables 0 and 1. Hence, improving the bias is very significant contribution in cryptanalysis.

In the present draft, we observe that if we can convert the classical ciphers in quantum ciphers, i.e, bits will be encoded by qubits and the classical gates used in the ciphers will be replaced by quantum gates, then we may exploit quantum advantage to improve the bias present in the cipher. Here, we consider a symmetric cipher named SIMON [13]. In SIMON, the sender and the receiver use the same secret key. SIMON is also a lightweight cipher designed by NSA (National Security Agency of USA).

In classical domain, it was observed that this cipher has some bias and the optimal bias found is 0.25 i.e., here $q = 0.75$. On the other hand, exploiting Boolean version of CHSH game, we can successfully improve the bias upto 0.35, i.e., in this case, $q$ will be 0.85.

Till date, Quantum Cryptanalysis on Symmetric Ciphers exploits Grover’s search algorithm [14], Simon period finding algorithm [15] and the combination of both. Block ciphers like AES [16, 19], Even-Mansour construction [20] and McEliece system [21] have been studied subsequently. It is also proven that classically secure ciphers can be broken with quantum algorithms [20, 22–25]. Quantum algorithm can be used to speed up classical attacks [26, 27] too. Contrary to these, in the current manuscript, we exploit CHSH game and improve the bias of the cipher. This improvement has major impact in linear and differential cryptanalysis [29]. This technique can be extended to any symmetric ciphers having the bias equal to 0.25. And hence, all the existing linear and differential attacks can be improved by uplifting the bias to 0.35. We believe that this will open up a new avenue of research in the paradigm of quantum cryptography.

The draft is organized as follows. Section II deals with a brief description of classical cipher SIMON, its encryption and decryption algorithms and some observations towards linear and differential cryptanalysis on the cipher. In Section III, we discuss Boolean implementation of CHSH game. In section Section IV we show how the Boolean circuit of the game can be exploited in SIMON. We implement the idea in IBMQ simulator for an arbitrary round i. In Section V, we discuss how the game improves a linear attack on the cipher. Section VI concludes the paper.

II. BRIEF DESCRIPTION OF SIMON

SIMON is a family of balanced Feistel structured [29] lightweight block ciphers with 10 different block sizes and key sizes (Table I).

![FIG. 1. SIMON round function.](image)

| Block Size (2n) | Key Size (k = mn) | word size (n) | keywords (m) | Rounds (T) |
|----------------|-------------------|--------------|-------------|-----------|
| 32             | 64                | 16           | 4           | 32        |
| 48             | 72                | 24           | 3.4         | 36.36     |
| 64             | 96, 128           | 32           | 3.4         | 42.44     |
| 96             | 96, 144           | 48           | 2.3         | 52.54     |
| 128            | 128, 192, 256     | 64           | 2.3.4       | 68.69, 72 |

TABLE I. SIMON parameters

The structure of one round SIMON encryption is depicted in Figure 1 where $S^j$ represents a left circular shift by $j$ bits, $L_i$ and $R_i$ are $n$-bit words which constitute the state of SIMON at the $i$-th round and $k_i$ is the round key which is generated by key scheduling algorithm. The description is out of the scope for the paper. Interested readers may explore [13] for detailed description of the lightweight ciphers, SIMON and SPECK.
The Boolean function ‘AND’ (&) plays a vital role in this linear relationship. A close observation reveals that if \( L_i(j) = L_i(j + 2) \), then due to the presence of ‘AND’ operation we can write the followings.

\[
\begin{align*}
\Pr(L_i(j) \oplus L_{i+1}(j) = 0) & = R_i(j) = K_i(j) = 3/4, \\
\Pr(L_i(j) \oplus L_{i+1}(j) = 1) & = R_i(j) = K_i(j) = 1/4.
\end{align*}
\]

These imply that there is certain bias in the cipher. Hence, for a sufficient number of plaintext-ciphertext pairs for a round \( i \), it is possible to find such bias. This can be further extended for two consecutive rounds, i.e., for \( i \) and \( i+2 \). This is because of the advantage of Feistel construction. In Feistel construction, \( L_{i+1}(j) = R_{i+2}(j) \). Hence, it is rather better to say that for a sufficient number of plaintext-ciphertext pairs for two rounds SIMON, it is possible to find the above bias.

The procedure would be the following.

1. For a given plaintext-ciphertext pairs for two round SIMON, check if \( L_i(j) = L_{i+1}(j + 2) \). Note that \( L_{i+1}(j + 2) = R_{i+2}(j + 2) \).
2. Calculate \( \Pr(L_i(j) \oplus L_{i+1}(j) = 0) \) and \( \Pr(L_i(j) \oplus L_{i+1}(j) = 1) \).
3. If, either \( \Pr(L_i(j) \oplus L_{i+1}(j) = 0) = 3/4 \) or \( \Pr(L_i(j) \oplus L_{i+1}(j) = 1) = 1/4 \), conclude \( K_i(j) = R_i(j) \).

The variants of such attack has been studied in [30, 33]. However, the bias better than 0.25 for a round has not been found yet. In this backdrop, we observed that as the bias comes from ‘AND’ operation, one can take the advantage of CHSH game and hence can improve the bias for a round. Before going to the implementation of CHSH game in SIMON, we like to discuss the Boolean implementation of CHSH game which is the pillar of improving the bias.

### III. BOOLEAN IMPLEMENTATION OF CHSH GAME

In this section, CHSH game will be viewed as a Boolean function \( f : \{0, 1\}^n \rightarrow \{0, 1\} \). Here, the function \( f : \{0, 1\}^4 \rightarrow \{0, 1\} \) such that \( f = (x \land y) \oplus (a \oplus b) \). The corresponding circuit is given below. The qubit \( b_0 \) stores the functional value \( f \).

According to the classical strategy for winning the game with maximum probability, Alice and Bob output the same bits. This has been depicted using first CNOT gate (from left) as a cloning operator on \( a_0 \). It copies \( a_0 \) in \( b_0 \) resulting \( a = b \) always. Hadamard gates are used to take care of all possible choices of \( x, y \) and \( a \). If we compute the probability considering the reduced density matrix of \( b_0 \), we will get 0.75 for the bit 0 and 0.25 for the bit 1.

Now, to implement quantum strategy we took the help of Controlled-Hadamard \((CH)\) and Controlled-\(U_3\) \((CU_3)\) gate, where \( U_3 = \begin{pmatrix} \cos \theta/2 & -\sin \theta/2 \\ \sin \theta/2 & \cos \theta/2 \end{pmatrix} \). The corresponding circuit is given in Fig 3. According to the quantum strategy, Alice and Bob share maximally entangle state prior to the game. Applying Hadamard gate on \( a_0 \) followed by CNOT gate on both \( a_0 \) and \( b_0 \), where \( a_0 \) is the controlled bit, we generate the maximally entangled state \( |00⟩ + |11⟩ \) between Alice and Bob. Controlled-Hadamard serves Alices’s strategy, i.e., if \( x = 0 \), Alice will measure her sub-system in \( \{0⟩, |1⟩\} \) basis (no Hadamard applied), else she will measure it in \( \{+⟩, |−⟩\} \) basis (Hadamard applied), where \( |+⟩ = \frac{1}{\sqrt{2}}(|0⟩ + |1⟩) \) and \( |−⟩ = \frac{1}{\sqrt{2}}(|0⟩ − |1⟩) \). Similarly, \( CU_3 \) serves Bob’s strategy, i.e., if \( y = 0 \), Bob will measure his sub-system in \( \{π/8⟩, −π/8⟩\} \) basis (first \( CU_3 \) from left) and else in \( \{3π/8⟩, −3π/8⟩\} \) basis (second \( CU_3 \) from left), where |\(π/8⟩ = \cos(π/8) |0⟩ + \sin(π/8) |1⟩, |−π/8⟩ = −\sin(π/8) |0⟩ + \cos(π/8) |1⟩, and \(3π/8⟩ = \cos(3π/8) |0⟩ + \sin(3π/8) |1⟩, |−3π/8⟩ = −\sin(3π/8) |0⟩ + \cos(3π/8) |1⟩\).

Here we set \( \theta = π/4 \) when \( U_3 \) has been constructed. We compute the probability considering the reduced density matrix of \( b_0 \). We obtained 0.85 (taking two decimal places) for the bit 0 and 0.15 for the bit 1.

In the following section, we will show how we exploit this Boolean circuit in SIMON and improve the bias.

### IV. BOOLEAN CHSH GAME FOR IMPROVING THE BIAS OF SIMON

To exploit the Boolean circuit of CHSH game in SIMON, we need to design SIMON round function in quantum domain. We assume that we have \( k\)-qubits reserved for the key, \( K \), and \( n\)-qubits each for \( L \) and \( R \). The classical Boolean operations are now replaced by the quantum
reversible gates. The replacement is as follows. For detail explanation one may explore [34].

1. ‘AND’ is replaced by Toffoli,

2. ‘XOR’ is replaced by CNOT.

Thus the quantum version of SIMON round function will be as follows.

\[
F(x, y) = CNOT((CNOT(K_i(j), R_i(j)), \\
CNOT((Toffoli(L_i(j + 1), \\
L_i(j + 8), R_i(j)), L_i(j + 2))))
\]

where, \(L_i(j + m)\) represents \(m\) bits shift on \(L_i(j)\), i.e., \(S^m(L_i(j))\). The corresponding circuit is presented in Fig 4. Here, \(q_0, q_1, q_2\) and \(q_3\) represent \(L_i(j), L_i(j + 1), L_i(j + 2)\) and \(L_i(j + 8)\) respectively. \(r_0\) represents \(R_i(j)\) and \(k_0\) stand for \(K_i(j)\). Hadamard gates are taking care of all possible input states. In this case, there is no bias found, i.e, probability of the random variable 0 is 1/2 and probability of the random variable 1 is also 1/2. However, we observe that if for a round \(i\), \(L_i(j) = L_i(j + 2)\), then the followings happen. Such situation is picturized by the circuit given in Fig 5.

\[
\begin{align*}
\Pr(L_i(j) \oplus L_{i+1}(j) = 0) & = R_i(j) = K_i(j) = 3/4, \\
\Pr(L_i(j) \oplus L_{i+1}(j) = 1) & = R_i(j) = K_i(j) = 1/4.
\end{align*}
\]

In this circuit, \(q_0, q_1, q_2\) and \(q_3\) represent \(L_i(j), L_i(j + 1), L_i(j + 2)\) and \(L_i(j + 8)\) respectively. As \(L_i(j) = L_i(j + 2)\), we put CNOT gate on \(q_0\) and \(q_2\) considering \(q_0\) as control bit. CNOT gate operates as a cloning machine here. \(q_0\) is copied into \(q_2\) making \(L_i(j) = L_i(j + 2)\). Similarly, as \(R_i(j) = K_i(j)\), we again apply CNOT gate on \(r_0\) so that it will be copied into \(k_0\). Other parts of the circuit remain same. After the second barrier, we apply CNOT gate on \(q_0\) and \(r_0\) to take care of the linear relation between \(L_i(j)\) and \(L_{i+1}(j)\), i.e., \(L_i(j) \oplus L_{i+1}(j)\).

We modify the circuit with Boolean CHSH game and observe that \(\Pr(L_i(j) \oplus L_{i+1}(j) = 0) = R_i(j) = K_i(j) = 0.85\) and \(\Pr(L_i(j) \oplus L_{i+1}(j) = 1) = R_i(j) = K_i(j) = 0.15\). The modified circuit is given in Fig 6. We also prove that the optimal probability is 0.85. Calculations for different choices of \(q_1\) and \(q_3\), i.e., for all possible options between \(L_i(j + 1)\) and \(L_i(j + 8)\) are shown in the supplementary material [35]. We do not consider other bits, as in this case, \(L_i(j) = L_i(j + 2)\) and \(K_i(j) = R_i(j)\). We have implemented all the circuits in IBMQ interface. For the experiments, we use IBMQ simulator. The codes for the linear approximation and its modified version are also provided in [35].

V. LINEAR CRYPTANALYSIS

In this section we briefly describe the linear cryptanalysis method and show the improvements which can be achieved over the existing results of linear cryptanalysis against SIMON.

Linear cryptanalysis is a powerful statistical method introduced by Matsui [36]. The method is used to analyze various symmetric primitives. In this attack model, the adversary tries to compute some linear relations between some plaintext bits \(p_i\), ciphertext bits \(c_i\) and some subkey bits \(k_i\). For a given cipher the following relation must hold with some non-random probability

\[
\Pr\left[\bigoplus_j p_i \oplus \bigoplus_j c_i = \bigoplus_j k_i \right] = p = \frac{1}{2} + \epsilon.
\]

The effectiveness of this linear expression depends on the bias \(|\epsilon|\). In general, the larger the bias \(|\epsilon|\) from the random, the more effective the linear approximation. To combine multiple approximations of a cipher, Matsui [36] proposed a Lemma, known as the Filing-up Lemma [35].

In [36], Matsui focused on Data Encryption Standard (DES) [29] and computed the success probability...
of the linear cryptanalysis for the given number of random plaintext-ciphertext pairs, $N$ and the probability of the linear approximation $p$. Later, Selcuk \cite{37} provides generalized computation for success probability and data complexity. He considered the problem where an attacker wants to obtain the right $m$-bit key within the $r$ most probable key candidates, with an approximation of probability $p$ using $N$ plaintext-ciphertext blocks. He showed that to achieve at least an 8-bit advantage, one needs $N = 8(p - 1/2)^{-2}$ with a success probability of about 99.7\%, \cite{37 Table 2].

In case of SIMON, for any round $i$, the ‘AND’ operation behaves equally on each bit of $L_i$. Hence, we will get the same bias $\epsilon$ for each approximation $L_i(j) \oplus L_{i+1}(j)$. Assuming we have $m$ number of approximations and applying piling-up lemma we can write $p = 1/2 + 2^{m-1} \cdot \epsilon^m$. In this case, the number of required known plaintext-ciphertext pairs will be $N = 8 \cdot (2^{m-1} \cdot \epsilon^m)^{-2} = 2^{-2m+5} \cdot (\epsilon^m)^{-2}$.

Now, for an exhaustive search for the right key, the attacker needs $2^n - 1$ known plaintext-ciphertext pairs (omitting all zero state), where $n$ is the block size of the cipher. Since, $m$ must be an integer, assuming $N = 2^{n-1}$ does not change the value of $|m|$. Therefore, for the sake of simplicity, we proceed with the calculations considering $N = 2^{n-1}$. To make the attack successful over exhaustive search with probability 99.7\% we must need the following.

$$2^{-2m+5} \cdot (\epsilon^m)^{-2} \leq 2^{n-1}. \quad (2)$$

Now, we consider SIMON 32/64 variant (i.e. $n = 32$). Using Eqn 2 and the improved bias, $\epsilon = 0.35 = 2^{-1.5}$, we get the number of approximations $m \leq 26$, while in \cite{30} it was $m \leq 13$ as the bias, $\epsilon$, was 0.25. This clearly indicates the improvements in the number of rounds that could be attacked and in the number of plaintext-ciphertext pairs. We will now see how it would be possible.

The general sequence of required approximations in every round, starting from a single bit in the middle of the rounds, for any variant of SIMON up to 21 rounds is $5, 5, 4, 4, 3, 3, 2, 2, 1, 1, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5$ \cite{30}. However, for SIMON 32/64 the sequence is slightly better; $5, 5, 4, 4, 3, 3, 1, 2, 1, 1, 0, 1, 1, 2, 1, 3, 3, 4, 4, 5, 5$ \cite{30}. For example, for 9 rounds of SIMON 32/64, the total number of approximations will be $1+2+1+1+0+1+1+2+1 = 10$, for 11 rounds it will be $3+1+2+1+1+0+1+1+2+1+3 = 16$, for 13 rounds the number would be $3+3+1+2+1+1+0+1+1+2+1+3+3 = 22$, for 15 rounds it would be $4+3+3+1+2+1+1+0+1+1+2+1+3+3+3+4 = 30 > 26$. So, the number of approximations for 15 rounds exceed the limit of the approximations for the bias 0.35. Therefore, we can make use of at most 13 round approximations here. In this case the number of known plaintext-ciphertext pairs would be $N = 2^{27}$. Contrary to this, in \cite{30} only 9 round approximations can be taken into account as the maximum limit for the approximations was 13.

It can also be shown that the number of rounds which can be attacked with the given approximations are obtained by appending one round at the bottom and another one at the top without additional workload. For example, if the approximations are taken for 9 rounds, then the attack can be mounted on 11 rounds and so on. In Table \ref{Table:2} we summarize the improvements which have been achieved due to the uplifting of the bias over some existing linear cryptanalysis against SIMON.

|           | # rounds | Approx m | Data     |
|-----------|----------|----------|----------|
| Abed et al. \cite{30} | 11       | 9        | $2^{25}$ |
| This work  | 11       | 9        | $2^{10}$ |
| Alizadeh et al. \cite{33} | 13      | 11       | $2^{24}$ |
| This work  | 13       | 11       | $2^{20}$ |
| This work  | 15       | 13       | $2^{27}$ |

\textbf{TABLE II. Linear Cryptanalysis of SIMON32/64 using Matsui’s method \cite{30}. $m =$ number of approximations, Approx $=$ number of rounds for linear approximation, #rounds $=$ number of attacked rounds.}

\section{VI. DISCUSSIONS AND CONCLUSION}

In the present initiative, we have shown how to improve the bias of a classical lightweight cipher, SIMON, exploiting CHSH game. In the domain of \textit{Quantum Cryptanalysis on Symmetric Ciphers} we mainly study the impact of Grover’s search algorithm \cite{14}, Simon period finding algorithm \cite{15} and the combination of both on block ciphers.

Contrary to these, in the present draft, we opt a completely different kind of approach where bias of a random variable has been improved exploiting quantum CHSH game. This has a major impact in linear and differential cryptanalysis.

Here, we consider lightweight cipher SIMON. However, this technique can be extended to the ciphers having the bias 0.25. We believe that this finding will open-up a new direction of research in the domain of quantum cryptography.

Finally, the result again proves the quantum advantage over classical paradigm. In quantum regime, the symmetric ciphers are not as secure as those are in classical domain. We may need less samples to distinguish two probability distribution functions $p$ and $q$ in quantum paradigm.

Our future research will be directed towards the linear and differential cryptanalysis of different symmetric ciphers having bias 0.25. It might be possible to design various CHSH like games which can be exploited to improve the bias of existing ciphers not having the bias of 0.25. We like to explore all such games in future.
Langenberg, B., Pham, H. and Steinwandt, R., Reducing the cost of implementing the advanced encryption standard as a quantum circuit. IEEE Transactions on Quantum Engineering, 1, pp.1-12, 2020.

Bonnetain, X., Naya-Plasencia, M. and Schrottenloher, A., Quantum security analysis of AES. IACR Transactions on Symmetric Cryptology, 2019(2), pp.55-93, 2019.

Leander, G. and May, A., Grover meets Simon–quantumly attacking the FX-construction. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 161-178). Springer, Cham, 2017.

Bernstein, D.J., Grover vs. Mceliece. In International Workshop on Post-Quantum Cryptography (pp. 73-80). Springer, Berlin, Heidelberg, 2010, May.

Kuwakado, H. and Morii, M., Security on the quantum-type Even-Mansour cipher. In 2012 International Symposium on Information Theory and its Applications (pp. 312-316). IEEE, 2012, October.

Kaplan, M., Quantum attacks against iterated block ciphers. arXiv preprint arXiv:1410.1434, 2014.

Kaplan, M., Leurent, G., Leverrier, A. and Naya-Plasencia, M., Breaking symmetric cryptosystems using quantum period finding. In Annual international cryptography conference (pp. 207-237). Springer, Berlin, Heidelberg, 2016.

Hosoyamada, A. and Sasaki, Y., Quantum demirci-serduk meet-in-the-middle attacks: applications to 6-round generic Feistel constructions. In International Conference on Security and Cryptography for Networks (pp. 386-403). Springer, Cham, 2018.

Hosoyamada, A. and Sasaki, Y., Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations. In Cryptographers? Track at the RSA Conference (pp. 198-218). Springer, Cham, 2018.

Leurent, G., Kaplan, M., Leverrier, A. and Naya-Plasencia, M., Quantum differential and linear cryptanalysis. In FSE 2017-Fast Software Encryption, 2017.

Santoli, T. and Schaffner, C., Using Simon’s Algorithm to Attack Symmetric-Key Cryptographic Primitives. Quantum Information and Computation, 17(1&2), pp.65-78, 2017.

Stinson, D.R., 2005, Cryptography: Theory and Practice, Third Edition, Chapman & Hall/CRC.

Abed, F., List, E., Lucke, S. and Wenzel, J., Differential and linear cryptanalysis of reduced-round SIMON. Cryptology ePrint Archive, Report 2013/526, 2013.

Alizadeh, J., Bagheri, N., Gauravaram, P., Kumar, A. and Sanadhya, S.K., Linear Cryptanalysis of Round Reduced SIMON. IACR Cryptol. ePrint Arch., 2013, p.663, 2013.

Alizadeh, J., Bagheri, N., Gauravaram, P., Kumar, A. and Sanadhya, S.K., Cryptanalysis of SIMON variants with connections. In International Workshop on Radio Frequency Identification: Security and Privacy Issues (pp. 90-107). Springer, Cham, 2015.

Anand, R., Maitra, A. and Mukhopadhyay, S., Grover on SIMON. Quantum Information Processing, 19(9), pp.1-
17, 2020.
[35] Supplementary Material; all the calculations and the codes for IBMQ implementation are available here.
[36] Matsui, M., Linear cryptanalysis method for DES cipher. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 386-397). Springer, Berlin, Heidelberg, 1993.
[37] Selçuk, A.A., On probability of success in linear and differential cryptanalysis. Journal of Cryptology, 21(1), pp.131-147, 2008.