IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 May 2023, accepted 22 June 2023, date of publication 26 June 2023, date of current version 7 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3289764

RESEARCH ARTICLE

Compact Quantum Circuit Design of PUFFIN and PRINT Lightweight Ciphers for Quantum Key Recovery Attack

SARAVANAN PARAMASIVAM[1], (Senior Member, IEEE), J. JENITHA[1], S. SANJANA[1], AND MAJID HAGHPARAST[2], (Senior Member, IEEE)

[1]Department of Electronics and Communication Engineering, PSG College of Technology, Coimbatore, Tamil Nadu 641004, India
[2]Faculty of Information Technology, University of Jyväskylä, 40014 Jyväskylä, Finland

Corresponding author: Majid Haghparast (majid.m.haghparast@jyu.fi)

This work was supported by the Academy of Finland under Project DEQSE 349945.

ABSTRACT Quantum computing plays a vital role in the next generation computing platforms as researchers have achieved quantum supremacy by proving that quantum computers can outperform classical computers. These high performance computers will pose a serious threat to the security of the conventional cryptographic algorithms. The secret key of the conventional cryptographic algorithms when implemented by quantum circuits can be recovered easily with the help of Grover key search algorithm. The Grover's algorithm requires low cost quantum implementation of cryptographic algorithms in order to mount the quantum key recovery attack successfully. Hence the low cost quantum implementation of conventional cryptographic algorithms to mount quantum key recovery attack using Grover search algorithm is an active area of research. For the first time in literature, this work proposes a novel quantum circuit implementation of two lightweight block ciphers namely PUFFIN and PRINT. Inplace method is used to optimize the quantum resources in these two ciphers which helps to build compact quantum circuits without extra ancilla inputs. The performance metrics considered in this work to quantify the quantum resources of the proposed circuits are number of quantum gates, quantum cost, latency and number of qubits. In addition, the quantum resources are also estimated to mount the quantum key recovery attacks on the proposed quantum circuit implementations of PUFFIN and PRINT using Grover-based key search algorithm.

INDEX TERMS Cryptography, Grover's search algorithm, lightweight cipher, PUFFIN, PRINT, quantum computing, quantum circuit, quantum cost, quantum key recovery attack.

I. INTRODUCTION

Quantum computing makes use of the phenomena of quantum mechanics to solve certain intractable problems which cannot be solved by using classical computers [1]. One such intractable problem is the brute force attack in cryptographic algorithms wherein the adversary guesses the secret key by trying all possible combinations of the secret keys. The cryptographers community claimed that it would take years of time to mount brute force attack due to the limitations in the performance of the conventional computing platforms. But due to the advent of Grover's quantum key search algorithm, the time complexity involved in guessing the secret key is reduced from O(n) to $O(\sqrt{n})$ due to the quantum parallelism in the quantum computers [2]. For a successful quantum key recovery attack, optimal design of quantum circuits for cryptographic algorithms is an active area of research.

Quantum supremacy was significantly demonstrated in the quantum algorithms of Shor, for solving the discrete logarithm problem of factorization and of Grover, for a brute-force key search of size n-bits with O($\sqrt{n}$) steps. Recently, classical search algorithm was used as a preprocessor to Grover's search algorithm in order to lower the quantum circuit complexity [3]. Quantum circuits are widely used

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

in cryptographic applications due to the improvement in performance when compared to their traditional counterparts. The time-space complexity of quantum search algorithms targeting cryptographic functions were investigated in [4]. Novel quantum circuits were presented for all the three standardized key lengths of AES with reduction in quantum gates in [5]. As a follow up, the work in [6] proposed quantum circuits for the block ciphers AES and LowMC and studied the cost of quantum key search attacks under depth restrictions.

Lightweight cryptography (LWC) aims at expanding the applications of cryptography to resource constrained environments by keeping a small footprint and low computational complexity in the target implementation platform. The preferred lightweight properties are the reduction in chip size and energy consumption for hardware implementations and reduction in code size and RAM size for software implementations. The compact quantum circuit design of several lightweight ciphers were presented in literature for quantum key recovery attack using Grover's algorithm. The work in [7] proposed quantum circuit for RECTANGLE lightweight cipher and estimated the quantum resources for both 80-bit and 128-bit key lengths. The Sbox designs were optimized by LIGHTER-R tool [8] and in-place implementation was carried out to remove the ancilla inputs and garbage outputs. The quantum circuits for PRESENT and GIFT block ciphers were presented in [9] with optimal number of quantum resources by minimizing qubits, quantum gates and circuit depth.

The quantum circuit design of all variants of SIMON lightweight cipher was presented in [10] and the quantum resources were enumerated to mount attack based on Grover's key search algorithm. The quantum circuit designs of the various Korean made lightweight block ciphers such as HIGHT, CHAM, LEA and the NSA made lightweight block cipher, namely SPECK were demonstrated in [11]. The in-place implementation of GIMLI lightweight cipher was presented in [12]. Quantum reversible circuit of a Korean standardized block cipher namely ARIA was presented in [13]. The upper bounds for the number of qubits and the number of Clifford+T gates required to mount Grover's key search attack were presented.

A compact block cipher with low hardware complexity known as PUFFIN was proposed in [14]. The PRINT block cipher was mainly proposed to exploit the properties of IC-printing technology [15]. The main objective of [16]search work is to attack the two cryptographic algorithms PUFFIN and PRINT with Grover's key search algorithm and to extract the secret keys. In order to mount the attack, novel quantum circuits are developed for the two lightweight block ciphers PUFFIN and PRINT. The PUFFIN block cipher follows Substitution and Permutation Network (SPN) and it absorbs 64-bit plaintext and 128-bit key to produce 64-bit ciphertext after 32 identical rounds of operations. The PRINT is based on the SPN structure which has the following two variants 48 and 96. In both the ciphers, in-place implementation using LIGHTER-R tool is employed to achieve optimal qubits without ancilla inputs and garbage outputs. The quantum resources required to mount the quantum key recovery attacks on the proposed quantum circuit implementations of PUFFIN and PRINT ciphers are also estimated.

TABLE 1. Sbox used in PUFFIN cipher.

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

The paper is organized as follows. A brief introduction to the two lightweight ciphers PUFFIN, PRINT and Grover's search algorithm are given in Section II and Section III respectively. Section IV describes the proposed quantum circuit for PUFFIN cipher, followed by its performance analysis in Section V. Section VI describes the proposed quantum circuit for PRINT cipher, followed by its performance analysis in Section VII. Section VIII presents a comparative analysis of the proposed quantum circuits with the existing ones. Section IX details the quantum resources estimation for applying Grover's search algorithm. Section X draws the conclusion of the paper along with noted references.

II. ABOUT THE ALGORITHM

A. PUFFIN LIGHTWEIGHT CIPHER

PUFFIN is a block cipher which takes 64-bit plaintext, 128-bit key and produces 64-bit ciphertext. It follows the substitution and permutation network (SPN) structure and performs an initial round followed by 32 identical rounds of operation as shown in Fig. 1. In this cipher, the round operations are involutional which means identical round operations are performed on both the encryption as well as decryption processes. Each round operation is carried out by using three layers of sub-operations.

The first layer also termed as Substitution layer (Sbox) performs nonlinear substitution operation on 64-bit input data using sixteen involutional 4×4 Sboxes and produces 64-bit output data. The Sbox used in PUFFIN cipher is given in Table 1.

The second layer also termed as AddRoundKey layer performs data whitening operation on 64-bit input data using 64-bit unique roundkey and produces 64-bit output data. The data whitening operation can be performed with logical XOR operation.

The third layer also termed as Permutation layer (P64) performs transposition of the 64-bit input data and produces 64-bit output data.

The three layers of operations are repeated among 32 identical rounds using 32 unique sets of 64-bit roundkey to produce the 64-bit ciphertext. In the initial round, the Substitution layer operation alone is skipped from the round operation and the remaining operations such as AddRoundKey and Permutation are performed. The key generation algorithm produces 33 64-bit round keys from

TABLE 2. Permutation used in PUFFIN cipher.

	0	1	2	3	4	5	6	7
0	13	2	60	50	51	27	10	36
1	25	7	32	61	1	49	47	19
2	34	53	16	22	57	20	48	41
3	9	52	6	31	62	30	28	11
4	37	17	58	8	33	44	46	59
5	24	55	63	38	56	39	15	23
6	14	4	5	26	18	54	42	45
7	21	35	40	3	12	29	43	64

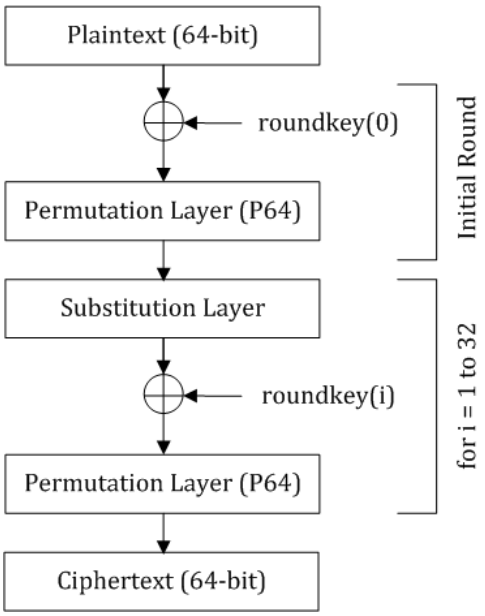

FIGURE 1. Algorithmic steps in PUFFIN encryption process.

the 128-bit secret key given by the user. In order to reduce the complexity, nonlinear operations are not used in the process and only permutation and selected bit inversions are involved. The permutation table for the transposition of 64-bit is given in Table 2. The selected key bit inversions are not performed in second, fifth, sixth and eighth rounds. In the remaining 28 rounds, the key bits 1, 2, 3 and 5 alone will be complemented. The compression operation selects 64 from the 128-bit key.

B. PRINT LIGHTWEIGHT CIPHER

PRINT is also a block cipher which takes b-bit blocks, b{48,96} as plaintext and produces b-bit blocks of ciphertext with the help of (5/3) x b bits of key. It follows the SPN structure and performs b identical rounds of operation. Each round operation is carried out by using five layers of sub-operations. The PRINT cipher-48 variant takes 48-bit plaintext and produces 48-bit ciphertext with 80-bit key using 48 rounds whereas the PRINT cipher-96 variant takes 96-bit plaintext and produces 96-bit ciphertext with 160-bit key using 96 rounds of operation.

TABLE 3. Sbox used in PRINT cipher.

X	0	1	2	3	4	5	6	7
S(x)	0	1	3	6	7	4	5	2

The first layer also termed as AddRoundKey layer performs bitwise XOR operation between the current state of the cipher and b-bit subkey.

The second layer also termed as Linear Diffusion Layer performs permutation of 48-bit input data and produces 48-bit output data on the current state of the cipher as per the equation (1).

$$P(i) = \begin{cases} 3 \text{ x } i \bmod b - 1 & for\ 0 \le i \le b-2 \\ b-1 & for\ i = b-1 \end{cases} \quad (1)$$

The third layer also termed as AddRoundCounter (RC_i) layer performs addition of round counter value on the least 6-bit of the current state using bitwise XOR operation for PRINT cipher-48 variant and on the least 7-bit of the current state using bitwise XOR operation for PRINT cipher-96 variant. The round counter value is generated by using a shift register and the contents of the shift register ($x_{n-1} \ldots x_0$) are updated as per the equation (2).

$$\begin{aligned} t &= 1 + x_{n-1} + x_{n-2} \\ x_i &= x_{i-1} \quad for\ n-1 \ge i \ge 1 \\ x_0 &= t \end{aligned} \quad (2)$$

The fourth layer also termed as Keyed Permutation Layer performs b/3 permutations on the current state based on the key values. The b bit of the current state is grouped as b/3 sets with each set consisting of 3-bit. There are four possible key dependent permutations and each b/3 permutation can be chosen from these four possibilities and the chosen permutation is used in the same set in every round.

The fifth layer also termed as Substitution layer (Sbox) performs nonlinear substitution operation on b-bit input data using b/3 3×3 Sboxes as given in Table 3 and produces b-bit output data.

The five layers of operations are repeated among b identical rounds using b sets of b-bit round key from (5/3) x b bits of user key and produce b-bit cipher text. The sequence of operations in the PRINT cipher is shown in Fig. 2. Out of the (5/3) x b-bit user supplied key, the first b bits of key are used in the AddRoundKey operation in each round. The remaining (2/3) x b bit user supplied key are decomposed into b/3 sets of two bits and these two bits are used to pick one from the four possible permutations as given in Table 4.

III. GROVER'S SEARCH ALGORITHM

Grover's Algorithm is a searching algorithm which enables us to find the element with high probability in lower time complexity. The classic method requires O(n) where Grover's

TABLE 4. Permutation used in PRINT cipher.

Input	Bit Position (b2 b1 b0)
00	b2 b1 b0
01	b1 b2 b0
10	b2 b0 b1
11	b0 b1 b2

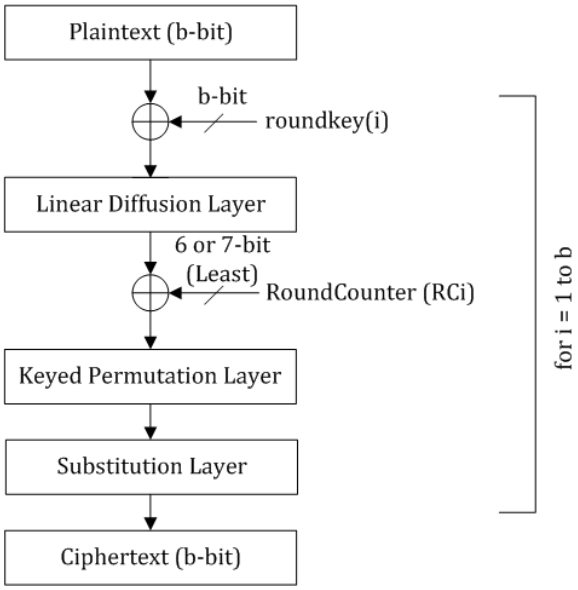

FIGURE 2. Algorithmic steps in PRINT encryption process.

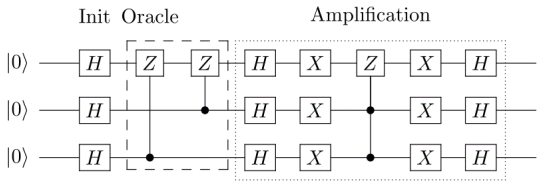

FIGURE 3. Grover's algorithm.

algorithm uses $O(\sqrt{n})$. The quantum description of Grover's algorithm for the three qubits is given in Fig. 3 [16], [17].

If the required element is found then the oracle function $f(x) = 1$, otherwise $f(x) = 0$. Then the oracle function flips the required element. In Fig. 4, if the required element is $|01\rangle$ then the qubit $|01\rangle$ is flipped and the required element's sign is also changed.

The amplification part of Grover's Algorithm deals with increasing the amplitude of the required element as shown in Fig. 5. Thus the amplitude of the required element is increased by performing Oracle and amplification repeatedly.

IV. PROPOSED QUANTUM CIRCUIT FOR PUFFIN CIPHER

In this work, the key steps of PUFFIN lightweight cryptographic algorithm such as AddRoundkey, Substitution Box, Permutation Layer, Key Scheduler are synthesized using ordinary gates and are then mapped to the quantum gates. The quantum gates are reused wherever possible as some of the outputs retains its original value which evenly reduces the quantum cost.

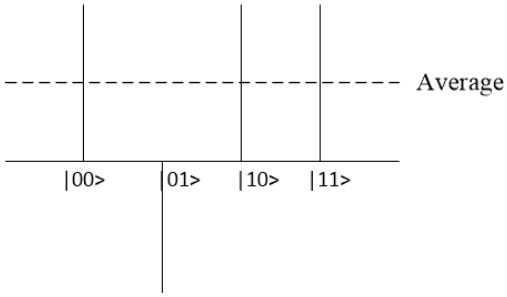

FIGURE 4. Oracle of grover's algorithm.

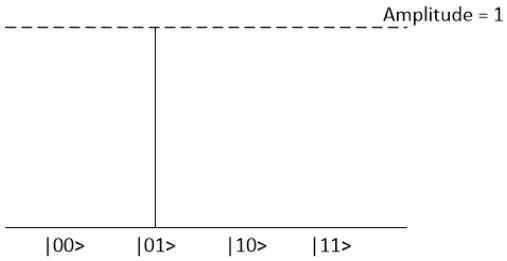

FIGURE 5. Amplification of grover's algorithm.

A. QUANTUM CIRCUIT FOR AddRoundKey

In the encryption module, the AddRoundKey of PUFFIN-64/128 lightweight cipher includes the XOR operation between the 64-bit data and the left most 64-bit of 128-bit key in the first round. In the remaining rounds, the output from substitution layer and Key scheduler are XORed and given to the permutation layer. The XOR operations in AddRoundKey are performed by using CNOT quantum gates. To complete one AddRoundKey operation, 64 CNOT gates are required.

B. QUANTUM CIRCUIT FOR SUBSTITUTION BOX

The PUFFIN algorithm uses 4-bit Sbox and a single substitution layer contains 16 Sboxes. Three variants of Sboxes are designed using quantum gates. The optimal Sbox with less quantum cost is used for designing the complete quantum circuit.

1) SBOX USING ANF

The first variant is designed using Algebraic Normal Form (ANF) method which uses only AND and XOR operation to build the circuit. The boolean expression of the PUFFIN Sbox-1 is derived and are mapped to the quantum gates. In this variant, AND and XOR operations are mapped to CCNOT and CNOT gates and hence consumes more quantum cost. The Quantum circuit design is given in Fig. 6 and the

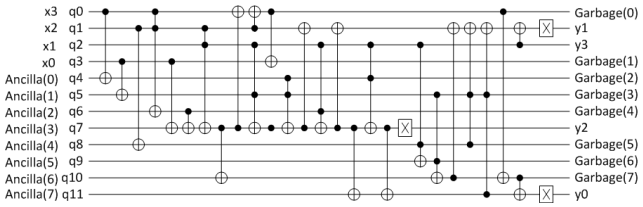

FIGURE 6. Quantum circuit design of Sbox-1 using ANF.

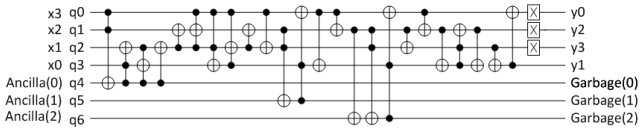

FIGURE 7. Quantum circuit design of Sbox-2 using non search based synthesis.

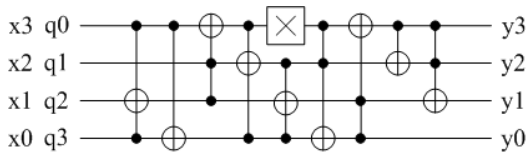

FIGURE 8. Quantum circuit design of Sbox-3 using inplace implementation.

ANF equation is as follows,

$$
\begin{aligned}
y0 &= x0*x2*x3 + x3*x2 + x3*x1 + x3 \\
&\quad + x1*x2*x0 + x1*x2 + x2 + x1*x0 + 1 \\
y1 &= x3*x1*x2 + x0*x1*x3 + x1*x2*x0 \\
&\quad + x2*x0 + x2 + x1*x0 + x1 + 1 \\
y2 &= x0*x2*x3 + x3*x2 + x3 + x1*x2 + x2 + x0 \\
y3 &= x3*x1*x2 + x0*x2*x3 + x3*x2 + x3*x1 \\
&\quad + x0*x3 + x1*x2 + x1*x0 + 1
\end{aligned}
$$

2) SBOX USING NON SEARCH BASED SYNTHESIS ALGORITHM

In the second variant, Non Search Based Synthesis algorithm is employed which makes use of the reversible approach to design the circuit. This results in optimized quantum circuit with reduced quantum cost and qubits than the ANF approach as shown in Fig. 7.

3) SBOX USING INPLACE IMPLEMENTATION

The final variant is designed using inplace method where the one-to-one mapping of this algorithm to the quantum gates results in the quantum circuit with zero ancilla qubits and reduced quantum cost as shown in Fig. 8. The Algorithm is as follows.

C. QUANTUM CIRCUIT FOR P-LAYER

The transposition of bits happens at permutation layer which requires only SWAP gates. The output from permutation layer is passed to the next round. In this operation no quantum cost calculation is involved as Swap gate operation can be obtained by rearranging the qubit labels [9].

Algorithm 1 Quantum circuit for Substitution Layer of PUFFIN using Inplace Method

Input: 4-qubit input x(x3, x2, x1, x0) (before entering Sbox).
Output: 4-qubit output y(y0, y1, y2, y3) (after performing Sbox).
1 : x1 ← Toffoli (x0, x3, x1)
2 : x0 ← CNOT (x3, x0)
3 : x3 ← Toffoli (x1, x2, x3)
4 : x2 ← Toffoli (x0, x3, x2)
5 : x1 ← Toffoli (x0, x2, x1)
6 : x3 ← X (x3)
7 : x0 ← Toffoli (x2, x3, x0)
8 : x3 ← Toffoli (x0, x1, x3)
9 : x2 ← CNOT (x3, x2)
10: x1 ← Toffoli (x2, x3, x1)
11: return x(x2, x1, x0, x3)

D. QUANTUM CIRCUIT FOR KEY SCHEDULER

The key scheduler of PUFFIN does not require any non-linear operation. It performs only permutation and selected bit inversion. The permutation operation can be done by using SWAP gates. For selected bit inversion, only four bits in the position 1, 2, 3 and 5 are inverted. Therefore for one round only four Pauli X gates are required. And this selected bit inversion will not happen at second, fifth, sixth and eighth key rounds.

V. PERFORMANCE ANALYSIS

A. QUANTUM COST ESTIMATION OF DESIGNED SBOXES

The quantum resources and cost estimation of the three variants of designed Sboxes are given in the Table 5. It is clear that Sbox-3 which is designed using inplace method consumes less quantum resources than the other two. In addition, the latency of Sbox-3 is also minimal which results in faster operation. Therefore Sbox-3 is considered for building the PUFFIN quantum circuit.

B. QUANTUM COST ESTIMATION OF PUFFIN CIPHER BUILDING BLOCKS

Quantum resources required for the designed AddRoundkey, Substitution Layer, Permutation Layer and Key-Scheduler are given in Table 6. As mentioned Earlier, the Sbox-3 which is designed using inplace method is considered for quantum cost calculation. Since the permutation operation uses only swap gates to just rearrange the wires, it is not included in the cost calculation.

C. QUANTUM COST ESTIMATION OF ROUND OPERATION

The quantum resources for the first round of operation in PUFFIN-64/128 is estimated and tabulated. Table 7 shows the

TABLE 5. Quantum cost estimation of designed Sboxes.

Sbox Designs	Number of Gates				Quantum Cost				Latency	Qubits	Ancilla
	Toffoli	CNOT	Pauli-X	Size	Toffoli	CNOT	Pauli-X	Total			
Sbox-1: ANF	14	11	3	28	70	11	3	84	20	12	8
Sbox-2: Non-Search Based	11	13	3	27	55	13	3	71	26	7	3
Sbox-3: Inplace Method	7	2	1	10	35	2	1	38	10	4	0

TABLE 6. Quantum cost estimation Of PUFFIN cipher building block.

Building Blocks	Number of Gates				Quantum Cost			
	Toffoli	CNOT	Pauli-X	Size	Toffoli	CNOT	Pauli-X	Total
AddRoundKey	0	64	0	64	0	64	0	64
SubColumn using Sbox-3	112	32	16	160	560	32	16	608
ShiftRows	0	0	0	0	0	0	0	0
Key scheduler-128	0	0	4	4	0	0	4	4

TABLE 7. Quantum cost estimation for one round of PUFFIN cipher.

Design Variants	Number of Gates				Quantum Cost				Qubits
	Toffoli	CNOT	Pauli-X	Size	Toffoli	CNOT	Pauli-X	Total	
PUFFIN 64/128 (Proposed)	112	96	20	228	560	96	20	676	192

quantum cost estimation of Round 1 operation implemented with Sbox designed using inplace technique (Sbox-3). The proposed quantum circuit for one round of PUFFIN cipher takes 228 quantum gates with a quantum cost of 676. The substitution layer has a latency of 10 and XORing each roundkey has a latency of 1. Hence the total delay estimation for 32 rounds would sum up to 353 along with a delay of 1 for XORing roundkey 0.

VI. PROPOSED QUANTUM CIRCUIT FOR PRINT CIPHER

A. QUANTUM CIRCUIT FOR KEY-XOR

The key length of (5/3) × b is XORed with plaintext. The XOR operation can be performed using Quantum CNOT gates for 48-bit plaintext 16 CNOT gates are required and for 96-bit plaintext 32 CNOT gates are required.

B. QUANTUM CIRCUIT FOR LINEAR DIFFUSION

The linear diffusion is a rewiring operation and can be done with only swap gates whose operation can be obtained by rearranging the qubit labels.

C. QUANTUM CIRCUIT FOR ROUND COUNTER

The RoundCounter RC_i is XORed with the least significant bits of the current values. Since the RoundCounter values are already known, Pauli-X gates which have unit quantum cost can be directly used based on the number of bit changes instead of using CNOT gates and additional qubits.

D. QUANTUM CIRCUIT FOR KEYED PERMUTATION

The permutation is based on the key values provided and this layer requires only the swapping of values which can be obtained by rearranging the qubit labels. The output of this layer is given to the substitution layer.

E. QUANTUM CIRCUIT FOR S-LAYER

The PRINT cipher uses 3 qubit Sbox circuits which can be derived using various classical techniques and can be mapped to the quantum circuit.

1) SBOX USING ANF

The first approach used to design the Sbox is Algebraic Normal Form (ANF) which employs only AND and XOR gates. The Boolean expressions of the PRINT Sbox are derived first and are then mapped to the quantum circuit. This method uses ancillas and consumes more quantum cost as given by Fig. 9. The ANF expressions are as follows,

$$y0 = x0 + x1 * x2$$
$$y1 = x0 + x1 + x0 * x2$$
$$y2 = x0 + x1 + x2 + x0 * x1$$

2) SBOX USING NON-SEARCH BASED SYNTHESIS ALGORITHM

The non-search based synthesis algorithm uses the reversible approach to obtain the circuit. This method consumes less

TABLE 8. Quantum cost estimation of designed Sboxes.

Sbox Designs	Number of Gates				Quantum Cost				Latency	Qubits	Ancilla
	Toffoli	CNOT	Pauli-X	Size	Toffoli	CNOT	Pauli-X	Total			
Sbox 1: ANF	3	5	0	8	15	5	0	20	8	5	2
Sbox 2: Non-Search Based	3	4	0	7	15	4	0	19	7	3	0
Sbox 3: Inplace Method	3	2	0	5	15	2	0	17	5	3	0

TABLE 9. Quantum cost estimation of PRINT-48 cipher building block.

Building Blocks	Number of Gates				Quantum Cost			
	Toffoli	CNOT	Pauli-X	Size	Toffoli	CNOT	Pauli-X	Total
Key-XOR	0	48	0	48	0	48	0	48
Linear Diffusion	0	0	0	0	0	0	0	0
Bitwise XOR based on Round-Counter (All rounds)	0	0	154	154	0	0	154	154
Keyed Permutation Layer	0	0	0	0	0	0	0	0
Substitution Layer using Sbox-3	48	32	0	80	240	32	0	272

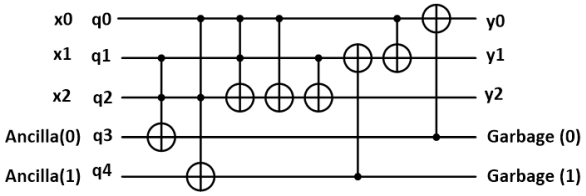

FIGURE 9. Quantum circuit design of Sbox-1 using ANF.

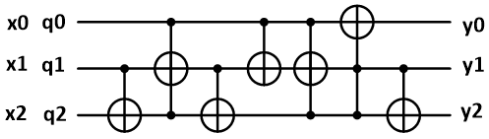

FIGURE 10. Quantum circuit design of Sbox-2 using non-search based synthesis algorithm.

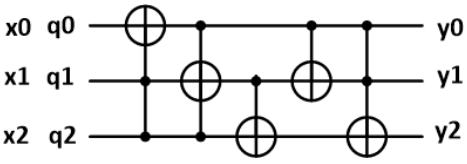

FIGURE 11. Quantum circuit design of Sbox-3 using inplace implementation.

quantum cost than the ANF method. The circuit is given in Fig. 10.

3) SBOX USING INPLACE IMPLEMENTATION

The final variant of Sbox is designed using inplace method. The steps involved in the quantum circuit of PRINT Sbox are deduced in Algorithm 2. The one-to-one mapping of this algorithm to a quantum circuit consumes less quantum cost when compared to the previous variants as shown in Fig. 11.

Algorithm 2 Quantum circuit for Substitution layer of PRINT using Inplace Method

Input: 4-qubit input x(x0, x1, x2) (before entering Sbox).
Output: 4-qubit output y(y0, y1, y2) (after performing Sbox).
1: x0 ← Toffoli (x1, x2, x0)
2: x1 ← Toffoli (x0, x2, x1)
3: x2 ← CNOT (x1, x2)
4: x1 ← CNOT (x0, x1)
5: x2 ← Toffoli (x0, x1, x2)
6: return x(x0, x1, x2)

VII. PERFORMANCE ANALYSIS

A. QUANTUM COST ESTIMATION OF DESIGNED SBOXES

The quantum resource estimation of designed Sboxes using various approaches are given in Table 8. The ANF method consumes more quantum resources than the other approaches. Non-search based Synthesis algorithm uses zero Ancillas but has increased quantum cost than the inplace approach.

B. QUANTUM COST ESTIMATION OF PRINT CIPHER BUILDING BLOCKS

The AddRoundKey operation uses only CNOT gates based on the size of plain text. PRINT-48 consumes 48 CNOT gates

TABLE 10. Quantum cost estimation of PRINT-96 cipher building block.

Building Blocks	Number of Gates				Quantum Cost			
	Toffoli	CNOT	Pauli-X	Size	Toffoli	CNOT	Pauli-X	Total
Key-XOR	0	96	0	96	0	96	0	96
Linear Diffusion	0	0	0	0	0	0	0	0
Bitwise XOR based on Round-Counter (All rounds)	0	0	352	352	0	0	352	352
Keyed Permutation Layer	0	0	0	0	0	0	0	0
Substitution Layer using Sbox-3	96	64	0	160	480	64	0	544

TABLE 11. Quantum cost estimation for first round of PRINT cipher.

Design Variants	Number of Gates				Quantum Cost				Qubits
	Toffoli	CNOT	Pauli-X	Size	Toffoli	CNOT	Pauli-X	Total	
PRINT-48 (Proposed)	48	80	1	129	240	80	1	321	128
PRINT-96 (Proposed)	96	160	1	257	480	160	1	641	256

TABLE 12. Comparison of quantum resources with other block ciphers.

Ciphers	Toffoli	CNOT	Pauli-X	Total Gates	Quantum Cost	Depth	Qubits
AES-128/128[5]	16,940	107,960	1507	126,407	194,167	1880	864
AES-128/192[5]	19,580	125,580	1692	146,852	225,172	1640	896
AES-128/256[5]	23,760	151,011	1992	176,763	271,803	2160	1232
RECTANGLE-64/80 [7]	2000	4964	567	7531	15,531	226	144
RECTANGLE-64/128 [7]	2400	6264	667	9331	18,931	226	192
PRESENT-64/80 [9]	2108	4683	1118	7909	16,341	311	144
PRESENT-64/128 [9]	2232	4838	1164	8234	17,162	311	192
GIFT-64/128 [9]	1792	1792	3261	6845	14,013	308	192
GIFT-128/128 [9]	6144	6144	10,953	23,241	47,817	528	256
SIMON-64/128 [10]	1408	7396	1216	10,020	15,652	2643	192
SIMON-128/128 [10]	4352	17,152	4224	25,728	43,136	8427	256
PHOTON 128/256 [18]	18,432	315,328	10369	344,129	417,857	3371	18,944
ASCON 128/256 [18]	55,296	159,232	97,346	311,874	533,058	2,487	35,136
XOODYAK 128/256 [18]	13,824	50,944	27,754	92,522	147,818	760	14,464
PUFFIN-64/128 (Proposed)	3584	3136	620	7340	21,676	353	192
PRINT-48/80 (Proposed)	2304	3840	154	6298	15,514	336	128
PRINT-96/160 (Proposed)	9216	15,360	352	24,928	61,792	672	256

TABLE 13. Resource Estimation for a Grover-based key search.

Design Variants	Toffoli	CNOT	Pauli-X	Total Gates	Quantum Cost	Qubits
PUFFIN-64/128	14,336	12,800	2480	29,616	86,960	385
PRINT-48/80	9216	15,520	616	25,353	62,216	257
PRINT-96/160	36,864	61,760	1408	100,032	247,488	513

and PRINT-96 consumes 96 CNOT gates. The linear diffusion layer and permutation layer do not consume quantum cost as they use only SWAP Gates. The addition of Round-Counter values can be performed with Pauli-X gates and the quantum cost varies based on the rounds. For substitution layer, the Sbox designed using inplace method is considered

for estimation. The Quantum Cost Estimation for PRINT-48 cipher is given in Table 9 and PRINT-96 cipher is given in Table 10.

C. QUANTUM COST ESTIMATION OF ROUND OPERATION

The circuit designed using Sbox-3 is used for resource calculation. The first round cost estimation of PRINT-48 and PRINT-96 ciphers is given in the Table 11. For remaining rounds, the cost varies based on the usage of Pauli-X gates for RoundCounter in respective rounds. The AddRoundKey, the RoundCounter and the substituion layer of the datapath has a latency of 1, 1 and 5 respectively. Hence the total latency of the PRINT cipher calculated from the datapath is 336 for PRINT-48 as it has 48 rounds and 672 for PRINT-96 as it has 96 rounds.

VIII. QUANTUM COST COMPARISON WITH OTHER BLOCK CIPHERS

The quantum resources and quantum cost involved in our proposed quantum circuits of PUFFIN and PRINT cipher are tabulated in Table 12. As there is no quantum circuit design for PUFFIN and PRINT cipher available in the literature, this work is the first of its kind to explore the quantum circuits for PUFFIN and PRINT lightweight cipher algorithm. The quantum resources and quantum cost involved in the quantum circuit design of other cryptographic algorithms are shown in Table 12 for analysis.

IX. APPLYING GROVER'S ALGORITHM ON PUFFIN AND PRINT CIPHER

In this work, Grover's key search algorithm is employed to search the keys in an exhaustive manner with less time complexity. The quantum cost and resources after applying Grover's algorithm are calculated by the method presented in [10]. The number of qubits is calculated by r.q+1, where r = (key size / block size) and q is the number of qubits required to implement the Cipher.

For PUFFIN-64/128, the value of r is 2. The quantum cost of PUFFIN-64/128 is 4 times the required quantum cost since it has 4 instances. For PRINT-48 and PRINT-96 ciphers, the r values are 2 and 1.66 respectively. The quantum cost of PRINT-48 and PRINT-96 is 4 times the required quantum cost since it has 4 instances. Adding to this, 2(r-1)(key size) additional CNOT gates are applied for parallel search. The quantum resources required after applying Grover is shown in the Table 13.

X. CONCLUSION

Compact quantum circuit implementations of conventional cryptographic algorithms pave the way to mount brute-force attack on the cryptographic implementations using Grover's key search algorithm. When a cryptographic algorithm is attacked by the quantum algorithm with enough quantum resources then the confidentiality service can no longer be achieved in it. This work presents novel quantum circuit implementations with minimal quantum resources for the two lightweight ciphers PUFFIN and PRINT in order to successfully mount the Grover's key recovery attack. The individual operations such as AddRoundKey, Sbox, ShiftRows and Key scheduler are implemented using compact quantum circuits with optimal quantum resources in both the ciphers. The proposed quantum circuits of PUFFIN cipher consume 7340 quantum gates with a quantum cost of 21,676 operated on 192 qubits with a latency of 353. The proposed quantum circuits of PRINT cipher 80-bit key variant consume 6298 quantum gates with a quantum cost of 15,514 operated on 128 qubits with a latency of 336 and 160-bit key variant consume 24,928 quantum gates with a quantum cost of 61,792 operated on 256 qubits with a latency of 672. In addition, the quantum resources are also estimated to mount the Grover's key search attack. For PUFFIN cipher, it requires 29,616 quantum gates with a quantum cost of 86,960 operated on 385 qubits. For PRINT cipher with 80-bit key variant, it requires 25,353 quantum gates with a quantum cost of 62,216 operated on 257 qubits and 160-bit key variant requires 100,032 quantum gates with a quantum cost of 247,488 operated on 513 qubits. In order to provide better security against Grover's key search attacks and other quantum attacks, the development of post quantum cryptographic algorithms is in progress (See, e.g., [16]).

ACKNOWLEDGMENT

This work was supported by the Academy of Finland under Project DEQSE 349945.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge, Univ. Press, 2010.
[2] A. Yamamura and H. Ishizuka, "Quantum cryptanalysis of block ciphers (algebraic systems, formal languages and computations)," *RIMS Kokyuroku*, vol. 1166, pp. 235–243, Feb. 2000.
[3] J.-F. Biasse and B. Pring, "A framework for reducing the overhead of the quantum Oracle for use with Grover's algorithm with applications to cryptanalysis of SIKE," *J. Math. Cryptol.*, vol. 15, no. 1, pp. 143–156, Nov. 2020.
[4] P. Kim, D. Han, and K. C. Jeong, "Time-space complexity of quantum search algorithms in symmetric cryptanalysis: Applying to AES and SHA-2," *Quantum Inf. Process.*, vol. 17, no. 12, pp. 1–39, 2018.
[5] B. Langenberg, H. Pham, and R. Steinwandt, "The cost of implementing the advanced encryption standardas a quantum circuit," *IEEE Trans. Quantum Eng.*, vol. 1, pp. 1–12, 2020.
[6] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "Implementing Grover oracles for quantum key search on AES and LowMC," in *Advances in Cryptology—EUROCRYPT2020*, vol. 12106. 2020, p. 280.
[7] P. Saravanan, J. Jenitha, S. R. Aasish, and S. Sanjana, "Quantum circuit design of RECTANGLE lightweight cipher," in *Proc. 25th Int. Symp. VLSI Design Test (VDAT)*, Sep. 2021, pp. 1–4.
[8] V. A. Dasu, A. Baksi, S. Sarkar, and A. Chattopadhyay, "LIGHTER-R: Optimized reversible circuit implementation for SBoxes," in *Proc. 32nd IEEE Int. Syst. Chip Conf. (SOCC)*, Sep. 2019, pp. 260–265.
[9] K. Jang, G. Song, H. Kim, H. Kwon, H. Kim, and H. Seo, "Efficient implementation of PRESENT and GIFT on quantum computers," *Appl. Sci.*, vol. 11, no. 11, p. 4776, 2021.
[10] R. Anand, A. Maitra, and S. Mukhopadhyay, "Grover on *SIMON*," *Quantum Inf. Process.*, vol. 19, no. 9, pp. 1–17, 2020.
[11] K. Jang, S. Choi, H. Kwon, H. Kim, J. Park, and H. Seo, "Grover on Korean block ciphers," *Appl. Sci.*, vol. 10, no. 18, p. 6407, 2020.
[12] L. Schlieper, "In-place implementation of quantum-gimli," 2020, *arXiv:2007.06319*.
[13] A. K. Chauhan and S. K. Sanadhya, "Quantum resource estimates of Grover's key search on ARIA," in *Proc. Int. Conf. Secur., Privacy, Appl. Cryptogr. Eng.* Cham, Switzerland: Springer, Dec. 2020, pp. 238–258.

[14] H. Cheng, H. M. Heys, and C. Wang, "PUFFIN: A novel compact block cipher targeted to embedded digital systems," in *Proc. 11th EUROMICRO Conf. Digit. Syst. Des. Archit., Methods Tools*, 2008, pp. 383–390.
[15] L. Knudsen, G. Leander, A. Poschmann, and J. B. M. Robshaw, "PRINTcipher: A block cipher for IC-printing," in *Proc. 12th Int. Workshop, Cryptograph. Hardw. Embedded Syst. (CHES)*, Santa Barbara, CA, USA, Aug. 2010, pp. 16–32.
[16] O. Pal, M. Jain, B. K. Murthy, and V. Thakur, "Quantum and post-quantum cryptography," *Cyber Security and Digital Forensics*. Hoboken, NJ, USA: Wiley, 2022, pp. 45–58.
[17] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, and C. Monroe, "Complete 3-qubit Grover search on a programmable quantum computer," *Nature Commun.*, vol. 8, no. 1, p. 1918, 2017.
[18] W. Lee, K. Jang, G. Song, H. Kim, S. O. Hwang, and H. Seo, "Efficient implementation of lightweight hash functions on GPU and quantum computers for IoT applications," *IEEE Access*, vol. 10, pp. 59661–59674, 2022, doi: 10.1109/ACCESS.2022.3179970.

SARAVANAN PARAMASIVAM (Senior Member, IEEE) received the B.E. degree in electrical and electronics engineering from the Thiagarajar College of Engineering, Madurai, India, in 2007, the M.E. degree in VLSI design from the PSG College of Technology, Coimbatore, India, in 2009, and the Ph.D. degree in hardware security from Anna University, Chennai, India, in 2015. Since 2009, he has been with the Department of Electronics and Communication Engineering, PSG College of Technology, where he is currently an Associate Professor. He has published more than 50 papers in various international and national journals and conferences. His current research interests include hardware security, quantum computing, and the multi-scale modeling of nanoelectronic devices. His history also includes around five years of industrial experience. He is a fellow of IETE and a member of ISSS, CRSI, and VLSI Society of India.

J. JENITHA received the B.E. degree in electronics and communication engineering from the PSG College of Technology, Coimbatore, India, in 2021. Her research interests include quantum computing and cryptographic algorithms. She is a member of IETE.

S. SANJANA is currently pursuing the B.E. degree in electronics and communication engineering with the PSG College of Technology, Coimbatore, India. She is also doing her internship with ARM Embedded Technologies Private Ltd., Bengaluru, India. Her research interests include computer architecture, VLSI design, and quantum logic design.

MAJID HAGHPARAST (Senior Member, IEEE) is currently a Researcher with the University of Jyväskylä, Finland. He is also an Associate Editor of the *Cluster Computing* (Springer) and *Journal of Computational Electronics* (Springer). He is also an Editorial Board Member of the *Optical and Quantum Electronics* (Springer). He has been a supervisor/advisor of more than ten Ph.D. and 150 M.Sc. students. He is an invited referee for more than 30 prestigious journals, including IEEE Internet of Things Journal, IEEE Transactions on Computer, IEEE Transactions on Circuits and Systems—I: Regular Papers, IEEE Transactions on Industrial Electronics, and IEEE Transactions on Quantum Engineering. His research interest includes quantum computing, where he has been involved in different projects.