Time-Space trade-offs analysis for ASCON S-box

Jinseob Oh and Dooho Choi*

Korea University Sejong, Sejong, Republic of Korea
{gnqorwptneh,doohochoi}@korea.ac.kr

Abstract

In quantum computing environments, resource allocation is a pivotal determinant of security strength. This research explores the intrinsic tradeoffs within quantum circuits, with a particular focus on S-box optimization in ASCON. We introduce a methodology to parallelize topological gate and applying various Toffoli decompositions and Quantum AND gate, we illustrate the balance between spatial and temporal resources.

Keywords: Quantum Security, Quantum Circuit, Lightweight Cryptography

1 Introduction

The rapid advent of quantum computers poses a serious threat to current cryptographic systems. Cryptography that rely on the factoring problems can be solved in polynomial time using Shor's algorithm [1]. In addition, time-complexity of arithmetic-based encryption schemes also halved in the quantum system, from $k - bits$ to $k/2 - bits$ due to Grover algorithm [2]. Quantum computer systems have different characteristics from classical computers. Therefore, algorithms must be reconstructed on the quantum system that usually called circuit. And in order to measure the security level of a cryptographic in quantum environments, it is necessary to perform a resource analysis on circuit. This allows us to objectively determine the security level of cryptographic on quantum computing and to show how much security strength it provides compared to the resources required for a classical implementation. In this study, we implement the ASCON's S-box with various quantum circuit based on the number of qubits, and analyze how the quantum resource changes as the circuit is reorganized to reduce depth of T.

2 Quantum Circuit of ASCON's S-box

ASCON adopts the permutation operation to facilitate diffusion and enhancing cryptographic security. Dobrau et al. [3] shows the sturcure of ASCON's substitution layer, one of ASCON's permutation operations. Therefore, it can be replaced by using quantum gates such as Pauli-X(NOT), Toffoli(AND), CNOT(XOR). We use ancilla qubit 2-4 for parallelizing the Toffoli gate within quantum circuits by designing the Toffoli operations to utilize distinct registers. Additionally, We reduced the number of qubits by placing two topological operations that share a single register first. Figure 1 shows an example that use 3 ancilla qubits and has toffoli depth of 3.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, JAPAN, Article No.P-27

*Corresponding author: Korea University Sejong, Sejong, 05006, Republic of Korea, Email: doohochoi@korea.ac.kr

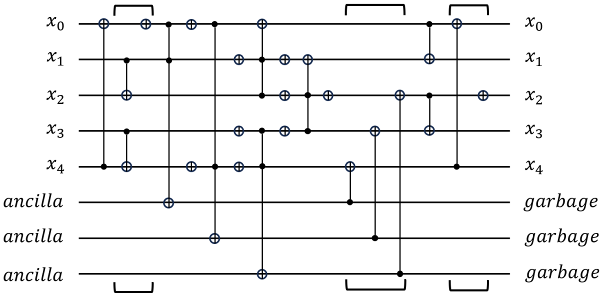

Figure 1: Quantum circuit of ASCON S-box using 3 ancilla qubit with toffoli

3 Resources of quantum circuits for the ASCON S-box with decomposed Toffoli

We applying Toffoli decompositions and Quantum AND, specifically those produced by Amy, Matthew, et al. [4]. These three type of decompositions have a T-depth ranging from 2 to 4, which we then utilized in our quantum circuits. By modifying the Toffoli decomposition to reduce the T-depth, we observed changes in quantum resources. Consequently, through our research findings Table 1, we can analyze the trade-offs between spatial and temporal resources in quantum systems as spatial resources vary.

Width	6	7	8	9	10	12
T-depth	186	15	10	6	4	2
Depth	577	54	67	27	26	21
#Gate	1013	99	114	103	89	99
T-DW cost	1116	105	80	54	40	24
DW cost	3046	378	536	243	260	252
#Garbage qubits	0	2	2	4	5	5
Decomposition method	T-T3	T-T3	T-T2	T-T3	QA-T2	QA-T1

- T-Tx: Decomposition using Toffoli gate with T-depth x
- QA-Tx: Decomposition using quantum AND gate with T-depth x

Table 1: Resource Analysis in ASCON‘s S-box circuit with various Toffoli Decompositions

Acknowledgement: This work was partly supported by Institute of Information & communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(Ministry of Science and ICT(MSIT)) (⟨Q—Crypton⟩, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity), by Quantum Computing based on Quantum Advantage challenge research through the National Research Foundation of Korea(NRF) funded by the Korean government(MSIT) (RS-2023-00256221), and by the MSIT, Korea, under the ITRC(Information Technology Research Center) support program(IITP-2023-RS-2022-0164800) supervised by the IITP.

References

[1] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. 1994. Available at https://ieeexplore.ieee.org/abstract/document/365700.

[2] Lov K Grover. A fast quantum mechanical algorithm for database search. 1996. Available at https://dl.acm.org/doi/pdf/10.1145/237814.237866.

[3] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1. 2. 2016. Available at https://competitions.cr.yp.to/round3/asconv12.pdf.

[4] Matthew Amy, Dmitri Maslov, Michele Mosca, and Martin Roetteler. A Meet-in-the-Middle Algorithm for Fast Synthesis of Depth-Optimal Quantum Circuits. 2013. Available at https://ieeexplore.ieee.org/abstract/document/6516700.