Depth Optimized Quantum Circuits for HIGHT and LEA

Kyungbae Jang, Yujin Oh, Minwoo Lee, Dukyoung Kim,
Hwajeong Seo

https://youtu.be/jjuplL3kvVY

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Contents

Contributions

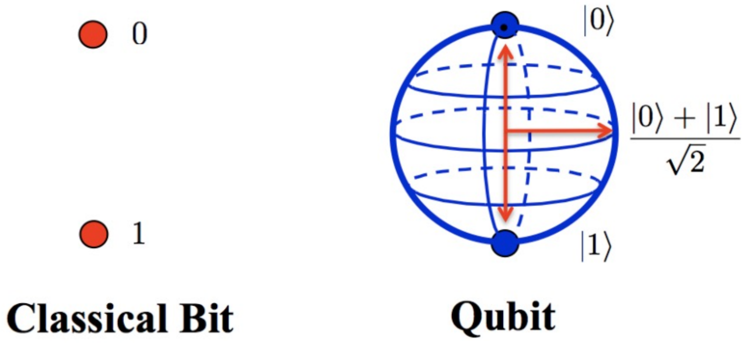
- **Depth-optimized quantum circuits for LEA and HIGHT**
  - **We achieve depth reductions of 48% and 74% for HIGHT and LEA**, respectively.

- **Multiple methods for effectively reducing circuit depth are gathered in this work.**
  - The implementation methods **can be adopted for generic quantum circuit implementations.**

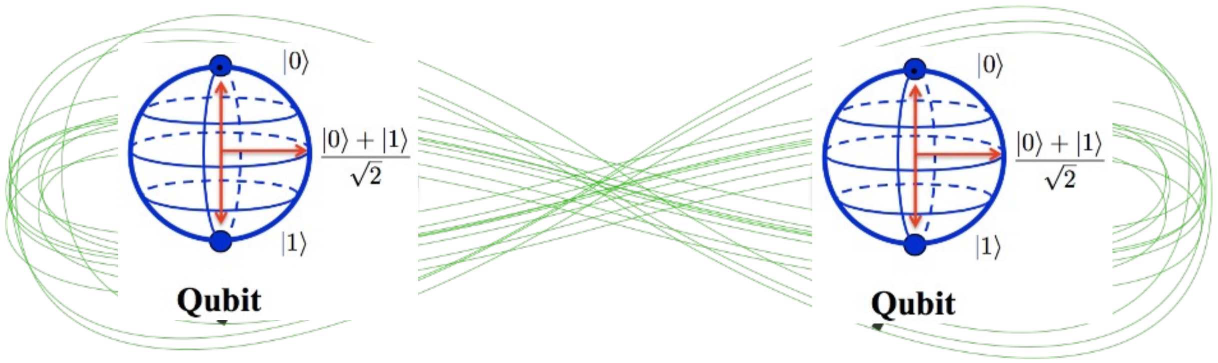
- **The required quantum complexities for HIGHT and LEA are redefined in this work.**
  - **Post-quantum security level for HIGHT and LEA are re-evaluated.**

Quantum Computing

- **Qubit (Quantum bit)**
  - **Superposition**

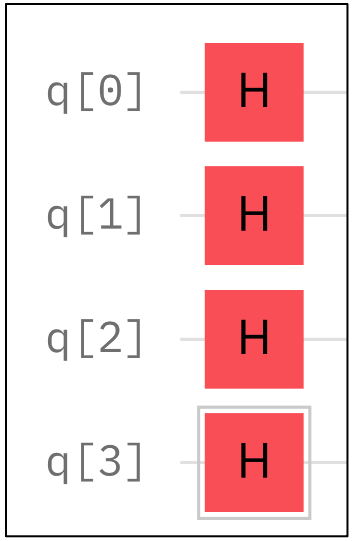


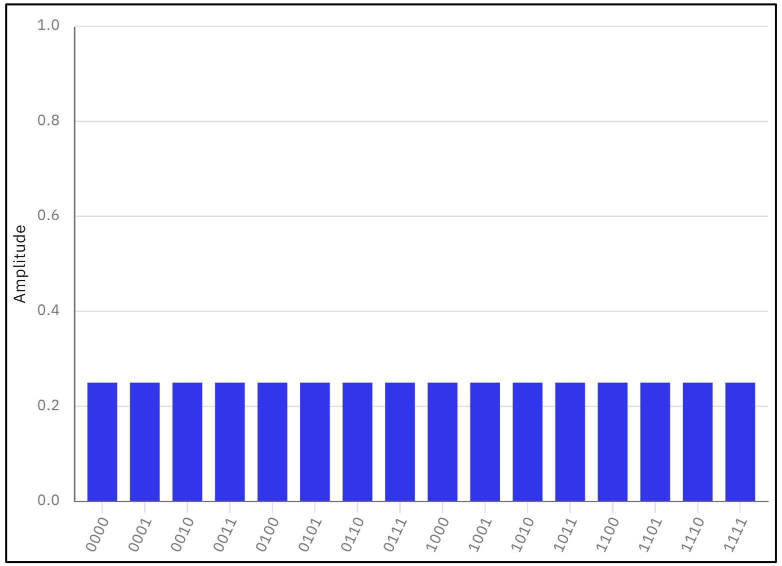
  - **Entanglement**



Quantum Computing

- n-qubit with superposition state?





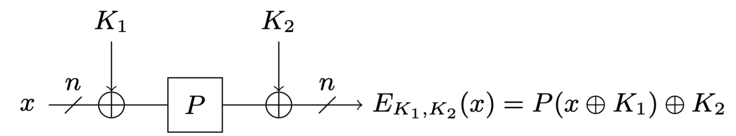


Fig. 2: The Even-Mansour construction. P is a public permutation.

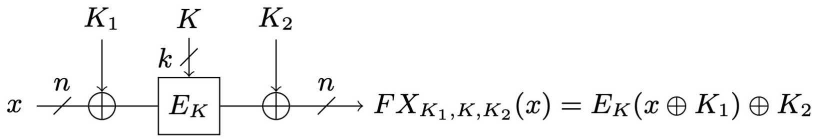


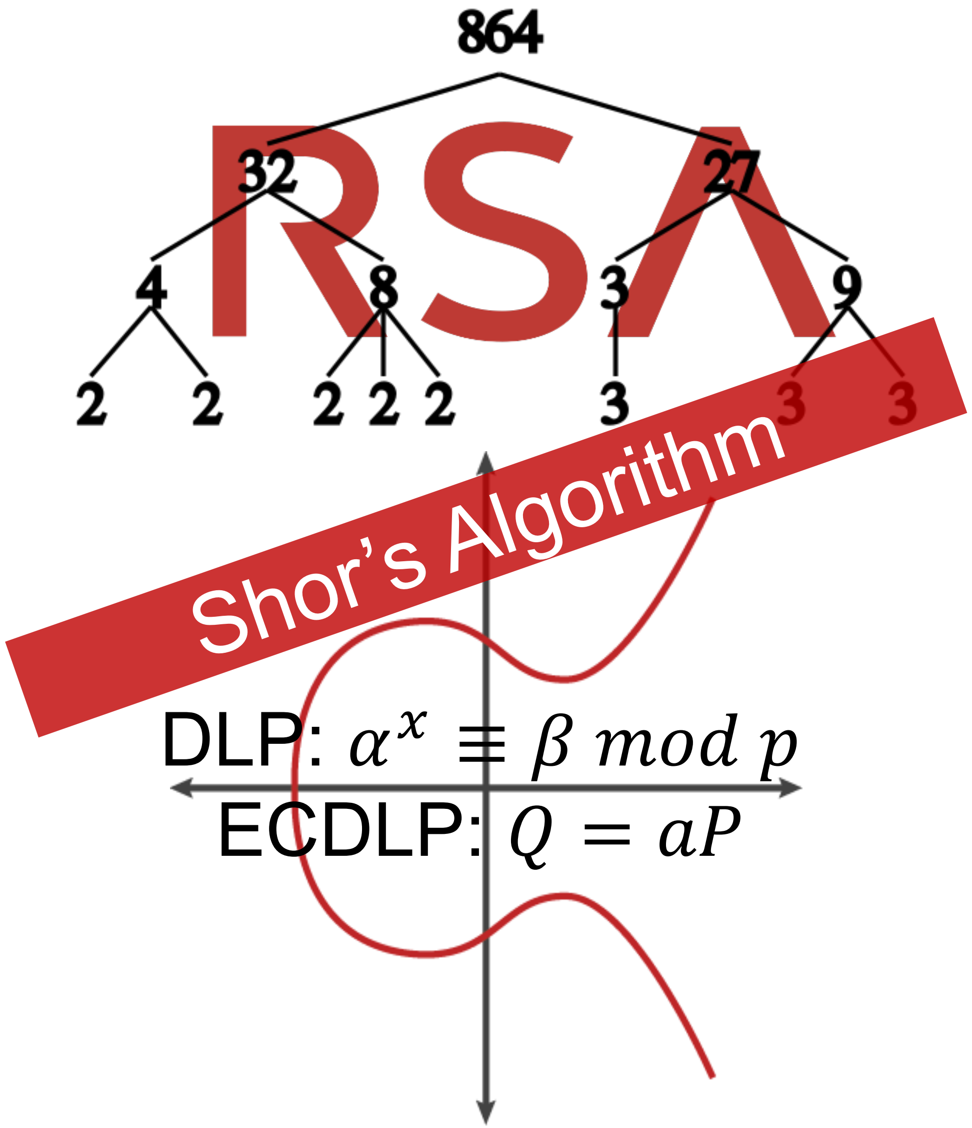
Fig. 3: The FX construction. E_K is a block cipher.

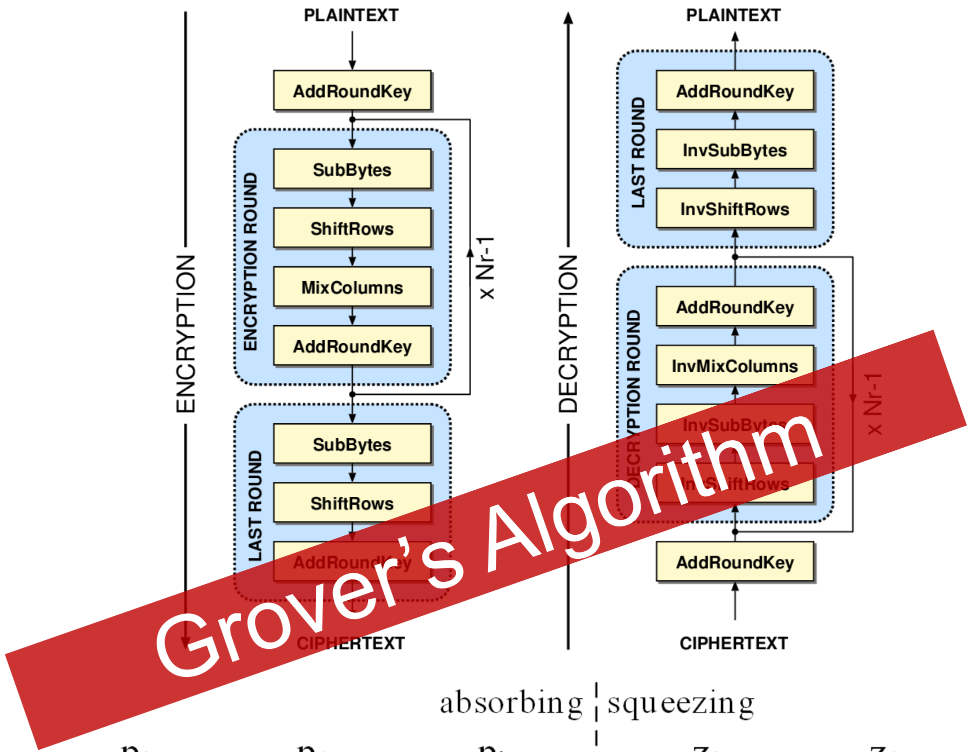
We can prepare 2^n states (as probability) at once!

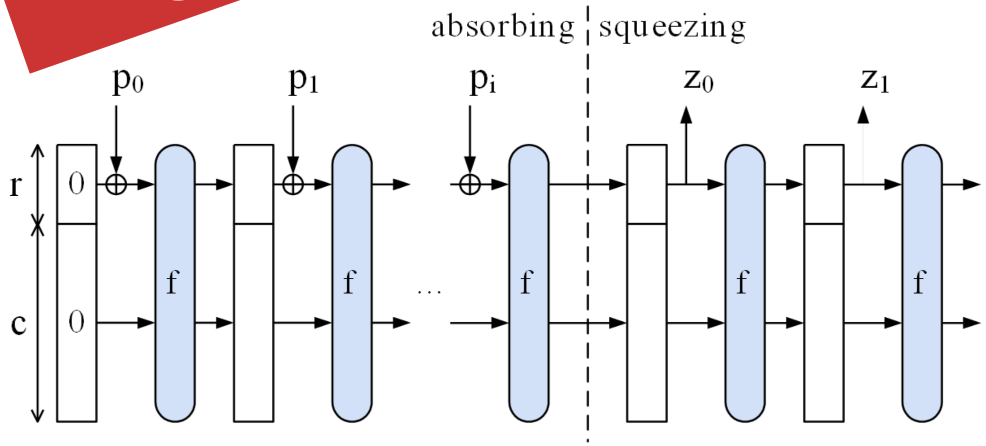
With proper quantum algorithm? (Shor, Grover, Simon etc…)

→ Meaningful result can be achieved

Cryptosystems in Quantum World

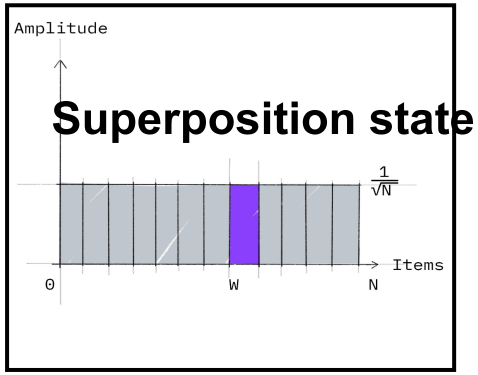


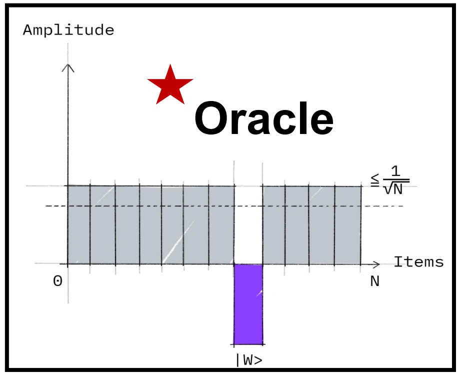


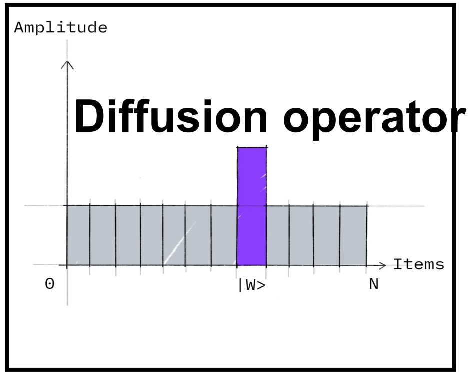


Grover's Algorithm

- Search complexity for N data elements
  - Classical: $O(N)$ → **Quantum (Grover): $O(\sqrt{N})$**



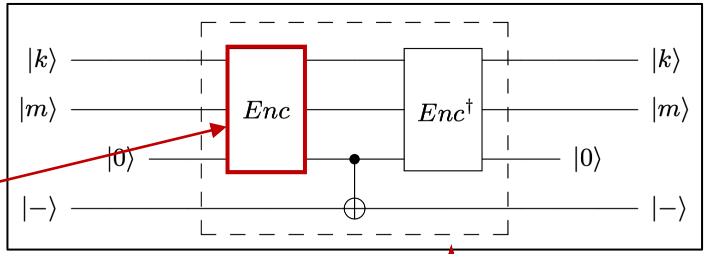




- Grover's key search for Symmetric key ciphers (k-bit key)
  - Prepare k-qubit in a superposition state (by using *Hadamard* gates)

$$|\psi\rangle = H^{\otimes k}|0\rangle^{\otimes k} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{2^{k/2}}\sum_{x=0}^{2^k-1}|x\rangle$$

  - Implement a **quantum circuit for the target cipher**, then encrypt $\sqrt{2^k}$ times
    → **Optimization target**



Oracle

Maximum Depth (MAXDEPTH)

- In Grover's search (single instance), numerous quantum queries are performed in sequential
  - **Total depth = Time-complexity.**

- NIST suggests the parameter, namely **MAXDEPTH (Maximum Depth)**

Level 1: $\mathbf{2^{40}}$ **Depth**

Level 3: $\mathbf{2^{64}}$ **Depth**

Level 5: $\mathbf{2^{96}}$ **Depth**

MAXDEPTH	Cycle time (faster →)		
	$1\mu s$	**200ns**	1ns
$\mathbf{2^{40}}$	12.7 days	**2.55 days**	18.3 mins
$\mathbf{2^{48}}$	8.92 years	**1.78 years**	3.26 days
2^{56}	2,280 years	457 years	2.28 years
2^{64}	585,000 years	117,000 years	585 years

: near-term and plausible

- If we do not satisfy the MAXDEPTH, Parallelization of Grover's search is required
  → Unfortunately, **Parallelization of Grover's search is poor**

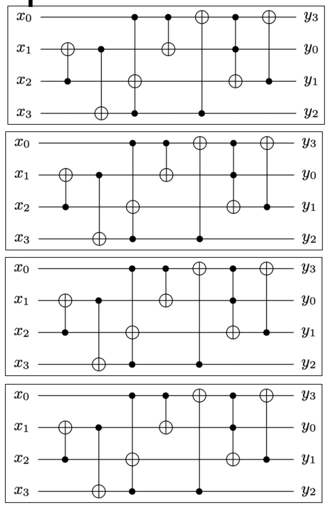
Grover parallelization

- **Poor performance** of Grover parallelization
  - If we operate Grover Instances of S in parallel, depth is only reduced by $\sqrt{S}$.
    → The **DW-cost (Depth × Width)** is transformed to the **D^2W-cost (Depth^2 × Width)**

Example) if we want to **reduce the depth by half (i.e., 1/2)**, width is **increased by a factor of 4 (S=4)**

FullDepth → 1/2 $(S = 2)$

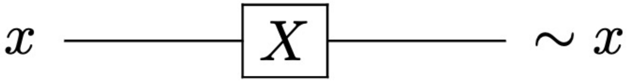
Width → X 4 (Qubits)



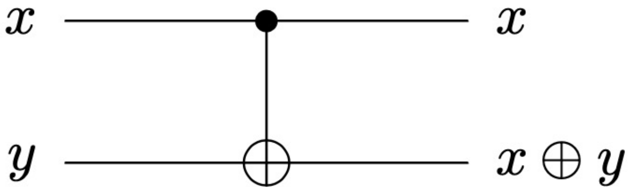
This is why we should optimize the depth for Grover's key search !!

Basic Quantum Gates

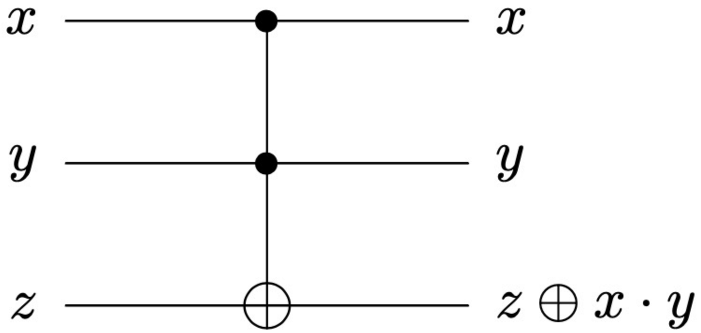
- **The NOT (X) gate** replaces **classical NOT operation**
- **The CNOT gate** replaces **classical XOR operation**
- **The Toffoli gate** replaces **classical AND operation**



(a) X (NOT) gate



(b) CNOT gate

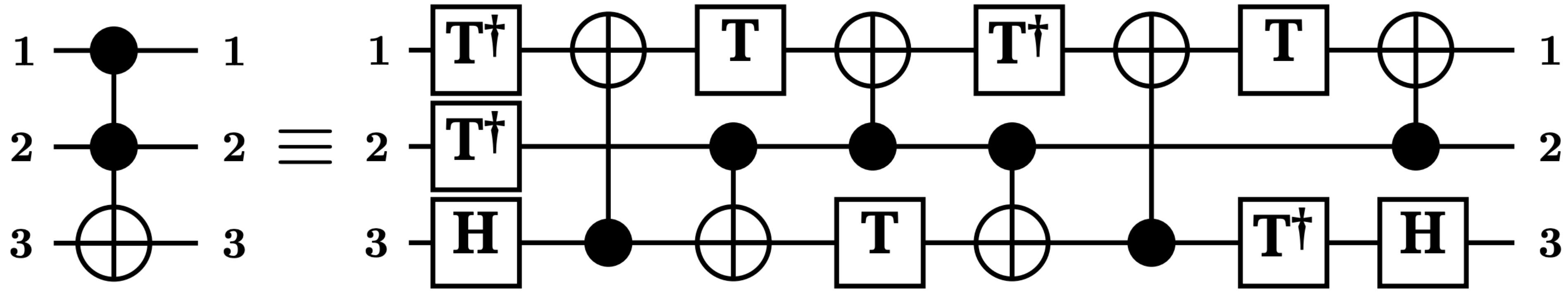


(c) Toffoli (CCNOT) gate

Toffoli gate

- **Actually, the Toffoli gates are more complex than other quantum gates**

*



(a) Toffoli gate (T-depth 4, total depth 8).

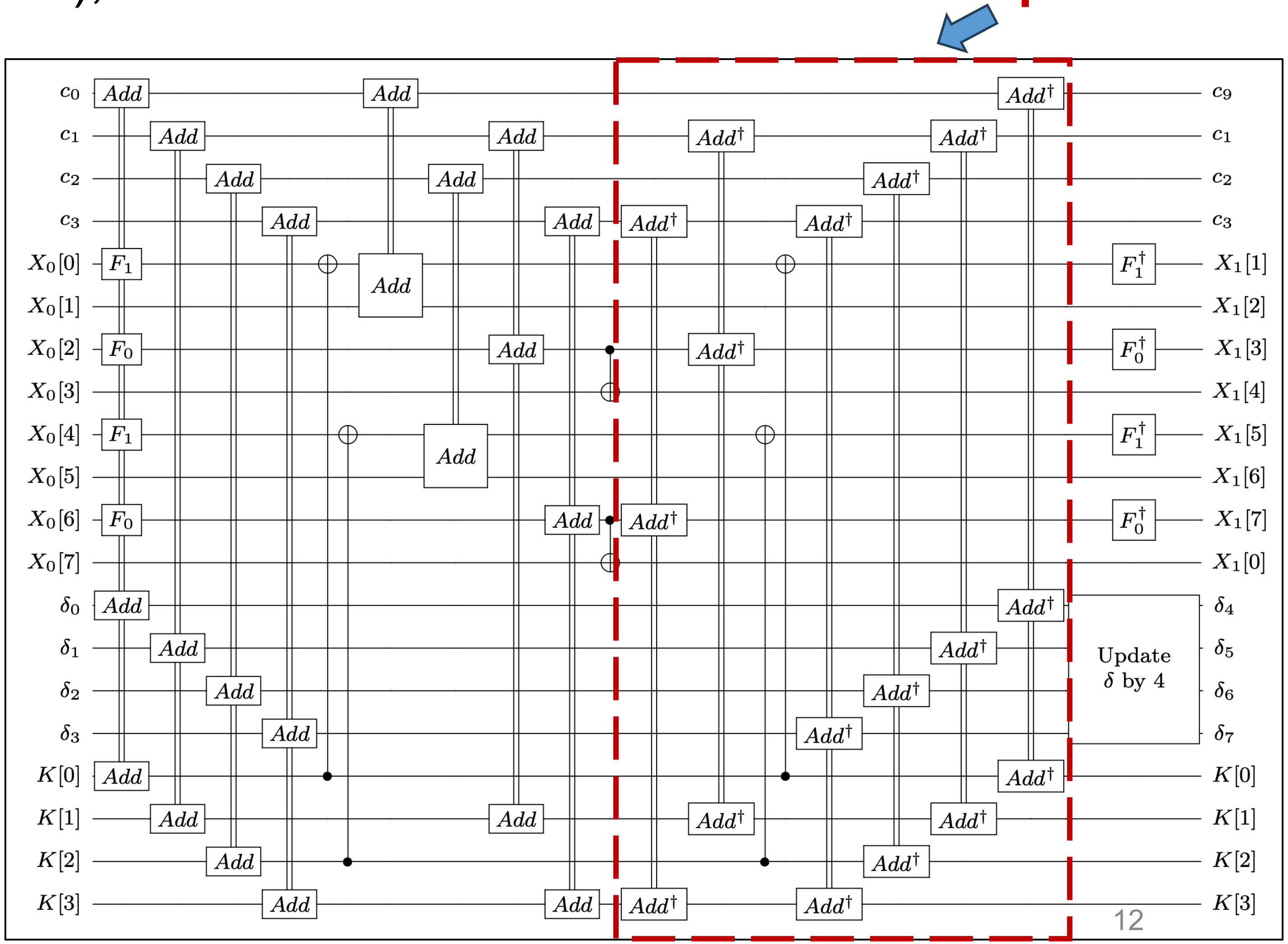
* M. Amy, D. Maslov, M. Mosca, M. Roetteler, and M. Roetteler, "A meet- in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits,"

HIGHT quantum circuit

- We present a ***Shallow architecture*** for HIGHT
  - In the previous implementation (QIP'22), there is an overhead for the **reverse operation**

- In quantum implementations, the reverse operation is often utilized to initialize ancilla qubits and reuse them.

- In our Shallow architecture, **there is no depth overhead for the reverse operation.**



* Jang et al "Parallel Quantum Addition for Korean Block Ciphers", Quantum Information Processing, 2022.

HIGHT quantum circuit

- In the previous work, **the subsequent round function is delayed** until the completion of the reverse operation of the current round function.
  → Since the current and subsequent round functions **share the ancilla qubits each other.**

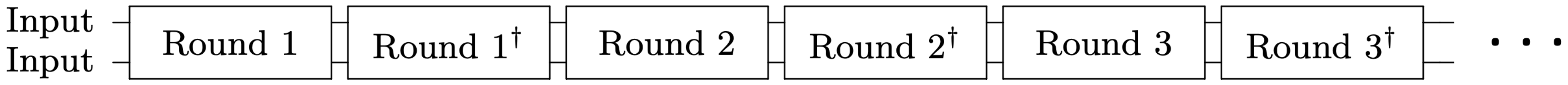


Fig. 2: The regular architecture adopted in [13]

- In the shallow architecture, the reverse operation of **the current round function is performed simultaneously with the subsequent round function** (i.e., in parallel).
  → we run **two sets of ancilla qubits** by allocating additional ancilla qubits for the subsequent round function.

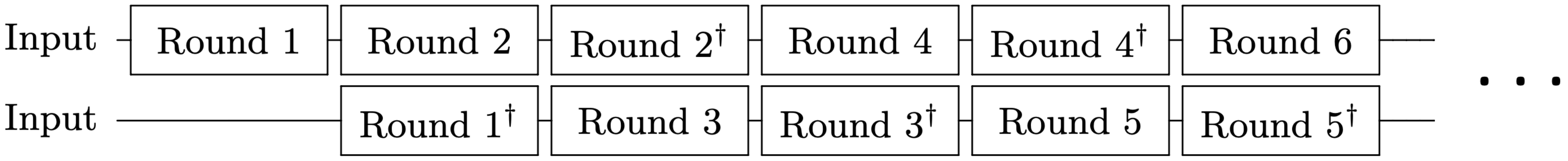


Fig. 3: The shallow architecture adopted in this work.

HIGHT quantum circuit

In HIGHT, linear layer operations which called $F_0(X)$ and $F_1(X)$ are given by:

$$F_0(x) = (x \lll 1) \oplus (x \lll 2) \oplus (x \lll 7)$$
$$F_1(x) = (x \lll 3) \oplus (x \lll 4) \oplus (x \lll 6)$$

In the previous work, **in-place implementation** was presented
→ **low qubit count but high circuit depth.**

We present an **out-of-place implementation**
→ **reduce the depth but increases the qubit count (but we reuse them)**

Operation	Source	#CNOT	#Qubit (reuse)	Depth
F_0	[14] and [13]	21	8	15
F_0	Ours	24	16 (8)	**3**
F_1	[14] and [13]	24	8	17
F_1	[14] and [13]	24	16 (8)	**3**

HIGHT quantum circuit

- We **effectively reduce the Toffoli/full depth** by allocating additional ancilla qubits.
  - **48% depth reduction**
  - All of the trade of metrics; $TD{-}M, FD{-}M, TD^2{-}M, FD^2{-}M$ are optimized.

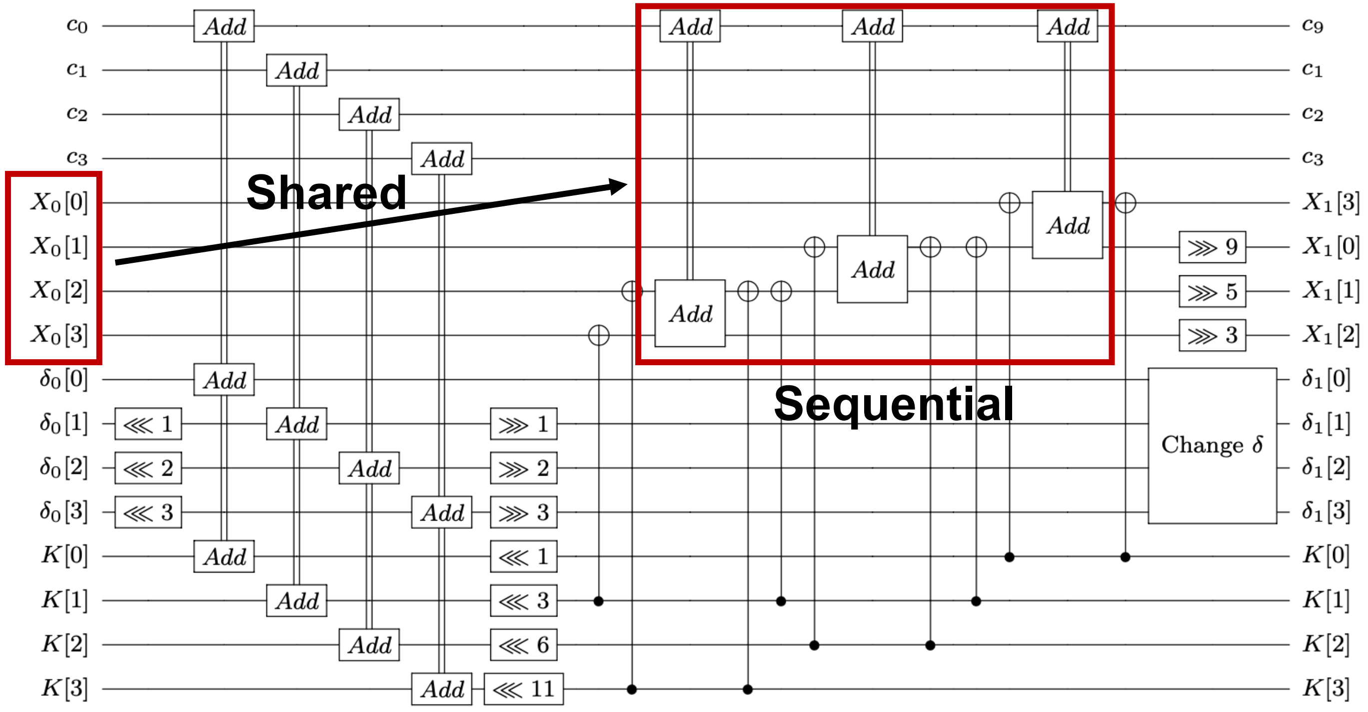
Source	#CNOT	#1qCliff	#T	Toffoli depth (TD)	#Qubit (M)	Full depth (FD)	TD-M	FD-M	TD^2-M	FD^2-M
[14]	64,799	13,444	50,176	·	201	68,415	·	$1.639 \cdot 2^{23}$	·	$1.711 \cdot 2^{39}$
[13]	57,558	16,144	40,540	1,664	228	14,058	$1.447 \cdot 2^{18}$	$1.528 \cdot 2^{21}$	$1.176 \cdot 2^{29}$	$1.311 \cdot 2^{35}$
Ours	57,440	16,598	40,422	**832**	296	**7,308**	$\mathbf{1.879 \cdot 2^{17}}$	$\mathbf{1.031 \cdot 2^{21}}$	$\mathbf{1.527 \cdot 2^{27}}$	$\mathbf{1.84 \cdot 2^{33}}$

TABLE II: Quantum resources required for implementations of HIGHT.

LEA quantum circuit

Parallel Additions for Round Function

- In the previous implementation, **sequential additions** are performed.
  - Since the **inputs ($X_0[0]$~$[3]$) are shared** in the three additions.



#

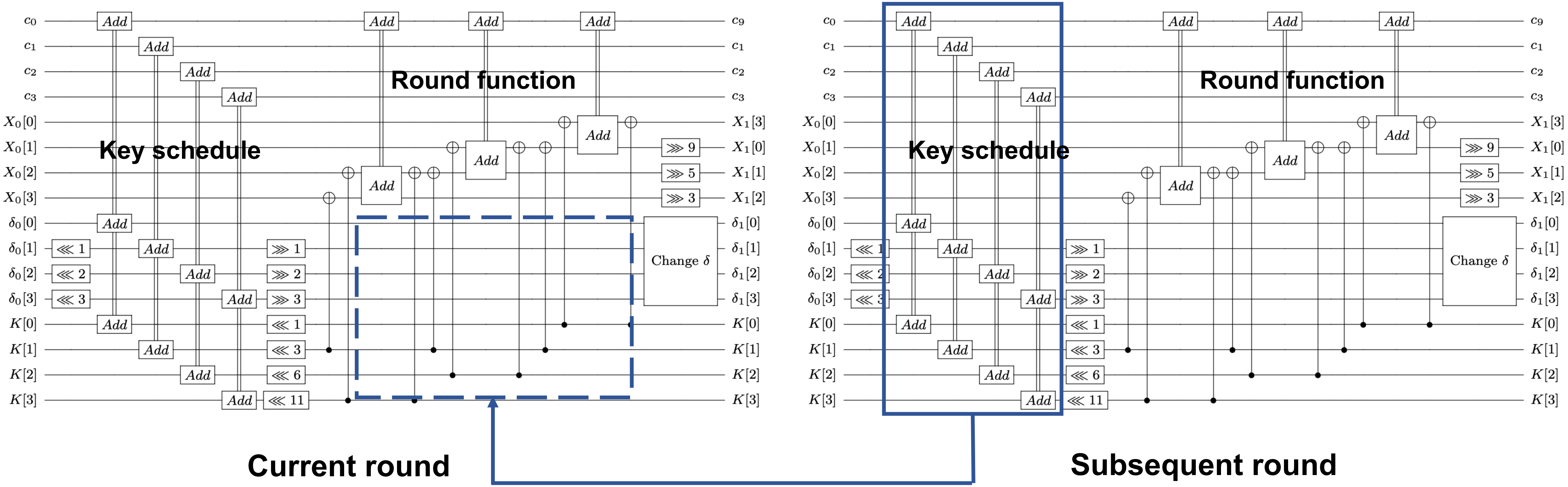
1. $X_{i+1}[0] \leftarrow ((X_i[0] \oplus K_i[0]) \boxplus (X_i[1] \oplus K_i[1])) \lll 9$
2. $X_{i+1}[1] \leftarrow ((X_i[1] \oplus K_i[2]) \boxplus (X_i[2] \oplus K_i[3])) \ggg 5$
3. $X_{i+1}[2] \leftarrow ((X_i[2] \oplus K_i[4]) \boxplus (X_i[3] \oplus K_i[5])) \ggg 3$
4. $X_{i+1}[3] \leftarrow X_i[0]$

- We perform the **three additions in parallel.**
  - To enable this, **we copy inputs ($X_0[0]$~$[3]$)** before the additions.

* Jang et al "Parallel Quantum Addition for Korean Block Ciphers", Quantum Information Processing, 2022.

LEA quantum circuit

- The subsequent key schedule and the current round function can be executed in parallel.
  - As we did before, to enable this, we allocate additional ancilla qubits.



* Jang et al "Parallel Quantum Addition for Korean Block Ciphers", Quantum Information Processing, 2022.

LEA quantum circuit

- We significantly reduce the Toffoli/full depth by allocating additional ancilla qubits.
  - **74% depth reduction**
  - Due to the **significant increases in qubit count**, the trade of metrics, $TD{-}M, FD{-}M$, **increases**
  - However, **thanks to the depth optimization**, the trade-off metrics for parallelization, $TD^2{-}M, FD^2{-}M$, **are optimized.**

Cipher	Source	#CNOT	#1qCliff	#T	Toffoli depth (TD)	#Qubit (M)	Full depth (FD)	TD-M	FD-M	TD^2-M	FD^2-M
LEA-128	[14]	94,104	30,592	71,736	·	289	82,825	·	$1.427 \cdot 2^{24}$	·	$1.803 \cdot 2^{40}$
	[13]	94,104	31,588	71,736	5856	388	47,401	$1.083 \cdot 2^{21}$	$1.096 \cdot 2^{24}$	$1.549 \cdot 2^{33}$	$1.586 \cdot 2^{39}$
	Ours	94,104	31,588	71,736	**1,464**	2,695	**12,326**	$1.881 \cdot 2^{21}$	$1.98 \cdot 2^{24}$	$\mathbf{1.345 \cdot 2^{32}}$	$\mathbf{1.49 \cdot 2^{38}}$
LEA-192	[14]	138,852	45,758	107,604	·	353	124,181	·	$1.306 \cdot 2^{25}$	·	$1.238 \cdot 2^{42}$
	[13]	138,852	47,748	107,604	6832	518	55,301	$1.688 \cdot 2^{21}$	$1.707 \cdot 2^{24}$	$1.407 \cdot 2^{34}$	$1.441 \cdot 2^{40}$
	Ours	138,852	47,748	107,604	**1,708**	3,209	**14,298**	$1.307 \cdot 2^{22}$	$1.367 \cdot 2^{25}$	$\mathbf{1.09 \cdot 2^{33}}$	$\mathbf{1.193 \cdot 2^{39}}$
LEA-256	[14]	156,672	36,753	129,024	·	417	175,234	·	$1.089 \cdot 2^{26}$	·	$1.456 \cdot 2^{43}$
	[13]	158,688	54,630	122,976	7808	582	63,108	$1.083 \cdot 2^{22}$	$1.095 \cdot 2^{25}$	$1.033 \cdot 2^{35}$	$1.054 \cdot 2^{41}$
	Ours	158,688	54,630	122,976	**1,952**	3,657	**16,257**	$1.702 \cdot 2^{22}$	$1.772 \cdot 2^{25}$	$\mathbf{1.622 \cdot 2^{33}}$	$\mathbf{1.758 \cdot 2^{39}}$

TABLE III: Quantum resources required for implementations of LEA.

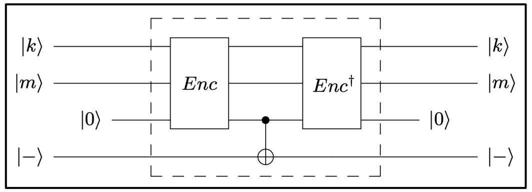
Evaluation of Post-Quantum Security

- Based on the optimized quantum circuits for Grover's key search, we estimate required resources for quantum key search.

Grover's key search (k-bit key) are estimated as follows: Quantum circuit $\times$ 2 $\times$ $\lfloor \frac{\pi}{4}\sqrt{2^k} \rfloor$.

Cipher	Total gates	Total depth	Complexity	NIST level
HIGHT	$1.372 \cdot 2^{81}$	$1.402 \cdot 2^{77}$	$\mathbf{1.924 \cdot 2^{158}}$	Level 1 (2^{157})
LEA-128	$1.183 \cdot 2^{82}$	$1.182 \cdot 2^{78}$	$\mathbf{1.398 \cdot 2^{160}}$	Level 1 (2^{157})
LEA-192	$1.763 \cdot 2^{114}$	$1.371 \cdot 2^{110}$	$\mathbf{1.209 \cdot 2^{225}}$	Level 3 (2^{221})
LEA-256	$1.008 \cdot 2^{147}$	$1.558 \cdot 2^{142}$	$\mathbf{1.57 \cdot 2^{289}}$	Level 5 (2^{285})

TABLE IV: Quantum resources required for Grover's key search for HIGHT and LEA.



$\times \lfloor \frac{\pi}{4}\sqrt{2^k} \rfloor$

Recall this

- We evaluate the post- quantum security level suggested by NIST.
  - **Level 1, 3, and 5** correspond to the attack complexity for **AES-128, -192, and -256,** respectively.
  - **HIGHT and LEA achieve the appropriate post-quantum security** level according to the key size.

Conclusion

- **Multiple techniques** are gathered in this work **to effectively reduce circuit depth.** (such as shallow architecture and copying for parallel operation)

- **Depth-optimized quantum circuits** offer optimal performance for Grover's key search.
  - We provide the **lowest quantum attack complexity** and the **best trade-off performance** for major metrics **under the depth constraint.**

- **We re-evaluate post-quantum security for HIGHT and LEA** (with NIST standard).
  - The quantum circuit of the target cipher is a **fundamental block in quantum cryptanalysis.**
  - Thus, the quantum circuits in this work can be utilized for other quantum algorithms (not only for Grover's exhaustive search).

Thank you!