Quantum Circuits of AES with a Low-depth Linear Layer and a New Structure

Haotian Shi[1, 2] Xiutao Feng[1]

[1] *Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China*

[2] *University of Chinese Academy of Sciences, Beijing, China*

2024.12.11

University of Chinese Academy of Sciences

Table of Contents

1. Background
2. Low-depth CNOT circuits
3. Compressed pipeline structure
4. Quantum circuits of AES

Outline

1. Background
2. Low-depth CNOT circuits
3. Compressed pipeline structure
4. Quantum circuits of AES

Background

- Rapid develepment of quantum computing.
  - Shor's algorithm.
- Threats in secret-key cryptography.
  - Grover's algorithm, Simon's algorithm. Both of them need the quantum oracle of attacked primitives.
  - NIST: categorize the post-quantum public-key schemes into different security levels by the complexity of the quantum circuit of AES.
- Synthesis and optimization of quantum circuits.
  - Qubits, decoherence.
  - width(W), depth(D), T-depth(TD) or Toffoli depth($TofD$).

Quantum computation

- A single qubit state: a unit vector $|u\rangle = \alpha|0\rangle + \beta|1\rangle$ in a Hilbert Space $\mathcal{H} = \mathbb{C}^2$, where $|\alpha|^2 + |\beta|^2 = 1$.
- An n-qubit state $|u\rangle$: a unit vector in $\mathcal{H}^{\otimes n}$, with computational basis states described as n-bit 0/1 string: $|x_1 x_2 \ldots x_n\rangle$.
- Quantum gates which compute classical vectorial boolean functions.

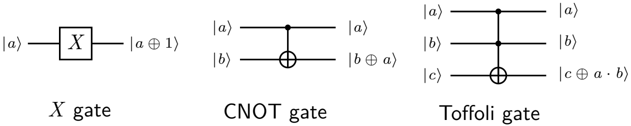

Figure 1: Circuits of X gate, CNOT gate and Toffoli gate. The changed qubit is called the target qubit.

The Toffoli gate and qAND gate

- The Toffoli gate:
  - T-depth 3, full depth 9.
  - T-depth 4, full depth 8.
  - T-depth 1, 4 ancilla qubits.
- The qAND gate with its adjoint: the target qubit must be $|0\rangle$.

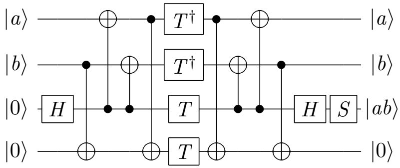

Figure 2: The qAND gate

Conditioned on the measurement result being $|1\rangle$

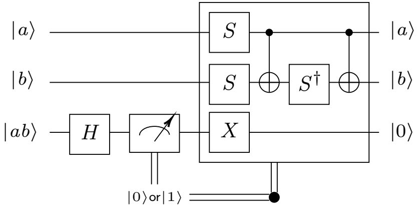

Figure 3: The qAND† gate

Encryption circuit and Encryption oracle

- Encryption circuit:

$$|x\rangle |k\rangle |0\rangle \mapsto |x\rangle |k'\rangle |Enc_k(x)\rangle ,$$

  where $Enc_k(x)$ is the encryption of message x under the seed key k.
- Encryption oracle: the key register does not exist since the seed key is pre-fixed.

$$|x\rangle |0\rangle \mapsto |x\rangle |Enc(x)\rangle ,$$

  where $Enc(x)$ is the encryption of message x.
- Quantum circuit: a general notation.

Outline

1 Background

2 Low-depth CNOT circuits

3 Compressed pipeline structure

4 Quantum circuits of AES

CNOT circuits

- Denote $E(i+j)$ as the type-3 elementary matrix, then the CNOT gate CNOT$(i,j) \Longleftrightarrow E(j+i)$.
- CNOT circuit of a matrix $A \Longleftrightarrow$ the matrix decomposition form below.

Theorem 1

Any A in GL$(2,n)$ *can be expressed as*

$$A = PE(i_1+j_1)E(i_2+j_2)\dots E(i_L+j_L),$$

where P is a permutation matrix.

Optimizing the depth of CNOT circuits

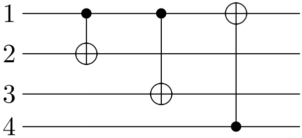

Figure 4: Quantum depth 3

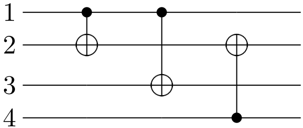

Figure 5: Quantum depth 2

- Computing the depth of existing circuits, especially the circuits provided in [XZL+20].
- Greedy methods based on matrix decomposition.

De Brugière *et al.*'s Greedy method

- A cost-minimization algorithm.
- The algorithm finds elementary row and column operations layer by layer, where every row(column) layer has depth 1.

$$E^d_{i_d} E^d_{i_d-1} \cdots E^d_1 \cdots E^1_{i_1} E^1_{i_1-1} \cdots E^1_1 A F^1_1 F^1_2 \cdots F^1_{j_1} \cdots F^d_1 F^d_2 \cdots F^d_{j_d} = P,$$

- Choices of cost function to guide the optimization of the gate count in [dBBV+21a] and the depth in [DBBV+21b]:

(1) $h_{sum}(A) = \sum_{i,j} a_{ij};$

(2) $H_{sum}(A) = h_{sum}(A) + h_{sum}(A^{-1});$

(3) $h_{prod}(A) = \sum_{i} \log_2(\sum_{j} a_{ij});$

(4) $H_{prod}(A) = h_{prod}(A) + h_{prod}(A^{-1}).$

Our method

- Based on De Brugière *et al.*'s Greedy method.
- Observation: their cost function is not depth oriented. Prioritizing the rows or columns with larger Hamming weights might be a preferable choice to obtain lower circuit depth, which leads to

$$h_{sq}(A) = \sum_i (\sum_j a_{ij})^2.$$

- Our cost functions consider row and column operation seperately.

$$H_{sqr}(A) = h_{sq}(A) + h_{sq}((A^{-1})^T);$$
$$H_{sqc}(A) = h_{sq}(A^T) + h_{sq}(A^{-1}).$$

- Additional judgement of implementation of depth 1.

Remarks

- Time complexity of determining of an operation to be done: $O(n^3)$.
- The algorithm is suitable for small scale matrices, and often falls into a local minima(an infinite loop) when n is larger.
- Repeat thousands of times and record the best implementation.

Applications on AES MixColumns

Table 1: Comparison of CNOT circuits of the AES MixColumns matrix.

Source	# CNOT	W	FD
[BFI21, LWF+22]	206	135	13
[LSL+19]	210	137	11
[JBK+22]	169	96	8
[JNRV20]	277	32	111
[GLRS16, ZWS+20]	277	32	39
[XZL+20]	92	32	30
[ZH22]	92	32	28
[LPZW23]	98	32	16
[DBBV+21b]	128	32	12
This paper	131	32	**10**

Applications on many MDS matrices and matrices used in block ciphers

Table 2: Comparison of the depth/gate count of CNOT circuits for matrices used in block ciphers.

Cipher	Size	Q#	[ZH22]	**This paper**	**[DBBV+21b]**
AES[a] [DR02]	32	30/92	28/92	**10**/131	12/128
ANUBIS [Bar00]	32	26/98	20/98	**10**/119	14/136
CLEFIA M0 [SSA+07]	32	30/98	27/98	**10**/110	13/126
CLEFIA M1 [SSA+07]	32	21/103	16/103	**10**/128	13/127
FOX MU4 [JV05]	32	55/136	48/136	**21**/265	**21**/200
QARMA128 [Ava17]	32	6/48	5/48	**3**/48	**3**/48
TWOFISH [SKW+98]	32	37/111	29/111	**15**/175	18/187
WHIRLWIND M0 [BNN+10]	32	65/183	51/183	**28**/331	**28**/286
WHIRLWIND M1 [BNN+10]	32	69/190	54/190	**22**/290	25/279
JOLTIK [JNP15]	16	20/44	17/44	**7**/52	9/48
MIDORI [BBI+15]	16	**3**/24	**3**/24	**3**/24	**3**/24
SmallScale AES [CMR05]	16	20/43	19/43	**10**/62	11/59
PRIDE L0 [ADK+14]	16	**3**/24	**3**/24	**3**/24	**3**/24
PRIDE L1 [ADK+14]	16	5/24	5/24	**3**/24	**3**/24
PRIDE L2 [ADK+14]	16	5/24	5/24	**3**/24	**3**/24
PRIDE L3 [ADK+14]	16	6/24	6/24	**3**/24	**3**/24
PRINCE M0 [BCG+12]	16	6/24	6/24	**3**/24	**3**/24
PRINCE M1 [BCG+12]	16	6/24	6/24	**3**/24	**3**/24
QARMA64 [Ava17]	16	6/24	5/24	**3**/24	**3**/24
SKINNY [BJK+16]	16	**3**/12	**3**/12	**3**/12	**3**/12

[a] A recent result of 16/98 is given in [LPZW23].

Table 3: Comparison of the depth/gate count of CNOT circuits for many constructed MDS matrices.

Matrices	Size	Move-eq	[ZH22]	**This paper**	**[DBBV+21b]**
4×4 matrices in GF(4, $\mathbb{F}_2$)					
[CTG16]	16	23/41	21/41	**10**/59	12/57
[JPST17]	16	24/41	18/41	**9**/49	**9**/48
[LS16]	16	27/41	26/41	**11**/63	12/65
[SKOP15]	16	25/44	22/44	**11**/59	**11**/59
[LW16]	16	29/44	27/44	**11**/62	12/65
[JPST17](Involutory)	16	15/41	14/41	**9**/54	13/54
[SKOP15](Involutory)	16	19/44	16/44	**7**/52	9/48
[LW16](Involutory)	16	27/44	25/44	**7**/52	9/48
[SS16](Involutory)	16	12/38	11/38	**8**/46	**8**/44
4×4 matrices in GF(8, $\mathbb{F}_2$)					
[CTG16]	32	56/144	47/144	**18**/208	20/188
[JPST17]	32	26/82	22/82	**9**/100	**9**/96
[LS16]	32	67/121	54/121	**21**/235	23/203
[LW16]	32	55/104	42/104	**13**/164	16/167
[SKOP15]	32	23/90	20/90	**10**/112	11/118
[SS16]	32	47/114	40/114	**20**/218	**20**/190
[JPST17](Involutory)	32	18/83	14/83	**9**/102	13/108
[SKOP15](Involutory)	32	18/91	16/91	**8**/101	9/96
[LW16](Involutory)	32	19/87	19/87	**8**/99	**8**/98
[SS16](Involutory)	32	19/93	18/93	**10**/121	12/119
8×8 matrices in GF(4, $\mathbb{F}_2$)					
[SS17]	32	54/183	44/183	**29**/351	33/302
[SKOP15]	32	59/170	49/170	**28**/349	29/286
[SKOP15](Involutory)	32	47/185	37/185	**29**/337	30/300
8×8 matrices in GF(8, $\mathbb{F}_2$)					
[SKOP15](Involutory)	64	50/348	37/348	**22**/484	25/412

Outline

1. Background
2. Low-depth CNOT circuits
3. Compressed pipeline structure
4. Quantum circuits of AES

Structures for iterative building blocks

- The structures based on the out-of-place oracle $\mathcal{O}_{\mathcal{R}_j}$ of round function $\mathcal{R}_j$: $|x\rangle |y\rangle \mapsto |x\rangle |y \oplus \mathcal{R}_j(x)\rangle$
  - The pipeline structure.
  - The zig-zag structure.
  - The out-of-place based round-in-place structure.
- The structure based on the in-place oracle of round function $\mathcal{R}_j$: $|x\rangle |0\rangle \mapsto |\mathcal{R}_j(x)\rangle |0\rangle$
  - The straight-line structure. Use in-place S-box.
- Decomposing the oracle of round function
  - The shallowed pipeline structure. Delay the uncomputation of round function to the next round. Combine computation and uncomputation to save qubits.

Structures based on the out-of-place oracle

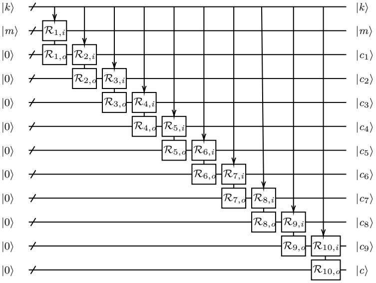

Figure 6: The pipeline structure $\mathcal{S}_p$ computes intermediate states one by one.

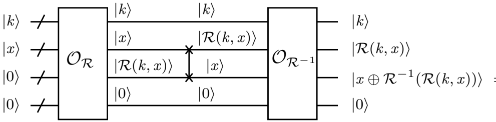

Figure 7: The OP-based round-in-place function in $\mathcal{S}_i$ cleans intermediate states immediately.

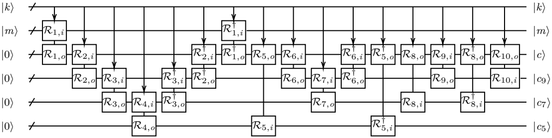

Figure 8: The zig-zag structure $\mathcal{S}_z$ uncomputes intermediate states occasionally..

Our compressed pipeline structure

- Compute of the next intermediate state and clean the previous one in parallel.
- A combination of the pipeline structure and the OP-based round-in-place structure.

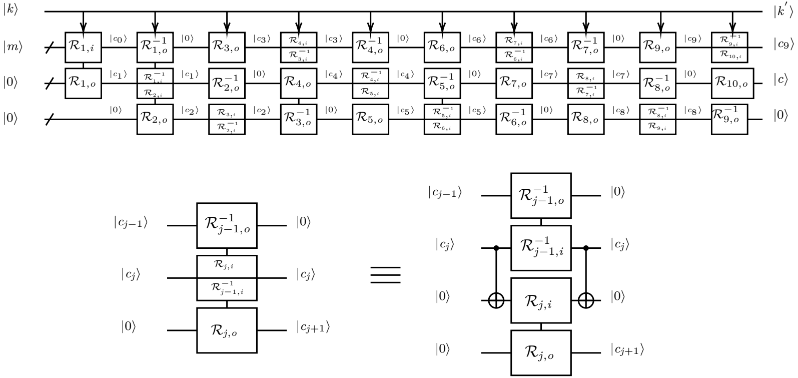

Figure 9: The compressed pipeline structure $\mathcal{S}_{cp}$. For convenience, the copy of the $|c_j\rangle$ state is simplified as "split into two parts".

Comparison

- $\mathcal{O}_{\mathcal{R}_j}$, $\mathcal{O}_{\mathcal{R}_j^{-1}}$: round depth 1, α ancilla qubits.
- State length n, number of rounds r.
- The key schedule needs k qubits (our structure needs k' qubits with a little more information).

Table 4: The comparison of different structures, where t is the minimal number such that $\sum_{i=1}^{t} i > r$.

Structure	Round depth	Width
$\mathcal{S}_p$	r	$k + (r+1)n + \alpha$
$\mathcal{S}_z$	$\approx 2r$	$k + tn + \alpha \approx k + \sqrt{2r}n + \alpha$
$\mathcal{S}_i$	$2r$	$k + 2n + \alpha$
This paper	r	$k' + 4n + 2\alpha$

Circuits for the Grover oracle and the Encryption oracle

- Grover oracle: refer to Table 4 with almost twice the round depth.
- Encryption oracle: since the roundkeys are prefixed, the remaining redundant states contains only $|c_{r-1}\rangle$, which can be cleaned with round depth 1.

Table 5: The depth and width of Encryption oracles with different structures

Encryption oracle	$\mathcal{S}_p$	$\mathcal{S}_z$	$\mathcal{S}_i$	**This paper**
round depth	$2r$	$\approx 4r$	$2r$	$\mathbf{r+1}$
width	$(r+1)n+\alpha$	$\approx \sqrt{2r}n+\alpha$	$(1+2)n+\alpha$	$(1+4)n+2\alpha$

Outline

1. Background
2. Low-depth CNOT circuits
3. Compressed pipeline structure
4. Quantum circuits of AES

Content

- Quantum circuits of AES S-box.
- Detailed quantum circuits of AES under our compressed pipeline structure.
- Improved encryption circuit of AES under the shallowed pipeline structure.

AES S-box and the circuit Sbox

- AES S-box.
  - $C_2 : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus S(x)\rangle$
  - $C_1 : |x\rangle |0\rangle \mapsto |x\rangle |S(x)\rangle$
  - $C_3 : |S(x)\rangle |x\rangle \mapsto |S(x)\rangle |0\rangle$
  - $C_4 : |x\rangle |0\rangle \mapsto |S(x)\rangle |0\rangle$

Table 6: Some Toffoli-based C_1 circuits of AES S-box

Source	#CNOT	#1qClifford	#Toffoli	Toffoli-depth	Ancilla qubits
[LXX+23]	193	4	57	24	5
[LXX+23]	195	4	57	22	6
[LGQW23]	197	4	44	32	4

- The circuit Sbox. It usually has low Toffoli depth and is used to construct low T-depth AES S-box.
  - Sbox: $|x\rangle |0\rangle |y\rangle \mapsto |x'\rangle |r\rangle |y \oplus S(x)\rangle$
  - SubS: $|x\rangle |0\rangle \mapsto |x'\rangle |r\rangle$, where $|r\rangle$ contains linear components of $S(x)$. SubS† is delayed to the next round to reduce the full depth in the shallowed pipeline structure.
  - Combined Sbox and SubS† to save idle $|0\rangle$ qubits.

Our input-invariant Sbox

- The input register may change to $|x'\rangle \neq |x\rangle$ before SubS† is done.
- Input-invariant: ensure $|x'\rangle = |x\rangle$ without additional Toffoli gates.
- A sufficient condition of making an Sbox input-invariant: the qubits used to update the input register can only be further updated by CNOT gates.
- Method: add a reverse sequence of CNOT gates which are related to the updating of the input register.

Table 7: Some low $TofD$ Sboxes

Source	#CNOT	#1qClifford	#Toffoli	$TofD$	Ancilla qubits	Input-invariant
[JNRV20]	186	4	34	6	120	✔
[HS22]	214	4	34	4	120	✔
[HS22]	356	4	78	3	182	✔
[LPZW23]	168	4	34	4	74	✘
This paper	179	4	34	4	74	✔
[LPZW23]	196	4	34	4	60	✘
This paper	207	4	34	4	60	✔
[JBK$^+$22]	313	4	78	3	136	✘[b]
[JBK$^+$22]	162	4	34	4	68[a]	✘[b]

[a] The full depth of this circuit is smaller when the Toffoli gates are decomposed.

[b] Since the authors do not give specific implementations, we cannot give detailed costs for their input-invariant versions.

Encryption circuit of AES-128

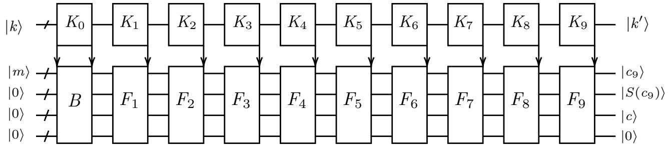

Figure 10: Our encryption circuit of AES-128. The arrows indicate the AddRoundKey process at the beginning or end of K_j.

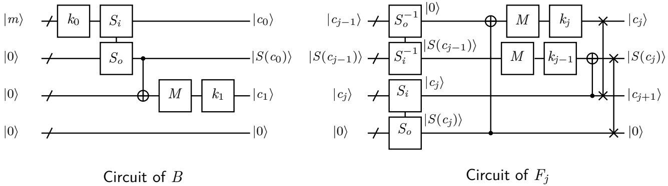

Figure 11: Circuits of B and F_j. S_i, S_o and S_i^{-1}, S_o^{-1} stand for the input and output registers of C_1 circuits and C_3 circuits, respectively. MixColmuns no longer acts on the first message register in F_9. ShiftRows are omitted for simplicity throughout the rest of the paper.

The key schedule

- Two consecutive roundkeys $|k_j\rangle, |k_{j+1}\rangle$ should be able to be computed simultaneously by CNOT gates.
- Store linear components of two consecutive roundkeys registers $|k_j^0\rangle\,|k_j^1\rangle\,|k_j^2\rangle\,|k_j^3\rangle\,|S(k_j^3)\rangle$ to save qubits.
- The dependency to compute k_{j+1}:

$$\begin{cases} k_{j+1}^0 = Const_{j+1} \oplus S(k_3^j) \oplus k_j^0 \\ k_{j+1}^1 = Const_{j+1} \oplus S(k_3^j) \oplus k_j^0 \oplus k_j^1 \\ k_{j+1}^2 = Const_{j+1} \oplus S(k_3^j) \oplus k_j^0 \oplus k_j^1 \oplus k_j^2 \\ k_{j+1}^3 = Const_{j+1} \oplus S(k_3^j) \oplus k_j^0 \oplus k_j^1 \oplus k_j^2 \oplus k_j^3 \end{cases},$$

where $Const_{j+1}$ is the $(j+1)$-th round constant in the key schedule.

The key schedule K_j and K_j'

Trivially 8 32-qubit registers $\longrightarrow$ only 6 or 5 32-qubit registers

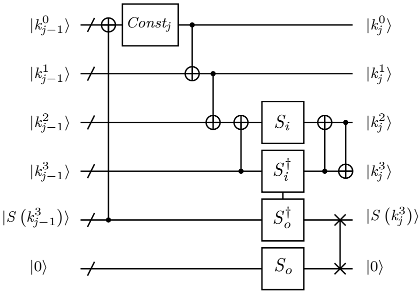

Figure 12: The j-th iteration K_j of the key schedule.

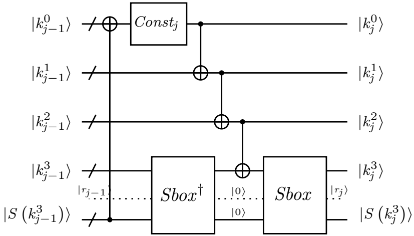

Figure 13: K_j' with Sbox and Sbox†. The dashed line represents the ancilla qubits of qAND-based Sbox.

- K_j' is only suitable for qAND-based Sbox, Sbox†.

Cost comparison

Table 8: Costs of encryption circuits of AES-128 for different structures

Circuits	C_p	C_i	C_{cp} **with** K_j	C_{cp} **with** $K_j^{'}$
Qubits of key registers	128	128	192	160
Qubits of message registers	128 $\times$ 11	128 $\times$ 2	128 $\times$ 4	128 $\times$ 4
$\mathcal{C}_1$ circuits in parallel	16	16	40	36
$\mathcal{C}_2$ circuits in parallel	4	2	0	0
Layers of AES S-box	10	20	10	10

Table 9: Condition of the S-box's ancilla qubits m for better cost

	Compared to $\mathcal{S}_p$	Compared to $\mathcal{S}_i$
Use K_j', better TD-W cost	$m < 54$	$m > 0$
Use K_j, better $TofD$-W cost	$m < 42$	$m < 16$

An AES-128 Encryption oracle with lower T-depth

- Previous researchers cannot break the limit of 2×10 layers of AES S-box.
- Under our compressed pipeline structure: $10 + 1$ layers of AES S-box. The last layer is the clear function below:

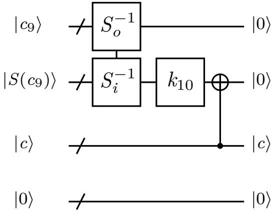

Figure 14: The clear function C.

- An AES-128 Encryption oracle with T-depth 33, using qAND-based C_1 circuits and C_3 circuits with T-depth 3.

Improved circuit for the shallowed pipeline structure

- Problem: if the Sbox is not input-invariant, the input register $|k^3_{j-1}\rangle$ will change before it is used later(since in the shallowed pipeline structure SubS† is delayed to the next round).

- Related works:
  - Use input-invariant Sbox with larger width. 32 qubits for storing each $|k^3_{j-1}\rangle$[JBK$^+$22].
  - Use Sbox that is not input-invariant with smaller width. 10 $\times$ 32 qubits for storing all $|k^3_{j-1}\rangle$ with $1 \leq j \leq 10$[LPZW23].

- Our work:
  - Make the Sbox input-invariant.
  - No additional qubits for each $|k^3_{j-1}\rangle$ by the key dependency $|k^3_{j-1}\rangle = |k^2_j\rangle \oplus |k^3_j\rangle$.
  - An Encryption circuit with a fewer width.

Comparison

Table 10: Comparison of encryption circuit metrics from various sources

Source	#CNOT	$\#X$	#Toffoli	$TofD$	W	$TofD$-W cost
[GLRS16]	166,548	1,456	151,552	12,672	984	12,469,248
[ASAM18]	192,832	1,370	150,528	-	976	-
[LGQW23]	53,360	1,072	16,688	12,168	264	3,212,352
[LPS20]	107,960	1,570	16,940	1,880	864	1,624,320
[ZWS+20]	128,517	4,528	19,788	2,016	512	1,032,192
[HS22]($p = 9$)	126,016	2,528	17,888	1,558	374	582,692
[LGQW23]	53,496	1,072	16,664	1,472	328	482,816
[HS22]($p = 18$)	126,016	2,528	17,888	820	492	403,440
[JBK+22]	81,312	800	12,240	40	6,368	254,720
[LXX+23]($m = 16$)	77,984	2,224	19,608	476	474	225,624
This paper[c]	96,364	2,172	21,660	220	944	207,680
[LPZW23] (out-of-place)	75,024	800	12,920	40	4,823	192,920
[LPZW23] (in-place)	65,736	800	12,920	40	3,667	146,680
[JBK+22]	63,868	816	12,380	40	3,428	137,120
This paper[a]	67,150	800	12,920	40	**3,368**	**134,720**
This paper[b]	64,750	800	12,920	40	**3,268**	**130,720**

[a] Using our improved shallowed pipeline structure and the input-invariant version of combined Sbox and Sbox† in [LPZW23].

[b] Using our improved shallowed pipeline structure and the input-invariant version of combined Sbox and Sbox† with fewer qubits in [JBK+22].

[c] Using our compressed pipeline structure and the C_1 circuit in [LXX+23] with $TofD$ 22 and 6 ancilla qubits.

Conclusion

- An **improved greedy algorithm** for finding **low-depth** CNOT circuits. The depth **10** implementation of AES MixColumns.
- A new **compressed pipeline structure** for iterative building blocks. It can be used to construct **Encryption oracles** with **low round depth** (T-depth).
- Some improvements in terms of quantum circuits of AES, including detailed **encryption circuits**, **low T-depth Encryption oracles**, and the **input-invariant Sbox** applied in the shallowed pipeline structure.

Similar independent work: Zhang M, Shi T, Wu W, et al. Optimized Quantum Circuit of AES with Interlacing-Uncompute Structure[J]. IEEE Transactions on Computers, 2024.

Thank you!

Martin R Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, and Tolga Yalçın.
Block ciphers–focus on the linear layer (feat. pride).
In *Advances in Cryptology–CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I 34*, pages 57–76. Springer, 2014.

Mishal Almazrooie, Azman Samsudin, Rosni Abdullah, and Kussay N Mutter.
Quantum reversible circuit of AES-128.
Quantum information processing, 17:1–30, 2018.

Roberto Avanzi.
The QARMA block cipher family. Almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency s-boxes.
IACR Transactions on Symmetric Cryptology, pages 4–44, 2017.

Paulo SLM Barreto.
The Anubis block cipher.
NESSIE, 2000.

Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni.
Midori: A block cipher for low energy.
In *Advances in Cryptology–ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3, 2015, Proceedings, Part II 21*, pages 411–436. Springer, 2015.

Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, et al.
Prince–a low-latency block cipher for pervasive computing applications.
In *Advances in Cryptology–ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18*, pages 208–225. Springer, 2012.

Subhadeep Banik, Yuki Funabiki, and Takanori Isobe.
Further results on efficient implementations of block cipher linear layers.
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 104(1):213–225, 2021.

Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim.
The SKINNY family of block ciphers and its low-latency variant MANTIS.
In *Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36*, pages 123–153. Springer, 2016.

Paulo Barreto, Ventzislav Nikov, Svetla Nikova, Vincent Rijmen, and Elmar Tischhauser.
Whirlwind: a new cryptographic hash function.
Designs, codes and cryptography, 56:141–162, 2010.

Carlos Cid, Sean Murphy, and Matthew JB Robshaw.
Small scale variants of the AES.
In *FSE*, volume 3557, pages 145–162. Springer, 2005.

Beierle Christof, Kranz Thorsten, and Leander Gregor.
Lightweight multiplication in gf (2n) with applications to mds matrices; crypto 2016. lncs 9814, 2016.

Timothée Goubault de Brugière, Marc Baboulin, Benoît Valiron, Simon Martiel, and Cyril Allouche.

Gaussian elimination versus greedy methods for the synthesis of linear reversible circuits.
ACM Transactions on Quantum Computing, 2(3):1–26, 2021.

Timothee Goubault De Brugiere, Marc Baboulin, Benoît Valiron, Simon Martiel, and Cyril Allouche.
Reducing the depth of linear reversible quantum circuits.
IEEE Transactions on Quantum Engineering, 2:1–22, 2021.

Joan Daemen and Vincent Rijmen.
The design of Rijndael, volume 2.
Springer, 2002.

Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt.
Applying grover ’ s algorithm to AES: quantum resource estimates.
In *International Workshop on Post-Quantum Cryptography*, pages 29–43. Springer, 2016.

Zhenyu Huang and Siwei Sun.
Synthesizing quantum circuits of AES with lower T-depth and less qubits.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 614–644. Springer, 2022.

Kyungbae Jang, Anubhab Baksi, Hyunji Kim, Gyeongju Song, Hwajeong Seo, and Anupam Chattopadhyay.
Quantum analysis of AES.
Cryptology ePrint Archive, 2022.

Jérémy Jean, Ivica Nikolić, and Thomas Peyrin.
Joltik v1. 3.
CAESAR Round, 2, 2015.

Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia.
Implementing grover oracles for quantum key search on AES and LowMC.
In *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 30*, pages 280–310. Springer, 2020.

Jérémy Jean, Thomas Peyrin, Siang Meng Sim, and Jade Tourteaux.
Optimizing implementations of lightweight building blocks.
IACR Transactions on Symmetric Cryptology, 2017(4):130–168, 2017.

Pascal Junod and Serge Vaudenay.
FOX: a new family of block ciphers.

In *Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers 11*, pages 114–129. Springer, 2005.

Zhenqiang Li, Fei Gao, Sujuan Qin, and Qiaoyan Wen.
New record in the number of qubits for a quantum implementation of AES.
Frontiers in Physics, 11:1171753, 2023.

Brandon Langenberg, Hai Pham, and Rainer Steinwandt.
Reducing the cost of implementing the advanced encryption standard as a quantum circuit.
IEEE Transactions on Quantum Engineering, 1:1–12, 2020.

Qun Liu, Bart Preneel, Zheng Zhao, and Meiqin Wang.
Improved quantum circuits for AES: Reducing the depth and the number of qubits.
In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 67–98. Springer, 2023.

Meicheng Liu and Siang Meng Sim.
Lightweight MDS generalized circulant matrices.

In *Fast Software Encryption: 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 101–120. Springer, 2016.

Shun Li, Siwei Sun, Chaoyun Li, Zihao Wei, and Lei Hu.
Constructing low-latency involutory MDS matrices with lightweight circuits.
IACR Transactions on Symmetric Cryptology, pages 84–117, 2019.

Yongqiang Li and Mingsheng Wang.
On the construction of lightweight circulant involutory MDS matrices.
In *Fast Software Encryption: 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 121–139. Springer, 2016.

Qun Liu, Weijia Wang, Yanhong Fan, Lixuan Wu, Ling Sun, and Meiqin Wang.
Towards low-latency implementation of linear layers.
IACR Transactions on Symmetric Cryptology, pages 158–182, 2022.

Da Lin, Zejun Xiang, Runqing Xu, Shasha Zhang, and Xiangyong Zeng.
Optimized quantum implementation of aes.
Quantum Information Processing, 22(9):352, 2023.

Siang Meng Sim, Khoongming Khoo, Frédérique Oggier, and Thomas Peyrin.
Lightweight MDS involution matrices.
In *Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers 22*, pages 471–493. Springer, 2015.

Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson.
Twofish: A 128-bit block cipher.
NIST AES Proposal, 15(1):23–91, 1998.

Sumanta Sarkar and Habeeb Syed.
Lightweight diffusion layer: Importance of Toeplitz Matrices.
IACR Transactions on Symmetric Cryptology, 2016(1):95–113, 2016.

Sumanta Sarkar and Habeeb Syed.
Analysis of Toeplitz MDS Matrices.
In *Australasian Conference on Information Security and Privacy*, pages 3–18. Springer, 2017.

Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata.
The 128-bit block cipher CLEFIA.

In *Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers 14*, pages 181–195. Springer, 2007.

Zejun Xiang, Xiangyoung Zeng, Da Lin, Zhenzhen Bao, and Shasha Zhang.
Optimizing implementations of linear layers.
IACR Transactions on Symmetric Cryptology, pages 120–145, 2020.

Chengkai Zhu and Zhenyu Huang.
Optimizing the depth of quantum implementations of linear layers.
In *International Conference on Information Security and Cryptology*, pages 129–147. Springer, 2022.

Jian Zou, Zihao Wei, Siwei Sun, Ximeng Liu, and Wenling Wu.
Quantum circuit implementations of AES with fewer qubits.
In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26*, pages 697–726. Springer, 2020.