Impact of Optimized Operations $A \quad B, A \quad C$ for Binary Field Inversion on Quantum Computers

Kyoungbae Jang, Seung Ju Choi, Hyeokdong Kwon,

Zhi Hu and Hwajeong Seo *

Hansung University

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

https://crypto.modoo.at

Contents

Introduction

Our Work

Evaluation

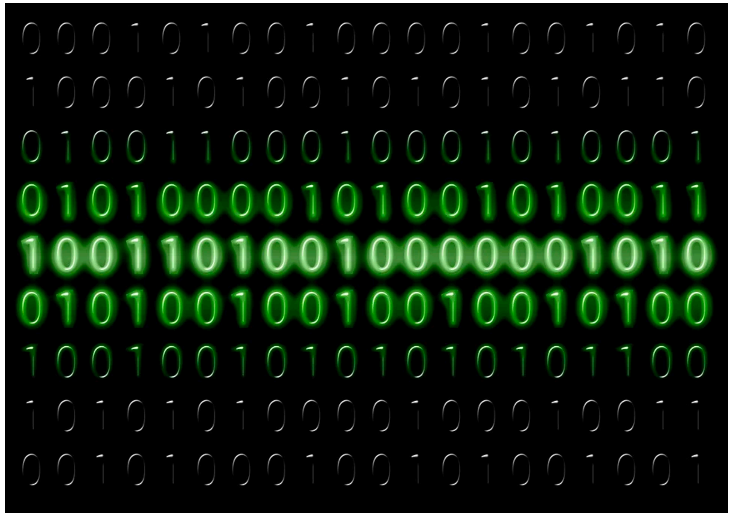
Conclusion

CryptoCraft LAB

Introduction

Quantum Computer

- How to apply a quantum algorithm?



Classic implementation

Quantum implementation

Binary Field Arithmetic

- $GF(2^n)$ $\longleftrightarrow$ 

  Binary field arithmetic — Cryptographic applications

- We Focus on binary field inversion operation on quantum computer

$$a \in GF(2^n),\ a \cdot a^{-1} = 1$$

Binary field Inversion Operation

- The inversion operation in cryptography.

A E S **E C C**

- How is the binary field inversion operation performed?

- **Itoh–Tsujii inversion algorithm**

Itoh-Tsujii-based Inversion for AES

Algorithm : Inversion for field polynomial $p = x^8 + x^4 + x^3 + x + 1$

Input : z satisfying $1 \leq z \leq p - 1$

output : Inverse t = z^{-1} mod p

$z_2 \leftarrow z^2 \cdot z$
$z_3 \leftarrow z_2^2 \cdot z$
$z_6 \leftarrow z_3^{2^3} \cdot z_3$
$z_7 \leftarrow z_6^2 \cdot z$
$t \leftarrow z_7^2$
return t

Multiplication + Squaring

Squaring is simple but multiplication ??

Squaring of $x^2 + x + 1$

Bit → 1 1 1

0 0 0

1 0 1 0 1

Multiplication in Binary Field

- Multiplying two polynomial + Modular reduction
  - Reduction → simple (Only XOR)
  - Multiplication → complicative

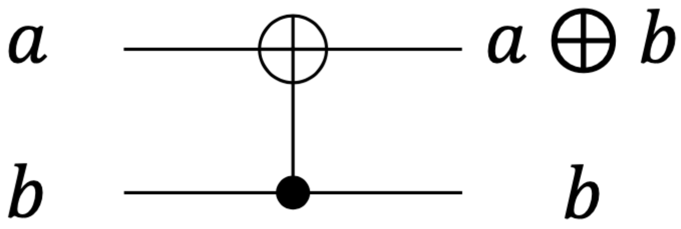
- Optimized polynomial multiplication
  - Karatsuba algorithm

Our Work

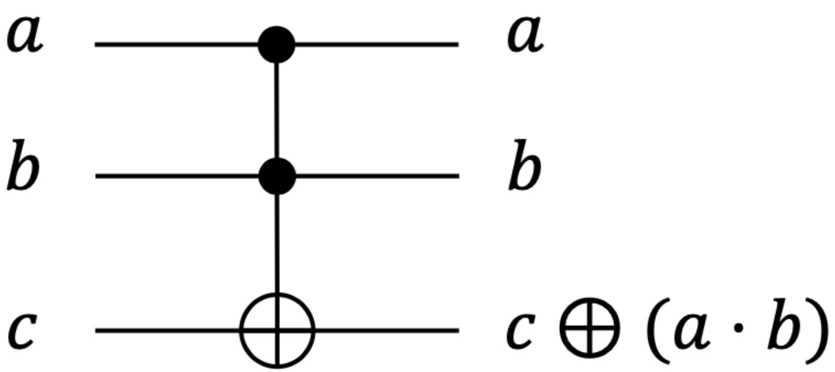
Our Work

- The Itoh-Tsujii algorithm for binary field inversion was optimized on the quantum computer
  - First, multiplication → Optimized by Karatsuba algorithm
  - Second, $A \cdot B$ and $A \cdot C$ pattern with Karatsuba algorithm is optimized by changing the reversible circuit to a non-reversible circuit
  - Lastly, qubits are saved efficiently after squaring operation by using non-reversible Karatsuba multiplication
  - The proposed method can be used for the binary field inversion of ECC

Quantum Gates (Background)



CNOT gate



Toffoli gate

- Toffoli gate → **AND** operation or F_2 multiplication
- CNOT gate → **XOR** operation
- Cost : Toffoli gate $>$ CNOT gate

  1 Toffoli gate $>$ 6 CNOT gate

Karatsuba Multiplication(Background)

- Karatsuba algorithm Replace one n - bit multiplication into three $\frac{n}{2}$ - bit multiplication with a few addition operations

  - Multiplying polynomial $\boldsymbol{f}$ and $\boldsymbol{g}$ of size n , divide into s $= \frac{n}{2}$

$$f = f_1 x^s + f_0$$
$$g = g_1 x^s + g_0$$

$$\boxed{f_0 \cdot g_0}$$
$$\boxed{(f_0 + f_1) \cdot (g_0 + g_1)}$$
$$\boxed{f_1 \cdot g_1}$$

  - After splitting, Karatsuba multiplication can be performed

$$\boxed{f_0 \cdot g_0} + \{\boxed{(f_0 + f_1) \cdot (g_0 + g_1)} + f_0 \cdot g_0 + \boxed{f_1 \cdot g_1}\} x^s + f_1 \cdot g_1 x^{2s}$$

Inversion Operation

Algorithm : Inversion for field polynomial $p = x^8 + x^4 + x^3 + x + 1$

Input : z satisfying $1 \leq z \leq p - 1$

output : Inverse t = z^{-1} mod p

$z_2 \leftarrow \boxed{z^2 \cdot z}$

$z_3 \leftarrow z_2^2 \cdot z$

$z_6 \leftarrow z_3^{2^3} \cdot z_3$

$z_7 \leftarrow z_6^2 \cdot z$

$t \leftarrow z_7^2$

return t

* Square operation is also simple in quantum computer

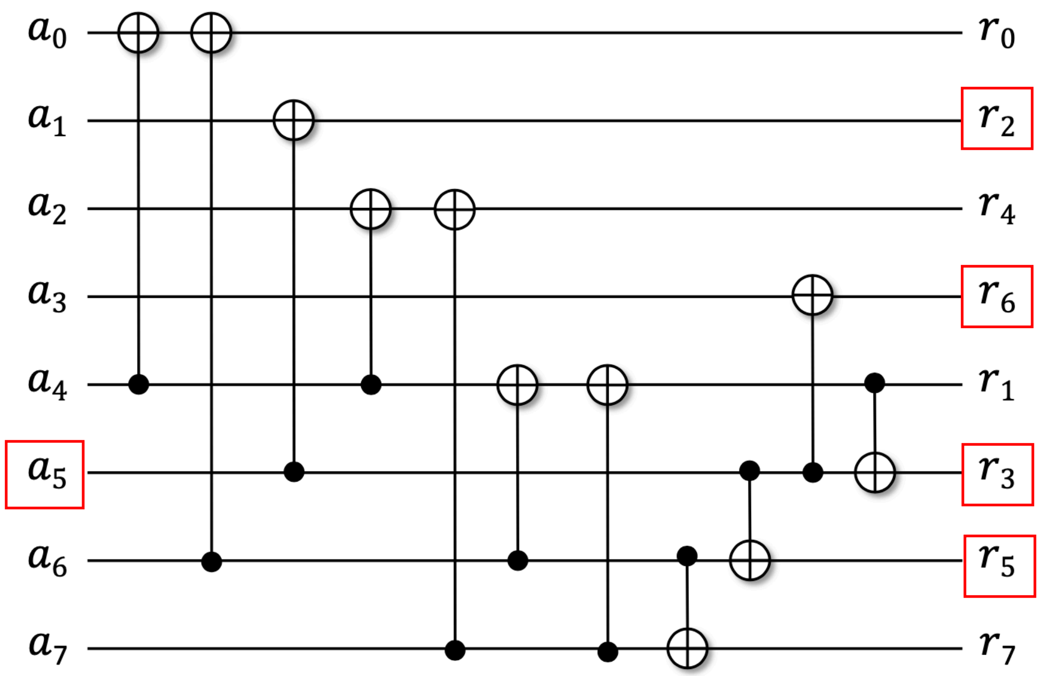
* 12.E. Mun˜oz-Coreas and H. Thapliyal, "Design of quantum circuits for Galois field squaring and exponentiation," in 2017 IEEE Computer Society Annual Symposium on VLSI

Squaring Operation in Quantum Circuit

Input : $a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1 a_0$ field polynomial $p = x^8 + x^4 + x^3 + x + 1$

$\boxed{0\ a_7\ 0\ a_6\ 0\ a_5\ 0\ a_4}\ 0\ a_3\ 0\ a_2\ 0\ a_1 0\ a_0$

modular



Example

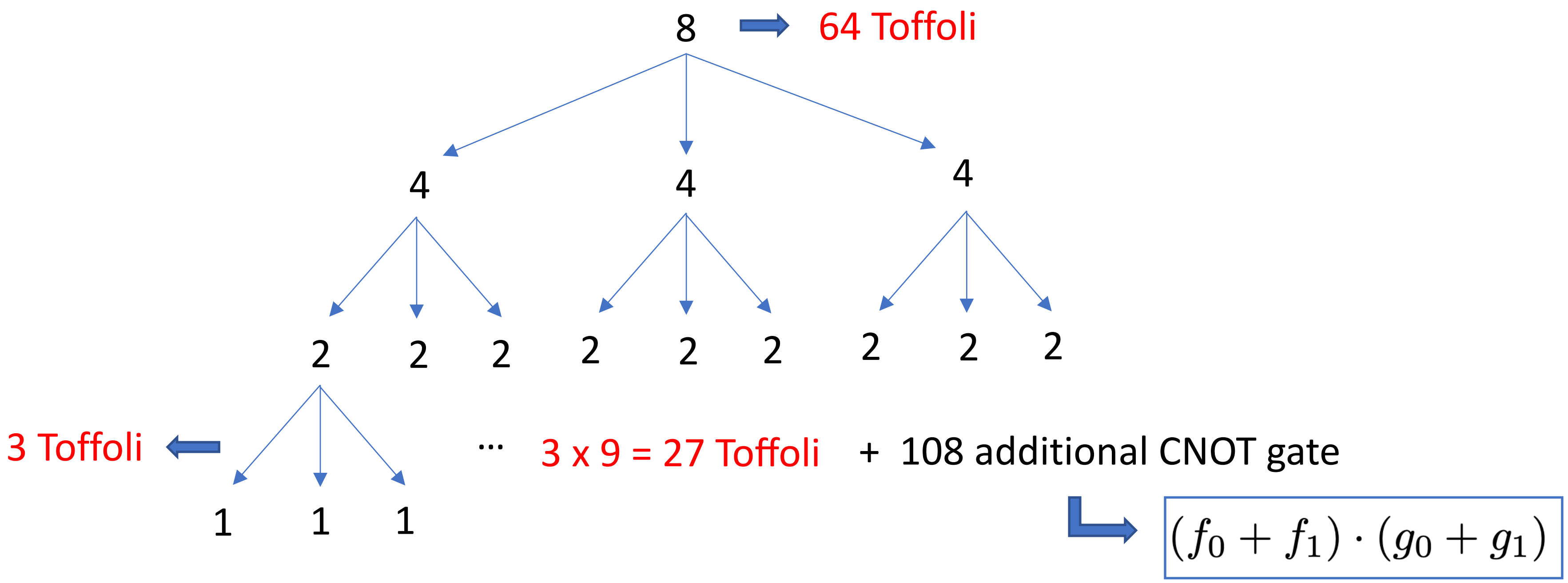
$$a_5 \rightarrow x^{10} = x^6 + x^5 + x^3 + x^2$$

Only 11 CNOT gate

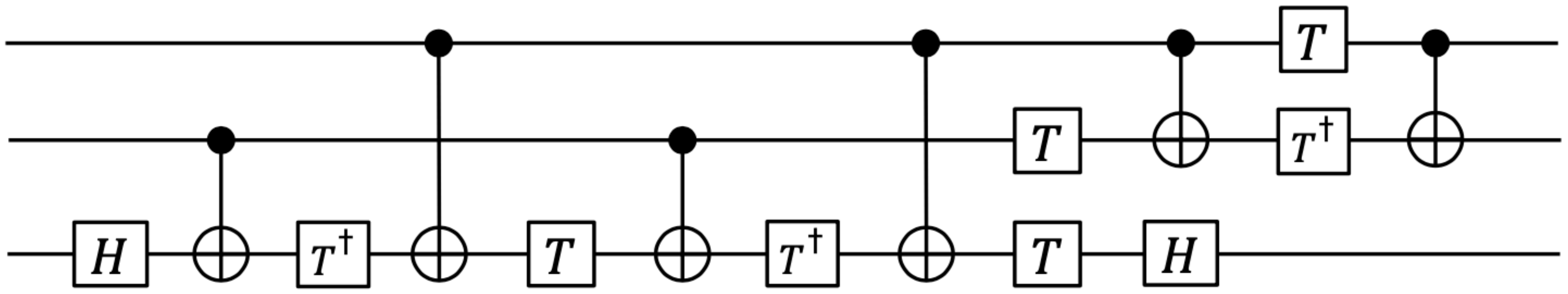
< Squaring operation on $x^8 + x^4 + x^3 + x + 1$ >

Karatsuba Multiplication in Quantum Circuit

- The multiplication operation is an expensive operation
- Generic 8 −bit multiplication uses 64 ($\boldsymbol{n^2}$) Toffoli gates
- If the Karatsuba algorithm is applied recursively, only **27 Toffoli gates ,**



Karatsuba Multiplication in Quantum Circuit



< Circuit configuration of the Toffoli gate >

- 1 Toffoli gate = 6 CNOT gates + 9 T-gates.
- 64 Toffoli vs 27 Toffoli + 108 CNOT

$A \cdot B$ and $A \cdot C$ Pattern in the Inversion Operation

Algorithm : Inversion for field polynomial $p = x^8 + x^4 + x^3 + x + 1$

Input : z satisfying $1 \le z \le p - 1$

output : Inverse $t = z^{-1} \bmod p$

1: $z_2 \leftarrow z^2 \cdot z$

2: $z_3 \leftarrow z_2^2 \cdot z$

3: $z_6 \leftarrow z_3^{2^3} \cdot z_3$

4: $z_7 \leftarrow z_6^2 \cdot z$

5: $t \leftarrow z_7^2$

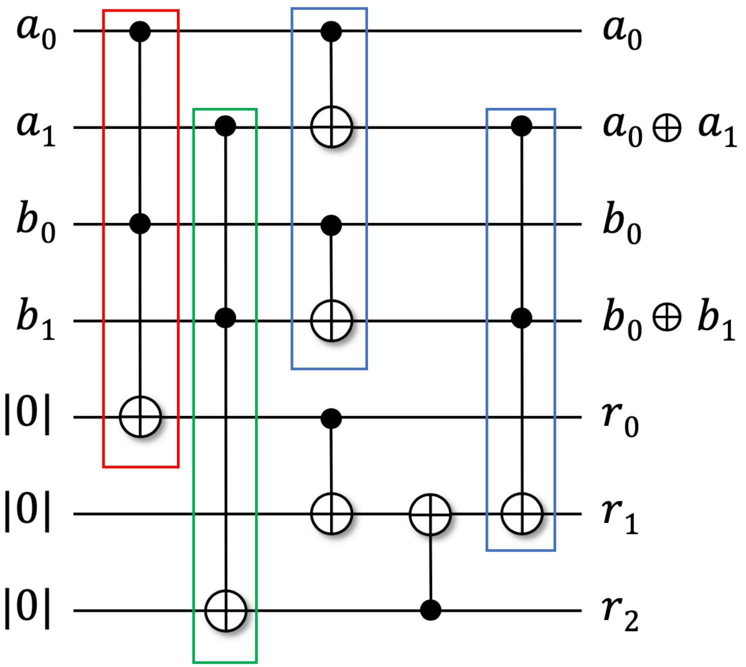
6: **return** t

$\longrightarrow$ $A \cdot B$

$A \cdot C$

Karatsuba Multiplication in Quantum Circuit

- 2-bit multiplication operations $A(a_0, a_1)$ and $B(\, b_{0,}\, b_1 \,)$



$$f = f_1 x^s + f_0$$
$$g = g_1 x^s + g_0$$

$\boxed{f_0 \cdot g_0}$

$\boxed{(f_0 + f_1) \cdot (g_0 + g_1)}$

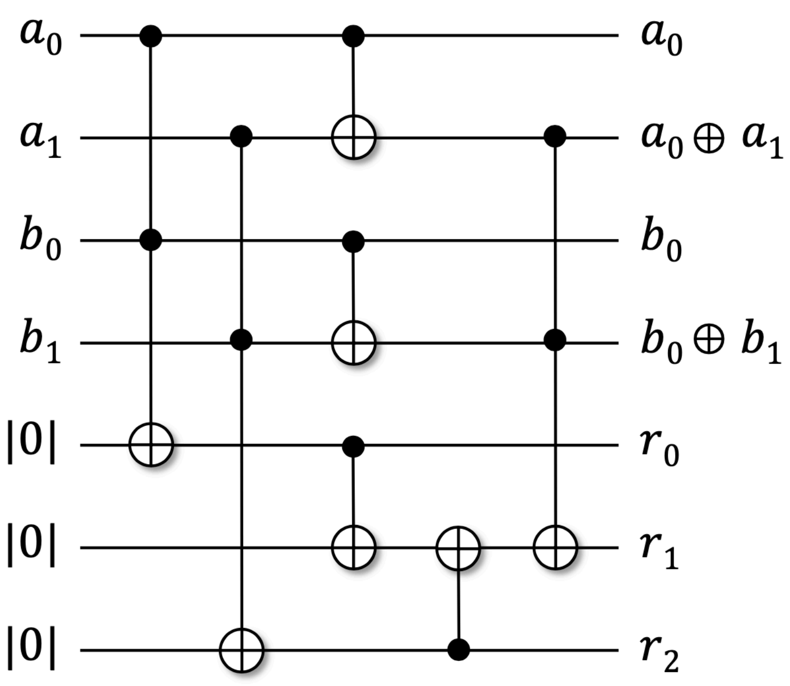
$\boxed{f_1 \cdot g_1}$

$$\boxed{f_0 \cdot g_0} + \{\boxed{(f_0 + f_1) \cdot (g_0 + g_1)} + f_0 \cdot g_0 + \boxed{f_1 \cdot g_1}\}x^s + f_1 \cdot g_1 x^{2s}$$

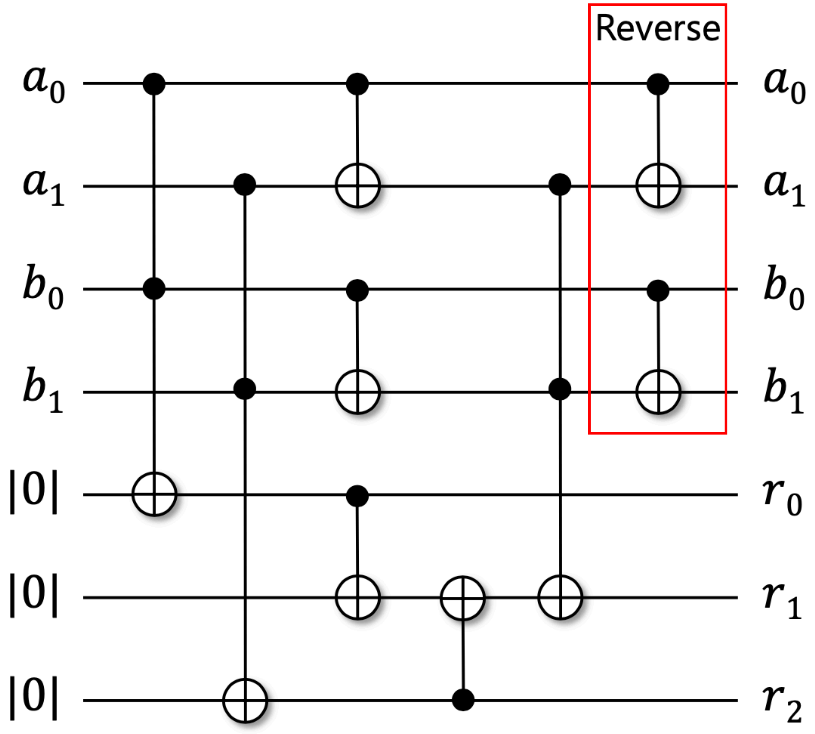
- a_1 and b_1 are changed after Karatsuba multiplication : non-reversible

Karatsuba Multiplication in Quantum Circuit

- The reversible circuit should be performed for the operand A cause of $A \cdot C$ multiplication



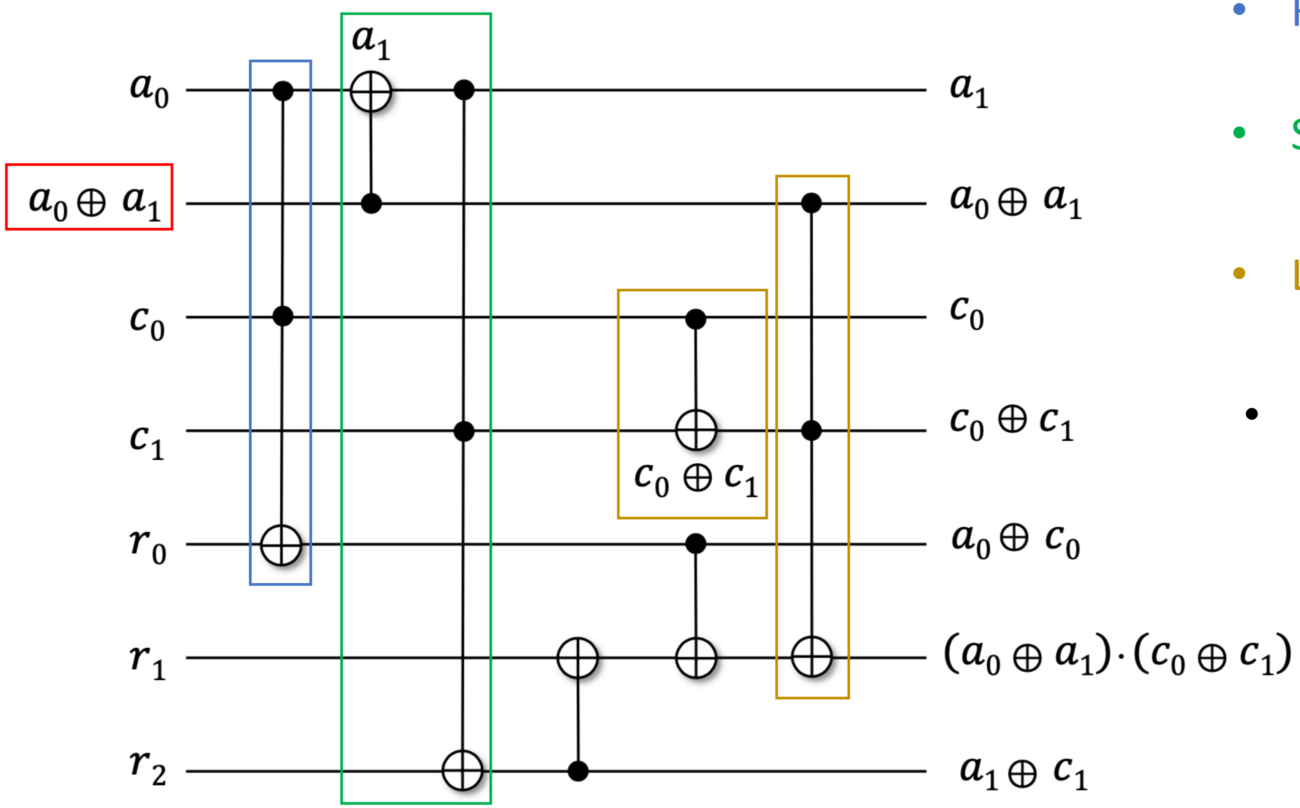
Non-reversible



Reversible

Non-Reversible based $A \cdot B$ and $A \cdot C$

- Proposed $A \cdot B$ and $A \cdot C$ structure reduces this overhead
  - Simple Case : 2-bit



- First, $a_0 \cdot c_0$
- Second, a_0 is changed to a_1 then $a_1 \cdot c_1$
- Lastly, $c_0 + c_1$, then $(a_0 + a_1) \cdot (c_0 + c_1)$
- $A \cdot B$ and $A \cdot C = A \cdot B$ and $A' \cdot C$

Reducing the Number of Qubits

- In the $A \cdot B$ **and** $A \cdot C$ structure, we can also reduce the total number of qubits

$$1: \; z_2 \leftarrow z^2 \cdot z$$
$$2: \; z_3 \leftarrow z_2^2 \cdot z$$

$\longrightarrow$ $A \cdot B$, $A \cdot C$

- B is the square of the A

$$\boxed{0\ a_7\ 0\ a_6\ 0\ a_5\ 0\ a_4}\ 0\ a_3\ 0\ a_2\ 0\ a_1 0\ a_0 \quad \rightarrow \quad B = (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0)$$

modular

  - B consists of combinations of the elements of A

Reducing the Number of Qubits

- B can be initialize to zero efficiently when we performing $A \cdot C$ operation.

$$\begin{aligned} &1:\ z_2 \leftarrow z^2 \cdot z \\ &2:\ z_3 \leftarrow z_2^2 \cdot z \end{aligned} \longrightarrow \begin{aligned} &A \cdot B \\ &A \cdot C \end{aligned}$$

Step 1. After multiplication(first row), B and $A \rightarrow B'$ and A' cause of Karatsuba algorithm

Step 2. In proposed non-reversible design C is multiplied by A'

Step 3. In $A' \cdot C$ the value of A' changed to A'' with the Karatsuba operation

We can effectively initialize the qubits(B') to zero

Reducing the Number of Qubits

- Combination of A values of B' after $A \cdot B$ computation on $GF(2^8)$
  - $A \rightarrow$ Squaring $\rightarrow B \rightarrow$ Karatsuba multiplication $\rightarrow B'$

k	B'_k	k	B'_k
0	$a_0 + a_2 + a_6 + a_7$	4	$a_2 + a_3 + a_4 + a_5 + a_7$
1	$a_4 + a_5 + a_7$	5	$a_5 + a_7$
2	$a_1 + a_3$	6	$a_3 + a_5 + a_6 + a_7$
3	$a_4 + a_5$	7	$a_6 + a_7$

- in $A' \cdot C$, * the value of A' changed to A'' for Karatsuba multiplication

On the next slide…

$$f = f_1 x^s + f_0$$
$$g = g_1 x^s + g_0$$

$f_0 \cdot g_0$

* $\boxed{(f_0 + f_1) \cdot (g_0 + g_1)}$

$f_1 \cdot g_1$

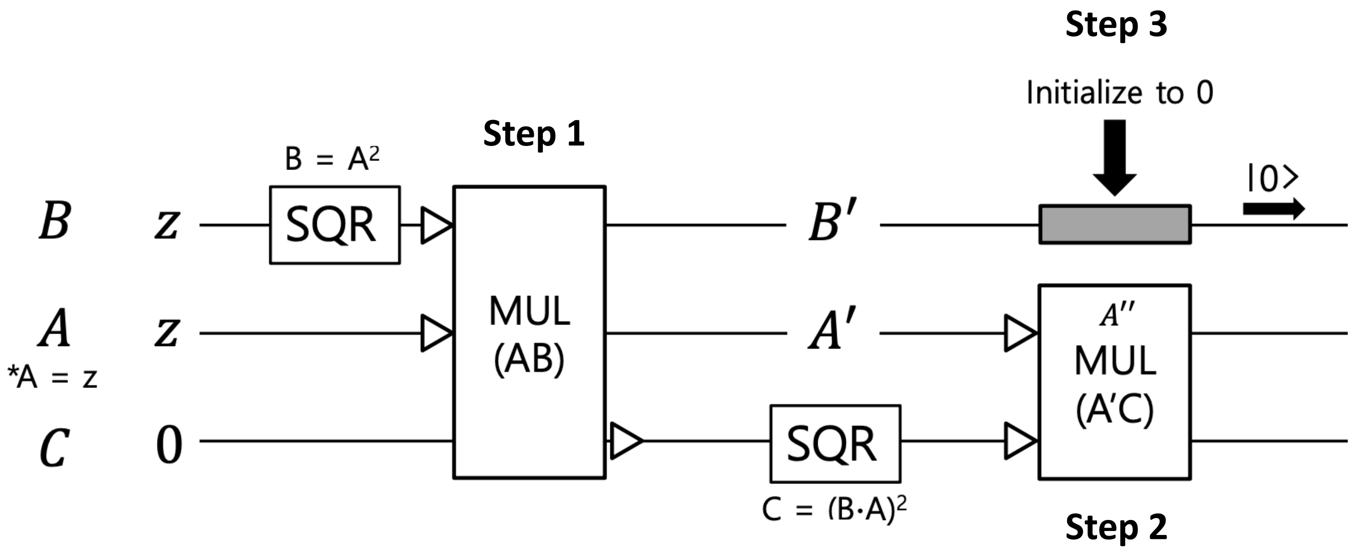
- By performing the CNOT operation on B_0 with k_6 and k_{14} $\rightarrow B_0$ is initialized into zero.

Combination of A values of A″ during A · C

k	A_k	R_k
0	a_0	a_0c_0
1	a_1	a_1c_1
2	a_0+a_1	$(a_0+a_1)(c_0+c_1)$
3	a_2	a_2c_2
4	a_3	a_3c_3
5	a_2+a_3	$(a_2+a_3)(c_2+c_3)$
6	a_0+a_2	$(a_0+a_2)(c_0+c_2)$
7	a_1+a_3	$(a_1+a_3)(c_1+c_3)$
8	$a_0+a_1+a_2+a_3$	$(a_0+a_1+a_2+a_3)(c_0+c_1+c_2+c_3)$
9	a_4	a_4c_4
10	a_5	a_5c_5
11	a_4+a_5	$(a_4+a_5)(c_4+c_5)$
12	a_6	a_6c_6
13	a_7	a_7c_7
14	a_6+a_7	$(a_6+a_7)(c_6+c_7)$
15	a_4+a_6	$(a_4+a_6)(c_4+c_6)$
16	a_5+a_7	$(a_5+a_7)(c_5+c_7)$
17	$a_4+a_5+a_6+a_7$	$(a_4+a_5+a_6+a_7)(c_4+c_5+c_6+c_7)$
18	a_0+a_4	$(a_0+a_4)(c_0+c_4)$
19	a_1+a_5	$(a_1+a_5)(c_1+c_5)$
20	$a_0+a_1+a_4+a_5$	$(a_0+a_1+a_4+a_5)(c_0+c_1+c_4+c_5)$
21	a_2+a_6	$(a_2+a_6)(c_2+c_6)$
22	a_3+a_7	$(a_3+a_7)(c_3+c_7)$
23	$a_2+a_3+a_6+a_7$	$(a_2+a_3+a_6+a_7)(c_2+c_3+c_6+c_7)$
24	$a_0+a_2+a_4+a_6$	$(a_0+a_2+a_4+a_6)(c_0+c_2+c_4+c_6)$
25	$a_1+a_3+a_5+a_7$	$(a_1+a_3+a_5+a_7)(c_1+c_3+c_5+c_7)$
26	$a_0+a_1+a_2+a_3+a_4+a_5+a_6+a_7$	$(a_0+a_1+a_2+a_3+a_4+a_5+a_6+a_7)$ $(c_0+c_1+c_2+c_3+c_4+c_5+c_6+c_7)$

Reducing the Number of Qubits

- Overview of proposed method



- By utilizing this feature, we can initialize 8 qubits with only 11 CNOT gates.

Evaluation & Conclusion

Evaluation

- Evaluated on $x^8 + x^4 + x^3 + x + 1$ inversion, which is used in the substitute layer of AES

Method	Toffoli gate	CNOT gate	Qubit
Kepley et al. [11]	54	252	70
This work (CNOT reduction)	54	**238**	70
This work (qubit recycle)	54	**249**	**62**

[11]. S. Kepley and R. Steinwandt, "Quantum circuits for F2 -multiplication with sub- quadratic gate count," Quantum Information Processing, vol. 14, no. 7, pp. 2373– 2386, 2015.

Conclusion

- Implementation of binary field inversion in quantum circuits for $A \cdot B$ and $A \cdot C$ structure.
  - Non-reversible circuits are used for $A \cdot B$ and $A \cdot C$ patterns
  - Qubit reuse technique is suggested
  - The quantum circuit for binary field inversion achieved the optimal number of Toffoli gates, CNOT gates and qubits.
  - The proposed method can be used for the binary field inversion of ECC

The Inversion Algorithm for sect283k1 and sect283r1

Algorithm 2 Itoh-Tsuji-based inversion for $p = x^{283} + x^{12} + x^7 + x^5 + 1$

Require: Integer z satisfying $1 \le z \le p - 1$.

Ensure: Inverse $t = z^{p-2} \bmod p = z^{-1} \bmod p$.

1: $z_2 \leftarrow z^2 \cdot z$ {cost: 1S+1M}
2: $z_4 \leftarrow z_2^{2^2} \cdot z_2$ {cost: 2S+1M}
3: $z_8 \leftarrow z_4^{2^4} \cdot z_4$ {cost: 4S+1M}
4: $z_{16} \leftarrow z_8^{2^8} \cdot z_8$ {cost: 8S+1M}
5: $z_{17} \leftarrow z_{16}^2 \cdot z$ {cost: 1S+1M}
6: $z_{34} \leftarrow z_{17}^{2^{17}} \cdot z_{17}$ {cost: 17S+1M}
7: $z_{35} \leftarrow z_{34}^2 \cdot z$ {cost: 1S+1M}
8: $z_{70} \leftarrow z_{35}^{2^{35}} \cdot z_{35}$ {cost: 35S+1M}
9: $z_{140} \leftarrow z_{70}^{2^{70}} \cdot z_{70}$ {cost: 70S+1M}
10: $z_{141} \leftarrow z_{140}^2 \cdot z$ {cost: 1S+1M}
11: $z_{282} \leftarrow z_{141}^{2^{141}} \cdot z_{141}$ {cost: 141S+1M}
12: $t \leftarrow z_{282}^2$ {cost: 1S}
13: **return** t

Future Works

- Another arithmetic structures ?
- Optimized implementation of ciphers in quantum computer

Thank you!

hwajeong84@gmail.com
starj1023@gmail.com