# Space-efficient quantum multiplication of polynomials for binary finite fields

최승주

https://youtu.be/-hpZiDPcOO4

HANSUNG UNIVERSITY 한성대학교

CryptoCraft LAB
https://crypto.modoo.at

# Space Efficient Multiplication

Space-efficient quantum multiplication of polynomials for binary finite fields with sub-quadratic Toffoli gate count

Iggy van Hoof

Technische Universiteit Eindhoven
i.v.hoof@student.tue.nl

**Abstract.** Multiplication is an essential step in a lot of calculations. In this paper we look at multiplication of 2 binary polynomials of degree at most $n-1$, modulo an irreducible polynomial of degree $n$ with $2n$ input and $n$ output qubits, without ancillary qubits, assuming no errors. With straightforward schoolbook methods this would result in a quadratic number of Toffoli gates and a linear number of CNOT gates. This paper introduces a new algorithm that uses the same space, but by utilizing space-efficient variants of Karatsuba multiplication methods it requires only $O(n^{\log_2(3)})$ Toffoli gates at the cost of a higher CNOT gate count: theoretically up to $O(n^2)$ but in examples the CNOT gate count looks a lot better.

# Space Efficient Multiplication

- 유한체 상에서 다항식간의 곱셈

  - 일반 컴퓨터에서는 카라추바 곱셈 기법을 기반으로 한 다양한 방식이 존재

- 차수가 n인 다항식을 연산하기 위해서는 2n 만큼의 공간을 사용했었음

  - n → O(long n) → 0(본 논문)

- 카라추바만큼 계산 속도라 빠른 다른 곱셈 제안 기법들은 다 추가적인 공간을 사용함

  - 본 논문에서는 추가 공간을 사용하지 않음

# Karatsuba Algorithm

- 아나톨리 알렉세예비치 카라추바

  - 큰 수들의 곱을 빠르게 진행할 수 있는 알고리즘

$$x = x_1B^m+x_0$$
$$y = y_1B^m+y_0$$

$$z_2 = \underline{x_1y_1}$$
$$z_1 = \underline{x_1y_0} + \underline{x_0y_1}$$
$$z_0 = \underline{x_0y_0}$$

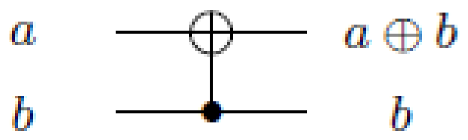
$$xy = (x_1B^m+x_0)(y_1B^m+y_0) = z_2B^{2m} + z_1B^m+z_0$$

# Karatsuba Algorithm

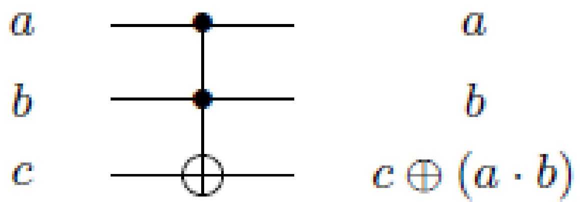
$$x = x_1 B^m + x_0$$
$$y = y_1 B^m + y_0$$

$$z_2 = \underline{x_1 y_1}$$
$$z_0 = \underline{x_0 y_0}$$
$$z_1 = x_1 y_0 + x_0 y_1$$
$$= (x_1 y_1 + x_1 y_0 + x_0 y_1 + x_0 y_0) - x_1 y_1 + x_0 y_0$$
$$= \underline{(x_1 + x_0)(y_1 + y_0)} - z_2 - z_0$$

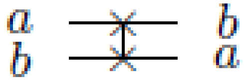
# Space Efficient Multiplication




Circuit 1: The CNOT gate




Circuit 2: The TOF gate




Circuit 3: The swap

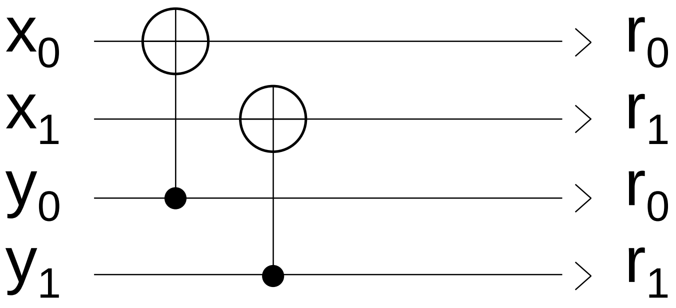
**xor** **AND** **INDEX**

# Space Efficient Multiplication

- Addition → CNOT

  - 차수가 n인 다항식간의 덧셈은 n+1개의 CNOT 사용

  - 결과가 input 자리를 대신해서 들어감



# Space Efficient Multiplication

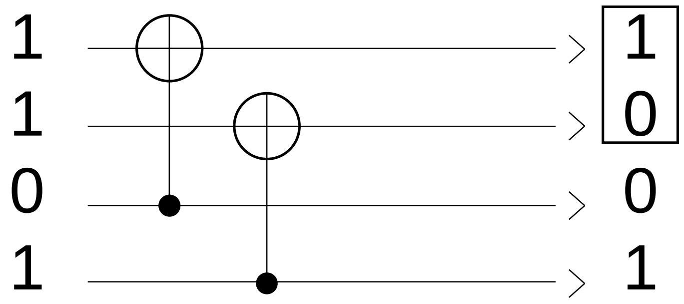
- Addition → CNOT

  - 차수가 n인 다항식간의 덧셈은 n+1개의 CNOT 사용

  - 결과가 input 자리를 대신해서 들어감

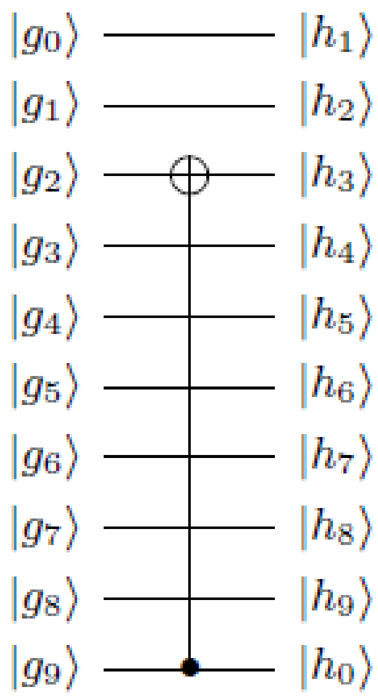
- x+1
- x

(x+1) + (x)
= 2x
= 1



# Space Efficient Multiplication

**Binary Shift**

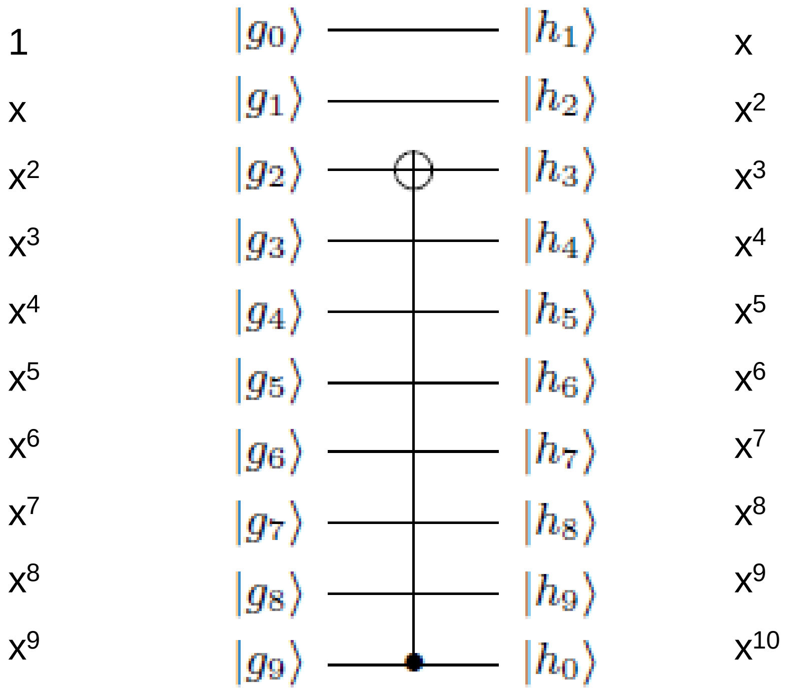



Circuit 4: Binary shift circuit for $\mathbb{F}_{2^{10}}$ with $g_0 + \cdots + g_9x^9$ as the input and $h_0 + \cdots + h_9x^9 = g_9 + g_0x + g_1x^2 + (g_2 + g_9)x^3 + g_3x^4 + \cdots + g_8x^9$ as the output.

# Space Efficient Multiplication

**Binary Shift**

multiplication with x

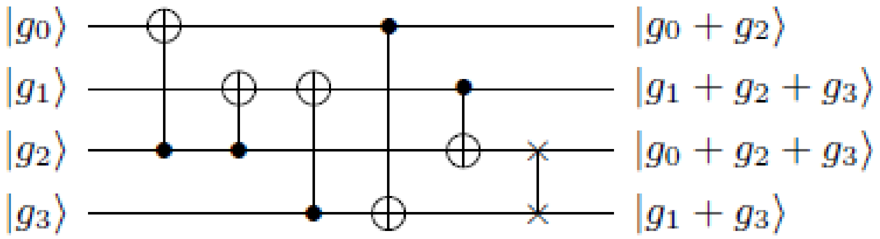



- $x^{1 \bmod n}$
- $m(x) = 1 + x^3 + x^{10}$
  $\rightarrow x^{10} = x^3 + 1$

Circuit 4: Binary shift circuit for $\mathbb{F}_{2^{10}}$ with $g_0 + \cdots + g_9 x^9$ as the input and $h_0 + \cdots + h_9 x^9 = g_9 + g_0 x + g_1 x^2 + (g_2 + g_9) x^3 + g_3 x^4 + \cdots + g_8 x^9$ as the output.

# Space Efficient Multiplication

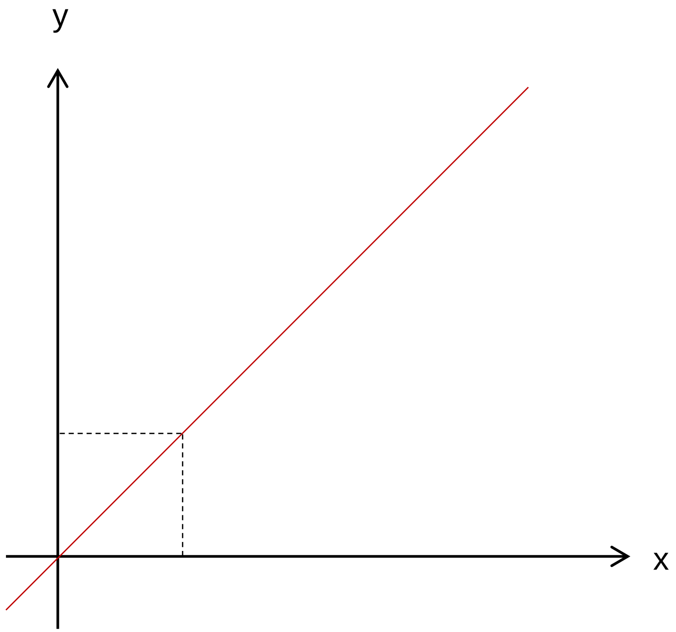
**Multiplication by a constant polynomial**



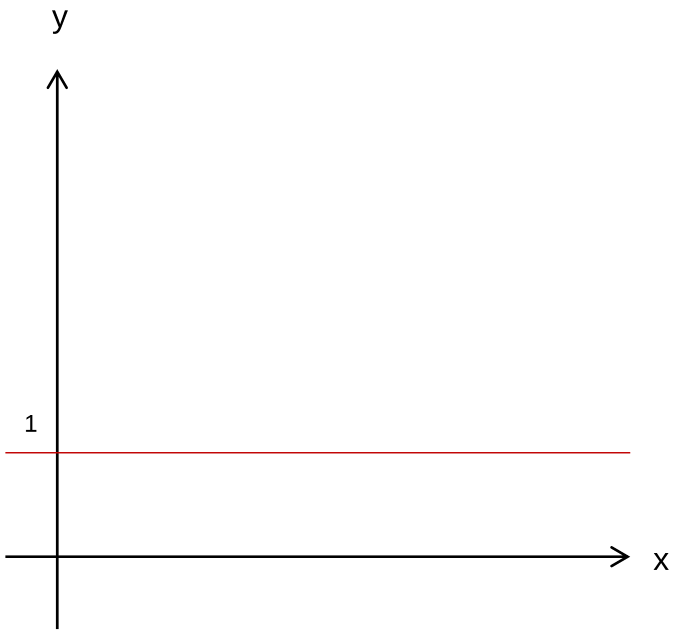

Circuit 5: Multiplication of $g$ by $1 + x^2$ modulo $1 + x + x^4$. Depth 4 and 5 CNOT gates.

# Space Efficient Multiplication

**Constant polynomial**



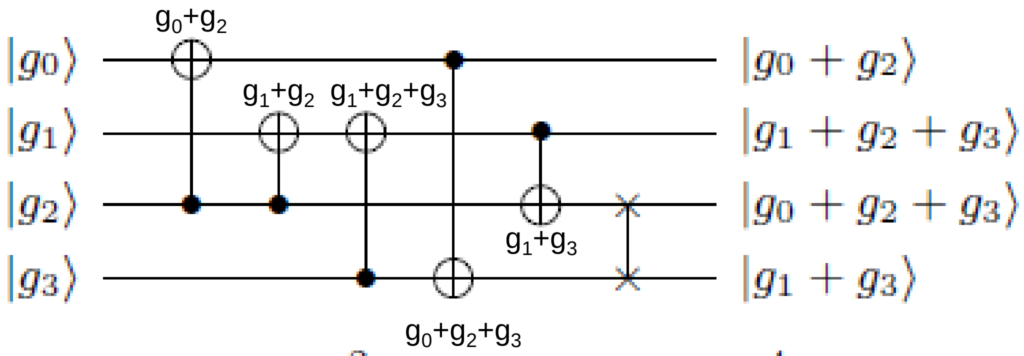

y = x
f(x) = x




f(x) = 1

# Space Efficient Multiplication

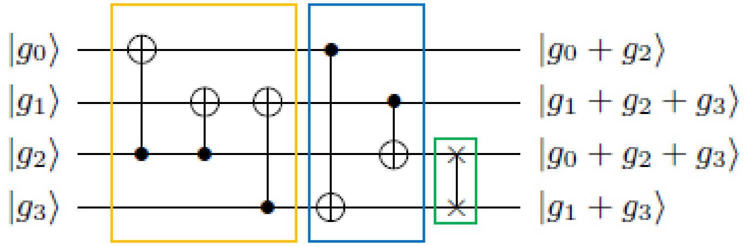
**Multiplication by a constant polynomial**




Circuit 5: Multiplication of $g$ by $1 + x^2$ modulo $1 + x + x^4$. Depth 4 and 5 CNOT gates.

# Space Efficient Multiplication

**Multiplication by a constant polynomial**




Circuit 5: Multiplication of $g$ by $1+x^2$ modulo $1+x+x^4$. Depth 4 and 5 CNOT gates.

$$\Gamma = \begin{pmatrix} 1&0&1&0\\ 0&1&1&1\\ 1&0&1&1\\ 0&1&0&1 \end{pmatrix} = P^{-1}LU = \boxed{\begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix}} \boxed{\begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&1&1&0\\ 1&0&0&1 \end{pmatrix}} \boxed{\begin{pmatrix} 1&0&1&0\\ 0&1&1&1\\ 0&0&1&0\\ 0&0&0&1 \end{pmatrix}}$$

# Space Efficient Multiplication

**LUP Decomposition**

$3x + 4y + 2z = 15$
$5x + 2y + 1z = 18$
$2x + 3y + 2z = 10$

$$L = \begin{pmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{pmatrix} \qquad U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{pmatrix}$$

1. $Ax = B$

2. $A = LU$
   $LUX = B$

3. $LY = B$
   where $UX = Y$

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

4. $UX = Y$

# Space Efficient Multiplication

**LUP Decomposition**

3x + 4y + 2z = 15
5x + 2y + 1z = 18
2x + 3y + 2z = 10

$$L = \begin{pmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{pmatrix} \qquad U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{pmatrix}$$

$\boxed{\text{1. Ax = B}}$

2. A = LU
LUX = B

3. LY = B
where UX = Y

$$Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

4. UX = Y

$$A = \begin{pmatrix} 3 & 4 & 2 \\ 5 & 2 & 1 \\ 2 & 3 & 2 \end{pmatrix} \qquad X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \qquad B = \begin{pmatrix} 15 \\ 18 \\ 10 \end{pmatrix}$$

# Space Efficient Multiplication

**LUP Decomposition**

3x + 4y + 2z = 15
5x + 2y + 1z = 18
2x + 3y + 2z = 10

$$L = \begin{pmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{pmatrix} \qquad U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{pmatrix}$$

1. Ax = B

2. A = LU
   LUX = B

3. LY = B
   where UX = Y $\quad Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$

4. UX = Y

$$A = \begin{pmatrix} 3 & 4 & 2 \\ 5 & 2 & 1 \\ 2 & 3 & 2 \end{pmatrix} \qquad X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \qquad B = \begin{pmatrix} 15 \\ 18 \\ 10 \end{pmatrix}$$

$$A = \begin{pmatrix} 3 & 4 & 2 \\ 5 & 2 & 1 \\ 2 & 3 & 2 \end{pmatrix} = LU = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ l_{21}u_{11} & l_{21}u_{12}+u_{22} & l_{21}u_{13}+u_{23} \\ l_{31}u_{11} & l_{31}u_{12}+l_{32}u_{22} & l_{31}u_{13}+l_{32}u_{23}+u_{33} \end{pmatrix}$$

# Space Efficient Multiplication

**LUP Decomposition**

3x + 4y + 2z = 15
5x + 2y + 1z = 18
2x + 3y + 2z = 10

$$L = \begin{pmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{pmatrix} \qquad U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{pmatrix}$$

1. Ax = B

2. A = LU
   LUX = B

3. LY = B
   where UX = Y  $Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$

4. UX = Y

$$A = \begin{pmatrix} 3 & 4 & 2 \\ 5 & 2 & 1 \\ 2 & 3 & 2 \end{pmatrix} \qquad X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \qquad B = \begin{pmatrix} 15 \\ 18 \\ 10 \end{pmatrix}$$

$$A = \begin{pmatrix} 3 & 4 & 2 \\ 5 & 2 & 1 \\ 2 & 3 & 2 \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ l_{21}u_{11} & l_{21}u_{12}+u_{22} & l_{21}u_{13}+u_{23} \\ l_{31}u_{11} & l_{31}u_{12}+l_{32}u_{22} & l_{31}u_{13}+l_{32}u_{23}+u_{33} \end{pmatrix}$$

$U_{11} = 3$, $U_{12} = 4$, $U_{13} = 2$
$l_{21} = 5/3$, $U_{22} = -14/3$, $U_{23} = -7/3$
$l_{31} = 2/3$, $l_{32} = -1/14$, $U_{33} = 1/2$

# Space Efficient Multiplication

**LUP Decomposition**

$3x + 4y + 2z = 15$
$5x + 2y + 1z = 18$
$2x + 3y + 2z = 10$

$$L = \begin{pmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{pmatrix} \qquad U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{pmatrix}$$

1. $Ax = B$
2. $A = LU$
   $LUX = B$
3. $LY = B$
   where $UX = Y$ $\quad Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$
4. $UX = Y$

$$A = \begin{pmatrix} 3 & 4 & 2 \\ 5 & 2 & 1 \\ 2 & 3 & 2 \end{pmatrix} \qquad X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \qquad B = \begin{pmatrix} 15 \\ 18 \\ 10 \end{pmatrix}$$

$U_{11} = 3$, $U_{12} = 4$, $U_{13} = 2$
$l_{21} = 5/3$, $U_{22} = -14/3$, $U_{23} = -7/3$
$l_{31} = 2/3$, $l_{32} = -1/14$, $U_{33} = 1/2$

$$\begin{pmatrix} 1 & 0 & 0 \\ 5/3 & 1 & 0 \\ 2/3 & -1/14 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 15 \\ 18 \\ 10 \end{pmatrix}$$

$y_1 = 15$, $y_2 = -7$, $y_3 = -1/2$

# Space Efficient Multiplication

**LUP Decomposition**

$3x + 4y + 2z = 15$
$5x + 2y + 1z = 18$
$2x + 3y + 2z = 10$

$$L = \begin{pmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{pmatrix} \qquad U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ 0 & u_{22} & u_{23} \\ 0 & 0 & u_{33} \end{pmatrix}$$

1. $Ax = B$

2. $A = LU$
   $LUX = B$

3. $LY = B$
   where $UX = Y$ $\quad Y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$

4. $\boxed{UX = Y}$

$U_{11} = 3,\ U_{12} = 4,\ U_{13} = 2$
$l_{21} = 5/3,\ U_{22} = -14/3,\ U_{23} = -7/3$
$l_{31} = 2/3,\ l_{32} = -1/14,\ U_{33} = 1/2$

$y_1 = 15,\ y_2 = -7,\ y_3 = -1/2$

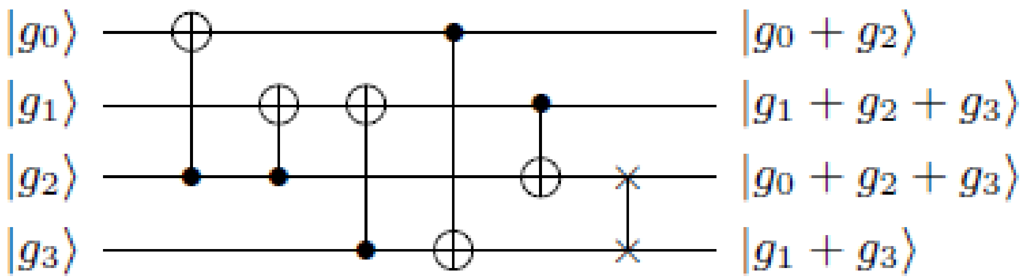
$$U = \begin{pmatrix} 3 & 4 & 2 \\ 0 & -14/3 & -7/3 \\ 0 & 0 & 1/2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 15 \\ -7 \\ -1/2 \end{pmatrix} \Rightarrow \begin{matrix} x_1 \\ x_2 \\ x_3 \end{matrix} = \begin{matrix} 3 \\ 2 \\ -1 \end{matrix}$$

# Space Efficient Multiplication

**Multiplication by a constant polynomial**

$1 + x + x^2 + x^3$ $\quad$ $1 + x^2$ $\quad$ $x + x^2$

1
1
1
1




0
1
1
0

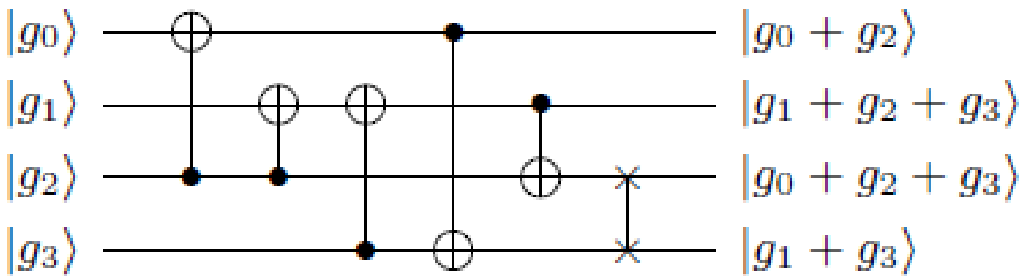
Circuit 5: Multiplication of $g$ by $1 + x^2$ modulo $1 + x + x^4$. Depth 4 and 5 CNOT gates.

# Space Efficient Multiplication

**Multiplication by a constant polynomial**

$1 + x + x^2 + x^3$ $\quad$ $1 + x^3$ $\quad$ $x + x^2 + x^3$

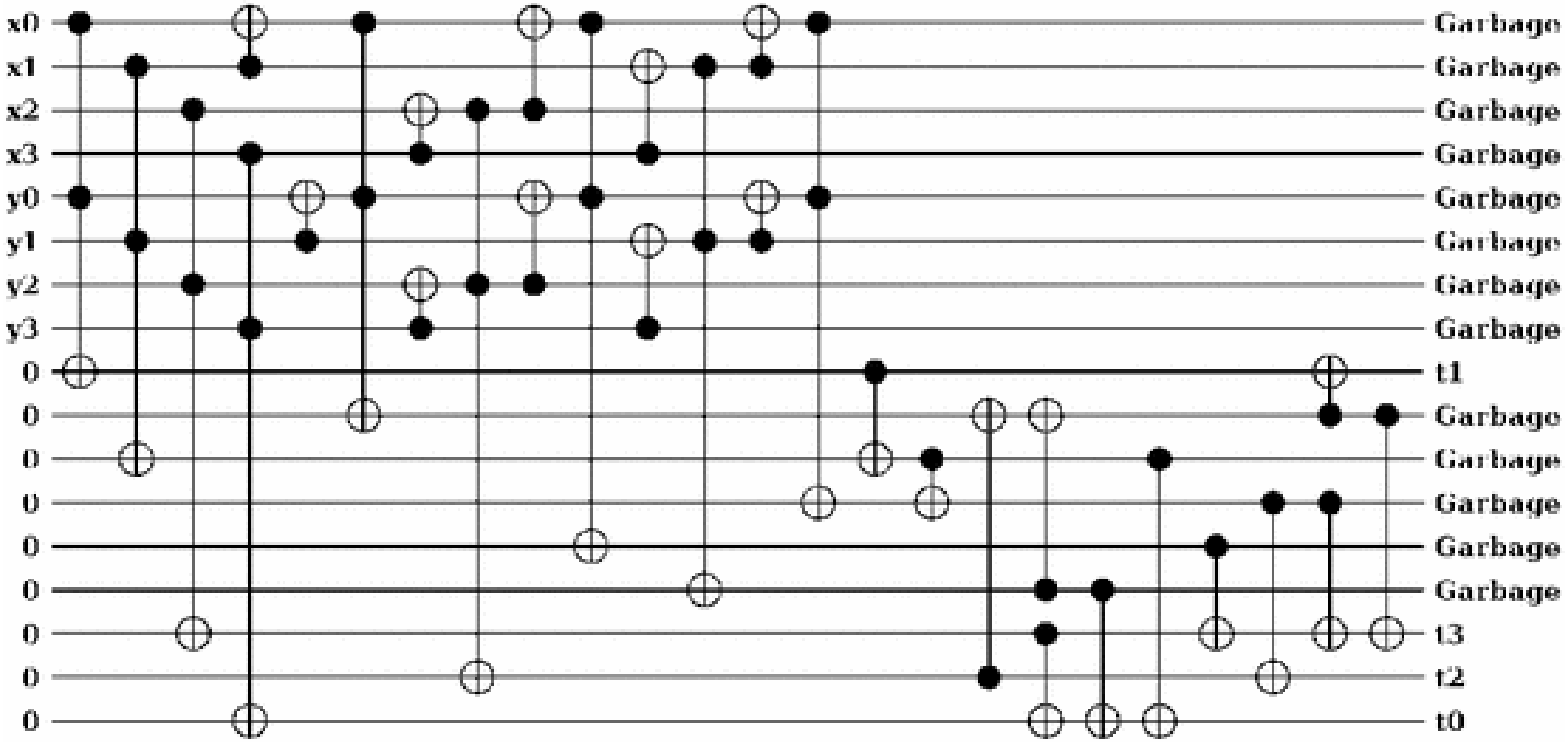
1
1
1
1




0
1
1
1

Circuit 5: Multiplication of $g$ by $1 + x^2$ modulo $1 + x + x^4$. Depth 4 and 5 CNOT gates.

# Space Efficient Multiplication



# Q & A