양자 게이트 설계 및 구현

장경배

https://youtu.be/8wF3-PWciUo

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Karatsuba Multiplication in Binary

- Size 가 n인 두개의 input 다항식 f(x), g(x) 그리고 output h(x) 에 대해서 아래와 같이 쪼갤 수 있음

$$f = f_0 + f_1 x^k,\ g = g_0 + g_1 x^k \quad \text{, 이때} \quad \frac{n}{2} \leq k < n$$

$$h = h_0 + h_1 x^k + h_2 x^{2k} + h_3 x^{3k}$$

- output을 위한 $\alpha,\ \beta, \gamma$ 를 계산해 준다.

$$\alpha = f_0 \cdot g_0,\ \beta = f_1 \cdot g_1 \text{ and } \gamma = (f_0 + f_1) \cdot (g_0 + g_1)$$

- 마지막으로 카라추바 곱을 수행해주면 완료

$$h + f \cdot g = h + \alpha + (\gamma + \alpha + \beta)x^k + \beta x^{2k}$$

Karatsuba - Wiki

$$x = x_1 B^m + x_0$$

$$y = y_1 B^m + y_0$$

(단, x_0과 y_0는 B^m보다 작다.)

$$z_2 = x_1 y_1$$

$$z_1 = x_1 y_0 + x_0 y_1$$

$$z_0 = x_0 y_0$$

라고 할 때, x와 y의 곱은

$$xy = (x_1 B^m + x_0)(y_1 B^m + y_0)$$

$$= z_2 B^{2m} + z_1 B^m + z_0$$

4번의 곱셈이 아닌, 덧셈 몇번으로 3번의 곱셈을 하는 분할 알고리즘

Karatsuba Multiplication in Binary

$$h + f \cdot g = h + \alpha + (\gamma + \alpha + \beta)x^k + \beta x^{2k}$$

- 결과가 Overlap 되는 것을 막기위해, $\alpha,\ \beta, \gamma$ 도 f(x), g(x) 를 나눈 방식과 동일하게 나눠 줌

$$h+f\cdot g = (h_0+\alpha_0)+(h_1+\alpha_0+\alpha_1+\beta_0+\gamma_0)x^k+(h_2+\alpha_1+\beta_0+\beta_1+\gamma_1)x^{2k}+(h_3+\beta_1)x^{3k}$$

$$f = f_0 + f_1 x^k,\ g = g_0 + g_1 x^k$$

Karatsuba Multiplication in Binary

3.1 Parameter set `kem/mceliece348864`

KEM with $m = 12$, $n = 3488$, $t = 64$, $\ell = 256$. Field polynomial $f(z) = z^{12} + z^3 + 1$. Hash function: SHAKE256 with 32-byte output. This parameter set is **proposed and implemented** in this submission.

f(x), g(x) 가 의 n = 12, 따라서 k = 6

$$\alpha = f_0 \cdot g_0,\ \beta = f_1 \cdot g_1 \text{ and } \gamma = (f_0 + f_1) \cdot (g_0 + g_1)$$

α_0

α_1

```
   1 1 1
   1 1 1
 -------
   1 1 1
 1 1 1
1 1 1
= 1 0 1 0 1   →  (2*n – 1)
```

$$h + f \cdot g = (h_0 + \alpha_0) + (h_1 + \alpha_0 + \alpha_1 + \beta_0 + \gamma_0)x^k + (h_2 + \alpha_1 + \beta_0 + \beta_1 + \gamma_1)x^{2k} + (h_3 + \beta_1)x^{3k}$$

6 6 6 5

3.9 Parameter set `kem/mceliece8192128`

KEM with $m = 13$, $n = 8192$, $t = 128$, $\ell = 256$. Field polynomial $f(z) = z^{13} + z^4 + z^3 + z + 1$. Hash function: SHAKE256 with 32-byte output. This parameter set is **proposed and implemented** in this submission.

f(x), g(x) 가 의 n = 13, 따라서 k = 7

$$\alpha = f_0 \cdot g_0,\ \beta = f_1 \cdot g_1 \text{ and } \gamma = (f_0 + f_1) \cdot (g_0 + g_1)$$

α_0

α_1

$$h + f \cdot g = (h_0 + \alpha_0) + (h_1 + \alpha_0 + \alpha_1 + \beta_0 + \gamma_0)x^k + (h_2 + \alpha_1 + \beta_0 + \beta_1 + \gamma_1)x^{2k} + (h_3 + \beta_1)x^{3k}$$

7 7 6 5

3.9 Parameter set `kem/mceliece8192128`

KEM with $m = 13$, $n = 8192$, $t = 128$, $\ell = 256$. Field polynomial $f(z) = z^{13} + z^4 + z^3 + z + 1$. Hash function: SHAKE256 with 32-byte output. This parameter set is **proposed and implemented** in this submission.

f(x), g(x) 가 의 n = 13 인데 14로 생각, 따라서 k = 7

$$\alpha = f_0 \cdot g_0,\ \beta = f_1 \cdot g_1 \text{ and } \gamma = (f_0 + f_1) \cdot (g_0 + g_1)$$

α_0 β_0
α_1 β_1

$$h + f \cdot g = (h_0 + \alpha_0) + (h_1 + \alpha_0 + \alpha_1 + \beta_0 + \gamma_0)x^k + (h_2 + \alpha_1 + \beta_0 + \beta_1 + \gamma_1)x^{2k} + (h_3 + \beta_1)x^{3k}$$

7 7 7 4

```
Toffoli | (a0, b0, c0)

Toffoli | (a1, b0, c1)
Toffoli | (a0, b1, c1)

Toffoli | (a2, b0, c2)
Toffoli | (a1, b1, c2)
Toffoli | (a0, b2, c2)

Toffoli | (a3, b0, c3)
Toffoli | (a2, b1, c3)
Toffoli | (a1, b2, c3)
Toffoli | (a0, b3, c3)

Toffoli | (a4, b0, c4)
Toffoli | (a3, b1, c4)
Toffoli | (a2, b2, c4)
Toffoli | (a1, b3, c4)
Toffoli | (a0, b4, c4)

Toffoli | (a5, b0, c5)
Toffoli | (a4, b1, c5)
Toffoli | (a3, b2, c5)
Toffoli | (a2, b3, c5)
Toffoli | (a1, b4, c5)
Toffoli | (a0, b5, c5)

Toffoli | (a6, b0, c6)
Toffoli | (a5, b1, c6)
Toffoli | (a4, b2, c6)
Toffoli | (a3, b3, c6)
Toffoli | (a2, b4, c6)
Toffoli | (a1, b5, c6)
Toffoli | (a0, b6, c6)  # a0
```

a0 = 1 1 1 1 1 1 1

b0 = 1 1 1 1 1 1 1

```
Toffoli | (a6, b1, c7)  # a1
Toffoli | (a5, b2, c7)
Toffoli | (a4, b3, c7)
Toffoli | (a3, b4, c7)
Toffoli | (a2, b5, c7)
Toffoli | (a1, b6, c7)

Toffoli | (a6, b2, c8)
Toffoli | (a5, b3, c8)
Toffoli | (a4, b4, c8)
Toffoli | (a3, b5, c8)
Toffoli | (a2, b6, c8)

Toffoli | (a6, b3, c9)
Toffoli | (a5, b4, c9)
Toffoli | (a4, b5, c9)
Toffoli | (a3, b6, c9)

Toffoli | (a6, b4, c10)
Toffoli | (a5, b5, c10)
Toffoli | (a4, b6, c10)

Toffoli | (a6, b5, c11)
Toffoli | (a5, b6, c11)

Toffoli | (a6, b6, c12)
```

```
Toffoli | (a7, b7, c7)

Toffoli | (a8, b7, c8)
Toffoli | (a7, b8, c8)

Toffoli | (a9, b7, c9)
Toffoli | (a8, b8, c9)
Toffoli | (a7, b9, c9)

Toffoli | (a10, b7, c10)
Toffoli | (a9, b8, c10)
Toffoli | (a8, b9, c10)
Toffoli | (a7, b10, c10)

Toffoli | (a11, b7, c11)
Toffoli | (a10, b8, c11)
Toffoli | (a9, b9, c11)
Toffoli | (a8, b10, c11)
Toffoli | (a7, b11, c11)

Toffoli | (a12, b7, c12)
Toffoli | (a11, b8, c12)
Toffoli | (a10, b9, c12)
Toffoli | (a9, b10, c12)
Toffoli | (a8, b11, c12)
Toffoli | (a7, b12, c12)

Toffoli | (a12, b8, c13)
Toffoli | (a11, b9, c13)
Toffoli | (a10, b10, c13)
Toffoli | (a9, b11, c13)
Toffoli | (a8, b12, c13)  # b0 + a1
```

a1 = 0 1 1 1 1 1 1
b1 = 0 1 1 1 1 1 1

```
Toffoli | (a12, b9, c21)  # b1
Toffoli | (a11, b10, c21)
Toffoli | (a10, b11, c21)
Toffoli | (a9, b12, c21)

Toffoli | (a12, b10, c22)
Toffoli | (a11, b11, c22)
Toffoli | (a10, b12, c22)

Toffoli | (a12, b11, c23)
Toffoli | (a11, b12, c23)

Toffoli | (a12, b12, c24)
```

$$(h_0+\alpha_0)+(h_1+\alpha_0+\alpha_1+\beta_0+\gamma_0)x^k+(h_2+\alpha_1+\beta_0+\beta_1+\gamma_1)x^{2k}+(h_3+\beta_1)x^{3k}$$

```
##COPY
CNOT | (c7, c14) # a1 + b0 -> part 3
CNOT | (c8, c15)
CNOT | (c9, c16)
CNOT | (c10, c17)
CNOT | (c11, c18)
CNOT | (c12, c19)
CNOT | (c13, c20)

CNOT | (c0, c7) # a1 + b0 + a0 -> part 2
CNOT | (c1, c8)
CNOT | (c2, c9)
CNOT | (c3, c10)
CNOT | (c4, c11)
CNOT | (c5, c12)
CNOT | (c6, c13)

CNOT | (c21, c14) # a1 + b0 + b1 -> part 3
CNOT | (c22, c15)
CNOT | (c23, c16)
CNOT | (c24, c17)
```

$$(h_0+\alpha_0)+(h_1+\alpha_0+\alpha_1+\beta_0+\gamma_0)x^k+(h_2+\alpha_1+\beta_0+\beta_1+\gamma_1)x^{2k}+(h_3+\beta_1)x^{3k}$$

```
# Multiplication Middle
CNOT | (a7, a0)
CNOT | (a8, a1)
CNOT | (a9, a2)
CNOT | (a10, a3)
CNOT | (a11, a4)
CNOT | (a12, a5)

CNOT | (b7, b0)
CNOT | (b8, b1)
CNOT | (b9, b2)
CNOT | (b10, b3)
CNOT | (b11, b4)
CNOT | (b12, b5)
```

$$\gamma = (f_0 + f_1) \cdot (g_0 + g_1)$$

$$(h_0+\alpha_0)+(h_1+\alpha_0+\alpha_1+\beta_0+\gamma_0)x^k+(h_2+\alpha_1+\beta_0+\beta_1+\gamma_1)x^{2k}+(h_3+\beta_1)x^{3k}$$

```
Toffoli | (a0, b0, c7)

Toffoli | (a1, b0, c8)
Toffoli | (a0, b1, c8)

Toffoli | (a2, b0, c9)
Toffoli | (a1, b1, c9)
Toffoli | (a0, b2, c9)

Toffoli | (a3, b0, c10)
Toffoli | (a2, b1, c10)
Toffoli | (a1, b2, c10)
Toffoli | (a0, b3, c10)

Toffoli | (a4, b0, c11)
Toffoli | (a3, b1, c11)
Toffoli | (a2, b2, c11)
Toffoli | (a1, b3, c11)
Toffoli | (a0, b4, c11)

Toffoli | (a5, b0, c12)
Toffoli | (a4, b1, c12)
Toffoli | (a3, b2, c12)
Toffoli | (a2, b3, c12)
Toffoli | (a1, b4, c12)
Toffoli | (a0, b5, c12)

Toffoli | (a6, b0, c13)
Toffoli | (a5, b1, c13)
Toffoli | (a4, b2, c13)
Toffoli | (a3, b3, c13)
Toffoli | (a2, b4, c13)
Toffoli | (a1, b5, c13)
Toffoli | (a0, b6, c13) #r0 (size 7)
```

```
Toffoli | (a6, b1, c14) #r1 (size 6)
Toffoli | (a5, b2, c14)
Toffoli | (a4, b3, c14)
Toffoli | (a3, b4, c14)
Toffoli | (a2, b5, c14)
Toffoli | (a1, b6, c14)

Toffoli | (a6, b2, c15)
Toffoli | (a5, b3, c15)
Toffoli | (a4, b4, c15)
Toffoli | (a3, b5, c15)
Toffoli | (a2, b6, c15)

Toffoli | (a6, b3, c16)
Toffoli | (a5, b4, c16)
Toffoli | (a4, b5, c16)
Toffoli | (a3, b6, c16)

Toffoli | (a6, b4, c17)
Toffoli | (a5, b5, c17)
Toffoli | (a4, b6, c17)

Toffoli | (a6, b5, c18)
Toffoli | (a5, b6, c18)

Toffoli | (a6, b6, c19)
```

$$(h_0+\alpha_0)+(h_1+\alpha_0+\alpha_1+\beta_0+\gamma_0)x^k+(h_2+\alpha_1+\beta_0+\beta_1+\gamma_1)x^{2k}+(h_3+\beta_1)x^{3k}$$

```
# Reversible
CNOT | (a7, a0)
CNOT | (a8, a1)
CNOT | (a9, a2)
CNOT | (a10, a3)
CNOT | (a11, a4)
CNOT | (a12, a5)

CNOT | (b7, b0)
CNOT | (b8, b1)
CNOT | (b9, b2)
CNOT | (b10, b3)
CNOT | (b11, b4)
CNOT | (b12, b5)
```

Modular Reduction

$$f(z) = z^{13} + z^4 + z^3 + z + 1$$

$$z^{13} = z^4 + z^3 + z + 1$$

c24 c13 c4 c3 c1 c0

```
# REDUCTION(여기 부터하면됨)
CNOT | (c13, c0)
CNOT | (c14, c1)
CNOT | (c15, c2)
CNOT | (c16, c3)
CNOT | (c17, c4)
CNOT | (c18, c5)
CNOT | (c19, c6)
CNOT | (c20, c7)
CNOT | (c21, c8)
CNOT | (c22, c9)
CNOT | (c23, c10)
CNOT | (c24, c11)
```

```
CNOT | (c13, c1)
CNOT | (c14, c2)
CNOT | (c15, c3)
CNOT | (c16, c4)
CNOT | (c17, c5)
CNOT | (c18, c6)
CNOT | (c19, c7)
CNOT | (c20, c8)
CNOT | (c21, c9)
CNOT | (c22, c10)
CNOT | (c23, c11)
CNOT | (c24, c12)
```

```
CNOT | (c13, c3)
CNOT | (c14, c4)
CNOT | (c15, c5)
CNOT | (c16, c6)
CNOT | (c17, c7)
CNOT | (c18, c8)
CNOT | (c19, c9)
CNOT | (c20, c10)
CNOT | (c21, c11)
CNOT | (c22, c12)
```

```
CNOT | (c13, c4)
CNOT | (c14, c5)
CNOT | (c15, c6)
CNOT | (c16, c7)
CNOT | (c17, c8)
CNOT | (c18, c9)
CNOT | (c19, c10)
CNOT | (c20, c11)
CNOT | (c21, c12)
```

```
CNOT | (c23, c0)
CNOT | (c24, c1)
CNOT | (c22, c0)
CNOT | (c23, c1)
CNOT | (c24, c2)
```

```
CNOT | (c23, c1)
CNOT | (c24, c2)
CNOT | (c22, c1)
CNOT | (c23, c2)
CNOT | (c24, c3)
```

```
CNOT | (c23, c3)
CNOT | (c24, c4)
CNOT | (c22, c3)
CNOT | (c23, c4)
CNOT | (c24, c5)
```

```
CNOT | (c23, c4)
CNOT | (c24, c5)
CNOT | (c22, c4)
CNOT | (c23, c5)
CNOT | (c24, c6)
```

Test vector

```c
#include <stdio.h>

void CNOT(int a, int *b);
void Toffoli(int a, int b, int *c);
int main(){

    int a[13] = {0,1,1,1,0,1,1,1,1,1,1,1,1}; //0x1fee
    int b[13] = {0,1,1,1,0,1,1,1,1,1,1,1,1}; //0x1fee
    int c[25] = {0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0};
```

Quantum Gate

```c
    for (int i=12;i>=0;i--)
      printf("%d ",c[i]);;
```

Result

```
1 0 1 0 0 0 0 0 1 1 0 1 1 Program ended with exit code: 0
```

Q & A