Hybrid Karatsuba Multiplication

20.04.19

https://youtu.be/AOscc-hPd4Q

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Karatsuba

3 List of parameter sets (part of 2.B.1)

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.

3.4 Parameter set `kem/mceliece460896f`

KEM with $m = 13$, $n = 4608$, $t = 96$, $\ell = 256$. Field polynomial $f(z) = z^{13} + z^4 + z^3 + z + 1$. Hash function: SHAKE256 with 32-byte output. Extra parameters $(\mu, \nu) = (32, 64)$. This parameter set is **implemented** in this submission as a **possible future proposal**.

Karatsuba

Algo. \ Param.	n	m	d	r	P	P_m	Security level (bits)
ROLLO-I-128	47	79	6	5	$X^{47}+X^5+1$	$X^{79}+X^9+1$	128
ROLLO-I-192	53	89	7	6	$X^{53}+X^6+X^2+X+1$	$X^{89}+X^{38}+1$	192
ROLLO-I-256	67	113	8	7	$X^{67}+X^5+X^2+X+1$	$X^{113}+X^9+1$	256

Table 3. ROLLO-I parameters for each security level

Instance	P	Π
RQC-I	$X^{67}+X^5+X^2+X+1$	$X^{97}+X^6+1$
RQC-II	$X^{101}+X^7+X^6+X+1$	$X^{107}+X^9+X^7+X^4+1$
RQC-III	$X^{131}+X^8+X^3+X^2+1$	$X^{137}+X^{21}+1$

Table 2: Polynomials considered for RQC. P is the polynomial used to define $\mathbb{F}_{q^m}^n$ as $\mathbb{F}_{q^m}[X]/\langle P\rangle$ and Π is the polynomial used to define $\mathbb{F}_{q^m}$ as $\mathbb{F}_q[X]/\langle\Pi\rangle$.

Karatsuba 2-way

$$(h_0+a_0) + (h_1+a_0+a_1+b_0+r_0)x^k + (h_2+a_1+b_0+b_1+r_1)x^{2k} + (h_3+b_1)x^{3k}$$

a_0	a_0	a_1	b_1
	a_1	b_0	
	b_0	b_1	
	r_0	r_1	

a[i]	f_0	f_1
b[i]	g_1	g_1
	alpah	beta

$$r = (f_0 + f_1) * (g_0 + g_1)$$

Karatsuba 3-way

$$A(x) \cdot B(x) =$$

$$(A_1 + A_2) \cdot (B_1 + B_2)x^{3s} \qquad r_c$$

$$+ (A_2 + A_0) \cdot (B_2 + B_0)x^{2s} \qquad r_b$$

$$+ (A_1 + A_0) \cdot (B_1 + B_0)x^{s} \qquad r_a$$

$$+ (A_2 \cdot B_2 x^{2s} + A_1 \cdot B_1 x^{s} + A_0 \cdot B_0) \cdot (x^{2s} + x^{s} + 1)$$

Karatsuba 3-way

0	k	2k	3k	4k	5k
a	b	c			
	a	b	c		
		a	b	c	
	r_a	r_b	r_c		

Karatsuba 2-bit

0 k 2k

a_0 a_1 b_1

b_0

r

$r = (f_0 + f_1) * (g_0 + g_1)$

f_1 f_0

a = 1 0

b = 1 0

g_1 g_0

beta alpha

10

10

100

$r = (1 + 0) * (1 + 0) = 1$

0 k 2k

0 0 1

1

1

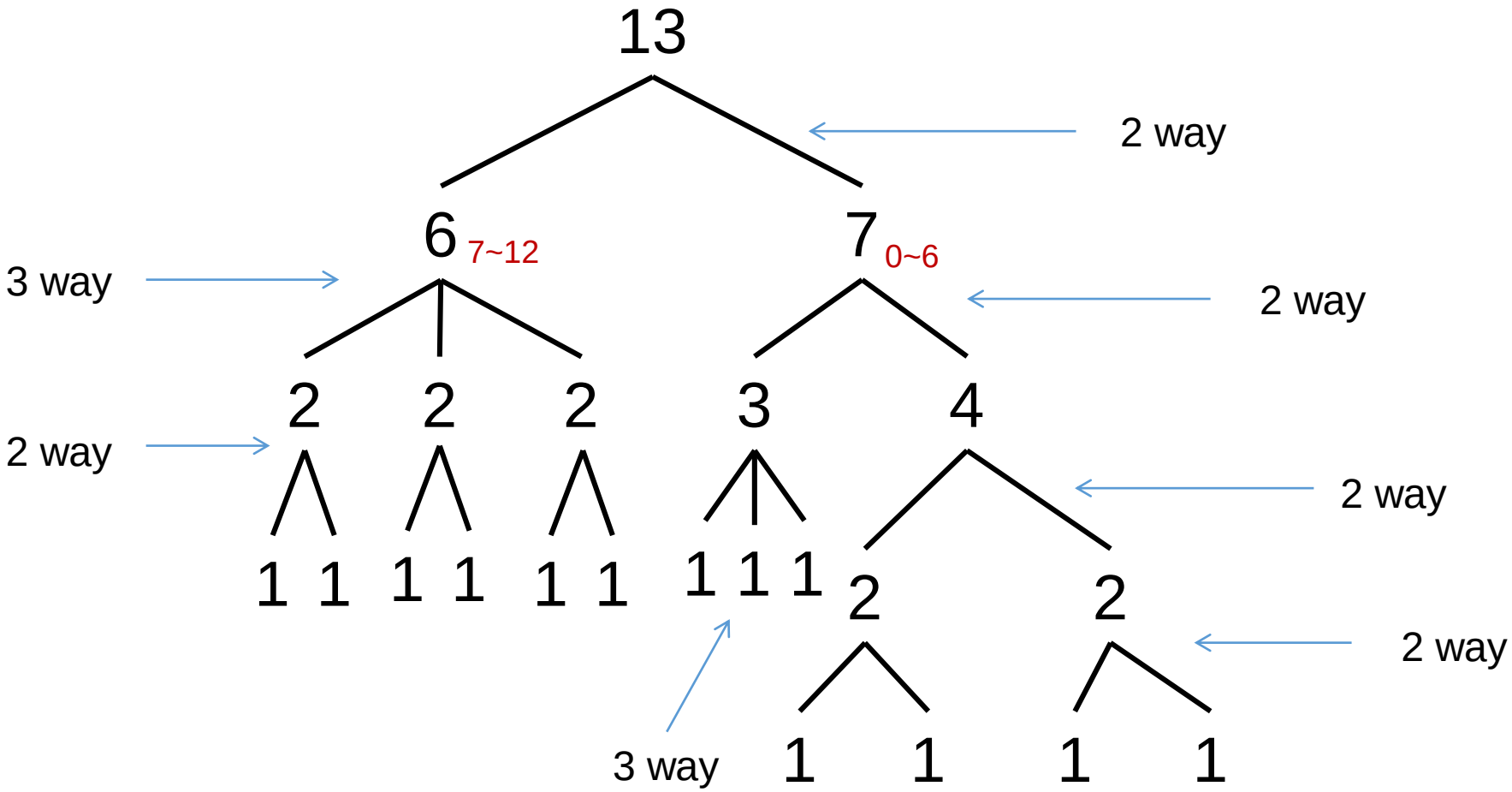
$r = (1 + 0) * (1 + 0) = 1$

Karatsuba 2-way & 3-way

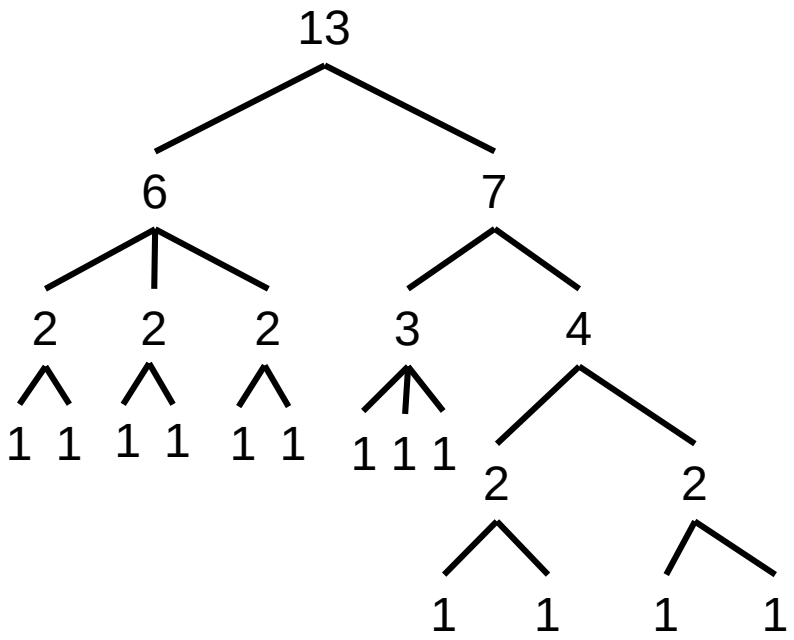
0	k	2k	3k
a_0	a_0	a_1	b_1
	a_1	b_0	
	b_0	b_1	
	r_0	r_1	

0	k	2k	3k	4k	5k
a	b	c			
	a	b	c		
		a	b	c	
	r_a	r_b	r_c		

Hybrid Karatsuba on 13



Hybrid Karatsuba on 13



2 way

a_0 a_1 b_1

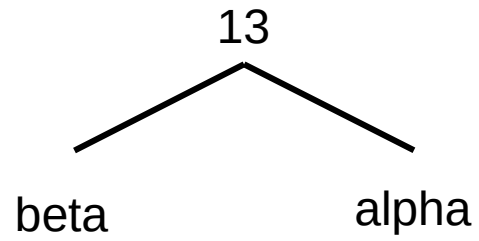
b_0

3 way

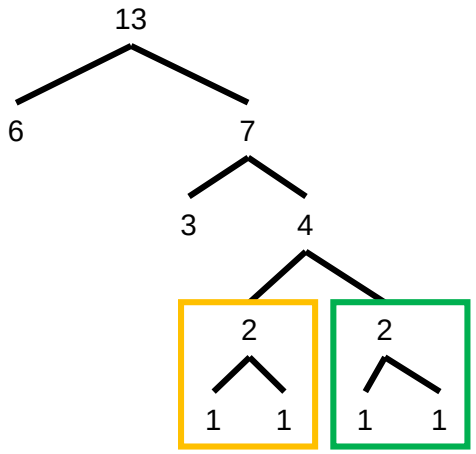
a

b

c



Hybrid Karatsuba on 13



13	$C_{0\sim6}$	$C_{7\sim13}$	$C_{14\sim20}$	$C_{21\sim24}$	
13 x 2 - 1 → 25	a0	a1			
13 / 2 = 6.5 → 7		b0		b1	

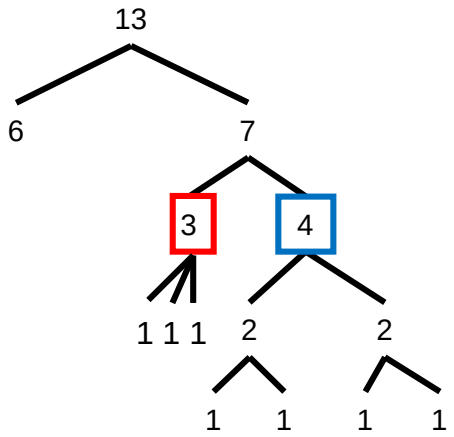
7	$C_{0\sim3}$	$C_{4\sim7}$	$C_{8\sim11}$	C_{12}	← 13의 a_0 a_1
7 x 2 - 1 → 13	a0	a1			
7 / 2 = 3.5 → 4		b0		b1	

4	$C_{0\sim1}$	$C_{2\sim3}$	$C_{4\sim5}$	C_6	← 7의 a_0 a_1
4 x 2 - 1 → 7	a0	a1			
4 / 2 = 2		b0		b1	

2	C_0	C_1	C_2
2 x 2 - 1 → 3	a0	a1	
2 / 2 = 1		b0	b1

2	C_2	C_3	C_6
2 x 2 - 1 → 3	a0	a1	
2 / 2 = 1		b0	b1

Hybrid Karatsuba on 13



13

13 x 2 - 1 → 25

13 / 2 = 6.5 → 7

$C_{0\sim6}$ a0 | $C_{7\sim13}$ a1 b0 | $C_{14\sim20}$ | $C_{21\sim24}$ b1

7

7 x 2 - 1 → 13

7 / 2 = 3.5 → 4

$C_{0\sim3}$ a0 | $C_{4\sim7}$ a1 b0 | $C_{8\sim11}$ | C_{12} b1 ← 13의 a_0 a_1

4

4 x 2 - 1 → 7

4 / 2 = 2

$C_{0\sim1}$ a0 | $C_{2\sim3}$ a1 b0 | $C_{4\sim5}$ | C_{6} b1 ← **7의 a_0 a_1**

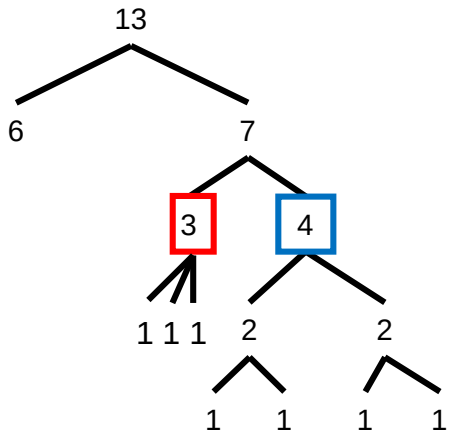
3

3 x 2 - 1 → 5

3 / 2 = 1.5 → 2

C_4 | C_5 A | C_6 | C_7 B | C_{12} C ← **7의 b_0 b_1**

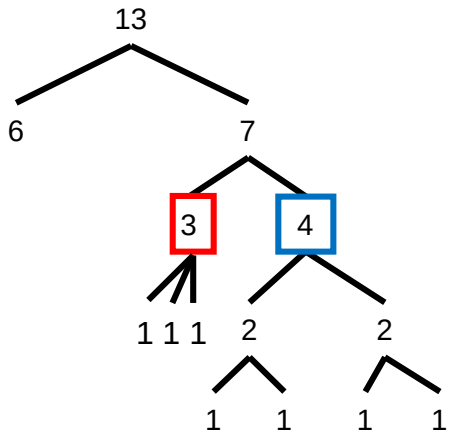
Hybrid Karatsuba on 13

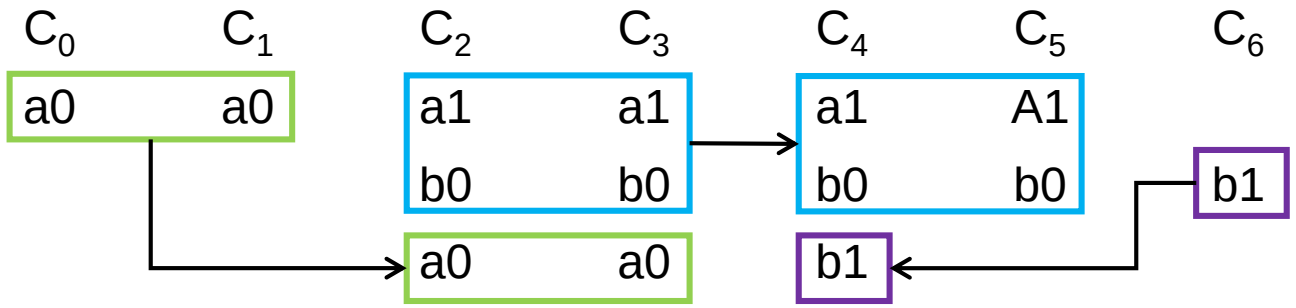


C_0	C_1	C_2	C_3	C_4	C_5	C_6
a0	a0	a1	a1			
		b0	b0			b1

C_4	C_5	C_6	C_7	C_{12}
	A			
			B	
				C

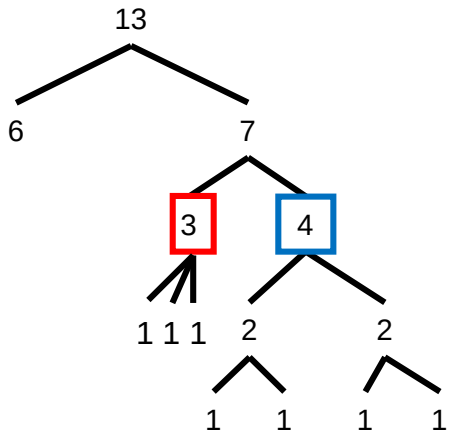
Hybrid Karatsuba on 13





C_4	C_5	C_6	C_7	C_{12}
A	B	C		
	A	B	C	
		A	**B**	**C**

Hybrid Karatsuba on 13



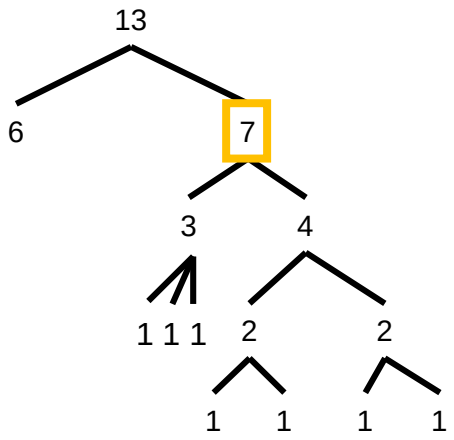
C_0	C_1	C_2	C_3
a0	a0	a1	a1
		b0	b0
		a0	a0

C_4	C_5	C_6
a1	A1	
b0	b0	b1
b1		

C_4	C_5	C_6	C_7	C_{12}
A	B	C		
	A	B	C	
		A	B	C

https://www.youtube.com/watch?v=m9VMjSfl3mA 12:40 → 순서 설명

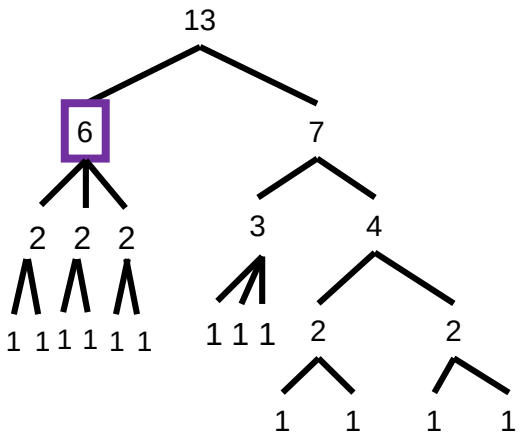
Hybrid Karatsuba on 13



13	$C_{0\sim6}$	$C_{7\sim13}$	$C_{14\sim20}$	$C_{21\sim24}$	
13 x 2 - 1 → 25	a0	a1			
13 / 2 = 6.5 → 7		b0		b1	

7	$C_{0\sim3}$	$C_{4\sim7}$	$C_{8\sim11}$	C_{12}	
7 x 2 - 1 → 13	a0	a1			← 13의 a_0 a_1
7 / 2 = 3.5 → 4		b0		b1	

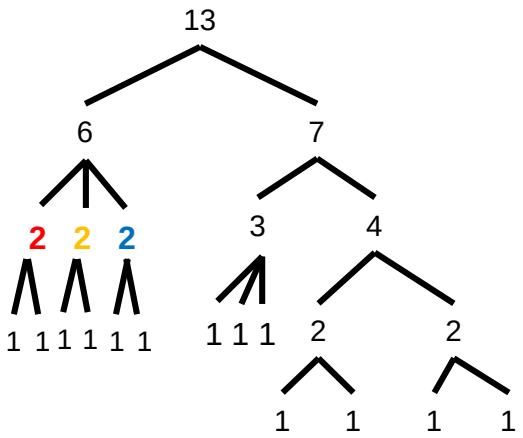
Hybrid Karatsuba on 13



13	$C_{0\sim6}$	$C_{7\sim13}$	$C_{14\sim20}$	$C_{21\sim24}$	
13 x 2 - 1 → 25	a0	a1			
13 / 2 = 6.5 → 7		b0		b1	

7	$C_{0\sim3}$	$C_{4\sim7}$	$C_{8\sim11}$	C_{12}	← 13의 a_0 a_1
7 x 2 - 1 → 13	a0	a1			
7 / 2 = 3.5 → 4		b0		b1	

Hybrid Karatsuba on 13



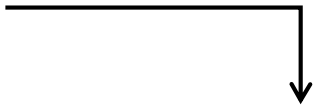
13	$C_{0\sim6}$	$C_{7\sim13}$	$C_{14\sim20}$	$C_{21\sim24}$
13 x 2 - 1 → 25	a0	a1		
13 / 2 = 6.5 → 7		b0		b1

7	$C_{0\sim3}$	$C_{4\sim7}$	$C_{8\sim11}$	C_{12}
7 x 2 - 1 → 13	a0	a1		
7 / 2 = 3.5 → 4		b0		b1

← 13의 a_0 a_1

6	$C_{7\sim8}$	$C_{9\sim10}$	$C_{11\sim12}$	$C_{13,21}$	$C_{22,23}$	C_{24}
6 x 2 - 1 → 11		a		a1		
6 / 2 = 3				b0	B1	
					c0	c1

a[i]
b[i]

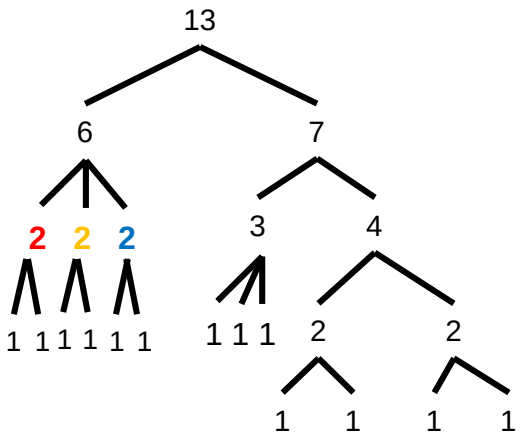


2	C_9	C_{10}	C_{13}
	a0	a1	
		b0	b1

2	C_{13}	C_{21}	C_{22}
	a0	a1	
		b0	b1

2	C_9	C_{10}	C_{13}
	a0	a1	
		b0	b1

Hybrid Karatsuba on 13



13	$C_{0\sim6}$	$C_{7\sim13}$	$C_{14\sim20}$	$C_{21\sim24}$
13 x 2 - 1 → 25	a0	a1		
13 / 2 = 6.5 → 7		b0		b1

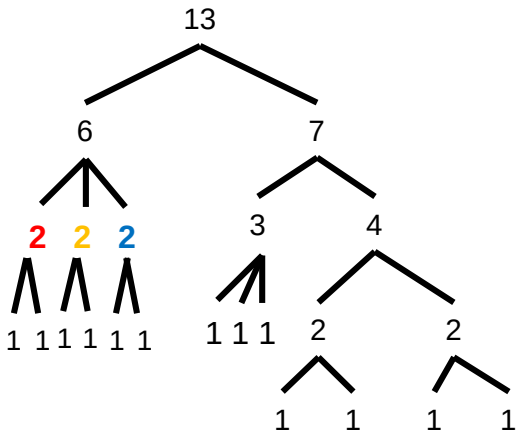
7	$C_{0\sim3}$	$C_{4\sim7}$	$C_{8\sim11}$	C_{12}	← 13의 a_0 a_1
7 x 2 - 1 → 13	a0	a1			
7 / 2 = 3.5 → 4		b0		b1	

6	$C_{7\sim8}$	$C_{9\sim10}$	$C_{11\sim12}$	$C_{13,21}$	$C_{22,23}$	C_{24}
6 x 2 - 1 → 11		a		a1		
6 / 2 = 3				b0	B1	
					c0	c1

C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{21}	C_{22}	C_{23}	C_{24}
		a0	a0			a1				
						b0	b0	b1		
								c0	c0	c1

https://www.youtube.com/watch?v=m9VMjSfl3mA 16:40 → 순서 설명

Hybrid Karatsuba on 13

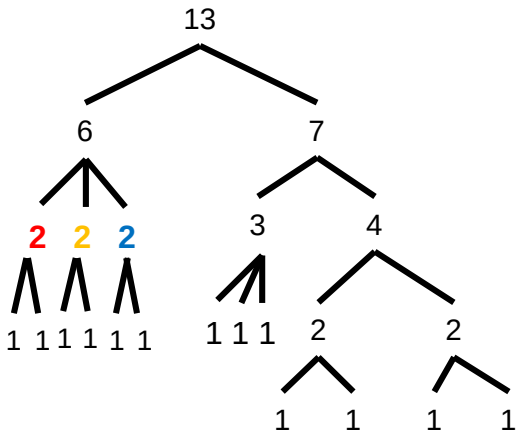


13	$C_{0\sim6}$	$C_{7\sim13}$	$C_{14\sim20}$	$C_{21\sim24}$
13 x 2 - 1 → 25	a0	a1		
13 / 2 = 6.5 → 7		b0		b1

7	$C_{0\sim3}$	$C_{4\sim7}$	$C_{8\sim11}$	C_{12}
7 x 2 - 1 → 13	a0	a1		
7 / 2 = 3.5 → 4		b0		b1

6	$C_{7\sim8}$	$C_{9\sim10}$	$C_{11\sim12}$	$C_{13,21}$	$C_{22,23}$	C_{24}
6 x 2 - 1 → 11		a0		a1		
6 / 2 = 3				b0	b1	
					c0	c1

Hybrid Karatsuba on 13



13

13 x 2 - 1 → 25

13 / 2 = 6.5 → 7

COPY

$C_{0\sim6}$	$C_{7\sim13}$	$C_{14\sim20}$	$C_{21\sim24}$
a0	a1		
	b0		b1
a_0	a_0	a_1	b_1
	a_1	b_0	
	b_0	b_1	
	r_0	r_1	

Hybrid Karatsuba

```
1 0 0 1 0 0 0 0 0 0 0 0
0 1 2 3 4 5 6 7 8 9 10 11


CNOT count : 167
Toffoli count : 78
```

```
1 1 0 1 1 0 0 0 0 0 0 0 0
0 1 2 3 4 5 6 7 8 9 10 11 12


CNOT count : 210
Toffoli count : 102
```

Hybrid Karatsuba

Hybrid

	12	13
Gate	47	51
CNOT	167	210
Toffoli	78	102

2 Way only

	12	13
Gate	47	51
CNOT	66	97
Toffoli	108	134

CNOT : Hybrid > 2 Way (100~110 average)

Toffoli : Hybird < 2 Way (30 average)

1 gate 9개 + CNOT 6개

Q & A