Hybrid Karatsuba Multiplication in Quantum Gates

장경배

https://youtu.be/m9VMjSfl3mA

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

3-way Karatsuba

$$A(x) \cdot B(x) = (A_1 + A_2) \cdot (B_1 + B_2)x^{3s}$$
$$+ (A_2 + A_0) \cdot (B_2 + B_0)x^{2s}$$
$$+ (A_1 + A_0) \cdot (B_1 + B_0)x^{s} +$$
$$(A_2 \cdot B_2 x^{2s} + A_1 \cdot B_1 x^{s} + A_0 \cdot B_0) \cdot$$
$$(x^{2s} + x^{s} + 1)$$

- n 번의 곱셈을 $\frac{2}{3}n$ 번에 수행할 수 있는 알고리즘

  Ex. 3 x 3 → 9번

  → 3-way Karatusba 는 6번

3-way Karatsuba

x	1	1	1
	1	1	1

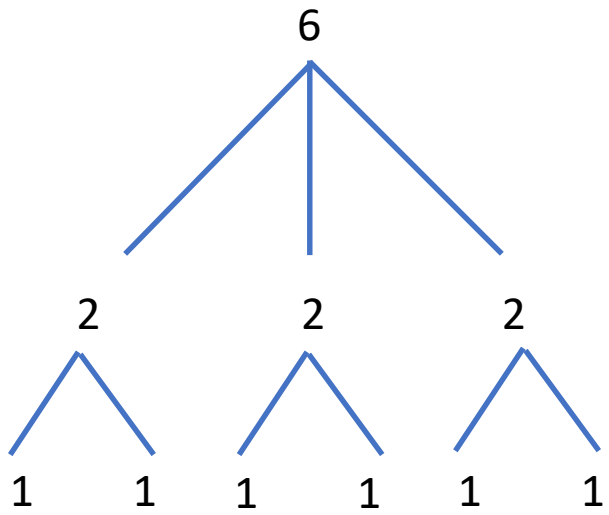
$$A(x) \cdot B(x) = (A_1 + A_2) \cdot (B_1 + B_2)x^{3s} + (A_2 + A_0) \cdot (B_2 + B_0)x^{2s} + (A_1 + A_0) \cdot (B_1 + B_0)x^{s} + (A_2 \cdot B_2 x^{2s} + A_1 \cdot B_1 x^{s} + A_0 \cdot B_0) \cdot (x^{2s} + x^{s} + 1)$$

<3-way>

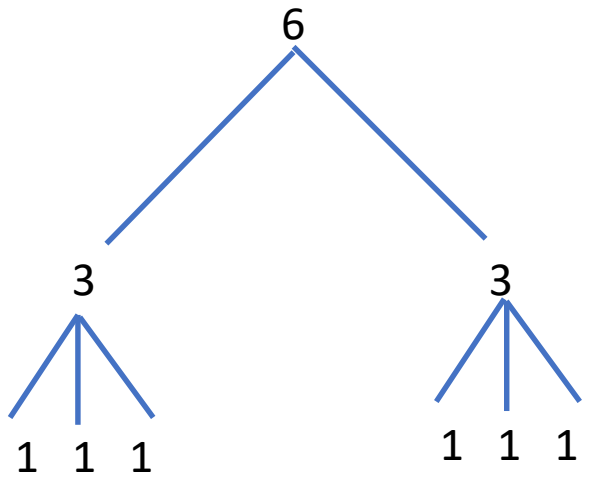
$$\alpha + (\gamma + \alpha + \beta)x^{k} + \beta x^{2k}$$

<2-way>

Hybrid-Karatsuba

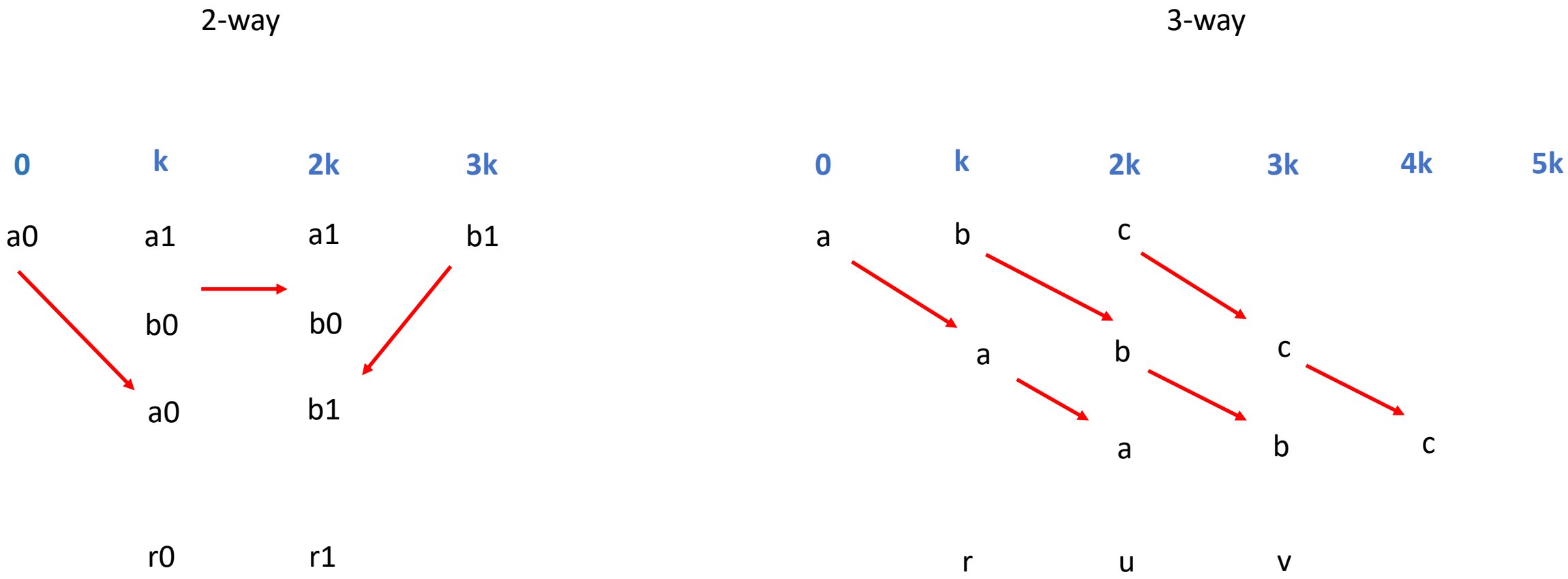


3-way
2-way



2-way
3-way

Hybrid-Karatsuba (2 ^ 13)



Hybrid-Karatsuba (2 ^ 13)

영 상

Result

```
Toffoli gate 실행횟수 : 78
Cnot gate 실행횟수 : 155
```

2^12 Modular 포함

```
Toffoli gate 실행횟수 : 102
Cnot gate 실행횟수 : 155
```

2^13 Modular 포함 안함

Modular → CNOT 63 +

218

Q & A