3-Way Toom-Cook 알고리듬의 유사부호

알고리듬 1. 3-Way Toom-Cook 알고리듬 $MUL^{3ToomCook}(A,B)$

입력: $flag$, n비트 정수 A, B
출력: AB

1. **procedure** $MUL^{3ToomCook}(A,B)$
2. **If** $flag \geq min\big(len(A), len(B)\big)$ **then**
3. **return** AB ▷ AB:일반곱셈
4. **end if**
5. $l \leftarrow max\big(len(A), len(B)\big) \,/\, 3$
6. $A_2, A_1, A_0 \leftarrow A_{[n:2l]},\ A_{[2l:l]},\ A_{[l:0]}$
7. $B_2, B_1, B_0 \leftarrow B_{[n:2l]},\ B_{[2l:l]},\ B_{[l:0]}$
8. $cnt \leftarrow 0$
9. $T \leftarrow [\,]$
10. **for** i **in** $[-2,-1,0,1,\infty]$ **do**
11. $T[cnt] \leftarrow MUL^{3ToomCook}\big(p(i), q(i)\big)$
12. $cnt \leftarrow cnt + 1$
13. $r \leftarrow T \cdot \mathcal{M}^T$
14. $R_{1[6l:4l]}, R_{1[4l:2l]}, R_{1[2l:0]} \leftarrow r[4], r[2], r[0]$
15. $R_{0[5l:3l]}, R_{0[3l:l]}, R_{0[l:0]} \leftarrow r[3], r[1], 0_l$
16. $R \leftarrow R_1 + R_0$
17. **return** R
18. **end procedure**

알고리듬 1은 3-Way Toom-Cook 알고리듬의 유사부호이다.

1워드를 32비트로 설정하여 두 정수 $A,\ B$ 의 워드길이가 둘 중 하나라도 $flag$보다 작아지는 경우, $MUL^{3ToomCook}(A,B)$ 함수의 재귀 호출을 멈추고 일반 곱셈 AB을 진행한다. 본 논문에서는 $flag$를 10으로 설정하여, 입력값인 두 정수 $A,\ B$가 10워드 보다 작은 경우 일반 곱셈 연산 결과를 반환하였다. Line 5-7은 분할 단계이다. Line 8-12에서는 평가와 재귀적 곱셈 단계를 동시에 수행하며, $p(i)$와 $q(i)$의 곱셈을 열벡터 T 에 저장한다. 이때 $p(i)$와 $q(i)$는 위에서 정의한 함수이다. Line 13에서는 열벡터 T와 보간 행렬 $\mathcal{M}$의 전치 행렬을 곱한다. Line 14-16은 재구성 단계이다.

3-Way Toom-Cook의 연산 속도

본 절에서는 알고리듬 1의 입력으로 두 정수가 7680비트일 때와 15360비트일 때 세 가지 상황에 대한 연산 속도를 측정한다. 구현 환경은 다음과 같다.

하드웨어	MacBook Air. Apple M2. 8GB RAM.
컴파일러	gcc 13.1.6 (-O2)
정수 연산 라이브러리	FLINT 2.9.0

RSA의 키 길이를 파라미터로 설정하여 세 가지 상황에 대해 연산 속도를 비교하였다. 192비트의 보안 강도를 가지는 RSA의 키 길이 경우 7680비트, 256비트의 경우 15360비트의 키에 대해 곱셈 연산을 수행한다. (상황 2)는 RSA-7680의 복호화 시 곱셈 횟수인 횟수인 15360회이고, (상황 3)은 RSA-15360의 복호화 시 곱셈 횟수인 30720회이다.
[표 1]은 두 가지 파라미터의 세 가지 상황에 대한 3-Way Toom-Cook 연산 시간을 측정한 결과이며, 시간 단위는 밀리초(ms)이다.

[표 1] 3-Way Toom-Cook 알고리듬 연산 시간 (단위: ms)

입력 정수의 비트 길이	7,680	15,360
(상황 1)	0.006	0.011
(상황 2)	104.084	182.981
(상황 3)	184.456	344.708

측정 결과, (상황 1)인 곱셈 연산 1회 수행에서는 입력값 7680/15360비트에 대해 0.006/0.011밀리초가 소요되었다. 입력 파라미터가 7680비트인 경우, 15360비트인 경우와 비교하여 최대 1.86배 빨랐다.