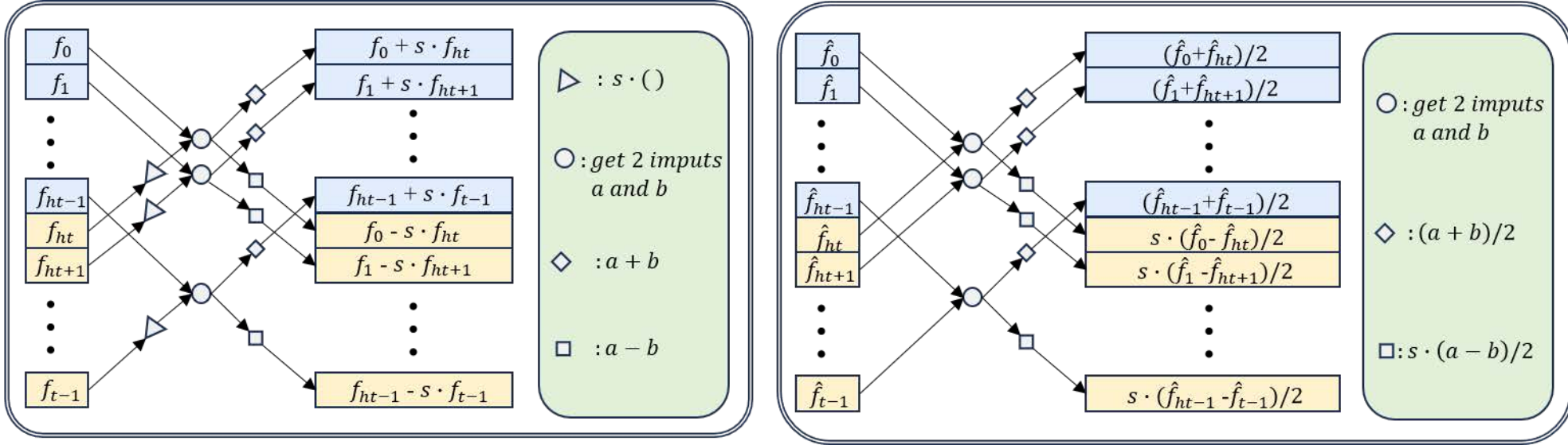
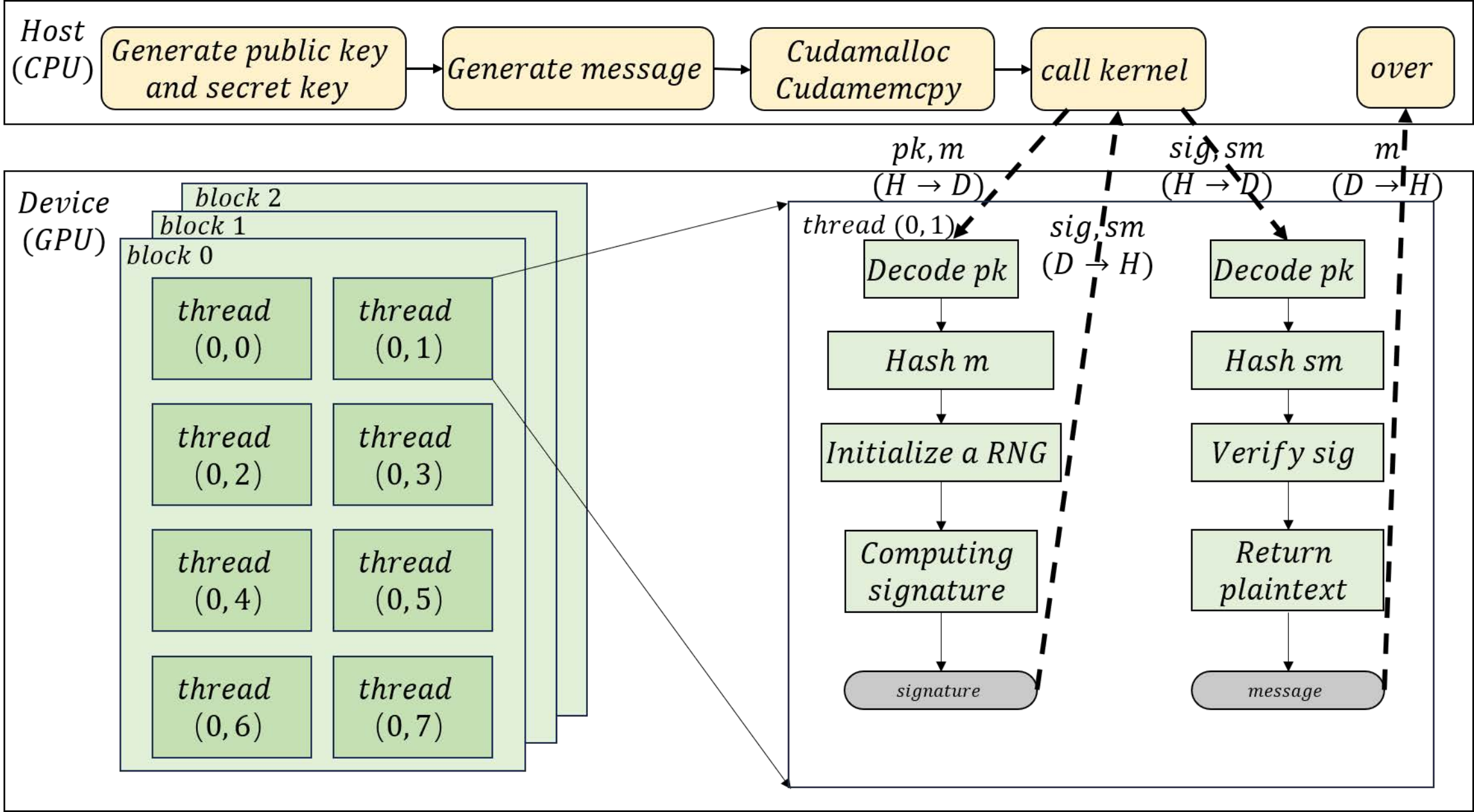
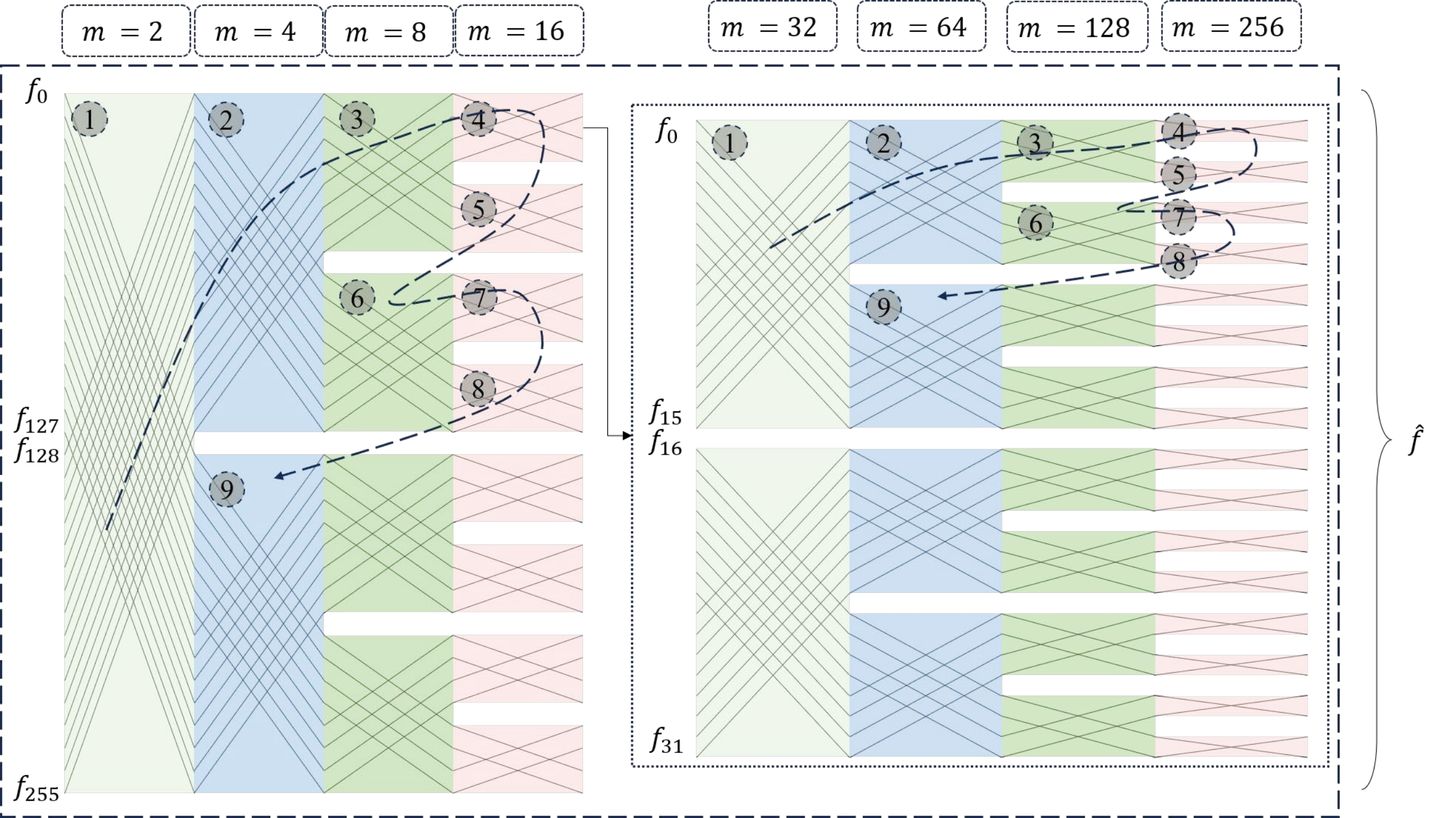
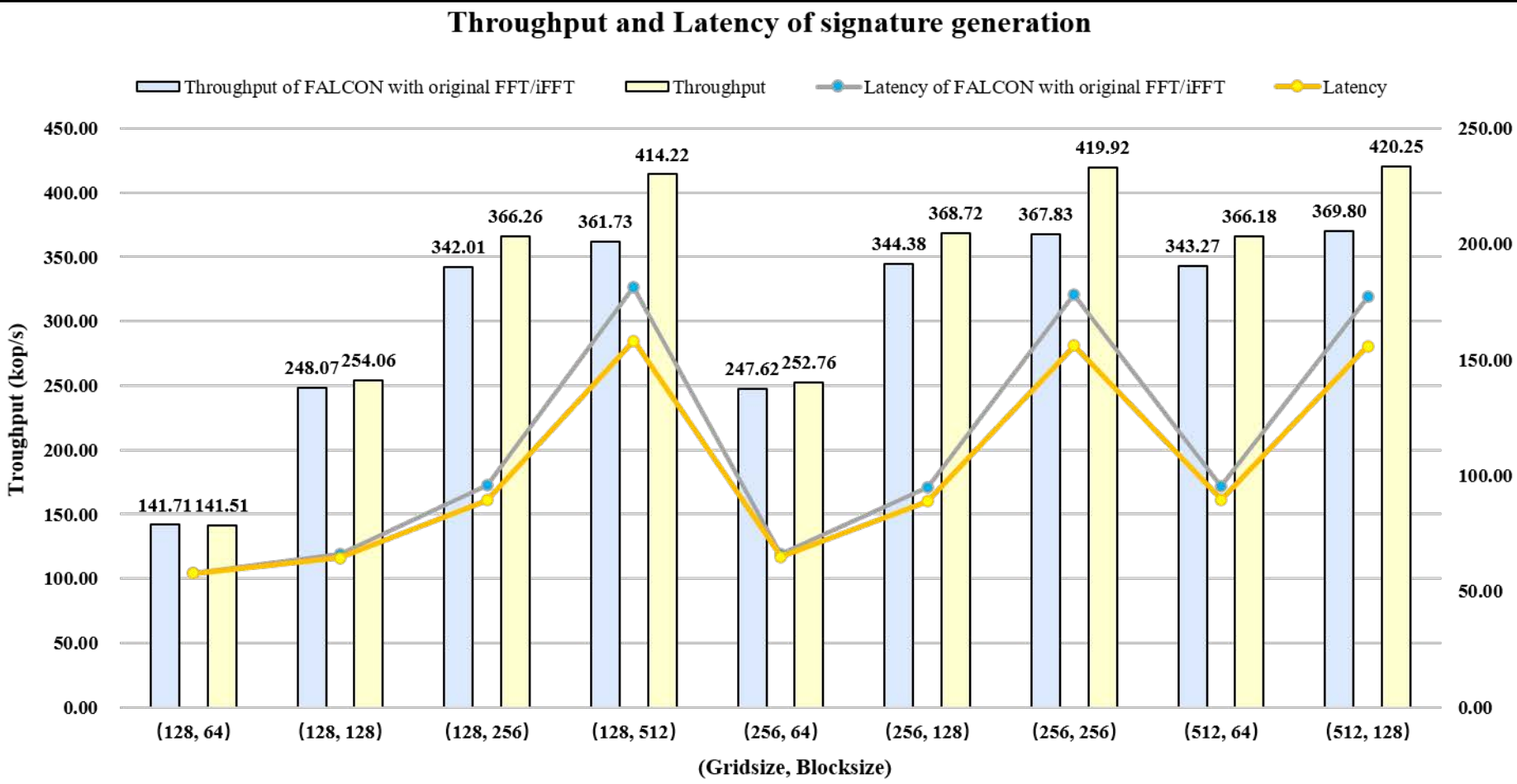
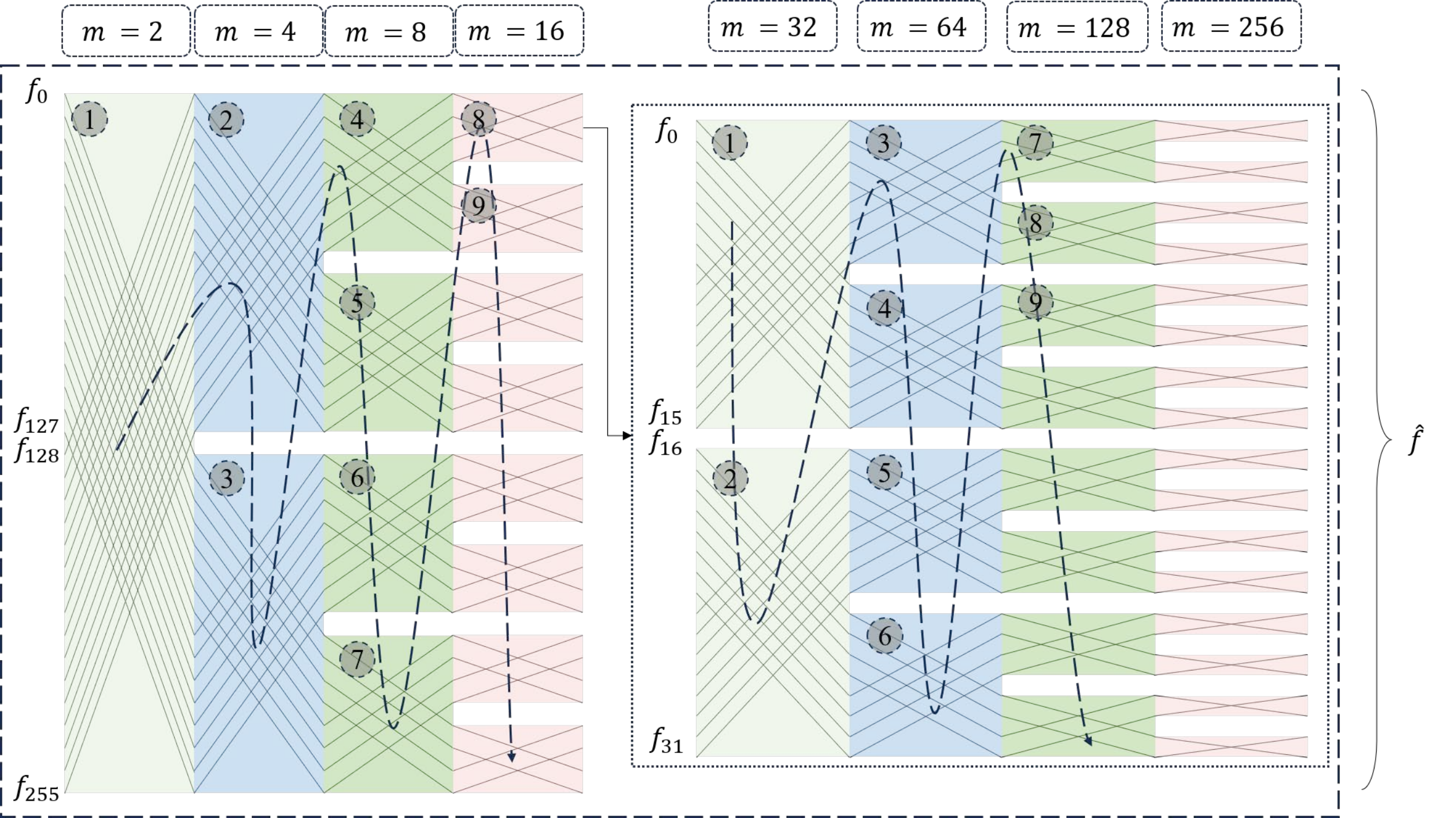
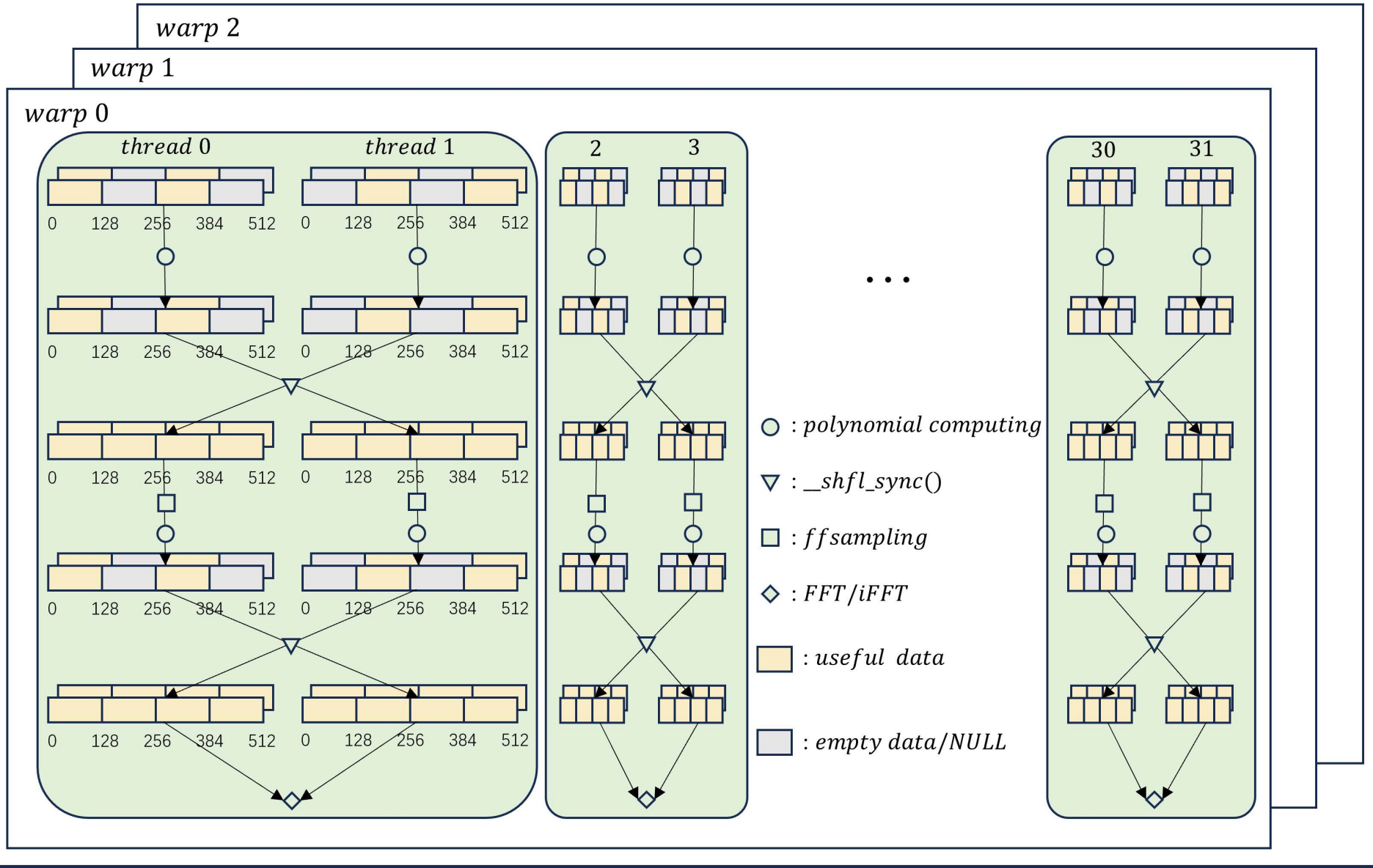

f_0
f_1
f_{ht-1}
f_{ht}
f_{ht+1}
f_{t-1}
$f_0 + s \cdot f_{ht}$
$f_1 + s \cdot f_{ht+1}$
$f_{ht-1} + s \cdot f_{t-1}$
$f_0 - s \cdot f_{ht}$
$f_1 - s \cdot f_{ht+1}$
$f_{ht-1} - s \cdot f_{t-1}$
$: s \cdot ( )$
: get 2 imputs a and b
$: a + b$
$: a - b$
$\hat{f}_0$
$\hat{f}_1$
$\hat{f}_{ht-1}$
$\hat{f}_{ht}$
$\hat{f}_{ht+1}$
$\hat{f}_{t-1}$
$(\hat{f}_0+\hat{f}_{ht})/2$
$(\hat{f}_1+\hat{f}_{ht+1})/2$
$(\hat{f}_{ht-1}+\hat{f}_{t-1})/2$
$s \cdot (\hat{f}_0 - \hat{f}_{ht})/2$
$s \cdot (\hat{f}_1 - \hat{f}_{ht+1})/2$
$s \cdot (\hat{f}_{ht-1} - \hat{f}_{t-1})/2$
: get 2 imputs a and b
$: (a + b)/2$
$: s \cdot (a - b)/2$

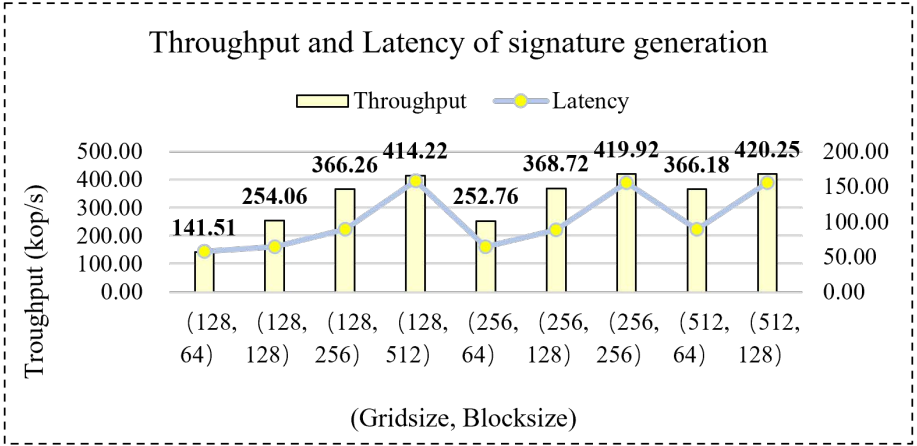

Host (CPU)
Generate public key and secret key
Generate message
Cudamalloc Cudamemcpy
call kernel
over
pk, m (H → D)
sig, sm (H → D)
m (D → H)
Device (GPU)
block 2
block 1
block 0
thread (0, 0)
thread (0, 1)
thread (0, 2)
thread (0, 3)
thread (0, 4)
thread (0, 5)
thread (0, 6)
thread (0, 7)
thread (0, 1)
Decode pk
Hash m
Initialize a RNG
Computing signature
signature
sig, sm (D → H)
Decode pk
Hash sm
Verify sig
Return plaintext
message

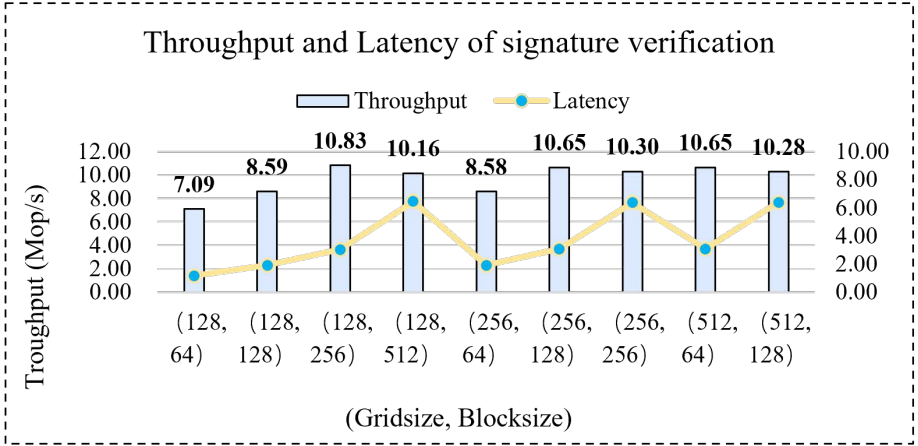

$m = 2$
$m = 4$
$m = 8$
$m = 16$
$m = 32$
$m = 64$
$m = 128$
$m = 256$
f_0
f_{127}
f_{128}
f_{255}
f_0
f_{15}
f_{16}
f_{31}
$\hat{f}$
1
2
3
4
5
6
7
8
9


Throughput and Latency of signature generation
Throughput of FALCON with original FFT/iFFT
Throughput
Latency of FALCON with original FFT/iFFT
Latency
Troughput (kop/s)
450.00
400.00
350.00
300.00
250.00
200.00
150.00
100.00
50.00
0.00
250.00
200.00
150.00
100.00
50.00
0.00
141.71
141.51
248.07
254.06
342.01
366.26
361.73
414.22
247.62
252.76
344.38
368.72
367.83
419.92
343.27
366.18
369.80
420.25
(128, 64)
(128, 128)
(128, 256)
(128, 512)
(256, 64)
(256, 128)
(256, 256)
(512, 64)
(512, 128)
(Gridsize, Blocksize)


$m = 2$
$m = 4$
$m = 8$
$m = 16$
$m = 32$
$m = 64$
$m = 128$
$m = 256$
f_0
f_{127}
f_{128}
f_{255}
f_0
f_{15}
f_{16}
f_{31}
$\hat{f}$


warp 2
warp 1
warp 0
thread 0
thread 1
2
3
30
31
0 128 256 384 512
: polynomial computing
: __shfl_sync()
: ffsampling
: FFT/iFFT
: useful data
: empty data/NULL


Throughput and Latency of signature generation
Throughput
Latency
Troughput (kop/s)
500.00
400.00
300.00
200.00
100.00
0.00
200.00
150.00
100.00
50.00
0.00
141.51
254.06
366.26
414.22
252.76
368.72
419.92
366.18
420.25
(128, 64)
(128, 128)
(128, 256)
(128, 512)
(256, 64)
(256, 128)
(256, 256)
(512, 64)
(512, 128)
(Gridsize, Blocksize)


Throughput and Latency of signature verification
Throughput
Latency
Troughput (Mop/s)
12.00
10.00
8.00
6.00
4.00
2.00
0.00
10.00
8.00
6.00
4.00
2.00
0.00
7.09
8.59
10.83
10.16
8.58
10.65
10.30
10.65
10.28
(128, 64)
(128, 128)
(128, 256)
(128, 512)
(256, 64)
(256, 128)
(256, 256)
(512, 64)
(512, 128)
(Gridsize, Blocksize)