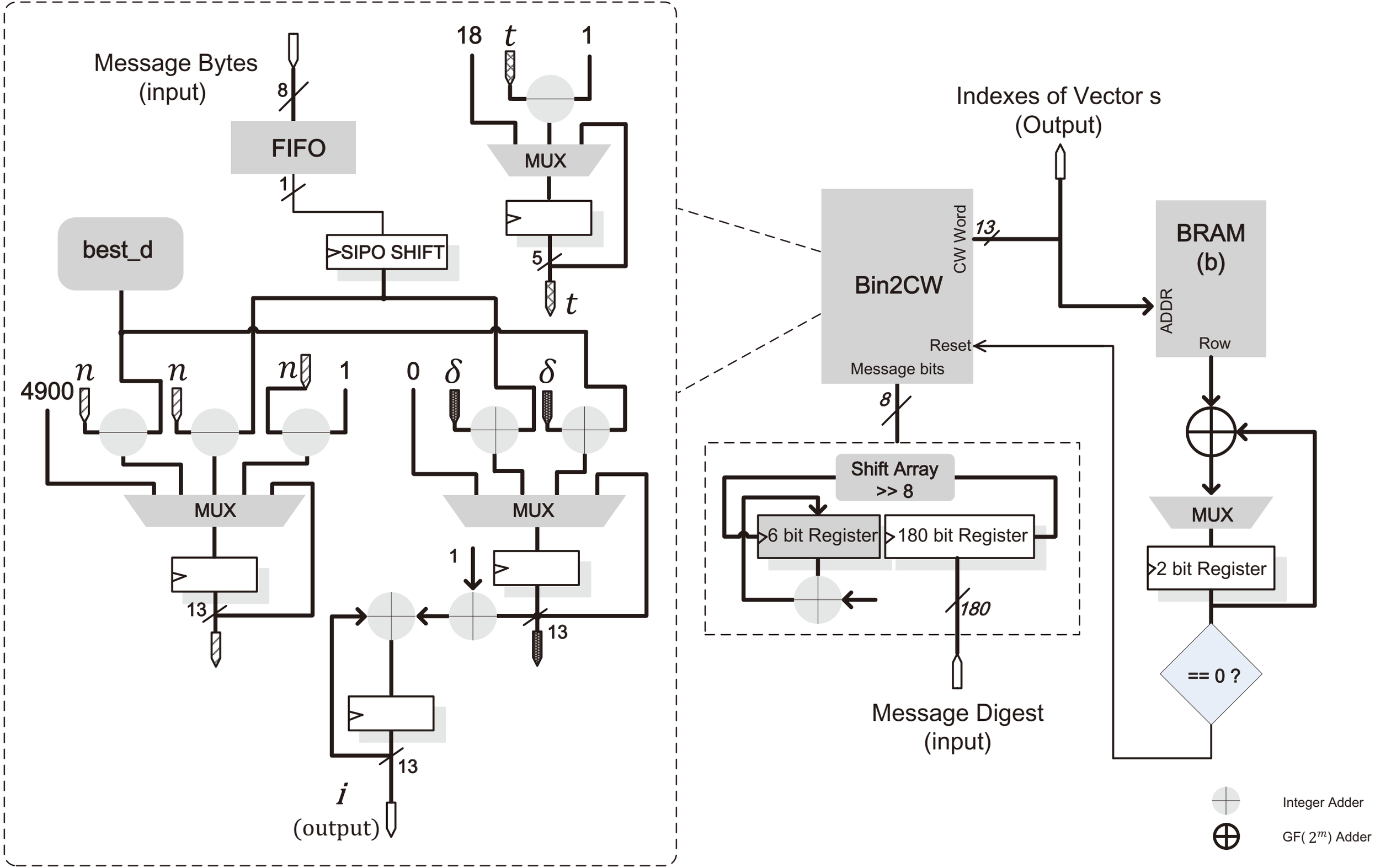
Message Bytes
(input)
8
FIFO
1
SIPO SHIFT
best_d
18
t
1
MUX
5
t
4900
n
n
n
1
0
δ
δ
MUX
MUX
13
1
13
13
i
(output)
Indexes of Vector s
(Output)
Bin2CW
CW Word
13
Reset
Message bits
8
BRAM
(b)
ADDR
Row
Shift Array
>> 8
6 bit Register
180 bit Register
180
Message Digest
(input)
MUX
2 bit Register
== 0 ?
Integer Adder
GF(2^m) Adder