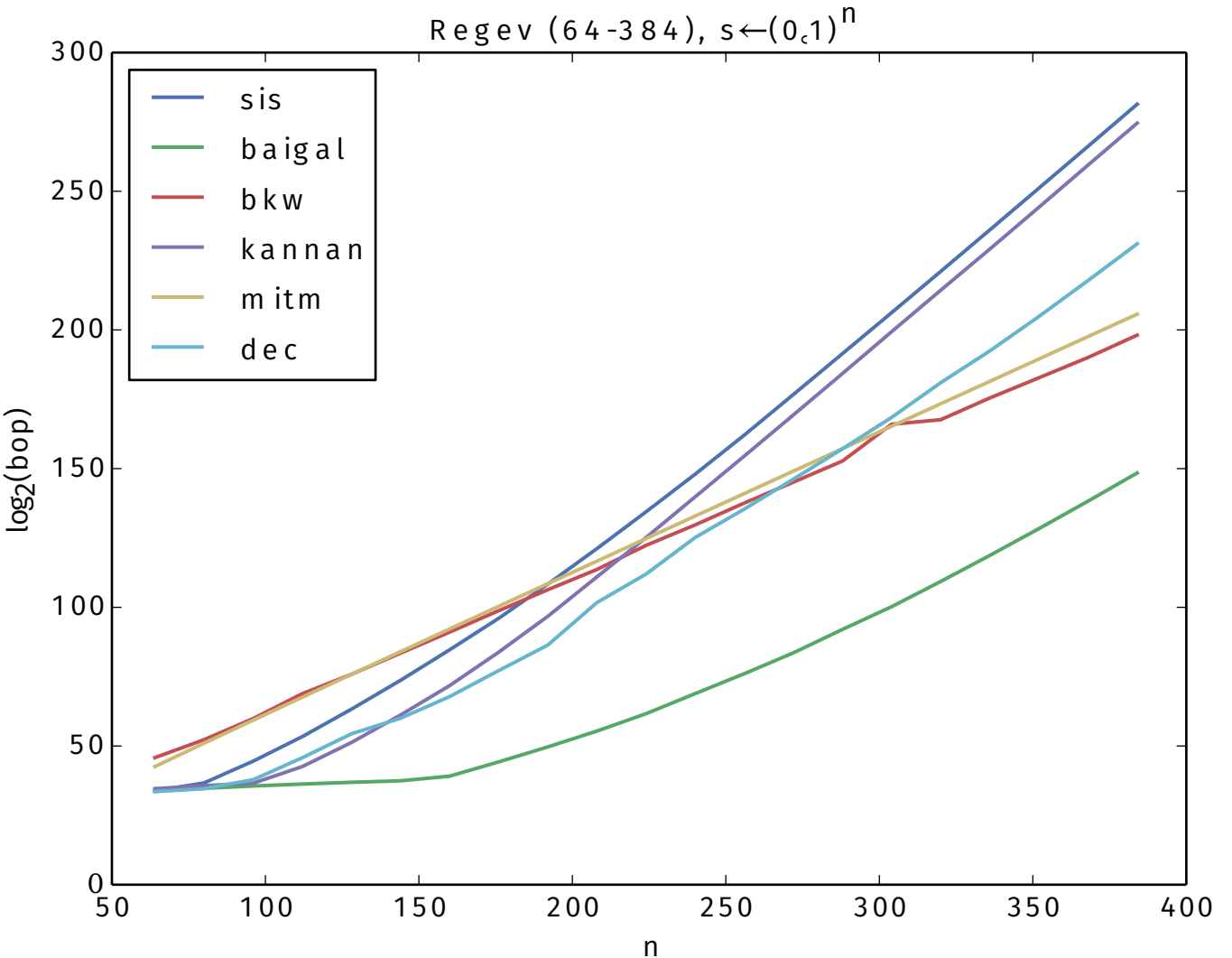
Regev (64-384), s←(0,1)^n
sis
baigal
bkw
kannan
mitm
dec
log2(bop)
n
0
50
100
150
200
250
300
50
100
150
200
250
300
350
400