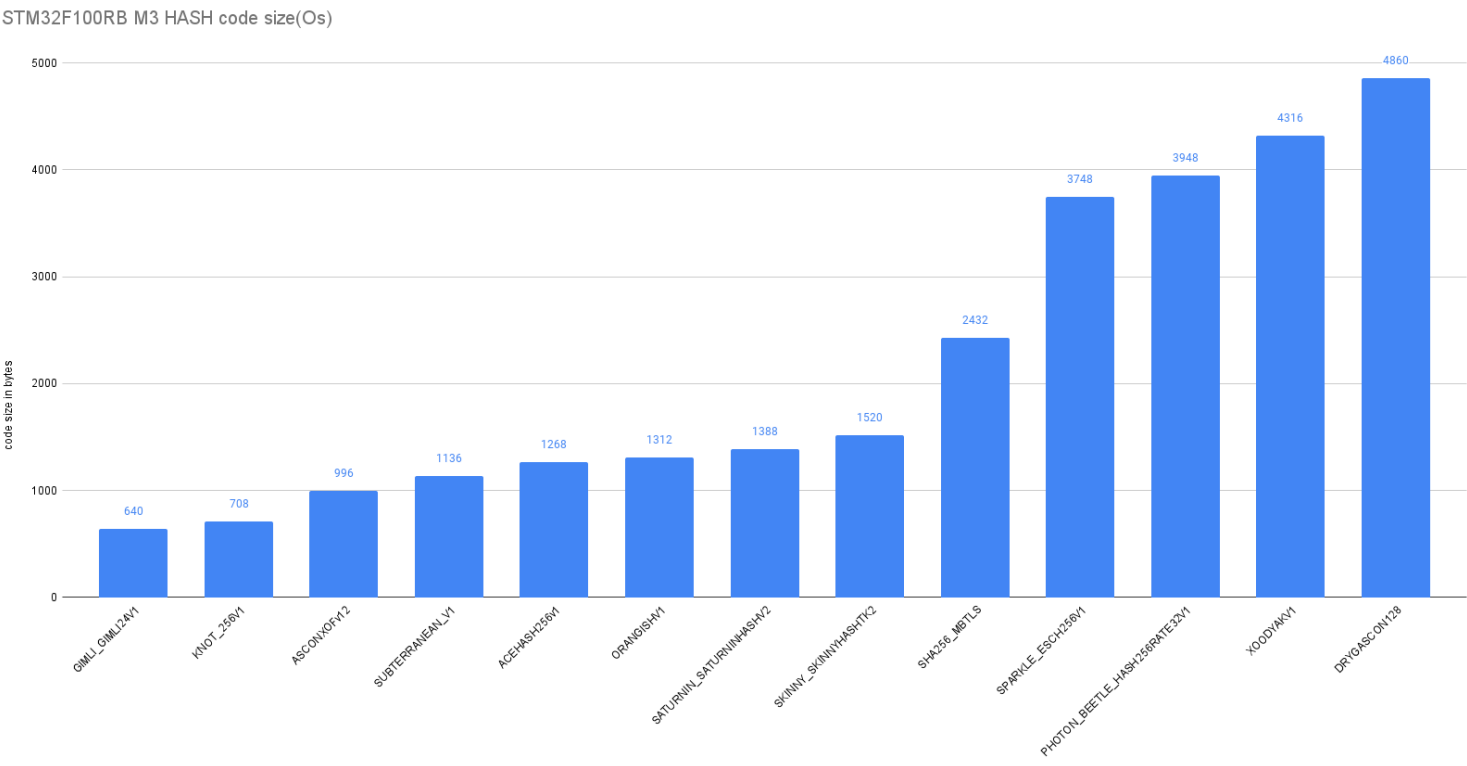
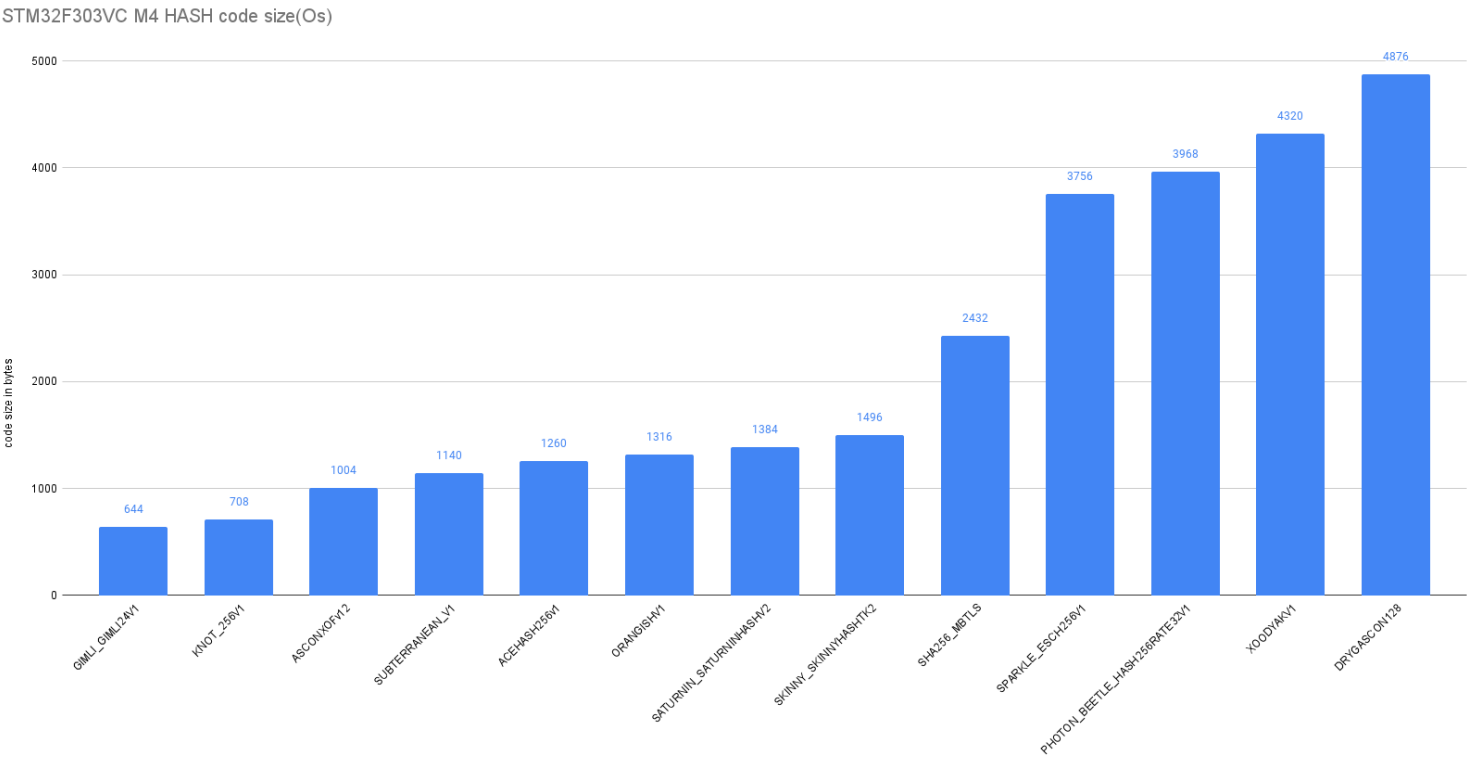
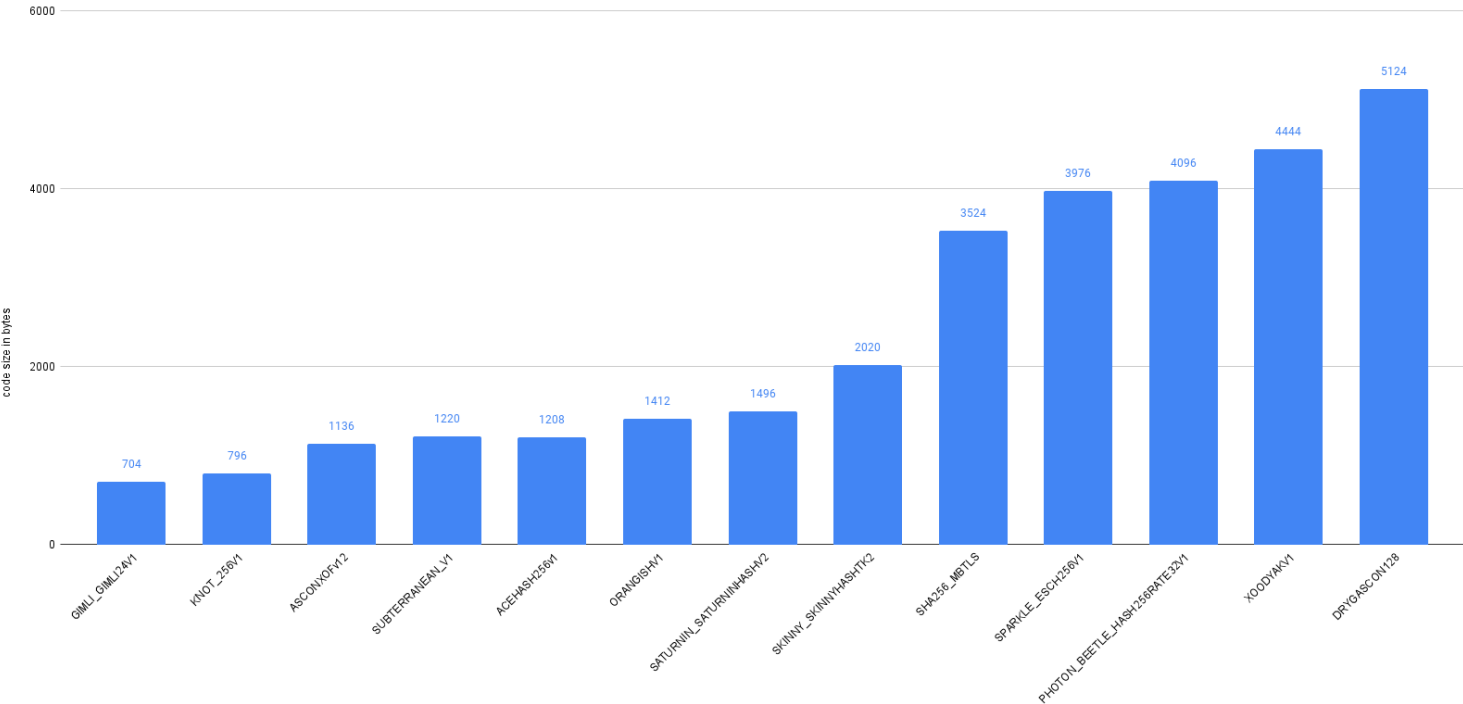


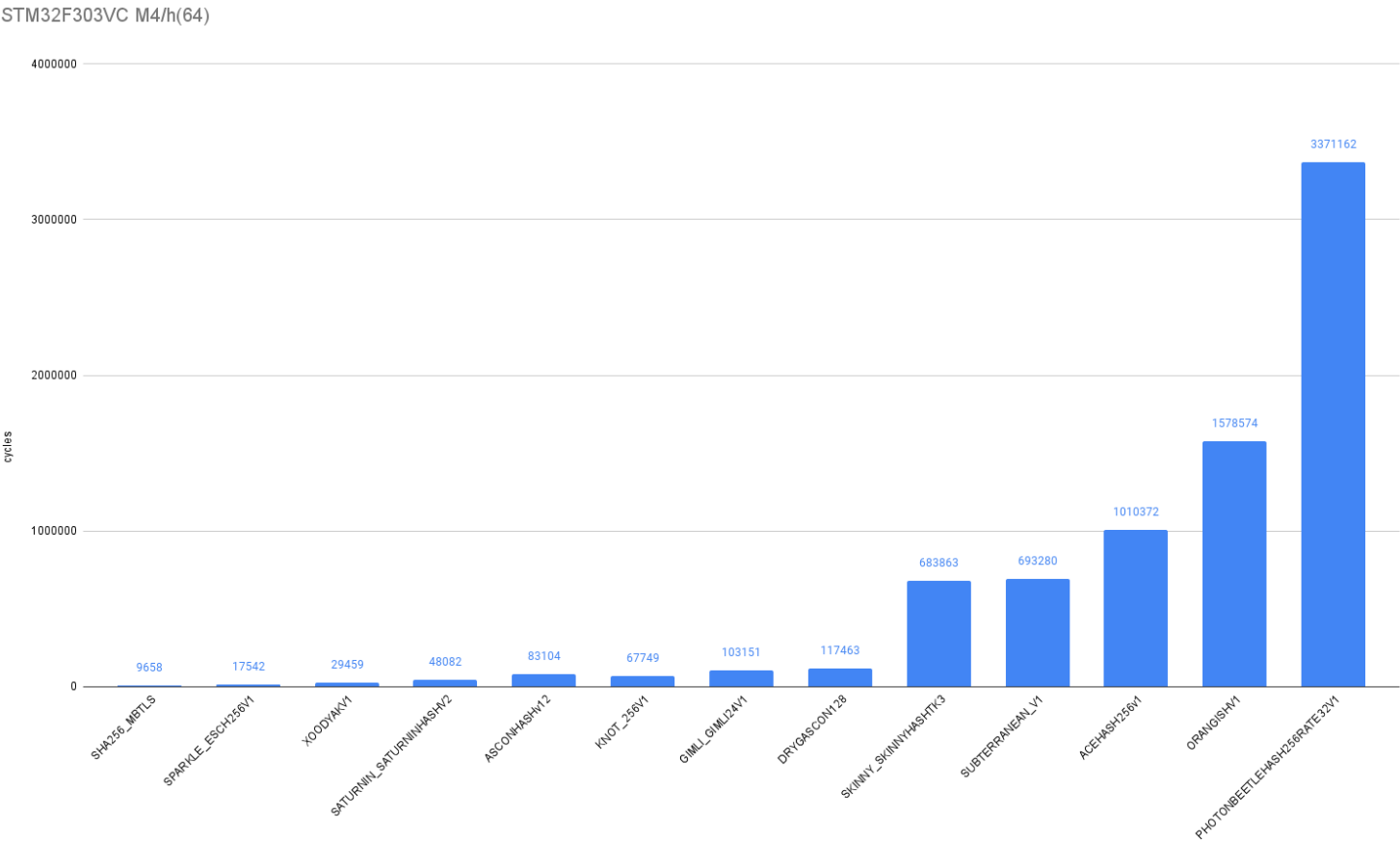
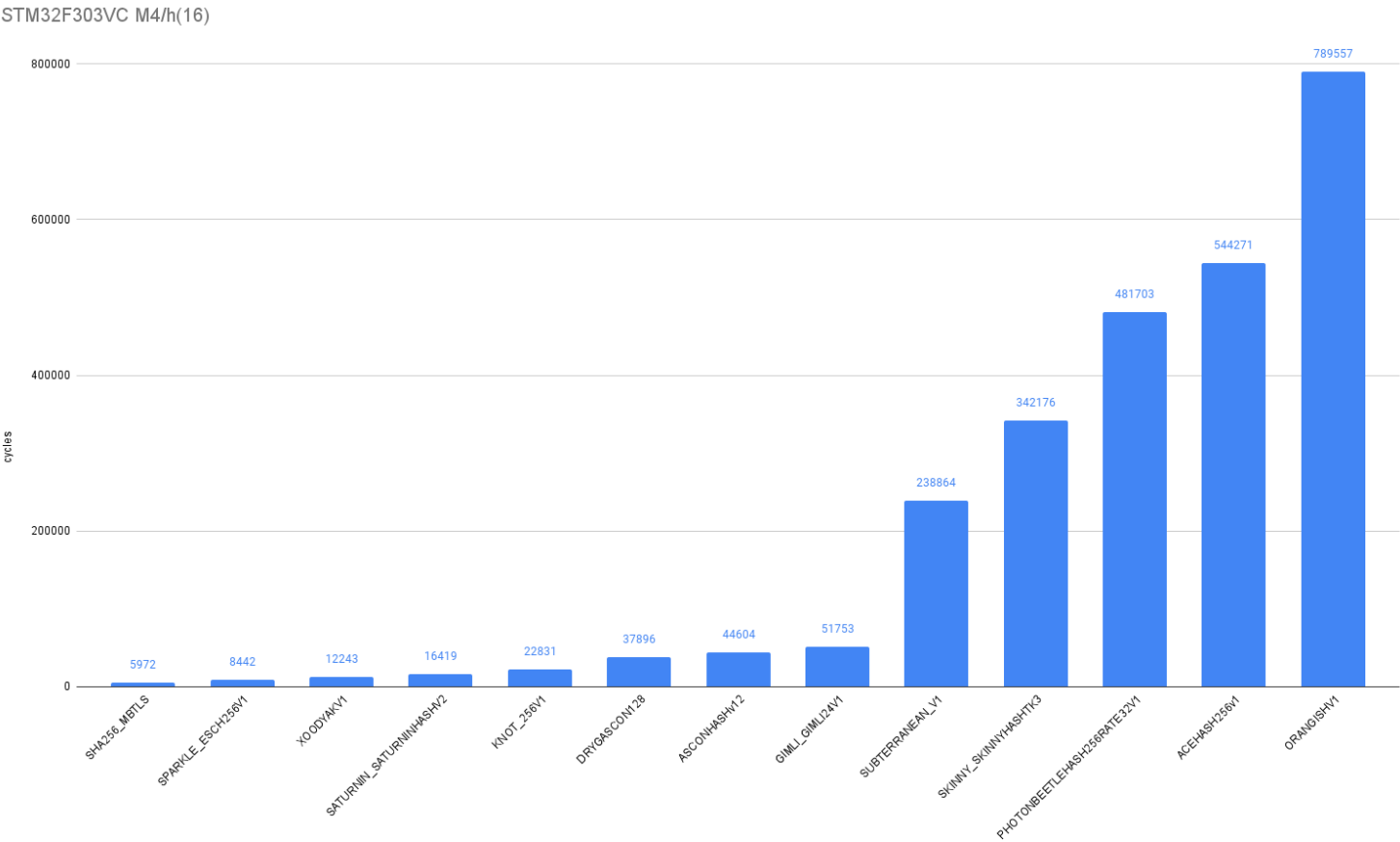
Code size of different HASH algorithms on Cortex-M0, Cortex-M3 and Cortex-M4 Platforms



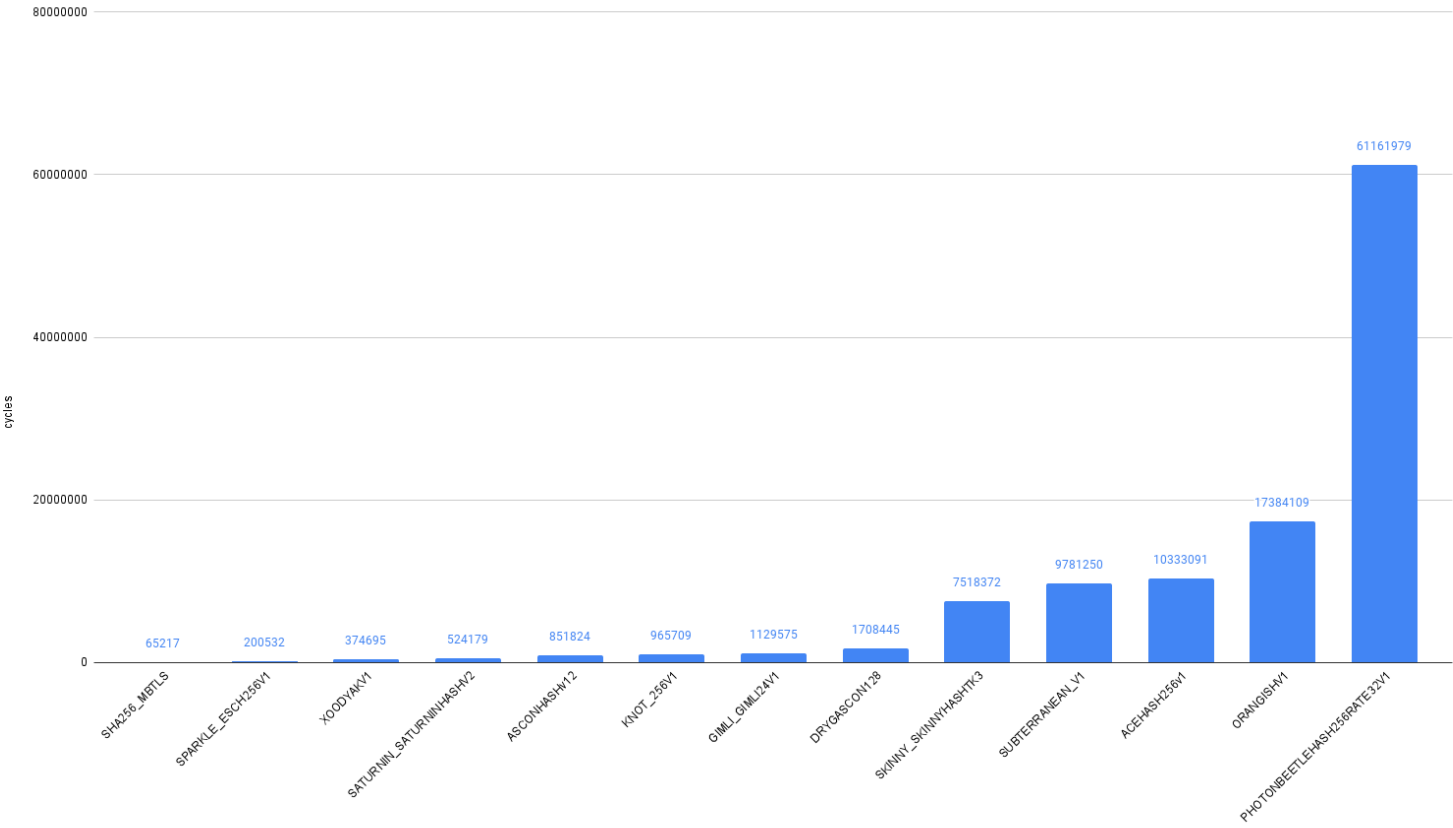
STM32F051R8 M0 HASH code size(0s)



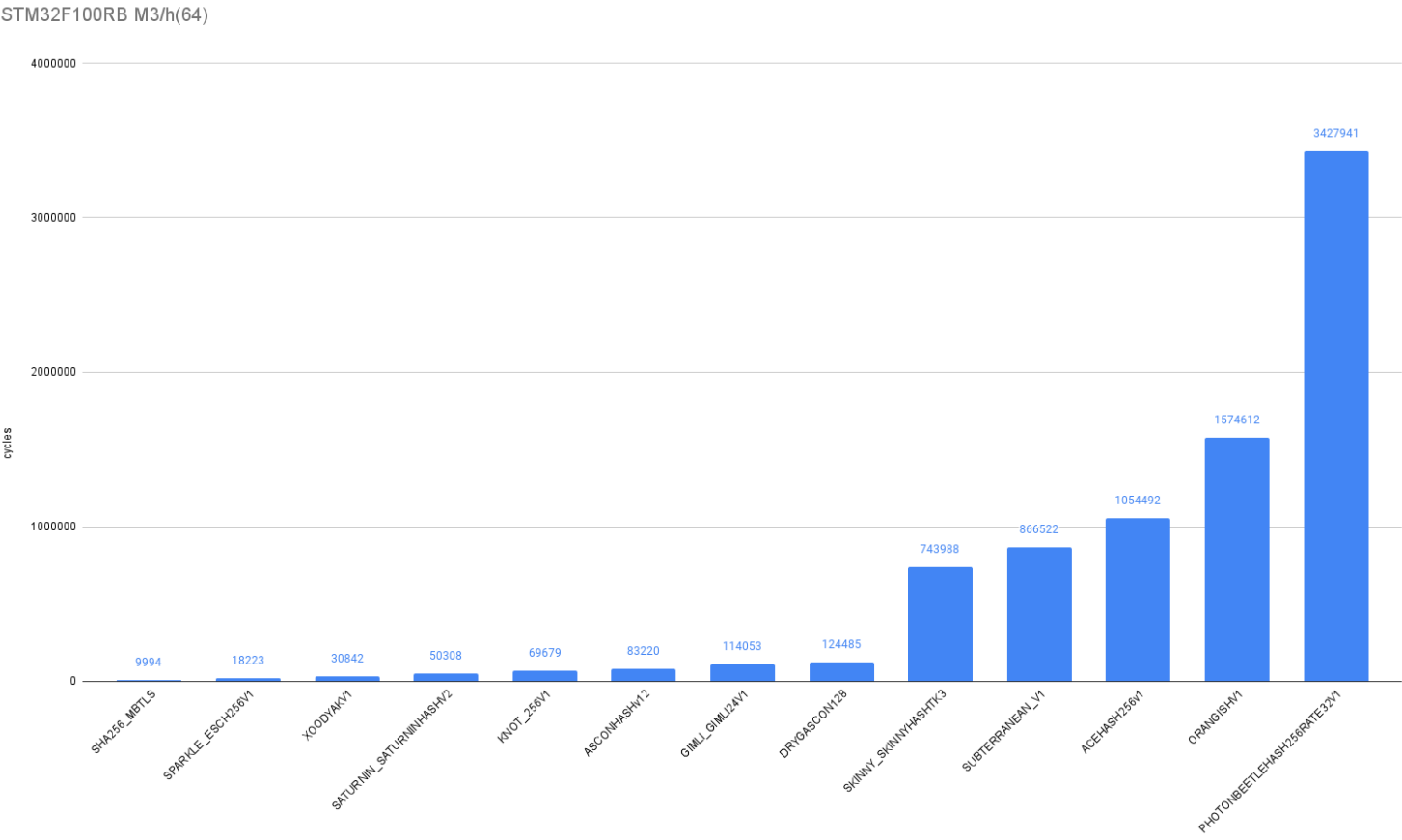
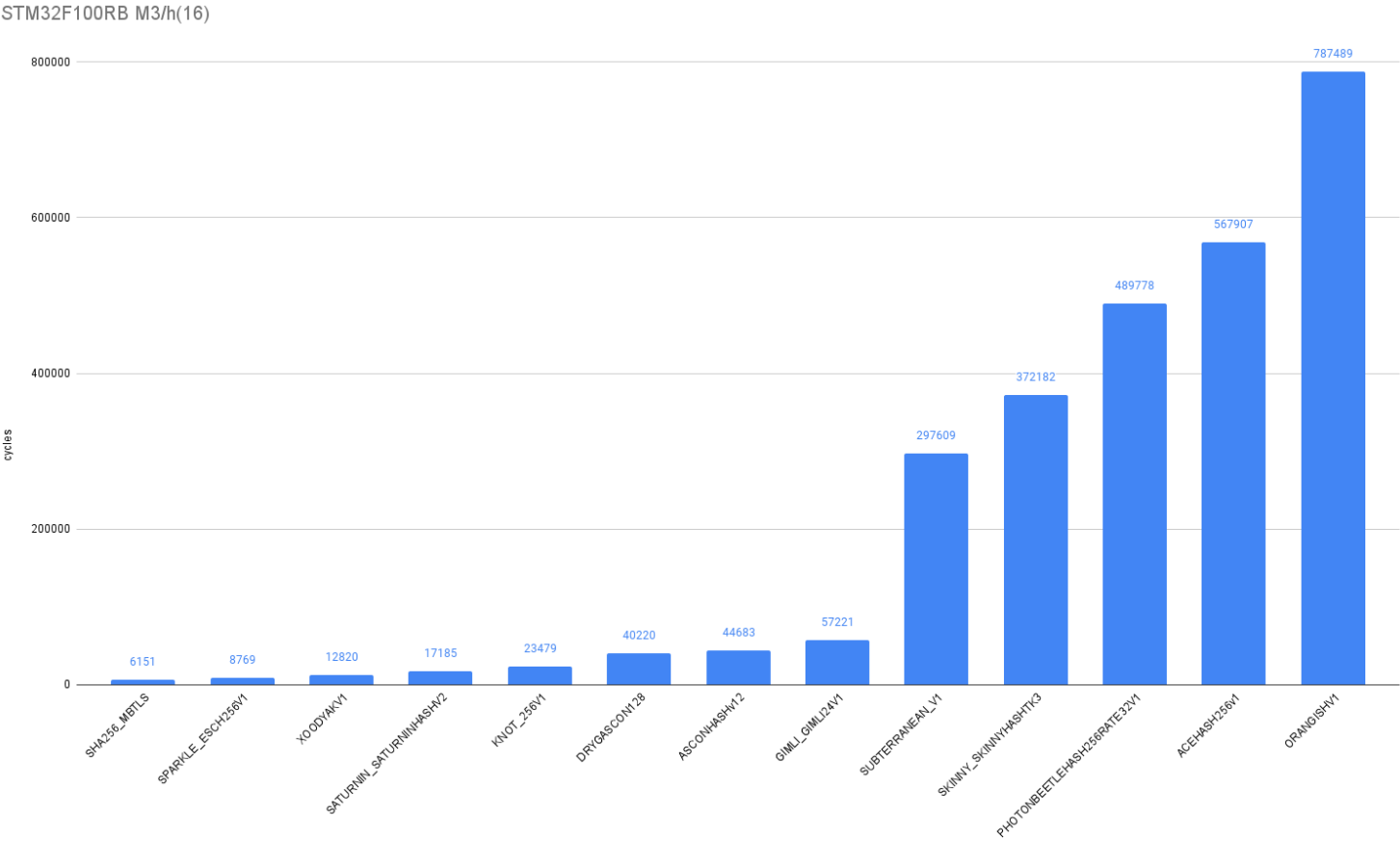
Execution cycles of different HASH algorithms on Cortex-M4



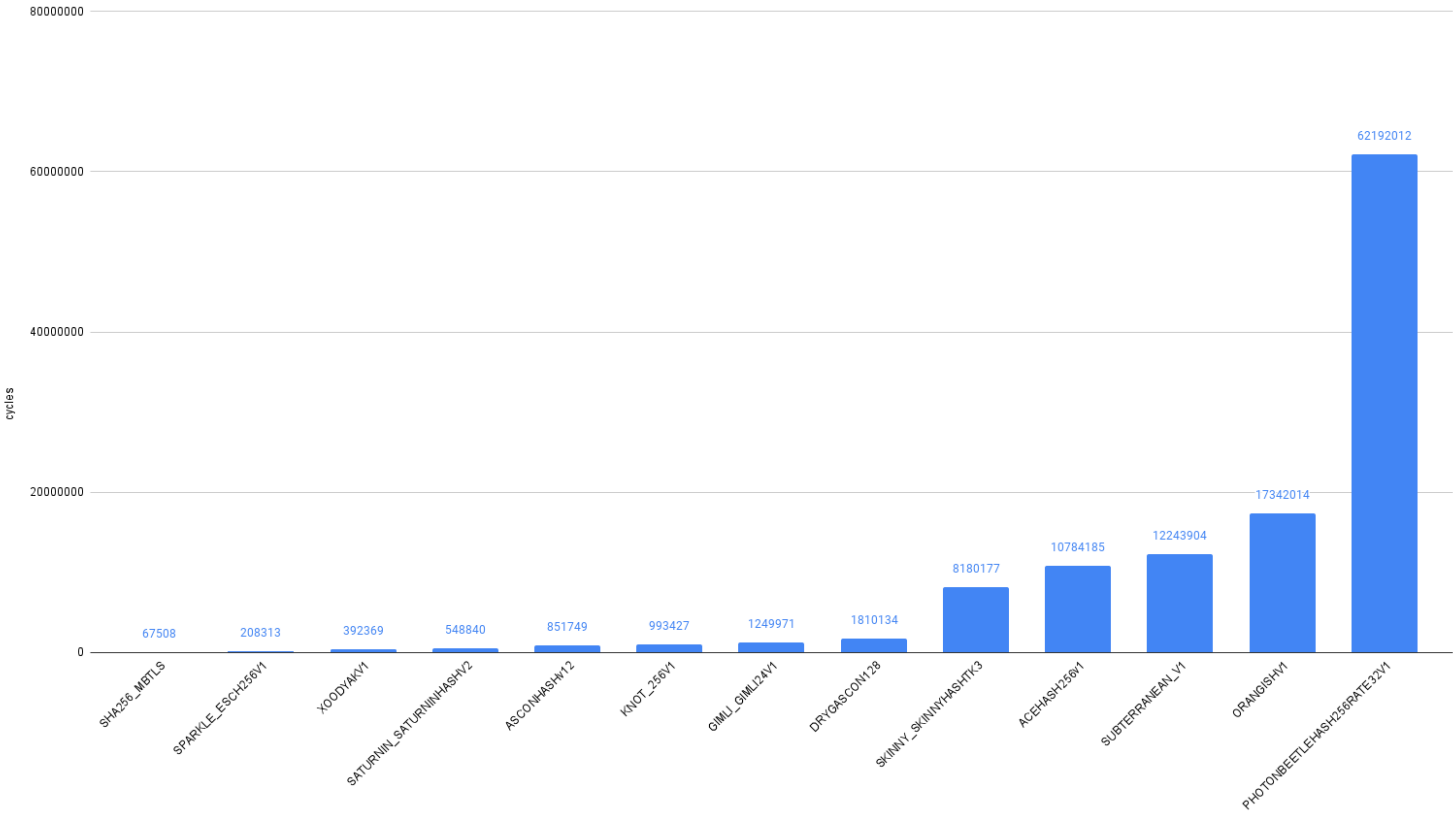
STM32F303VC M4/h(1024)



Execution cycles of different HASH algorithms on Cortex-M3

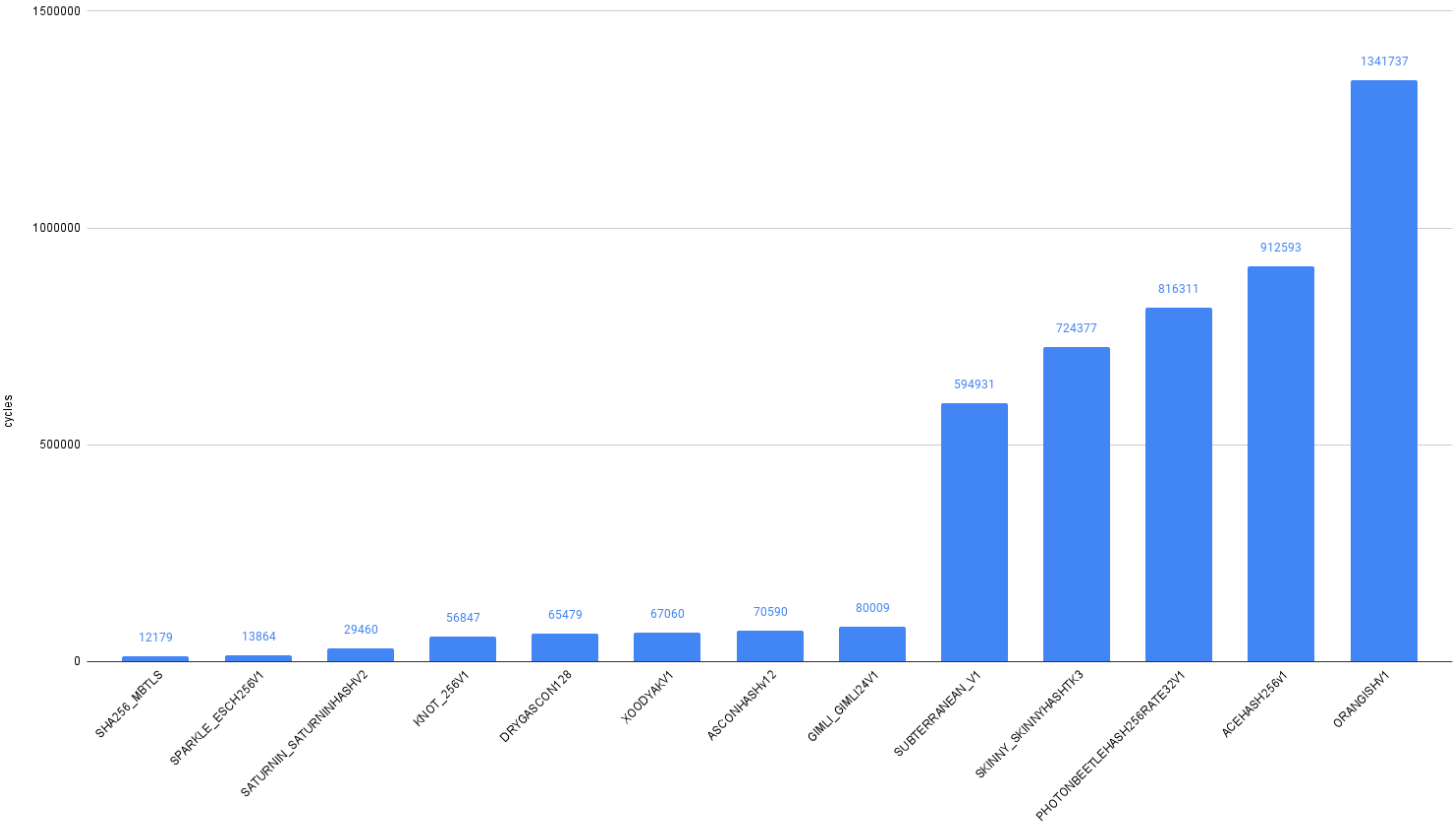


STM32F100RB M3/h(1024)

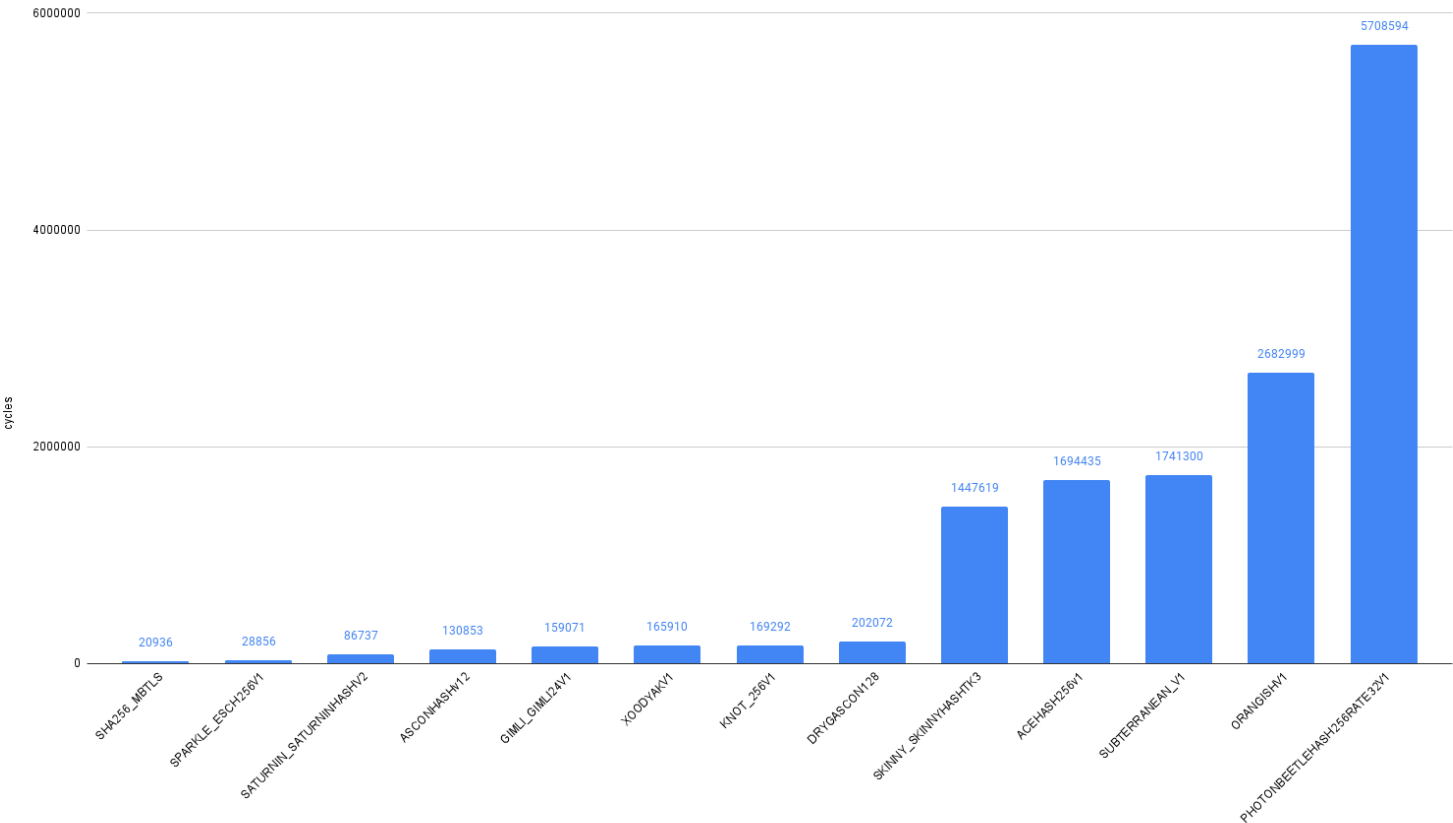


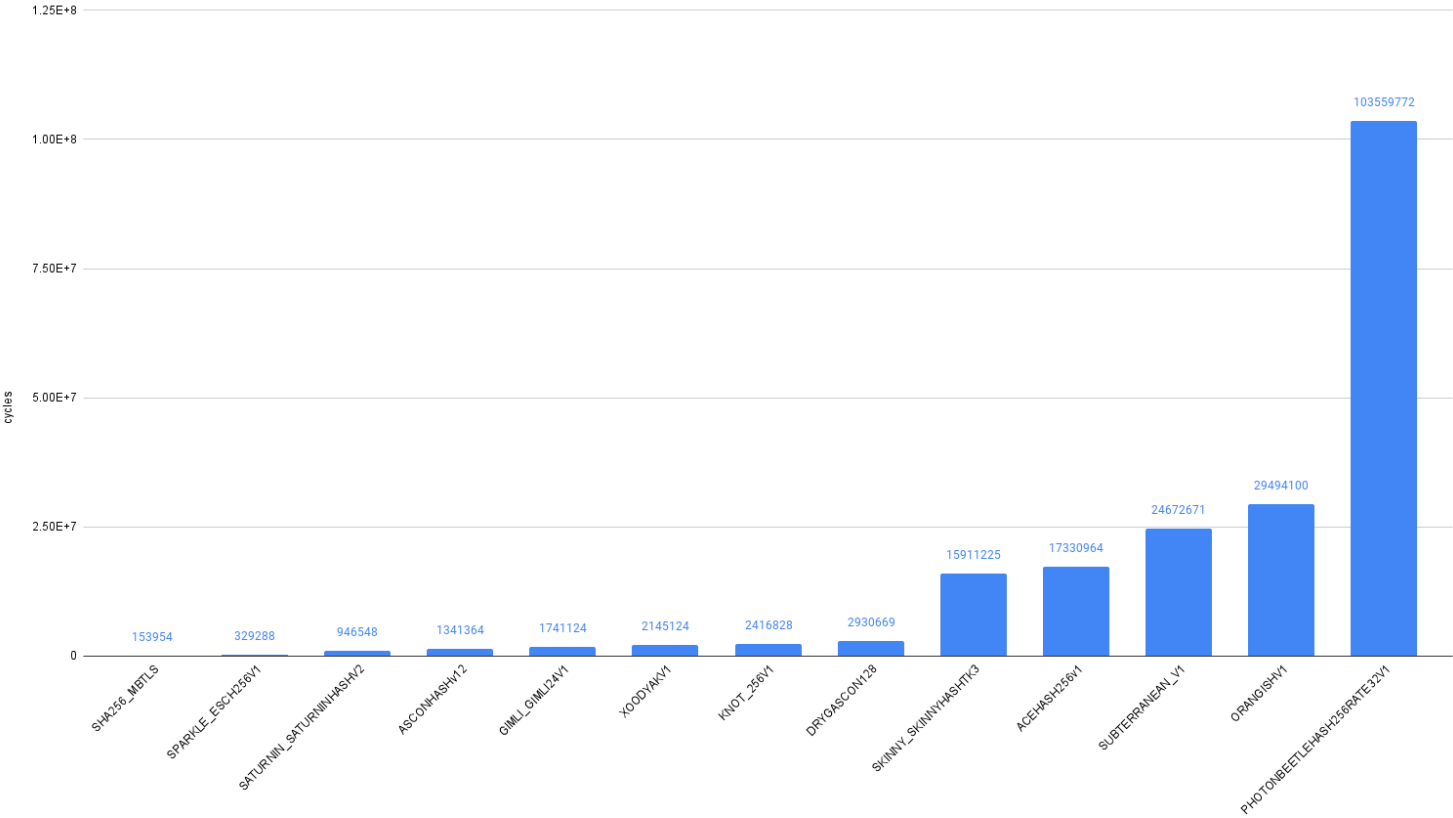
Execution cycles of different HASH algorithms on Cortex-M0

STM32F030R8 M0/h(16)



STM32F030R8 M0/h(64)

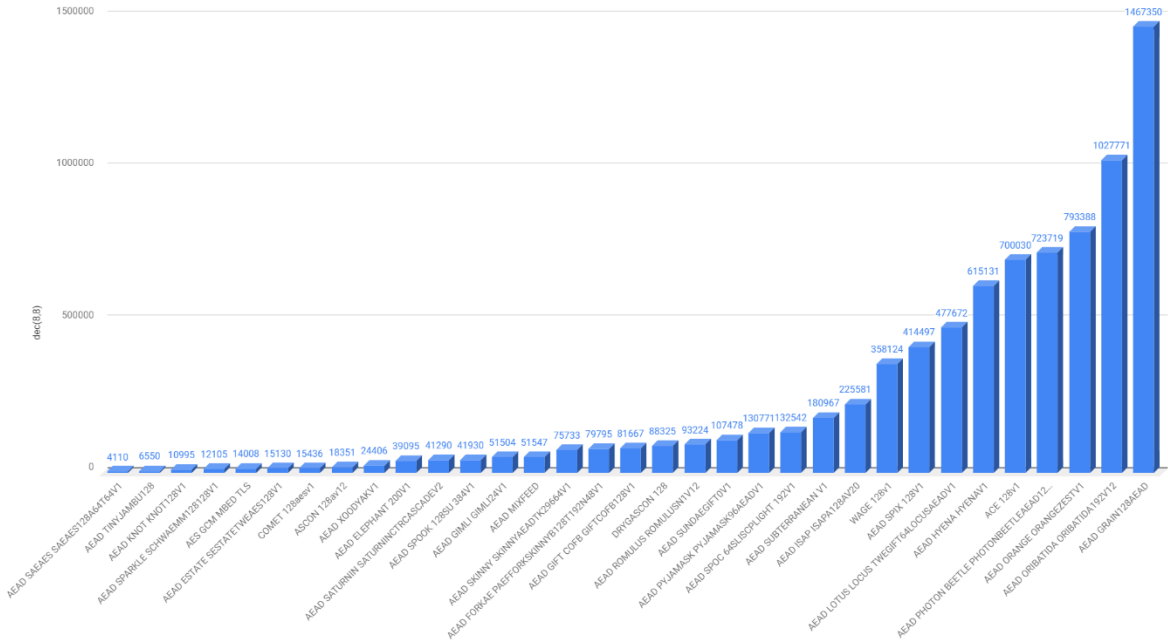




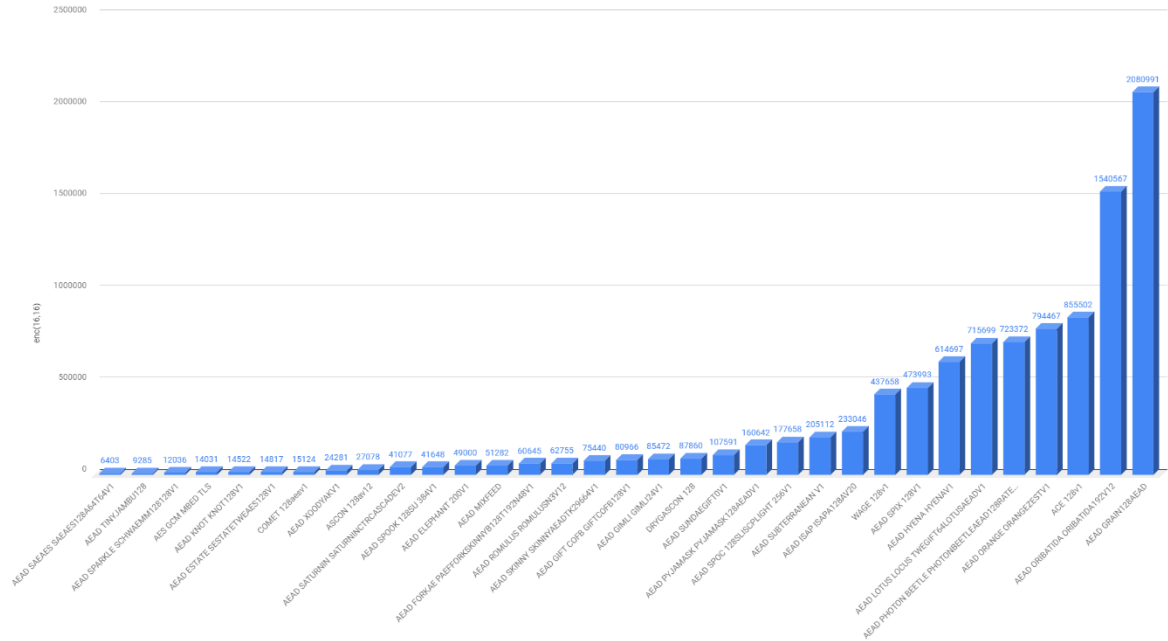
Model	Code Size (bytes)
AEO TH JAMBU128	1104
AEO GIML GIML4xV1	1504
AEO KNOT KNOT128V1	1640
AEO GIFT GIFT128P128V1	1764
AEO SUNGAE4xV1	1988
AEO ESTATE ESTATE4xV1	2032
AEO SATURNIN SATURNIN2xV1	2184
AEO ESTATE ESTATE2xV1	2184
AEO INTRACAS4xV2	2220
AEO MUXED	2224
AEO SUBTERANEAN V1	2236
AEO SPOOK 128x128V1	2344
AEO HYENA HYENA V1	2424
COMET 64x64m1	2512
AEO ELEPHANT 160V1	2628
AEO ORANGE ORANGE2xV1	2732
AEO KOLUUS KOLUUS2xV1	2792
AEO LOTUS LOCUS 128P128L4xV1	3048
ASCPN 128x12	3052
AEO SKINNY SKINNY4xV1	3124
AEO FORKAE SAFFORCAE4xV1	3972
AEO ORBITDA ORBITDA128V1	4104
AES GCM 128P128L	4120
AEO SPOC 128P128L4xV1	4232
AEO PHOTON BEETLE PHOTONBEETLE4xV1	4304
AEO SPK 128V1	4332
AEO SPARKLE SCHWAGM128V1	4552
AEO KODAK V1	4888
AEO ISAP ISAP4xV1	4968
DRAGON 128	4996
WAGE 128x1	5112
	5116
	5608
	5888

Project Name	Count
AEAD-SAGEBASE-SAGEBASE128M4041	4080
AEAD-THYANUS-738	6489
AEAD-ANOT-MOT128V1	11024
AEAD-SIMPLE-SIMPLEMOT13232V1	11977
AEAD-GCM-MED-13	13856
AEAD-ESTATE-BESTPETHREAD128V1	14908
COMET-128mem1	14930
AEAD-ESTATE-BESTPETHREAD128V1	16189
AEAD-CON-128V1	18276
AEAD-CON-128V1	23527
AEAD-CON-128V1	24238
AEAD-SATURNI-SATURNI128V1	29001
AEAD-SATURNI-SATURNI128V1	40970
AEAD-CON-128V1	51241
AEAD-CON-128V1	51306
AEAD-CON-128V1	51422
AEAD-CON-128V1	60706
AEAD-CON-128V1	60855
AEAD-CON-128V1	62804
AEAD-CON-128V1	75632
AEAD-CON-128V1	81462
AEAD-CON-128V1	87948
AEAD-CON-128V1	107206
AEAD-CON-128V1	130560
AEAD-CON-128V1	132494
AEAD-CON-128V1	180903
AEAD-CON-128V1	225494
AEAD-CON-128V1	358052
AEAD-CON-128V1	414366
AEAD-CON-128V1	477345
AEAD-CON-128V1	615147
AEAD-CON-128V1	700012
AEAD-CON-128V1	723272
AEAD-CON-128V1	793263
AEAD-CON-128V1	1027524
AEAD-CON-128V1	1457446
AEAD-CON-128V1	2113267

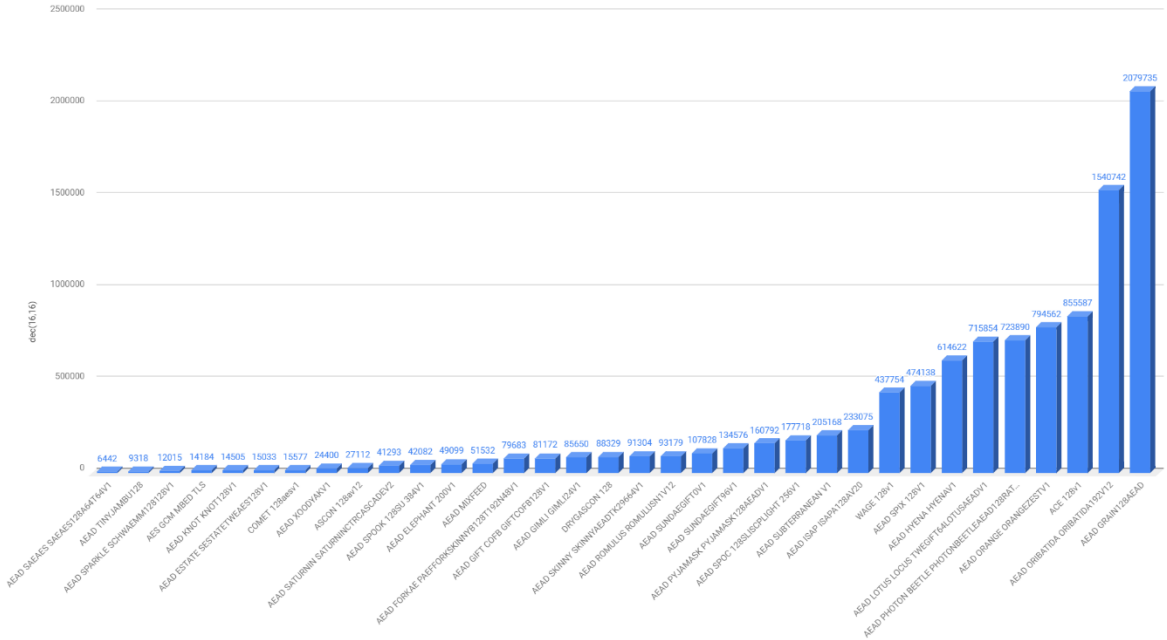
STM32F303VC M4 AEAD / dec(8,8)



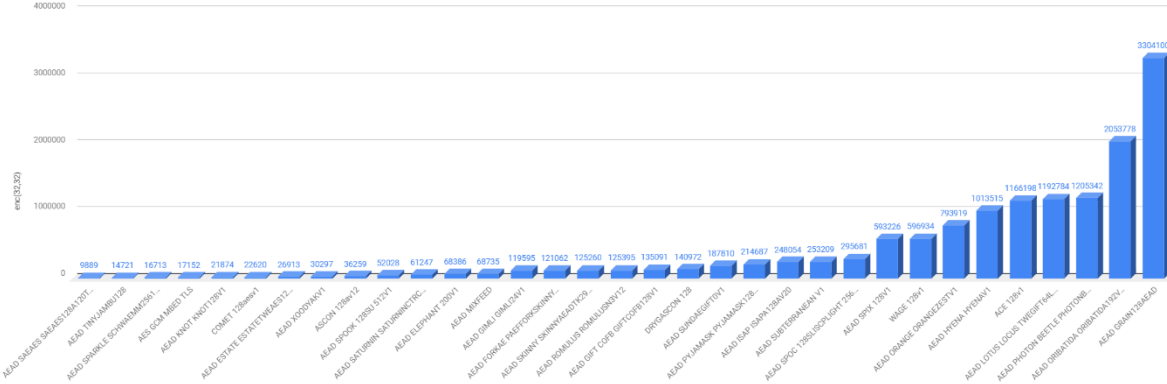
STM32F303VC M4 AEAD / enc(16,16)



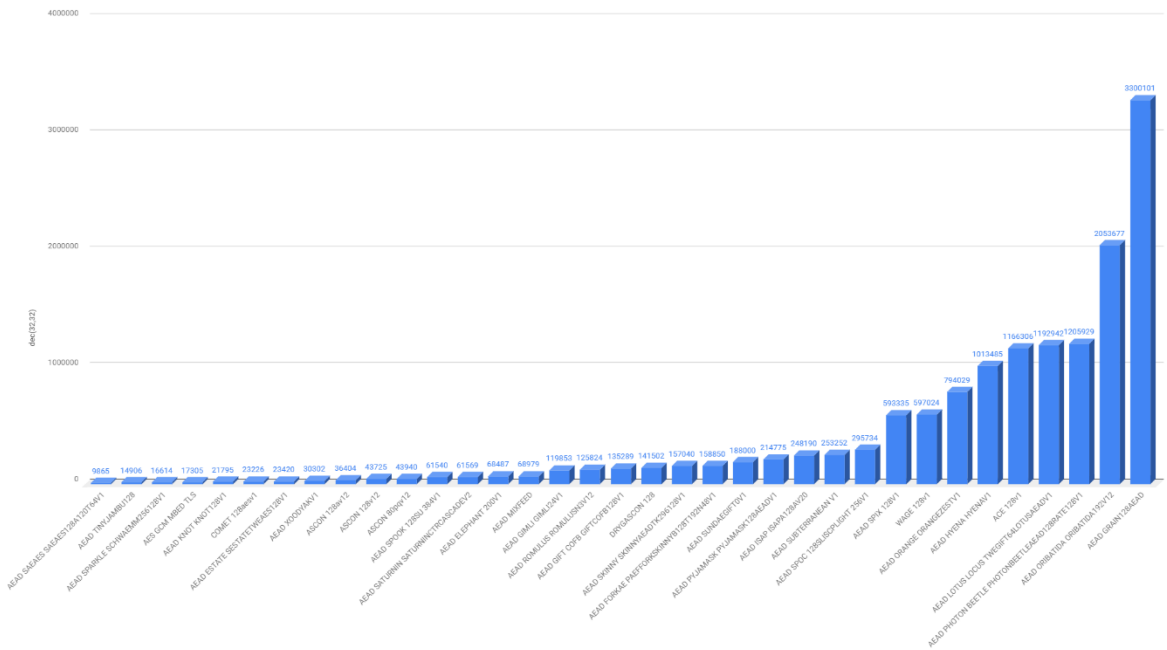
STM32F303VC M4 AEAD / dec(16,16)



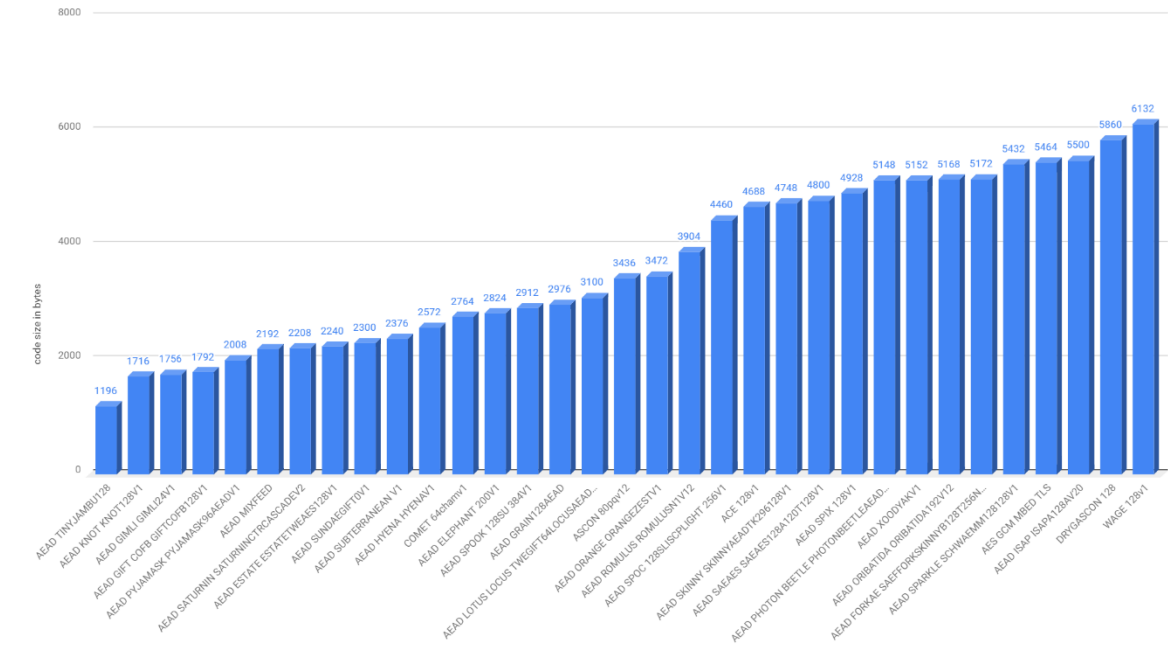
STM32F303VC M4 AEAD / enc(32,32)



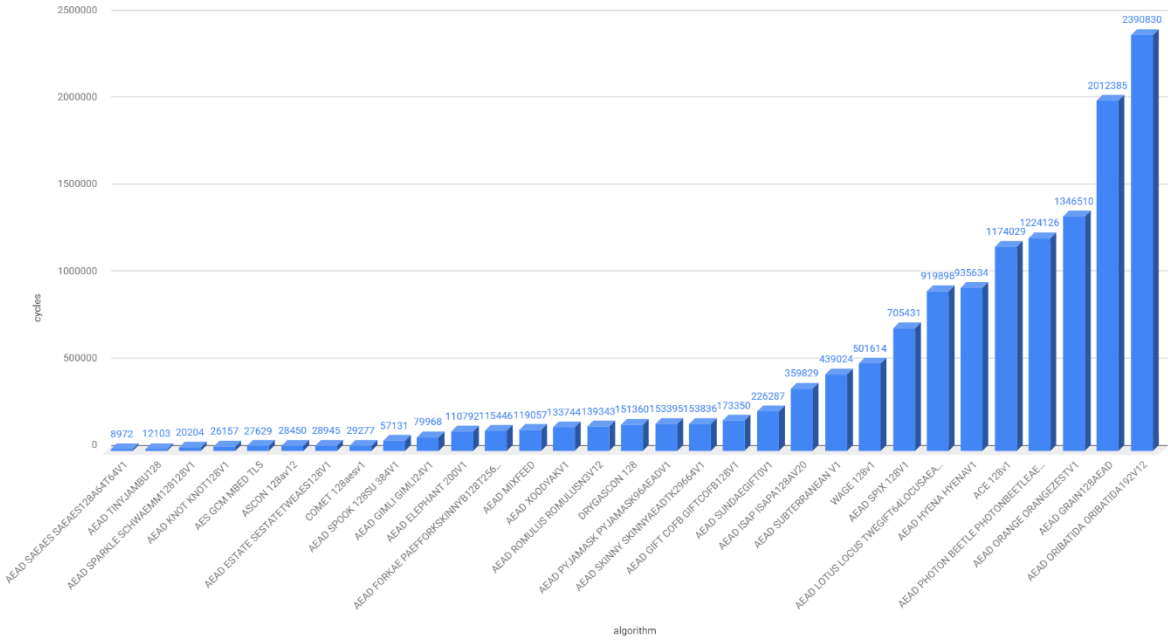
STM32F303VC M4 AEAD / dec(32,32)



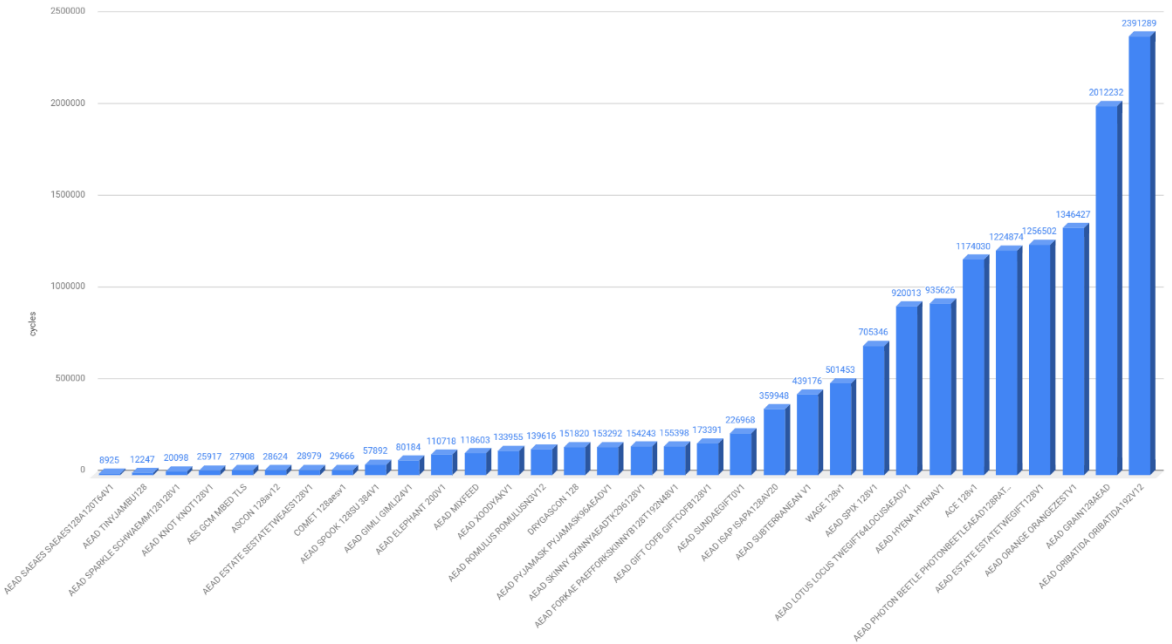
STM32F051R8 M0 AEAD code size(Os)



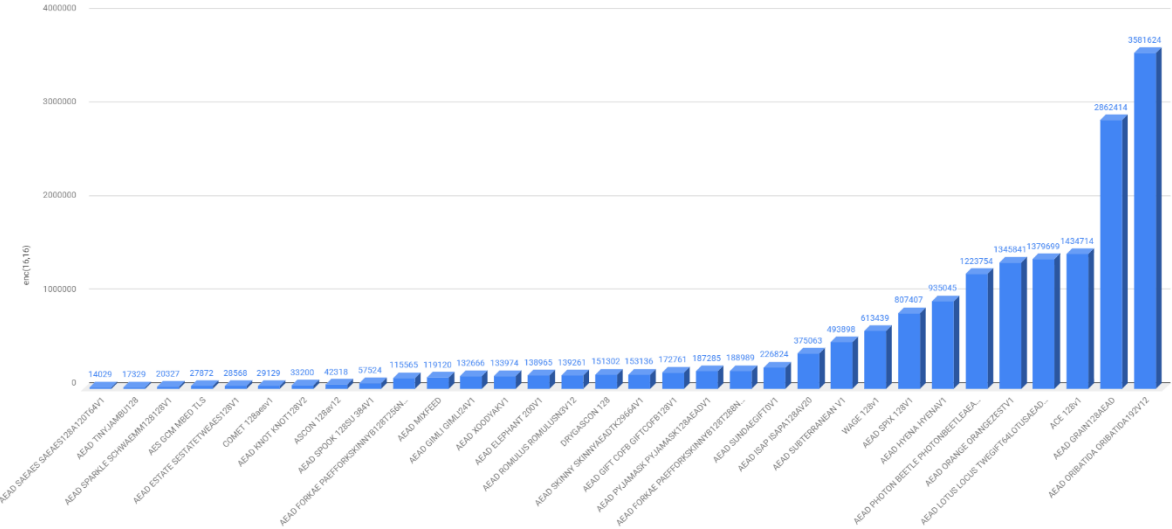
STM32F051R8 M0 AEAD / enc(8,8)



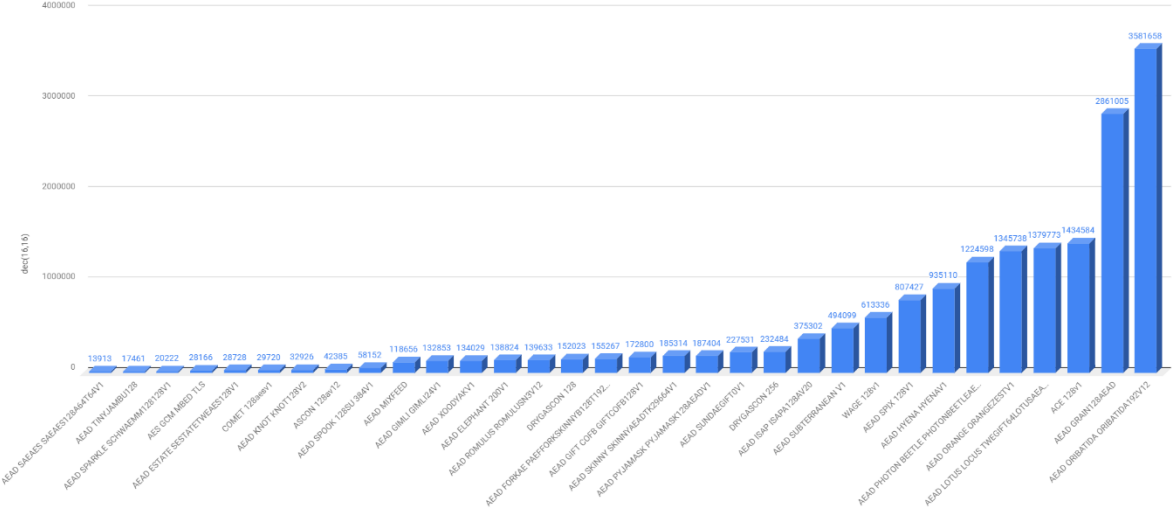
STM32F051R8 M0 AEAD / dec(8,8)



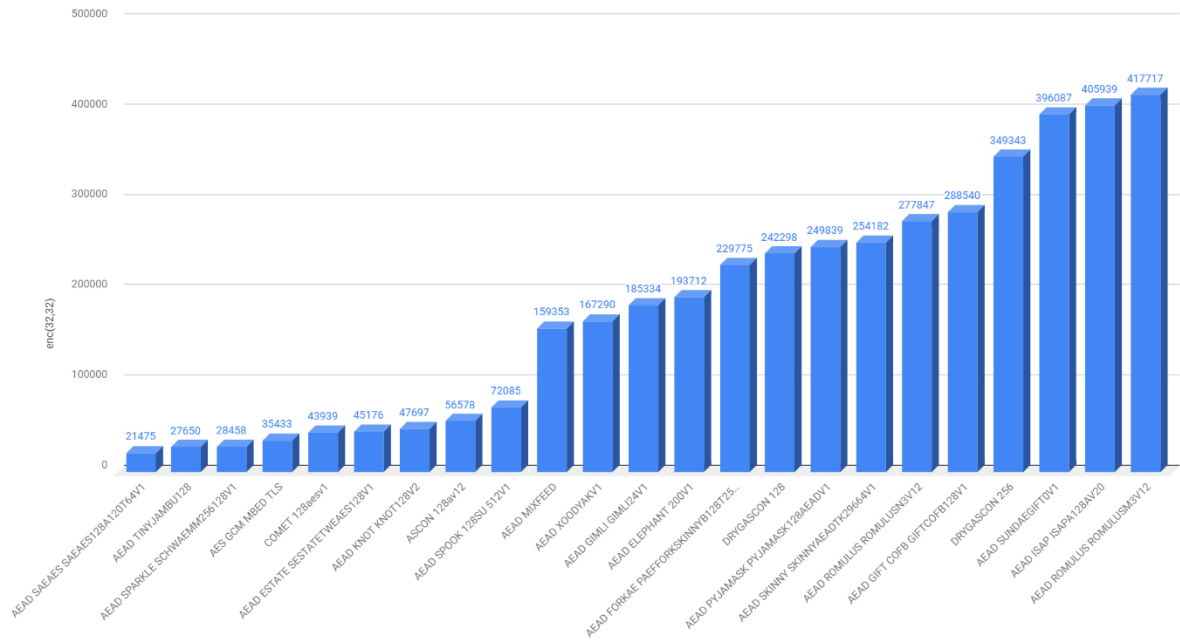
STM32F051R8 M0 AEAD / enc(16,16)



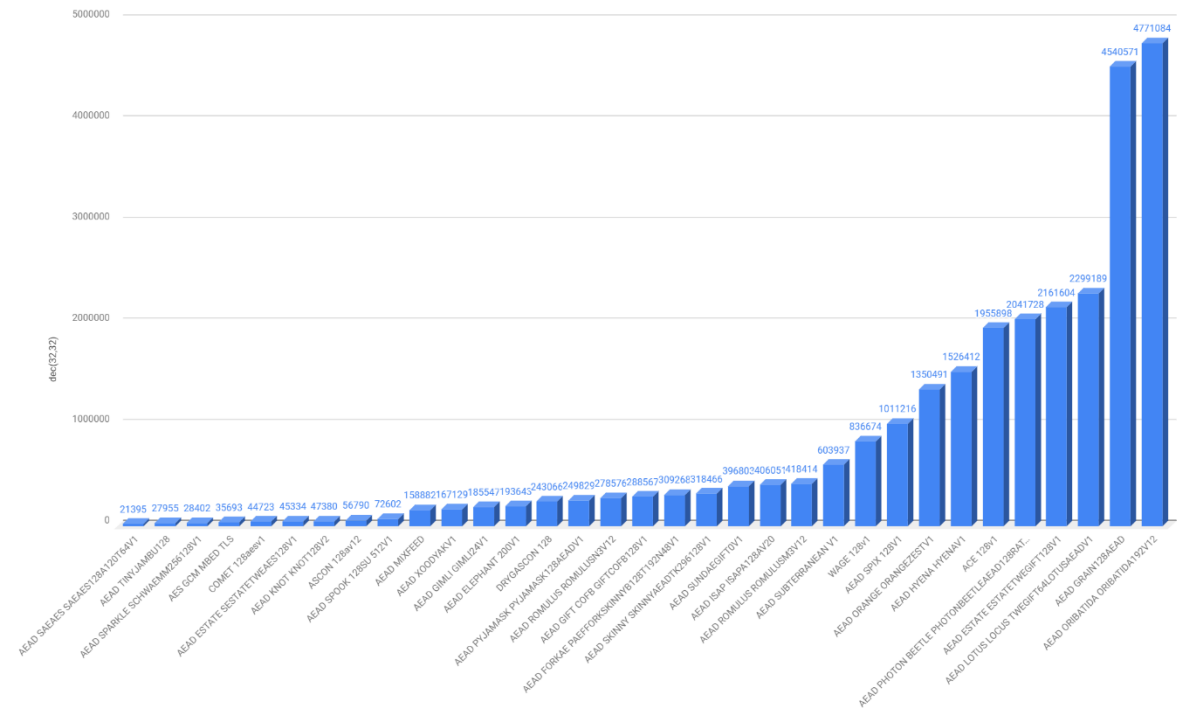
STM32F051R8 M0 AEAD / dec(16,16)



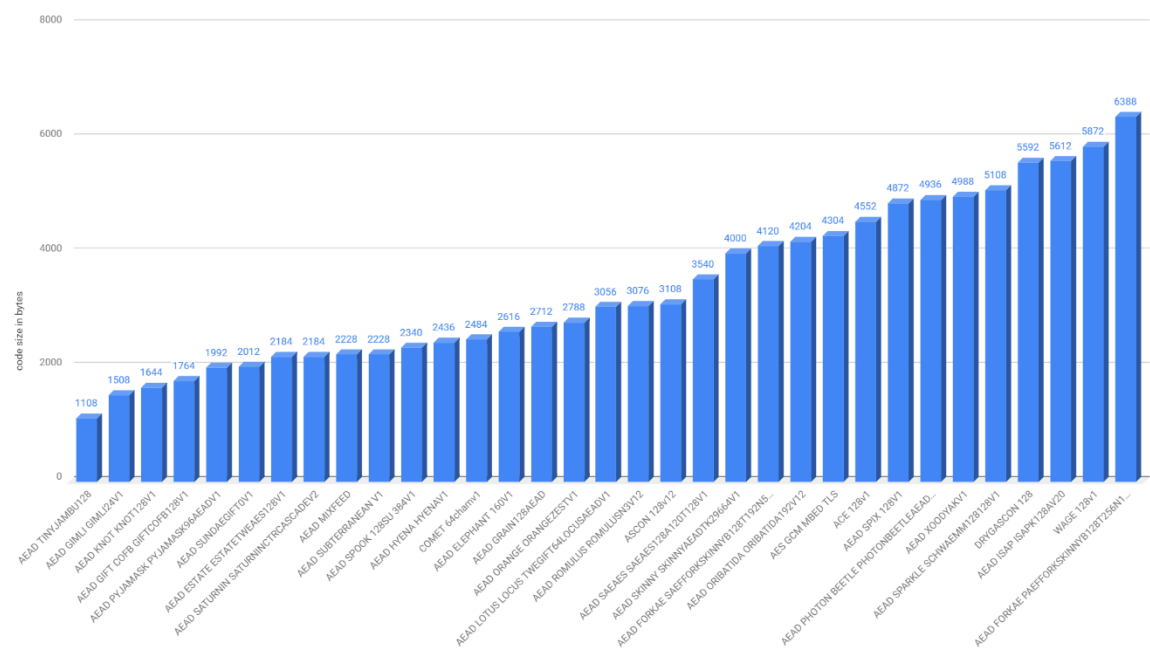
STM32F051R8 M0 AEAD / enc(32,32)



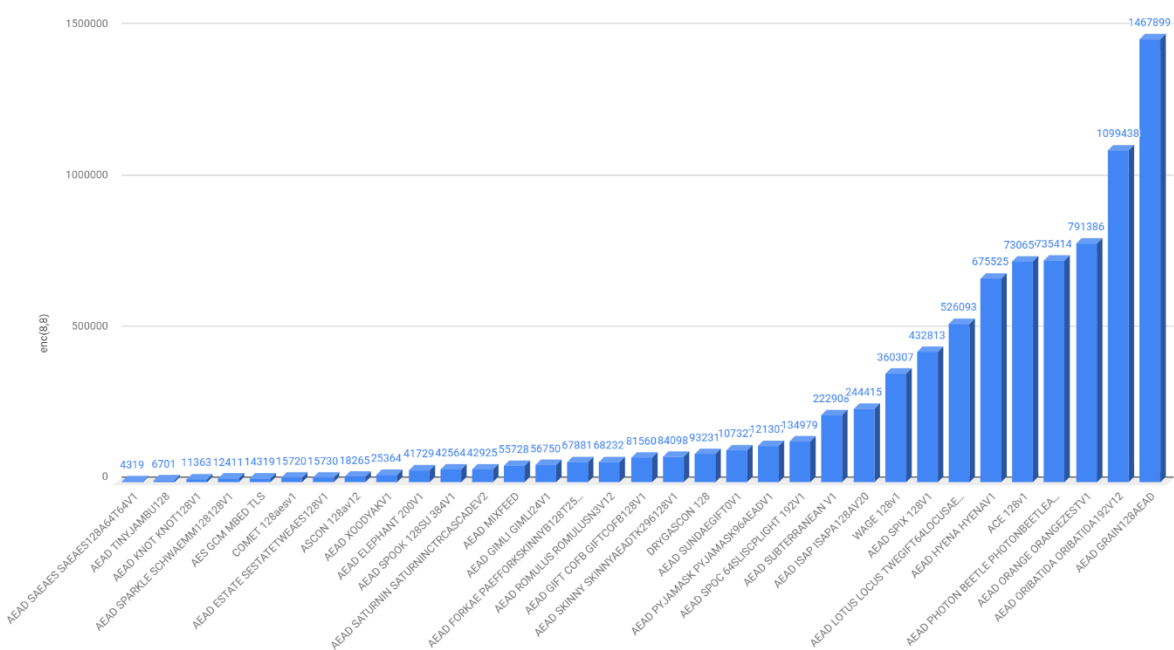
STM32F051R8 M0 AEAD / dec(32,32)



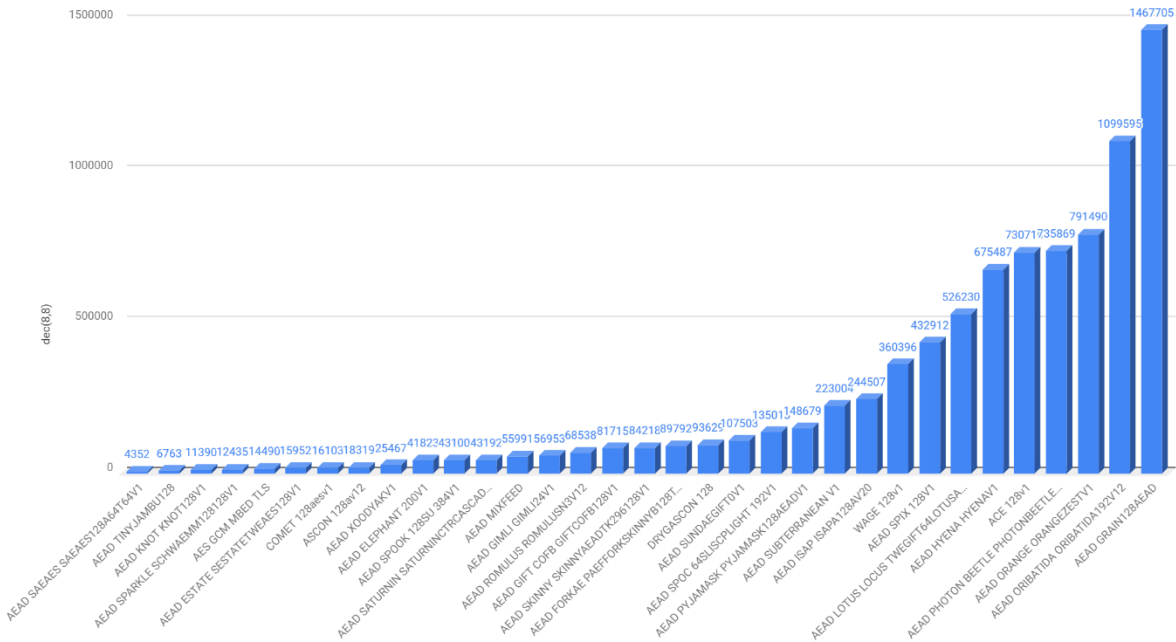
STM32f100RB M3 AEAD code size(0s)



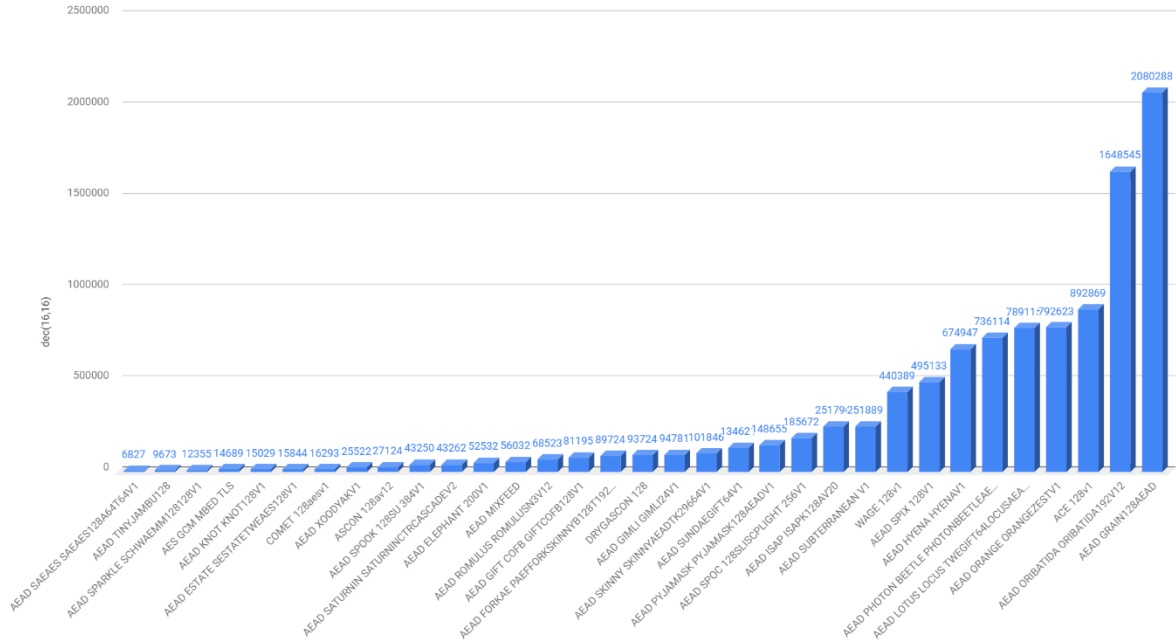
M32f100RB M3 AEAD / enc(8,8)

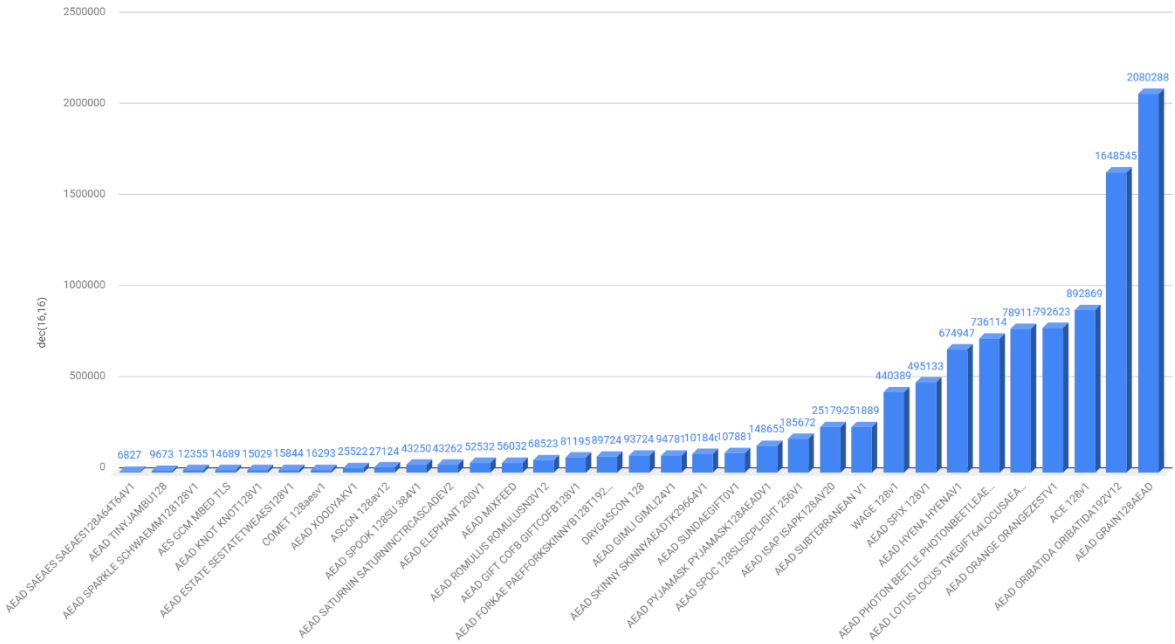


STM32f100RB M3 AEAD / dec(8,8)

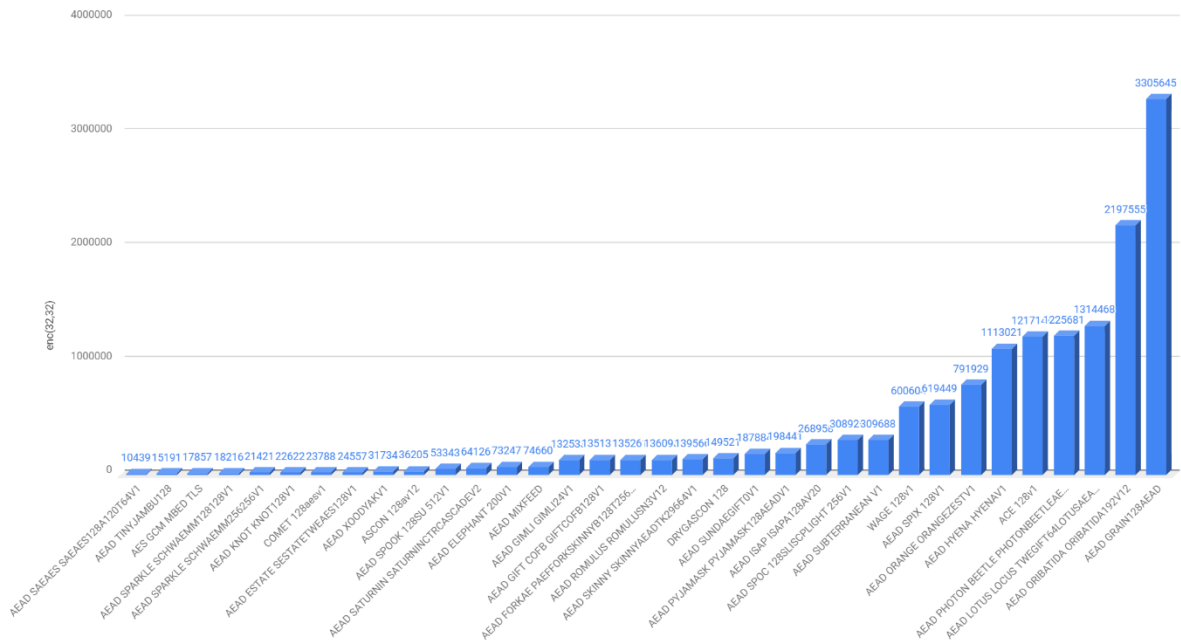


STM32f100RB M3 AEAD / enc(16,16)





STM32f100RB M3 AEAD / enc(32,32)



STM32f100RB M3 AEAD / dec(32,32)

