

Table 1: Classical and quantum collision attacks on AES-MMO, AES-MP, Grøst1

Collision attacks on AES-MMO and AES-MP						
Settings	Attack	Rounds	Time	c-Memory	qRAM	Source
Classic	Dedicated	5	2^{56}	2^4	0	[MRST09]
	Dedicated	6	2^{56}	2^{32}	0	[GP10,LMR ⁺ 09]
Q-Model I	Dedicated	7	$2^{42.50}$	0	2^{48}	[HS20]
	Dedicated	7	$2^{45.4}$	0	2^{16}	Section 4
	Generic	all	2^{56}	0	2^{16}	[BHT98]
	Generic	all	$2^{42.66}$	0	$2^{42.66}$	[BHT98]
Q-Model II	Dedicated	7	$2^{59.5}$	0	0	[HS20]
	Dedicated	7	$2^{45.8}$	0	0	Section 5
	Generic	all	$2^{51.2}$	$2^{25.6}$	0	[CNS17]
Collision attacks on Grøst1-512						
Classic	Dedicated	3	2^{192}	2^{64}	0	[Sch11]
	Dedicated	4	2^{128}	2^{64}	0	Section 6
	Dedicated	5	2^{240}	2^{64}	0	Section 6
Q-Model I	Dedicated	4	$2^{88.4}$	0	2^{16}	Section 6
	Dedicated	5	$2^{200.4}$	0	2^{16}	Section 6
	Generic	all	2^{248}	0	2^{16}	[BHT98]
	Generic	all	$2^{170.7}$	0	$2^{170.7}$	[BHT98]
Q-Model II	Dedicated	4	$2^{89.3}$	0	0	Section 6
	Dedicated	5	$2^{201.3}$	0	0	Section 6
	Generic	all	2^{205}	$2^{102.4}$	0	[CNS17]
Semi-free-start collision attacks on Grøst1-256						
Classic	Dedicated	6	2^{120}	2^{64}	0	[Sch11]
	Dedicated	6	2^{112}	2^{64}	0	Section 6
Q-Model II	Dedicated	6	$2^{91.8}$	0	0	Section 7
	Generic	6	$2^{102.4}$	$2^{51.2}$	0	[CNS17]

Q-Model I and II are quantum settings with qRAM and without qRAM, respectively.