

# Broken hash functions beyond the birthday paradox

	Year	Collision
MD5	2013	$2^{24}$ evaluations ( $2^{39}$ with prefix)
SHA-1	2015	$2^{57}$ evaluations

# Message Authentication Code