Quantum Collision Finder

	Classical algorithms	Quantum algorithms
Block cipher **E: K × X → X** exhaustive search	$O(\,|K|\,)$	$O(\,|K|^{1/2}\,)$
Hash function **H: M → T** collision finder	$O(\,|T|^{1/2}\,)$	$O(\,|T|^{1/3}\,)$