In October of 2012 on the NIST Hash mailing list, researchers estimated
that practical SHA-1 collision attacks would be plausible by 2018. On
August 5 of 2015 NIST updated their policy on hash functions to say
agencies should stop using SHA-1 for all applications that require
collision resistance. Our research extends existing algorithms for finding
collisions by parallelizing the attacks. We have constructed a 12 node
cluster from commodity hardware and the OpenMPI library. Using our
cluster, we have investigated SHA-1 collision attacks in a parallel
computing environment. Our results show that attacks based on exhaustive
search benefit the most from parallel computation, although are not yet
practical. In addition, we show that collision attacks based on properties
of the SHA-1 hash show significant speedup and that widespread successful
collision attacks will almost certainly be possible before 2018.