

Supplemental Reading for SHA1 Attacks

During the 2000s, a bunch of [theoretical attacks](#) against SHA1 were [formulated](#) and some [partial collisions](#) were demonstrated. In early 2017, the first [full collision of SHA1](#) was published.