

This technical report has been superseded by our Usenix Security 2003 paper, available at

<http://www.cs.rice.edu/~scrosby/hash/>

In addition to the attacks, the final paper version also discusses solutions. The URL above also includes source code for our universal hashing library.