

## Re: SHA1 broken

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-02/3150.html>

---

*tomstdenis\_at\_gmail.com*

**Date:** 02/16/05

Date: 16 Feb 2005 09:24:36 -0800

Paul Rubin wrote:

> *"tomstdenis@gmail.com" <tomstdenis@gmail.com> writes:*  
> > *It means a given characteristic through the cipher cannot have a*  
> > *probability of occurring above a given threshold. Early today I*  
> *quoted*  
> > *2<sup>-72</sup> [iirc] for 4 rounds... that means any four round differential*  
> > *pattern would hold 2<sup>-72</sup> of the time.*  
>  
> *OK, say I check for the pattern 2<sup>20</sup> times. Does that give me a*  
> *2<sup>-52</sup>*  
> *chance of spotting the differential? Is that a distinguishing*  
> *attack?*

The distinguisher works like this, if  $A \Rightarrow B$  [these are deltas] with high probability than the values that differ  $[p \text{ xor } q == A]$  to cause  $A \Rightarrow B$  are known.

When the diff occurs only a limited subset of keys are possible.

So when I rotate through all  $2^{63}$  inputs  $p$  and their  $q = p \text{ xor } A$  I expect to see one output difference  $[B]$  more than others. For the specific value of " $p$ " that that occurs I know probable keys.

Therefore, if all output differences are equally probably of resulting for all  $p$  then the attack can't work.

Gets worse than that though, because the attack usually exploits the last round in a chain, e.g..

$A \Rightarrow B \Rightarrow C \Rightarrow D \Rightarrow E$

So  $A \Rightarrow E$  is what you see, you expect  $B, C, D$  because you're really attacking  $A \Rightarrow B$ . So... if  $B$  didn't happen but you still got  $E$  then you have "noise".

Then it gets worse than that though.

sci.crypt: Re: SHA1 broken

Suppose you don't care what B,C,D are and just want a distinguisher. Then you have a "differential" [or hull... though hull was used in linear crypto the idea applies].

But we change it a bit. We only want  $A \Rightarrow D$  to be a sure thing. So B,C we don't care provided we get  $A \Rightarrow D$ . Now if  $A \Rightarrow D$  occurs enough then we can guess the E key and divide and conquer the sucker [e.g. correct keys would show  $A \Rightarrow D$  more often].

...

wide trails really only provably stop the case of  $A \Rightarrow E$  where B,C,D are fixed. In practice it makes hulls harder too since the # of members of the  $A \Rightarrow D$  set are fixed and the sum of their probabilities is still going to be low [because they're all wide trails].

Tom