

Re: SHA-1 Variants

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-05/5501.html>

From: Tom St Denis (tomstdenis_at_iahu.ca)

Date: 05/31/04

Date: Mon, 31 May 2004 12:32:08 GMT

Jim Steuert wrote:

- > I have attempted to create secure variants of SHA-1's symmetric 160-bit
- > cipher
- > by adding additional multipermutations mixers to it's round function,
- > which do not adversely affect the strong cryptanalysis of SHA-1.

Pardon me. Why? You said yourself SHA-1 is secure. Wouldn't a variant specially one of the same size be just undue risk?

- > The "safe" variant of SHA-1 I call SHAMOD and a sample round is the
- > following:

>

> $T = (A \ll 5 / A \gg 27) + ((B \& C) / ((0xffffffff \wedge B) \& D)) + E + *WP++ + 0x5a827999;$

Why not just use the \ll and \gg for rotation? That makes it way easier to read.

> $NEW ==> T = T + ((C \ll 13 / C \gg 19) \wedge B) + ((C \ll 10 / C \gg 22) \wedge D) + ((B \ll 11 / B \gg 21) \wedge D);$

> $E = D; D = C; C = (B \ll 30 / B \gg 2); B = A; A = T;$

Rewrote for the sake of humanity.

$T = T + (C \ll 13 \wedge B) + (C \ll 10 \wedge D) + (B \ll 11 \wedge D);$

Right away I can see that the lsb of D is canceled out.

- > Does anyone have an opinion as to the validity of this particular method
- > of "adding"
- > to a hash or cipher without invalidating it's cryptanalysis.

Well differential trails through the design depend on the function itself [this isn't a wide-trail design afterall]. So your change [which makes SHA much slower] would have to be analyzed on it's own.

- > Note, this is not the same as the discredited (MITM attackable)
- > double encryption, rather, adding complexity to the round functions.
- > This is
- > taking an already strong cipher and making it "stronger". Why bother?

sci.crypt: Re: SHA-1 Variants

> *For one, computers are much faster than when SHA-1 was invented (1993).*

First, SHA-256 is what people should be starting with in new applications. Second, prove that your mods actually do "make it stronger". Essentially [my guess] is you would have to drop your design to less than 40 rounds [say 40 rounds for the purpose of this thread] to get the same speed as SHA-1 on an Athlon.

So are 40 rounds of your design as secure as 80 rounds of SHA-1?

> *In like manner, I created a 224-bit variant called SHAMODX (7 digest
> vars of 32-bits each)
> I realize that this is a bit shakier than simply modifying a known hash,
> but the
> cipher structure and form of cryptanalysis would be the same.*

Um SHA-224 already exists. Do your homework.

> *(there are also more rounds $4*4*7 \Rightarrow 112$ versus $4*4*5 \Rightarrow 80$ for SHA-1).*

SHA-224 has only 64 rounds. So your design is faster or slower?

>
> $T = (A \ll 5/A \gg 27) + ((B \& C) / ((0xffffffff^B) \& D)) + *WP++ + 0x5a827999;$
> $T = T + ((B \ll 13/B \gg 19)^D) + ((C \ll 10/C \gg 22)^F) + ((D \ll 11/D \gg 21)^E);$
> $T = T + ((E \ll 29/E \gg 3)^C) + ((F \ll 18/F \gg 14)^B);$
> $T = T + ((B \ll 19/B \gg 13)^F) + ((C \ll 11/C \gg 21)^E) + ((D \ll 23/D \gg 9)^B);$
> $T = T + ((E \ll 6/E \gg 26)^C) + ((F \ll 17/F \gg 15)^D);$
> $T = T + ((B \& F) \wedge (C \& D) \wedge ((C^D) \& E)) + G;$
> $G = F; F = E; E = D; D = C; C = (B \ll 30/B \gg 2); B = A; A = T;$

Where do these rotation counts come from? Have you timed this? Can you prove anything about it?

> *The sample code for SHAMODX is incomplete in that it does not include a
> revised key schedule
> algorithm. It needs to be improved by using SHA-1 itself to generate the
> key parts W[0-111],
> rather than the old SHA-1 key expansion algorithm.*

As a developer if I have to lug around SHA-1 [a standard] just to use SHAMODX [not standard] I'd give you the finger and use SHA-256 ;-)

> *Again, does anyone have an opinion as to the "security" of extending SHA-1
> in this manner?*

Well your designs seem slower, have no claims of security that are valid and otherwise show exactly why I'm right about going after newbies.

See I go after newbies and pounce on them todo their homework, be patient, read, read, read and then try to come up with ideas that extend

sci.crypt: Re: SHA-1 Variants

what they have learned over the course of their study. I routinely shoot down out-of-left-field newbie designs by pointing out obvious flaws and telling them to stop designing stuff until they can learn to use a PDF/PS reader.

Then a few people backlash calling me rude and what have not.

Well see people, this is EXACTLY what I'm talking about. This isn't Jim's first appearance on sci.crypt and look what we have here. Yet another useless poorly thought out "idea". Instead of using his time to learn more about the field and proposing ideas that at least stand a chance of being useful he spends his time convincing himself he doesn't need the meds [cuz only sick people need meds] and writes more ciphers/ashes.

Tom