From: Apon, Daniel C. (Fed)
To: (b) (6)
Subject: RE: hash-and-sign
Date: Monday, June 8, 2020 12:36:00 PM

Ummm. I guess it's possible you could play with the cost of AES vs SHA to shorten the length of signatures mildly, yes. (I think that was what you are asking?)

I don't think it's necessary to do that

From: Daniel Smith (b) (6)
Sent: Friday, June 5, 2020 9:22 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: hash-and-sign

I bet that question wasn't clear. hash and sign... message m, hash H, verifier V. adversary tries to get a collision by randomly generating sigs s and messages m to get H(m)=V(s). If there are 250 bits of entropy in the verification string space, then collisions should cost on the order of 2^125, and if the min cost of verification or hashing is 2^18, then you get 2^(125+18)=2^143. So do you think that this is reasonable or bunk? Or course, if all symmetric is 2^15 for you, then there is no difference, but let's suppose that one SHA-3 hash costs as much as one SHA-3 hash for a moment...

On Fri, Jun 5, 2020 at 8:11 AM Daniel Smith (b) (6) wrote:

> I posed the same question to Ray. Let me ask it in a different way. Would you be okay with signatures of length 250, assuming sha-3 takes 2^18 bit operations? Level I, I mean.
>
> On Fri, Jun 5, 2020 at 03:33 Apon, Daniel C. (Fed) <daniel.apon@nist.gov> wrote:
>
> > Is this question about 2^128 vs 2^143?
> >
> > If so, then multiply in the bit operations to compute the hash (i.e. times the number of hash guesses)
> >
> > From my end, every symmetric primitive takes 2^15 bit operations, and no one will convince me anything else truly matters
> >
> > ---
> >
> > **From:** Apon, Daniel C. (Fed)
> > **Sent:** Friday, June 5, 2020 3:28 AM
> > **To:** Daniel Smith (b) (6)
> > **Subject:** RE: hash-and-sign
> >
> > "I just want to get your take on this."
> >
> > As far as I can tell, ALL practical lattice signatures in the hash-and-sign paradigm, e.g. Falcon, have a security proof that treats this issue explicitly

I.e. not being children, they take the output length of their hash function (where collision resistance is required) to be 2 * security_parameter bits long. (Level 1 = 256, Level 5 = 512)

Is that not enough somehow?

From: Daniel Smith (b) (6)
Sent: Thursday, June 4, 2020 3:56 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: hash-and-sign

Hi, Daniel,

I wanted to ask your opinion on our measurement of security for hash-and-sign signatures. We have declared our security level I stuff as being as hard to break as AES-128, so 2^143 bit operations. I am curious if you think that this is a relevant metric for collision attacks on the hash function for hash-and-sign signatures. My thinking is that it is not reasonable to measure collision resistance to 2^143, since even modeling the signature algorithm as a random oracle, we get collisions based on the size of the codomain. So even perfect AES can't do better. I just want to get your take on this.

Cheers,
Daniel