From: Kelsey, John M. (Fed)
To: Perlner, Ray A. (Fed); Cooper, David (Fed)
Subject: Re: Paper questions
Date: Tuesday, May 24, 2022 8:44:55 PM

Ray,

Yes, I think we should split all the cost calculations for the parallel collision search, multitarget attacks, etc., into their own section, and then reference them as appropriate.

--John

> On 5/24/22, 19:02, "Perlner, Ray A. (Fed)" <ray.perlner@nist.gov> wrote:
>
> Ok. I put in cost formulas for k=3 and 4 in both the free memory and the square root memory cost models. Do you think the section on “batched multitarget multicollision” search (or possibly the whole section on parallel collision search and related techniques) should move to the
> “optimizations and cost estimates” section?

> **From:** Kelsey, John M. (Fed) <john.kelsey@nist.gov>
> **Sent:** Tuesday, May 24, 2022 5:32 PM
> **To:** Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>
> **Subject:** Re: Paper questions
>
> Good. I’m trying to work out how to summarize the attacks in the table. (Right now I have a bunch of blanks.). Probably we want to specify compression function computations (or the cost equivalent using our memory model) as the cost. I was thinking in terms of listing the cost of each distinct step independently, but it might be better to just list a single cost. We should probably also mention the minimum number of signatures we must see from the key to be able to mount our attack. Basically, if we can manage to fit 2^k keys into our diamond structure, we need to find 2^k keys with low-enough checksums that we can get a signature to work.
>
> Also, right now, we have a lot of high-level explanation and not much in-depth explanation. I’ve got the introduction and conclusion pretty nailed down, and I’m planning to try to move some of the descriptions around to make everything flow better.
>
> --John
>
> > On 5/24/22, 17:18, "Perlner, Ray A. (Fed)" <ray.perlner@nist.gov> wrote:
> >
> > Hi John,
> >
> > The rules for submission are here: https://2022.pqcrypto.org/index.html#cfp

Relevant sentences for page limit:

Submissions must not exceed 20 pages, including references and excluding appendices, in a single column format in 10pt fonts using the default llncs class without adjustments.

If the submission is accepted, the length of the final version will be at most 20 pages including references and at most an additional 10 pages for appendices, in the llncs class format.

Btw should I add a cost estimate for the cost of batched 3-collisions (I don't think that's ever going to be a significant cost compared to the other steps, but it might be good to have a concrete number for it) and costs for 3 collisions and 4 collisions ignoring memory costs? If so, I think I can type them in around 7 or 8 pm.

--Ray

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Tuesday, May 24, 2022 4:51 PM
To: Cooper, David A. (Fed) <david.cooper@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Paper questions

Guys,

What's the page limit? Are we going to need to move things out to appendices or something?

Right now I think the attack details are in an appendix. I'm going to try to move some stuff around to make the organization make more sense.

--John