

From: [Miller, Carl A. \(Fed\)](#)
To: [Moody, Dustin \(Fed\)](#); [Kelsey, John M. \(Fed\)](#); [internal-pqc](#)
Subject: Re: Style conventions
Date: Monday, June 15, 2020 1:52:27 PM

Hi all --

Agree that consistency in verb tenses is good for easy reading. Here's a possible way to uniformize:

- Anything that doesn't happen at a definite point in time (e.g., "the user computes her key via a hash function") should be in the present tense. And, any references to things that happen within a protocol specification (e.g., "the authors use the Fiat-Shamir transformation") should be in the present tense.
- Anything that does occur at a definite point in time (e.g., "the authors retracted ten of their parameter sets") should be past/present/future tense appropriately (relative to the time we're planning to release our report).

I'm not entirely sure about references to changes made in round 2 – possibly those could either be past or present tense, depending on the setup ...

-Carl

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, June 15, 2020 at 10:53 AM
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: Style conventions

John,

Thanks for noticing these sorts of things. Please just correct them as you find them. In particular, I agree with you about using "first round" is usually better than round 1. I also agree that it's better to write out small numbers like seven or eight. For tense issues, yes, let's do as you described.

Dustin

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Monday, June 15, 2020 10:37 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Style conventions

Everyone,

I've noticed a couple inconsistencies in the way different people are writing their sections that will have to be ironed out sooner or later. The ones I've noticed so far:

- a. Different sections are written in different verb tenses—sometimes we're in the present tense, sometimes in the past tense, sometimes even in the conditional or future tense. We should try to make the verb tenses consistent. (It makes sense to refer to past things in the past tense and conditional things in the conditional tense, but it's jarring when the verb tense changes mid-paragraph because there were two different writers....)
- b. Do we want to call it "first round, second round, third round" or "round 1, round 2, round 3?" We ***can*** do both, but I think the document will flow better if we use a consistent phrase (I think nth round sounds better than round n, though at least after this we won't have an algorithm named "round n" to deal with.
- c. I think it looks better to spell out small numbers ("seven" instead of 7). It's not a big deal either way, but we should at least be consistent.

Thanks,

--John