From: Peralta, Rene (Fed)
To: (b) (6); Peralta, Rene C. (Fed)
Subject: Fw: primality paper
Date: Thursday, July 20, 2017 2:38:07 PM

From: Moody, Dustin (Fed)
Sent: Monday, June 12, 2017 2:09 PM
To: Peralta, Rene (Fed)
Subject: RE: primality paper

Rene,

I'll sign off on the WERB form whenever it gets here. If you submit it to a journal, it probably needs some more text added to it. A few minor comments for you below.

Dustin

p1 - The sentence "There are several widely-used methods for testing whether an odd number N, of unknown provenance, is prime." doesn't indicate that what you're actually testing is "prime, with a high degree of confidence". Could be explained a bit more, or explained why cryptographers only need "probably prime", and not just provably prime. This is also relevant to the third paragraph.

p1 - "Iterating r times yields a failure probability of (1/4)^r." Should this be "at most"?

p3 - The Output of Fig 2 states "a randomly chosen prime". as above, this might lead one to conclude the output is provably prime, which isn't the case.

p3 - 1st paragraph of sect 3: figure 2 -> Figure 2

p4 - section 2 -> Section 2

p4 - Theorem 1 statement: algorithm 2 -> Algorithm 2

p4 - is Table 3 supposed to be Figure 5?

p5 - In Figure 5, perhaps give give the upper bound on P(x) in terms of 2^- instead of e^-.

p5 - Perhaps cite something for the argument about elliptic curve algorithms can factor N if P is sufficiently semi-smooth?

p5 - Section 4. Perhaps explain why you are discussing smooth and semi-smooth before just defining them.

p5 - Any citations/explanations to help explain the cost estimates at the very bottom of p5?

p5 - Section 5 conists pretty much of definitions, with out a lot of explanation. Perhaps combine Sections 4 and 5 and add some explanation?

p6 - first paragraph of section 6. Why could you not do P=SHA512(u)||SHA512(u+1) until you get a prime of Type 1 (or Type 2)? The cost estimate says it should only be twice as expensive to generate a type 1 prime as a type 0 prime.

p7 - checking, P - r = 2(r+i)Q+1-r=(2Q-1)r+iQ+1. Why is it that P-r \leq kn ?

p7 - table 7 -> Figure 7

p7 - Section 7 and caption for Fig. 7. Is this expected run time, or actual run time? Why is it just expected if it wouldn't take very long to run?

p7 - Section title for Section 7 - sieving isn't talked about much in this section.

From: Peralta, Rene (Fed)
Sent: Friday, June 09, 2017 4:08 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: primality paper

Hi Dustin,

Yes. It is for WERB. I haven't decided whether to submit it to
a journal or make it into a NISTIR.

Thanks, Rene.

From: Moody, Dustin (Fed)
Sent: Friday, June 9, 2017 3:05 PM
To: Peralta, Rene (Fed)
Subject: RE: primality paper

Rene,
I forget – is this for WERB? Or something else?

Dustin

From: Peralta, Rene (Fed)
Sent: Wednesday, June 07, 2017 3:58 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: primality paper

Hi Dustin,

I am attaching the primality paper. Thanks for agreeing to be a reviewer.

I can discuss this with you anytime.

Rene.