From: Stephen Jordan
To: Glancy, Scott C. (Fed); Liu, Yi-Kai (Fed)
Subject: Re: WERB
Date: Thursday, November 10, 2016 2:18:07 PM

Thanks, Scott. I'll incorporate these improvements when it becomes possible to do so.

-Stephen

On 11/09/2016 05:47 PM, Scott Glancy wrote:
> Stephen and Yi-Kai,
>
> Here are a few comments about your article about post-quantum
> cryptography. I will also take care of the WERB approval.
>
> Maybe the magazine will give you advice about the accessibility of the
> article, because that is something that I am not qualified to talk about.
>
> I was surprised that you do not say much about cryptographic schemes
> that are resistant to all known quantum algorithms. I would consider
> talking about these schemes in more detail. I also think that a table
> of cryptographic schemes that lists schemes and tells whether the
> scheme is known to be broken by quantum computers and if so what
> algorithm breaks it.
>
> Here are some more detailed suggestions:
>
> Page 2: "A full description of the state of a quantum computer with
> only 80 qubits would already be too large to store on all the hard
> drives ever manufactured." Do you mean to store the amplitudes as
> double precision numbers?
>
> Page 2: "... current prototypes of universal quantum computers use
> only tens of qubits." I am not aware of an existing universal quantum
> computer with tens of qubits. Can you give a citation?
>
> Page 4: "After a number of queries small compared to \sqrt{s}, one
> will not encounter any pair x, y such that f(x) = f(y) and
> consequently one will have learned nothing about the period." This
> sentence is confusing. Does this apply only to classical algorithms?
> Is this supposed to support the claim that "one requires exponentially
> many queries"? Why do you mention \sqrt{s}? Is it impossible to find
> collision or just unlikely? Not finding a collision in \sqrt{s}
> queries is not sufficient to claim that one needs exponential queries.
>
> Page 5: "In a hidden shift problem, we are given oracle access to some
> function f, and we know that f(x) = g(x+s) for some fixed known
> function g and unknown shift s." For all x?
>
> Page 8: "In particular, many of the security proofs for lattice-based
> cryptosystems make use random samples from certain periodic
> distributions over R^n, as well as the Fourier transforms of these
> periodic distributions." needs "of" between "use" and "random".

>
> Page 10: "A number of promising public-key cryptosystems hoped to be
> resistant to quantum attack have been proposed." There is confusion
> of passive voice and past-tense. Do you mean that "people used to
> hope" or that "people now hope"?
>
> Scott
>
>
>
> On 11/02/2016 09:34 AM, Jordan, Stephen P (Fed) wrote:
>> Thanks, Scott. I have attached the current draft.
>>
>>
>> Best regards,
>>
>>
>> Stephen
>>
>>
>>
>>
>> ---
>> *From:* Scott Glancy <scott.glancy@nist.gov>
>> *Sent:* Thursday, October 27, 2016 9:51 PM
>> *To:* Jordan, Stephen P (Fed)
>> *Subject:* Re: WERB
>>
>> Yes, I can do that.
>>
>> On 2016-Oct-27 14:29, Jordan, Stephen P (Fed) wrote:
>>> Hi Scott,
>>>
>>>
>>> Would you be willing to serve as division reader for a magazine article
>>> that Yi-Kai and I are writing about post-quantum cryptography?
>>>
>>>
>>> Best regards,
>>>
>>>
>>> Stephen
>>>
>>>
>