From: Liu, Yi-Kai (Fed)
To: Jordan, Stephen P (Fed)
Subject: Re: WERB?
Date: Tuesday, November 1, 2016 9:37:43 PM
Attachments: cryptanalysis2.bib
cryptanalysis2.tex
cryptanalysis2.pdf

Great, thanks. Here is an updated version with my changes.

Cheers,

--Yi-Kai

From: Jordan, Stephen P (Fed)
Sent: Thursday, October 27, 2016 4:28:31 PM
To: Liu, Yi-Kai (Fed)
Subject: Re: WERB?

Sounds great. Here's the source. I'll add you as an author and subtract you as a reader in WERB.

-Stephen

From: Liu, Yi-Kai (Fed)
Sent: Thursday, October 27, 2016 4:26 PM
To: Jordan, Stephen P (Fed)
Subject: Re: WERB?

All right, I'll see if I can write something while keeping it at a general audience level. When you get a chance, can you send me the tex file? You can still keep editing it, and merge in my changes later.

Thanks!

--Yi-Kai

From: Jordan, Stephen P (Fed)
Sent: Thursday, October 27, 2016 2:46:35 PM
To: Liu, Yi-Kai (Fed)
Subject: Re: WERB?

Overall, I think it would be awesome to beef up the paper with such material, provided it can remain accessible to a "general computer science audience". Also, people might see the paper as more authoritative if a real computer scientist is a coauthor. Sorry I didn't contact you earlier. To be honest, I was pretty preoccupied and not thinking about this paper at all until recently.

-Stephen

From: Liu, Yi-Kai (Fed)
Sent: Thursday, October 27, 2016 1:42 PM
To: Jordan, Stephen P (Fed)
Subject: Re: WERB?

Ok. If you would like me to join as coauthor, I can write some stuff about exponential speedup using quantum walks, connections between the quantum Fourier transform and lattice problems, and the hardness of solving the non-Abelian HSP. Alternatively, I could simply WERB the paper for you. Either way is fine with me, just let me know...

Cheers,

--Yi-Kai

From: Jordan, Stephen P (Fed)
Sent: Thursday, October 27, 2016 12:38:15 PM
To: Liu, Yi-Kai (Fed)
Subject: Re: WERB?

I can ask Mike Mosca. Also, I think it is not essential that WERBing is done before I send in the manuscript. Even though the submission was solicited, it still has to go through a referee process, so there will be a significant amount of time to make changes after November 1.

-Stephen

From: Liu, Yi-Kai (Fed)
Sent: Thursday, October 27, 2016 12:36 PM
To: Jordan, Stephen P (Fed)
Subject: Re: WERB?

That's a pretty short deadline. Can you get an extension?

--Yi-Kai

From: Jordan, Stephen P (Fed)
Sent: Wednesday, October 26, 2016 4:20:40 PM
To: Liu, Yi-Kai (Fed)
Subject: Re: WERB?

Thanks! Incidentally, if you feel that there is an important subtopic that I have missed and you'd like to join as a coauthor I'd be open to that too. The only catch is that the first draft has to be submitted to IEEE by Nov 1.

-Stephen

From: Liu, Yi-Kai (Fed)
Sent: Wednesday, October 26, 2016 3:53 PM

To: Jordan, Stephen P (Fed)
Subject: Re: WERB?

Hi Stephen,

Sure, I can do that!

--Yi-Kai

____

From: Jordan, Stephen P (Fed)
Sent: Wednesday, October 26, 2016 12:58:13 PM
To: Liu, Yi-Kai (Fed)
Subject: WERB?

Hi Yi-Kai,

Recently I encountered Mike Mosca at a conference and he asked me to submit an article about quantum cryptanalysis to an upcoming special issue of magazine called IEEE Security and Privacy. I was wondering whether you would be willing to serve as my in-division WERB reviewer. I have attached my current draft. The instructions I received were that the article should be no more than 6000 words and should cite no more than 15 references. I'm at the limit for references but well below the word count limit. My impression from browsing past issues of the magazine (https://www.computer.org/security-and-privacy/) is that the articles should not be too technical.
IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
www.computer.org
David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
www.computer.org
David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

www.computer.org<http://www.computer.org>
The Community for Technology Leaders • IEEE Computer Society <http://www.computer.org/>
www.computer.org
The IEEE Computer Society is the world's premier organization of computing professionals, with rich offerings in publications, standards, certifications, conferences, and more.

David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
www.computer.org
David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
www.computer.org<http://www.computer.org>
David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

www.computer.org<http://www.computer.org>
The Community for Technology Leaders • IEEE Computer Society <http://www.computer.org/>
www.computer.org<http://www.computer.org>
The IEEE Computer Society is the world's premier organization of computing professionals, with rich offerings in publications, standards, certifications, conferences, and more.

David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
www.computer.org<http://www.computer.org>
David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
IEEE Security & Privacy<https://www.computer.org/security-and-privacy/>
www.computer.org<http://www.computer.org>
David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

www.computer.org<http://www.computer.org>
The Community for Technology Leaders • IEEE Computer Society <http://www.computer.org/>
www.computer.org<http://www.computer.org>
The IEEE Computer Society is the world's premier organization of computing professionals, with rich offerings in publications, standards, certifications, conferences, and more.

David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

www.computer.org<http://www.computer.org>
The Community for Technology Leaders • IEEE Computer Society <http://www.computer.org/>
The Community for Technology Leaders • IEEE Computer Society <http://www.computer.org/>
www.computer.org<http://www.computer.org>
The IEEE Computer Society is the world's premier organization of computing professionals, with rich offerings in

publications, standards, certifications, conferences, and more.

www.computer.org<http://www.computer.org>
The IEEE Computer Society is the world's premier organization of computing professionals, with rich offerings in publications, standards, certifications, conferences, and more.

David Nathans on Security Operations Centers and Medical Device Security. by Gary McGraw, Cigital. David Nathans is a security professional with Siemens Healthcare ...

Best regards,

Stephen