From: Apon, Daniel C. (Fed)
To: Lichtinger, Jacob T. (Fed); Perlner, Ray A. (Fed)
Subject: Re: No Time to Hash with Adversaries
Date: Wednesday, September 29, 2021 10:48:19 PM

nice- it compiled! i love it when that happens

i'll do some ape-hand banging on plastic brick (typing) and get back to you soon

From: Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>
Sent: Wednesday, September 29, 2021 9:42 AM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: Re: No Time to Hash with Adversaries

Here are the hybrid models. The updated version is in the second section.

From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Monday, September 20, 2021 11:54 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>
Subject: RE: No Time to Hash with Adversaries

Ok. I finally got around to making a crude writeup of the DFR analysis for Frodo.

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Friday, September 17, 2021 9:13 PM
To: Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: No Time to Hash with Adversaries

This is very good -- but we also want the security experiment to be much more independent of the particular construction we have in mind.. I'll think about this, and we can discuss Monday =)

From: Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>
Sent: Friday, September 17, 2021 1:03 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: No Time to Hash with Adversaries

Here is an updated version. I tried describing our adversarial model(s), so that could be a good thing to look at today.

From: Lichtinger, Jacob T. (Fed)
Sent: Wednesday, September 15, 2021 1:08 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: No Time to Hash with Adversaries

Here is what I have so far.

From: Lichtinger, Jacob T. (Fed)
To: Perlner, Ray A. (Fed); Apon, Daniel C. (Fed)
Subject: Re: No Time to Hash with Adversaries
Date: Wednesday, September 29, 2021 9:42:22 AM
Attachments: adversarial_sources.pdf
adversarial_sources.tex

Here are the hybrid models. The updated version is in the second section.

From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Monday, September 20, 2021 11:54 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>
Subject: RE: No Time to Hash with Adversaries

Ok. I finally got around to making a crude writeup of the DFR analysis for Frodo.

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Friday, September 17, 2021 9:13 PM
To: Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: No Time to Hash with Adversaries

This is very good -- but we also want the security experiment to be much more independent of the particular construction we have in mind.. I'll think about this, and we can discuss Monday =)

From: Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>
Sent: Friday, September 17, 2021 1:03 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: No Time to Hash with Adversaries

Here is an updated version. I tried describing our adversarial model(s), so that could be a good thing to look at today.

From: Lichtinger, Jacob T. (Fed)
Sent: Wednesday, September 15, 2021 1:08 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: No Time to Hash with Adversaries

Here is what I have so far.

From: Perlner, Ray A. (Fed)
To: Apon, Daniel C. (Fed); Lichtinger, Jacob T. (Fed)
Subject: RE: No Time to Hash with Adversaries
Date: Monday, September 20, 2021 11:54:56 AM
Attachments: Rowhammer Draft.docx

Ok. I finally got around to making a crude writeup of the DFR analysis for Frodo.

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Friday, September 17, 2021 9:13 PM
To: Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: No Time to Hash with Adversaries

This is very good -- but we also want the security experiment to be much more independent of the particular construction we have in mind.. I'll think about this, and we can discuss Monday =)

From: Lichtinger, Jacob T. (Fed) <jacob.lichtinger@nist.gov>
Sent: Friday, September 17, 2021 1:03 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Re: No Time to Hash with Adversaries

Here is an updated version. I tried describing our adversarial model(s), so that could be a good thing to look at today.

From: Lichtinger, Jacob T. (Fed)
Sent: Wednesday, September 15, 2021 1:08 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: No Time to Hash with Adversaries

Here is what I have so far.