From:	Mustafa Khairallah <khairallah@ieee.org>
Sent:	Thursday, August 1, 2019 7:16 PM
To:	lwc-forum; lightweight-crypto
Subject:	OFFICIAL COMMENT: COMET
Attachments:	iacrdoc.pdf

Dear all,

I have found attacks based on weak key analysis that allow forgery with probability 2^-64 (the adversarial advantage is D/2^64, where D is the number of online queries), i.e. it needs 2^64 online queries and negligible offline cost. These attacks allow privacy attacks/key recovery attacks with 2^64 Online Queries and 2^64 Offline Queries.

I have informed the designers about these attacks four days ago and they have confirmed that my analysis is correct. My understanding is that they are working on a security proof that includes these bad events. We disagree on whether these attacks contradict the claims made in the submission document. However, I assert again as I assert in the document that I make no conclusions on whether these attacks affect the security in practice and I leave this judgment to the designers and the readers.

My analysis is attached.

Regards,
Mustafa

From: Mridul Nandi <mridul.nandi@gmail.com>
Sent: Monday, August 5, 2019 5:46 AM
Cc: lwc-forum; lightweight-crypto; Shay Gueron; Ashwin Jha
Subject: Re: [lwc-forum] OFFICIAL COMMENT: COMET

Dear all,

We would like to clarify that Mustaf's observations on COMET does not violate our security claims, as specified in the specification document. We will soon publish a formal security proof on ePrint.

The COMET team

Thanks and regards,
Mridul Nandi
Associate Professor
Indian Statistical Institute
Kolkata

Thanks and regards,
Mridul Nandi
Associate Professor
Indian Statistical Institute
Kolkata

On Fri, Aug 2, 2019 at 4:46 AM Mustafa Khairallah <khairallah@ieee.org> wrote:

> Dear all,
>
> I have found attacks based on weak key analysis that allow forgery with probability 2^-64 (the adversarial advantage is D/2^64, where D is the number of online queries), i.e. it needs 2^64 online queries and negligible offline cost. These attacks allow privacy attacks/key recovery attacks with 2^64 Online Queries and 2^64 Offline Queries.
>
> I have informed the designers about these attacks four days ago and they have confirmed that my analysis is correct. My understanding is that they are working on a security proof that includes these bad events. We disagree on whether these attacks contradict the claims made in the submission document. However, I assert again as I assert in the document that I make no conclusions on whether these attacks affect the security in practice and I leave this judgment to the designers and the readers.
>
> My analysis is attached.
>
> Regards,
> Mustafa
>
> --
> To unsubscribe from this group, send email to
> lwc-forum+unsubscribe@list.nist.gov
> Visit this group at
> https://groups.google.com/a/list.nist.gov/d/forum/lwc-forum