From: Mouha, Nicky W. (IntlAssoc)
To: Nicky Mouha; lightweight-crypto
Subject: Re: SUPERCOP results
Date: Monday, February 11, 2019 10:56:09 AM

An error that SUPERCOP doesn't catch, is that Limdolen has a padding issue. The failure in the test vectors is that it can't distinguish between "AD = " (empty string) and "AD = 00" (one zero byte). Both are zero-padded to a complete block.

From: Nicky Mouha (b) (6)
Sent: Sunday, February 10, 2019 7:38 PM
To: lightweight-crypto
Subject: Re: SUPERCOP results

Incomplete list in the previous e-mail, sorry. Here is the full list:

crypto_aead comet128aesv1 tryfails crypto_aead/comet128aesv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet128aesv1 tryfails crypto_aead/comet128aesv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet128giftv1 tryfails crypto_aead/comet128giftv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet128giftv1 tryfails crypto_aead/comet128giftv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet128simonv1 tryfails crypto_aead/comet128simonv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet128simonv1 tryfails crypto_aead/comet128simonv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead comet128speckv1 tryfails crypto_aead/comet128speckv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet128speckv1 tryfails crypto_aead/comet128speckv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet64giftv1 tryfails crypto_aead/comet64giftv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet64giftv1 tryfails crypto_aead/comet64giftv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet64simonv1 tryfails crypto_aead/comet64simonv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet64simonv1 tryfails crypto_aead/comet64simonv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet64speckv1 tryfails crypto_aead/comet64speckv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111

crypto_aead comet64speckv1 tryfails crypto_aead/comet64speckv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/littleendian gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/littleendian gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/sse gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/sse gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/ssealt gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/ssealt gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead saeaes128a120t128v1 tryfails crypto_aead/saeaes128a120t128v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes128a120t128v1 tryfails crypto_aead/saeaes128a120t128v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes128a120t64v1 tryfails crypto_aead/saeaes128a120t64v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes128a120t64v1 tryfails crypto_aead/saeaes128a120t64v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes128a64t128v1 tryfails crypto_aead/saeaes128a64t128v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes128a64t128v1 tryfails crypto_aead/saeaes128a64t128v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes128a64t64v1 tryfails crypto_aead/saeaes128a64t64v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes128a64t64v1 tryfails crypto_aead/saeaes128a64t64v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes192a120t128v1 tryfails crypto_aead/saeaes192a120t128v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes192a120t128v1 tryfails crypto_aead/saeaes192a120t128v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes192a64t128v1 tryfails crypto_aead/saeaes192a64t128v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes192a64t128v1 tryfails crypto_aead/saeaes192a64t128v1/ref gcc_-

march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes192a64t64v1 tryfails crypto_aead/saeaes192a64t64v1/ref gcc_-
march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes192a64t64v1 tryfails crypto_aead/saeaes192a64t64v1/ref gcc_-
march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes256a120t128v1 tryfails crypto_aead/saeaes256a120t128v1/ref gcc_-
march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes256a120t128v1 tryfails crypto_aead/saeaes256a120t128v1/ref gcc_-
march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes256a64t128v1 tryfails crypto_aead/saeaes256a64t128v1/ref gcc_-
march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes256a64t128v1 tryfails crypto_aead/saeaes256a64t128v1/ref gcc_-
march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output
crypto_aead saeaes256a64t64v1 tryfails crypto_aead/saeaes256a64t64v1/ref gcc_-
march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead saeaes256a64t64v1 tryfails crypto_aead/saeaes256a64t64v1/ref gcc_-
march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_encrypt writes after output

On Sun, Feb 10, 2019 at 7:11 PM Nicky Mouha (b) (6) wrote:

> I finally found the time to run the submissions through SUPERCOP. Source code in attachment, results below.
>
> First, we make some small modifications (mainly to allow compilation):
>
> PhotonBeetle:
> - #define PC was added to photon.h (to compile without the -DPC compiler flag)
>
> Comet, Lotus/Locus, SAEAES:
> - encrypt.c needs to contain #include "crypto_aead.h" (requirement from call for submissions)
>
> Gimli
> - #define CRYPTO_NSECBYTES 32 needs to be #define CRYPTO_NSECBYTES 0 (requirement from call for submissions)
>
> Then, SUPERCOP returns the following errors:
>
> crypto_aead comet128aesv1 tryfails crypto_aead/comet128aesv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
> crypto_aead comet128aesv1 tryfails crypto_aead/comet128aesv1/ref gcc_-march=native_-

mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet128giftv1 tryfails crypto_aead/comet128giftv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet128giftv1 tryfails crypto_aead/comet128giftv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet128simonv1 tryfails crypto_aead/comet128simonv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet128simonv1 tryfails crypto_aead/comet128simonv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead comet128speckv1 tryfails crypto_aead/comet128speckv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet128speckv1 tryfails crypto_aead/comet128speckv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet64giftv1 tryfails crypto_aead/comet64giftv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet64giftv1 tryfails crypto_aead/comet64giftv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet64simonv1 tryfails crypto_aead/comet64simonv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet64simonv1 tryfails crypto_aead/comet64simonv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead comet64speckv1 tryfails crypto_aead/comet64speckv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead comet64speckv1 tryfails crypto_aead/comet64speckv1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt returns nonzero
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/littleendian gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/littleendian gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/ref gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/sse gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/sse gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/ssealt gcc_-march=native_-mtune=native_-std=gnu99_-O2 error 111
crypto_aead gimli24v1 tryfails crypto_aead/gimli24v1/ssealt gcc_-march=native_-mtune=native_-std=gnu99_-O2 crypto_aead_decrypt allows trivial forgeries