From: Bassham, Lawrence E (Fed)
To: Moody, Dustin (Fed)
Subject: Re: DRBG-AES based implementation
Date: Wednesday, April 12, 2017 12:11:49 PM

Interesting results. Can’t rely on AES-NIT being available, but even without CTR_CRBG didn’t do poorly. Dan will complain that it’s susceptible to timing attack, though. I agree with your “CTR_DRBG faster, but ChaCha less memory”.

Contacting them is an option.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, April 12, 2017 at 10:09 AM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: Re: DRBG-AES based implementation

Did you see this recent paper?

https://eprint.iacr.org/2017/298.pdf

If I understand it right, does it show AES CTR DRBG is faster than Cha-Cha? But Cha-Cha needs less memory?

Also, at the very end the authors say:

We have conducted extensive testing of core components and various schemes within Lattice-based cryptography as part of the SAFEcrypto project. We will be releasing open-source implementations over the course of the NIST post-quantum submission period.

Perhaps we should ask them if we they have an implementation we could use?

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, April 12, 2017 9:29:02 AM
To: Chen, Lily (Fed); Moody, Dustin (Fed)
Subject: Re: DRBG-AES based implementation

Not sure about Kris having software, but we could reach out to him. I found OpenSSL has some useful pieces in it (including an AES/Rijndael implementation from the Rijndael team). It seems like it would be usable if the copyright notices are kept intact. Still looking around though.

From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Wednesday, April 12, 2017 at 8:13 AM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: DRBG-AES based implementation

Hi, Larry:

We talked about DRBG implementation yesterday. I do not know if you have received any response from Shay. Here is another thought. Some professors/academic researchers may be more willing to share since they do not have private company's legal constraints. Do you think that possibly GMU team, Kris Gaj's team, may have some implementations which we can share?

Lily