From: Manoj Kumar <manoj63.ga@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Digest for pqc-forum@list.nist.gov - 2 updates in 1 topic
Date: Tuesday, October 25, 2022 10:08:55 AM ET

Looks like some (header) files are missing from the tar file

_____

manoj63@fermi:..kem/mceliece8192128> make
./build
In file included from operations.c:5:0:
crypto_hash.h:3:10: fatal error: libkeccak.a.headers/SimpleFIPS202.h: No such file or directory
#include <libkeccak.a.headers/SimpleFIPS202.h>
^~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
compilation terminated.
Makefile:5: recipe for target 'kat' failed
make: *** [kat] Error 1
manoj63@fermi:..kem/mceliece8192128>

_____

Thanks for helping out. Manoj.

On Tue, Oct 25, 2022 at 8:24 AM <pqc-forum@list.nist.gov> wrote:

pqc-forum@list.nist.gov Google Groups

Topic digest

View all topics

• ROUND 4 OFFICIAL COMMENT: Classic McEliece - 2 Updates

ROUND 4 OFFICIAL COMMENT: Classic McEliece

"D. J. Bernstein" <djb@cr.yp.to>: Oct 25 02:00PM +0200

The round-4 Classic McEliece submission is available here:

https://classic.mceliece.org/nist/mceliece-20221023.tar.gz

As before, KATs have been split into a separate file:

https://classic.mceliece.org/nist/mceliece-kat-20221023.tar.gz

---D. J. Bernstein, on behalf of the Classic McEliece team

Wrenna Robson <wren.robson@gmail.com>: Oct 25 01:17PM +0100

Thanks for this, Dan.

Obviously I've just had a quick glance, and will read in detail in the fullness of time, but I just want to say that I love the restructuring of the supporting documentation and the separation of content into the different documents for different purposes, and the rewriting and clarification of the content that I've seen already. It looks really great.

Best,

Wrenna

Back to top

forum/CABpUMhHbk5DF_Z-Ee-7u1_c1d9L3vCG_Dw%2B7QpiAw8PG0iHFCQ%40mail.gmail.com.

From: D. J. Bernstein <djb@cr.yp.to> via pqc-forum@list.nist.gov
To: pqc-forum@list.nist.gov
Subject: Re: [pqc-forum] Digest for pqc-forum@list.nist.gov - 2 updates in 1 topic
Date: Tuesday, October 25, 2022 12:07:06 PM ET
Attachments: smime.p7m

Manoj Kumar writes:

> Looks like some (header) files are missing from the tar file
  [...]
> #include <libkeccak.a.headers/SimpleFIPS202.h>

https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs says "Submitters may assume that these libraries are installed on the reference platform and do not need to provide them along with their submissions". NIST's pqc-forum email dated 30 Aug 2017 14:19:29 +0000 (which seems to be missing from Google's pqc-forum archive) guarantees that code can simply use <libkeccak.a.headers/SimpleFIPS202.h> etc. Presumably these details are all clear from the scripts that NIST used to test the submitted code, but those scripts don't seem to be public.

Anyway, below is a script to

   (1) download and compile the official Keccak libraries,
   (2) download the Classic McEliece submission tarballs, and
   (3) re-run the Classic McEliece code to check the KATs.

This script assumes Linux with xsltproc and standard compiler tools installed, running on a CPU with AVX2. Please speak up if you encounter any problems.

Alternatively, just use https://bench.cr.yp.to/supercop.html, which includes the Keccak libraries, includes more comprehensive KEM tests, and isn't AVX2-specific.

Beware that buffer overflows have recently been reported in the official Keccak libraries, in particular "when partial data with some specific sizes are queued, where at least one of them has a length of 2^32 - 200

bytes or more":

   https://mouha.be/sha-3-buffer-overflow/
   https://github.com/XKCP/XKCP/security/advisories/GHSA-6w4m-2xhg-2658

KEMs typically use Keccak for short fixed-length inputs, and the Classic
McEliece code uses only the all-in-one SHAKE256() function rather than
the partial-data functions, but this buffer overflow is still a useful
reminder that much more work needs to be done to ensure the correctness
of cryptographic software.

——Dan (speaking for myself)

```
cd
git clone https://github.com/XKCP/XKCP.git
cd XKCP
time make AVX2/libXKCP.a
time make AVX2/libXKCP.so

mkdir -p $HOME/include
mkdir -p $HOME/lib
ln -s $HOME/XKCP/bin/AVX2/libXKCP.a.headers $HOME/include/libkeccak.a.headers
ln -s $HOME/XKCP/bin/AVX2/libXKCP.a $HOME/lib/libkeccak.a
ln -s $HOME/XKCP/bin/AVX2/libXKCP.so $HOME/lib/libkeccak.so

export CPATH="$CPATH:$HOME/include"
export LIBRARY_PATH="$LIBRARY_PATH:$HOME/lib"
export LD_LIBRARY_PATH="$LD_LIBRARY_PATH:$HOME/lib"

cd
wget https://classic.mceliece.org/nist/mceliece-20221023.tar.gz
tar -xf mceliece-20221023.tar.gz
wget https://classic.mceliece.org/nist/mceliece-kat-20221023.tar.gz
tar -xf mceliece-kat-20221023.tar.gz

cd mceliece-20221023
```

```
for x in *Impl*/kem/mceliece*
do
  find "$x" -type d \
  | while read dir
  do
    [ -e "$dir"/Makefile ] || continue
    ( cd "$dir"
      echo "$dir"
      make
      for kat in kat_kem.req kat_kem.rsp kat_kem.int
      do
        p=`basename "$x"`
        cmp $kat "$HOME/mceliece-kat-20221023/KAT/kem/$p/$kat"
      done
    )
  done
done
```

From: Fatima ASEBRIY <fatima.asebriy@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: D. J. Bernstein <djb@cr.yp.to>
Subject: Re: [pqc-forum] Digest for pqc-forum@list.nist.gov - 2 updates in 1 topic
Date: Tuesday, October 25, 2022 06:40:05 PM ET

---

hello
why saber is not selected among the candidates of round 4 (nist)
Le mardi 25 octobre 2022 à 16:53:37 UTC+1, D. J. Bernstein a écrit :

> Manoj Kumar writes:
> > Looks like some (header) files are missing from the tar file
> [...]
> > #include <libkeccak.a.headers/SimpleFIPS202.h>
>
> https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs says
> "Submitters may assume that these libraries are installed on the
> reference platform and do not need to provide them along with their
> submissions". NIST's pqc-forum email dated 30 Aug 2017 14:19:29 +0000
> (which seems to be missing from Google's pqc-forum archive) guarantees
> that code can simply use <libkeccak.a.headers/SimpleFIPS202.h> etc.
> Presumably these details are all clear from the scripts that NIST used
> to test the submitted code, but those scripts don't seem to be public.
>
> Anyway, below is a script to
>
> (1) download and compile the official Keccak libraries,
> (2) download the Classic McEliece submission tarballs, and
> (3) re-run the Classic McEliece code to check the KATs.
>
> This script assumes Linux with xsltproc and standard compiler tools
> installed, running on a CPU with AVX2. Please speak up if you encounter
> any problems.
>
> Alternatively, just use https://bench.cr.yp.to/supercop.html, which
> includes the Keccak libraries, includes more comprehensive KEM tests,
> and isn't AVX2-specific.

> Beware that buffer overflows have recently been reported in the official
> Keccak libraries, in particular "when partial data with some specific
> sizes are queued, where at least one of them has a length of 2^32 - 200
> bytes or more":
>
> https://mouha.be/sha-3-buffer-overflow/
> https://github.com/XKCP/XKCP/security/advisories/GHSA-6w4m-2xhg-2658
>
> KEMs typically use Keccak for short fixed-length inputs, and the Classic
> McEliece code uses only the all-in-one SHAKE256() function rather than
> the partial-data functions, but this buffer overflow is still a useful
> reminder that much more work needs to be done to ensure the correctness
> of cryptographic software.
>
> ---Dan (speaking for myself)
>
>
> cd
> git clone https://github.com/XKCP/XKCP.git
> cd XKCP
> time make AVX2/libXKCP.a
> time make AVX2/libXKCP.so
>
> mkdir -p $HOME/include
> mkdir -p $HOME/lib
> ln -s $HOME/XKCP/bin/AVX2/libXKCP.a.headers $HOME/include/libkeccak.a.headers
> ln -s $HOME/XKCP/bin/AVX2/libXKCP.a $HOME/lib/libkeccak.a
> ln -s $HOME/XKCP/bin/AVX2/libXKCP.so $HOME/lib/libkeccak.so
>
> export CPATH="$CPATH:$HOME/include"
> export LIBRARY_PATH="$LIBRARY_PATH:$HOME/lib"
> export LD_LIBRARY_PATH="$LD_LIBRARY_PATH:$HOME/lib"
>
> cd
> wget https://classic.mceliece.org/nist/mceliece-20221023.tar.gz
> tar -xf mceliece-20221023.tar.gz
> wget https://classic.mceliece.org/nist/mceliece-kat-20221023.tar.gz

```
tar -xf mceliece-kat-20221023.tar.gz

cd mceliece-20221023
for x in *Impl*/kem/mceliece*
do
find "$x" -type d \
| while read dir
do
[ -e "$dir"/Makefile ] || continue
( cd "$dir"
echo "$dir"
make
for kat in kat_kem.req kat_kem.rsp kat_kem.int
do
p=`basename "$x"`
cmp $kat "$HOME/mceliece-kat-20221023/KAT/kem/$p/$kat"
done
)
done
done
```

--