```
commit d34102b9ed2859a8d2a1a1529f6356d09947283d (HEAD -> 5.2.0)
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon May 24 23:52:30 2021 -0700

    added XMSS and LMS to responder and exec engine

[33mcommit a7335debf1feeda2fc94b8eeb0f6e5c3de0458cd   [m   [33m (   [m   [1;36mHEAD ->
    [m   [1;32m5.2.0   [m   [33m,    [m   [1;33mtag: release-5.2.0-RC2   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com> Date:
Sun May 23 18:03:06 2021 -0700

    added XMSS and LMS to random testbench

[33mcommit bdb862e70176791e8a27c61b0d0b00b5cf058ea8   [m   [33m (   [m   [1;36mHEAD ->
    [m   [1;32m5.2.0   [m   [33m,    [m   [1;33mtag: release-5.2.0-RC1   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com> Date:
Fri May 21 18:51:41 2021 -0700

    updated with licensing data for 5.2.0

   [33mcommit ed796627227f24a5cfc62e758682a94e98d40037   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com> Date:
Thu May 20 21:57:36 2021 -0700

    updated mudsum

   [33mcommit ba98cbd66b1337ac9b1fd61d0ac6e471f3808210   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com> Date:
Thu May 20 21:56:30 2021 -0700

    updated schema, docs, WASP, product DAT

   [33mcommit 9e6c7ce11f293ec2473dcabca583406f5977b16f   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com> Date:
Mon May 17 20:48:18 2021 -0700

    updated mudsums

   [33mcommit c2b531befb21c81de130744a5aba42222a87778d   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com> Date:
Mon May 17 20:43:36 2021 -0700

    updated XMSS with NIST versions of XMSS_KeyGen and XMSS_Sign

   [33mcommit 7a6e504235cf335acad269e791764b68ddd93cae   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com> Date:
Sun May 16 18:25:58 2021 -0700

    added NIST versions of algorithm 10 and 12

   [33mcommit 987823978978ee0e713aa976596d03557afda421   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com> Date:
Tue May 11 21:26:02 2021 -0700
```

```
    updated images for LMS/XMSS

   [33mcommit c6a5568a8e199b0ffb0a6ee38c095300c8ec0b33   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue May 11 21:25:33 2021 -0700

    debugged test LMS vector 2 that uses psuedorandom key generation

   [33mcommit ee89967721a00bb18e851bcbaea11440b53875fb   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon May 10 21:56:44 2021 -0700

    updated to allow leaf value to be passed into LMOTS, fixed LMS, updated unit tests

   [33mcommit 4dfc6634725e17f17ad584aa7b7fc9b408db61a2   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun May 9 20:22:14 2021 -0700

    partial debug of LMS

   [33mcommit b098f7c0bbb8959703725fd392fe542096bce679   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu May 6 21:59:16 2021 -0700

    added conformance vectors for LMS

   [33mcommit b7dd45eea6d67e7ec9ea6345217767e9e868ddb0   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun May 2 14:29:18 2021 -0700

    updated mudsums

   [33mcommit c36498167b52255db71b83264a3242ced2fb6c95   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun May 2 14:28:03 2021 -0700

    compiling LMS, updated unit tests, updated documentation

   [33mcommit aad7f851cf077585621dbfdd497e55085f5a259d   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Apr 27 20:58:28 2021 -0700

    updated mudsums

   [33mcommit 072a72a863d4dfe1f7c601deccd0300e4c2e6362   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Apr 27 20:55:21 2021 -0700

    updated LMS documentation

   [33mcommit 2041547e492359ed69e42f674897074224e13b5b   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Apr 27 07:02:22 2021 -0700
```

```
    updated mudsums

   [33mcommit b5f603282550cd254d6545fab26c3488a2669399   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Apr 27 06:59:57 2021 -0700

    removed LMS files that are not needed

   [33mcommit 5f21376550d1b92955165f1b493bf9efed2bcf42   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 25 21:23:12 2021 -0700

    updated mudsums

   [33mcommit 50333d5ac0def00dea6b21fb13c555289ff26317   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 25 21:16:29 2021 -0700

    updated mudsums

   [33mcommit b7bd7ff586833868b1e76d6098af6c84e14cedda   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 25 21:16:00 2021 -0700

    updated schema for protocolpp(protocol++) moved cryptopp

   [33mcommit 68b38eda726fa66e0799eafcfe22df9322b37b19   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 25 12:26:12 2021 -0700

    finished coding LMS, needs debug

   [33mcommit 6a22bb5335af36eb10c1f3cd8a6e343f144f57a8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 21 21:30:22 2021 -0700

    updated mudsums, LMS keygen, and signature

   [33mcommit 510b14fbea0df1cd1d4b5ea4a4974da0ea9f7e73   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Apr 19 18:08:39 2021 -0700

    fixed Wifi PBKDF2

   [33mcommit 9a0356d459c95d73fcfa859232809dd2ddca6c00   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Apr 17 22:12:09 2021 -0700

    updated versions

   [33mcommit 98c4b027944ad01cf10eef3b6460bbe768f921de   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Apr 17 21:48:25 2021 -0700
```

```
    updated copyrights, licensing banners

   [33mcommit 943aaede7516fc076d1e155e789295a2d21eb231   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Apr 17 21:00:38 2021 -0700

    crossing t's, dotting i's

   [33mcommit 3284fded75dedfca8c95eeeea693ae07cf765891   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Apr 17 00:52:56 2021 -0700

    fixed typo for LMS enums, fixed replay prediction bug

   [33mcommit 9ed95aa22b22d48ffaa435fdc1836e01a9d4aec3   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Apr 16 18:06:13 2021 -0700

    finished coding LMOTS

   [33mcommit a9df98e15d231a905faa787508e58163fc652a2d   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Apr 15 23:01:59 2021 -0700

    initial checkin of LMS Signature Scheme

   [33mcommit 929c712aa34d61d34680779634b8ba211c285615   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 14 21:16:15 2021 -0700

    updated mudsums

   [33mcommit 5a8178866f93d290e65e40176e9b74c560550a1d   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 14 21:12:37 2021 -0700

    updated XMSS documentation

   [33mcommit 5bbd2e68d0e63d4a0cea09b50cfe1eac0d2c742a   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 14 05:26:06 2021 -0700

    updated mudsums, full log

   [33mcommit 5065fc565f3af4bfc41faea1821bc583bdb23d6c   [m   [33m (   [m   [1;36mHEAD ->
   [m   [1;32m5.2.0   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 11 16:15:18 2021 -0700

    updated documentation for XMSS classes

   [33mcommit a22978c531c469cbcf176e78de07707ca494737f   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
```

```
Date:   Sat Apr 10 20:52:54 2021 -0700

    added security association for XMSS, debug of new XMSS inteface for protocolpp

  [33mcommit e39ccb2aa6faaed53b53feb28251e7a7c9e62de6  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 7 20:25:18 2021 -0700

    updated to crypto++ 8.5.0

  [33mcommit 322a051e69278e0bb8c83cad216e5e1a01cc25fc  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Apr 5 23:02:50 2021 -0700

    updated Doxyfiles for lastest version

  [33mcommit 1634d818995430568d850721d6e650e1380b2c02  [m  [33m (  [m  [1;33mtag: release-5.1.2-
final  [m  [33m,  [m  [1;32m5.1.2  [m  [33m)  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Apr 5 21:47:09 2021 -0700

    fixed doxygen warnings after moving to newer version

  [33mcommit 60437cca90cd4f16cceb232759b6d27a50d7331b  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Apr 5 18:48:30 2021 -0700

    added params for XMSS and WOTS, cleared out addrbyte except where needed

  [33mcommit 4b8772af23c4d02c9ed7b06772fd112b34979670  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Apr 5 18:01:18 2021 -0700

    updated with XMSS

  [33mcommit b34c792234ae1d513043023fdeae7d0486d61eaa  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Feb 14 21:03:01 2021 -0700

    put back removed runs for coverage

  [33mcommit 94fa49471f2a4b133f3dd4671420b1bf947ed915  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Feb 14 21:00:54 2021 -0700

    updated ppp files to create more combinations for coverage, added jxmss to interface

  [33mcommit d2f6c51bf66760c2f5e63318cd60602e2b3563ad  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Feb 13 12:56:39 2021 -0700

    updated

  [33mcommit a3b0e22c342c8ae50c656fdb845387e85e7c48c3  [m
```

```
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Feb 9 00:01:55 2021 -0700

    debug for hi-res timers

  [33mcommit ed246d35c6e61b035123c0f3185ce9d349775c29  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Feb 8 23:29:21 2021 -0700

    updated test.cpp sources to add jexec, added hi-res timer to jexec for latencies, updated jtestcfg to pass units to cfg
object

  [33mcommit 9b00f49f2a98e48a095386a5ffb7270ca4906c10  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Feb 7 19:28:27 2021 -0700

    updated with additional test configurations

  [33mcommit fffd078fb9fe9914e6876140e308bc89fdd6141e  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Feb 7 19:22:37 2021 -0700

    minor updates for version, formatting, version checking

  [33mcommit 23c83168d7213fe344f67f8576949f1de6c5ea58  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Feb 6 23:34:49 2021 -0700

    updated unit tests

  [33mcommit 45167480c274adba3894e861e7aaf81ac2f43d3f  [m  [33m (  [m  [1;33mtag: release-5.1.1-
final  [m  [33m,  [m  [1;32m5.1.1  [m  [33m)  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Feb 6 17:31:05 2021 -0700

    updated unit tests

  [33mcommit 333afb953e4a9e1cf6c2acdaf7821f052ed48533  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Feb 1 19:39:16 2021 -0700

    fixed boundary checking in array class to check sizes before creating temp array

  [33mcommit e5c4cf919f3715617e2a7e041a5f46e2a5d6c78a  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Feb 1 19:17:20 2021 -0700

    debugged rsa unit tests, generating keypairs, updating fields, etc

  [33mcommit dfce6f2a70f6823408f4e75dc08617ff57d79f86  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 31 22:38:37 2021 -0700

    added unit tests for jintegrity, jconfident, jrsa, fixed some names in RSA header file doxygen

  [33mcommit
```

```
   [33mcommit 58577359b11e52c01ded20bb28b782fe90e1b0d2   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Jan 30 23:08:11 2021 -0700

    added more unit tests for jconfident and jdata

   [33mcommit 318d87a02e7c92739d8510d42b9d9011994911e0   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Jan 30 00:18:09 2021 -0700

    updated with blob unit tests

   [33mcommit 9570e11612ead7465a177aa6f37cfc4532cb9913   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Jan 26 01:16:42 2021 -0700

    updated default constructor for TLS

   [33mcommit 4e0ee089c92716b4eab4d50e342bd55da3e1bee1   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 24 02:29:38 2021 -0700

    updated usage banner for copyright, fixed finish banner to correctly report seconds of elasped time

   [33mcommit 50b4db82cb120347c5c49f9c74aaac51c4f50e5a   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 17 17:00:21 2021 -0700

    missing files for cryptopp 8.4.0

   [33mcommit 134e25268ac388c8680f46fda72fd7890c7678d9   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 17 16:56:17 2021 -0700

    fixed missing stream flag for BLOB

   [33mcommit 05972e698349bddf6a86b64984a4055e8a5f28de   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 17 15:59:41 2021 -0700

    fixed some comments from cut-n-paste error, fixed an extraction in BLOB

   [33mcommit 9e4bc1be51bcbc9463fce5e753c790edfdd668c7   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 17 14:16:45 2021 -0700

    removed mtrand from CMake, fixed range issue uncovered by distribution, fixed unit test to no pass NULL pointer

   [33mcommit 3005fc5d32487bdc6063d57a3a1ca587dc371029   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 17 13:06:24 2021 -0700

    updated to Cryptopp 8.4.0
   [33mcommit dcce00737bf2035d2efabdae8f1e883e80eca32d   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Jan 11 19:50:27 2021 -0700

    updated to use distribution for ranges

   [33mcommit c2c7a4ed11558c8a456d6d9c1f31630bd1a01ca6   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 10 01:56:48 2021 -0700

    removed all shared pointers from security associations to remain persistent

   [33mcommit ed50cd29eecf945ef9fc3ce1a94ec7f4af11ca33   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 10 01:55:23 2021 -0700

    fixed a range issue for getbyte(), changed to using standard c++ randomizer

   [33mcommit 629881bb874758e16fe9e3d8339e94c37045aad5   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Jan 9 07:08:31 2021 -0700

    added missing documentation

   [33mcommit e8a74cf17085b2e640286a2fd71cb3d9d569c445   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Jan 9 06:54:55 2021 -0700

    fixed missing jsecass, added post processing for BLOB

   [33mcommit 0fcff754236dc3202469a306c14dcd488e4692dd   [m   [33m (   [m   [1;33mtag: release-5.1.0-
final   [m   [33m,   [m   [1;32mrelease-5.1.0   [m   [33m,   [m   [1;32mdev510   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Dec 12 15:51:06 2020 -0700

    updated release notes, mudsums, full GIT log (from initial checkin)

   [33mcommit 64ccc8facf9acf1fd763f1a25934d7693ea065d4   [m   [33m (   [1;36mHEAD   [m   [33m,
   [1;32mdev510   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Dec 12 15:37:54 2020 -0700

    updated parsing of schema, updated schema for security associations

   [33mcommit b73e88ddd7ce1e9555d2546b343d87b5e926057a   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Dec 8 08:27:17 2020 -0700

    updated blob with randomizer, wasp blob debug, release 5.1.0

   [33mcommit 63095fc7f5a16a3bce09c8b33cd5065672392761   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 22 14:45:20 2020 -0700
```

```
    updated with images for BLOB doxygen, debug of WASP for BLOB, add get_blob to protocolpp

  [33mcommit 1c31e3b19ba65418fa26d3d84de275333b6f887b   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 22 12:36:20 2020 -0700

    debugged jmemblob and jmemblobsa, added TCP support for IKEv2

  [33mcommit 44a01b4b03b8a54efd21ad25100c03c776262b31   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 22 10:35:35 2020 -0700

    updated src files with 5.0.0 copyright, added jmemblob class, documented jmemblob, generated doxygen

  [33mcommit 42934dad71c7b94539ff87e6ca0b35f8432151b6   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 27 12:36:59 2020 -0700

    debug for tls1.3

  [33mcommit 293011a6b9123a5fb66696acdc507093cde7c7ae   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 20 17:34:25 2020 -0700

    fixed some SA names in W.A.S.P

  [33mcommit 0a1b377997dcc73d0b4da3866aaf4f71239f9994   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 20 17:23:00 2020 -0700

    added additional assertions in unit tests

  [33mcommit d8d3c5b3d98c5d47c9c340e95e277c6fe1919b44   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Sep 19 14:46:55 2020 -0700

    fixed parsing issue after rewriting TLS ciphersuite selection and checking for version

  [33mcommit b56aafb4707d2d65b74e2b766d90c5a9673de8b5   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Sep 17 06:23:03 2020 -0700

    HKDF unit tests debugged and passing

  [33mcommit 129dbc50a555364cd994dc5cf2beb2195060661e   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Sep 16 22:14:45 2020 -0700

    partial HKDF debug, conformance vectors 1-4 pass, 5-7 fail (likely a cut and paste error of the conformance vectors)

  [33mcommit 860a2be173249ce3fe6c7e208c758952149c51c6   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Sep 15 20:33:42 2020 -0700
```

```
    updated with HKDF conformance vectors

  [33mcommit 67889275e4a327da0f4e692b90e4e95267ce4485  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 13 11:54:23 2020 -0700

    updated with new HKDF key material function for TLS1.3

  [33mcommit 681cf9c6bd79af74be1da8d6cdb2edbe3db480fd  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Sep 8 22:09:38 2020 -0700

    added TLS1.3 application record code with padding

  [33mcommit 618ae12ffe753068bfddfc700b1f005a1b875a21  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Sep 4 21:11:46 2020 -0700

    updated mudsums

  [33mcommit 920a95c7617184e7e8af00b8eb089263a140aea0  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Sep 3 22:40:03 2020 -0700

    fixed some parser issues, schema checking

  [33mcommit 49bb58c259a835cf1301049100aac96707ee4b02  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Sep 1 22:36:20 2020 -0700

    added intersection to jarray, code cleanup on jproducer, jrsa, updated wasp for TLS1.3

  [33mcommit f8bd25d1a8f4694a163fffe6be721c9e5a0eb94f  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Aug 30 21:23:46 2020 -0700

    updated version

  [33mcommit a8bcab8f537f45a8cfa41ecb0768074d6b8175b1  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Aug 30 21:21:49 2020 -0700

    updated constructors, fixed secass lookup

  [33mcommit 0ff4f9afbd8753980d382aeda9a39fb6f320b1d4  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Aug 29 19:42:38 2020 -0700

    fix for zero length array copy construction

  [33mcommit 611d0ce0c9b474bd3a25eb697736620345ba61ff  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Aug 27 20:45:54 2020 -0700
```

```
    updated for WASP

  [33mcommit 45e1fbd2f60f3115b331b06d8cfd0160f0172943  [m  [33m (  [1;32mdev500  [m  [33m)  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Jun 2 20:47:13 2020 -0700

    added Validate function for PKI key pairs, fixed key pair encoding to HEX for XML

  [33mcommit ee837a291f35ee140e657cba0e7468b5ad40408e  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Jun 1 22:00:13 2020 -0700

    partial debug of RSA simulation

  [33mcommit 2c52e83ff1f82cdf828bc2f123a958c2a80cc62c  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu May 28 21:25:29 2020 -0700

    updated for PKI, clean compile

  [33mcommit a2ebee851ffc4feec8d408b5a3964873207e1248  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue May 12 23:57:12 2020 -0700

    added DSA and RSA security associations for running standalone

  [33mcommit 4e89baa89f19fc6c4e8541bb5f8623623fdbc1a7  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat May 2 20:10:10 2020 -0700

    added units to execution units

  [33mcommit 5829ff637565f7a4b99942435047c82244d16e81  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Apr 28 18:52:02 2020 -0700

    updated mudsums

  [33mcommit b3755e348233d4be08561aaa86eca634c9f80c4a  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Apr 28 18:43:40 2020 -0700

    updated all versions to 5.0.0

  [33mcommit f70a10602bd159d8e505d39c895c8ea364dfaf4e  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 26 18:32:42 2020 -0700

    fixed TLS bug for multiple execution units

  [33mcommit 828a23dca90ef45e766b569088c3dfeac755006c  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 26 11:21:57 2020 -0700
```

```
    fixed TLS anti-replay for multiple execution units

  [33mcommit 8cc5227aa85bee7aa1a53b915451e1054c62baec  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 26 11:10:51 2020 -0700

    fixed WiMAX anti-replay for multiple execution units

  [33mcommit 225bd3dd4d7f644ec965088f0ca893084f37f692  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 26 11:04:32 2020 -0700

    fixed SRTP anti-replay for multiple execution units

  [33mcommit 87b90857ddf532ad347c53c1540777357153eb32  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 26 10:42:18 2020 -0700

    fixed MACsec anti-replay for multiple execution units

  [33mcommit d70624f7fd7ae9bddecbd9b0ca68e630025a3c21  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Apr 25 18:51:19 2020 -0700

    fixed Wifi anti-replay for multiple execution units

  [33mcommit 183b1f578c282575b4448cfe89ec479bad635860  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Apr 25 12:21:52 2020 -0700

    fixed IPsec anti-replay for multiple execution units

  [33mcommit c46266c4911096cf1410c8e1747c9604c2974838  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 8 22:15:31 2020 -0700

    beginning work on multiple threads and responders

  [33mcommit 154fdbc16daac262b93e1f85c9da9d73cb148d05  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 8 21:57:56 2020 -0700

    updated for new test configuration

  [33mcommit 5339d7c379ebc28729cdb9c9841849760e19d75a  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 8 21:57:03 2020 -0700

    cleaned some code to be more generic

  [33mcommit 0b41d199499c627c0c7839748490f9d4336a6e42  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 8 21:55:40 2020 -0700
```

```
    version bump

   [33mcommit f308003580c7e129ef10ec4406056958fb2af3e8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 8 21:53:38 2020 -0700

    updated

   [33mcommit 0b9c7eb7fbabfa307a1d9e1de751f539f33b1656   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 8 21:49:44 2020 -0700

    moved to TinyMXL2 8.0.0

   [33mcommit 508bc963d9fa0463855cd2ff4e0c42d36c207d64   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Apr 8 21:48:34 2020 -0700

    fixed epoch to be zero when not DTLS

   [33mcommit 58092328c374dc45cbed6349ba1f499d2e542d77   [m   [33m (   [1;32mmaster   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Apr 5 21:45:37 2020 -0700

    removed 4.1.0 documentation

   [33mcommit 88cfa0964d4182ac268dec7a49efe4be440108f3   [m   [33m (   [1;33mtag: release-4.1.0   [m   [33m,
   [1;32mrelease-4.1.0-final   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Apr 2 21:00:44 2020 -0700

    updated mudsums

   [33mcommit 058b7509a0920bab046b932f1609f258f71efcb2   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Apr 2 21:00:28 2020 -0700

    updated distribution

   [33mcommit b1cf9fe33187452d7b92efec3733ee243adabdfb   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Apr 2 20:58:23 2020 -0700

    updated mudsums

   [33mcommit 07dbf79fe46c3b9b6021a749b2f3eb103f04c2e4   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Apr 2 20:58:01 2020 -0700

    updated Filelist to add test configurations, distribution install to include test configs

   [33mcommit c0c0ececa743044067e177151b7d1553abc2b48e   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
```

```
Date:   Thu Apr 2 20:54:03 2020 -0700

  [33mcommit e5f57ee8eadc35385fd384634469b100907a1757  [m  [33m (  [1;36mHEAD  [m  [33m,  [1;33mtag: release-4.1.0  [m  [33m,  [1;32mrelease-4.1.0-final  [m  [33m,  [1;32mmaster  [m  [33m)  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Mar 27 22:18:04 2020 -0700

    updated cppunit tests, mudsums, documentation, and release for 4.1.0 final release checkin

  [33mcommit 17be8873ac50af770084624cc7981f42e66fae74  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Mar 26 23:55:31 2020 -0700

    updated makefile and mudsums

  [33mcommit bb92e96f3acfcc632390c55089f3aaef2e2e3c5f  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Mar 26 23:38:13 2020 -0700

    updated mudsums

  [33mcommit ee9eb26bd54436b14c29da62686c46f02daa4e35  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Mar 26 23:37:12 2020 -0700

    updated runprotpp with new configuration files

  [33mcommit e040d9b50de8fccf8fe0cb7b0636f1a0ff83a80d  [m  [33m (  [1;33mtag: release-4.1.0-rc1  [m  [33m,
  [1;32mrelease-4.1.0-rc2  [m  [33m)  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Mar 26 12:52:54 2020 -0700

    updated mudsums

  [33mcommit c33256aaa5e65a1b5111a31b076f45d72a425832  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Mar 26 12:50:20 2020 -0700

    updated product DAT and ID for licensing

  [33mcommit 45dab11dd35c4200af73b9a44028c91f3d29998c  [m  [33m (  [1;33mtag: release-4.1.0-rc0  [m  [33m,
  [1;32mrelease-4.1.0-rc1  [m  [33m)  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Mar 25 23:39:35 2020 -0700

    updated README

  [33mcommit 231492ace8cb62e62220059e2cd6b983f9773d28  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Mar 25 23:37:47 2020 -0700

    added valgrind test configuration, added mudsums to distribution

  [33mcommit 20b730daea9f3cda77eab1bbf43c8900439c73e5  [m
```

```
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Mar 25 23:29:31 2020 -0700

    updated test configurations with correct version

  [33mcommit 6f1aa60b2b00e558efb6c0024e780460f27bcc31   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Mar 25 23:15:13 2020 -0700

    updated License for distribution, fixed SRTP replay bug

  [33mcommit 1759d032909de1d31d7dc82c7a3f23b778ceaae1   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Mar 25 21:13:48 2020 -0700

    turned off debug for replay packets

  [33mcommit 691826d868bc93609ccda3f01266e06d10cfd90c   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Mar 25 19:05:35 2020 -0700

    added random replay packets to wimax

  [33mcommit f21a758bb1d3298fbda2e447cb78144854a5b66f   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Mar 25 18:02:25 2020 -0700

    updated source code legal verbage

  [33mcommit 3fe88b5f9ac50825a7fa158a98f58486f828fbc5   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Mar 22 23:04:58 2020 -0700

    updated wifi with random replay packets, added testbench configurations for all protocols

  [33mcommit 249e5a7ade0aa238cc172a356d75a84c9f059c29   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Mar 22 17:39:27 2020 -0700

    bumped version, added copyright for v4.0.0 to all files

  [33mcommit 767f3634bdc49146ac8a42f038c86dc73da3cf6f   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Mar 21 23:57:42 2020 -0700

    replay support for SRTP and TLS

  [33mcommit ee6d701e8fda2250adea9978ad0335cd6e7feb73   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Mar 21 14:53:03 2020 -0700

    removed excess debug logging for antireplay

  [33mcommit 2587d207632963de3a3c4826be33b0bd933cbc70   [m
```

```
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Mar 21 14:27:44 2020 -0700

    fixed TLS generated replay packets

  [33mcommit fb4a5c9044f3e2cfb3749a8d0a7dcd3ac9246185   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Mar 17 23:27:13 2020 -0700

    more random replay packet debug

  [33mcommit b4723fa6f2fc363f94f2fa8c8a25f47f546e5b0d   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Mar 15 15:50:24 2020 -0700

    added replay feature to protocol

  [33mcommit 9a0fe039150dffc582bf8afab85ebb9480facf02   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Mar 15 05:48:26 2020 -0700

    added random generated replay packets for IPsec (NORMAL, SHIFT, WINDOW, REPLAY, LATE)

  [33mcommit 5c05fd0b158a62e36fd5e0f276fc60d000d0549b   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Mar 3 22:21:34 2020 -0700

    checked in reference testbench configuration

  [33mcommit 0e5022a0252c0288e4eb206acafd9cea8323c8b2   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Mar 3 21:54:05 2020 -0700

    updated copyright dates, bumped version

  [33mcommit b25439d8ee27008e438c22db7a99845bdf8fa099   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Mar 3 21:00:40 2020 -0700

    fixed reproducibility for new testbench configuration

  [33mcommit 7d305ef87804486c2d98e2ed14d34210da9606c8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Mar 1 19:41:17 2020 -0700

    added support for testbench configuration with parser, support for multiple responders running in parallel. Needs
debug, support for multiple threads per responder, arbitration when running multiple responders (should be configurable
for type ROUNDROBIN, ONEHOT, PRIORITY)

  [33mcommit 0f0c5bd68af35a27e182f23a95b2f15ddc262f49   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Feb 26 22:49:11 2020 -0700

    debugging of testbench configuration parser
```

```
   [33mcommit b24977407eec8eb4f66065637e6927558e1d5f7a   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Feb 19 22:23:42 2020 -0700

    jtestcfg parser debug to remove output from iring

   [33mcommit 5af949df4266a69f8e538906c7dcaecfe585b994   [m   [33m (   [1;36mHEAD   [m   [33m,
   [1;32mdev500   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Feb 15 14:21:34 2020 -0700

    new testbench configuration parser

   [33mcommit 7fd605de408bce09ba17e1fb8a734452a9c5da00   [m   [33m (   [1;33mtag: release-4.0.0-final-
release   [m   [33m,   [1;32mrelease-4.0.0-final   [m   [33m,   [1;32mmaster   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Jan 13 21:16:09 2020 -0700

    updated licensing to reduce number of calls to server

   [33mcommit 5a9f03ffba4138af7726d980b3c1d32c43ff0ea2   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Jan 13 21:12:44 2020 -0700

    updated licensing to reduce number of calls to server

   [33mcommit f6a33e2f4d9e5f16ff22a3c5e00cfb3290792e0a   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 12 20:56:36 2020 -0700

    updated mudsums

   [33mcommit 2c689c83c983384f84d55a4b47516a993bd7ee37   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 12 17:41:18 2020 -0700

    updated mudsums

   [33mcommit 355d513843704d04a09d3a5b3da4eac7ade58469   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 12 17:35:09 2020 -0700

    added better status reporting for licensing software

   [33mcommit 64158e44bdd172d9b38f89795ca7450b8a84c828   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Jan 12 06:59:51 2020 -0700

    updated product data and mudsums

   [33mcommit 99e40702f25e81161e1230e54a0668f7afd8fc99   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Jan 11 23:06:11 2020 -0700
```

```
    updated mudsums

   [33mcommit 44222a6654dbb10cfff2c48fc4bd874101372b19   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Jan 11 23:04:54 2020 -0700

    updated to active license if none detected before activating trial

   [33mcommit 93742d5330a482982effd9c4cafcd6c8b33ab9d8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Jan 1 23:56:04 2020 -0700

    updated mudsums

   [33mcommit a8740117c407b69970926c2a752621bd0d91cc50   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Jan 1 23:33:19 2020 -0700

    fixed CRC to use uint32_t instead of a byte array

   [33mcommit 6473720aa3611700d4e08cc971c1f1b688193435   [m   [33m (   [1;33mtag: release-4.0.0-
rc2   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Dec 28 21:01:23 2019 -0700

    debugged integrity for all modes, fixed distribution to only install library headers, fixed product version

   [33mcommit 0c1bf0ec8210071be337c9556e9509ac54c99398   [m   [33m (   [1;33mtag: release-4.0.0-rc1   [m   [33m,
   [1;32mrelease-4.0.0-rc1   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Dec 27 00:17:58 2019 -0700

    debug of CRC

   [33mcommit 63334e60a3608caa4a2295a842313765d7379871   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Dec 22 16:18:12 2019 -0700

    added Serpent documentation, updated install script, finalized distribution

   [33mcommit 11ffbb447525dc31b8156b8873db31a170a127a0   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Dec 21 22:40:53 2019 -0700

    debug of ciphers

   [33mcommit 3d769e371be3cfd72b8e17e876e88ebb710f8198   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Dec 14 23:08:05 2019 -0700

    added general CRC

   [33mcommit 0f311f877eaba245c34d1c4bd0bdef385b3eb892   [m
```

```
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Dec 10 22:46:58 2019 -0700

    updated mudsums

  [33mcommit 2d6a03dc90cbec5745b8382c1d2a0303f7339d99  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Dec 10 22:34:24 2019 -0700

    Fixed flow count

  [33mcommit f13374a9d5101a0c909aa5e35ff405dd0c137ed9  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Dec 10 21:06:32 2019 -0700

    ****************** Protocol++ 4.0.0 ***********************

    Protocol++(Protocolpp) is the property of John Peter Greninger
    and requires the use of a fee based license for ALL use cases
    please see

    www.protocolpp.com
    www.protocolpp.org
    www.protocolpp.net
    www.jpgnetworks.net
    www.jpgnetworks.org

    For license fees, evaluation licenses, and additional information

    The following copyrights have been issued for ProtocolPP(Protocol++)
    (copyright covers both names) and ALL derivative works are owned,
    controlled, and managed by John Peter Greninger under license found
    on www.protocolpp.com. Trademarks and further copyrights are pending

    Copyrights:

    Protocolpp(Protocol++) 1.0.0 - TXu002059872
    Protocol++(Protocolpp) 1.2.7 - TXu002066632
    Protocolpp(Protocol++) 1.4.0 - TXu002082674
    Protocol++(Protocolpp) 2.0.0 - TXu002097880
    Protocol++(Protocolpp) 3.0.1 - TXu002169236
    JPGNetworks                  - VAu001334497

    Trademark:

    JPGNetworks                  - 87708008

    ************************************************************
    ***************** ALL RIGHTS RESERVED ******************
    ************************************************************

    JPGNetworks, LLC and Protocolpp(Protocol++) is wholly owned (100%) by John
    Peter and Sheila Rocha Greninger. If you have received this software from
    any other source other than www.protocolpp.com, immediately report the
```

offending party to https://www.ic3.gov/complaint/default.aspx for software, IP, and Copyright theft.

ProtocolPP(Protocol++) is NOT the property of Intel Corp. Intel has no rights to sell, distribute, license, or represent JPGNetworks, LLC or ProtocolPP(Protocol++). If you have received this software from anyone representing Intel, please contact Federal authorities immediately as they are infringing this copyright and contact JPGNetworks, LLC at the address found in the license

If your copy of this software has been delivered by Robert W. Santucci or Norma Bettine you have received a fake copy and have paid the wrong distributor and I would suggest you sue to recover you money. If you have received a license from any other source other than www.protocolpp.com, immediately report the offending party to https://www.ic3.gov/complaint/default.aspx for software, IP, and Copyright theft. ProtocolPP(Protocol++) is NOT the property of Bob or Norma and they have no rights to sell, distribute, license, or represent Protocolpp or to represent themselves as employees or managers of JPGNetworks, LLC. Any license from Norma or Bob or Intel will not be honored with support, updates, or new features

JPGNetworks, LLC and Protocolpp(Protocol++) is NOT the property of NXP Semiconductor. NXP has no rights to sell, distribute, license, or represent JPGNetworks, LLC or Protocolpp(Protocol++). If you have received this software from anyone representing NXP, please contact Federal authorities immediately as they are infringing this copyright and contact JPGNetworks, LLC at the address found in the license

Only www.protocolpp.com or this website has the rights to update, modify, license, distribute, sell, or make copies of Protocolpp(Protocol++). Evaluation licenses that last 60-days are available from the website

Full licenses last a year and include support and updates

Protocol++ has several different interfaces and can be configured in different ways. Preview the Makefile to see the target. Descriptions of the different targets are found below. Contrary to some people's opinion, ProtocolPP(Protocol++) is not a "WORK IN PROGRESS". The core library has remained unchanged for several years. Changes have only been added when updating to new versions of tinyxml2 parser or the Crypto++ library. NEW items have been added (drivers, IKEv2, Security Associations) that sit on top of the core library of protocols, ciphers, and authentication algorithms with randomizers, parsers, anti-replay, and structures necessary for complete functionality

protocolpp - Executable of the full set of protocols, ciphers, testbench, and responders to provide a command line interface for connecting and testing a device under test (DUT). A user can opt to use the jresponder (default) or use QorIQ and Layerscape compatible testbench by setting PLATFORM to SECPLAT. If using the SEC platform, the testbench only reads and writes to the software rings as it is expected that the SEC connected to the other side of the software rings. See the file jbuilder.cpp libprotocolpp.a - Static library of the protocolpp.h interface, wasp.h, and ciphers.h

libprotocolpp.so.4.0.0 - Shared library of the protocolpp.h interface, wasp.h, and ciphers.h

winprot++.lib - Static library for Windows compiled under VC++ 17

rdriver - Ring driver that for UDP, TCP, TLS, or SRTP. Underlying protocols include ICMP, IP, IPsec, MACsec, Ethernet, LTE, RLC, Wifi, WiGig, WiMax with separate threads that run both the send and receive functions from the rings

ddriver - Same as the ring driver except the input and output are queues rather than rings and have push and pop routines to send and receive packets

driver - Unlike the two previous drivers, the calling program must feed the driver with single packets that are driven onto the socket. The calling program must also poll the receive method continually to obtain packets from the receive socket

ikev2   - Support for Internet Key Exchange (IKE) version 2 for IPsec ESP with CHACHA20 AES-GCM, AES-CCM, AES-CBC, AES-CTR, and Camellia. All Diffie-Hellman curves supported including 448 and 25519. Suppoort for all authentication methods now supported (RSA, PSK, ECDSA, DSA)

test - Runs the CPPUNIT tests for Protocol++. Message outputs are for negative testing

USE CASES

Protocol++(ProtocolPP) can be used for several different use cases in development, software, hardware development, stacks, and testbenches.

* TESTBENCHES - Protocolpp comes with a testbench to allow the interface to be connected to a Device Under Test (DUT) through software rings for test of protocols, encryption, and authentication algroithms, replay windows, randomization, Diffie-Hellman routines, and other items. In addition, Protocol++ can be used to generate XML output for all of the above items that can be read back in to drive Verilog or software drivers for development of hardware accelerators and software

* STACKS - The drivers in ProtocolPP show examples of how to write software stacks that support all levels of the OSI model to allow full manipulation of all features and methodologies of the protocol stack. Want to try out a new retry routine for TCP? Change the code in level 4 of your software stack to try it out. Want to try a new algorithm for IPsec? Add it to level 3 of the stack. Developing a driver for extended packet numbers in Macsec? Run your software against the Protocol++ testbench to ensure conformance. Additional protocols that do not need need the stack and require direct access to level 3 (IP/IPsec) such as Real Time Protocol (RTP) or its secure version (SRTP)? Disable TCP/UDP and TLS to drive IP/IPsec directly

* HARDWARE DEVELOPMENT - Protocol++ can be used for testing hardware accelerators that support encryption and authentication algorithms. Developing an AES-GCM engine for your hard drive controller? Instantiate AES-GCM using the "ciphers" interface of ProtocolPP in your SystemC testbench to driver your Verilog or VHDL through your UVM driver. Received your silicon back from manufacting and need to verify there are no defects? Read back in the XML files generated during pre-silicon testing that achieves

100% coverage, and execute them through ProtocolPP's driver (or your own driver) and compare to the expected value. Have some conformance vectors from the specification? Enter the conformance data into the XML format specified by Protocol++'s XML schema, read the data into the testbench or driver, and test the silicon and or RTL

* SOFTWARE - The elements of ProtocolPP can be incorporated into larger software projects to encrypt data, authenticate, generate CRC32 values, create Signatures, verify signatures, create PRF material, generate random data over ranges as bytes, words, or double words, enable SMFT mode and generate millions of random bytes from hardware is little or no time

These are the use cases currently being used. Development continues for Internet Key Exchange (IKEv2), additional driver features (ICMP message generation and return), offline key protection, key ring use, etc.

Please see the documentation found above and www.protocolpp.com for all options

INSTALLATION

To install Protocol++, the cryptopp library must first be compiled. Go to the cryptopp directory and type 'make'. After the compilation type './cryptest.exe v' to verify the library is correct. Cryptopp also allows the user to install the library and header files by typing 'make install'

To compile and install, add the path for libcryptopp and libprotocolpp to LD_LIBRARY_PATH and type 'make protocolpp'. Once compilation is done protocolpp will respond as found in the USAGE below. To verify build, make the directory "logs" then type './runprotpp'

Both libcryptopp and libprotocolpp can be installed by typing 'make install' in their respective directories. This requires administrative privileges.

USAGE: protocolpp [options]

Options:

```
  --help, -h   Print usage and exit
  --in, -i     Input file (either *.ppp or *.protopp)
  --out, -o    Output file (*.protpp)
  --seed, -s   Seed for reproducibility
  --log, -l    Path to output simulation log
  --size, -z   Size of the rings in entries
  --resp, -r   Number of responders
  --thread, -t Number of threads per responder
  --plat, -p   Platform to run (WASPLAT or SECPLAT)
  --endian, -e Endiness of the platform (BIG or LITTLE)
  --ptr, -q    Size of address pointers in bytes (4 or 8 default=8)
  --sgt, -g    Size of SG entries in bytes (8 or 16 default=16)
  --irg, -n    Address of the input ring
  --org, -z    Address of the output ring
```

Examples:

```
  protocolpp --in file1.ppp
  protocolpp -i file1.protpp
  protocolpp --in file1.ppp --out file2.protpp
  protocolpp --seed 1234567890 -i file1.protpp
  protocolpp --seed 1234567890 -i file1.ppp
  protocolpp -i file1.ppp -l filelog -z 50
  protocolpp --in file2.protpp --log filelog -r 2 -z 40
  protocolpp --seed 1234567890 --in file2.protpp --log filelog --resp 2
  protocolpp --seed 1234567890 --plat SECPLAT --in file2.protpp --log filelog
  protocolpp --seed 1234567890 -i file1.ppp -l filelog

For W.A.S.P usage, see the doxygen section

* New in 4.0.0 (Thu Oct 17 04:22:21 2019 -0700)

-- Bumped version
-- Added jconfident and jintegrity to run one-off jobs
-- Added jconfidentsa and jintegritysa to support one-off jobs
-- Added support for BLOB in SEC platform
-- Fixed RSA encrypt and decrypt
-- Updated DSA, RSA, ECDSA with new constructor for key-pair construction
-- Moved to tinyxml2 7.1.0
-- Moved to ChaChaTLS
-- Added copyright for version 3.0.1 (TXu002169236)
-- Improved coverage
-- Documenation Updates

* New in 3.0.1 (Thu Oct 17 04:22:21 2019 -0700)

-- Bumped version
-- Improved coverage
-- Documenation Updates
-- Updated licensing calls
-- Added format to all protpp and ppp files

* New in 3.0.0 (Sun Oct 14 12:22:21 2019 -0700)

-- Bumped version
-- Fixed ICMP regeneration
-- Updated time logging to be cross-platform
-- Updated drivers to look for destination on local network first
-- Updated drivers to handle IP routing headers
-- Updated drivers to handle ICMP messaging
-- Removed get_prf() and get_skseed() from IPsec and replaced with jikeprf
-- Added new parameters for MacSec (enreceive, entransmit, inuse, protectframes)
-- Fixed time reporting in the testbench to work across multiple days
-- Moved to final version of Crypto++ 8.2.0
-- Fixed missing base class calls in security associations
-- Added ability to change logging colors in jlogger
-- Added licensing calls to libraries and executables
-- Added multiple policies to IKEv2 configuration
-- Improved coverage
-- Fixed parser to reject unknown formats
-- Added ability to request multiple responders, each with it's own software ring
-- Added *.cpp file for jsecass to allow insertion of licensing API
-- Added Wifi key derivation function (KDF) to jwifi with support for IEEE802.11-2016
-- Added KDF use to wasp when generating Wifi keys
-- Added KDF use to cppunit tests
-- Added AES-GCM to Wifi, fixed NONCE generation for AES-GCM
-- Added documentation for AES-GCM to jwifi and jwifisa
-- Added BIP mode to WIFI with AES-CMAC and AES-GMAC
-- Streamlined interface for jdata and jpacket
-- Added VLAN support in Macsec for 1 or 2 tags
-- Added documentation for BIP mode to jwifi and jwifisa
-- Updated licensing and copyright notice
-- Added registration for trademark
-- Documenation Updates

* New in 2.5.6 (Sun Feb 10 23:37:22 2019 -0700)

-- Fixed memory leak in IKEv2
-- Added conformance vectors for SM4, SM3, CHACHA20, and POLY1305
-- Fixed a bug in SM3 key size checking
-- Fixed some EnumString() values for ERR_*
-- Coverage updates
-- Added images for IKEv2 payload format documentation

* New in 2.5.5 (Sun Feb 10 23:37:22 2019 -0700)

-- Moved to Crypto++ 8.2.0

* New in 2.5.4 (Sun Feb 10 23:37:22 2019 -0700)

-- Moved to Crypto++ 8.1.0

* New in 2.5.3 (Sun Feb 10 23:37:22 2019 -0700)

-- Split out signature classes as separate functions
-- Used new classes in IKEv2 to streamline code
-- Updated documentation to fix math symbols and equations using LaTeX math
-- Removed obsolete ciphers, authentication, dh curves from IKEv2
-- Generated PDF from all documentation (901 pages)
-- Updated schema to include restrictions

* New in 2.5.2 (Sun Jan 20 21:30:58 2019 -0700)

-- New class jdsa
-- New class jecdsa
-- New class jrsa
-- Updated copyright to 2019

* New in 2.5.1 (Sun Jan 6 12:45:27 2019 -0700)

-- Moved to Crypto++ v8.0.0
-- Moved to tinyxml2 v7.0.1

* New in 2.5.0 (Mon Dec 31 21:15:03 2018 -0700)
```

```
    -- Separated IKEv2 functions into separate classes
    -- New class jikeparse
    -- New class jikev2dh
    -- New class jikencrypt
    -- New class jikeprf

    * New in 2.4.3 (Sat Dec 23 21:39:15 2018 -0700)

    -- All encryption schemes for IKEv2 working (CBC, CTR, GCM, CCM, DES, 3DES, CHACHA)
    -- All integrity schemes for IKEv2 working (MD5, SHA, SHA2-256, SHA2-384, SHA2-512, AES-CMAC, AES-
GMAC, POLY1305)
    -- All PRF schemes for IKEv2 working (MD5, SHA, SHA2-256, SHA2-384, SHA2-512, AES-CMAC, AES-XCBC-
MAC)
    -- 80% of Key exchange schemes working (MODP, ECP, missing curve25514 and curve448)
    -- All encryption, integrity, Diffie-Hellman, and Signatures tested against StrongSwan IKEv2 (www.strongswan.org)
    -- Added all conformance vectors for CCM, CMAC, XCBC-MAC, GCM, CHACHA20, POLY1305, SM3, SM4,
ARIA to cppunit tests
    -- Fixed small bug in jrand
    -- Added Appendix A from employment agreement to clarify ownership
    -- Crypto++ support for curve25519 and curve448 not quite ready
https://stackoverflow.com/questions/50408019/crypto-ed448-unknown-oid

    * New in 2.4.2 (Sun Dec 24 15:22:38 2018 -0700)

    -- GIT log for all time

    * New in 2.4.1 (Sun Dec 24 17:58:22 2018 -0700)

    -- Working IKEv2 for AES-CBC, SHA256, MODP1024 (see log files)

    * New in 2.4.0 (Mon Nov 26 22:13:39 2018 -0700)

    -- Added delete_sa() to IKEv2
    -- Fixed SKEYSEED and KEYMAT generation
    -- Fixed AUTH payload generation
    -- Fixed preshared key authentication
    -- Fixed key ring issues
    -- Added key ring to drivers
    -- Added ability to daemonize IKEv2

    * New in 2.3.3 (Tue Oct 30 19:02:06 2018 -0700)

    -- Moved from pthread to std::thread
    -- Moved to CryptoPP 7.0.0 for SM3, SM4, Poly1305, ARIA encryption engines
    -- Documentation updates

    * New in 2.3.2 (Sun Oct 21 19:02:35 2018 -0700)

    -- Support for all IKEv2 encryption algorithms (CHACHA20, AEAD, Camellia)
    -- Support for all IKEv2 Diffie-Hellman curves (including 22855 and 485)
    -- Support for multiple IPsec connections

    * New in 2.3.0 (Sun Oct 7 17:59:27 2018 -0700)
```

```
-- IKE configuration parser working
-- Updated DH parameters with all RFC value except group 31 and 32
-- Fixed gateway lookup of HWADDR
-- Updated to include Ethernet
-- Discard of packet not for this interface

* New in 2.2.0 (Fri Sep 14 22:36:21 2018 -0700)

-- Split SKEYSEED and Key material generation for IPsec and IKEv2
-- Valgrind clean ring and direct drivers
-- IKEv2 initial checkin

* New in 2.1.0 (Fri Aug 31 22:38:31 2018 -0700)

-- Added ring driver
-- Added direct driver
-- Added driver
-- Added function to interpret status word as a string for printing
-- Fixed several testbench bugs
-- Logging levels now configuration from command line with --loglvl
-- Valgrind is completely clean, fixed the remaining issue that left 168 bytes of data in use at simulation end

* New in 2.0.0 (Tue May 15 01:41:28 2018 -0700)

-- Fixed support for SEC/CAAM with new security associations
-- Added new classes and base clase jsecass for security associations
-- Moved to tinyxml2 v6.2.0
-- Removed memory leaks
-- Updated all files and testbenches to use new security associations
-- Fedora28 libraries
-- Re-qualified code

* New in 1.5.0 (Sat Mar 31 20:57:46 2018 -0700)

-- Added namespaces for ProtocolPP, InterfacePP, DriverPP, and PlatformPP

* New in 1.4.2 (Wed Mar 14 19:18:10 2018 -0700)

-- Updated driver
-- Static link of libgcc and libstdc++ in libraries

* New in 1.4.1 (Mon Feb 12 00:52:10 2018 -0700)

-- Moved to Crypto++ 6.0
-- Stripped out dead code
-- Added in template specialization

* New in 1.4.0 (Sun Jan 28 21:12:41 2018 -0700)

-- Fixed several parser and randomization issues
-- Fixed overrun issue in responder
-- updated copyright for 2018 and second copyright
-- added outlen to ringin API
```

```
    -- Fixed RLC control plane bug
    -- Fixes for Windows compile to configuration files VC++
    -- Added Phanton colorization theme

    * New in 1.3.1 (Sat Dec 23 11:10:19 2017 -0700)

    -- Updated copyright with newly granted copyright reference number
    -- Added mudsums for all files

    * New in 1.3.0 (Thu Nov 30 00:08:31 2017 -0700)

    -- Fixed next header processing for IPv6 in IP and IPsec
    -- Fixed some randomization issues that were affecting reproduction of simulations
    -- Generation of random extension headers for IPv6 when respective NH is selected (IPv6_Frag, IPv6_Route,
IPv6_Opts, Jumbogram)
    -- Found and fixed segmentation faults related to next header generation and processing
    -- Fixed issue with status not being updated when generating descriptors
    -- Fixed <data> nodes

    * New in 1.2.7 (Fri Oct 20:38:49 2017 -0700)

    -- Removed --native compile option, re-enabled SFMT randomizer
    -- Fixed memory leaks in the library, still looking in testbench
    -- Fixed parser bug when reading *.protpp files for SRTP

    * New in 1.2.6 (Sat Sep 16 19:56:44 2017 -0700)

    -- Fixed PRF generation issues for AES-CCM
    -- Remove shared objects

    * New in 1.2.5 (Thu Sep 14 22:28:19 2017 -0700)

    -- Added #define for SFMT_MODE to enable use of SFMT Mersenne Twister otherwise uses previous randomizer

    * New in 1.2.4 (Thu Sep 14 20:51:00 2017 -0700)

    -- fixed makefile to build correctly with given repository structure

    * New in 1.2.3 (Sat Aug 29 11:49:09 2017 -0700)

    -- fixed formulas in doxygen
    -- added back PRF usage for TLS and IPsec in W.A.S.P

    * New in 1.2.2 (Sat Jul 29 16:15:55 2017 -0700)

    -- Port to Windows VC++ 15
    -- Updated header files
    -- Linux debug for Windows port

    * New in 1.2.1 (Tue Jul 25 19:25:10 2017 -0700)

    -- Changed RDSEED to RDRAND in hardware random number generation

    * New in 1.2.0 (Sun Jul 23 17:37:04 2017 -0700)
```

```
-- Support for IKEPRFv1, IKEPRFv2, TLSPRF1.0, TLSPRF1.2 as static functions in the jipsec and jtls classes
-- Added try/catch blocks in jmodes when calling encryption engines
-- Added generation and usage of PRF material for IPsec and TLS in the W.A.S.P randomizer

* New in 1.1.1 (Sat Jul 22 03:12:49 2017 -0700)

-- updated jrand for SFMT usage

* New in 1.1.0 (Sat Jul 22 03:12:49 2017 -0700)

-- SIMD based random number generation using SFMT
-- New build system to support versioning

* New in 1.0.0 (Sat Jul 15 11:43:00 2017 -0700)

-- First production release of Protocolpp(Protocol++)

* New in beta-2.5 (SUn Jul  2 22:38:00 2017 -0700)

-- Added SEC updates
-- Doxygen Updates

* New in beta-2.3 (Wed Jun 28 20:55:27 2017 -0700)

-- Updates for the SEC platform
-- Updated examples

* New in beta-2.1 (Mon Jun 19 23:14:25 2017 -0700)

-- Doxygen updates
-- Removed submodules

* New in beta-2.0 (Wed Jun 14 11:12:30 2017 -0700)

-- Print packet name when there's an error
-- Fixed randomizer to randomize on each pass
-- Fixed IP/IPSec decap with extension headers

* New in beta-1.0 (Sat Jun 10 12:30:08 2017 -0700)

-- GitHub site secured
-- First working release for Protocolpp(Protocol++) with testbench, all protocols,
   all cipher, all algorithms present and working on GitHub
-- Previously for sale on www.protocopp.com

* www.protocolpp.com goes LIVE! (Sat May 6 10:47:35 2017 -0700)

-- Source code for sale
-- Documentation Available
-- Examples Available
-- Testbench Available
-- Able to run regressions with parser, testbench, responders
-- As STC informed me many times, there's no free lunch (so my code isn't free either)
```

```
    -- No one has ever paid me for my code not NXP or Intel even though I was told I would be
    -- I was to be "handsomely rewarded" for it. Still haven't seen a penny
    -- There will be no free copies
    -- Documented above

    * Working testbench before Intel (Mon Apr 23 04:02:03 2017 -0700)

    -- Fully working testbench
    -- Screenshots taken with date and time
    -- Documented above

    * Protocol++ genesis (Sun Feb 8 2015 -0700)

    -- jrand.h first file created with the IDE (hence the date, see file above)
    -- I had been told by someone at STC to "go home and learn how to program"
    -- When it was up and running, was told they didn't want my "crap code", ah well
    -- I won't let NXP, Courtney McQuien, STC, Secuirty Investigators, or anyone else define me again
    -- Documented above

    * Additions

    -- Added CPPUNIT tests as examples of usage
    -- Added test executable to run CPPUNIT tests
    -- QorIQ and Layerscape support has been added
    -- Enabled input and output ring address pass in
    -- removed responder for SEC to allow connection to device/testbench

    * Fixes

    -- dynamic memory tracking in the testbench
    -- Fixed TLS random IV postprocessing
    -- minor code clean up
    -- Fixed randomization when <protocol> is present to randomize prot and dir with each pass
    -- Fixed testbench to print packet name when an error occurs
    -- Doxygen updates
    -- Added CYGWIN compiled libraries
    -- Fixed "free" bug

    * Outstanding Issues

    -- Arbitration of threads in execution units
    -- Realignment of packets in execution units when finished out-of-order
    -- See "Upcoming Features" on www.protocolpp.com for additional information
       -- AES-XTS mode
       -- Reordering of output from jexec
       -- Multiple jexec units per responder
       -- Support for KEK protection for sensitive information (Keys, IV, Salt)

 [33mcommit ebc4d9c13176a28f311ce53f7eb4f7a9494e08c9 [m [33m ( [1;36mHEAD [m [33m, [1;33mtag: release-4.0.0 [m [33m, [1;32mmaster [m [33m) [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Dec 8 17:07:02 2019 -0700

    updated with new copyright
```

```
   [33mcommit 6f4255c08151321ab097b6faa446dbdc6e945d3b   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Dec 8 16:33:49 2019 -0700

    Debug for INTEGRITY

   [33mcommit dda9a1757cac95f00c7d83e999a020feb8c8b601   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Dec 5 20:29:12 2019 -0700

    updated mudsums

   [33mcommit 7337934673db078cf4a3bd5ba1715fdc12fc84c0   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Dec 5 20:21:05 2019 -0700

    fixed ChaChaTLS and ECB modes in jconfident and randomizer

   [33mcommit 8465240225df4a432a6be6245b5e66d37ea97810   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Dec 5 00:00:25 2019 -0700

    updated README and mudsums

   [33mcommit 4666e98135dd7fb69d142b59a3f0ebbd51ccbcf8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Dec 4 23:51:42 2019 -0700

    fixed confident randomization, fixed blocksize, changed to ChaChaTLS for jmodes

   [33mcommit 3d3cf1cbd9c8e38cae55d1c3006cc9033c63fd94   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Dec 2 22:42:35 2019 -0700

    updated mudsums

   [33mcommit 81a44cc20bf71ed2e04674b96c9bca440714eee6   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Dec 2 20:26:18 2019 -0700

    fixed m_dir collision

   [33mcommit eb2d18d036a405d9567d472d37d28084b52c8ffa   [m   [33m (   [1;32mrelease-4.0.0   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Dec 1 21:44:43 2019 -0700

    update checksum

   [33mcommit 1fe97ecd9f548fb7da55945fbfe0ebf44f3781f9   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Dec 1 21:44:15 2019 -0700

    debug for jintegrity
   [33mcommit 378f271de746a59626def7888509bdcaa09f6c45   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Nov 30 15:44:35 2019 -0700

    fixed GCM and CCM for jconfident decrypt

   [33mcommit 17f6b08f63cd56f5c2eb6d2a04204b106b24d13e   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Nov 30 15:43:28 2019 -0700

    updated mudsums

   [33mcommit db9eb1901d2893d8b440493523d8c55d5a21b7e8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Nov 30 15:42:57 2019 -0700

    fixed GCM and CCM for jconfident decrypt

   [33mcommit 6523a5ceff8bfd1afe075fc13fc7fdc1af96b695   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Nov 30 14:05:07 2019 -0700

    updated README

   [33mcommit 3c7d8f50a3526bd71256d0d6d267a4ec6c214a2c   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Nov 30 14:03:31 2019 -0700

    moved to tinyxml2 7.1.0

   [33mcommit 7aa3125c209eb6be891e24f5aa377e230d939181   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Nov 30 08:25:31 2019 -0700

    updated copyright

   [33mcommit 3bfa29df17036e778d81055b2770025cb11b0cc6   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Nov 29 22:32:59 2019 -0700

    updated checksums

   [33mcommit f2b8dcadee28c9d9fe3f8e3d1a658bc42874974a   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Nov 29 22:32:15 2019 -0700

    updated with Snow3G documentation

   [33mcommit 29d959005b5910b74bbbda2da44ed02bcdaf69b6   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Nov 28 19:58:12 2019 -0700

    updated mudsums
```

```
  [33mcommit 7c57875e12125e42c4c41f9d63552613eb0ddedc   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Nov 28 19:44:53 2019 -0700

    updated documentation

[33mcommit 2574f0c95bb9e27058fbcc9225d54543df22d568[m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Nov 28 18:49:37 2019 -0700

    documentation for ZUCE

  [33mcommit 6ff7ad076abe3cba5b78717e83a92cbfb9714ff0   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Nov 28 01:14:28 2019 -0700

    additional debug for CONFIDENT mode

  [33mcommit 9e9d9b2802c29631a52b5b6afe05969226fc048c   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Nov 22 22:26:55 2019 -0700

    fixed a bug for a missing variable in the initializer list, additional debug for CONFIDENT

  [33mcommit 83d9e725138942efeef847ea7b40fc720b0a36a7   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Nov 21 23:44:31 2019 -0700

    updated with debugged code

  [33mcommit 9f3a9c59cf4f55deefcda51832fb8908fbb26ae2   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Nov 20 23:11:09 2019 -0700

    debugged randomization of jconfident

  [33mcommit 45e9be7f4c0ff26cee77866de11a36048606332d   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Nov 18 23:22:18 2019 -0700

    debugged integrity protocol with randomization

  [33mcommit b421d20828b862c7b21880e572c0855a8f268c06   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 17 22:18:40 2019 -0700

    fixed licensing software

  [33mcommit 30ede9bd68eb15f29a3a92b7e32da1e435fab9f9   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 17 00:53:35 2019 -0700

    debugged jintegrity and jconfident
  [33mcommit 4645b6d3a05093f1f743e7f6d0344eedd224d773   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Nov 16 00:59:18 2019 -0700

    updated jconfident and jintegrity with additional images

  [33mcommit 3242d61ac0c60ceaa1767773ab48f873a5503baf   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Nov 13 20:52:26 2019 -0700

    updated jcipher to include AAD data, fields adde to jenum

  [33mcommit 93c97129c43aac64316512346fcf4173cf5cf9b8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Nov 13 20:48:52 2019 -0700

    updated jcipher to include AAD data, fields adde to jenum

  [33mcommit 78ae4f0978b55d1ad3174a1ee412008d3820aee0   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Nov 12 22:10:16 2019 -0700

    debugged jcipher and jauth for compilation, fixed some documentation

  [33mcommit 85c5c662857b0fa888ab119a3f00c4da310856be   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 10 20:07:31 2019 -0700

    updated full_log for development

Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 10 19:57:23 2019 -0700

    updated mudsums

  [33mcommit b2a519bdcdea5fa427edca1e24c928aefe66bbc3   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 10 19:56:58 2019 -0700

    updated README

  [33mcommit 7a8fce34dc8181ed0cb7418c44d665385c26249e   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 10 19:53:18 2019 -0700

    update

  [33mcommit 37396779422f6ef515639cff3560d68fcbcca7fc   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 10 19:42:27 2019 -0700

    updated
```

```
   [33mcommit 0f42c60929176ed289a9965c9390e97e371d6a2a   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 10 19:37:11 2019 -0700

    added support for one-off cipher and authentication processing

   [33mcommit 081637d793dcb96ae1346994b81b70978b7f8657   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Nov 10 19:36:39 2019 -0700

    added support for one-off cipher and authentication processing

   [33mcommit 411c7b7a3d0d6abe6e462448fde2d2d4bf0d7c84   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Oct 27 21:15:18 2019 -0700

    added regression make target, updated ikev2 and jrsa

   [33mcommit 8ca33ba3b99ff64b6a35778150db893395393fd5   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Oct 27 20:31:29 2019 -0700

    added new constructors for DSA, RSA, ECDSA to construct from keys or key pairs

   [33mcommit 81a30a57def8b67a5c9006458428ca066fa7bba2   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Oct 26 17:35:08 2019 -0700

    documentation updates

   [33mcommit c8bc7e1b7a38ae552ac040cb6a35b11bfa2cf3cc   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Oct 20 21:42:15 2019 -0700

    fixed RSA encrypt/decrypt functions, added additional set/get fields

   [33mcommit e80cbe62438ba52e92c36907bf548dbe83f38dc5   [m   [33m (   [1;33mtag: release-3.0.1   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Oct 14 08:06:44 2019 -0700

    updated with license checking fixes

   [33mcommit 59ae156c4c149787ab6fe30587cc125608c1474c   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Oct 13 12:23:08 2019 -0700

    updated licensing terms and copyright notice

   [33mcommit a88f5ea4044c507d0f9fb779e2132661ce476c48   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Oct 13 12:21:59 2019 -0700

    updated licensing terms and copyright notice
```

```
 [33mcommit ba096d57a6999664faea6d0e2a523bce8e2b7f0b [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Oct 12 19:52:28 2019 -0700

    updated documentation for most of the testbench classes

 [33mcommit a4fd651efa2fb9171dd2ebfe1e643d6ee4b9176c [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Oct 12 00:29:55 2019 -0700

    documentation update

 [33mcommit 029be64b58848edbe07e93bc6435647b171c85cb [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Oct 12 00:12:59 2019 -0700

    updated documentation

 [33mcommit 9d5b54e9f4a7261b45b60c4cd8f94af0b3e120f1 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Oct 11 21:48:59 2019 -0700

    documentation updates

 [33mcommit c7039d0bf3ac46e1de36670efddf0e991bc0c72a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Oct 7 23:43:12 2019 -0700

    updated mudsums

 [33mcommit f5b41b4f0ba8431d8e004cc7d807ddc765ba358a [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Oct 7 23:42:37 2019 -0700

    updated documentation

 [33mcommit 5bdb8ac1408c71160008d9e40f025202ce9170d3 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Mon Oct 7 23:39:51 2019 -0700

    updated documentation

 [33mcommit d9edbd300394cf39aea977984e0ab7cbe78923c2 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Oct 2 21:19:12 2019 -0700

    fixed default value of colors in jikev2 configuration

 [33mcommit 7e42dc1b6d53bb40ce0f4c5c6425f54265edb572 [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Oct 2 20:28:25 2019 -0700

    fixed doxygen issues
```

```
   [33mcommit ba4e262e82a75fbef36f758417836147472fb9e4   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Sep 28 18:17:08 2019 -0700

    added cpp files for jpacket, jstream, and jdata

   [33mcommit f16003dde826a10a0e128399ff2c6678ce5f3fe4   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Sep 25 19:36:52 2019 -0700

    fixed logger issue

   [33mcommit 60c057f21614d7076f15a233a0849af6b7159578   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 22 20:32:56 2019 -0700

    updated mudsums

   [33mcommit 92c307f41e6ee0fa8f98790005bc2aaee4c9e665   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 22 20:28:37 2019 -0700

    updated mudsums and README, removed man page generation

   [33mcommit 88d46aa3e1937c628ba5a2d4851f5122b9f2e239   [m   [33m (   [1;36mHEAD   [m   [33m,
   [1;32mmaster   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 22 19:53:34 2019 -0700

    fixed some doxygen issues

   [33mcommit a33300312476bb2cdea259d5c5e88ad5ee4c186f   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 22 19:17:56 2019 -0700

    streamlined interface for jdata and jpacket, added VLAN images for documentation

   [33mcommit 61264ac5b52f141e0f337481653842537a8a1b74   [m   [33m (   [1;31morigin/master   [m   [33m,
   [1;31morigin/HEAD   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Sep 14 08:26:52 2019 -0700

    added VLAN tagging to macsec, support of two tags and CVLAN, SVLAN, and IVLAN tags

   [33mcommit c4b6b6bef83b7792bb023a9f7943062d2281ddeb   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Sep 14 07:06:55 2019 -0700

    fixed missing return values

   [33mcommit 88b552aa9f7a460b2ba032020a1afe1b256ba2e6   [m   [33m (   [1;32mikerecode   [m   [33m)   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Sep 13 17:12:18 2019 -0700
```

```
    added specs

   [33mcommit 7f5dfda1e41716f1673e6a25232d6292260fda4f   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Sep 5 21:14:46 2019 -0700

    fixed GMAC/CMAC in WIFI when in decap

   [33mcommit 84e64826f2ba3734f374e4b2effbb70951760104   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Sep 5 19:53:29 2019 -0700

    fixed some missing items in status to string converter for printing

   [33mcommit 715760fadf0b4eb77e3a9bec1322a4c751d3f05b   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Sep 5 19:45:23 2019 -0700

    fixed randomizer issue when using WIFI

   [33mcommit 3957ac8579f789b2d22cd5df2d7d455b5320bbb8   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Sep 4 00:46:13 2019 -0700

    added GIB mode to wifi, randomized ciphers, authentication, fixed a bug

   [33mcommit de39de70db62325eeb3e3f215fc6a7fd38841f6e   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sun Sep 1 22:27:42 2019 -0700

    addes AES-GCM support to Wifi, fixed it's Nonce generation, added AES-GCM documentation to jwifi and jwifisa

   [33mcommit 59be7e6ae0241f9534ef0d56b64f4e6b8030a744   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Aug 28 22:06:44 2019 -0700

    added WIFI PRF test vectors to unit test, debugged WIFI PRF function

   [33mcommit 81627e70b5ff44dc653293739d2ffc2ae763d586   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Wed Aug 28 20:53:23 2019 -0700

    updated label length for kdf in jwifi

   [33mcommit 96e1c67ce3bf90612313fdb9e962b025d96353d4   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Tue Aug 27 23:54:29 2019 -0700

    added ability to add logging colors in jikev2 per configuration, fixed PRF and KDF in JWIFI according to the spec

   [33mcommit c4bb2b388d14289c6c44810e63b77b5d278d2daf   [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Aug 24 16:16:37 2019 -0700
```

```
    added ability to change colors in jlogger

  [33mcommit 2e39d7efd442b9c75a9e6e88139ce4b8ecabed5c  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Aug 10 23:55:53 2019 -0700

    update

  [33mcommit 07e23a6ccd8aef817b9cfbccfeff09b155675c1e  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Sat Jul 27 08:42:04 2019 -0700

    updates for wasp coverage

  [33mcommit 22879433b307c91d7c88d27d2d24893c8c2f1a7c  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Thu Jul 25 20:50:19 2019 -0700

    improved coverage in jreplay

  [33mcommit 07273d5dda1853cff233c8b1882ef3a965daa1d2  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Jun 21 23:20:36 2019 -0700

    fixed parser issues in jikeparse

  [33mcommit b141960484fffe4d6891f68f77cef76532ffc147  [m
Author: John Peter Greninger (JPGNetworks, LLC) <jgreninger@hotmail.com>
Date:   Fri Jun 21 22:50:59 2019 -0700

    recoding IKEv2 to handle multiple policies
```