Run time comparison between SGX and regular OpenSSL functionality from Erlang NIF

Setup

Ubuntu 18.04, NUC7PJYH, DCAP 1.5 driver, SGX SDK 2.9.1

Erlang/OTP 23 [erts-11.0] [source] [64-bit] [smp:4:4] [ds:4:4:10] [async-threads:1]

Eshell V11.0

Erlang compiled from source without HiPE

GCC / G++ 10.1.0-2

Execution

Both SGX and non-SGX versions are located in erlang-nif_SSL, this includes old increment functionality as well as some new RSA functions performed in OpenSSL 1.1.1d.

```
erl
c(enclave_communicator).
enclave_communicator:eval_rsa().
enclave_communicator:eval_increment().
```

These functions perform simple (time) evaluations for calling Erlang NIF functions. In the background timer:tc is used in Erlang to measure time.

HW Release Mode

```
make sgx SGX_DEBUG=0 SGX_MODE=HW
```

eval_rsa

```
Running RSA keygen, sign, and encrypt together
Calling rsa_basic_operations, 30 times
Average time: 1349624.2666666666 microseconds
Average time excluding first element: 1389217.2413793104 microseconds
Raw data: [201428,710525,1329479,1212152,1521520,1229589,426689,1111910,
           2531939,1262472,1320354,2756141,3195494,1187874,1705678,2048262,
           1622328,1320962,1317989,2733033,611052,92785,2238959,1213102,
           510368,335672,1546954,1170406,1204547,819065]

Running RSA these functions separately
Calling rsa_key_gen, 30 times
Average time: 1306003.0 microseconds
Average time excluding first element: 1323085.551724138 microseconds
```

```
Raw data: [810609,1354884,150391,3993619,1353936,576288,2429567,1487026,
           910381,2898635,818858,1645158,1795175,151063,843480,526788,2496977,
           1504991,567941,318076,2499582,1060961,1388320,877149,1838692,
           869747,1370621,902044,702278,1036853]

Calling rsa_sign, 30 times
Average time: 14137.266666666666 microseconds
Average time excluding first element: 14033.896551724138 microseconds
Raw data: [17135,14066,14094,14021,14011,14020,14010,14117,14010,14020,14010,
           14066,14124,14021,14009,14024,14007,14019,14009,14021,14011,14111,
           14010,14020,14009,14020,14009,14019,14075,14020]

Calling rsa_encrypt, 30 times
Average time: 373.3666666666667 microseconds
Average time excluding first element: 371.55172413793105 microseconds
Raw data: [426,372,370,370,372,384,370,371,369,370,373,369,372,371,369,369,
           380,369,368,370,370,373,370,370,369,370,369,384,371,371]
```

eval_rsa - 2nd run for comparison

```
Running RSA keygen, sign, and encrypt together
Calling rsa_basic_operations, 30 times
Average time: 1535870.4666666666 microseconds
Average time excluding first element: 1518466.2758620689 microseconds
Raw data: [2040592,735562,685916,2308531,3744627,1772549,1003087,
            393524,2439300,802722,3131870,510473,3869326,4702860,
            845700,193362,1254721,1386996,769186,686550,1245634,
            1204138,987392,752503,1270258,259779,1821499,618760,2323616,2315081]

Running RSA these functions separately
Calling rsa_key_gen, 30 times
Average time: 1266289.8666666667 microseconds
Average time excluding first element: 1215949.896551724 microseconds
Raw data: [2726149,1085886,1195178,1019812,1169233,693907,660521,
            1511599,4202745,1619789,334555,334232,1870819,1161935,
            635276,1119226,1027553,2054949,1244194,2230131,1436832,
            226257,2285472,935589,159021,92400,1996572,1337872,919178,701814]

Calling rsa_sign, 30 times
Average time: 14137.5 microseconds
Average time excluding first element: 14035.758620689656 microseconds
Raw data: [17088,14209,14156,14058,14007,14017,14007,14128,
            14007,14016,14006,14018,14007,14017,14006,14016,14006,
            14106,14007,14019,14010,14006,14016,14006,14018,14119,
            14018,14006,14017,14008]

Calling rsa_encrypt, 30 times
Average time: 376.2 microseconds
Average time excluding first element: 372.62068965517244 microseconds
Raw data: [480,390,384,369,369,371,370,371,370,370,373,372,369,
            381,371,372,372,372,371,371,370,372,373,376,371,
            371,369,373,372,371]
```

eval_increment

```
Calling increment, 30 times
Average time: 76.26666666666667 microseconds
Average time excluding first element: 59.44827586206897 microseconds
Raw data: [564,60,60,59,60,59,59,59,59,60,59,59,59,60,
            59,60,59,59,59,59,62,60,59,59,59,59,60,60,60,59]

Calling rtrn, 30 times
Average time: 60.56666666666667 microseconds
Average time excluding first element: 60.44827586206897 microseconds
Raw data: [64,60,60,59,59,59,59,59,60,59,59,59,59,59,
            91,59,59,59,59,59,59,59,59,60,60,60,60,60,60,60]
```

eval_increment - 2nd run for comparison

```
Calling increment, 30 times
Average time: 65.0 microseconds
Average time excluding first element: 61.55172413793103 microseconds
Raw data: [165,60,60,73,113,59,59,59,59,59,59,59,59,59,59,
            59,59,60,59,59,59,59,59,59,59,60,60,59,59,60]

Calling rtrn, 30 times
Average time: 60.5 microseconds
Average time excluding first element: 60.310344827586206 microseconds
Raw data: [66,59,60,60,59,59,59,59,59,59,59,59,59,59,59,59,
            59,59,59,60,60,90,60,59,60,59,60,59,59,59]
```

Simulated Release Mode

```
make sgx SGX_DEBUG=0 SGX_MODE=SIM
```

eval_rsa

```
Running RSA keygen, sign, and encrypt together
Calling rsa_basic_operations, 30 times
Average time: 1604126.6 microseconds
Average time excluding first element: 1594696.2068965517 microseconds
Raw data: [1877608,157455,1794176,2078710,363619,364691,901833,
            950866,3378818,2430897,575533,809807,860904,1495821,
            1512164,644843,2296674,1297911,6678954,2287462,2620055,
            1370473,752419,983299,2837715,909766,1562568,2488515,848487,991755]

Running RSA these functions separately
Calling rsa_key_gen, 30 times
Average time: 1568162.8666666667 microseconds
Average time excluding first element: 1596015.6551724137 microseconds
Raw data: [760432,1444788,2163204,3130905,1239269,1463464,
            1619029,2773439,1585385,3615827,1412065,1642588,
            645041,3815667,561359,446065,222694,1988400,759810,
            1164147,710071,1429162,991400,2236859,2682164,966256,
            1982170,355189,1411992,1826045]
```

```
Calling rsa_sign, 30 times
Average time: 13938.8 microseconds
Average time excluding first element: 13836.068965517241 microseconds
Raw data: [16918,13866,13861,13983,13818,13823,13818,13825,
           13818,13818,13825,13818,13823,13818,13822,13817,
           13824,13818,13867,13819,13819,13824,13818,13825,
           13818,13823,13819,13938,13818,13863]

Calling rsa_encrypt, 30 times
Average time: 367.1666666666667 microseconds
Average time excluding first element: 363.44827586206895 microseconds
Raw data: [475,365,362,361,364,363,361,362,370,363,365,363,
           364,362,362,362,364,363,362,371,363,366,362,
           362,363,361,362,365,365,362]
```

eval_rsa - 2nd run for comparison

```
Running RSA keygen, sign, and encrypt together
Calling rsa_basic_operations, 30 times
Average time: 1317200.1666666667 microseconds
Average time excluding first element: 1353760.7931034483 microseconds
Raw data: [256942,776776,677506,789187,1008455,2567675,1891370,
           1173047,216239,2346717,949700,991435,1792516,826267,
           1337456,504754,1040253,1397231,764368,1882935,2757453,
           2660051,677823,2156786,198882,2578817,2295692,
           999238,901122,1099312]

Running RSA these functions separately
Calling rsa_key_gen, 30 times
Average time: 1608280.6333333333 microseconds
Average time excluding first element: 1580508.0344827587 microseconds
Raw data: [2413686,1033028,2747680,1396000,173831,611257,1990077,
           1874887,1718523,2707728,1288109,421440,1263411,
           2419685,2153043,894208,1714094,1065674,1015189,
           2363838,231616,3331024,652955,1024361,1463516,
           986123,5064900,1503018,1858271,867247]

Calling rsa_sign, 30 times
Average time: 14020.466666666667 microseconds
Average time excluding first element: 13923.931034482759 microseconds
Raw data: [16820,13832,13869,13831,13827,13925,13827,
           13936,13827,14119,13831,13866,13871,13827,13832,
           13826,13833,14107,13837,13865,13921,13828,13831,
           14138,14351,14249,13832,13827,13831,14298]

Calling rsa_encrypt, 30 times
Average time: 366.56666666666666 microseconds
Average time excluding first element: 363.86206896551727 microseconds
Raw data: [445,389,363,362,360,365,361,363,361,361,362,363,
           368,365,361,363,363,363,364,361,364,361,362,
           373,363,363,362,362,362,362]
```

eval_increment

```
Calling increment, 30 times
```

```
Average time: 47.4 microseconds
Average time excluding first element: 45.10344827586207 microseconds
Raw data: [114,47,46,44,45,45,45,45,45,45,45,45,
            45,45,45,45,45,45,45,45,45,46,45,45,
            45,45,45,45,45,45]

Calling rtrn, 30 times
Average time: 47.7 microseconds
Average time excluding first element: 47.62068965517241 microseconds
Raw data: [50,46,45,45,45,118,46,45,45,45,45,45,
            45,45,45,45,45,45,45,45,45,45,45,45,
            45,45,45,45,46,45]
```

eval_increment - 2nd run for comparison

```
Calling increment, 30 times
Average time: 47.266666666666666 microseconds
Average time excluding first element: 44.93103448275862 microseconds
Raw data: [115,45,45,45,45,44,45,45,45,45,45,45,45,45,
            45,45,45,45,45,45,45,45,44,45,45,45,45,45,45,45]

Calling rtrn, 30 times
Average time: 46.733333333333334 microseconds
Average time excluding first element: 46.55172413793103 microseconds
Raw data: [52,46,46,47,45,85,46,45,45,45,45,45,45,45,
            45,45,45,45,45,45,45,45,45,45,45,45,45,45,45,45]
```

No SGX

```
make no-sgx SGX_DEBUG=0
```

eval_rsa

```
Running RSA keygen, sign, and encrypt together
Calling rsa_basic_operations, 30 times
Average time: 1317428.3 microseconds
Average time excluding first element: 1319427.448275862 microseconds
Raw data: [1259453,739225,828763,179403,2799639,755797,2092528,
            966774,244620,1915815,2646888,876961,1769421,1323146,
            852805,3326962,884995,1031088,901734,625799,1129793,
            1347458,876946,2059292,1696289,1517870,2005642,812400,1137832,917511]

Running RSA these functions separately
Calling rsa_key_gen, 30 times
Average time: 1292506.4 microseconds
Average time excluding first element: 1287413.6896551724 microseconds
Raw data: [1440195,1388633,1071691,1648425,324967,999555,105894,
            803759,81732,1087840,2077240,3312600,861716,1201191,
            365716,2588802,1713756,2914882,1655547,730733,105991,
            2060986,1160684,2661524,641192,1297437,771691,1339033,1517258,844522]

Calling rsa_sign, 30 times
Average time: 13888.033333333333 microseconds
Average time excluding first element: 13796.379310344828 microseconds
Raw data: [16546,13793,13810,13792,13785,13830,13787,13784,13790,
            13786,13790,13785,13790,13785,13898,13786,13784,13792,13786,
            13789,13829,13790,13785,13790,13786,13790,13785,13786,13789,13823]

Calling rsa_encrypt, 30 times
Average time: 228.0 microseconds
Average time excluding first element: 225.6206896551724 microseconds
Raw data: [297,231,223,219,233,223,225,227,237,227,227,225,
            223,226,223,228,224,231,230,220,233,221,221,223,
            226,227,225,221,219,225]
```

eval_rsa - 2nd run for comparison

```
Running RSA keygen, sign, and encrypt together
Calling rsa_basic_operations, 30 times
Average time: 1513691.4333333333 microseconds
Average time excluding first element: 1533443.7586206896 microseconds
Raw data: [940874,625616,1087950,398365,1128800,747870,
            2459919,4231213,739626,5294203,601548,991249,
            1705166,1590873,649895,884926,2012816,1128373,
            1250649,414814,1640043,560785,2589272,1103892,
            584868,1023207,2986426,2385394,1704265,1947846]

Running RSA these functions separately
Calling rsa_key_gen, 30 times
Average time: 1329274.1333333333 microseconds
Average time excluding first element: 1309351.2413793104 microseconds
Raw data: [1907038,1079442,1103932,414072,1225231,933053,
            1169128,2474677,1858674,3384006,1143906,1175951,
            438309,2409540,495116,1022524,511557,1047545,
            389711,1077948,2378005,916990,1841772,1428910,
            1347865,1980021,2109508,1573849,633718,406226]

Calling rsa_sign, 30 times
Average time: 13890.0 microseconds
Average time excluding first element: 13798.551724137931 microseconds
Raw data: [16542,13859,13796,13790,13794,13790,13790,13797,
            13790,13794,13832,13794,13797,13795,13790,13796,
            13790,13828,13795,13789,13795,13789,13794,13789,
            13833,13790,13789,13791,13788,13794]

Calling rsa_encrypt, 30 times
Average time: 225.63333333333333 microseconds
Average time excluding first element: 224.17241379310346 microseconds
Raw data: [268,224,224,224,225,221,226,223,227,230,228,221,
            218,223,226,227,218,221,223,230,220,223,
            223,222,223,221,223,240,225,222]
```

eval_increment

```
Calling increment, 30 times
Average time: 0.03333333333333333 microseconds
Average time excluding first element: 0.0 microseconds
Raw data: [1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]
```

```
Calling rtrn, 30 times
Average time: 0.03333333333333333 microseconds
Average time excluding first element: 0.0 microseconds
Raw data: [1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]
```

eval_increment - 2nd run for comparison

```
Calling increment, 30 times
Average time: 0.13333333333333333 microseconds
Average time excluding first element: 0.0 microseconds
Raw data: [4,0,0,0,0,0,0,0,0,0,0,0,0,0,
            0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]
```

```
Calling rtrn, 30 times
Average time: 0.13333333333333333 microseconds
Average time excluding first element: 0.06896551724137931 microseconds
Raw data: [2,0,0,2,0,0,0,0,0,0,0,0,0,0,0
            ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]
```