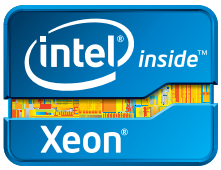
WHITE PAPER
Proof of Concept: Data Encryption

Increasing Security by Accelerating Data Encryption with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI): Testing by DuPont and Intel Corporation



Executive Summary

IT engineers from DuPont Central Research and Development (CR&D) and Intel collaborated to explore the performance benefits of Intel® Xeon® processor-based servers with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). In a proof of concept and extended laboratory testing environment, the engineers saw performance improvements of up to 300 percent in encryption and decryption, depending on factors such as size of the encrypted database and type of the queries. The tests used servers based on the Intel Xeon processor E5 and E7 families with Intel AES-NI, Oracle Database* with Intel AES-NI–enabled Oracle Advanced Security Transparent Data Encryption* (TDE*), and CR&D's chemical information management application.

Enterprise software vendors are extending their applications to exploit the full advantages of Intel AES-NI, which is built into the Intel Xeon processor E5 and E7 families. By deploying Intel AES-NI with enabled software solutions, enterprises can dramatically reduce the historical performance penalty for data encryption and decryption, making it feasible to enhance data protection throughout the enterprise.

Introduction

DuPont is a science-based company and one of the world's largest research and development organizations. It has more than 150 R&D facilities worldwide and more than 9,500 scientists and engineers with an annual research spend of approximately USD 2 billion. Managing the data and systems for such a large and diverse R&D effort requires an infrastructure that is not only fast, efficient, and flexible, but also 100 percent compliant with regulatory and security standards.

Protecting the company's intellectual property is critically important to DuPont, and is of increasing concern to enterprises around the world. With the number of security breaches growing and the complexity of the attacks making them harder to detect, encryption provides a defense mechanism so that if systems are compromised and information is exfiltrated, the data is unusable due to symmetric and asymmetric cryptographic schemes.

Historically, data encryption has brought an unwelcome performance degradation that discouraged organizations from taking full advantage of the increased security benefits

and led many to limit encryption to suboptimal data sets. DuPont emphasizes the importance of enhanced data protection for its intellectual property and was interested in exploring options to improve encryption performance through hardware acceleration.

DuPont CR&D collaborated with Intel to explore potential performance enhancements by using Intel Xeon processor-based servers with Intel AES-NI and enabled software solutions. Advanced Encryption Standard (AES) was adopted by the U.S. government starting in 2001, and is widely used across the software ecosystem to protect network traffic, data, and corporate IT infrastructure. With Intel AES-NI, new instructions were added and some of the complex and performance-intensive steps of the AES algorithm were implemented in hardware, thus accelerating the execution of the AES algorithms versus a software-only methodology.

Engineers from DuPont CR&D and Intel's Software and Services Group (Intel SSG) performed proof of concept and extended laboratory testing of database encryption performance gains and benefits of using Intel Xeon processor E5 and E7 families with Intel AES-NI–enabled Oracle Advanced Security Transparent Data Encryption (TDE). This paper describes the team's methods and summarizes the results. It includes a detailed set of procedures, commands, configurations settings, and best practices for those who want to undertake similar assessments. The paper also highlights an open source database performance tool, HammerDB*, used during the tests.

Addressing Customer Database Security Needs and Challenges

Data security breaches are often highly complex (for example, APT) and can involve unauthorized access to a wide variety of data types (for example, business, customer, intellectual property) that are targeted by the perpetrator. These breaches can have a serious impact on a business's competitiveness, reputation, and customer relations. Data security can also be an essential component for meeting many government regulations.

Deploying and applying an effective data encryption strategy is one method to help businesses proactively minimize the impact of data breaches by providing data protection that renders exfiltrated data unreadable.

Historically, the benefits of encryption were balanced against the performance impact of software-only encryption, thus discouraging many enterprises from deploying encryption to the fullest extent. However, applications (including Oracle Database and IBM DB2*) capable of utilizing Intel AES-NI can reduce those historical barriers by taking advantage of seven new hardware-based AES instructions that accelerate encryption, decryption, key generation, and matrix manipulation.[1] These new instructions provide overall cryptographic acceleration, expanding the utility of AES-based encryption while minimizing the end-users' perceived performance impact.

Beyond database applications, AES is also used to encrypt communication protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL). Voice over IP (VoIP), instant messaging, and e-mail can also be protected with these protocols. Virtual private networks (VPNs) and electronic payments are other popular encryption applications providing additional performance enhancement opportunities.

Intel AES-NI consists of four instructions for AES encryption (AESENC, AESENCLAST) and decryption (AESDEC, AESDECLAST), plus two more instructions for AES key expansion (Table 1). All three AES key lengths are supported (128-, 192-, and 256-bit with 10, 12, and 14 rounds of substitution and permutation).

The Intel AES-NI instructions also improve data protection through steps that help prevent side-channel snooping attacks. These attacks use software agents to analyze how a system processes data and searches for cache and memory access patterns. The agents try to gather patterns or other system data to deduce elements of the cryptographic processing, making it easier to break the cypher. Intel AES-NI helps hide critical elements such as table lookups, making it harder for a malicious agent to determine what elements of crypto-processing are happening.

Table 1. Intel AES-NI Instruction Sets

Instruction	Description
AESENC	Perform one round of an AES encryption flow
AESENCLAST	Perform the last round of an AES encryption flow
AESDEC	Perform one round of an AES decryption flow
AESDECLAST	Perform the last round of an AES decryption flow
AESKEYGENASSIST	Assist in AES round key generation
AESIMC	Assist in AES inverse mix columns
PCLMULQDQ	Carry-less multiply

The enabled Oracle TDE takes advantage of Intel AES-NI capability to provide increased performance and data security, where data is automatically encrypted and decrypted when written to and read from the physical media, respectively. Intel Xeon processors with Intel AES-NI provide standards-based, hardware-accelerated encryption, hardware-based exploit prevention using non-executable memory tagging, and tamper-resistant key storage that meets strict government standards.

Enabling Data Security with Intel AES-NI Data Encryption: Customer Proof of Concept and Laboratory Testing

Engineers from DuPont CR&D and Intel SSG collaborated to run comprehensive encryption database testing that measured performance gains for encrypting and decrypting some of DuPont's critical business data and records. The team completed two parallel sets of detailed testing on Intel Xeon processor E5 family-based servers with hardware-enabled Intel AES-NI and Oracle Database.

- CR&D engineers completed a proof of concept test on the DuPont premises in Wilmington, Delaware, to test the performance impact of TDE on the tablespace encryption used by a copy of DuPont CR&D's public chemical information management applications. To test the access and execution queries of the decryption, first Intel AES-NI was enabled and a set of queries was executed against tables in the encrypted tablespace and the SQL* execution time was recorded. Then, the same set of queries was run with Intel AES-NI disabled. The two sets of execution time were then compared to measure the performance of Intel AES-NI.
- Intel SSG engineers at an Intel lab in the U.K. completed a second comprehensive encryption performance test at the Intel Laboratory using a software stack and hardware platform that replicated the DuPont environment. They used a larger database, and created scripts to simulate increases in the numbers of concurrent users and queries onto the database. The emphasis was on measuring the impact of Intel AES-NI on TDE in a controlled environment to provide control results that could be contrasted against the tests performed at DuPont. The tests were based on the industry-standard database query benchmark TPC-H*, available at www.tpc.org.

Data Encryption Tests Scenarios

The performance test included these test scenarios:

- Database access/query to a clear text schema
- Database access/query software-only encryption without Intel AES-NI
- Database access/query with Intel AES-NI hardware-enabled Intel Xeon processor-based servers

All the tests used and executed an identical set of test cases, queries, and workloads.

Configuration of the Encryption Tests and Environments

- Intel Xeon processor systems configurations
- Enterprise Linux* configuration
- Oracle VM*
- Database setting and configuration
  - Using SQL*Plus command line or Oracle Enterprise Manager*
  - Specifying an Oracle wallet file
  - Creating TDE master encryption
  - Opening for use against the database
  - Installing Oracle Database
  - Applying the patch to enable TDE to use Intel AES-NI by default
  - Set up TDE by creating an encryption wallet directory in the admin directory

To set up TDE, create an encryption wallet directory in the admin directory as follows:

```
/xxxxx/wallet
```

Next, ensure that the permissions are set correctly to keep the directory secure as shown:

```
[oracle@xxxxx]$ ls -ld wallet/

drwxr-x--- 2 xxx xxxx 4096 Jun 14 16:01 wallet/
```

Create a sqlnet.ora file in the network admin directory:

```
/xxxxx/network/admin
```

Add the following line to this file (keeping the entry all on the same line):

```
ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/xxxxxx/wallet/)))
```

You can then create an open wallet as follows using your own chosen password:

```
[oracle@xxxxxx]$ sqlplus / as sysdba

...

SQL> alter system set encryption key;

System altered.

SQL>

WALLET created
```

You can then create an unencrypted tablespace as normal and an encrypted tablespace by specifying encryption options as follows:

```
SQL> create bigfile tablespace TPCH_ENCRYPT datafile '+DATA' size 50g encryption using 'AES256'
default storage(encrypt);

Tablespace created.
```

and check that the tablespace is indeed encrypted.

```
SQL> select tablespace_name, encrypted from dba_tablespaces;

TABLESPACE_NAME ENC

------------------------------ ---

SYSTEM NO

SYSAUX NO

UNDOTBS1 NO

TEMP NO

USERS NO

TPCH_CLEAR NO

TPCH_ENCRYPT YES

7 rows selected.
```

You can use HammerDB, an open-source, freely available Oracle load-test tool to create identical scale factor 10, 10 GB schemas based on the TPC-H specification in both clear-text and encrypted forms. In the control environment, the team used HammerDB to run and capture an example query to use against this data and keep the predicates the same so the query run would be identical each time. We also used autotrace and timing to test query performance. For consistency, Oracle parallel query was disabled to test query times running as a single process.

Clear Text Unencrypted Data Test

First, we examined the clear text schema with the following query (which is TPC-H query 1):

```
1.SQL> connect tpch/tpch
2.Connected.
3.SQL> set autotrace on;
4.SQL> set timing on;
5.SQL> select l_returnflag, l_linestatus,
sum(l_quantity) as sum_qty,
sum(l_extendedprice) as sum_base_price,
sum(l_extendedprice * (1 - l_discount)) as sum_disc_price,
sum(l_extendedprice * (1 - l_discount) * (1 + l_tax)) as sum_charge,
avg(l_quantity) as avg_qty,
avg(l_extendedprice) as avg_price,
avg(l_discount) as avg_disc,
count(*) as count_order from lineitem
where l_shipdate <= date '1998-12-01' interval '119' day (3)
group by l_returnflag, l_linestatus
order by l_returnflag, l_linestatus;
```

The query, as expected, returned four rows, and the timing value showed it took almost 29 seconds:

```
Elapsed: 00:00:28.80
```

The execution plan shows "TABLE ACCESS FULL" on "LINEITEM," which is a full table scan on the biggest table in the schema. The statistics results show that these were physical reads, which means that the data was not cached in memory but instead read from disk. After running the same query again, you can observe that the elapsed time and the number of physical reads remain the same:

```
Elapsed: 00:00:28.74
1.Statistics
2.----------------------------------------------------------
3....
4.1038269 physical reads
5....
```

The first time, Oracle did not cache the LINEITEM table in the buffer cache (the system global area [SGA]). When we ran the query a second time, it fetched the data from disk again and continued to do this every time the query was run, with consistent timing each time. This test highlights the important usage model of Oracle TDE, that data is decrypted as it is read from disk (that is, physical read), but cached in memory in clear form. However, as this example illustrates, with larger tables, Oracle Database performs a direct-path read, bypassing the Oracle Database SGA and reading the data directly into the user session private program global area (PGA) memory instead. Consequently, each time the query is run, the data is read from disk and, therefore, the full benefits of Oracle TDE and its acceleration with Intel AES-NI can be used.

Software-Only Encryption Data Test

Step two for encryption testing includes using and executing identical sets of queries on encrypted data. Oracle TDE is controlled by hidden parameters, so you need a query to see the parameters:

```
1.SQL> li

2.1* select a .ksppinm “Parameter”, b.ksppstvl “Session Value”, c.ksppstvl “Instance
Value” from x$ksppi a, x$ksppcv b, x$ksppsv c where a.indx = b.indx AND a.indx =
c.indx AND ksppinm like ‘%encryption%’

3.SQL> /

4.Parameter

5.--------------------------------------------------------------------------------

6.Session Value

7.--------------------------------------------------------------------------------

8.Instance Value

9.--------------------------------------------------------------------------------

10._use_platform_encryption_lib

11.TRUE

12.TRUE

13._use_hybrid_encryption_mode

14.TRUE

15.TRUE

16._db_disable_temp_encryption

17.FALSE

18.FALSE
```

To use Intel AES-NI, the parameter _use_platform_encryption_lib needs to be set to TRUE. To use Intel AES-NI for both encryption and decryption, _use_hybrid_encryption_mode needs to be set to FALSE. The impact of hardware encryption acceleration performance can be tested by turning these parameters on and off. For example:

```
1.SQL> alter system set “_use_platform_encryption_lib”=FALSE scope=both;

2.System altered.
```

Restart the database and open the wallet before running queries against the encrypted data without Intel AES-NI for hardware-accelerated encryption. In this case, Oracle is using software only to do the decryption and is not using Intel AES-NI at all.

```
SQL> alter system set wallet;

1.System altered.
```

The query again returned four rows, and the timing value is 136 seconds, including the time to do the software-only decryption.

```
Elapsed: 00:02:16.41
```

You can observe the decryption rate with the v$ view v$encrypted_tablespace or by reviewing the statistics from an Automatic Workload Repository (AWR) report. The following example notes that blocks were decrypted at the rate of 7,479.2 per second:

```
Statistic           Total           per Second       per Trans

-------------------------------------------------------------

blocks decrypted    1,039,488       7,479.2          94,498.9
```

Encrypted Data Test

The execution plan shows "TABLE ACCESS FULL" on "LINEITEM" and again, the statistics show that the full table scan was based on physical reads. Each time the same statement is re-executed, the data is read from disk. In this example, each time the data was decrypted with software acceleration, it took approximately 4.7 times longer than the same query on clear text.

Next, restart the database, but this time, enable hardware-accelerated encryption to use Intel AES-NI.

```
SQL> alter system set "_use_platform_encryption_lib"=TRUE scope=both;

System altered.
```

In this example, the same query ran with the following timing value:

```
Elapsed: 00:00:45.30
```

As expected, the execution plan again shows "TABLE ACESS FULL" on "LINEITEM" with the full table scan based on physical reads. The same query was run each time (the data was read from disk and decrypted), but we made use of Intel AES-NI for acceleration. An AWR report shows that blocks were being decrypted at the rate of 20,323.9 per second, improving the decryption performance by almost a factor of three.

```
Statistic              Total          per Second     per Trans

---------------------------------------------------------------

blocks decrypted       1,039,488      20,323.9       94,498.9
```

Intel AES-NI Encryption Test Results

Testing the performance of Oracle TDE with hardware acceleration using Intel AES-NI showed significant performance gains (Table 2). The same query consistently shows that with Intel AES-NI, the query completed three times faster than that using software-only encryption and was only 1.55 times slower compared to using no encryption at all. There are clear security benefits of using Oracle TDE for encryption, and with Intel Xeon processors with Intel AES-NI, you should see significantly improved performance.

The goal with Oracle Transparent Database Encryption, as the name implies, is for encryption to be transparent without needing to modify practices. The simple tests DuPont CR&D and Intel performed show that you can achieve this by using Intel Xeon processors with Intel AES-NI for Oracle Database encryption acceleration.

Insights into the Test Results

Why was there such a big difference between the performance gains (20 to 140 percent) seen at DuPont CR&D and the 300 percent improvement in the Intel test environment? The main reason is likely due to the fact that the DuPont CR&D tests were not conducted in a well-controlled environment. The back-end storage for the Oracle Database at DuPont CR&D resides in a storage system that is shared by many applications and in which the workload can vary greatly. Therefore, performance is highly dependent on subsystem load. For this reason, for the tests, each query was run three times (at different times and on different days), and the execution time was averaged for the comparison.

Another important factor is that Oracle tablespace encryption with TDE encrypts data at rest. Oracle TDE encrypts and decrypts the data whenever it is written to or read from the physical storage, respectively. Consequently, data that has been read, but is cached in memory, is not encrypted. This means that the Oracle Database performance on data that is stored in a TDE tablespace but has been read, decrypted, and held in memory is identical to that of data read from an unencrypted tablespace. In both solutions, all the data cached in memory is in clear text form.

As a result, data encryption performance can vary significantly depending upon how the data is accessed and whether it is read from disk or already held in memory. With Oracle Database, not all data read is cached in the buffer cache in the main Oracle memory store (the SGA). In some cases, Oracle Database prefers an operation called a direct path read, bypassing the SGA and reading the data directly from disk in the user sessions private memory area within the PGA.

Oracle Database does this in circumstances such as executing a parallel query or running a serial query on a table that exceeds a particular size threshold. When this occurs, Oracle Database rereads the same data from the physical store and decrypts it each time. As a result, tests running queries against large tables are likely to benefit more from improved decryption with Intel AES-NI than queries on smaller tables where data may already be cached.

The differences in the test environments and in how data is accessed likely account for the different encryption and decryption performance results observed between the Intel lab environments and those at DuPont CR&D.

Summary

AES encryption and instruction-based hardware acceleration provide a technology solution that enables enterprises to balance the need to enhance security through the application of encryption and long-standing performance barriers. No longer are businesses left to develop policies based on performance impacts with criteria founded on size and data criticality. Instead, they can develop broader strategies that enhance the overall effectiveness of their security.

The Intel Xeon processor E5 and E7 families with hardware acceleration of Intel AES-NI dramatically reduce the overhead typically associated with encryption and decryption, while making encryption stronger. These solutions will help organizations protect their information while maximizing the return on their hardware investments.

Table 2. Database Encryption Test

Database Encryption Test			
Intel Laboratory Tests			
Test#	**Type of Data**	**Execution Time**	**Comments**
1	Query on clear text	00:00:28.80	
2	Software-only encryption without Intel AES-NI hardware-based server	00:02:16.41	300 percent slower than encryption with Intel AES-NI hardware
3	Accelerated with Intel AES-NI hardware-based server	00:00:45.30	300 percent faster than encryption without Intel AES-NI hardware
DuPont CR&D Production Tests			
Test#	**Type of Data**	**Execution Time**	**Comments: Database size of 60 to 70 GB**
1	Query on clear text	N/A	
2	Software-only encryption without Intel AES-NI hardware server	4.96	98 percent slower than encryption with Intel AES-NI hardware
3	Accelerated with Intel AES-NI hardware-based server	2.51	98 percent faster than encryption without Intel AES-NI hardware

Note: For DuPont CR&D test, the above result was only for one query (acd-1a). We ran five queries. The improvement ranged from 20 to 140 percent.

[1] See a list of software that supports Intel® AES-NI at http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/aes-ni-ecosystem-update.html.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to http://www.intel.com/performance

Intel does not control or audit the design or implementation of third party benchmark data or Web sites referenced in this document. Intel encourages all of its customers to visit the referenced Web sites or others where similar performance benchmark data are reported and confirm whether the referenced benchmark data are accurate and reflect performance of systems available for purchase.

Copyright © 2013 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others

0213/LJ/TDA/XX/PDF 328593-001US