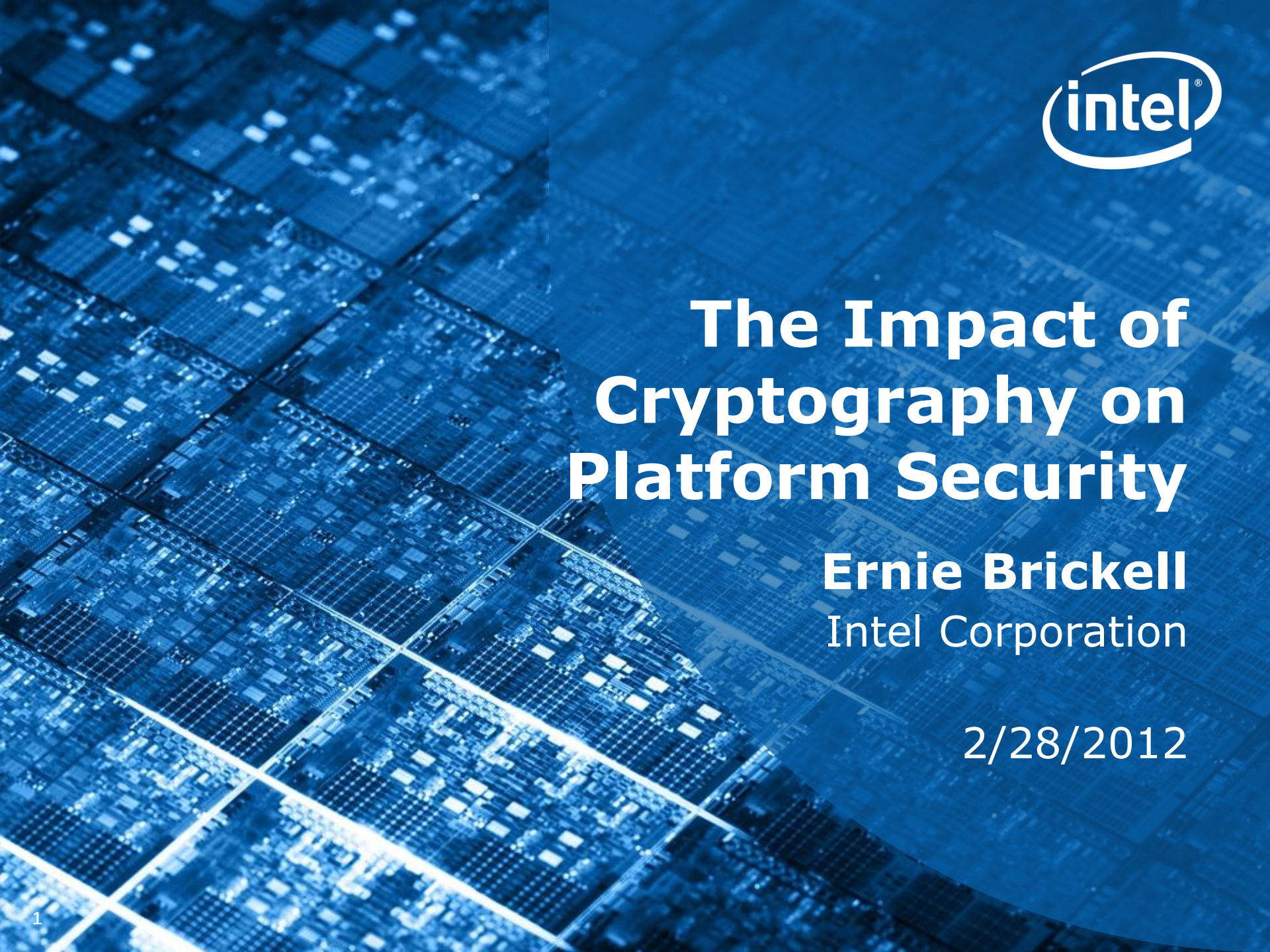


The Impact of Cryptography on Platform Security

Ernie Brickell
Intel Corporation

2/28/2012

Security is Intel's Third Value Pillar

Paul Otellini
Intel CEO

Intel is positioning itself to lead in three areas:

- *energy-efficient performance silicon,*
- *connectivity, and*
- *security.*

There's an urgent need for security innovation as people are spending more time online and the amount of data is growing.

Outline

- Digital signatures on FW updates
- Hardware Random number generation
- Anonymous platform attestation
- Trusted Boot
- Improved protection for user authentication
- Enhancements for cryptographic performance
- Protection from Side Channel Attacks

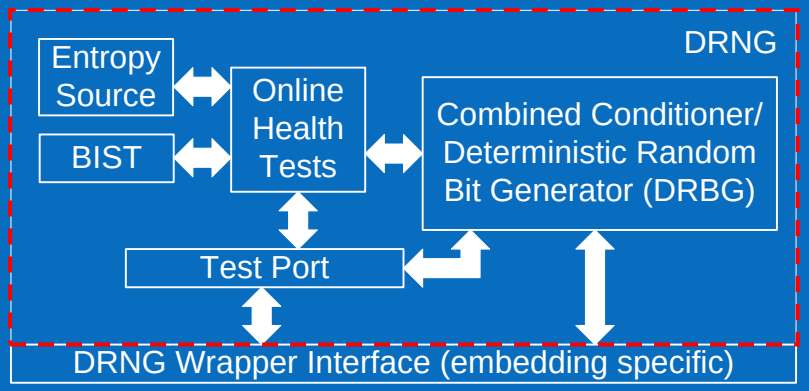
Digital Signatures on FW Updates

- Intel FW updates are validated with a digital signature
- NIST recommending digital signatures for BIOS updates.
  - NIST SP800-147 – BIOS protection Guidelines
    - Use digital signatures to verify the authenticity of BIOS updates.
    - BIOS updates verified using a Root of Trust for Update which includes:
      - The key store used to verify signatures on updates.
      - The digital signature verification algorithm.
    - Use of NIST-approved crypto algorithms.
    - Recommend rollback protection.
    - http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf

Outline

- Digital signatures on FW updates
- **Hardware Random number generation**
- Anonymous platform attestation
- Trusted Boot
- Improved protection for user authentication
- Enhancements for cryptographic performance
- Protection from Side Channel Attacks

Digital Random Number Generator (DRNG)



A reusable circuit that provides an autonomous/self contained, complete DRNG

Provides a hardware source of high quality, high performance entropy to be embedded across Intel products. It is composed of

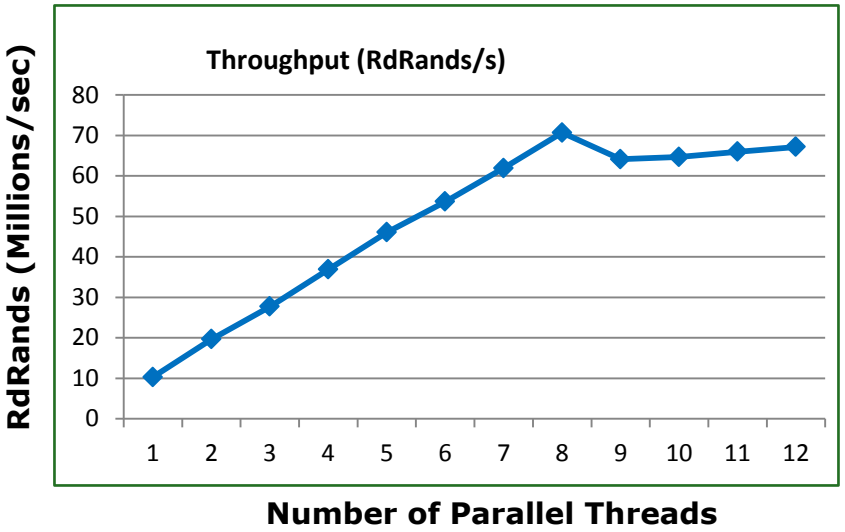
- An all-digital Entropy Source, (3 Gbps, 90% Entropic)
- Runtime Entropy Source health measurement via Online Health Test,
- Conditioning (via AES CBC-MAC mode) and DRBGing (via AES CTR mode) post processing and
- Built In Self Test (BIST) and Test Port

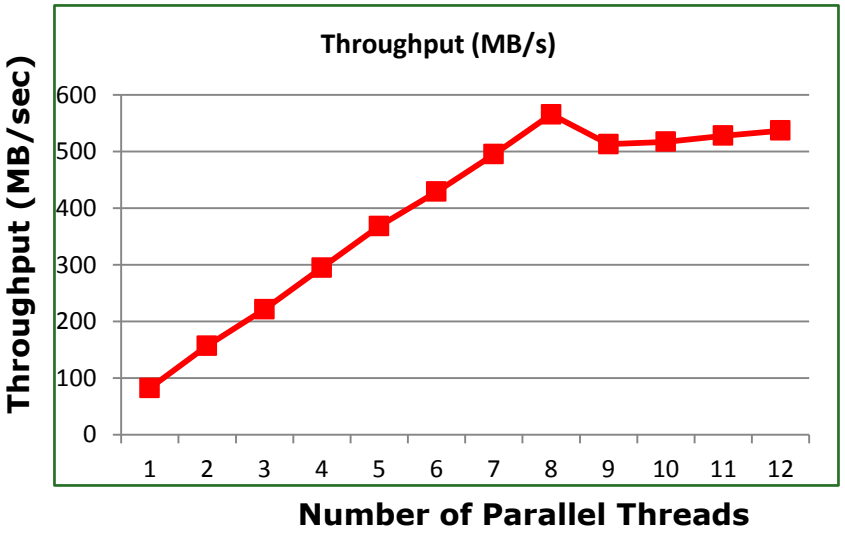
Standards compliant (NIST SP 800-90)

RDRAND Performance

Preliminary data from pre-production Ivy Bridge sample[1]

- RdRand – new CPU instruction which provides access to DRNG
- Up to 70 million RdRand invocations per second
- 500+ Million Bytes of random data per second
- Throughput ceiling is insensitive to number of contending parallel threads
  - ❑ Steady state maintained at peak performance





[1]Data taken from Intel® processor codename Ivy Bridge early engineering sample board. Quad core, 4 GB memory, hyper-threading enabled. Software: LINUX* Fedora 14, gcc version 4.6.0 (experimental) with RdRand support, test uses pthreads kernel API

RdRand Response Time and Reseeding Frequency

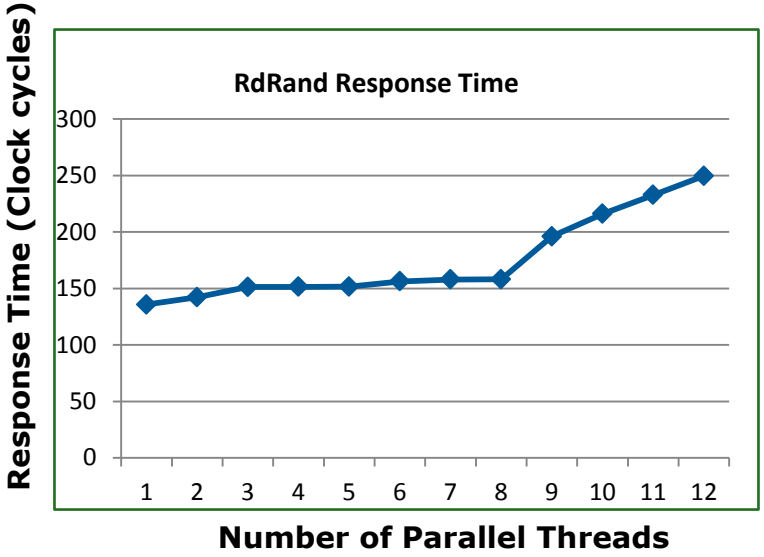
Preliminary data from pre-production Ivy Bridge sample[1]

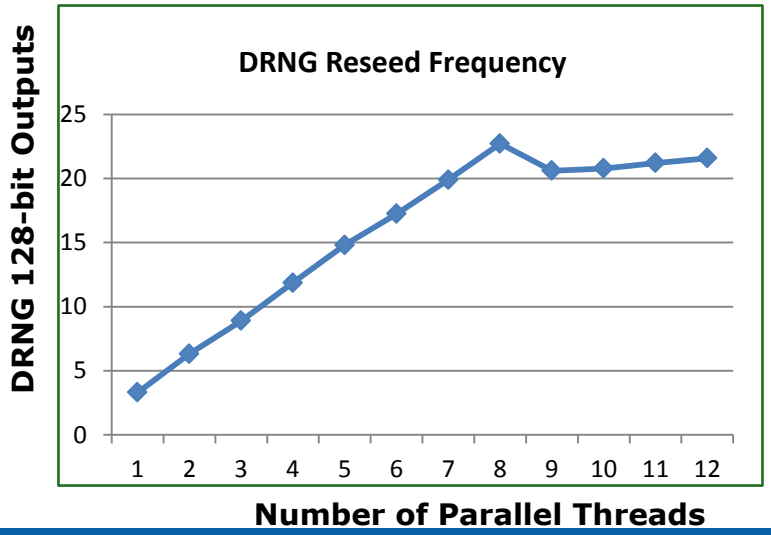
RdRand Response Time

- ~150 clocks per invocation
- Little contention until 8 threads
  - (or 4 threads on 2 core chip)
- Simple linear increase as additional threads are added

DRNG Reseed Frequency

- Single thread worst case: Reseeds every 4 RdRand invocations
- Multiple thread worst case: Reseeds every 23 RdRand invocations
- At slower invocation rate, can expect reseed before every 2 RdRand calls
  - ❑ NIST SP 800-90 recommends ≤ 2^{48}



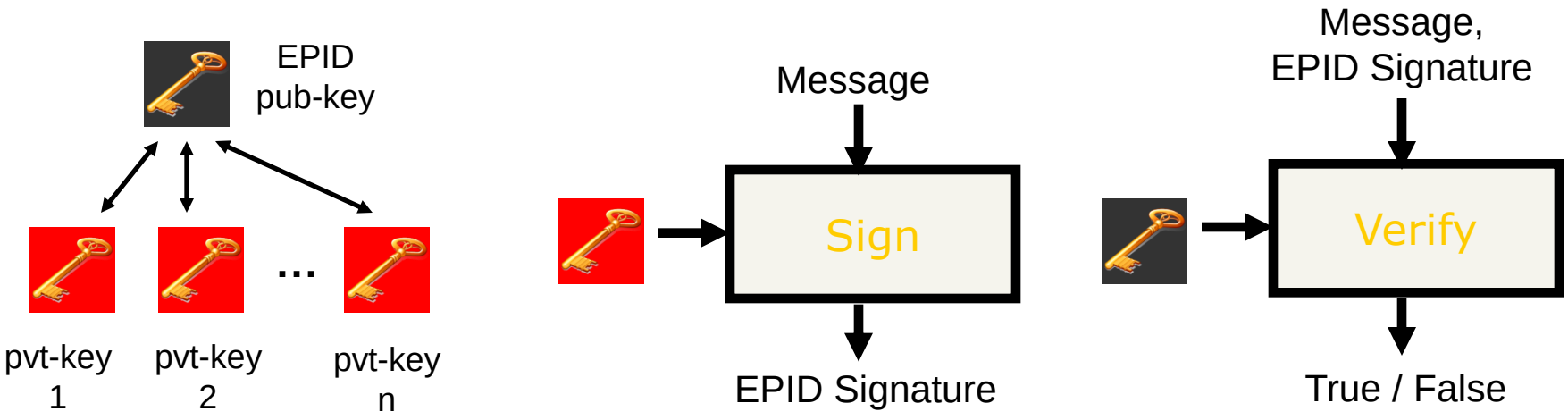


[1]Data taken from Intel® processor codename Ivy Bridge early engineering sample board. Quad core, 4 GB memory, hyper-threading enabled. Software: LINUX* Fedora 14, gcc version 4.6.0 (experimental) with RdRand support, test uses pthreads kernel API

Outline

- Digital signatures on FW updates
- Hardware Random number generation
- **Anonymous platform attestation**
- Trusted Boot
- Improved protection for user authentication
- Enhancements for cryptographic performance
- Protection from Side Channel Attacks

Overview of EPID



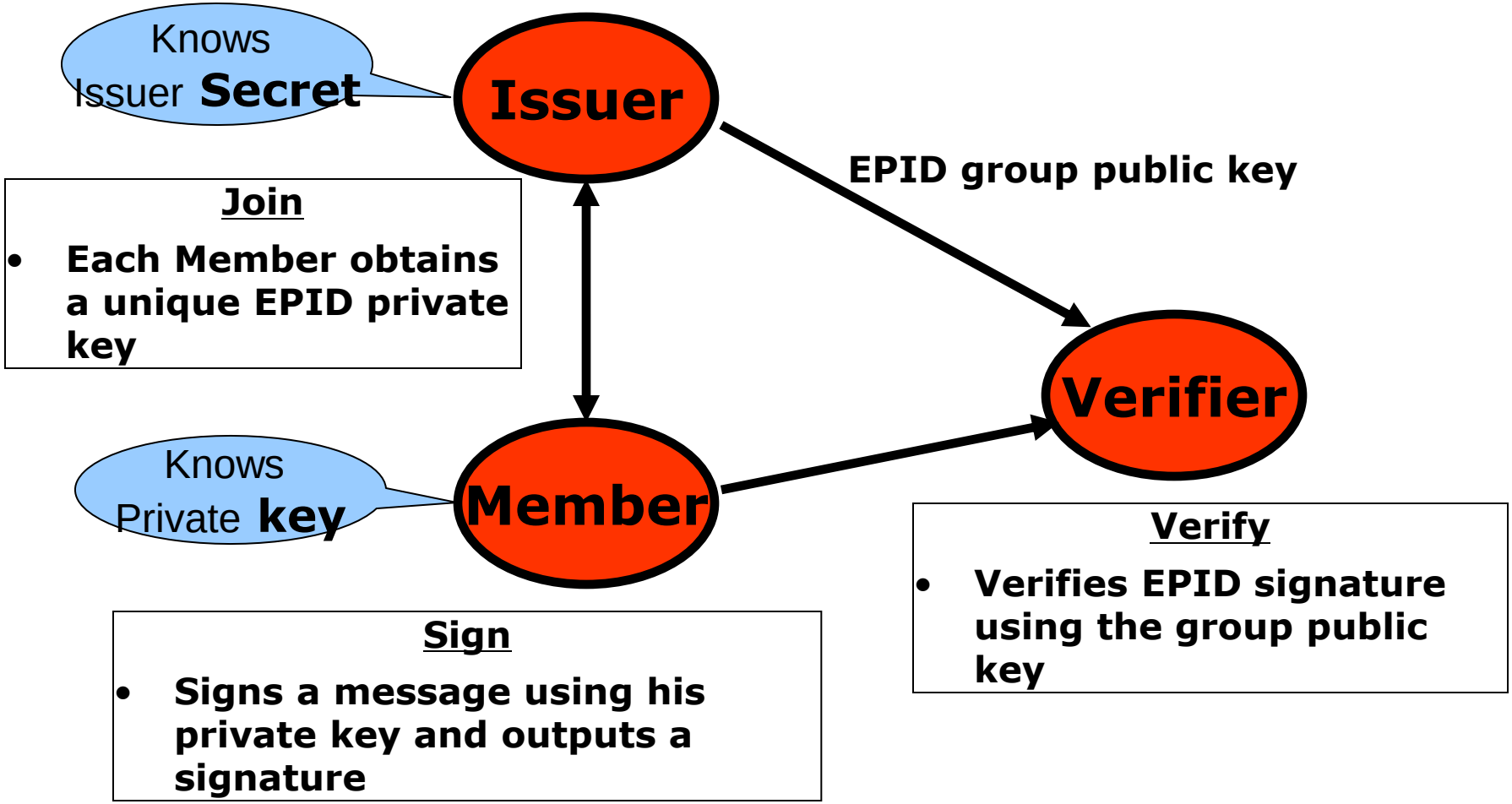
- EPID is a digital signature scheme with special properties
  - One group public key corresponds to multiple private keys
  - Each unique private key can be used to generate a signature
  - Signature can be verified using the group public key

Enhanced Privacy ID (EPID)

- Direct Anonymous Attestation (DAA)
  - A crypto scheme for providing anonymous signatures
  - DAA is designed specifically for TPM
  - RSA based DAA scheme adopted by TCG TPM Spec v1.2

- EPID is an extension of DAA
  - Flexible key generation and signature creation options
  - Additional revocation capabilities
  - Pairing based EPID scheme has improved efficiency

What is EPID


Knows
Issuer Secret
Issuer
EPID group public key
Join
Each Member obtains a unique EPID private key
Verifier
Knows
Private key
Member
Verify
Verifies EPID signature using the group public key
Sign
Signs a message using his private key and outputs a signature

Privacy Features of DAA/EPID

- EPID key issuing can be blinded
  - Issuer does not need to know Member Private Key
- EPID signatures are anonymous
- EPID signatures are untraceable
  - Nobody including the issuer can open an EPID signature and identify the member
  - This is the main difference between group signatures
- Unlinkability property depends upon Base
  - Signature includes a pseudonym B^f where
    - B is base chosen for a signature and revealed during the signature
    - f is unique per member and private
  - Random base: Pseudonym R^f where R is random
    - signatures are unlinkable
  - Name base: Pseudonym N^f all where N is name of verifier
    - Signatures still unlinkable for different verifiers
    - Signatures using common N are linkable

Revocations in EPID

- Private key revocation (Revealed Key List)
  - Ex: Private key is corrupted and is published
  - Revocation check performed by verifier
- Verifier Local Revocation using name base
  - Ex: Verifier can revoke a Pseudonym for his name (N^f)
  - Revocation check performed by verifier
- Signature based revocation (Signature Revocation List)
  - Issuer and/or verifier decide that they no longer want to accept signatures from whatever signed a "revoked" message with pseudonym B^f
  - For each future signature,
    - Member signs as normal
    - Member proves he didn't sign the revoked message
  - Retains same anonymity and unlinkability properties

More on signature based revocation

- Signature Revoke list
  - $K_i = B_i^{fi}$ for many pseudonyms
- Member produces a pseudonym $K = B^f$ in a signature
- The Member performs a Not My Pseudonym Proof, for each pseudonym in Signature Revoke list, i.e., for each (B_i, K_i), the member proves that $K_i \neq B_i^f$
- Signature Revoke list signed by Revocation authority and checked by Member device

Outline

- Digital signatures on FW updates
- Hardware Random number generation
- Anonymous platform attestation
- **Trusted Boot**
- Improved protection for user authentication
- Enhancements for cryptographic performance
- Protection from Side Channel Attacks

TPM Measured Boot

- Measured boot –
  - Boot anything
  - Store a trusted measurement of the boot process
  - Provide trusted reporting of the measurement
- TPM – Trusted Platform Module
  - Separate microprocessor
- During platform boot, the HW does a hash of the initial boot code and sends that to the TPM.
- TPM can digitally sign the hash

Verified Boot

- Verified boot –
  - Boot only code that passes verification
- Uses Intel's Trusted eXecution Technology Launch Control Policy
- The HW verifies that the measurements made during launch are good
- If not, then the selected policy option is invoked. Examples:
  - Platform boots to a fall back environment
  - Platform does not boot

Outline

- Digital signatures on FW updates
- Hardware Random number generation
- Anonymous platform attestation
- **Improved protection for user authentication**
- Enhancements for cryptographic performance
- Protection from Side Channel Attacks

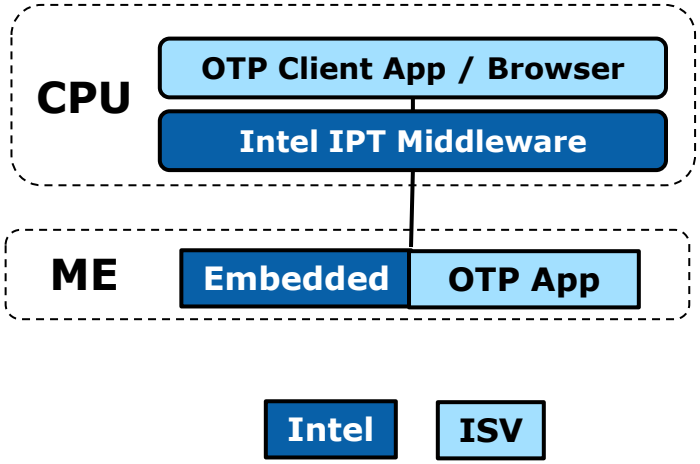
IPT 1.0: One Time Password (OTP)

The first generation of Intel® IPT is a dynamic code generated on an embedded microprocessor that is protected from malware in the OS.

- Single use, (i.e. 30 second, time-limited code → OTP)
- A hardware level 2nd factor of authentication
- Works with leading OTP Solutions from Symantec & Vasco

Traditional hardware token

Now embedded into your PC



Outline

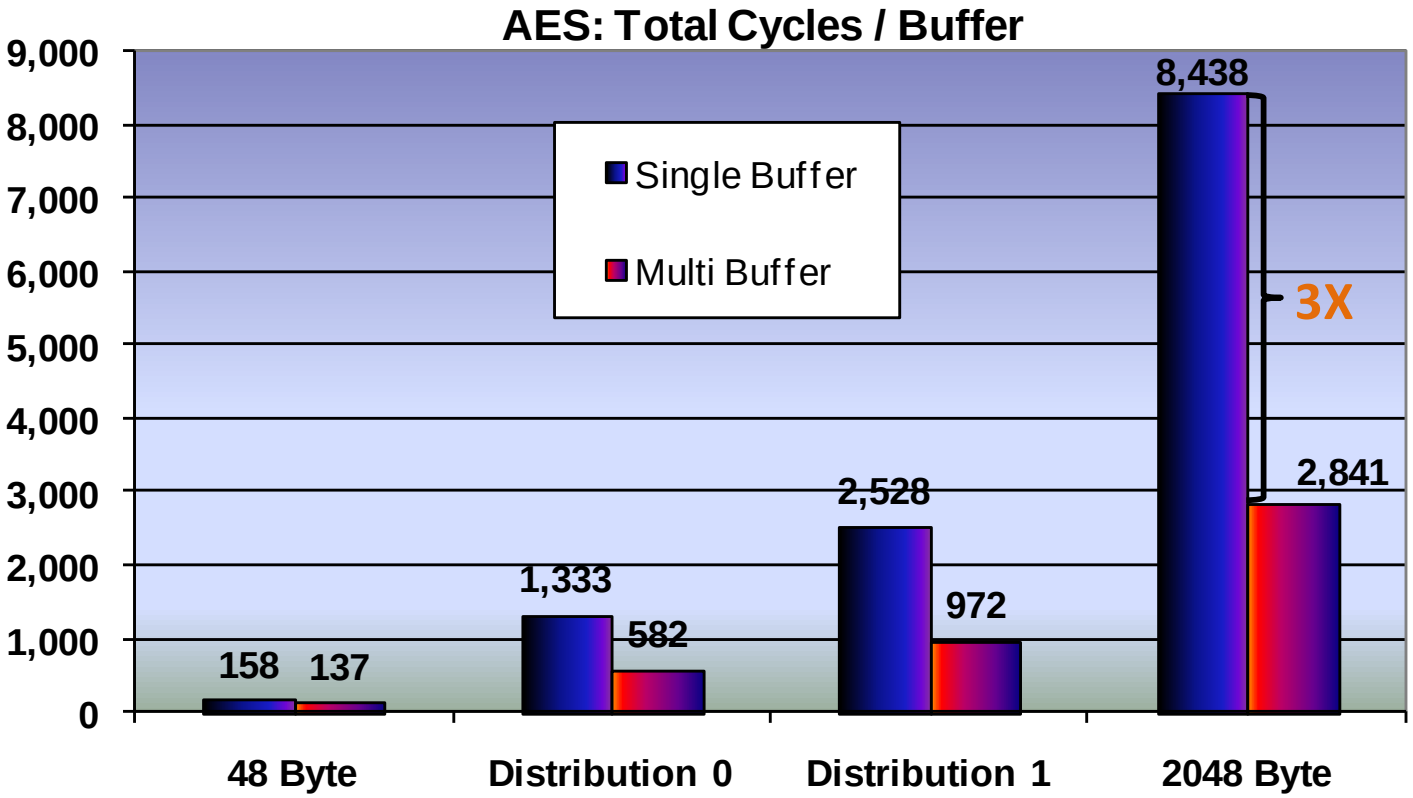
- Digital signatures on FW updates
- Hardware Random number generation
- Anonymous platform attestation
- Improved protection for user authentication
- **Enhancements for cryptographic performance**
- Protection from Side Channel Attacks

Crypto Performance

- Software improvements
  - Multi-buffer
  - Function Stitching
- Hardware improvements
  - AES-NI
  - PCLMULQDQ
  - Microarchitecture improvements

Multi Buffer Performance – 1 WSM Core

Multi-buffer: Perform the same function on multiple independent data buffers

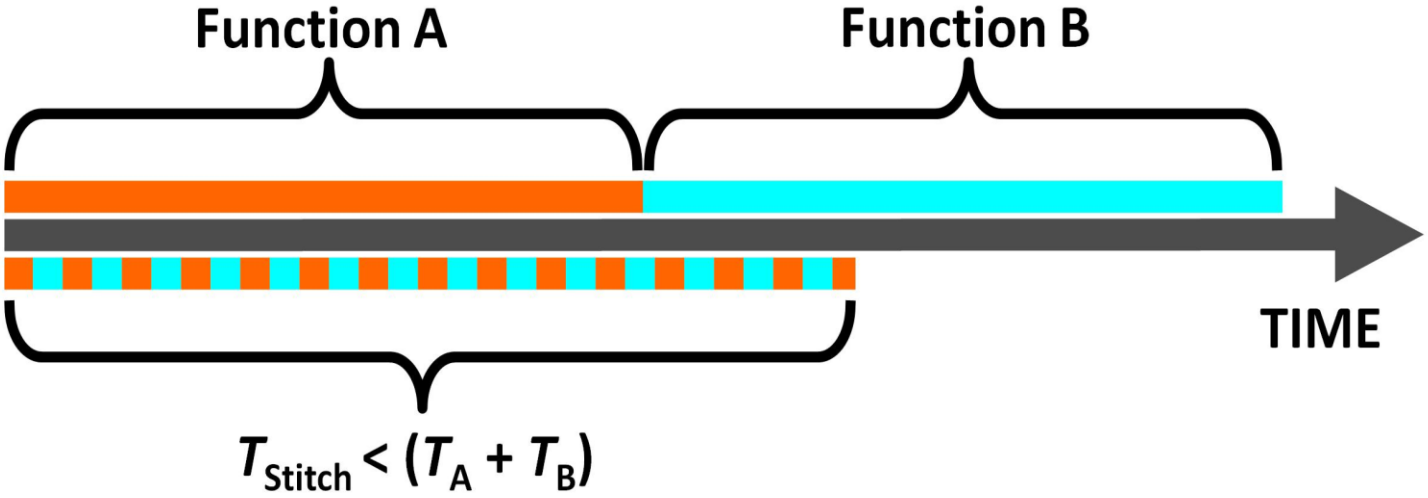


Excellent performance on AES CBC Encrypt

**See Intel technical paper # 2 for full description of methodology and results.*

Function Stitching

- Protocols such as SSL/TLS and IPsec apply two functions, confidentiality and integrity
- Improved performance by using multiple execution units more efficiently
- Fine grain integration achieves higher performance
- 1.4X Speedup on AES128 CBC-Encrypt with SHA1 (Cycles/Byte)



Method to speedup combined Encrypt/Authenticate

***See Intel technical paper # 3 for full description of methodology and results.**

OpenSSL Performance Improvements

- Intel developed and released highly optimized cryptographic functions into OpenSSL
- ~28 Gigabits/second of large secure connections using AES256-SHA1 with RSA1024 for session setup
- 4.8x faster than latest default version at the system level
- Dual Intel® Xeon® Processor X5680 system running the Apache Web-Server application, sending HTTP over SSL to clients on a network.

*See Intel technical paper # 14 for full description of methodology and results.

Sandy Bridge Performance

- SNB 2nd Generation Intel® Core™ improves:
  - AES-NI Throughput
  - SIMD Processing via AVX ISA extensions
  - Large-integer processing (public-key crypto)

- Multi Buffer Performance (Cycles/byte)

Algorithm	i5-650	i7-2600	i7-2600 Gain
MD5	1.46	**1.27**	**1.15**
SHA1	2.96	**2.2**	**1.35**
SHA256	6.96	**5.27**	**1.32**
AES128-CBC-Encrypt	1.52	**0.83**	**1.83**

- Modular Exponentiation Performance (Cycles)

Algorithm	i5-650	i7-2600	i7-2600 Gain
512-bit Modular Exponentiation	360,880	**246,899**	**1.46**
1024-bit Modular Exponentiation	2,722,590	**1,906,555**	**1.43**

1.2-1.8X additional performance gain on SNB!

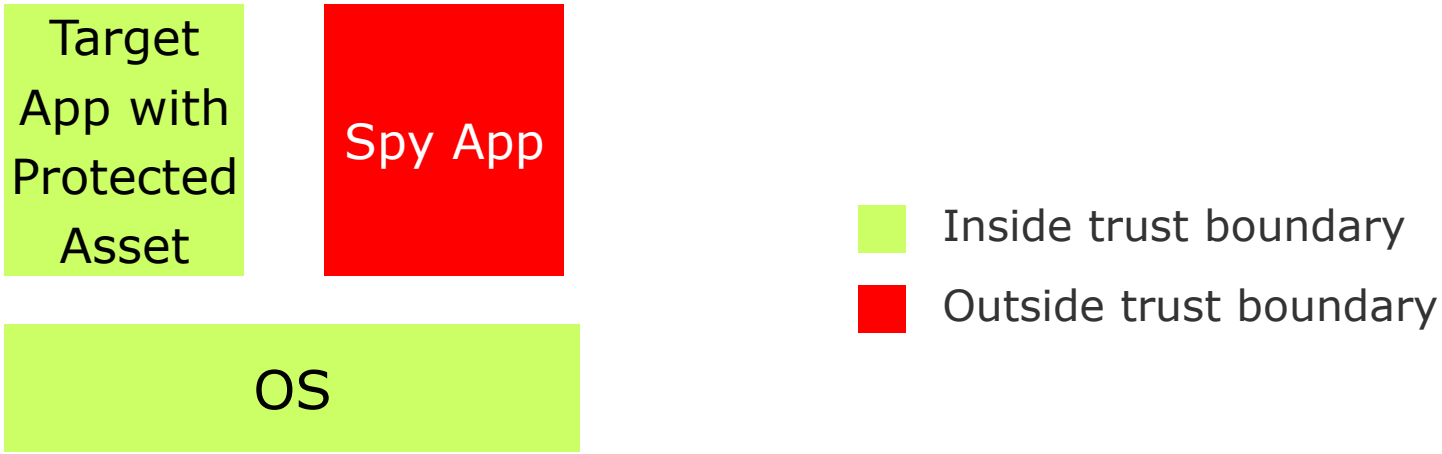
**See Intel technical paper # 10 for full description of methodology and results.*

Outline

- Digital signatures on FW updates
- Hardware Random number generation
- Anonymous platform attestation
- Improved protection for user authentication
- Enhancements for cryptographic performance
- **Protection from Side Channel Attacks**

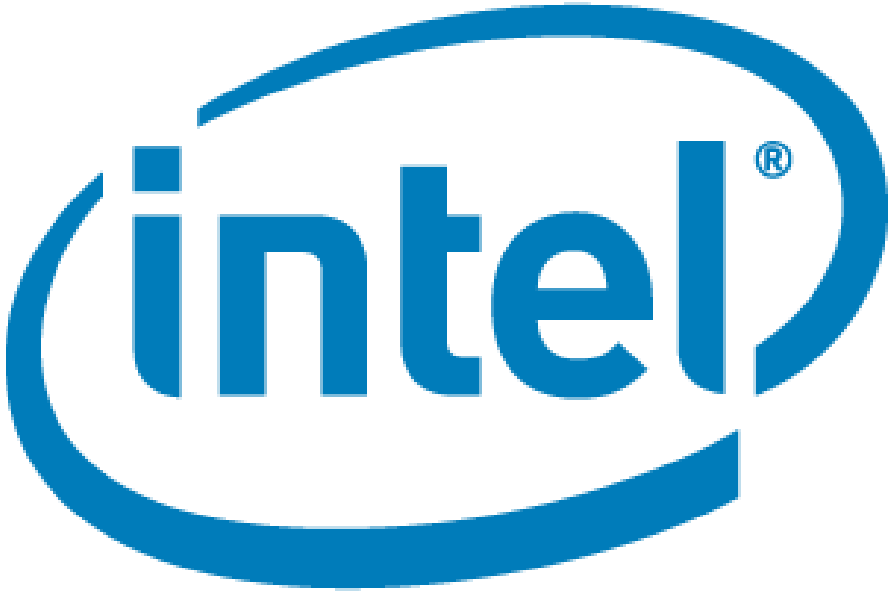
Software Side Channels

- Not Hardware Side Channel where adversary has physical access.
- Not Software Covert Channel where adversary has malware in a high security partition and a low security partition
- Software Side Channel – Adversary has malware executing in a spy process, and tries to obtain information about an uncompromised target process executing on same platform.



Protection from software side channels

- Platform approach for software side channels
  - AES-NI: CPU instructions for a round of AES
  - PCLMULQDQ: CPU instructions for GF(2) Multiplication
  - Recommend side channel mitigated implementations of other crypto algorithms
    - No secret key or data dependent memory access (at coarser than cache line granularity)
    - No secret key or data dependent code branching
    - Ex: RSA implemented with <6% performance reduction in OpenSSL


intel

Technical Papers - 1

1. **Breakthrough AES performance with Intel AES New Instructions**
   http://software.intel.com/file/26898
2. **Processing Multiple buffers in parallel**
   http://download.intel.com/design/intarch/papers/324101.pdf
3. **Fast Cryptographic computation on IA processors via Function Stitching** http://download.intel.com/design/intarch/PAPERS/323686.pdf
4. **Fast and Constant-time Implementation of Modular Exponentiation**
   http://www.cse.buffalo.edu/srds2009/escs2009_submission_Gopal.pdf
5. **Fast CRC Computation for iSCSI Polynomial using CRC32 Instruction**
   http://download.intel.com/design/intarch/papers/323405.pdf
6. **Optimized Galois-Counter-Mode Implementation on IA Processors**
   http://download.intel.com/design/intarch/PAPERS/324194.pdf
7. **High Performance Storage Encryption on Intel® Architecture Processors**
   http://download.intel.com/design/intarch/PAPERS/324310.pdf

Technical Papers - 2

8. **Fast CRC Computation for Generic Polynomials using PCLMULQDQ Instruction** http://download.intel.com/design/intarch/papers/323102.pdf
9. **High Performance DEFLATE Decompression on Intel® Architecture Processors** http://edc.intel.com/Link.aspx?id=3972
10. **Cryptographic Performance on the 2nd Generation Intel Core Processor** http://download.intel.com/design/intarch/PAPERS/324952.pdf
11. **Fast Parallel CRC Computation using the Nehalem CRC32 instruction** http://drdobbs.com/cpp/229401411
12. **Using Intel® AES New Instructions and PCLMULQDQ to Significantly Improve IPSec Performance on Linux** http://download.intel.com/design/intarch/papers/324238.pdf
13. **IDF 2010 Presentation with Voice: Examining the Performance of Intel AES New Instructions on Intel Core i7 Processor** http://intelstudios.edgesuite.net/idf/2010/sf/aep/SFTS012/SFTS012.html
14. **Improving OpenSSL Performance on IA** http://download.intel.com/design/intarch/papers/326232.pdf