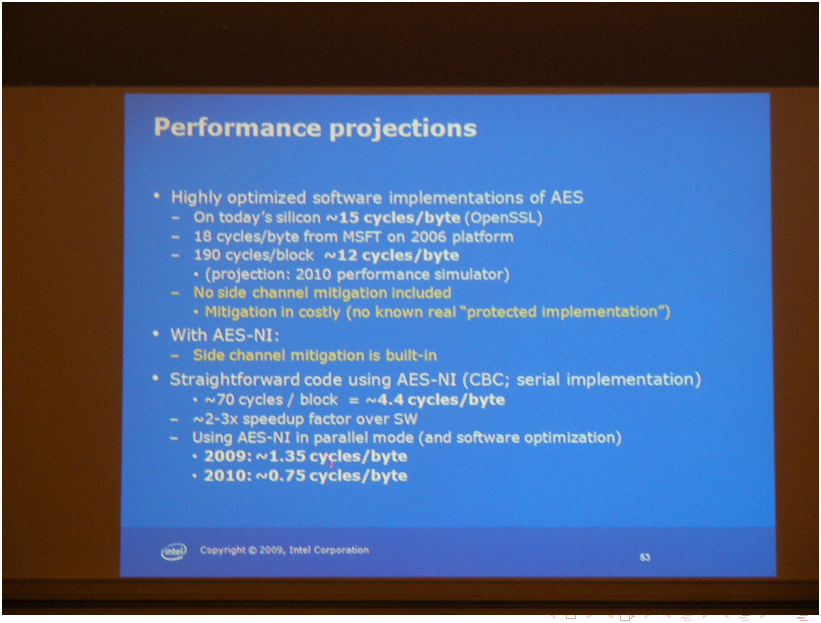
Fast Software Encryption: How Fast is AES?

Emilia Käsper, Peter Schwabe

K.U. Leuven, TU Eindhoven

FSE 2009
Leuven, February 2009

What Intel says...



Performance projections

- Highly optimized software implementations of AES
  - On today's silicon **~15 cycles/byte** (OpenSSL)
  - 18 cycles/byte from MSFT on 2006 platform
  - 190 cycles/block **~12 cycles/byte**
    - (projection: 2010 performance simulator)
  - No side channel mitigation included
    - Mitigation in costly (no known real "protected implementation")
- With AES-NI:
  - Side channel mitigation is built-in
- Straightforward code using AES-NI (CBC; serial implementation)
    - ~70 cycles / block = **~4.4 cycles/byte**
  - ~2-3x speedup factor over SW
  - Using AES-NI in parallel mode (and software optimization)
    - **2009: ~1.35 cycles/byte**
    - **2010: ~0.75 cycles/byte**

53

What we said last year...

Bernstein, Schwabe: New AES software speed records, Indocrypt 2008

- Motorola PowerPC G4 7410: **14.57** cycles/byte
- Intel Pentium 4, f12: **14.13** cycles/byte
- Sun UltraSparc III: **12.06** cycles/byte
- Intel Core 2 Quad Q9550: **10.57** cycles/byte
- AMD Athlon 64 X2 3800+: **10.43** cycles/byte

AES implemented in CTR mode

What we say now...

Käsper: Even faster AES on Core 2

- AES in CTR mode
- Written in assembly using 128-bit XMM registers
- Processing 8 AES blocks in parallel
- Bitsliced implementation = cache-timing resistant
- Intel Core 2 Quad Q9550: **8.1** cycles/byte (in full compatibility mode)
- First bitsliced implementation that is also fast for short packet encryption

Applications

- Hashing
  - Bitslicing is possible for SHA-3 candidates LANE, ECHO which process multiple AES blocks in parallel
- Authenticated encryption
  - Galois Counter Mode
  - Intel Core 2 Quad Q9550: **11.5** cycles/byte