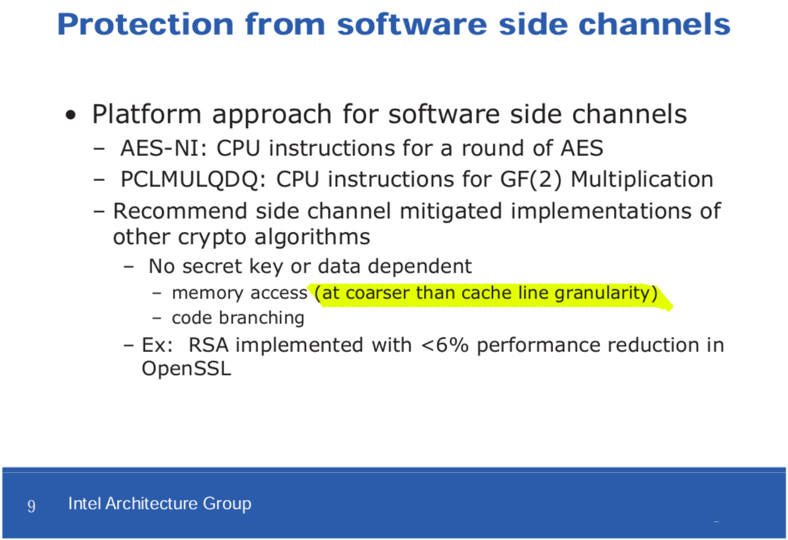
A word of warning

Daniel J. Bernstein and Peter Schwabe

August 22, 2013

CHES 2013 Rump Session

“Accesses to different memory locations within the same cache line take the same amount of time”



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)
      - code branching
    - Ex: RSA implemented with <6% performance reduction in OpenSSL

9 Intel Architecture Group

(Ernie Brickell in his invited talk at CHES 2011)

```
(uint32) secret &= 7
(uint32) secret <<= 3
secret += 4096

x = 0
y = 0

loop = 1000000
mainloop:
  x = *(uint64 *) (storage + 0)
  *(uint64 *) (storage + secret) = y

                 signed>? loop -= 1
goto mainloop if signed>
```

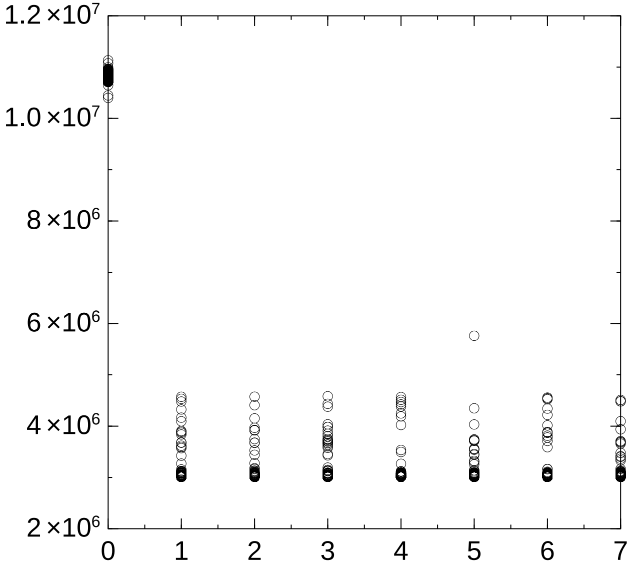
```
(uint32) secret &= 7
(uint32) secret <<= 3
secret += 4096

x = 0
y = 0

loop = 1000000
mainloop:
  x = *(uint64 *) (storage + 0)
  *(uint64 *) (storage + secret) = y

                 signed>? loop -= 1
goto mainloop if signed>
```

. . . approximation to actual cryptographic code, but clearly following the rules.


1.2×10^7
1.0×10^7
8×10^6
6×10^6
4×10^6
2×10^6
0
1
2
3
4
5
6
7