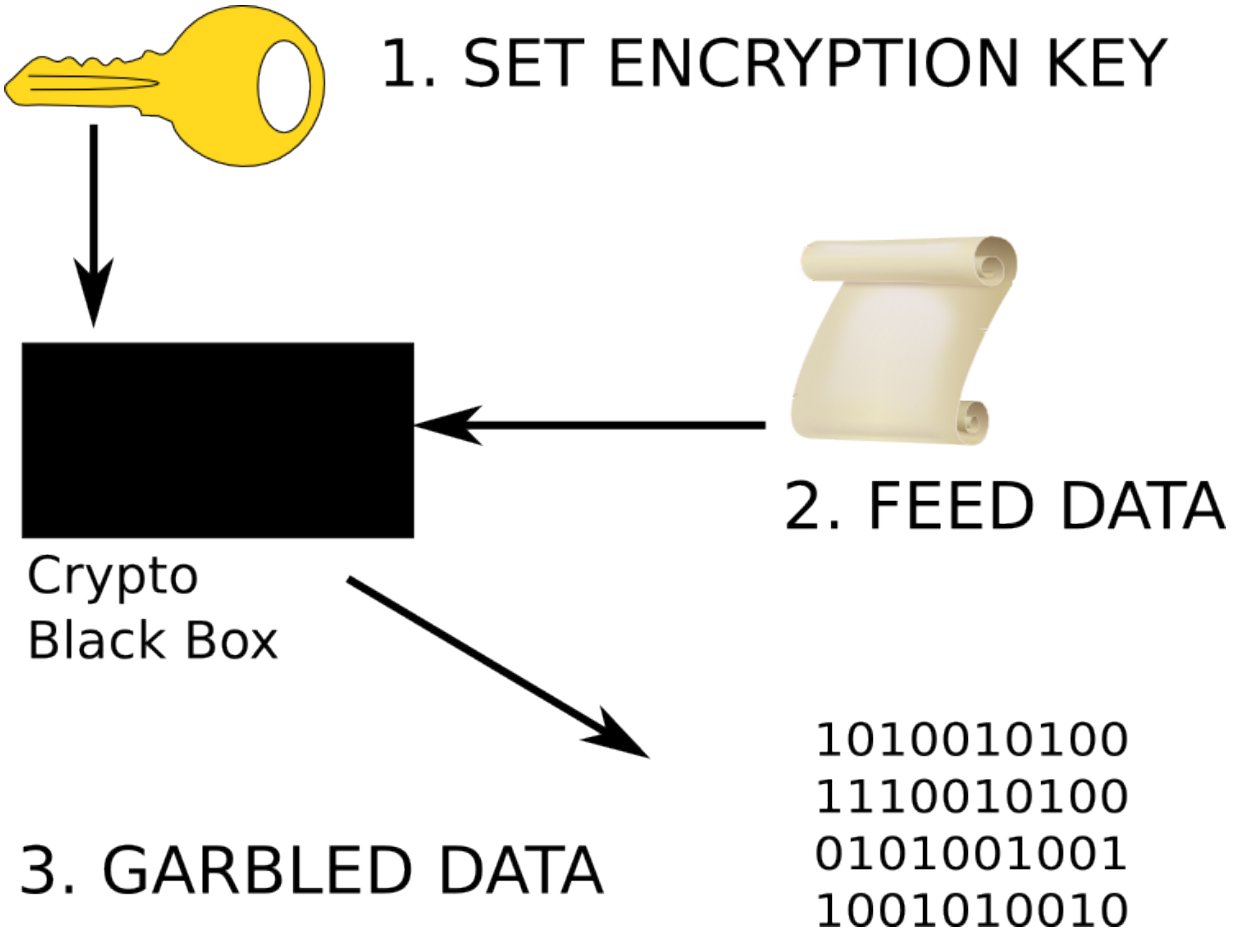
Snails on Speed

Short History of Commodity Crypto Acceleration

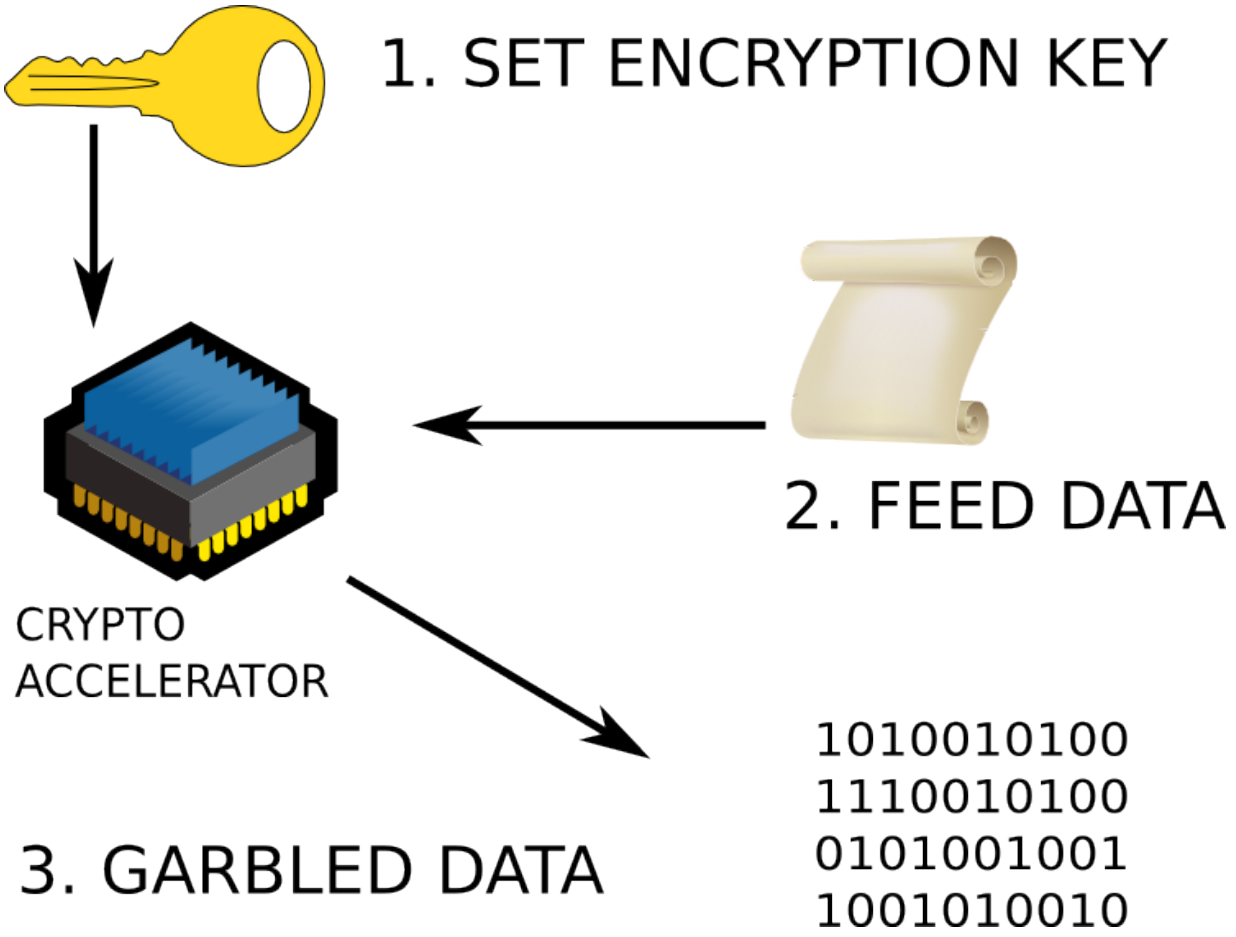
Presented for DC4420
2015-02-24

Mika Boström <mika.bostrom@iki.fi>

Crypto Overview



Crypto Overview - Accelerated



Chronology

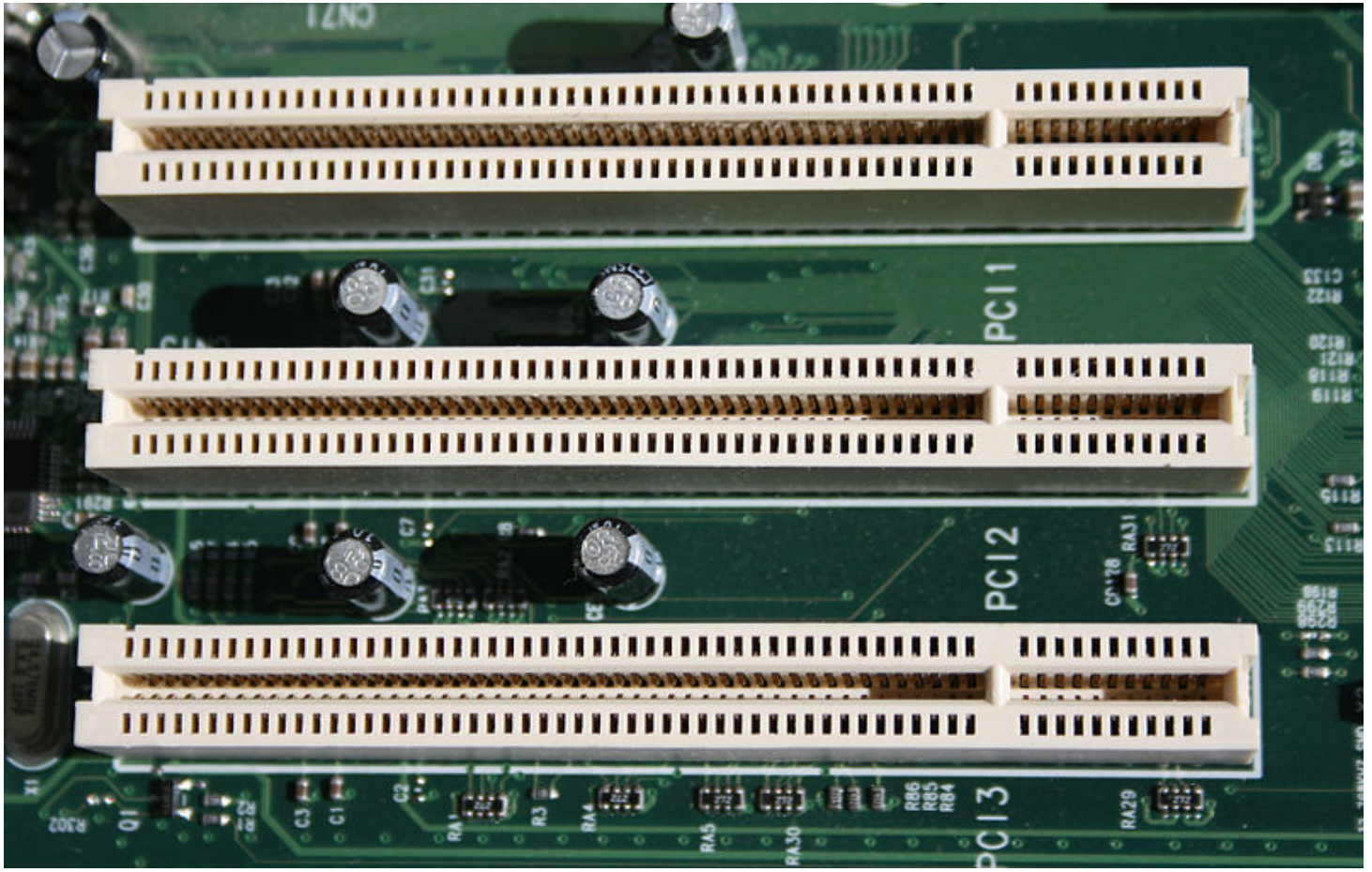
- Smart Cards
- Peripheral chips – hifn
- VIA Padlock
- SoC built-in – NXP & others
- AES-NI – Intel
- Other embedded

Image source: http://www.nite.ac.in/images/smart_card.png

External Accelerator

Source: http://soekris.com/products/vpn14x1/vpn-1401.html

PCI: peripheral bottleneck



Peak transfer rate: 133 MB/s
Effective crypto engine rate: ≤ 66 MB/s

OpenSSL speed

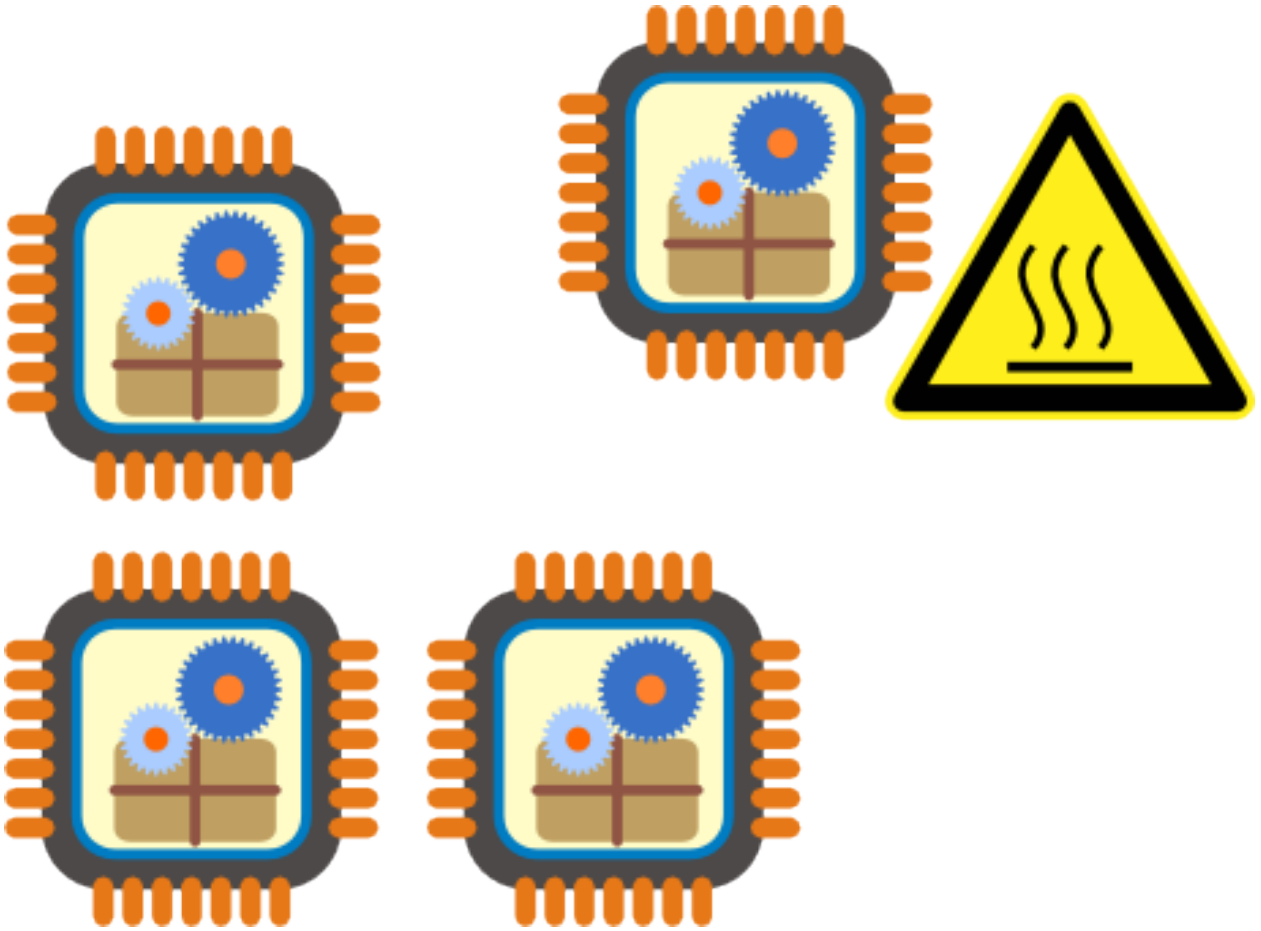
Software on single core (low-end laptop)

TYPE (CBC)	16B	64B	256B	1024B	8192B
AES-128	117 MB/s	131 MB/s	134 MB/s	134 MB/s	135 MB/s
AES-192	101 MB/s	109 MB/s	111 MB/s	111 MB/s	112 MB/s
AES-256	87 MB/s	93 MB/s	95 MB/s	95 MB/s	96 MB/s

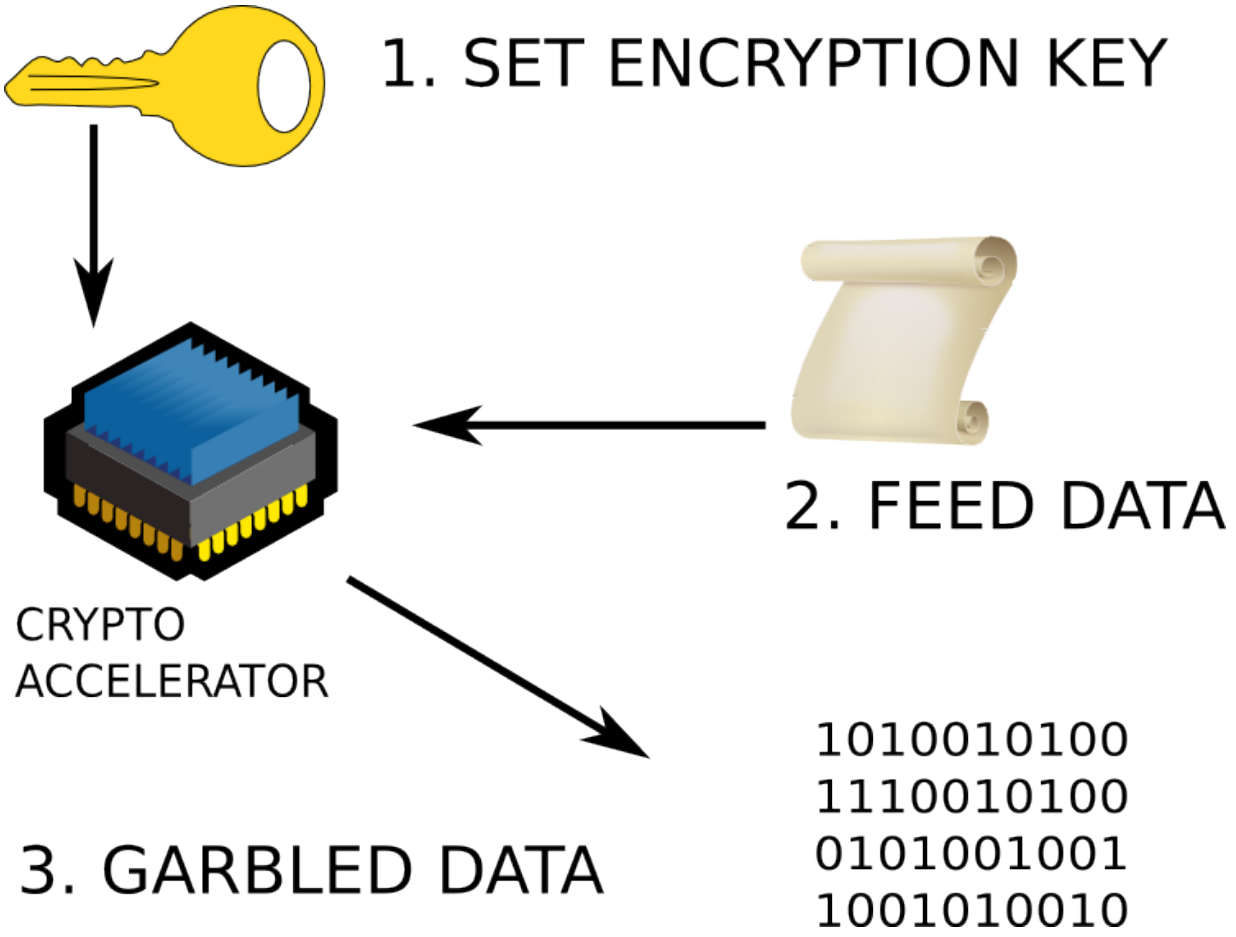
Way faster than with any peripheral PCI device

Generate your own numbers:
% `openssl speed aes`

”Software Acceleration”



Hardware Acceleration



Commodity Implementations

Linux

CryptoAPI

= Kernel drivers

`cryptsetup`

`IPSec (XFRM)`

OpenBSD

`/dev/crypto`

Patch for OpenSSL

Build option for GnuTLS

Java 8 with AES Intrinsics

Cryptodev for Linux: http://cryptodev-linux.org/
NOTE: not maintained anymore

Pros

- Immutable
- ASIC
- Low overhead
- Constant time

Cons

- Immutable
- ASIC
- Impossible to verify
- Requires protective shielding and casing

Pros / Cons

- Immutable
- ASIC
- Low overhead
- Constant time
- Drop-in replacement for library implementations

- Immutable
- ASIC
- Impossible to verify
- Requires protective shielding and casing
- How does one drop out?

Random Fallacies

”Nobody would ever peel off the contact and poke platinum electrodes inside the chip”

Random Fallacies

”The execution times are key-independent”

Random Fallacies

”Power consumption is not a side channel”

Random Fallacies

Or the more generic form...

Universal Fallacy

”*Nobody would ever do that*”

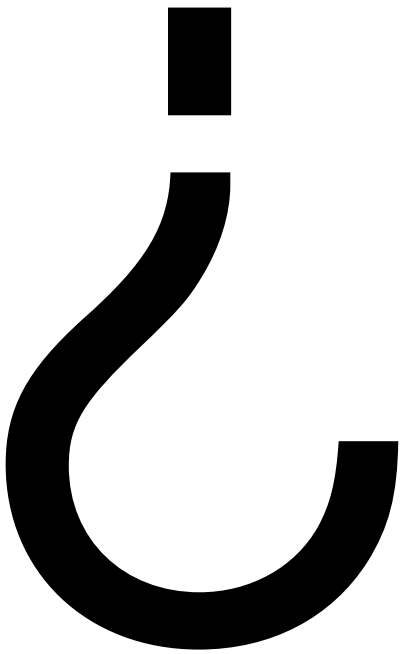
Easy Ways To Screw Up

- Hardware Crypto != Security Module
- Forget Key Cleanup *
- Lookup Timings
- Bad Software

+ Bad AppSec

* See: reduced-round [differential] attacks against AES

Question Time



Mika Boström <mika.bostrom@iki.fi>

No Twitter. No Facebook.

This page had an image of beer