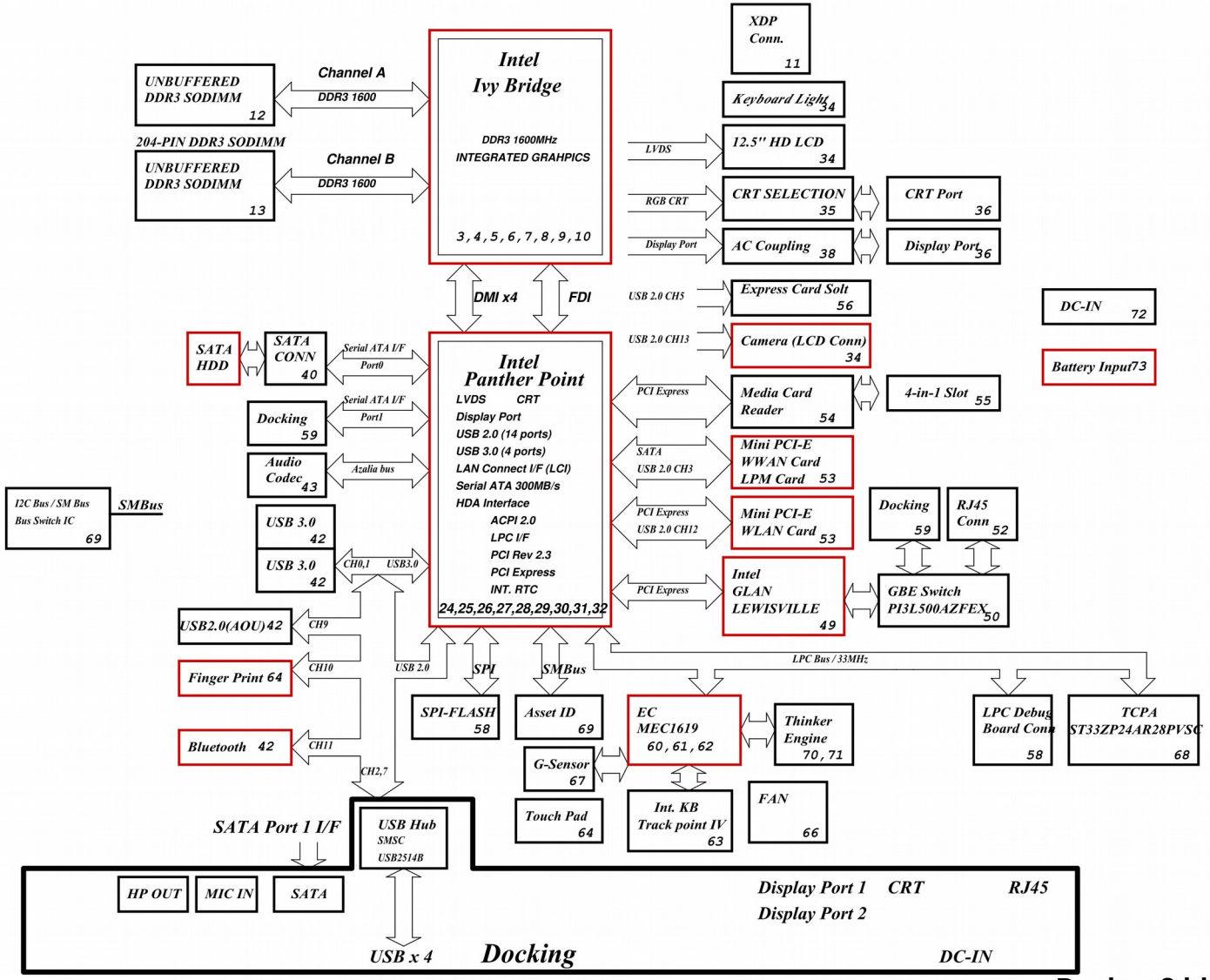
Regaining Trust in Everyday Computers the Hacky Way™

<33c3@jaseg.net>

What is the problem?

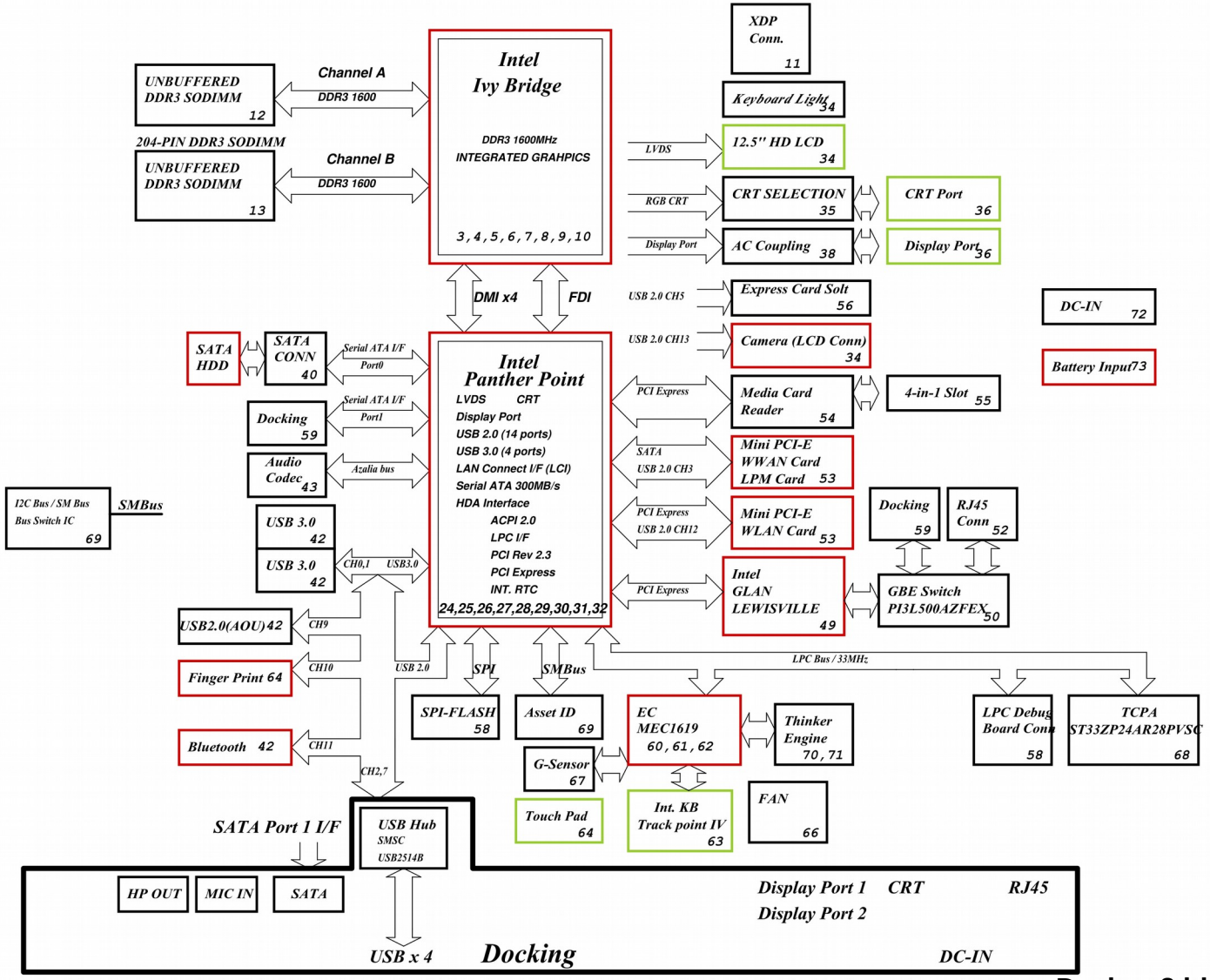
The NSA, The NSA, 2006 or so (public domain)

Specifically...

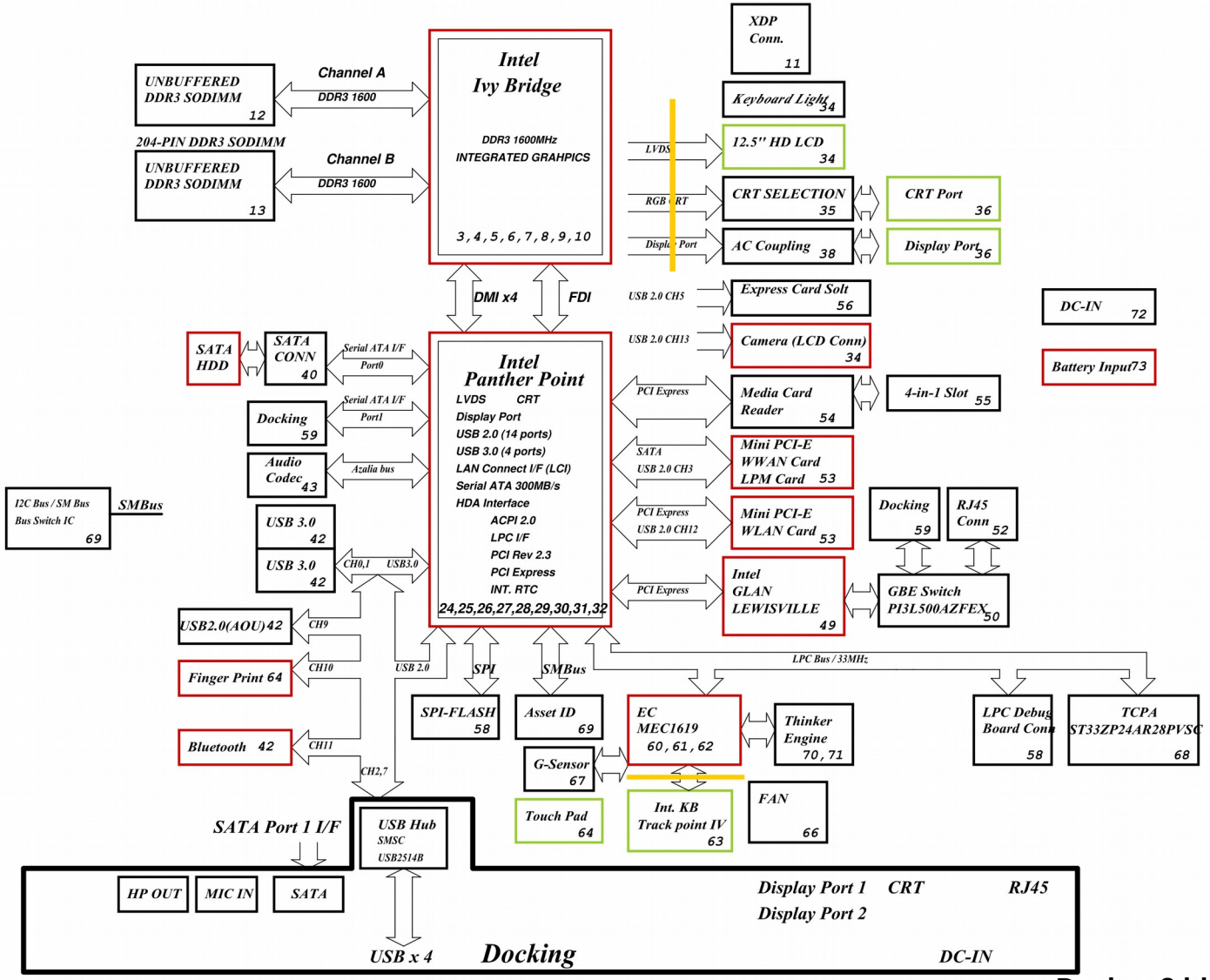


Dasher-2 block diagram, Lenovo

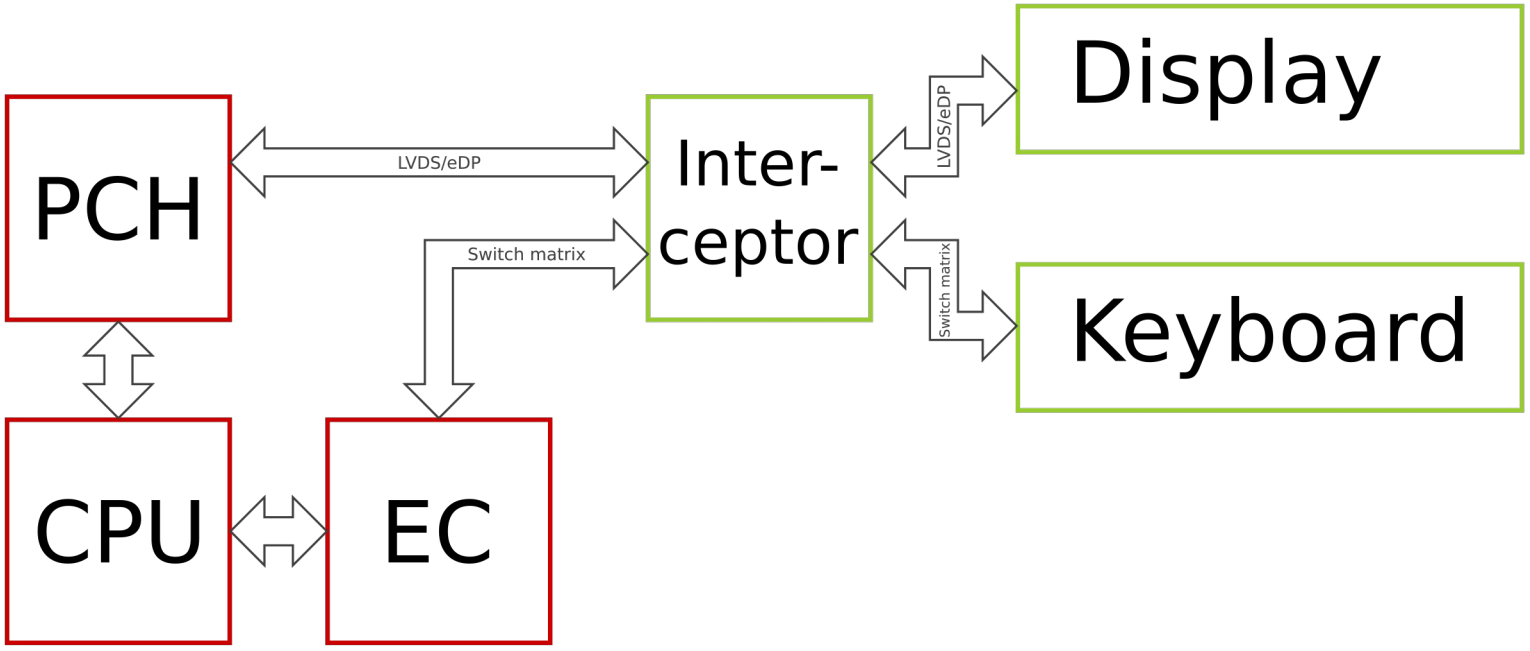
The NSA, The NSA, 2006 or so (public domain)

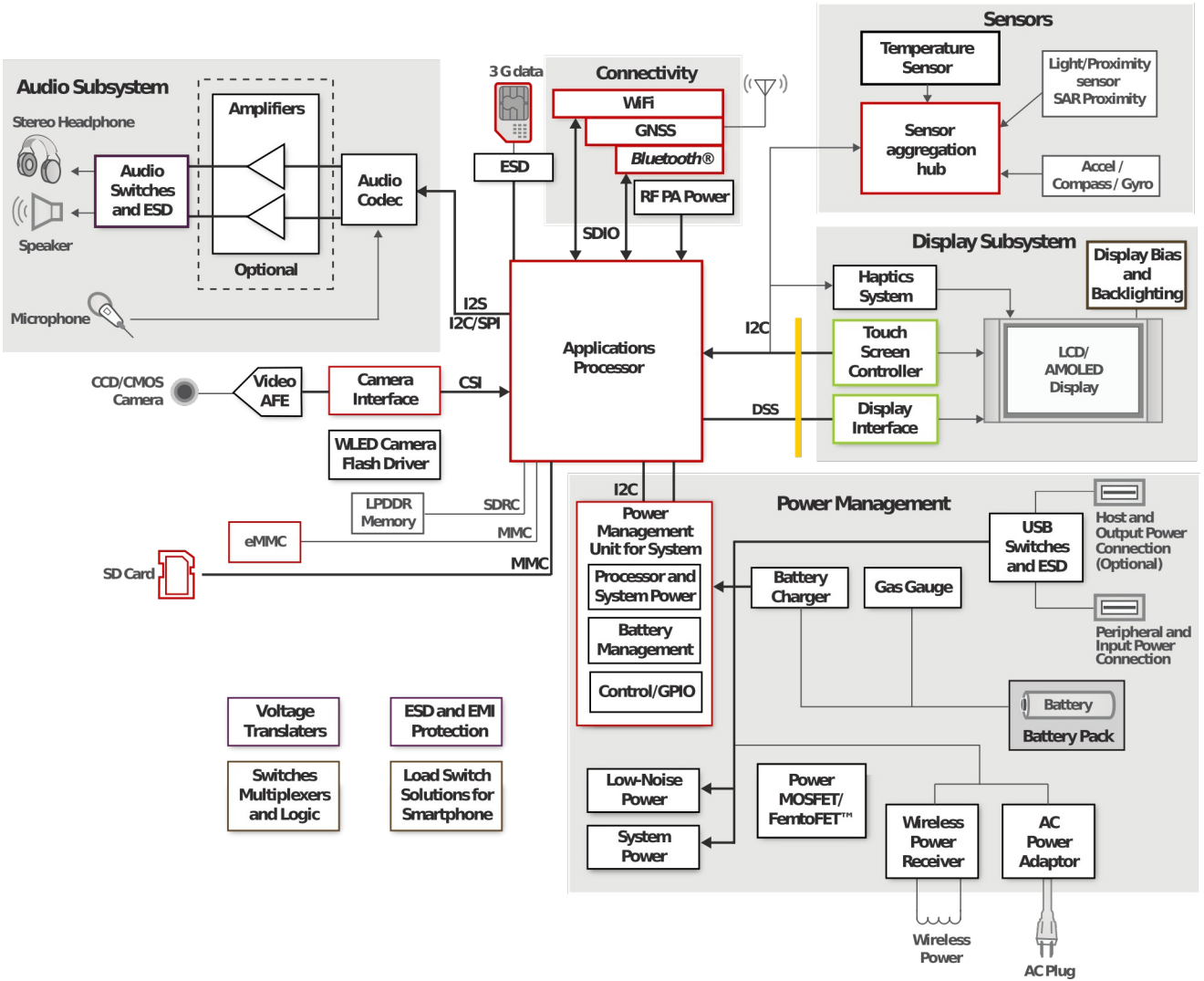


Dasher-2 block diagram, Lenovo

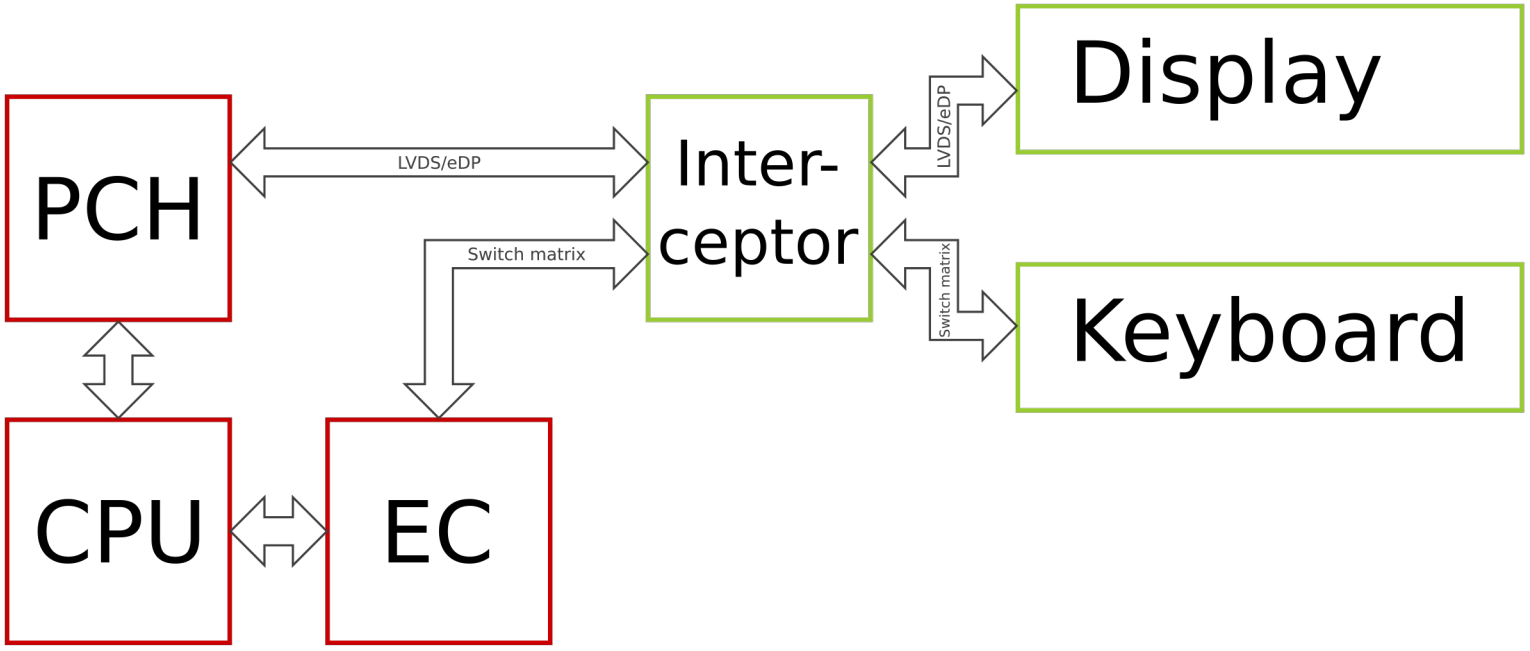


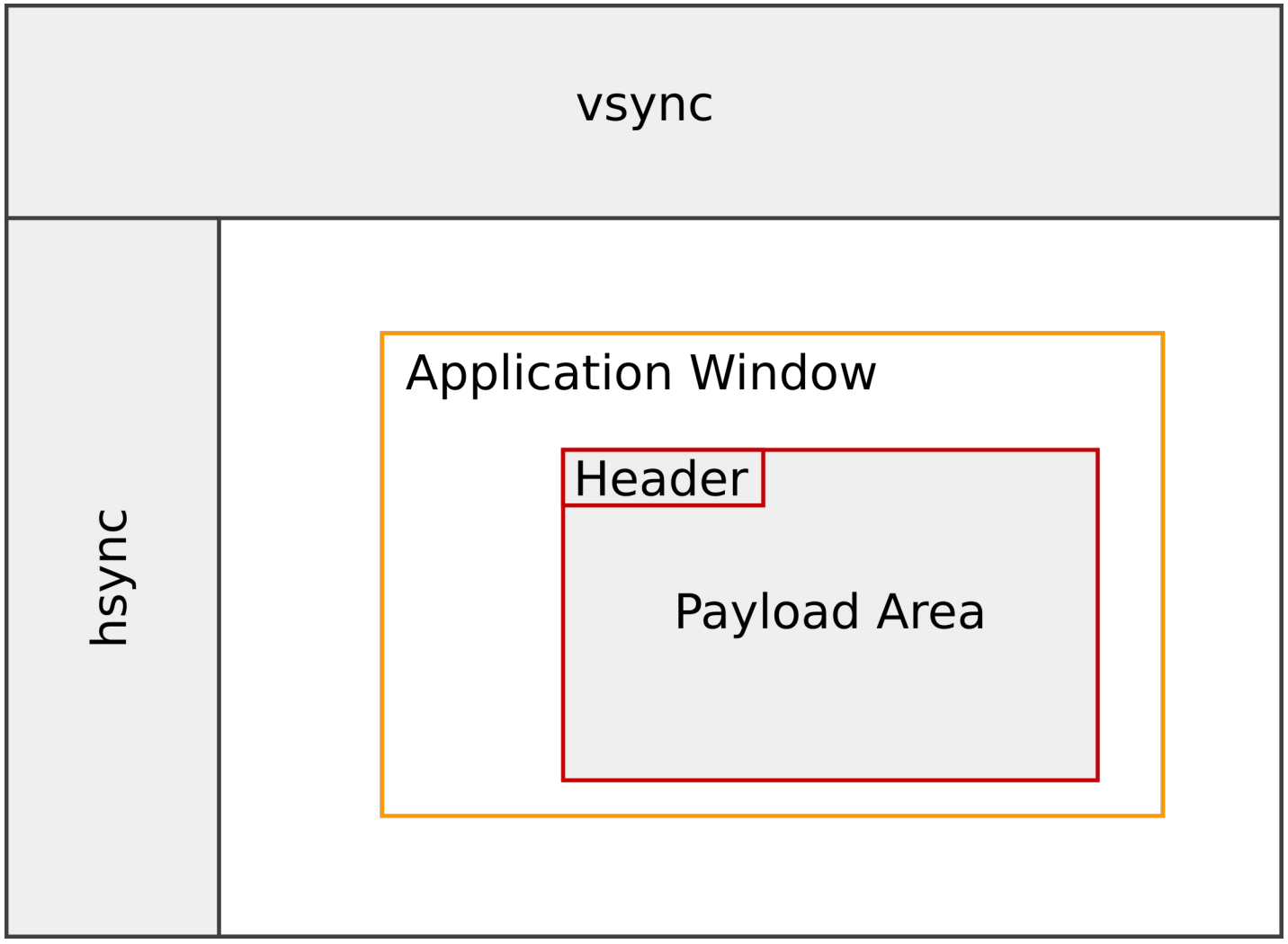
Dasher-2 block diagram, Lenovo

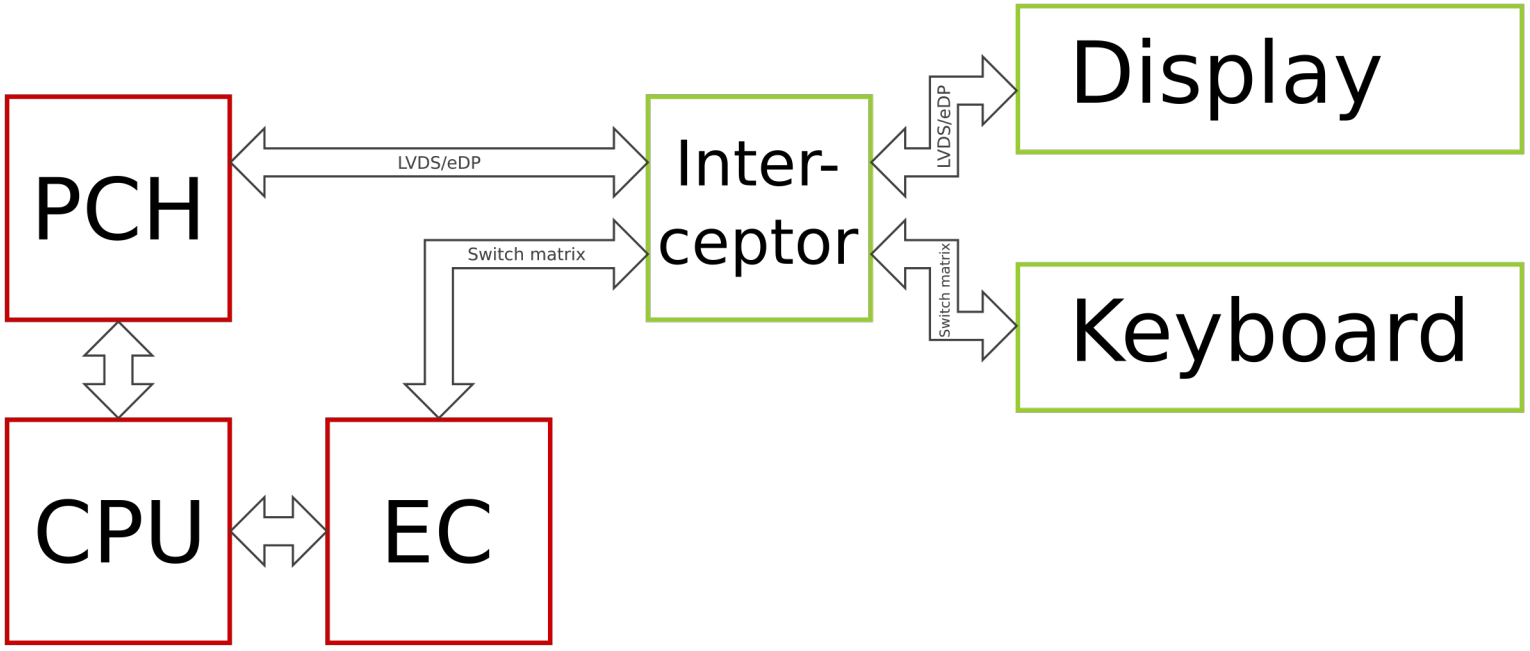

PCH
LVDS/eDP
Inter-
ceptor
LVDS/eDP
Display
Switch matrix
Switch matrix
Keyboard
CPU
EC

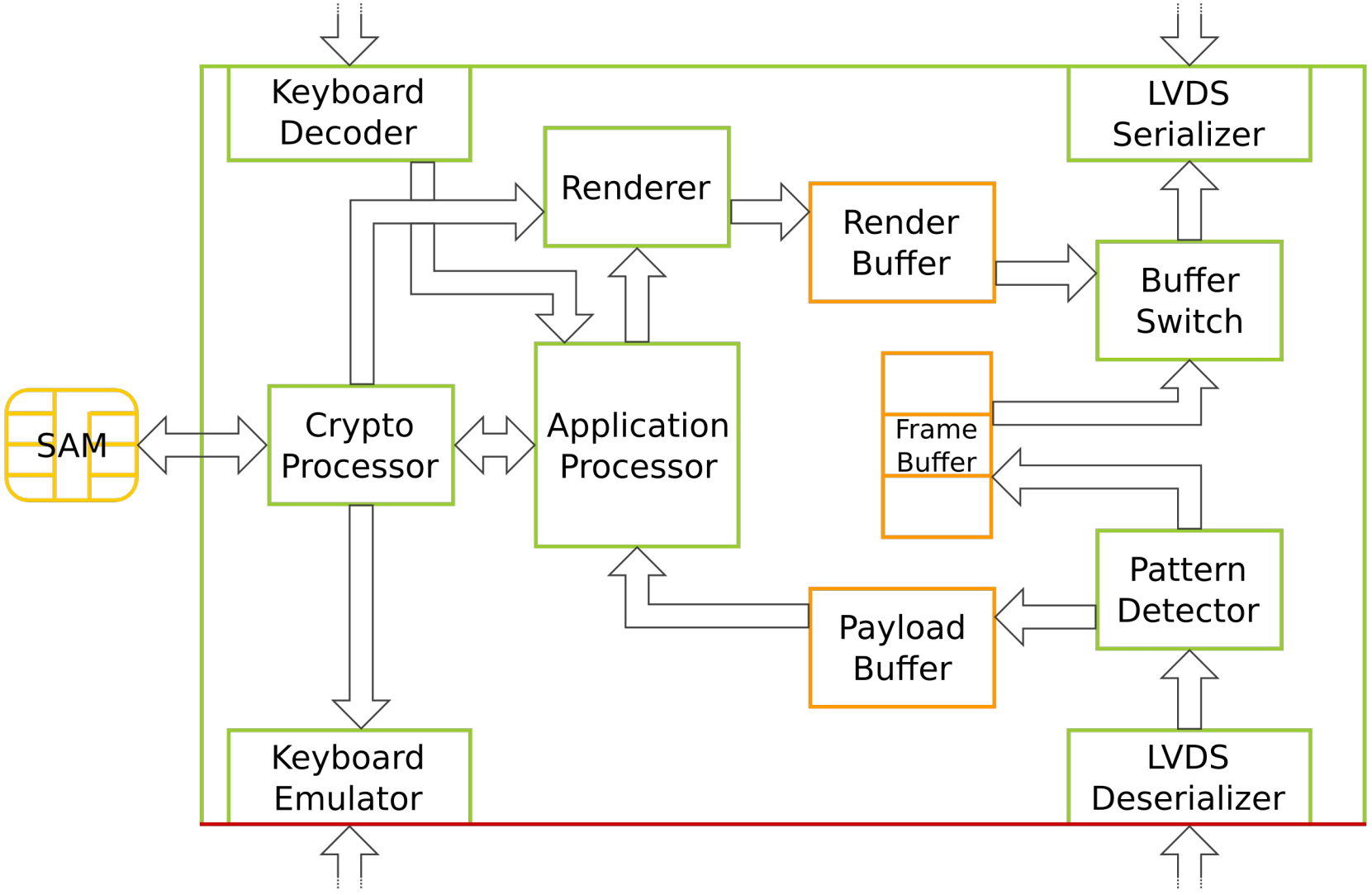


TI Smartphone Solutions Guide, Texas Instruments 2014


PCH
LVDS/eDP
Inter-
ceptor
LVDS/eDP
Display
Switch matrix
Switch matrix
Keyboard
CPU
EC


vsync
hsync
Application Window
Header
Payload Area


PCH
LVDS/eDP
Inter-
ceptor
LVDS/eDP
Display
Switch matrix
Switch matrix
Keyboard
CPU
EC


Keyboard Decoder
LVDS Serializer
Renderer
Render Buffer
Buffer Switch
SAM
Crypto Processor
Application Processor
Frame Buffer
Pattern Detector
Payload Buffer
Keyboard Emulator
LVDS Deserializer

HSM Intrusion Detection

- Mesh: Continuity testing a printed maze trace on case inside
- RF Interference: Continuously measuring RF characteristics of wire stuffed into case chaotically
- Ultrasonic: Continuously measuring ultrasonic propagation inside potting material
- Triboluminescence: Photodiodes detecting mechanical disturbance of clear potting material loaded with “friction-glow”/”smash-glow” crystals

Attack Surface

Protocol Decoder	→	Keep it simple, in hardware
Social Engineering	→	You are not idiots
Physical Compromise	→	Limited HSM features
FPGA Backdoor	→	Not terribly realistic?
Logic Flaws	→	Hardware-level Countermeasures
Device Loss	→	Continuous Re-authentication

Attack Scenarios

	w/o Interceptor	with Interceptor
Lost Device	?	✔
Police Raid/Unlocked Device Stolen	✘	✔
Targeted Attack	✘	✔
Audio/Video Bugging	✘	✘
Physical Access (Shipping/Border Checkpoint)	?	?
1984-style Total Communication Surveillance	✔	✔
Backdoored Interceptor	n/a	✘

Major Tasks

- Disassembling and reassembling LVDS/eDP
- Rendering Unicode
- Defining a secure packet format
- Getting keyboard pass-through semantics right
- Splitting crypto in a meaningful way
- Finding and making use of a smart card

33c3@jaseg.net
GPG: 7657 BF97 C679 07BD 7BC4 4B44 2877 9768 6E40 E32F
github.com/jaseg/tachibana_talk