HOW NOT TO PROTECT PC'S FROM POWER ANALYSIS

Yossi Oren and Adi Shamir
Computer Science Dept
The Weizmann Institute
Israel

The most dangerous part in a PC:

Its USB port!

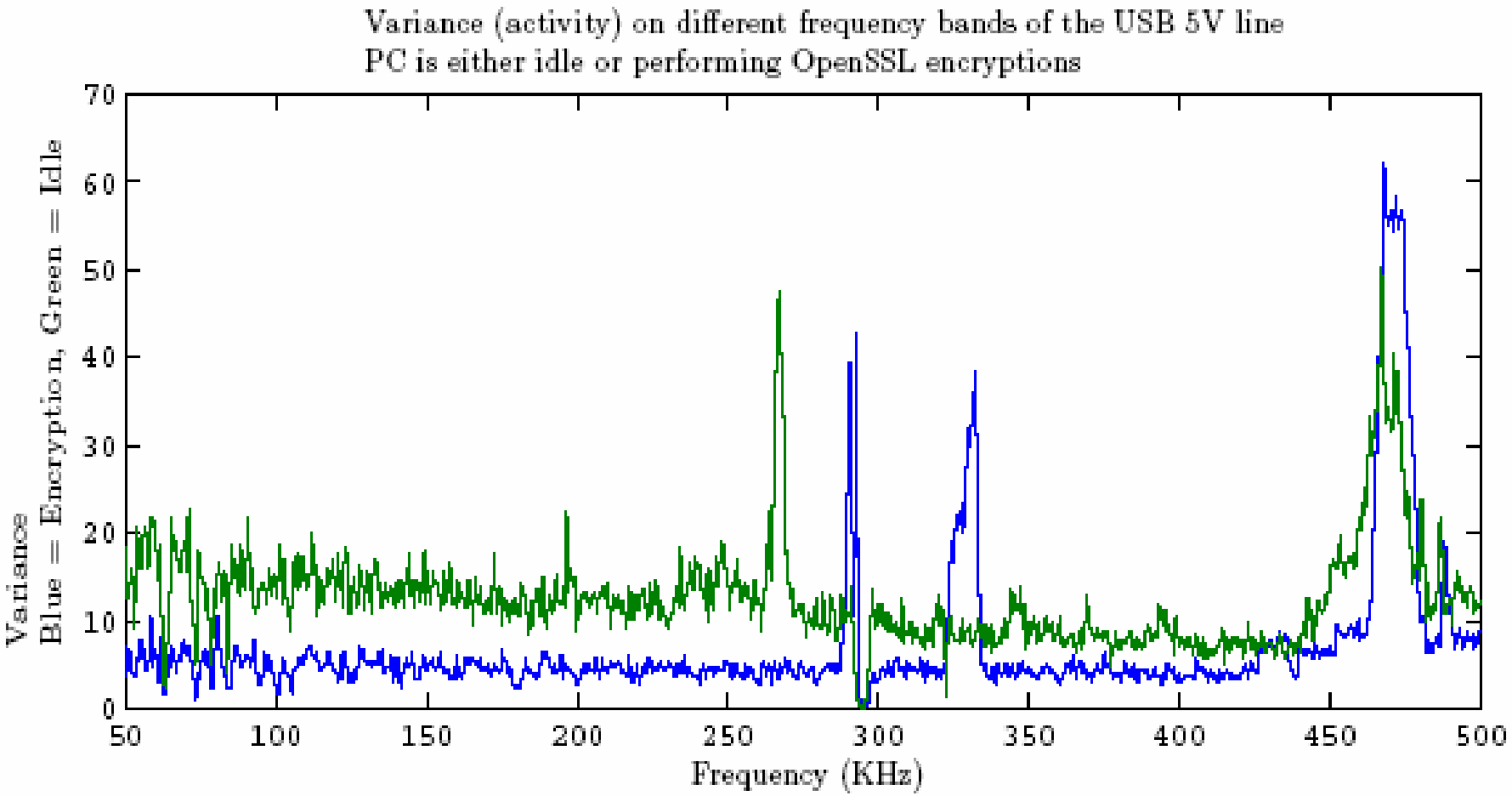
Many companied disable these ports to prevent data downloading

However, its also an an excellent way to carry out power analysis

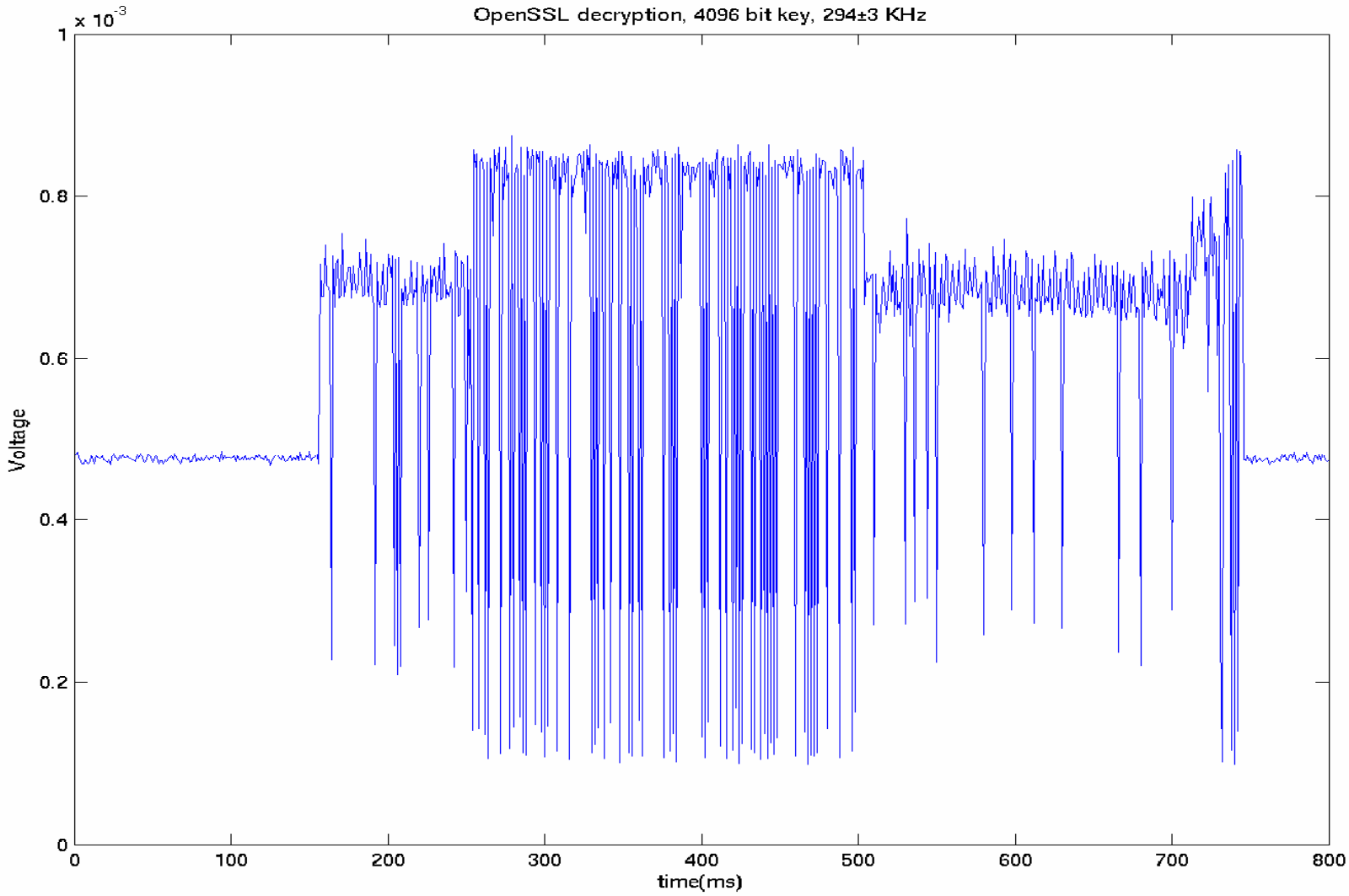
Lunchtime PA attack on an office PC:

- A PC doing crypto is accessible for a few minutes in an unattended office
- Cutting the power cord or opening the box to carry out power analysis is cumbersome and can turn off the computer
- A DOK with A/D conversion and large memory can easily record the power consumption curve using a conveniently located USB port (even if its device driver was disabled and it can't communicate)

The Spectrum of USB power



The real-time signal of USB power at 294 KHz during OPENSSL decryption



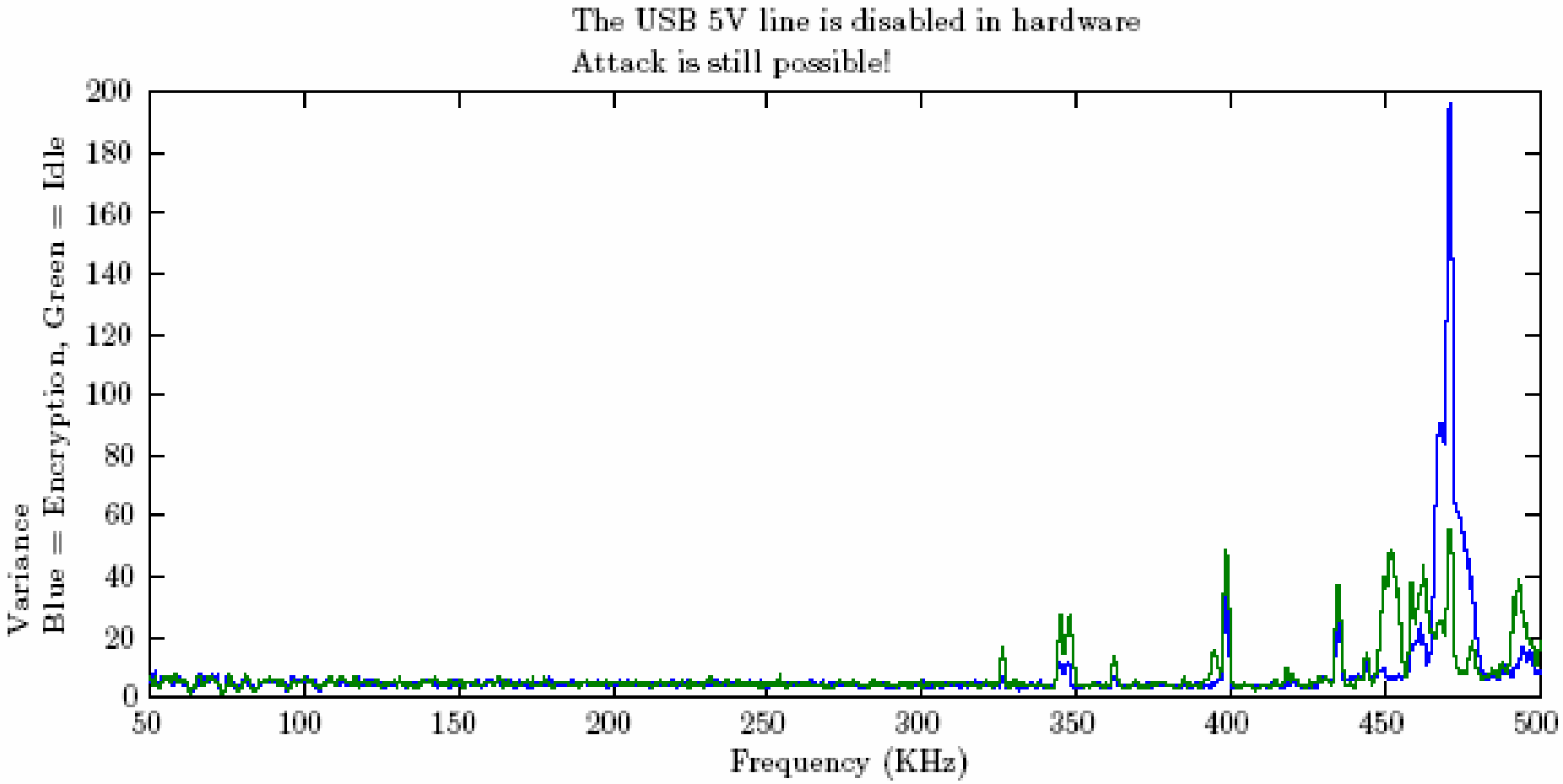
We tried to disable the USB power:

- We couldn't do it with the operating system
- We couldn't do it with the BIOS
- We couldn't do it with USB security programs

Our last resort:

- USB ports have an overload protection mechanism
- We short-circuited the two USB power lines
- Success: No power was available

The spectrum of USB power with power cutoff



A Research Breakthrough:

Power analysis

Does not require power

To do the analysis!

(and the only real solution to the USB security problem is to use epoxy glue!)

Thank you!