

TEMPEST inception

Andrea Barisani <andrea@inversepath.com>

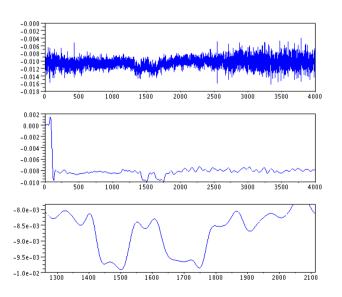
Daniele Bianco daniele@inversepath.com/

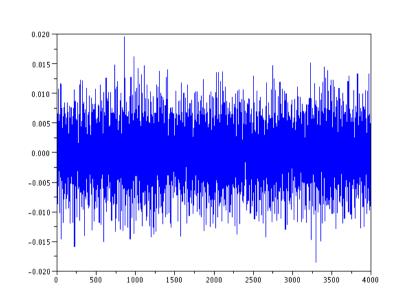


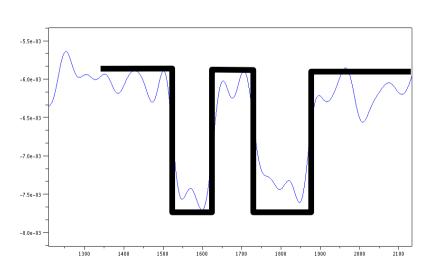
Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage (CanSecWest, 2009)











Copyright 2014 Inverse Path S.r.l.

TEMPEST inception

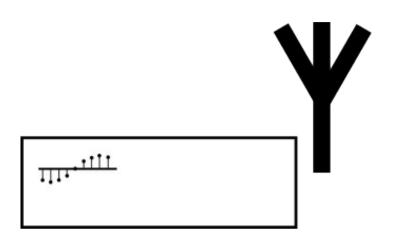
taking the INVERSE PATH

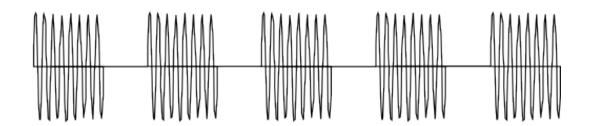
INVERSE PATH





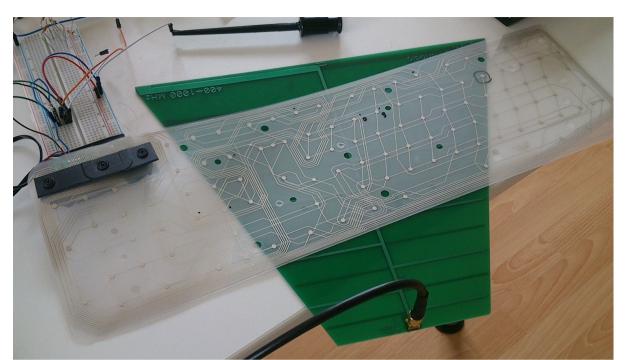




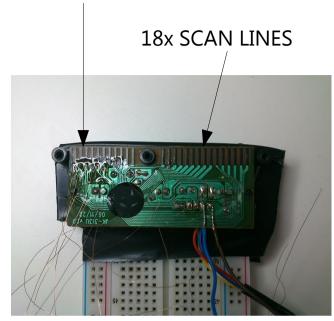


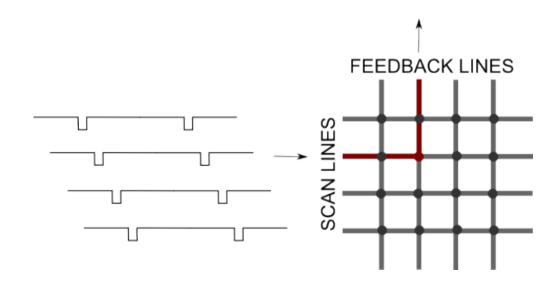






8x FEEDBACK LINES

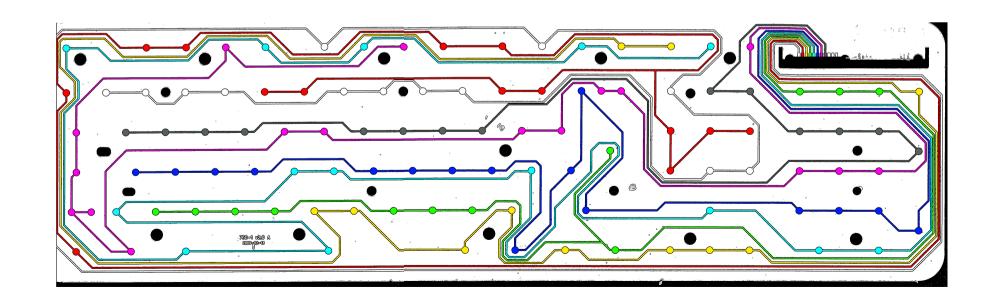




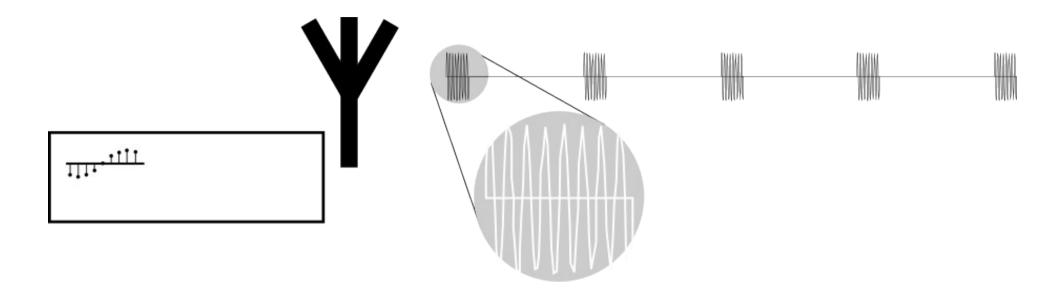


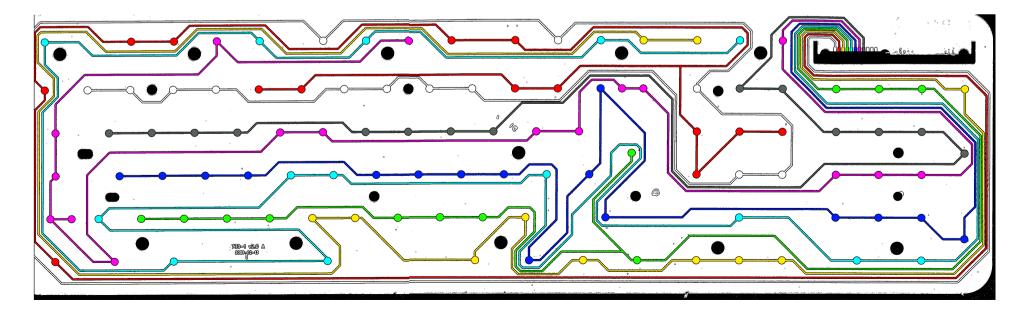


White	1536 mm	92.9 MHz
Red	1387 mm	102.8 MHz
Yellow	1138 mm	125.3 MHz
Green	677 mm	210.7 MHz
Light blue	1423 mm	100.2 MHz
Dark blue	773 mm	184.5 MHz
Purple	954 mm	149.5 MHz
Gray	633 mm	225.3 MHz

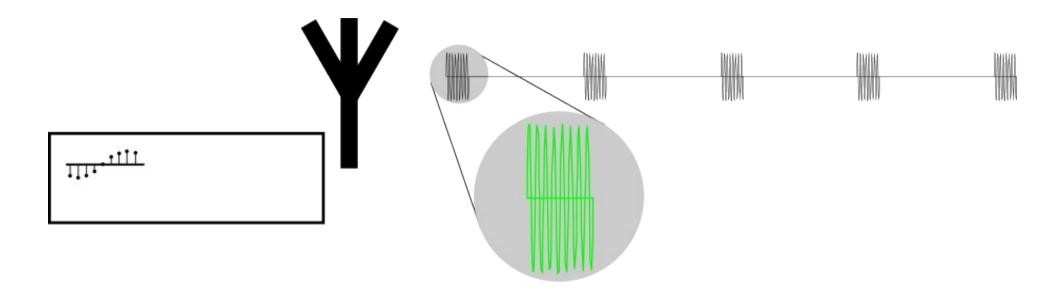


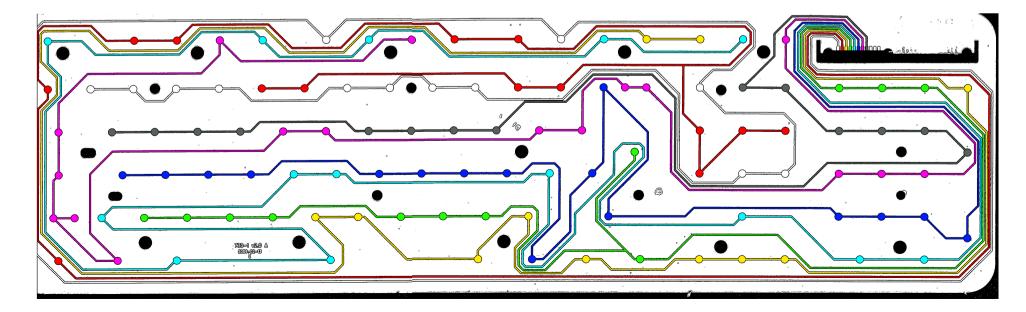




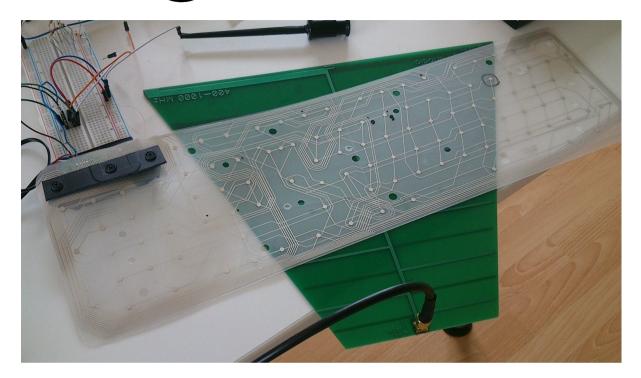




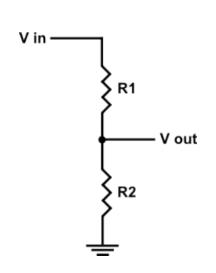


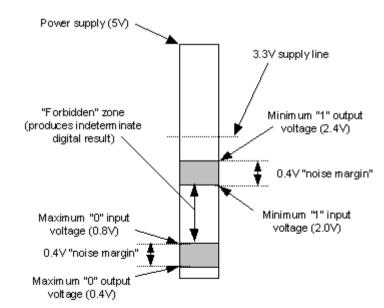


INVERSE PATH

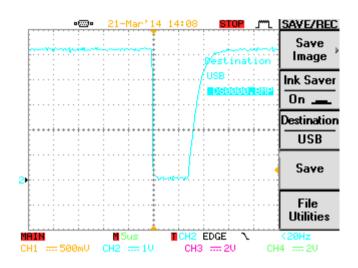


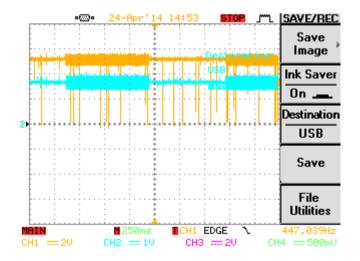












Scan line signal characteristics:

~10 µs low period

~2260 µs high period

~440 Hz

To successfully generate a keystroke a certain feedback line must be low for more than just one scan period.



DOES IT ACTUALLY WORK ?!



