Power Consumption by AES and T-Test Results Comparing Unprotected AES vs AES Protected by FortifyIQ Side-Channel Attacks Protected AES Core

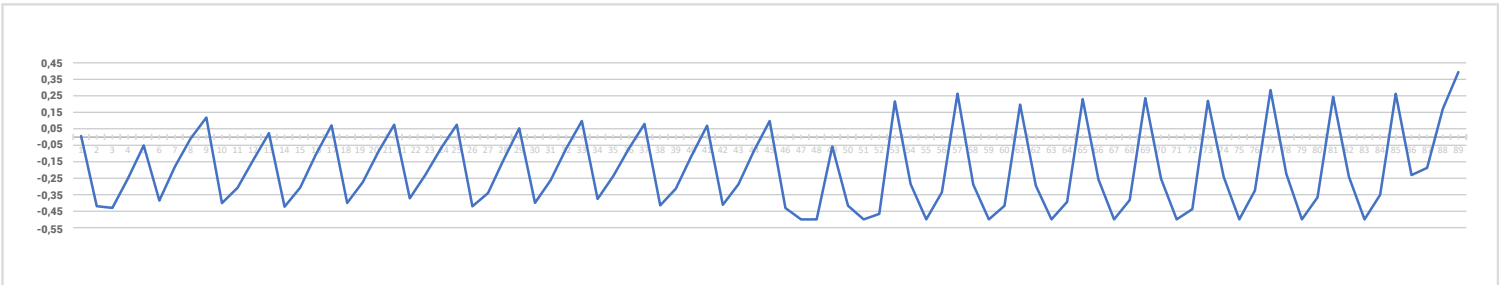

Figure 1. *Power Consumption by AES (FPGA), the average of power consumption from 1 million traces*

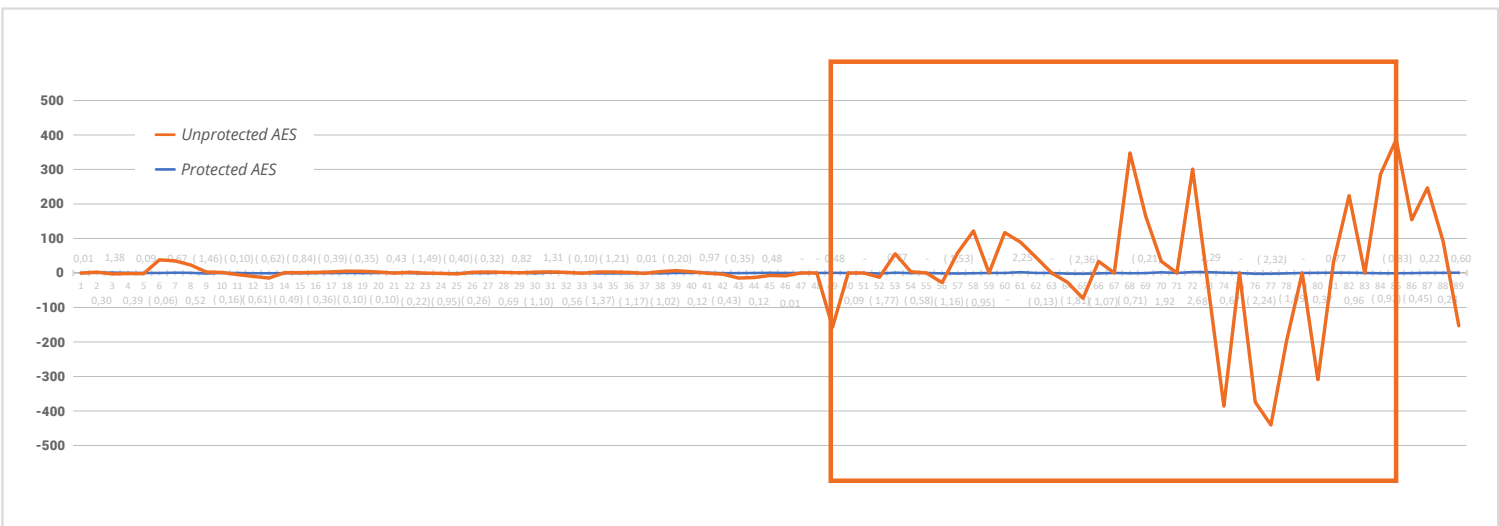

Figure 2. *Protected vs Unprotected Mode of the Scheme, Zero T-test*

Figure 2 shows that in unprotected design the leakage is present and the secret key that occurs during key encryption, may be revealed, whereas when protected by **FortifyIQ Side-Channel Attacks Protected AES Core** all values of the t-test are below the desired threshold (4.5)