

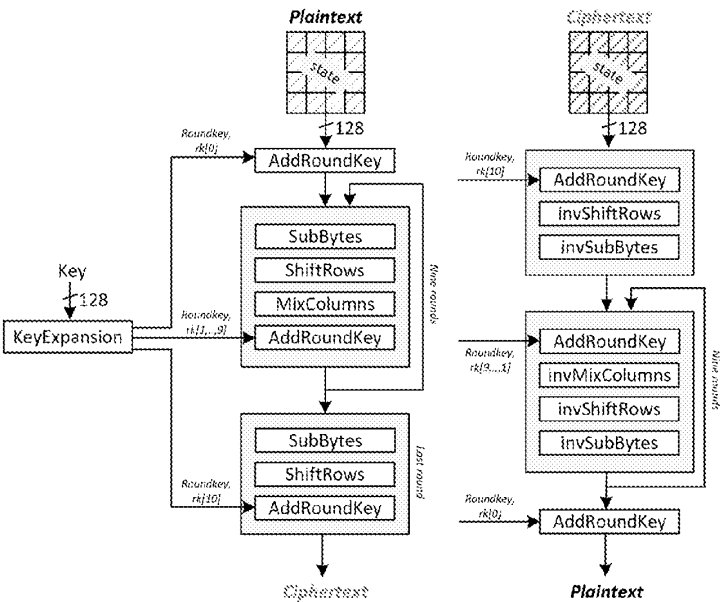


Figure 1

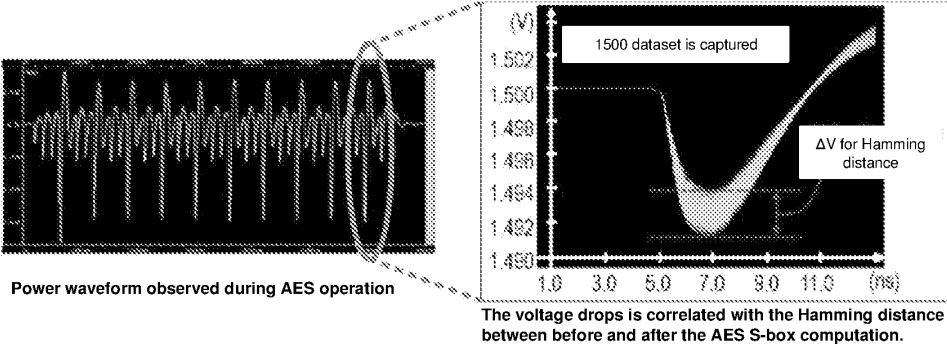


Figure 2

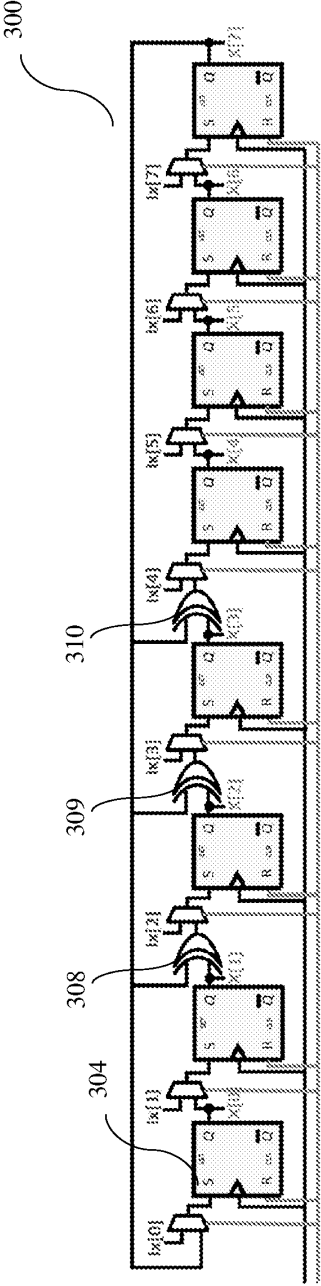


Figure 3A

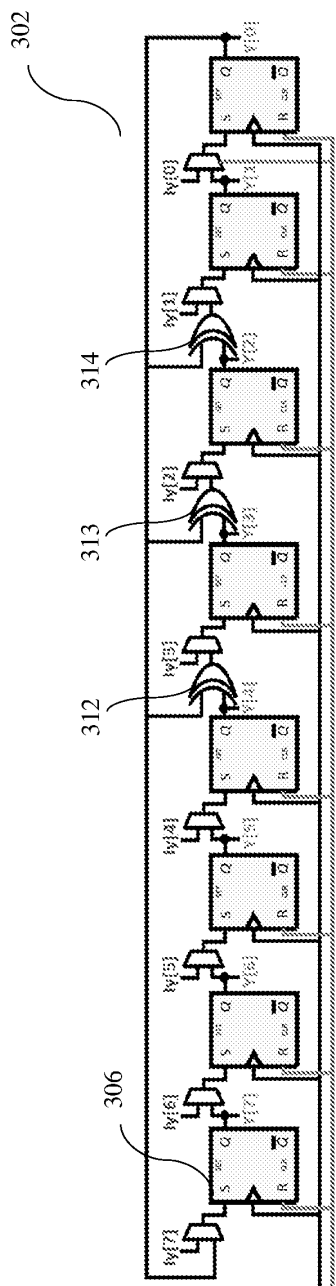


Figure 3B

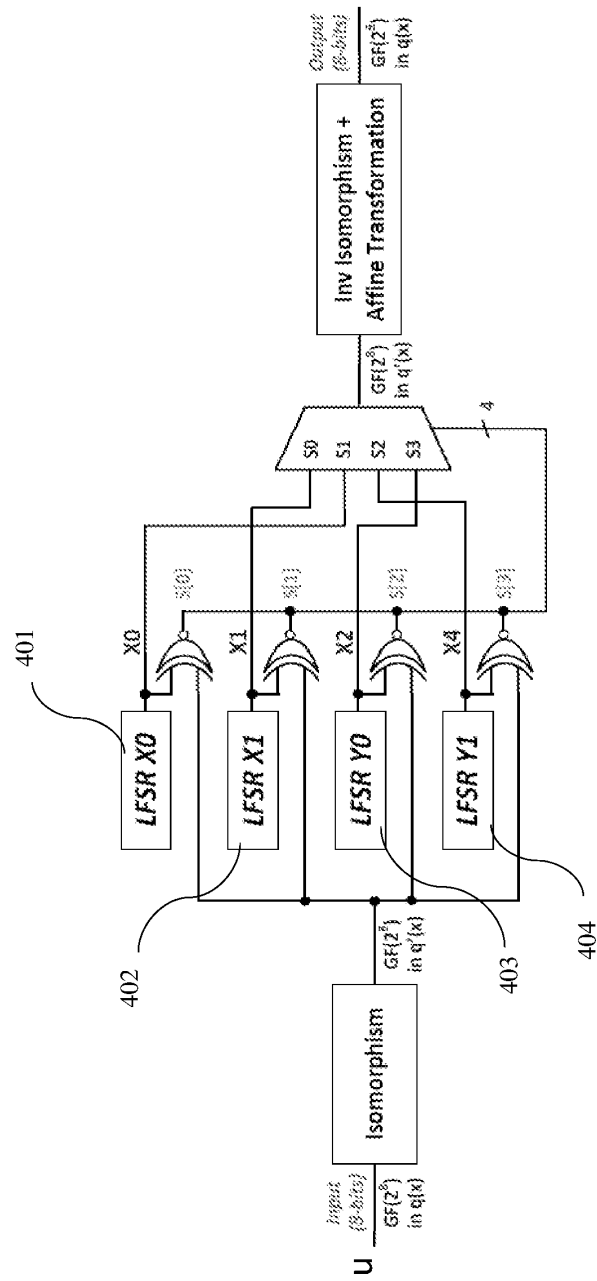


Figure 4

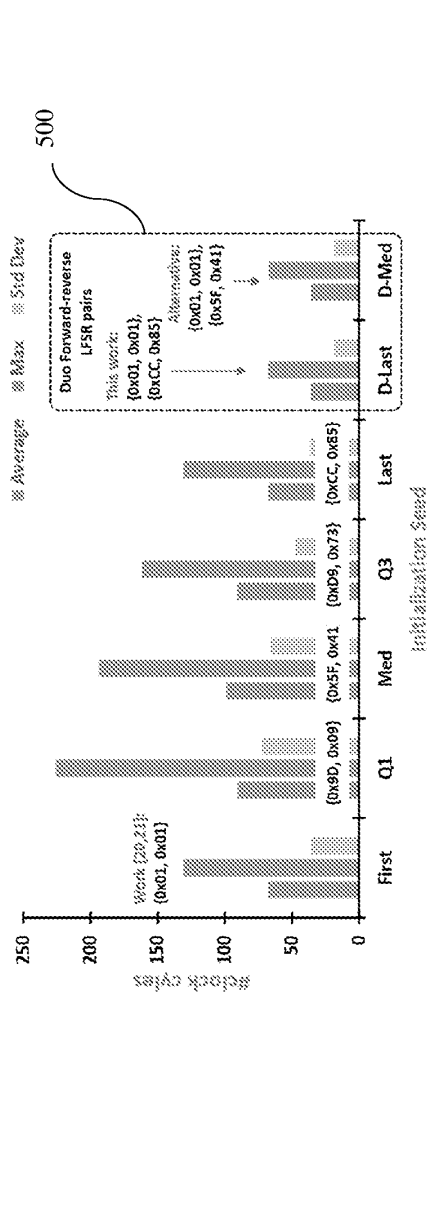


Figure 5

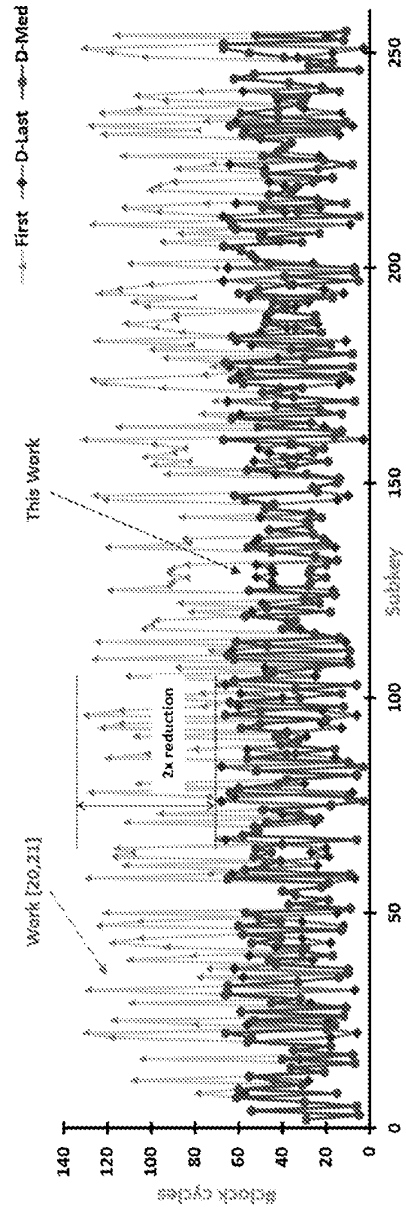


Figure 6

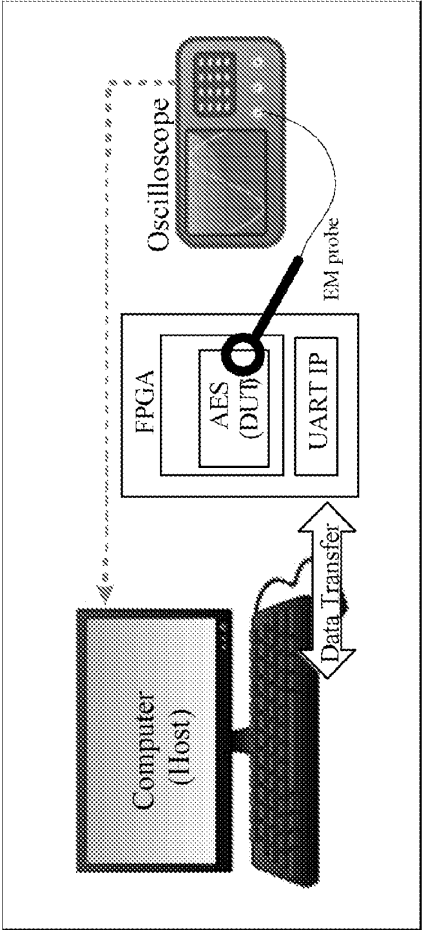


Figure 7

6/10

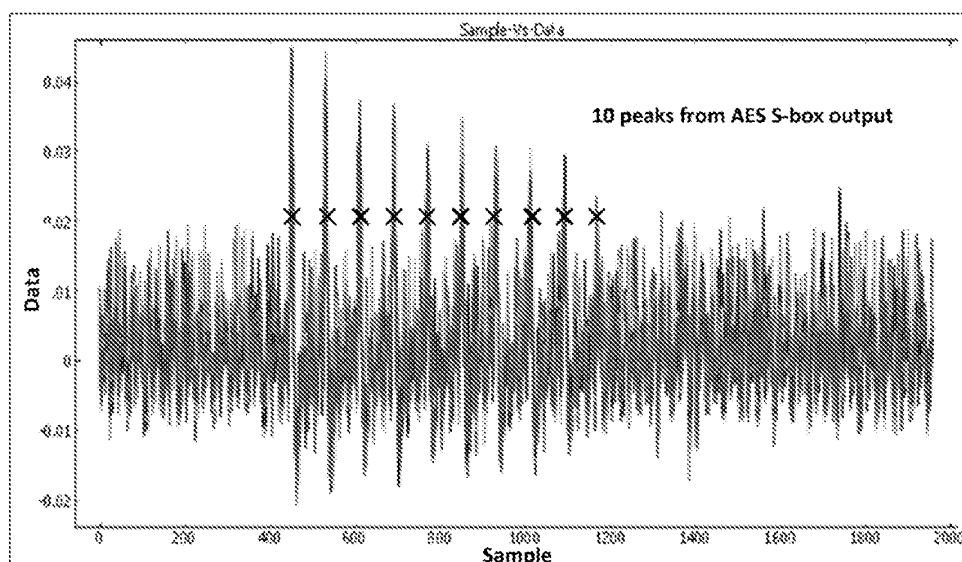


Figure 8A

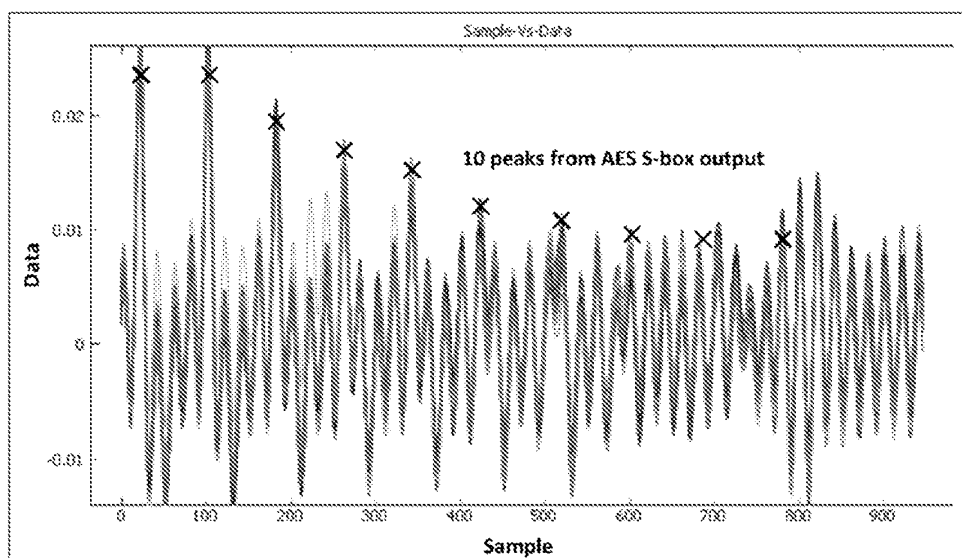


Figure 8B

7/10

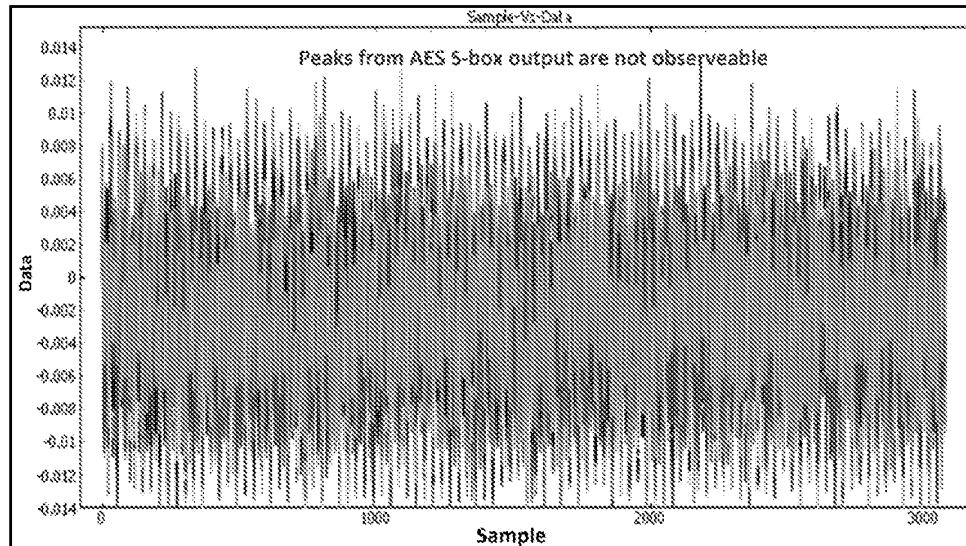
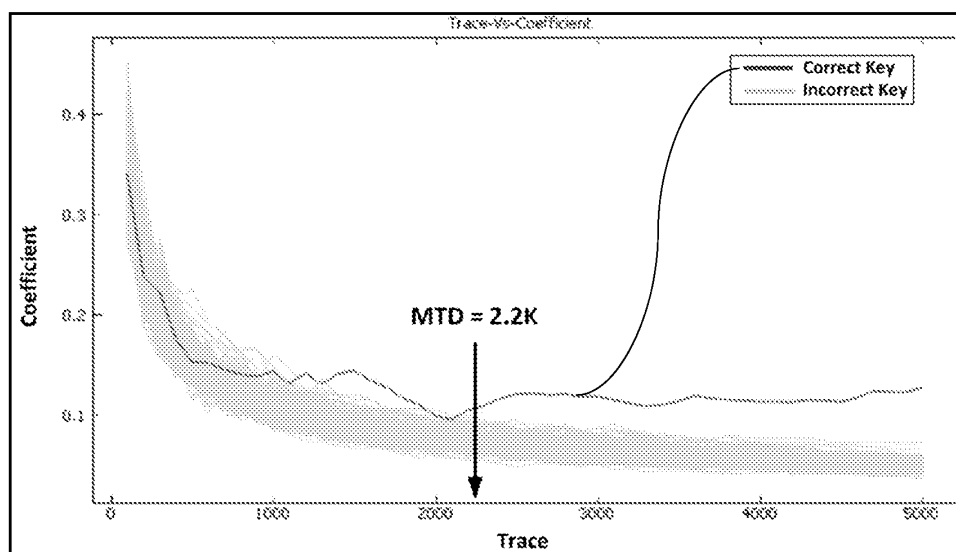


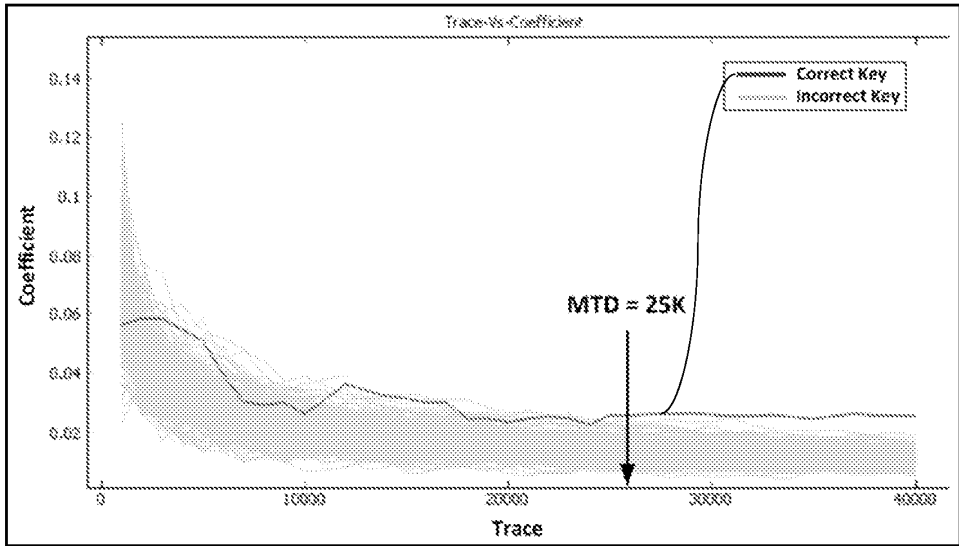
Figure 8C



MTD = 2.2K traces to unveil all 16 subkeys.

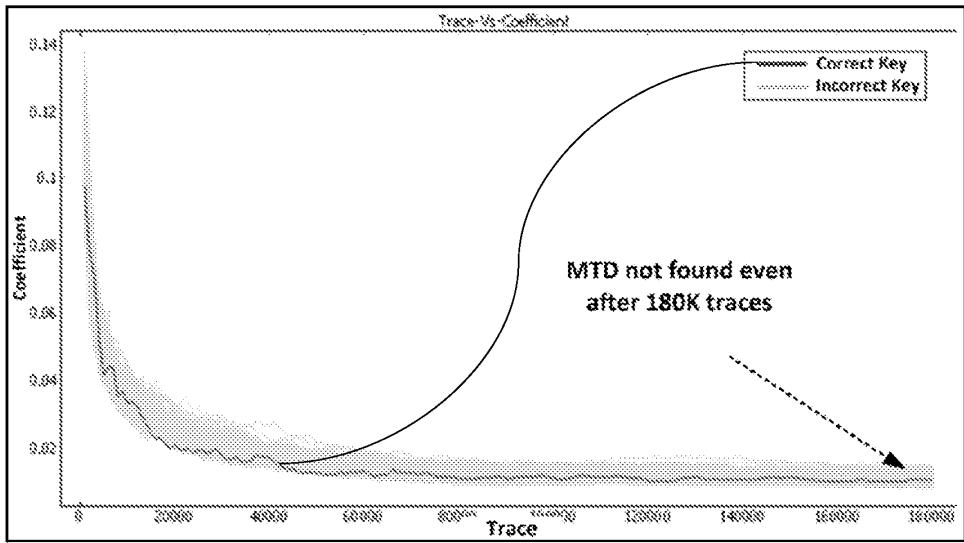
Figure 8D

8/10



MTD = 25K traces to unveil all 16 subkeys.

Figure 8E



MTD > 180K (unable to unveil any subkey)

Figure 8F

9/10

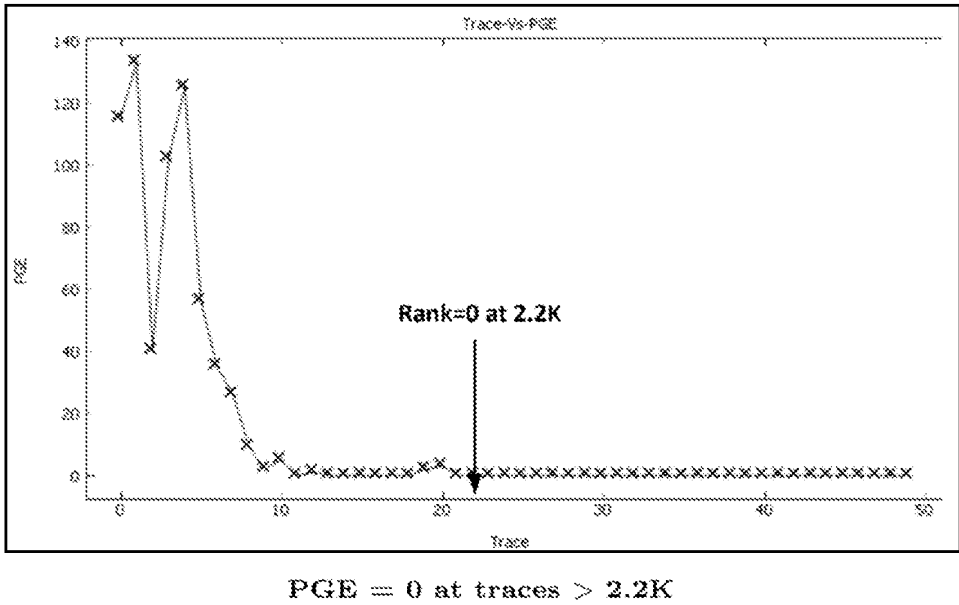


Figure 8G

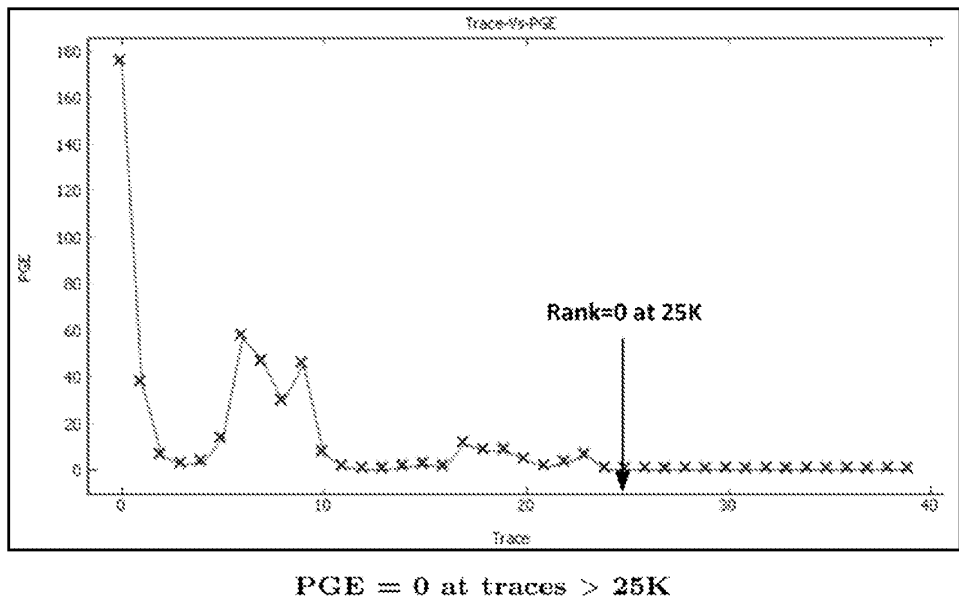
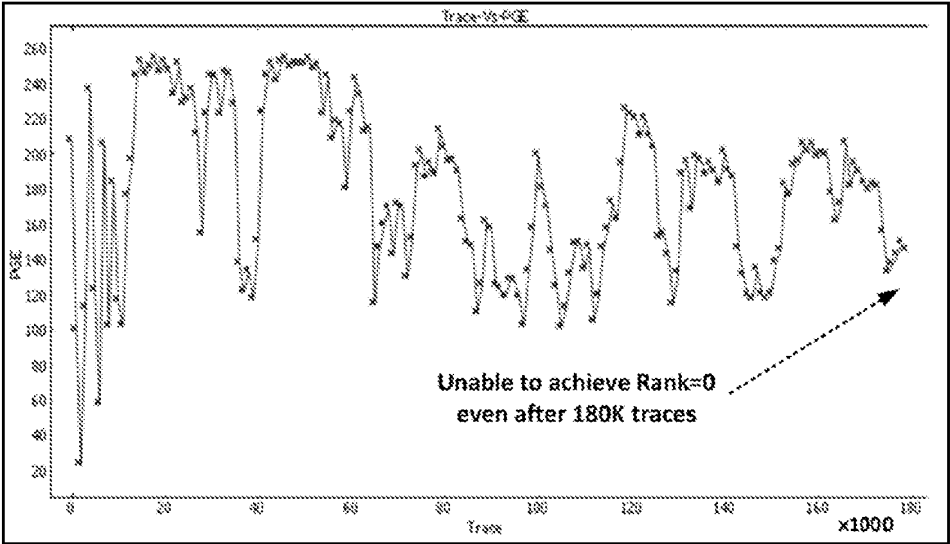


Figure 8H

10/10



PGE never reaches 0 (unable to resolve the correct key)

Figure 8l

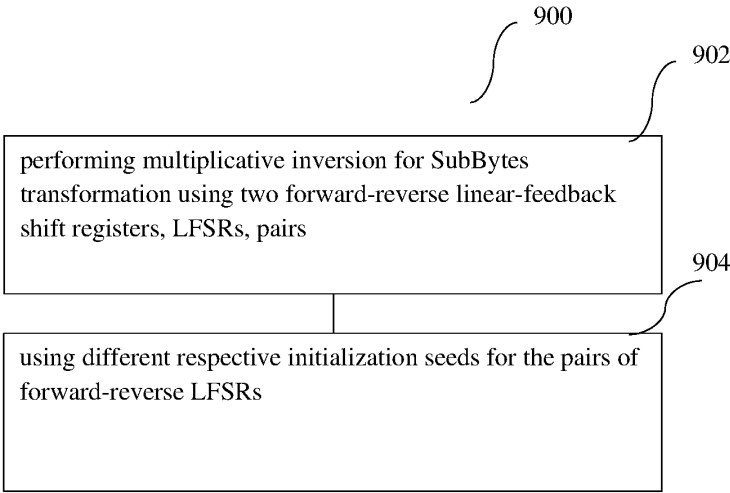


Figure 9