APPARATUS AND METHOD TO
Prevent Side Channel Power Attacks In Advanced Encryption Standard

BACKGROUND
This invention relates to the Advanced Encryption Standard (AES) outlined in the Federal Information Processing Standards (FIPS) Publication 197. The AES standard defines the FIPS approved algorithm that is used to encrypt and decrypt 128 bits of data using a 128, 192, or 256 bit key. When data is encrypted, or enciphered, the output data is called ciphertext. When data is decrypted, or deciphered, the output data is called plaintext.

INVENTION SUMMARY
An object of the present invention is to provide an apparatus and method to prevent side

![A functional diagram of the AES encryption algorithm. (Courtesy illustration)](continued >)
channel power attacks from determining the key when the AES algorithm is implemented in hardware.

Another object of the present invention is to provide a method and apparatus to foreclose the opportunity to measure and detect the power consumed during round one of the AES encryption process.

The present invention provides an apparatus and method for obscuring round one power consumption of hardware implementation of the AES algorithm. Additional hardware circuitry will provide consistent power consumption during round one of the AES algorithm. This prevents the opportunity to determine the AES key value during a side channel power attack.

One embodiment of the present invention is a method for obfuscating power consumption during round one of an AES encryption process where the standard has a data bit and a key bit for each bit of an encryption key. Each data bit is exclusive OR’d with an inverted version of each key bit. The output of the exclusive OR is then latched and the latched output is capacitively stored and obfuscates the power consumption of the encryption process.

In addition, a capacitor having a first terminal and a second terminal, where an inverted version of the key bit connected to the first input and the data bit is connected to said second input. The exclusive OR output is connected to the signal input and the latched output is connected to the first terminal of said capacitor and the second terminal of said capacitor is connected to ground.

For a better understanding of the invention, please review the entire patent for accompanying drawings, claims and detailed description.

A functional diagram of the AES decryption algorithm. (Courtesy illustration)