numbers, are slow, tie up the microprocessor with the task, clog memory buses, and consume a lot of power/energy (resulting in increased heat dissipation and battery drain).

An additional drawback of prior art pseudorandom number generators is that they are unprotected from side channel attacks, which creates significant risks in IT security applications. During operation of electronic devices that are processing data, some information about secret keys or sensitive data always leaks in side channels (physical sources of unintended information dissemination), including data dependent variation of response times, fluctuation of power use, or ultrasonic or electromagnetic wave radiation. This is why the secrecy and integrity of stored or transmitted data can generally be assured by cryptographic means when no adversary has physical access to the electronic devices.

Thus, it is desirable to have an improved pseudorandom number generator that generates many pseudorandom numbers in one clock cycle and enables improvements in security by reducing side channel leakage without significantly increasing processing time, system complexity, the size of electronic circuits, or energy usage.

BRIEF SUMMARY

In view of the foregoing background, example implementations of the present disclosure provide a system and method for generating pseudorandom numbers. The method includes the steps of initializing a counter value for a call-counter, sending a bit-wise form of the counter value from the call-counter to a mixing function, and mixing the bit-wise form of the counter value to generate a pseudorandom number. The system includes a call-counter that is initialized with a counter value and a mixing function that mixes a bit-wise form of the counter value to generate a pseudorandom number. The counter value is incremented by a predetermined value and the generated pseudorandom number can be used as an input value for a subsequent cycle of the mixing function. The system and method for generating pseudorandom numbers may also include the steps of filling an input register by repeating the counter value in its entirety as many times as possible without exceeding capacity of the input register, and filling any remaining, unfilled bits of the input register with individual bits of the counter value. Encrypted data may be stored in the memory of a storage device based on the generated pseudorandom number.

In implementations of the present disclosure, the mixing step is performed by a mixing function. The mixing function maps a first segment of the bit-wise form of