World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:04, 2017

# Design and Implementation of Pseudorandom Number Generator Using Android Sensors

**Authors :** Mochamad Beta Auditama, Yusuf Kurniawan

**Abstract :** A smartphone or tablet require a strong randomness to establish secure encrypted communication, encrypt files, etc. Therefore, random number generation is one of the main keys to provide secrecy. Android devices are equipped with hardware-based sensors, such as accelerometer, gyroscope, etc. Each of these sensors provides a stochastic process which has a potential to be used as an extra randomness source, in addition to /dev/random and /dev/urandom pseudorandom number generators. Android sensors can provide randomness automatically. To obtain randomness from Android sensors, each one of Android sensors shall be used to construct an entropy source. After all entropy sources are constructed, output from these entropy sources are combined to provide more entropy. Then, a deterministic process is used to produces a sequence of random bits from the combined output. All of these processes are done in accordance with NIST SP 800-22 and the series of NIST SP 800-90. The operation conditions are done 1) on Android user-space, and 2) the Android device is placed motionless on a desk.

**Keywords :** Android hardware-based sensor, deterministic process, entropy source, random number generation/generators
**Conference Title :** ICCSCPS 2017 : International Conference on Cyber Security of Cyber Physical Systems
**Conference Location :** Boston, United States
**Conference Dates :** April 24-25, 2017