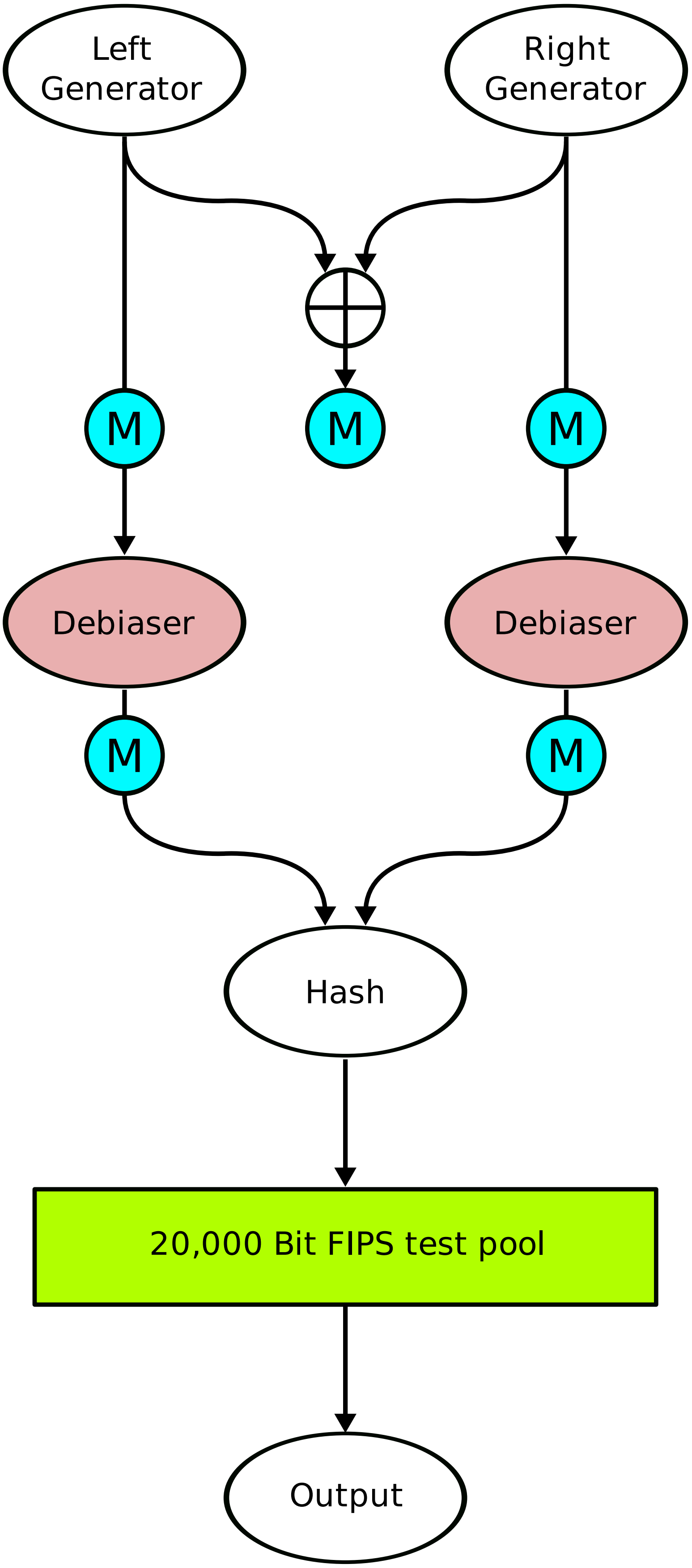
Entropy Key

http://www.entropykey.co.uk/

The Entropy Key is a small, affordable and easily installed high-quality random number generator that attaches to any free USB socket. Along with its two isolated and shielded noise generators, it has a 72MHz CPU to make sure the numbers it provides are high-quality and tamper-evident.



Two independant noise generators based on PN junctions near breakdown are sampled at high rates.

Each generator is tested using Üli Maurer's universal test for random bit generators, as well as both outputs being Exclusive-ORed together and also tested using the same test. This gives the Entropy Key an idea of how each generator is performing, as well as an indication of if the generators have become correlated.

The stream of bits is then subjected to John von Neumann's debiasing scheme, where the ratio of 0s to 1s becomes close to 50:50, and is again tested by Maurer's randomness test, and the amount of entropy estimated by this test is retained.

Finally, the bits are injected into a 256-bit cryptographic hash. Using the information gathered in the Maurer randomness test in the previous step, when the amount of entropy that has been injected reaches at least 150% of the hash's output size, it is finalised and emitted.

The output from the hash is collected until 20,000 bits have been generated. At this point, they are subjected to the randomness tests stipulated by FIPS for randomness, and statistics are tracked.

The 20,000 bit blocks are then divided up into 256 bit blocks, encrypted using the current session key, and transmitted to the host, which then decrypts them and uses them as it wishes. At this point, each 256 bit block has been generated from around 5000 bits read off the generators.

1.0 20090908