Pengembangan pembangkit bilangan acak berbasis discrete time chaos satu dimensi untuk menghasilkan rangkaian bit yang acak dengan nilai entropi tinggi = The development of one-dimension discrete time chaos based random number generator to improve randomness and obtain the high entropy value

Magfirawaty, author

Abstrak

ABSTRAK
Pada penelitian ini dilakukan perancangan random number generator RNG berbasis discrete time DT chaos dengan menggunakan modifikasi chaos satu dimensi sebagai fungsi deterministik pada proses destilasi. Sistem chaos satu dimensi 1D merupakan sistem dinamik sederhana yang banyak diterapkan dalam pembangkitan bilangan acak. Pada penelitian awal, kami telah mengkombinasikan ring oscillator RO sebagai sumber entropi dari RNG dengan logistic map sebagai fungsi deterministik. Telah dilakukan beberapa penelitian terkait dengan menggunakan sistem chaos 1D, yang mampu menghasilkan rangkaian bit acak secara statistik. Pada penelitian ini kami melakukan modifikasi logistic map yang akan diaplikasikan sebagai RNG berbasis DT chaos. Logistic map merupakan sistem chaos yang sering diterapkan pada sistem kripto. Selain karena mudah diimplementasikan pada perangkat keras, logistic map juga memiliki tingkat keamanan yang lebih baik dibandingkan sistem chaos fungsi nonlinier lainnya. Modifikasi menghasilkan dua persamaan deterministik baru yaitu MLP I dan MLP II, yang mampu mengolah data real, -1, 1 untuk menghasilkan luaran berupa bilangan potisif dan negatif, -1, 1 . Dengan menggunakan pembuktian secara empiris dan teoritis, didapatkan fungsi ekstraktor dengan nilai tertentu untuk mengubah bilangan real yang dihasilkan oleh fungsi deterministik menjadi rangkaian bit dengan nilai entropi tinggi. Hasil uji keacakan dengan menggunakan NIST 800-22 menunjukkan bahwa rangkaian bit yang diperoleh dinyatakan acak dengan nilai proporsi yang dihasilkan untuk seluruh uji berada pada interval 0.9804-0.9994 dengan P-value>. Jika dibandingkan dengan zigzag map sebagai fungsi deterministik pada RNG berbasis DT chaos, MLP II mampu menghasilkan rangkaian bit yang lebih acak dibandingkan zigzag map tanpa post-processing. Pengujian keacakan menggunakan uji DieHard menunjukkan bahwa 80 Mbit output MLP II dinyatakan acak dengan P-value = 0, 1 . Implementasi metode RNG berbasis DT chaos dengan fungsi MLP II menggunakan ZedBoard Zynq 7000 memperlihatkan jumlah source yang digunakan lebih efisien dibandingkan RNG berbasis DT chaos dengan fungsi zigzag map yaitu look up tables LUT sebanyak 2 , flip flop FF sebanyak 1 dan digital signal processing DSP sejumlah 4.5 .
<hr />
ABSTRACT
This research designs a discrete time DT chaos based random number generator RNG , which uses one-dimension chaos modification as deterministic function in the destillation process. One-dimensional chaos 1D is a simple dynamic system, which is widely applied to generate random numbers. In the preliminary research, we have combined ring oscillator RO as the RNG entropy source with logistic map as a deterministic function. We have done some related research using a 1D chaos system, which is capable to generate random bits statistically. Our work modifies logistic map that will be applied as DT chaos-based

RNG. The logistic map is a chaotic system that is usually applied in the cryptosystem. In addition to easy hardware implementation, the logistic map also has a better level of security than other nonlinear chaos function. The modification performed yields two new deterministic equations, namely MLP I and MLP II, which are capable to process data of real numbers, -1, 1 , and generate positive and negative numbers, -1, 1 . Through empirical and theoretical verification the extractor function is obtained with a certain value to convert the real number that is generated by a deterministic function into a sequence of bits which has high entropy value. Through NIST 800-22 randomness test it is revealed that the obtained bit sequence is random with the proportion values at intervals 0.9804-0.9994 and P-value > ? . Comparing with the zigzag map as a deterministic function in the DT chaos-based RNG, MLP II map generates more random bit sequence than the zigzag map. Furthermore as much as 80Mbit MLP II output passed the Diehard test with P-value = 0, 1 . Implementation of the DT chaos-based RNG method with the MLP II function using ZedBoard Zynq 7000 shows the number of sources used more efficient than the DT chaos-based RNG with the zigzag map function of 2 look up tables LUT , flip flop FF as much as 1 and digital signal processing DSP of 4.5 .