mgr inż. Krzysztof Mańk
Wojskowa Akademia Techniczna
Wydział Cybernetyki, Instytut Matematyki i Kryptologii

Zbieranie entropii

Fizyczne generatory ciągów losowych są bardzo istotnym elementem wielu systemów kryptograficznych. Bez nich trudno sobie wyobrazić funkcjonowanie któregokolwiek z systemów klucza publicznego, nie mówiąc już o tak ekstremalnych potrzebach, jak szyfr z kluczem jednokrotnym. Urządzenia te wykorzystują rozmaite zjawiska fizyczne, cechują się różnorodnymi parametrami środowiskowymi i szybkościami pracy, mają zaś jedną wspólną cechę — źródła dobrej jakości są drogie. W naszej prezentacji pokażemy jak przy pomocy trywialnego układu, jakim jest rejestr przesuwny z liniowym sprzężeniem zwrotnym, możemy nawet bardzo słabe źródło zamienić w doskonały generator. Według naszej wiedzy rozwiązanie takie nie jest nowe, nowością jest natomiast sposób podejścia do analizy jakości statystycznej uzyskiwanego w ten sposób ciągu.

Metoda, jak i uzyskane przez nas wyniki, bazują na pojęciu entropii oraz własnościach macierzy stochastycznych.