SEMINÁRIO DE INICIAÇÃO CIENTÍFICA E TECNOLÓGICA DO IFG

EXPLORANDO O BILHAR ANULAR NA GERAÇÃO DE NÚMEROS PSEUDOALEATÓRIOS

SILVA, João Victor Alves Pereira da

Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Goiânia

SOUZA, Fabiano Caetano

Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Câmpus Goiânia

A segurança das chaves na criptografia depende fortemente da produção de números aleatórios confiáveis. Gerar números aleatórios é geralmente um processo lento, pois exige utilizar processos físicos estocásticos, como o lançamento de dados. Mas é possível gerar números aleatórios falsos, ou pseudoaleatórios, bons o suficiente para essas aplicações, a partir de modelos matemáticos ou físicos. Algumas propostas na literatura sugerem utilizar modelos físicos caóticos para os geradores de números pseudoaleatórios. Neste trabalho, foi proposto, implementado e testado um gerador de números pseudoaleatórios, ou PRNG na sigla em inglês, utilizando o modelo bilhar anular. O bilhar anular é um mapeamento que descreve a trajetória de uma partícula entre colisões elásticas na região delimitada por dois círculos, que apresenta comportamento misto: regularidade e caos. O modelo foi investigado e adaptado para gerar sequências de bits, que foram avaliadas com 10 testes de aleatoriedade, da suíte de testes do *National Institute of Standards and Technology* (NIST). Esse gerador produziu sequências de bits que passaram em 9 dos 10 testes realizados, quando geradas a partir de condições iniciais para as quais o modelo tem comportamento caótico. Os resultados promissores alcançados nesses testes qualificam o PRNG baseado no bilhar anular como um bom candidato para produzir números aleatórios para as diversas aplicações em que eles são utilizados.

Palavras-chave

Mecânica Clássica; Caos; Números PseudoAleatórios, Bilhar Anular, NIST SP 800-22.

Agradecimentos

O presente trabalho foi realizado com apoio do Instituto Federal de Educação, Ciência e Tecnologia de Goiás. Agradecemos ao CNPq pela bolsa concedida.