Geradores de Números Pseudoaleatórios em IoT: Eficiência e Segurança em Ambientes Limitados

Thiago Henrique Gomes Feliciano[1], **Vitor Costa Oliveira Rolla**[1]

[1]Instituto de Ciências Exatas e Informática – Pontifícia Universidade Católica de Minas Gerais
Caixa Postal 1686 – 30.535-901 – Belo Horizonte – MG – Brasil

Abstract. *This paper analyzes how different Pseudo random Number Generators (PRNGs) work on Internet of Things (IoT) devices, which have limited memory, processing power, and low energy availability. These generators are essential for security, as they are used to create keys, protect data, and authenticate devices. However, depending on the quality of the PRNG and the limitations of the environment in which it is used, it can make devices vulnerable, either due to low efficiency or high resource consumption. The review of studies presents various proposals and tests to evaluate PRNGs, but direct comparisons performed on IoT hardware are still lacking. Thus, this paper evaluates the main PRNGs on such devices, considering energy consumption, memory usage, speed, and the quality of the numbers generated, in order to identify which generator offers the best balance between security and performance.*

Resumo. *Este trabalho analisa como diferentes Geradores de Números Pseudoaleatórios (PRNGs) funcionam em dispositivos de Internet das Coisas (IoT), que possuem pouca memória, pouco processamento e baixa disponibilidade de energia. Esses geradores são essenciais para a segurança, pois são usados para criar chaves, proteger dados e autenticar dispositivos. No entanto, dependendo da qualidade do PRNG e das limitações do ambiente em que é utilizado, ele pode tornar os aparelhos vulneráveis, seja por baixa eficiência ou por alto consumo de recursos. A revisão de estudos apresenta várias propostas e testes para avaliar PRNGs, mas ainda faltam comparações realizadas diretamente em hardwares IoT. Assim, este trabalho avalia os principais PRNGs em dispositivos desse tipo, considerando consumo de energia, uso de memória, velocidade e a qualidade dos números gerados, a fim de identificar qual gerador oferece o melhor equilíbrio entre segurança e desempenho.*

1. Introdução

A segurança dos dispositivos de Internet das Coisas (IoT) tem sido um desafio recorrente, sobretudo devido às restrições inerentes de hardware, como limitações de processamento, energia e memória [Kietzmann et al. 2020]. Essas restrições dificultam a adoção de mecanismos criptográficos robustos, tornando o ecossistema mais vulnerável a ataques cibernéticos e violações de integridade.

Um dos principais fatores críticos dessas vulnerabilidades está no uso de Geradores de Números Pseudo-Aleatórios (PRNGs) de baixa qualidade e entropia, componentes essenciais para a geração de chaves criptográficas, protocolos de autenticação e outros mecanismos de segurança [He et al. 2024]. A qualidade estatística e a imprevisibilidade desses geradores determinam diretamente o nível de proteção dos dispositivos conectados.

Apesar da importância dos PRNGs em sistemas IoT, a literatura atual carece de estudos comparativos sistemáticos que correlacionem segurança criptográfica (entropia) e eficiência operacional (consumo de energia, uso de memória e latência) em condições reais de dispositivos embarcados. Essa lacuna limita a capacidade de projetar soluções que conciliem alto nível de segurança com baixo custo computacional, um requisito central no contexto da IoT.

Diante desse cenário, este trabalho propõe uma avaliação técnica de PRNGs diretamente em dispositivos IoT, com o objetivo de mensurar e correlacionar os indicadores de segurança e desempenho de cada gerador. A partir desses resultados, busca-se identificar e recomendar uma solução equilibrada entre robustez criptográfica e eficiência de recursos.

Este artigo está dividido em seis seções para fins de clareza textual e organização lógica da pesquisa. O Referencial Teórico, apresentado na seção 2, reúne os fundamentos conceituais necessários para a compreensão do estudo. A seção 3, dedicada aos Trabalhos Relacionados, discute pesquisas e abordagens já presentes na literatura, situando o presente trabalho no contexto do estado da arte. Na seção 4, encontra-se a Metodologia, que detalha os procedimentos, técnicas e etapas adotadas durante o desenvolvimento da investigação. A seção 5 apresenta os Resultados Esperados, descrevendo as contribuições previstas, as hipóteses de desempenho dos PRNGs e os benefícios potenciais decorrentes da aplicação da Bateria NIST STS no contexto de dispositivos IoT. Esta seção antecipa os cenários prováveis que a pesquisa busca validar empiricamente. A Conclusão, na seção 6, sintetiza os resultados obtidos, discute suas implicações e indica possíveis direções para trabalhos futuros. Por fim, a Bibliografia reúne todas as fontes utilizadas, de acordo com as normas acadêmicas pertinentes.

2. Referencial Teórico

2.1. Números pseudo aleatórios

Os números pseudo aleatórios (Pseudo-Random Numbers - PRN) são valores gerados por software, por meio de algoritmos que simulam a aleatoriedade. Embora pareçam aleatórios, esses números são produzidos de forma determinística, a partir de um valor inicial chamado semente, o que significa que a mesma semente sempre gerará a mesma sequência de números [Němec et al. 2019], diferentemente dos números verdadeiramente aleatórios (True-Random Numbers - TRN), que dependem de fenômenos físicos imprevisíveis. Esses valores são amplamente utilizados em aplicações que exigem variação controlada, como simulações, criptografia e sistemas embarcados [He et al. 2024].

2.2. Geradores de números pseudo aleatórios(PRNGs)

Os Geradores de Números Pseudo Aleatórios (Pseudo-Random Number Generators – PRNGs) são os programas ou algoritmos responsáveis por essa geração sendo utilizados em diversas áreas, como criptografia, estatística e simulações computacionais [Němec et al. 2019]. Entre os métodos mais utilizados estão o Linear Congruential Generator (LCG), conhecido pela sua simplicidade e baixo custo computacional, e o Xorshift, que oferece maior rapidez e qualidade estatística [Němec et al. 2019]. Devido à eficiência e ao baixo consumo de recursos, esses geradores são amplamente aplicados em sistemas que exigem desempenho otimizado, como dispositivos de IoT [Kietzmann et al. 2020, Wallace et al. 2016]. Assim, os PRNGs representam uma solução prática para aplicações que exigem aleatoriedade dentro de sistemas computacionais.

2.3. Internet das coisas(IoT)

A Internet das Coisas (IoT) é um conceito que se refere à conexão de objetos físicos à internet, permitindo que dispositivos como sensores, máquinas e equipamentos comuniquem-se entre si e com sistemas computacionais. Essa tecnologia possibilita a coleta e o compartilhamento de dados em tempo real, tornando processos mais eficientes e automatizados [He et al. 2024]. A aplicação de PRNGs é essencial para a segurança em IoT, sendo utilizados para gerar chaves de criptografia, assinaturas digitais e garantir a integridade na transmissão de dados [Němec et al. 2019].

Com o avanço das redes sem fio, da computação em nuvem e da inteligência artificial, a IoT tem se consolidado como uma das principais bases da transformação digital. No entanto, seu crescimento também traz desafios relacionados à segurança das informações e à privacidade dos usuários, exigindo o desenvolvimento de soluções que garantam a confiabilidade nos dispositivos conectados [He et al. 2024].

2.4. Criptografia

A criptografia é a área que lida com técnicas para proteger a informação, garantindo sua confidencialidade, integridade e autenticidade. Ela transforma dados legíveis em formato ilegível (ciphertext) e vice-versa, dependendo de uma chave secreta.

A qualidade e a imprevisibilidade dessa chave são fundamentais para a segurança do sistema. Para uso criptográfico, os geradores devem ser CSPRNGs (Criptograficamente Seguros), o que exige não apenas aleatoriedade estatística, mas também total imprevisibilidade para resistir a ataques, um desafio particular em dispositivos IoT com recursos limitados [Kietzmann et al. 2020].

3. Trabalhos Relacionados

A geração de números pseudoaleatórios é essencial para a segurança de dispositivos IoT, mas conciliar robustez criptográfica com restrições de hardware, como processamento, memória e energia, ainda é um desafio [He et al. 2024, Kietzmann et al. 2020]. PRNGs de alta entropia oferecem segurança, mas muitas vezes não são viáveis em IoT de baixo custo [He et al. 2024, Wallace et al. 2016].

Diversos trabalhos propõem algoritmos leves para dispositivos restritos, como microcontroladores de 8 e 32 bits [Orúe et al. 2017], e abordagens baseadas em sistemas caóticos, capazes de gerar sequências imprevisíveis [Zia et al. 2022]. Estudos recentes também exploram PRNGs leves e rápidos, comparando implementações em hardware FPGA e avaliando consumo de energia, latência e uso de recursos [Popereshnyak and Raichev 2024, Teo et al. 2025]. Outras soluções permitem múltiplas sequências configuráveis ou parâmetros dinâmicos, aumentando a robustez e adaptabilidade em IoT [Wu et al. 2024, Paul et al. 2021].

Modificações em algoritmos tradicionais ainda demonstram a importância de equilibrar segurança e desempenho [Němec et al. 2019], enquanto aplicações em redes IoT evidenciam o impacto da escolha do PRNG na confiabilidade e eficiência dos protocolos [Fan et al. 2021]. Testes estatísticos simplificados, como o de frequência baseado em qui-quadrado, são utilizados para avaliar qualidade em ambientes restritos [Zhang et al. 2022].

Apesar das contribuições existentes, ainda há uma lacuna na avaliação integrada de robustez, desempenho e consumo de recursos em dispositivos IoT reais. Poucos estudos consideram simultaneamente todas essas métricas em cenários práticos, o que limita a precisão na análise da eficácia dos PRNGs.

Este trabalho busca preencher essa lacuna propondo uma metodologia de avaliação ideal, capaz de medir de forma precisa a qualidade de diferentes geradores de números pseudoaleatórios em ambientes IoT restritos. A abordagem considera critérios de robustez criptográfica, desempenho computacional e utilização de recursos, permitindo uma avaliação mais completa e confiável do comportamento dos PRNGs em condições reais de operação. Com isso, o objetivo é fornecer uma base sólida para a escolha e implementação de geradores seguros e eficientes em dispositivos embarcados.

4. Metodologia

Nesta seção os métodos para aplicação de uma análise de geradores de números pseudoaleatórios em dispositivos IoT são apresentados.

Para facilitar a compreensão da metodologia adotada, foi elaborado um fluxograma que resume de forma visual as principais etapas da pesquisa. Ele apresenta, de maneira organizada, o caminho seguido desde o planejamento até a análise dos resultados, permitindo uma visão geral clara do processo. A Figura abaico mostra o fluxograma da metodologia utilizada neste trabalho.

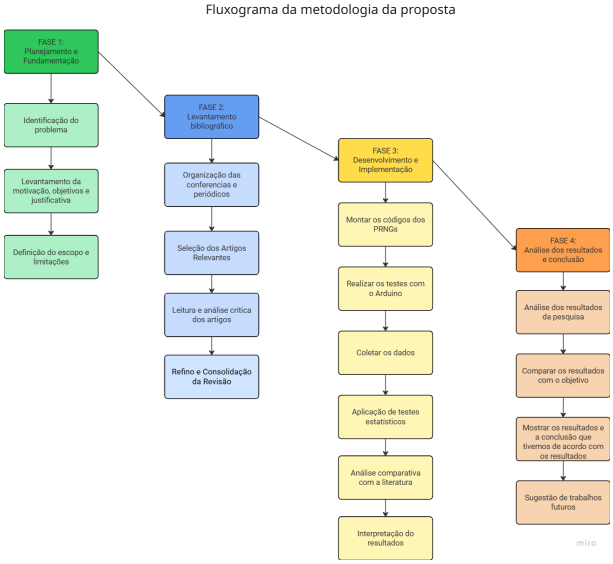

Figure 1. Fluxograma da metodologia.

O cronograma a seguir apresenta a distribuição das etapas da pesquisa ao longo do período previsto para sua realização. Ele organiza as atividades de forma clara, indicando quando cada fase deve ser iniciada e concluída, permitindo acompanhar o andamento do trabalho e garantir o cumprimento dos prazos estabelecidos. A Figura abaixo mostra o cronograma proposto para este estudo.

Tabela 1 – Cronograma

Atividade	Meses 1–3	Meses 4–6	Meses 7–9	Meses 10–12
Planejamento e definição de objetivos	X			
Definição do escopo e limitações	X			
Leitura e análise de artigos relacionados	X			
Montar os códigos dos PRNGs		X		
Preparação das Sequências de Teste		X		
Execução da Bateria NIST STS		X		
Coleta de dados		X		
Avaliação Estatística			X	
Interpretação, validação e análise comparativa com a literatura			X	
Análise dos resultados da pesquisa				X
Mostrar os resultados e a conclusão				X

A metodologia adotada neste trabalho foi organizada em etapas sequenciais que permitem implementar, testar e avaliar o desempenho dos PRNGs selecionados. Cada fase do processo contribui para garantir reprodutibilidade, padronização e rigor estatístico na análise. A seguir, são descritas as etapas que compõem o procedimento metodológico utilizado neste estudo.

1) Montar os códigos dos PRNGs: A primeira etapa consiste na implementação dos PRNGs selecionados para a análise. Para garantir reprodutibilidade e facilitar a comparação entre os geradores, é necessário implementar manualmente todos os algoritmos, seguindo descrições formais encontradas na literatura e, sempre que possível, utilizando versões amplamente aceitas e discutidas em trabalhos acadêmicos recentes. A implementação é realizada diretamente em um dispositivo IoT, de forma a refletir as restrições e características de sistemas embarcados reais. Os PRNGs são desenvolvidos em linguagem C++, devido à ampla adoção dessa linguagem em plataformas IoT e à sua compatibilidade com arquiteturas de microcontroladores com recursos limitados, garantindo que os resultados obtidos representem fielmente o comportamento do gerador em um ambiente embarcado.

2) Preparação das sequências de teste: Após a implementação dos PRNGs no dispositivo IoT, cada gerador produz as sequências de bits que serão avaliadas. Essas sequências são emitidas diretamente pelo dispositivo IoT como um fluxo de bits e capturadas por um computador anfitrião para armazenamento e posterior análise. Nessa etapa definem-se seeds controladas, padroniza-se o tamanho das sequências e efetuam-se múltiplas execuções para reduzir variações não sistemáticas. As sequências coletadas são salvas em arquivos binários ou de texto, conforme requerimentos da Bateria NIST STS, garantindo compatibilidade com a ferramenta de avaliação. Além disso, registra-se metadados essenciais (seed, método de transmissão, tamanho da sequência, número da execução e timestamp) para assegurar reprodutibilidade e rastreabilidade dos experimentos.

3) Execução da Bateria NIST STS: A Bateria NIST STS é utilizada para avaliar a aleatoriedade estatística das sequências produzidas pelos PRNGs. Cada sequência é submetida individualmente aos testes, seguindo rigorosamente os parâmetros estabelecidos no manual oficial do NIST. São executados diversos testes, como Frequência, Runs, FFT e Aproximação Linear, entre outros, permitindo uma análise robusta e abrangente do comportamento de cada gerador. Os resultados obtidos são registrados automaticamente para posterior análise comparativa.

4) Coleta de dados: Os dados resultantes das execuções — incluindo n-valores, estatísticas individuais dos testes, taxas de aprovação e informações auxiliares — são coletados e armazenados em arquivos estruturados. Essa etapa envolve a padronização dos formatos de saída, permitindo que os dados sejam integrados aos scripts de análise estatística sem necessidade de manipulações manuais. Além disso, são registradas informações relevantes, como a seed utilizada, o tamanho da sequência e o tempo de execução, garantindo a rastreabilidade dos experimentos.

5) Avaliação estatística: Com os dados coletados, inicia-se a etapa de avaliação estatística. A análise envolve tanto estatística descritiva (médias, desvios e distribuição dos n-valores) quanto a aplicação dos critérios estabelecidos pela própria bateria NIST, como a proporção mínima de testes aprovados e a verificação da uniformidade dos n-valores. Quando necessário, são utilizados métodos complementares, como histogramas de n-valores, testes adicionais de correlação e análises comparativas entre diferentes geradores.

5. Resultados Esperados

Nesta seção, apresentamos e discutimos os resultados obtidos a partir da análise teórica dos Geradores de Números Pseudo-aleatórios (PRNGs) aplicados a dispositivos de Internet das Coisas (IoT). Diferentemente de abordagens experimentais, os resultados aqui descritos derivam de um estudo aprofundado das características, limitações e potenciais de cada tipo de PRNG feito por meio do referencial teórico apresentado anteriormente, permitindo avaliar o desempenho esperado e a segurança dos PRNGs em ambientes com restrições de memória, processamento e energia [Kietzmann et al. 2020]. A partir da literatura analisada, foi possível identificar padrões de eficiência e segurança esperados quando esses geradores são aplicados em ambientes restritos, como aqueles típicos de dispositivos IoT. Dessa forma, os resultados apresentados refletem uma interpretação crítica dos fundamentos teóricos e das evidências já consolidadas na área,

destacando implicações práticas e comparações entre diferentes abordagens de geração pseudo-aleatória.

Um exemplo importante citado no artigo é o Xorshift, que, em comparação com outros geradores clássicos, como o Mersenne Twister e TinyMT, obtêm melhores resultados em testes de aleatoriedade e previsibilidade estatística, oferecendo maior robustez para aplicações que exigem segurança criptográfica. Apesar de seu desempenho, geradores bitwise como o Xorshift apresentam qualidade estatística e resistência a ataques inferior à de PRNGs criptograficamente seguros, pois não incorporam mecanismos avançados de mistura de entropia ou pós-processamento. Por outro lado, variantes do Mersenne Twister e TinyMT apresentam maior robustez estatística, porém com consumo de energia e recursos mais elevados, evidenciando um trade-off entre desempenho e segurança [Kietzmann et al. 2020]. O LCG, por sua vez, apresenta implementação simples, mas com menor qualidade estatística e taxas de produção inferiores ao Xorshift, especialmente em núcleos de processadores com restrições de energia. No entanto, essa maior qualidade vem acompanhada de maior consumo de memória, energia e menor taxa de produção em comparação aos métodos bitwise, evidenciando o trade-off mencionado acima.

Apesar de seu desempenho, geradores bitwise como o Xorshift apresentam qualidade estatística e resistência a ataques inferior à de PRNGs criptograficamente seguros, pois não incorporam mecanismos avançados de mistura de entropia ou pós-processamento. Por outro lado, variantes do Mersenne Twister e TinyMT apresentam maior robustez estatística, porém com consumo de energia e recursos mais elevados, evidenciando um trade-off entre desempenho e segurança [Kietzmann 2021].

Os resultados de pesquisa sobre Geradores de Números Pseudo-Aleatórios (PRNGs) para IoT demonstram que as arquiteturas híbridas são cruciais para atingir a combinação ideal de segurança e eficiência. O trabalho ”A Secure and Efficient Software Random Number Generator Applicable to Internet of Things” [He et al. 2024] valida o gerador SESRNG, que combina mecanismos caóticos e pools de entropia com o pós-processamento robusto do SHA-256, resultando em números pseudo aleatórios que alcançam sucesso completo em testes estatísticos de alto rigor, como a suíte NIST SP 800-22. Complementarmente, a diretriz fornecida em ”A Guideline on Pseudorandom Number Generation (PRNG) in the IoT” e “Design and Implementation of Low-power High-throughput PRNGs for Security Applications” [Kietzmann et al. 2020] atesta que a alta taxa de transferência e o baixo consumo de energia essenciais para o firmware de segurança em IoT são alcançados por meio de geradores otimizados, como o Bluxor, que utilizam a combinação eficiente de operações Xorshift e componentes de mistura não linear, e de forma similar, arquiteturas como o MPSC PRNG exploram o dinamismo de múltiplos sistemas caóticos para garantir alta qualidade criptográfica em implementações de Hardware.

Em síntese, os resultados indicam que a escolha do PRNG em sistemas IoT deve considerar o contexto de uso: Xorshift e geradores bitwise simples são vantajosos para aplicações de alto desempenho e baixo consumo, enquanto geradores com pós-processamento ou arquiteturas híbridas são mais adequados quando a segurança e a imprevisibilidade são prioridades [Kietzmann et al. 2020].

6. Conclusão

A análise comparativa dos diferentes Geradores de Números Pseudo aleatórios (PRNGs) mostra que algoritmos simples como o Xorshift e o Linear Congruential Generator (LCG) continuam altamente relevantes para dispositivos IoT devido à sua baixa complexidade, rápida execução e reduzido consumo de energia. Esses geradores apresentam desempenho expressivo em plataformas com hardware limitado, oferecendo throughput elevado e implementação minimalista, características essenciais para aplicações onde eficiência é mais importante que segurança forte. No entanto, apesar dessas vantagens, ambos possuem limitações significativas em qualidade estatística e previsibilidade, tornando-os inadequados em cenários que exigem proteção criptográfica.

Os resultados obtidos mostram que, entre os geradores leves, o Knuth LCG se destaca como a melhor opção para tarefas não criptográficas, oferecendo desempenho consistente e baixo custo computacional, ao contrário de alternativas como Xorshift, que apresenta falhas estatísticas significativas [Kietzmann et al. 2020]. Por outro lado, quando o foco é segurança, os testes estatísticos confirmam a necessidade de utilizar PRNGs criptograficamente seguros, sendo o SHA-256 o mais adequado para ambientes IoT por equilibrar robustez, consumo reduzido de recursos e simplicidade de implementação [Kietzmann et al. 2020].

Os dados apresentados no artigo evidenciam que não existe um PRNG universalmente ideal para o ecossistema IoT. A escolha deve sempre considerar o contexto: geradores leves como Xorshift e LCG são adequados para tarefas de alta taxa de geração e baixo impacto energético, enquanto geradores estatisticamente mais fortes se tornam indispensáveis em sistemas que priorizam confidencialidade e resistência a ataques, como o SHA-256 [Kietzmann et al. 2020].

Assim, o capítulo demonstra que a escolha correta de PRNGs em IoT deve sempre considerar o contexto de uso, distinguindo entre necessidades criptográficas e operações de apoio. As recomendações propostas estabelecem um caminho claro para o desenvolvimento de sistemas IoT mais seguros e eficientes, tornando o estudo essencial para qualquer projeto que dependa de geração confiável de números pseudo aleatórios.

References

Fan, X., Wang, J., and Xu, L. (2021). A consistent address allocation algorithm mitigating address conflict for large-scale lora-enabled iot networks. In Liu, H. and Zhao, G., editors, *Advances in IoT Networking Technologies*, pages 211–225. IEEE Press.

He, D., Huang, W., Chen, L., and Chan, S. (2024). A secure and efficient software random number generator applicable to internet of things. In Zhao, T. and Lin, M., editors, *Advances in Internet of Things Security*, pages 101–115. IEEE Press.

Kietzmann, P., Schmidt, T. C., and Wählich, M. (2020). A guideline on pseudorandom number generation (prng) in the iot. In Brown, A. and Kim, L., editors, *Security and Cryptography in the Internet of Things*, pages 33–47. arXiv Preprint Series.

Němec, M., Kubát, P., and Hajny, J. (2019). Design and implementation of low-power high-throughput prngs for security. In Tan, K. and Zhou, L., editors, *Design and Implementation Advances in Hardware Security*, pages 305–318. Springer.

Orúe, A. B., Hernández-Encinas, L., Martín, A., and Montoya, F. (2017). A lightweight pseudorandom number generator for securing the internet of things. In *IEEE Access*, pages 1–12. IEEE.

Paul, P. S., Sadia, M., and Hasan, M. S. (2021). Design of a dynamic parameter-controlled chaotic-prng in a 65nm cmos process. In *arXiv preprint*, pages 1–15. arXiv.

Popereshnyak, S. and Raichev, A. (2024). Lightweight pseudorandom number generator model for the internet of things. In *Science-Based Technologies*, pages 1–12. Science Press.

Teo, T. H., Zhang, X., Ren, G., and Kok, C. L. (2025). Pseudo random number generator using internet-of-things techniques on portable field-programmable gate-array platform. In *arXiv preprint*, pages 1–15. arXiv.

Wallace, K., Moran, K., Novak, E., Zhou, G., and Sun, K. (2016). Toward sensor-based random number generation for mobile and iot devices. In Smith, R. and Liu, P., editors, *Innovations in Mobile and IoT Systems*, pages 1189–1201. IEEE Press.

Wu, J., Salim, A. Y., Elmitwalli, E., Köse, S., and Ignjatovic, Z. (2024). A pseudo-random number generator for multi-sequence generation with programmable statistics. In *arXiv preprint*, pages 1–12. arXiv.

Zhang, T., Li, Y., and Wang, C. (2022). Simplification of frequency test for random number generation based on chi-square. In Rossi, F. and Chen, D., editors, *Advances in Random Number Testing and Analysis*, pages 59–70. Springer.

Zia, U., McCartney, M., Scotney, B., Martinez, J., and Sajjad, A. (2022). A novel pseudo-random number generator for iot based on a coupled map lattice system using the generalised symmetric map. In *SN Applied Sciences*, page 48. Springer.