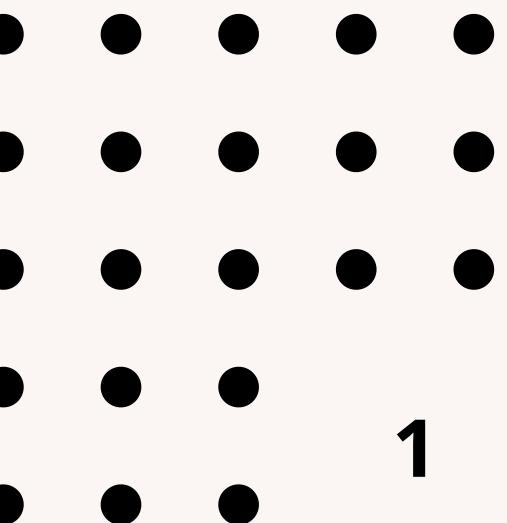


GERADORES DE NÚMEROS PSEUDO ALEATÓRIOS EM IOT: EFICIÊNCIA E SEGURANÇA EM AMBIENTES LIMITADOS

Por Thiago gomes e Vitor Costa



NOSSA DUPLA

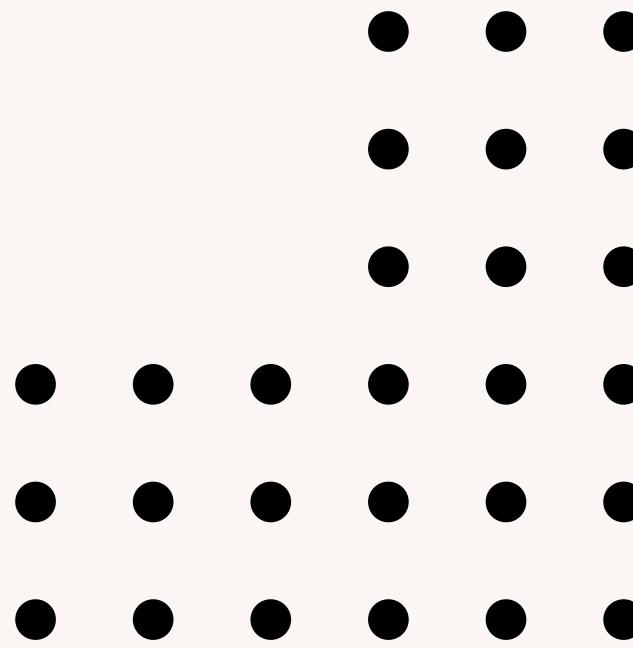


THIAGO GOMES



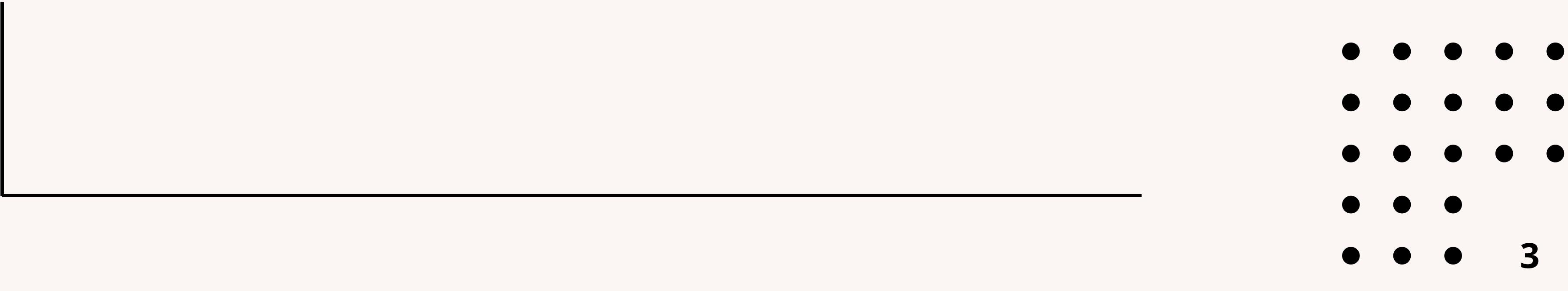
VITOR COSTA

ORIENTADOR: JOÃO PEDRO SANTOS PEREIRA



Introdução

CONTEXTUALIZAÇÃO
MOTIVAÇÃO
OBJETIVOS



CONTEXTUALIZAÇÃO

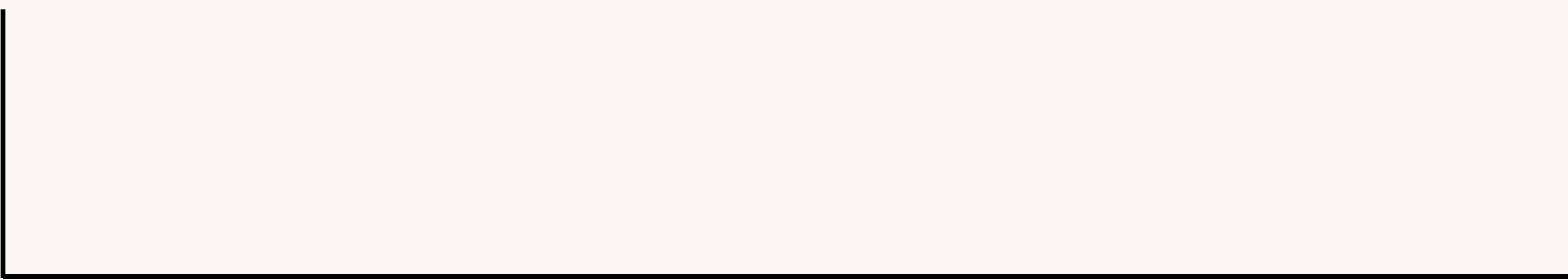
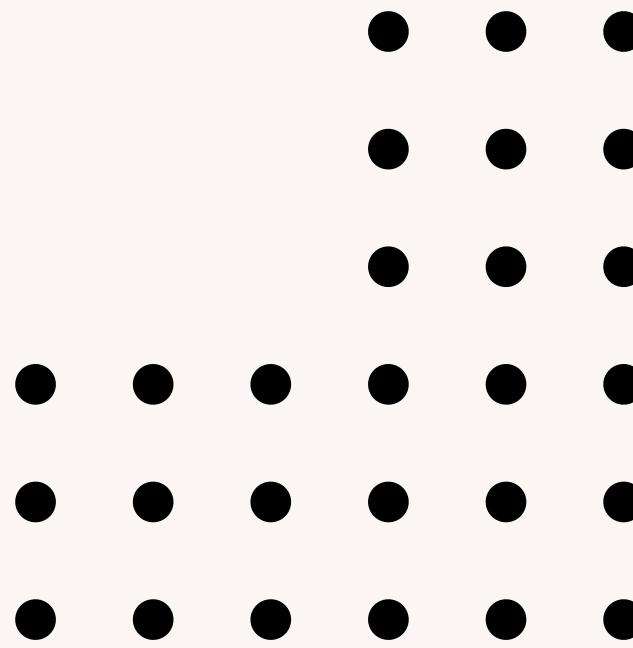
- A Internet das Coisas (IoT) conecta bilhões de dispositivos (sensores, câmeras, etc.);
- Esses dispositivos são restritos em recursos: pouca memória, processamento e energia;
- A segurança da IoT depende de criptografia forte, que exige números aleatórios de alta qualidade;
- PRNGs leves são a principal opção prática em IoT;
- RNGs fracos já causaram falhas graves em protocolos de segurança.

MOTIVAÇÃO

- 1 Poucos artigos que tratam sobre o tema
- 2 Existe uma grande variedade de PRNGs, mas falta uma análise comparativa sistemática
- 3 Falta de testes práticos
- 4 Segurança começa na aleatoriedade confiável.
- 5 Tema atual e relevante, pois ataques em IoT estão crescendo.

OBJETIVOS

- Fazer uma análise comparativa precisa dos principais PRNGs.
- Revisar a literatura recente sobre o tema.
- Comparar desempenho e segurança.
- Mostrar qualidade estatística, eficiência computacional
(tempo, memória, energia).
- Apontar recomendações para avaliações de PRNGs.



Referêncial Teórico

REFERENCIAL TEÓRICO

NÚMEROS PSEUDO ALEATÓRIOS

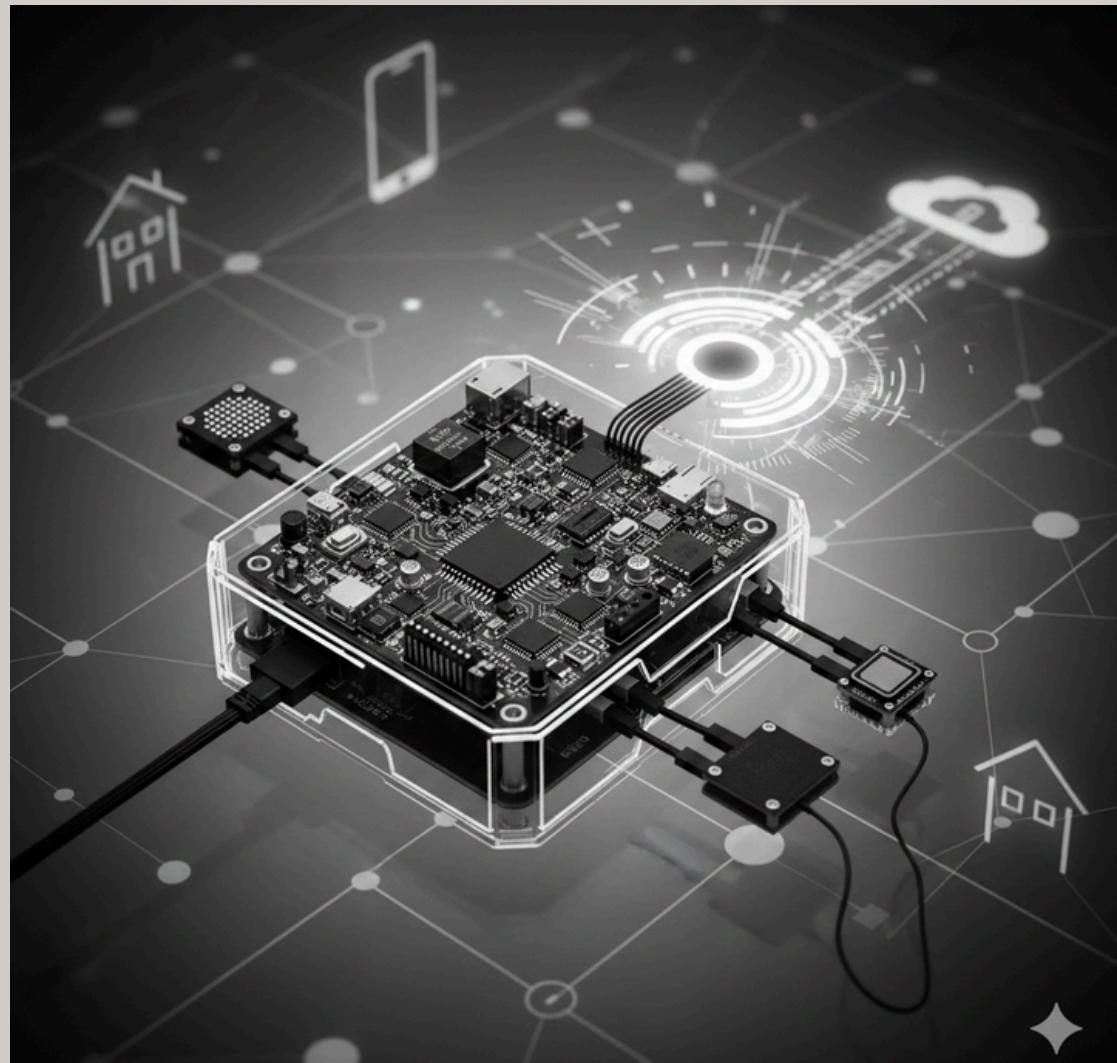
Sequência gerada por algoritmo determinístico que parece aleatória, usada em simulações e criptografia por ser eficiente e fácil de gerar.

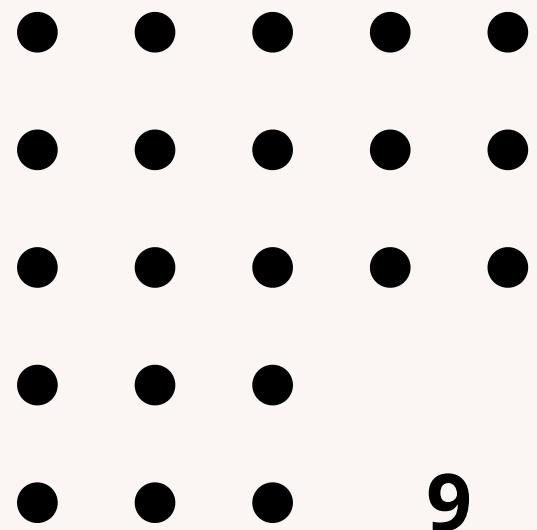
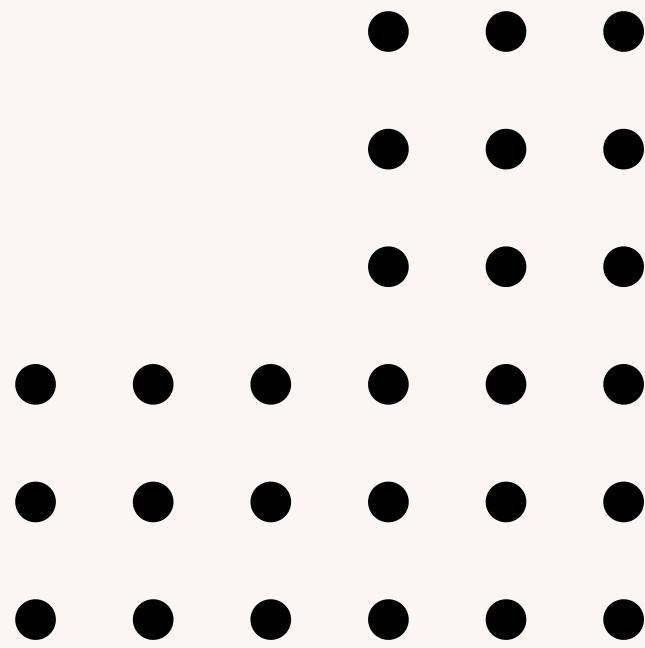
INTERNET DAS COISAS (IOT)

Internet das Coisas (IoT) é a rede de objetos físicos (“coisas”) equipados com sensores, software e conectividade, de modo que possam coletar, trocar e processar dados com outros dispositivos ou sistemas via rede.

CRIPTOGRAFIA

A Criptografia é a área que lida com técnicas para proteger a informação, garantindo sua confidencialidade, integridade e autenticidade.





Trabalhos relacionados

TRABALHOS RELACIONADOS

“

*A GUIDELINE ON
PSEUDORANDOM NUMBER
GENERATION (PRNG) IN THE
IOT (QUALIS A1)*

Esse artigo foi essencial para a construção da análise dos PRNGs, e também trouxe grande parte da fundamentação teórica sobre os principais PRNGs para IoT.

*A SECURE AND EFFICIENT
SOFTWARE RANDOM NUMBER
GENERATOR APPLICABLE TO
INTERNET OF THINGS
(QUALIS A1)*

O artigo reforça a importância conciliar robustez com restrições de hardware. Os algoritmos usados se destacam pela imprevisibilidade.

*TOWARD SENSOR-BASED
RANDOM NUMBER GENERATION
FOR MOBILE AND IOT
DEVICES (QUALIS A1)*

O artigo aborda fontes de entropia eficientes e baseada em sensores e evidencia complicações em hardware restrito.

TRABALHOS RELACIONADOS

“

SIMPLIFICATION OF FREQUENCY TEST FOR RANDOM NUMBER GENERATION BASED ON CHI-SQUARE (QUALIS A3)

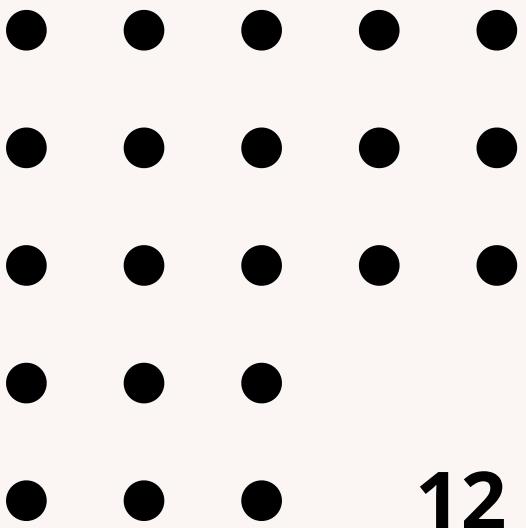
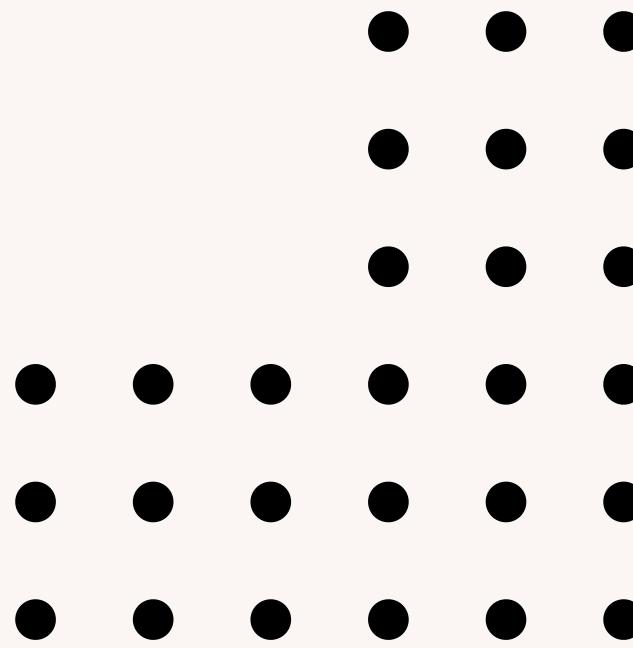
O artigo foi usado para o entendimento sobre os principais testes usados para a analise da qualidade de PRNGs, fundamental para o trabalho.

DESIGN AND IMPLEMENTATION OF LOW-POWER HIGH-THROUGHPUT PRNGS FOR SECURITY (QUALIS A4)

Esse artigo trás como tema principal PRNGs híbridos, que são muito uteis para atingirem com mais eficiênciam um objetivo específico.

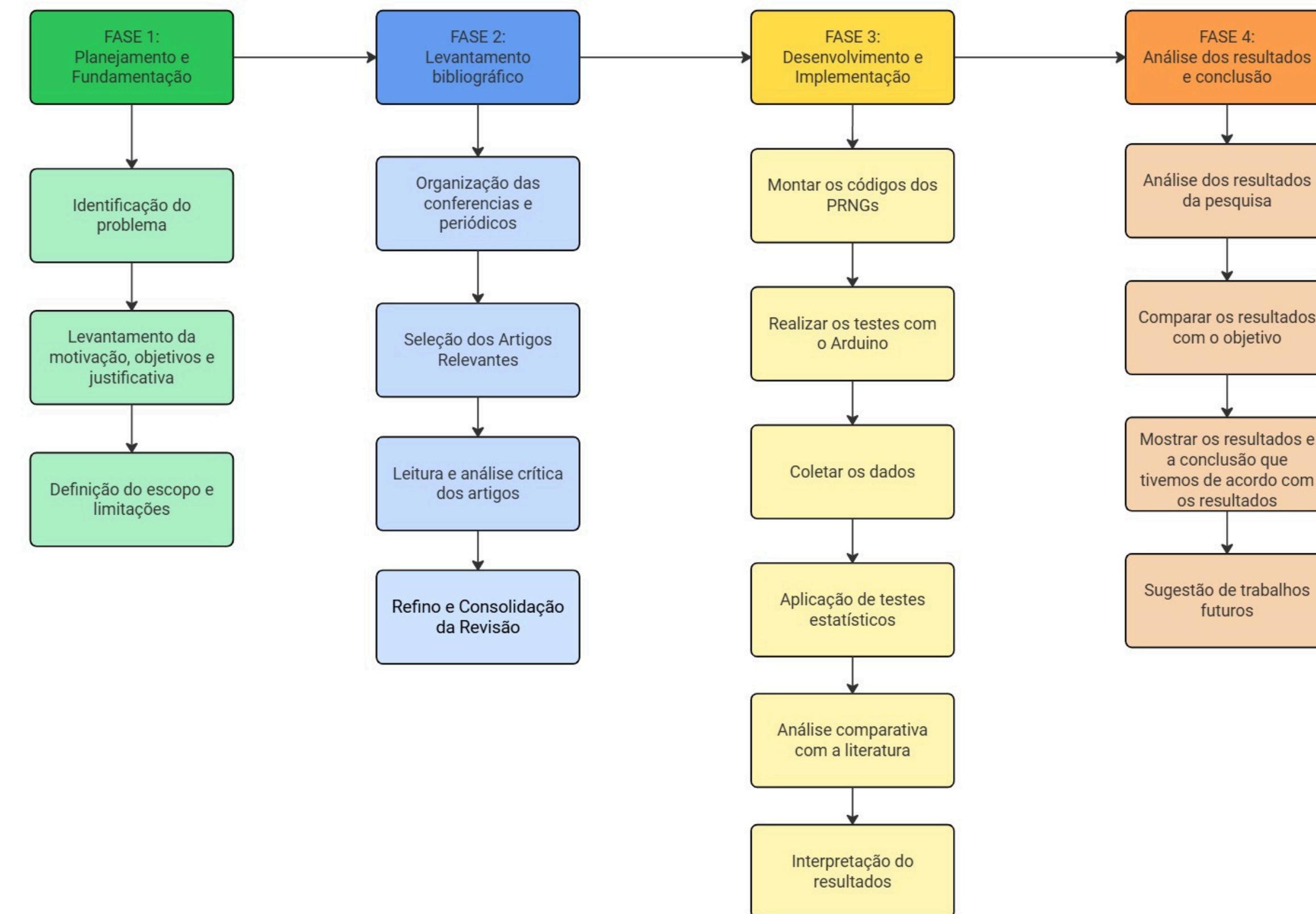
A CONSISTENT ADDRESS ALLOCATION ALGORITHM MITIGATING ADDRESS CONFLICT FOR LARGE-SCALE LORA-ENABLED IOT NETWORKS (QUALIS A4)

O estudo mostra uma aplicação prática de um PRNG, o xorshift, para diminuir os conflitos de endereço em um dispositivo IoT.



Metodologia

METODOLOGIA-FLUXOGRAMA



METODOLOGIA

- 1 Montar os códigos dos PRNGs
- 2 Preparação das sequências de teste
- 3 Execução da Bateria NIST STS
- 4 Coleta de dados
- 5 Avaliação estatística

CRONOGRAMA

	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 dos Resultados e Análise comparativa com a literatura			X	
Análise dos resultados da pesquisa				X
Mostrar os resultados e a conclusão				X

Resultados

RESULTADOS

XORSHIFT

- Alta velocidade e bom desempenho estatístico.
- Melhor que Mersenne Twister e TinyMT em testes de aleatoriedade.
- Limitação: menor segurança por ausência de mecanismos avançados de entropia.

MERSENNE TWISTER E TINYMT:

- Maior robustez estatística.
- Contra: maior consumo de energia e recursos (trade-off desempenho × segurança).

RESULTADOS

LCG:

- Implementação simples e leve.
- Baixa qualidade estatística e menor taxa de produção de números aleatórios.

PRNGS HÍBRIDOS E AVANÇADOS (EX.: SESRNG):

- Combinação de fontes caóticas, pools de entropia e pós-processamento criptográfico (SHA-256).
- Resultados excelentes em testes rigorosos (ex.: NIST SP 800-22).

Conclusão

CONCLUSÃO

- Xorshift e LCG são adequados para tarefas de alta taxa de geração e baixo impacto energético, mas o LCG se destaca entre os geradores mais leves, em operações não criptográficas;
- Enquanto geradores estatisticamente mais fortes se tornam indispensáveis em sistemas que priorizam confidencialidade e resistência a ataques, como o SHA-256;
- Os dados apresentados no artigo evidenciam que não existe um PRNG universalmente ideal para o ecossistema IoT. A escolha deve sempre considerar o contexto;

Bibliografia

BIBLIOGRAFIA

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.

BIBLIOGRAFIA

1. Popreshnyak, S. and Raichev, A. (2024). Lightweight pseudorandom number generator model for the internet of things. In Science-Based Technologies, pages 1-12. Science Press.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.

MUITO OBRIGADO PELA
ATENÇÃO!

Por Thiago gomes e Vitor Costa