Análise de PRNGs em Hardware para Otimização de Memória na Amplificação de Privacidade em CV-QKD

José B. de Souza Júnior [1,2], Ramylla L. B. G. Bezerra [1,3], Henrique N. Teixeira [1,3], Hugo S. C. Bessa [1], Linton T. C. Esteves [1], Valéria L. Silva [1] Nelson A. F. Neto [1]

[1] QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC
Competence Center in Quantum Technologies, SENAI CIMATEC, Salvador/BA, Brasil

[2]Programa de Pós-Graduação em Modelagem Computacional e Tecnologia Industrial (PPGMCTI)
Universidade SENAI CIMATEC, Salvador/BA, Brasil

[3]Programa de Pós-Graduação em Engenharia Elétrica e de Computação (PPGEEC)
Escola Politécnica, Universidade Federal da Bahia (UFBA), Salvador/BA, Brasil

{jose.juniors,linton.esteves,hugo.bessa}@fbter.org.br
{nelson.neto,valeria.dasilva}@fieb.org.br
{ramyllabezerra,henrique.teixeira}@ufba.br

Abstract. *Continuous-Variable Quantum Key Distribution (CV-QKD) is a promising technology for metropolitan quantum networks. However, privacy amplification based on Toeplitz matrices imposes a memory bottleneck that limits node scalability. This work proposes an architecture where the matrix-defining vector is generated on-the-fly using hardware-based Pseudo-Random Number Generators (PRNGs), eliminating the need for massive external storage. A comparative analysis of PRNGs selected via the NIST SP 800-22 suite and hardware metrics (LUTs/FFs in FPGA; area in ASIC) identifies solutions with throughput exceeding 13 Gbps (FPGA) and up to 39 Gbps (ASIC) with low resource consumption. The impact on the control plane and end-to-end latency is discussed, demonstrating that dynamic generation simplifies signaling and enables high-performance CV-QKD nodes.*

Resumo. *A Distribuição Quântica de Chaves com variáveis contínuas (CV-QKD) é uma tecnologia promissora para redes quânticas metropolitanas, mas a amplificação de privacidade baseada em matrizes de Toeplitz impõe um gargalo de memória que limita a escalabilidade dos nós. Este trabalho propõe uma arquitetura em que o vetor definidor da matriz é gerado dinamicamente (on-the-fly) por geradores pseudoaleatórios (PRNGs) em hardware, eliminando o armazenamento externo massivo. A análise comparativa de PRNGs selecionados pela suíte NIST SP 800-22 e por métricas de hardware (LUTs/FFs em FPGA; área em ASIC) identifica soluções com vazão superior a 13 Gbps (FPGA) e até 39 Gbps (ASIC) e baixo consumo de recursos. Discute-se o impacto no plano de controle e na latência fim-a-fim, mostrando que a geração dinâmica simplifica a sinalização e viabiliza nós CV-QKD.*

1. Introdução

A computação quântica ameaça a criptografia assimétrica atual, como o RSA [Dwivedi et al. 2023], enquanto as redes quânticas surgem como uma possível solução para esse problema através da Distribuição Quântica de Chaves (QKD). A QKD com

variáveis contínuas (CV-QKD) destaca-se por sua compatibilidade com infraestruturas de telecomunicações já implantadas [Zhang et al. 2024]. No pós-processamento do CV-QKD, a amplificação de privacidade (PA) elimina informações parciais de um espião [Van Assche 2006], sendo as matrizes de Toeplitz amplamente utilizadas por sua eficiência computacional.

Para maximizar a taxa de chave secreta em tamanho finito, os blocos de entrada podem atingir de 10^8 a 10^{10} bits [Wang et al. 2018, Yan et al. 2022]. O vetor semente de uma matriz de Toeplitz pode chegar a centenas de megabits, excedendo a memória interna de FPGAs e forçando o uso de memórias externas, o que introduz latência e limita a escalabilidade dos nós QKD.

Este trabalho propõe uma arquitetura em que o vetor definidor da matriz de Toeplitz é gerado dinamicamente por geradores pseudoaleatórios (PRNGs) em hardware. Alice e Bob compartilham apenas uma semente curta, eliminando o armazenamento externo e reduzindo a latência. Adicionalmente, essa abordagem reduz a sobrecarga no canal clássico, pois apenas a semente curta precisa ser transmitida entre os nós. Realizamos uma análise comparativa de PRNGs aprovados no NIST SP 800-22, avaliando métricas de hardware (LUTs/FFs para FPGA; área para ASIC) e vazão, visando identificar o melhor compromisso entre qualidade estatística, desempenho e uso de recursos para integração em nós CV-QKD de alto desempenho em redes quânticas futuras.

O artigo está organizado como segue. A Seção 2 apresenta o referencial teórico. A Seção 3 descreve a arquitetura de geração dinâmica. A Seção 4 detalha a metodologia de seleção. A Seção 5 analisa as implementações em FPGA e ASIC. A Seção 6 discute os resultados e implicações para redes quânticas. Por fim, A Seção 7 apresenta as conclusões.

2. Fundamentação Teórica

Esta seção fundamenta os conceitos de amplificação de privacidade bem como as plataformas de *hardware* alvos deste trabalho.

2.1. Amplificação de Privacidade com Matrizes de Toeplitz

A amplificação de privacidade (PA) reduz a informação que um espião (Eve) pode ter sobre a chave bruta em QKD. O método baseado em hashing universal com matrizes de Toeplitz é o mais difundido em sistemas práticos [Krawczyk 1994, Ma et al. 2007]. Uma matriz de Toeplitz T de dimensões $m \times n$ é definida por um vetor semente de $m + n - 1$ bits (primeira linha e primeira coluna). Sua aplicação à chave bruta de n bits produz uma chave final de m bits. A família de funções hash deve garantir universalidade (baixa probabilidade de colisão) e uniformidade da saída, assegurando a segurança da chave [Renner 2005]. No contexto de QKD, o *Leftover Hash Lemma* garante que, se a chave bruta possui entropia mínima suficiente, a aplicação de uma função hash universal produz uma chave final estatisticamente indistinguível de uma sequência uniformemente aleatória.

2.2. Plataformas de Hardware: FPGA e ASIC

FPGAs (*Field-Programmable Gate Arrays*) são dispositivos reconfiguráveis cujo consumo de recursos é medido por LUTs e flip-flops (FFs) [Kuon and Rose 2007]. ASICs (*Application-Specific Integrated Circuits*) oferecem maior densidade e eficiência

energética, sendo quantificados por área física (μm²) ou equivalentes de porta (kGE) [Weste and Harris 2015]. A arquitetura proposta explora o melhor de cada plataforma: alta vazão com baixa ocupação em FPGA, e compactação com eficiência energética em ASIC.

3. Arquitetura de Geração Dinâmica

Na arquitetura proposta, ilustrada na Figura 1, substitui-se o armazenamento estático pela geração dinâmica dos coeficientes utilizando PRNGs em hardware: Alice e Bob compartilham antecipadamente uma semente curta via canal clássico autenticado, que é carregada nos PRNGs de ambos os nós; durante a amplificação de privacidade, cada nó gera dinamicamente os bits do vetor definidor da matriz de Toeplitz no momento da operação de hashing, eliminando a necessidade de memórias externas para armazenar os vetores geradores.

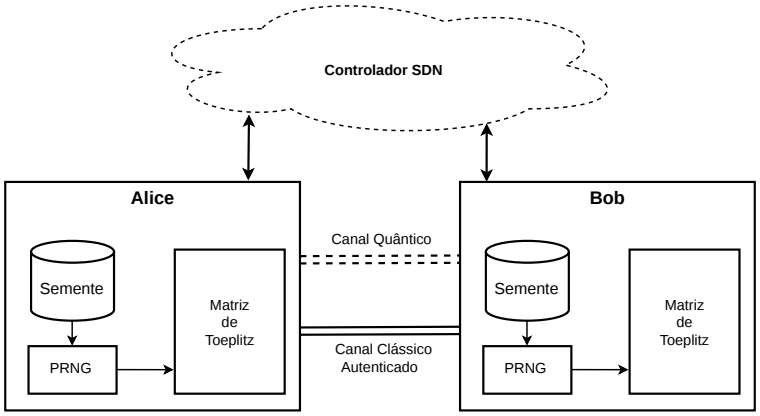

Figura 1. Arquitetura de geração dinâmica para amplificação de privacidade em redes CV-QKD.

4. Metodologia de Seleção e Avaliação

Esta seção descreve o processo sistemático para identificar arquiteturas de PRNGs em hardware adequadas à geração dinâmica de coeficientes da matriz de Toeplitz em nós CV-QKD.

A busca foi realizada nas bases IEEE Xplore, Scopus e Web of Science (2020–2025) utilizando termos como *"pseudo-random number generator"*, *"hardware implementation"*, *"FPGA"*, *"ASIC"*, *"NIST SP 800-22"* e *"throughput"*. Foram incluídos apenas trabalhos com implementação explícita em hardware, métricas quantitativas de recursos e vazão, aprovação em todos os testes NIST SP 800-22 e reprodutibilidade determinística. A busca inicial resultou em 122 artigos, reduzidos para 57 após leitura de títulos e resumos e, em seguida, para 21 após leitura integral. Destes, selecionaram-se 5 trabalhos representativos, abrangendo diferentes famílias de PRNGs (LFSR dinâmico, mapas caóticos discretizados, *stream ciphers* leves e primitivas hash).

5. Análise das Arquiteturas

Esta seção detalha as implementações em hardware dos PRNGs selecionados, avaliando sua adequação à geração dinâmica de coeficientes da matriz de Toeplitz em nós CV-

QKD. A análise concentra-se no compromisso entre ocupação de recursos (LUTs/FFs para FPGA; área em μm² ou kGE para ASIC) e vazão.

5.1. Soluções em FPGA

A Tabela 1 consolida os resultados dos trabalhos finalistas em FPGA.

Tabela 1. Comparação de desempenho, consumo e eficiência dos trabalhos em FPGA.

Trabalho	Throughput (Gbps)	Recursos (LUTs+FFs)	Freq. Máx. (MHz)	Eficiência (Mbps/Recursos.)
Akter et al. (2025)	0,50	118	500,0	4,23
Souza et al. (2025) PRNG 2 (Z_2^{32})	24,00	339	375,0	**70,79**
Souza et al. (2025) PRNG 2 (Z_2^{64})	19,20	696	150,0	27,58
Souza et al. (2025) PRNG 1 (Z_2^{64})	16,00	315	250,0	50,79
Souza et al. (2025) PRNG 1 (Z_2^{32})	13,12	158	410,0	**83,03**
Souza et al. (2023)	3,80	270	122,5	14,07
Adharsh et al. (2025)	2,78	5193	277,8	0,53
Abbassi et al. (2022)	23,99	671	187,4	35,75

Destacam-se as arquiteturas de [Souza et al. 2025] (PRNG 1 em $Z32_2$) com 13,12 Gbps e apenas 158 LUTs+FFs, sendo particularmente atrativa para nós QKD embarcados com área lógica limitada. Por outro lado, [Abbassi et al. 2022] atinge 23,99 Gbps com 671 recursos, evidenciando que o paralelismo intensivo sustenta vazões elevadas.

5.2. Soluções em ASIC

A Tabela 2 resume as implementações em ASIC. Como os trabalhos utilizam diferentes nós tecnológicos (7 nm, 14 nm, 45 nm), as comparações devem ser interpretadas em termos de tendências.

Tabela 2. Comparação de desempenho e área dos trabalhos em implementação ASIC.

Trabalho / Arquitetura	Tech	Throughput (Gbps)	Área	Freq. (MHz)
[Crocetti et al. 2022] - SHA-3-256	7 nm	39.06	78.43 kGE	4120.0
[Crocetti 2023] - SHA-2-256	7 nm	16.52	46.51 kGE	4325.0
[Akter et al. 2025] - LFSR Dinâmico	14 nm	3.57	27.4 μm^2	3570.0
[Allahverdi and Mooney 2025] - Hybrid (Non-AEAD)	45 nm	0.30	4402 μm^2	300.0
[Allahverdi and Mooney 2025] - Hybrid (AEAD)	45 nm	0.30	5650 μm^2	300.0
[Allahverdi and Mooney 2025] - TRIVIUM	45 nm	0.30	5627 μm^2	300.0
[Allahverdi and Mooney 2025] - Espresso	45 nm	0.30	5894 μm^2	300.0
[Allahverdi and Mooney 2025] - Grain-128AEADv2	45 nm	0.30	6401 μm^2	300.0

As soluções baseadas em SHA-3-256 e SHA-2-256 em 7 nm oferecem as maiores vazões (até 39 Gbps), porém com área significativa (78,43 kGE), sendo indicadas para nós QKD centrais ou pontos de agregação. O LFSR dinâmico de [Akter et al. 2025] alcança 3,57 Gbps com apenas 27,4 μm² em 14 nm, apresentando excelente compactação para dispositivos de borda. As arquiteturas em 45 nm de [Allahverdi and Mooney 2025] operam abaixo de 0,31 Gbps, não atendendo ao requisito de 2 Gbps para geração dinâmica em alta velocidade.

6. Resultados e Discussões

Conforme a Tabela 1, múltiplas arquiteturas em FPGA atingem vazão superior a 2 Gbps: o PRNG 1 (Z_2^{32}) de [Souza et al. 2025] (13,12 Gbps, 158 LUTs+FFs) é ideal para nós QKD de borda, enquanto arquiteturas de [Abbassi et al. 2022] e [Souza et al. 2025] (PRNG 2) oferecem vazões próximas a 24 Gbps com maior consumo de recursos (671 e 339 LUTs+FFs), sendo mais adequadas para backbones. Em ASIC, a Tabela 2 mostra que SHA-3-256 (7 nm) atinge 39 Gbps com área de 78,43 kGE, posicionando-se como alternativa de alto desempenho, enquanto o LFSR dinâmico de [Akter et al. 2025] (14 nm) alcança 3,57 Gbps com área de 27,4 μm² e potência de 33,4 μW, sendo o mais compacto e eficiente energeticamente.

A escolha da arquitetura de PRNG impacta diretamente a escalabilidade e o desempenho de redes CV-QKD: arquiteturas compactas (PRNG 1 em FPGA ou LFSR dinâmico em ASIC) são ideais para nós de borda com restrição de área e potência, enquanto arquiteturas de alta vazão (SHA-3-256 ou PRNG 2) atendem a nós de backbone onde o pós-processamento não pode limitar a taxa de chave.

7. Conclusões

Este trabalho apresentou uma arquitetura para amplificação de privacidade em sistemas CV-QKD baseada na geração dinâmica dos coeficientes da matriz de Toeplitz por PRNGs em hardware, eliminando a necessidade de armazenamento externo massivo e, consequentemente, o gargalo de memória presente em implementações convencionais. A abordagem proposta permite que apenas uma semente curta seja compartilhada entre os nós, reduzindo a latência, simplificando o plano de controle e favorecendo a escalabilidade de redes quânticas de alta velocidade.

Como trabalhos futuros, pretende-se desenvolver uma microarquitetura de amplificação de privacidade baseada em q-análogos [Souza et al. 2023], avaliando sua integração com PRNGs em hardware e validando sua operação em blocos de até 10^{10} bits. Adicionalmente, planeja-se a implementação completa da cadeia de pós-processamento CV-QKD com geração dinâmica, permitindo a avaliação fim-a-fim do impacto na taxa de chave secreta e na latência do sistema.

Agradecimentos

Este trabalho foi totalmente financiado pelos projetos “QRNG: Pós-processamento e Experimento”e “HW DSP: Desenvolvimento e Prototipagem de SoC Multicore com Aceleradores Dedicados e DSP RISC-V”suportados pelo QuIIN - Quantum Industrial Innovation, Centro de Competência EMBRAPII CIMATEC em Tecnologias Quânticas, com recursos financeiros oriundos do PPI IoT/Manufatura 4.0 do MCTI, através do Termo de Cooperação 053/2023, firmado com a EMBRAPII.

Referências

Abbassi, N., Gafsi, M., Hajjaji, M. A., and Mtibaa, A. (2022). Hardware design and implementation of a lightweight stream-cipher cryptosystem: A chaotic/reversible cellular automata approach. In *2022 IEEE 21st international Ccnference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, pages 255–260.

Akter, S., Khalil, K., and Bayoumi, M. (2025). A high performance and efficient method for enhancing randomness in linear feedback shift registers(lfsr). In *2025 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5.

Allahverdi, A. and Mooney, V. J. (2025). A hardware-efficient aead stream cipher based on a hybrid nonlinear feedback register structure. In *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, pages 1016–1023.

Crocetti, L. (2023). Can the sha-3 algorithm be used for the construction of efficient and robust hardware cryptographic random number generators? In *2023 IEEE 2nd Industrial Electronics Society Annual On-Line Conference (ONCON)*, pages 1–6.

Crocetti, L., Di Matteo, S., Nannipieri, P., Fanucci, L., and Saponara, S. (2022). Design and test of an integrated random number generator with all-digital entropy source. *Entropy*, 24(2):139.

Dwivedi, A., Saini, G. K., Musa, U. I., and Kunal (2023). Cybersecurity and prevention in the quantum era. In *2023 2nd International Conference for Innovation in Technology (INOCON)*, pages 1–6.

Krawczyk, H. (1994). Lfsr-based hashing and authentication. In *Advances in Cryptology — CRYPTO '94*, pages 129–139. Springer.

Kuon, I. and Rose, J. (2007). Measuring the gap between fpgas and asics. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 26(2):203–215.

Ma, X., Fung, C.-H. F., and Lo, H.-K. (2007). Quantum key distribution with entangled photon sources. *Physical Review A*, 76:012307.

Renner, R. (2005). *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich.

Souza, C. E. C., Moreno, D., Figueiredo, R. B. D., Chaves, D. P. B., and Pimentel, C. (2023). q-analogs over finite fields: Definition, algebraic properties, and application in pseudo-random number generators. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 70(8):3064–3068.

Souza, C. E. C., Moreno, D., Sousa, M. H. S., Chaves, D. P. B., and Pimentel, C. (2025). High-throughput pseudo-random number generators over discrete chaos. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 72(9):1303–1307.

Van Assche, G. (2006). *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, Cambridge, UK.

Wang, X., Zhang, Y., Yu, S., and Guo, H. (2018). High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution. *IEEE Photonics Journal*, 10(3):1–9.

Weste, N. and Harris, D. (2015). *CMOS VLSI Design: A Circuits and Systems Perspective*. Addison-Wesley, 4 edition.

Yan, B., Li, Q., Mao, H., and Chen, N. (2022). An efficient hybrid hash based privacy amplification algorithm for quantum key distribution. *Quantum Information Processing*, 21(4):130.

Zhang, Y., Bian, Y., Li, Z., Yu, S., and Guo, H. (2024). Continuous-variable quantum key distribution system: Past, present, and future. *Applied Physics Reviews*, 11(1).