57º SBPO
SIMPÓSIO BRASILEIRO DE PESQUISA OPERACIONAL
Gramado • RS
DE 5 A 9 DE OUTUBRO DE 2025

# AVALIAÇÃO DA ROBUSTEZ DO SPHINCS+ SOB SIMULAÇÕES DE COMPORTAMENTOS QUÂNTICOS

**Bruno Leonardo Santos Menezes**
FAETEC Resende – RJ
Resende, RJ, Brasil
bruno.menezes@faetecresende.com

**Franklin de Lima Marquezino**
Universidade Federal do Rio de Janeiro
Rio de Janeiro, RJ, Brasil
flmarquezino@cos.ufrj.br

**Claudio Miceli de Farias**
Universidade Federal do Rio de Janeiro
Rio de Janeiro, RJ, Brasil
cmfarias@cos.ufrj.br

**RESUMO**

Computadores quânticos podem comprometer algoritmos criptográficos clássicos, tornando essencial o estudo de soluções pós-quânticas. Este artigo investiga o comportamento do esquema de assinaturas digitais SPHINCS+ frente à execução simultânea de circuitos quânticos simulados. Inicialmente é apresentada uma revisão bibliográfica sobre criptografia baseada em funções de hash e sobre o SPHINCS+. Em seguida, propomos uma metodologia que integra a compilação do SPHINCS+ em C com a simulação de circuitos quânticos em Python/Qiskit (estados GHZ, emaranhamento de múltiplos qubits e algoritmo de Grover). São descritas as rotinas de geração de chaves, assinatura, execução dos circuitos e verificação das assinaturas. Os resultados mostram que as assinaturas permanecem válidas mesmo após a co-execução com circuitos quânticos simulados, indicando a robustez do SPHINCS+ no ambiente avaliado. Discussões teóricas e perspectivas de pesquisa futura complementam o estudo.

**PALAVRAS CHAVE. Computação Quântica. Criptografia Pós-Quântica. SPHINCS+.**

***Tópicos:*** **OQ–Otimização Quântica; SIM – Simulação; PO em Defesa e Segurança.**

**ABSTRACT**

The prospect of quantum computers compromising classical cryptographic algorithms motivates the search for post-quantum solutions. This paper investigates the behavior of the SPHINCS+ digital signature scheme under the simultaneous execution of simulated quantum circuits. We first review the literature on hash-based cryptography and SPHINCS+. A methodology is then proposed that integrates compilation of SPHINCS+ in C with the simulation of quantum circuits using Python/Qiskit (GHZ state generation, multi-qubit entanglement and Grover's algorithm). The routines for key generation, signature, circuit execution and signature verification are described. Experimental results show that signatures remain valid after co-execution with simulated quantum circuits,

**DOI:** 10.59254/sbpo-2025-212673
https://proceedings.science/p/212673?lang=pt-br

indicating the robustness of SPHINCS+ in the evaluated environment. Theoretical discussions and future research directions are also presented.

**KEYWORDS. Quantum Computing. Post-Quantum Cryptography. SPHINCS+.**

***Paper topics:*** **OQ–Quantum Optimization; SIM – Simulation; PO in Defense and Security.**

**DOI:** 10.59254/sbpo-2025-212673
https://proceedings.science/p/212673?lang=pt-br

## 1. Introdução

O desenvolvimento da computação quântica coloca em risco diversos algoritmos criptográficos clássicos, pois computadores quânticos poderão executar rotinas como a fatoração e a busca de forma significativamente mais eficiente. Vários autores apontam que rotinas pós-quânticas emergem como alternativas seguras nesse cenário [Bavdekar et al., 2022; Khurram e Hussain, 2024]. Nesse contexto, o SPHINCS+ destaca-se por ser um esquema de assinaturas baseado em funções de hash e árvores de Merkle, cuja segurança é fundamentada na dificuldade de encontrar colisões ou inversões nessas funções. Entretanto, entender como tal esquema se comporta quando executado em ambiente quântico (ainda que simulado) é essencial para avaliar sua robustez.

Este trabalho visa analisar a integridade e a robustez do SPHINCS+ quando chaves e assinaturas são geradas e verificadas paralelamente à execução de circuitos quânticos simulados. A abordagem consiste em compilar o SPHINCS+ em C, gerar chaves e assinaturas e, em seguida, rodar circuitos quânticos em Python por meio da biblioteca Qiskit. Ao final, as assinaturas são verificadas novamente para detectar possíveis alterações. Este artigo está organizado da seguinte forma: a Seção 2 apresenta a revisão bibliográfica; a Seção 3 descreve a metodologia proposta e os ambientes de teste; a Seção 4 traz os resultados obtidos; a Seção 5 encerra com as conclusões e perspectivas futuras.

## 2. Revisão bibliográfica

Os primeiros esquemas de assinaturas baseados em hash surgiram nos anos 1970 com as propostas de Lamport e Merkle. Posteriormente, Bernstein e other authors [2015] introduziram o SPHINCS, uma assinatura hash sem estado, eliminando a necessidade de rastrear o estado do sistema e simplificando sua implementação. O SPHINCS+ foi proposto posteriormente e selecionado pelo NIST para padronização [Bernstein e other authors, 2019]. Seu principal diferencial é a combinação de múltiplas camadas de árvores XMSS e blocos FORS (Forest of Random Subsets), o que melhora a segurança ao custo de chaves e assinaturas maiores.

Estudos recentes discutem o cenário pós-quântico e as vantagens de esquemas baseados em hash. Bavdekar et al. [2022] revisam técnicas de criptografia pós-quântica e apontam que assinaturas de hash são inovadoras, mas podem ser vulneráveis a ataques de canal lateral e apresentam tempos de processamento superiores em comparação com algoritmos como CRYSTALS-DILITHIUM ou FALCON. Singh [2019] exploram os parâmetros do SPHINCS+, como o tamanho da saída da função de hash ($n$), o parâmetro Winternitz ($w$) e o número de camadas da árvore XMSS ($d$), mostrando que tais parâmetros impactam no tamanho das assinaturas e na eficiência. Outros trabalhos [Khurram e Hussain, 2024; Krishan, 2024] discutem a necessidade de segurança pós-quântica em aplicações como VPNs e data centers, reforçando a importância de analisar a robustez de novos esquemas.

No contexto de avaliação experimental do SPHINCS+, Menezes et al. [2024] apresentaram uma primeira simulação de ataque quântico em ambiente hipotético, focando na geração de estados básicos. Contudo, não há registros de estudos que integrem a compilação do SPHINCS+ com a execução de circuitos quânticos de maior complexidade, como estados GHZ, emaranhamento de quatro qubits ou o algoritmo de Grover. Este trabalho se propõe a preencher essa lacuna.

## 3. Metodologia

Esta pesquisa adapta e expande a metodologia de Menezes et al. [2024]. O processo é estruturado conforme ilustrado na Figura 1. Inicialmente, o repositório oficial do SPHINCS+[1] é clonado e compilado em uma máquina x86_64 com processador Intel Core i5-10400, 16 GB de RAM e sistema Fedora 40. O compilador GCC é utilizado com as opções `PARAMS=sphincs-shake-256f`

[1] `https://github.com/sphincs/sphincsplus`

**DOI:** 10.59254/sbpo-2025-212673
https://proceedings.science/p/212673?lang=pt-br

e `THASH=robust`. Os programas geram chaves (*genKAT*) e assinaturas de acordo com o esquema. Em paralelo, são desenvolvidos scripts em Python usando a biblioteca Qiskit para simular três circuitos quânticos: (i) geração do estado GHZ de 3 qubits; (ii) emaranhamento de 4 qubits com portas Hadamard, CNOT, SWAP e X; e (iii) uma instância simples do algoritmo de Grover com 2 qubits.

O experimento consiste nos seguintes passos:

1. Gerar um par de chaves pública e privada e assinar uma mensagem de teste utilizando o SPHINCS+.

2. Executar um circuito quântico simulado em Qiskit. Para o estado GHZ, espera-se superposição igualitária entre $|000\rangle$ e $|111\rangle$; para o circuito de 4 qubits, espera-se distribuição aproximadamente uniforme entre oito estados; e, para o algoritmo de Grover, espera-se a amplificação da probabilidade do estado $|11\rangle$.

3. Após a execução do circuito, gerar outro par de chaves e assinar outra mensagem. Verificar ambas as assinaturas para detectar qualquer falha.

4. Registrar as distribuições de probabilidade dos estados medidos em cada circuito e os tempos de geração/assinatura antes e depois da execução quântica.

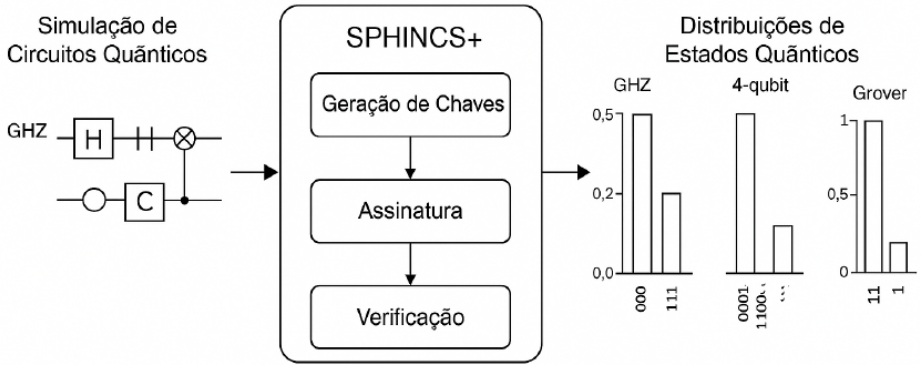



Figura 1: Visão geral do experimento: simulação de circuitos quânticos combinada à geração e verificação de assinaturas SPHINCS+. À esquerda, um circuito GHZ; ao centro, o núcleo do SPHINCS+ (geração de chaves, assinatura e verificação); e à direita, as distribuições de estados para os circuitos GHZ, 4 qubits emaranhados e Grover.

Fonte: Autores (2025)

Todo o código fonte utilizado nos experimentos — incluindo os programas em C para gerar e verificar assinaturas SPHINCS+ e os scripts em Python com Qiskit e está publicamente disponível em um repositório GitHub: `https://github.com/brunoleomenezes/quantum_sphincs_api_demo`. Essa publicação elimina a necessidade de anexar o código no texto e facilita a reprodução dos experimentos.

Para controlar a legibilidade, os nomes de variáveis e funções são escritos em itálico ou modo matemático: o tamanho da saída da função hash é denotado por $n$, o parâmetro Winternitz por $w$, o número de camadas por $d$, a função de hash por $H : \{0,1\}^* \to \{0,1\}^n$ e a derivação de chaves por $\mathrm{KDF}(\mathrm{seed}, i)$. As chaves secretas e públicas são referidas como $sk$ e pk, respectivamente, e a assinatura completa é $\sigma = (\sigma_{\mathrm{FORS}}, \sigma_{\mathrm{XMSS}})$.

**DOI:** 10.59254/sbpo-2025-212673
https://proceedings.science/p/212673?lang=pt-br

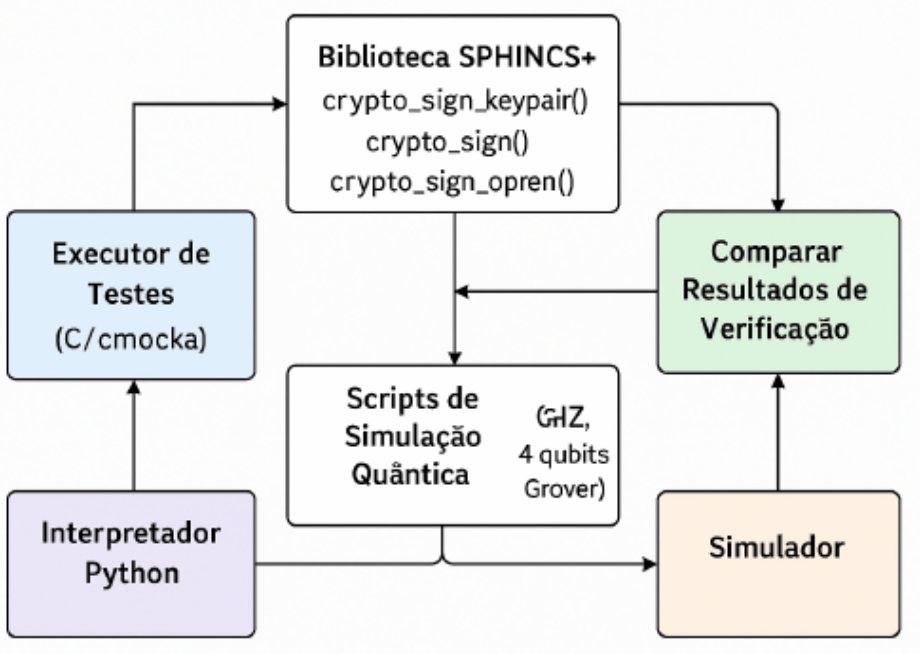



Figura 2: Fluxo de alto nível das interações entre a biblioteca SPHINCS+ (funções `crypto_sign_keypair()`, `crypto_sign()` e `crypto_sign_open()`), o interpretador Python, os scripts de simulação quântica e o executor de testes.

Fonte: Autores (2025)

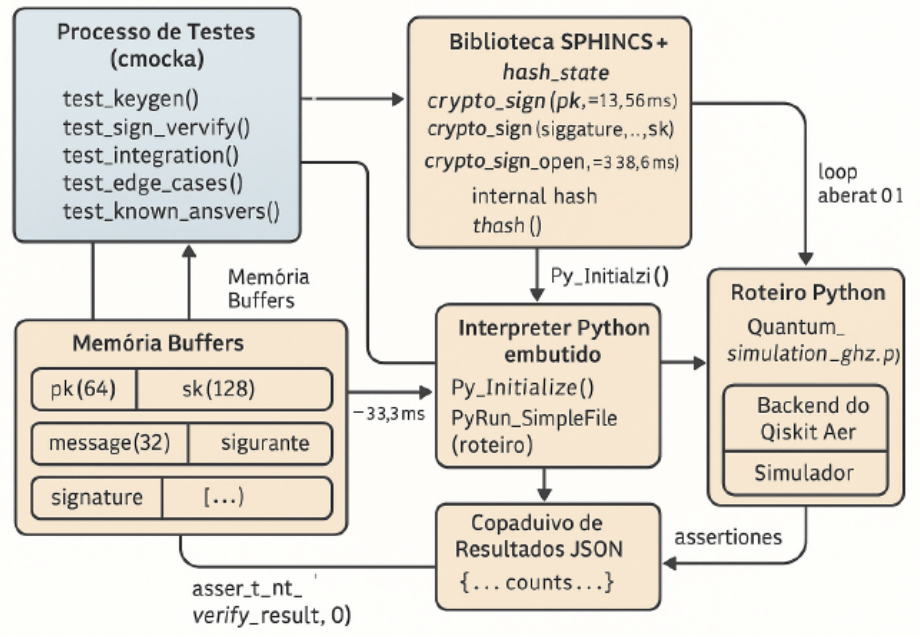



Figura 3: Fluxo de baixo nível detalhando o processo de testes via `cmocka`, os buffers de memória utilizados pelo SPHINCS+, o interpretador Python embutido e a interação com o simulador Qiskit.

Fonte: Autores (2025)

**DOI:** 10.59254/sbpo-2025-212673
https://proceedings.science/p/212673?lang=pt-br

## 4. Implementação e resultados

A geração de estados GHZ em Qiskit produziu distribuições próximas a 50 % para $|000\rangle$ e 50 % para $|111\rangle$, confirmando o emaranhamento esperado. No circuito com quatro qubits, foram observados oito estados com frequências próximas a 1/8 cada (por exemplo: `0001` : 122, `1000` : 134, `1100` : 151 etc.), conforme mostra a Tabela 1. Essa distribuição uniforme é compatível com a superposição criada pelas portas Hadamard, CNOT, SWAP e X. No algoritmo de Grover, após uma iteração, todas as medições retornaram o estado $|11\rangle$, mostrando a eficácia da amplificação quântica.

Tabela 1: Resultados consolidados dos circuitos quânticos. Cada linha descreve o circuito, o número de qubits, os resultados (estados e contagens) e um comentário sobre a aderência ao esperado. As colunas de texto usam larguras fixas para evitar que a tabela ultrapasse a margem.

| **Circuito** | **Qubits** | **Resultados** | **Comentários** |
|---|---|---|---|
| GHZ | 3 | Estado alvo: $\|000\rangle$ e $\|111\rangle$; contagens: $\|000\rangle$: 503, $\|111\rangle$: 521 | Emaranhamento evidenciado com superposição quase uniforme entre os estados $\|000\rangle$ e $\|111\rangle$. |
| 4 qubits emaranhados | 4 | Estados e contagens: 0001: 122, 1000: 134, 1100: 151, 1010: 126, 1110: 123, 0101: 122, 0011: 129, 0111: 117 | Superposição aproximadamente uniforme entre oito estados; a ausência de viés indica que o circuito de emaranhamento múltiplo está correto. |
| Grover | 2 | Estado alvo: $\|11\rangle$; contagem: 1024 | Após uma iteração, a amplificação quântica concentra quase 100 % da probabilidade em $\|11\rangle$, conforme esperado no algoritmo de Grover. |
| Teste de robustez | – | Todas as assinaturas permaneceram válidas antes e depois das simulações | A geração e a verificação de assinaturas do SPHINCS+ não foram afetadas pela co-execução com circuitos quânticos simulados, indicando robustez no ambiente testado. |

Fonte: Autores (2025)

Em todos os casos, a geração de chaves e assinaturas ocorreu com sucesso antes e depois da execução dos circuitos. Os tempos de processamento variaram em torno de poucos milissegundos e não apresentaram diferenças significativas entre as execuções. Assim, conclui-se que a integridade das assinaturas SPHINCS+ não é afetada pela co-execução com circuitos quânticos simulados no ambiente estudado.

## 5. Conclusões e trabalhos futuros

Este artigo avaliou experimentalmente a robustez do esquema de assinaturas SPHINCS+ quando submetido à execução simultânea de circuitos quânticos simulados. Por meio da integração de código C e Python, foram compiladas rotinas de geração e verificação de assinaturas e, paralelamente, executados circuitos GHZ, de emaranhamento com quatro qubits e uma instância do algoritmo de Grover. As medições obtidas nos circuitos quânticos corresponderam ao comportamento teórico esperado; por exemplo, o circuito GHZ produziu aproximadamente 50 % de $|000\rangle$ e 50 % de $|111\rangle$, enquanto o algoritmo de Grover convergiu para $|11\rangle$ em todas as execuções. Em nenhum dos cenários houve comprometimento da integridade das assinaturas ou falhas na verificação, reforçando a robustez do SPHINCS+ no ambiente simulado.

**DOI:** 10.59254/sbpo-2025-212673
https://proceedings.science/p/212673?lang=pt-br

Como trabalhos futuros, pretende-se explorar ataques quânticos reais, como busca de colisões em funções de hash e exploração de canais laterais, além de analisar o desempenho do SPHINCS+ em hardware quântico emergente. Outra linha de pesquisa envolve avaliar variantes do SPHINCS+ com diferentes parâmetros ($n$, $w$, $d$) e comparar seu desempenho com outros candidatos da NIST. A disponibilização do código em repositório público visa facilitar a reprodução dos experimentos e fomentar colaborações futuras.

**Agradecimentos**

Os autores agradecem à Fundação de Apoio à Escola Técnica do Estado do Rio de Janeiro (FAETEC RJ) e a unidade FAETEC Resende pelo apoio institucional e pela infraestrutura disponibilizada durante o desenvolvimento desta pesquisa. Agradecem também à Universidade Federal do Rio de Janeiro (UFRJ) pelo suporte acadêmico e científico que possibilitou a realização deste trabalho.

**Referências**

Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., e Daniel, S. J. (2022). Post quantum cryptography: techniques, challenges, standardization, and directions for future research. *arXiv preprint*, arXiv:2202.02826. URL https://arxiv.org/abs/2202.02826.

Bernstein, D. J. e other authors (2015). Sphincs: practical stateless hash-based signatures. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, p. 368–397, Berlin, Heidelberg. Springer. URL https://link.springer.com/chapter/10.1007/978-3-662-46800-5_15.

Bernstein, D. J. e other authors (2019). The sphincs+ signature framework. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, p. 2129–2146. ACM. URL https://dl.acm.org/doi/10.1145/3319535.3363229.

Khurram, R. e Hussain, K. (2024). Ai-driven data centers: Leveraging quantum algorithms for optimizing renewable energy integration and enhancing cyber security. ResearchGate preprint. URL https://www.researchgate.net/publication/387502248.

Krishan, K. (2024). Implementation of quantum-safe vpn. URL https://is.muni.cz/th/f2ag6/Implementation_of_QS_VPN_Archive.pdf.

Menezes, B. L. S., Marquezino, F. d. L., e Farias, C. M. d. (2024). Uma simulação de ataque quântico ao sphincs+. In *Simpósio de Excelência em Gestão e Tecnologia 2024 (SEGeT 2024)*, Resende, RJ, Brasil. URL https://www.aedb.br/seget/arquivos/artigos24/10335113.pdf. Anais, 2024.

Singh, H. (2019). Code based cryptography: Classic mceliece. *arXiv preprint*, arXiv:1907.12754. URL https://arxiv.org/abs/1907.12754.

**DOI:** 10.59254/sbpo-2025-212673
https://proceedings.science/p/212673?lang=pt-br