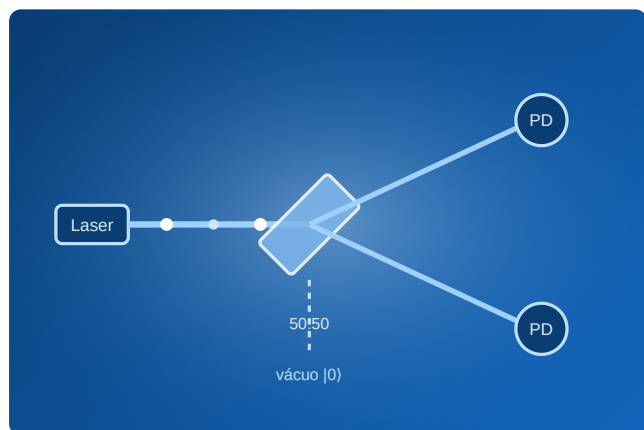


Redefinindo a Aleatoriedade

KUAPOÃ

Gerador de Números Aleatórios Quântico — a fonte de entropia verdadeira para criptografia, comunicação segura, distribuição de chaves quânticas e simulação científica.

A DOBSLIT apresenta o **KUAPOÃ**, um gerador de números aleatórios quântico (QRNG) que extrai entropia verdadeira diretamente das flutuações quânticas do vácuo óptico. Diferente dos geradores pseudoaleatórios (PRNG) e dos geradores clássicos (TRNG), o KUAPOÃ baseia-se em um processo físico fundamentalmente imprevisível, entregando aleatoriedade de alta qualidade a uma taxa de **25 Mbps** através de uma plataforma compacta e pronta para integração.



Detecção homódina das flutuações do vácuo — o coração do KUAPOÃ.

- ✓ Intrínseca e comprovadamente aleatório
- ✓ Fonte de entropia robusta e controlada
- ✓ Alta taxa: 25 Mbps de aleatoriedade quântica
- ✓ Pronto para integração via Ethernet, USB e serial

APLICAÇÕES



Geração de chaves criptográficas

AES, RSA, ECC, TLS, IPSEC, SSH



Distribuição de chaves quânticas (QKD)

Infraestrutura quantum-safe



Infraestrutura crítica e data centers

Entropia sob demanda em larga escala



Segurança de transporte e comunicação

Redes e enlaces protegidos



Simulações estatísticas (Monte Carlo)

Pesquisa científica e financeira



Blockchain e transações financeiras

Nonces e tokens imprevisíveis

Aleatoriedade verdadeira, imprevisível e à prova do futuro

Diferente de fontes de entropia determinísticas ou não comprovadamente seguras, os geradores quânticos são intrinsecamente aleatórios e baseiam-se em processos físicos bem compreendidos. O KUAPOÃ é uma fonte robusta de entropia de alta qualidade.

POR QUE GERAÇÃO QUÂNTICA?

A segurança de qualquer sistema criptográfico moderno depende da qualidade das chaves geradas. Pelo princípio de Kerckhoff, o sistema deve permanecer seguro mesmo que tudo seja conhecido — exceto a chave. Toda essa fundação ruir se os números usados para criar a chave não forem únicos ou forem previsíveis.

Muitas chaves ainda são criadas por geradores pseudoaleatórios (PRNG): programas determinísticos que partem de uma semente. Em data centers e dispositivos isolados, as fontes de entropia disponíveis são limitadas, e os números resultantes não são verdadeiramente imprevisíveis.

Geradores físicos clássicos (TRNG), como circuitos auto-oscilantes, comportam-se como caixas-pretas: o processo físico ocorre de forma caótica e não controlada, sendo impossível garantir que um atacante não o influencie. A única forma de produzir aleatoriedade verdadeira é compreender e validar o processo físico que a origina.

Os QRNGs apoiam-se na física quântica, probabilística em nível fundamental. Como a fonte de entropia é descrita por modelos bem conhecidos, suas propriedades são compreendidas e a segurança pode ser comprovada — desde o primeiro bit.

TECNOLOGIA CENTRAL

O KUAPOÃ explora o princípio de **detecção homódina das flutuações do vácuo**. Um laser DFB de baixa potência é dividido em um acoplador óptico 50:50; uma das portas recebe o estado de vácuo quântico. As flutuações de fase/quadratura do vácuo — fundamentalmente imprevisíveis — são medidas por dois fotodetectores em configuração balanceada.

A diferença entre os fotodetectores é amplificada e digitalizada por um ADC. O sinal bruto passa então por **extração de Toeplitz**, que destila a entropia de origem quântica em uma sequência de bits uniforme e imparcial, processada no SoC/FPGA Xilinx Zynq 7010.

O uso de componentes acoplados em fibra, com baixas perdas, garante grande aproveitamento da potência óptica e baixo consumo de energia — apenas 11 W para uma taxa contínua de 25 Mbps.

Entropia de origem física

O ruído quântico do vácuo não pode ser previsto, reproduzido ou influenciado por um atacante — mesmo com poder computacional ilimitado.

PROTEGENDO UM MUNDO CONECTADO

Em IoT, dispositivos inteligentes, comunicação e infraestrutura crítica, os sistemas estão cada vez mais conectados — e as ameaças, mais fortes. Uma rede é tão segura quanto seu elo mais fraco: uma única falha pode comprometer todo o conjunto. Garantir entropia de alta qualidade na origem é, portanto, uma questão de segurança e de confiança pública. O KUAPOÃ entrega essa entropia de forma transparente, auditável e em alto volume.

Confiável para segurança da informação

O KUAPOÃ é uma fonte de entropia verdadeira que sustenta segurança da informação no presente e no futuro pós-quântico.

SEGURANÇA DA INFORMAÇÃO

Apenas sistemas criptográficos que utilizam uma fonte robusta e imprevisível de entropia, produzindo números verdadeiramente aleatórios, podem alcançar segurança teórica da informação.

Tanto PRNGs baseados em algoritmos quanto TRNGs clássicos são vulneráveis. Os PRNGs, por serem determinísticos, são previsíveis em seu núcleo. Nos TRNGs clássicos, nunca se sabe com certeza quanta aleatoriedade verdadeira foi produzida — a resiliência depende fortemente do pós-processamento e de testes estatísticos práticos.

Os princípios sobre os quais o KUAPOÃ gera aleatoriedade são fundamentalmente compreendidos, podendo ser modelados, controlados e otimizados. Além de sequências com excelentes propriedades estatísticas, oferecem aleatoriedade verdadeira em seu sentido mais formal e seguro.

VALIDAÇÃO E DESEMPENHO

O KUAPOÃ é avaliado segundo a metodologia **NIST SP 800-90B**, padrão internacional para validação de fontes de entropia. Os resultados abaixo foram obtidos em avaliação interna da DOBSLIT:

7,139 bits/byte

Min-entropia conservadora (não-IID)

valor de referência para divulgação técnica

Estimador NIST SP 800-90B	Entropia
IID	7,938 bits/byte
Não-IID — MCV bitstring	0,996 bits/bit
Não-IID — Markov bitstring	0,997 bits/bit
Não-IID — Collision bitstring	0,964 bits/bit
Não-IID — Compression bitstring	0,913 bits/bit
Não-IID — Final conservador	7,139 bits/byte

Números obtidos em avaliação interna. Especificações sujeitas a alteração sem aviso prévio.

POR QUE O KUAPOÃ?

Fonte quântica de entropia verdadeira

Detecção homódina das flutuações do vácuo

Aleatoriedade desde o primeiro bit

Sem necessidade de "aquecimento" estatístico

Avaliado por NIST SP 800-90B

Min-entropia não-IID de 7,139 bits/byte

Integração simples

Ethernet Gigabit, USB e serial

Alta taxa de geração

25 Mbps contínuos

À prova do futuro — quantum-safe

Compatível com algoritmos clássicos e PQC

Baixo consumo

Apenas 11 W em operação contínua

Plataforma SoC/FPGA dedicada

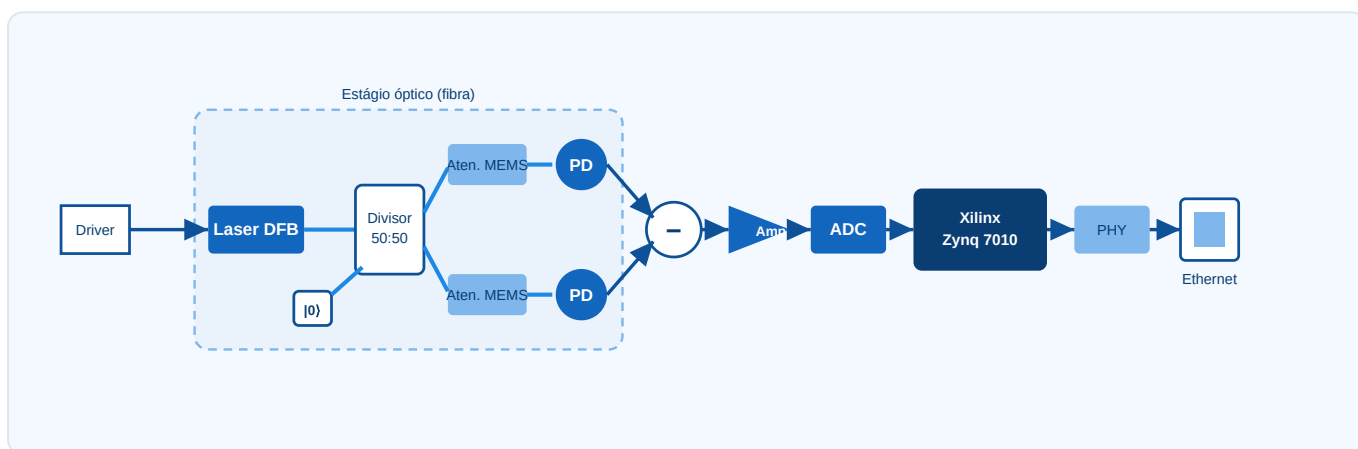
Xilinx Zynq 7010, 512 MB RAM, 32 GB

Arquitetura óptica-eletrônica integrada

Da fonte óptica à interface de rede, todo o caminho do sinal foi projetado para máxima eficiência, baixo consumo e entropia auditável.

DIAGRAMA DE BLOCOS

O laser DFB é dividido por um acoplador 50:50; a porta livre recebe o estado de vácuo. Atenuadores MEMS ajustam a potência sobre dois fotodetectores balanceados. A diferença é amplificada, digitalizada (ADC) e processada no SoC/FPGA Xilinx Zynq 7010, que aplica a extração de Toeplitz e disponibiliza os bits pela interface PHY/Ethernet.



DESTAQUES DE ENGENHARIA

Deteção balanceada

Cancelamento de ruído clássico de modo comum, isolando o sinal quântico

Extração de Toeplitz no FPGA

Pós-processamento determinístico de alta vazão, sem gargalos

Componentes acoplados em fibra

Baixas perdas ópticas e estabilidade mecânica

25 Mbps

Taxa de geração contínua de números aleatórios de origem quântica.

11 W · plug-and-play

Operação em 5 V / ± 10 V, com saída por Ethernet Gigabit, USB e serial — pronto para data centers e laboratórios.

KUAPOÃ EM RESUMO

NÚCLEO QRNG	
Princípio físico	Detecção homódina das flutuações do vácuo
Extração de entropia	Extração de Toeplitz
Fonte óptica	Laser de baixa potência, tipo DFB
Taxa de geração	25 Mbps
Validação de entropia	NIST SP 800-90B — min-entropia 7,139 bits/byte (avaliação interna)
PLATAFORMA DE PROCESSAMENTO	
SoC / FPGA	Xilinx Zynq 7010
Memória RAM	512 MB
Armazenamento	32 GB
CARACTERÍSTICAS ELÉTRICAS	
Tensão de operação	5 V, 2 A · ±10 V, 100 mA
Consumo	11 W
INTERFACES E FORMATO	
Interfaces	Ethernet 10/100/1000 Mbps, USB, serial
Dimensões	Compactas
DESEMPENHO NIST SP 800-90B (AVALIAÇÃO INTERNA)	
Min-entropia conservadora (não-IID)	7,139 bits/byte
Entropia IID	7,938 bits/byte
Não-IID — MCV bitstring	0,996 bits/bit
Não-IID — Markov bitstring	0,997 bits/bit
Não-IID — Collision bitstring	0,964 bits/bit
Não-IID — Compression bitstring	0,913 bits/bit

As informações e especificações deste documento estão sujeitas a alteração a qualquer momento pela DOBSLIT, sem aviso prévio. Resultados de entropia obtidos em avaliação interna.