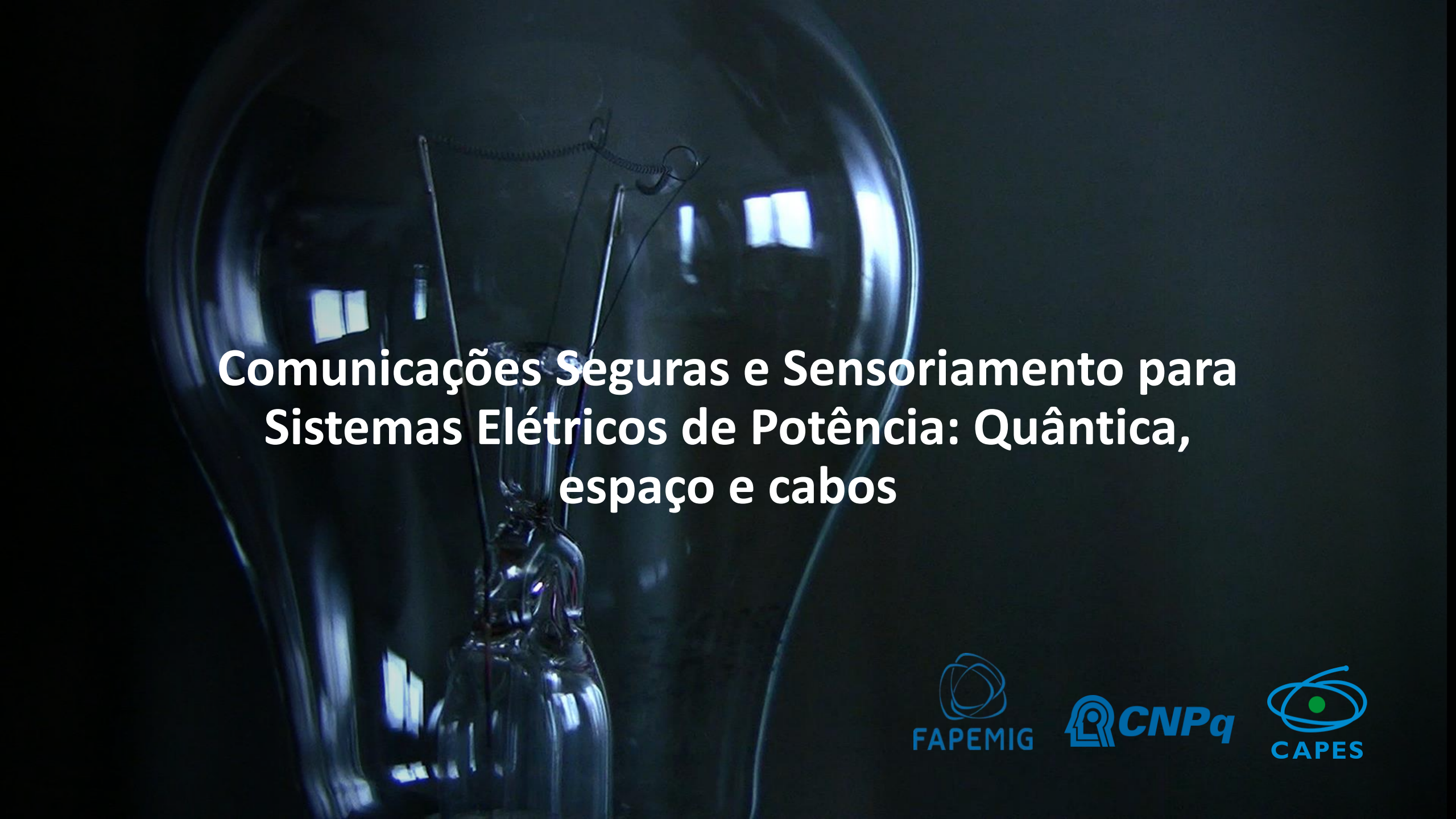


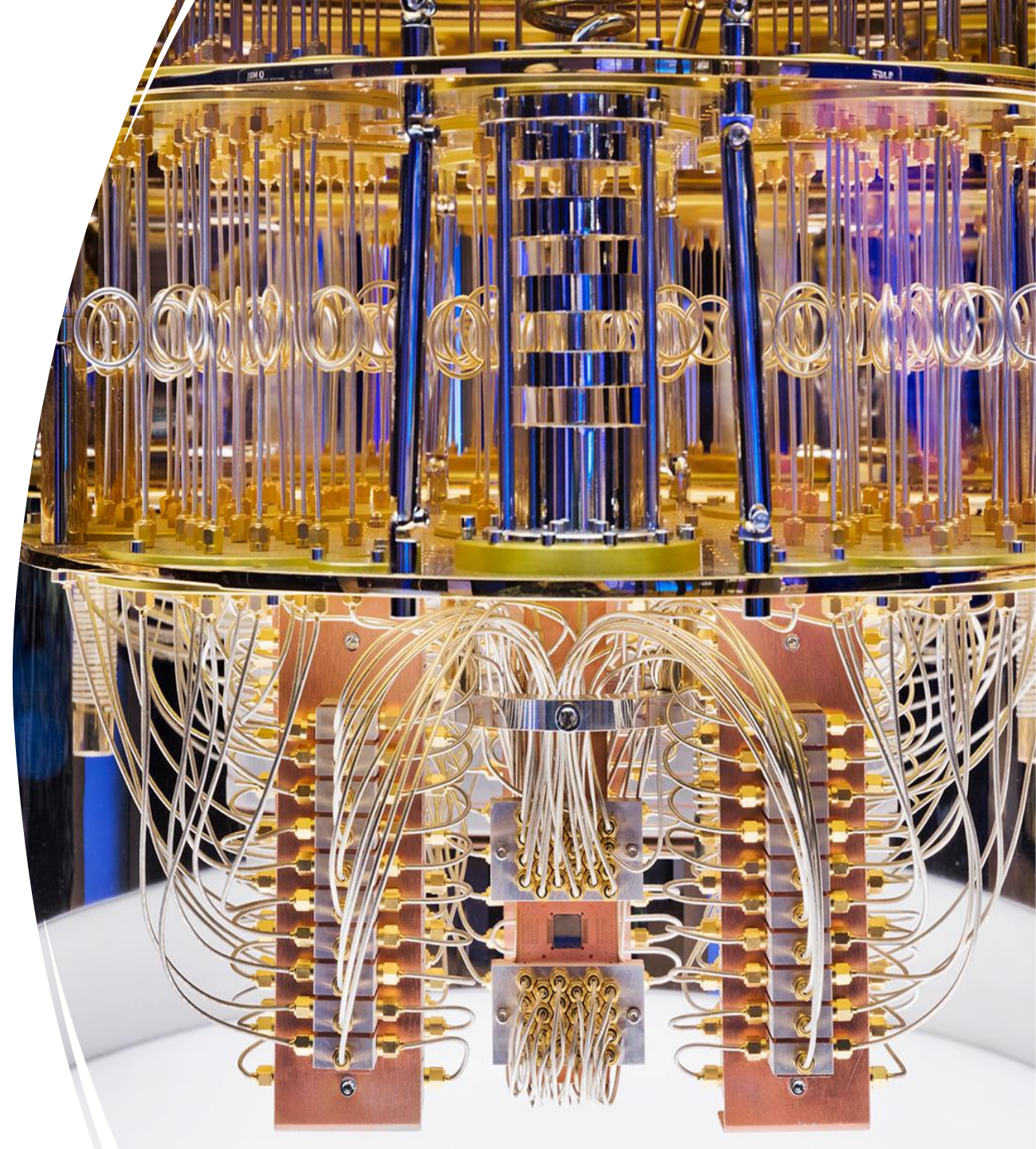


Comunicações Seguras e Sensoriamento para Sistemas Elétricos de Potência: Quântica, espaço e cabos



Criptografia Pós-Quântica

- **Criptografia pós-quântica** (PQC - *Post-Quantum Cryptography*) refere-se a um conjunto de algoritmos criptográficos projetados para resistir a ataques realizados por **computadores quânticos**, que ameaçam esquemas tradicionais como RSA e ECC.



Desafios para a segurança

1. Criptografia atual em risco

- **Algoritmo de Shor:** compromete RSA, ECC e Diffie-Hellman (fatoração rápida).
- **Algoritmo de Grover:** reduz segurança de protocolos baseados em buscas.

2. Confidencialidade a longo prazo

- Dados criptografados hoje poderão ser vulneráveis no futuro.

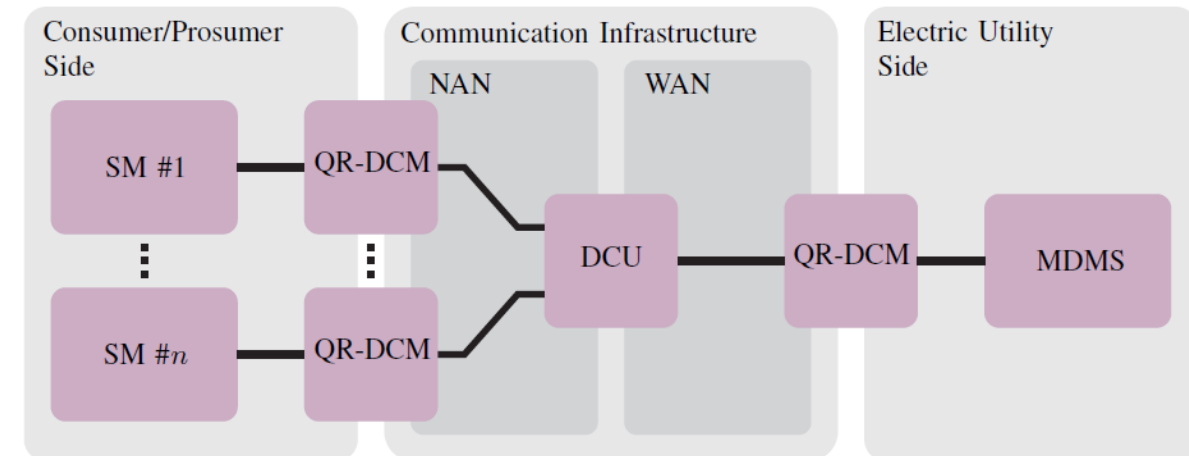
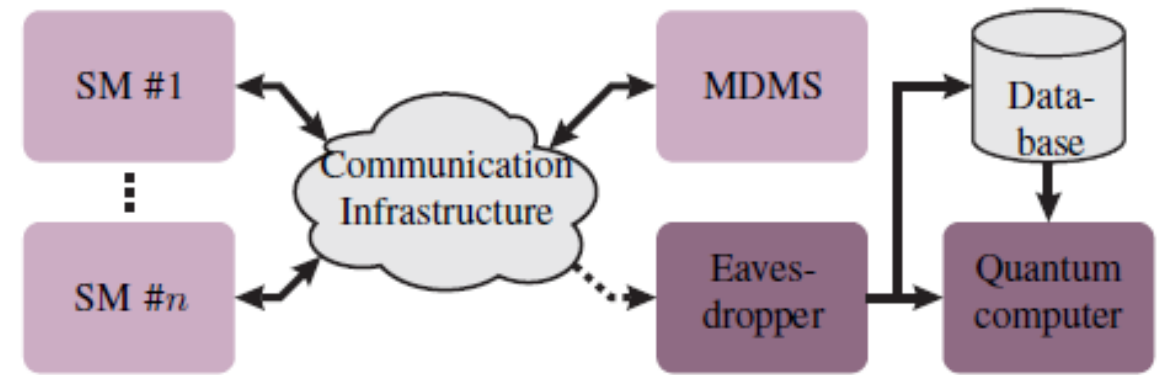
3. Infraestrutura e Integração

- Grandes desafios na adaptação de sistemas existentes para novas tecnologias criptográficas.

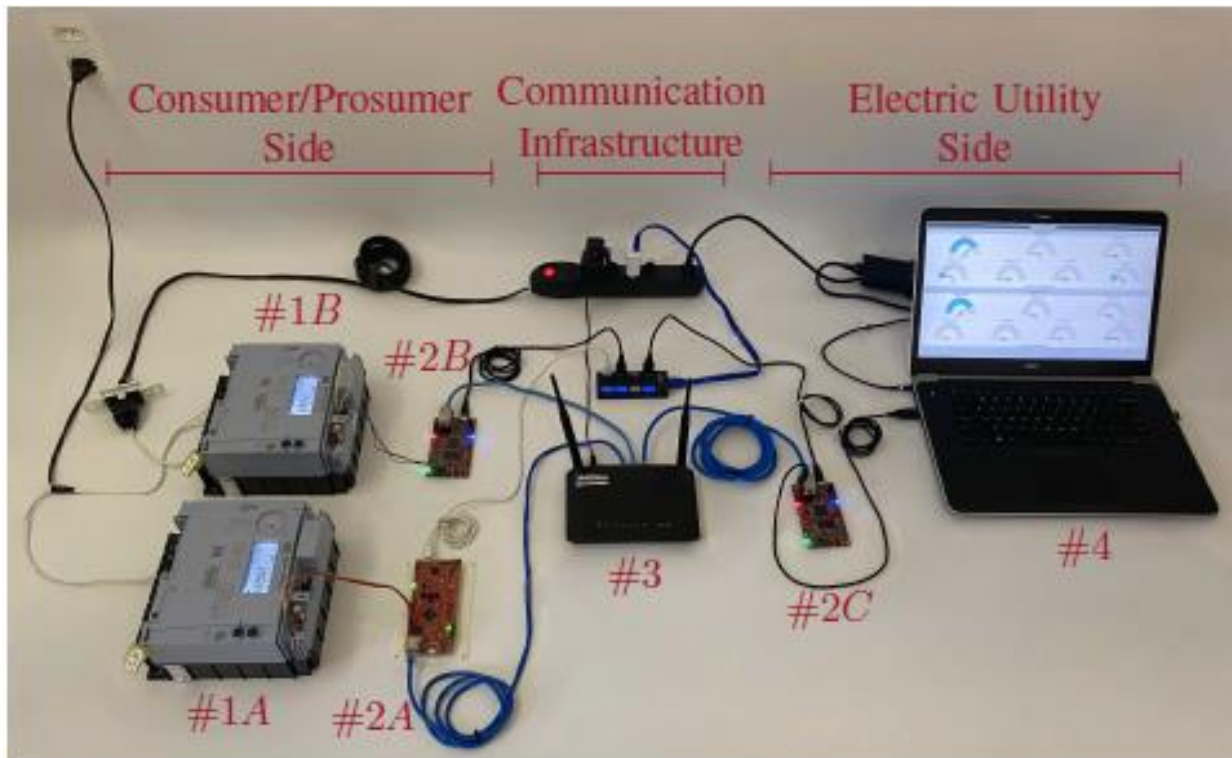


Medição inteligente resistente aos ataques quânticos

O bloco DCM passa a se chamar QR-DCM, posto que inclui esquema criptográfico pós-quântico



Exemplo de Implementação



	FrodoKEM 640/976/1344	CRYSTALS-Kyber 512/768/1024
Class	Lattice	Lattice
Mathematical Problem	LWE	M-LWE
Public Key Size (bytes)	9616/15632/21520	800/1184/1568
Private Key Size (bytes)	19888/31296/43088	1632/2400/3168
Ciphertext Size (bytes)	9720/15744/21632	768/1088/1568
Approach	Conservative	Lightweight

Scheme	Impl.	Time (ms)	Power (W)	Energy (mJ)
FrodoKEM	Impl. #1	4186.57	0.35	1454.79
	Impl. #2	1757.33	1.65	2903.11
	Impl. #3	559.72	2.05	1147.43
CRYSTALS-Kyber	Impl. #1	40.02	0.35	13.91
	Impl. #2	12.81	1.65	21.16
	Impl. #3	4.05	1.83	7.43

Comunicações satelitais em **baixa órbita** para sistemas elétricos de potência

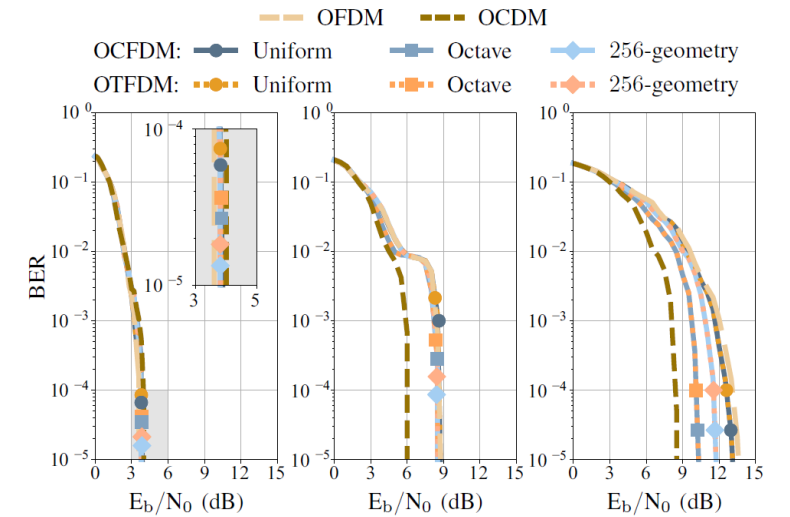
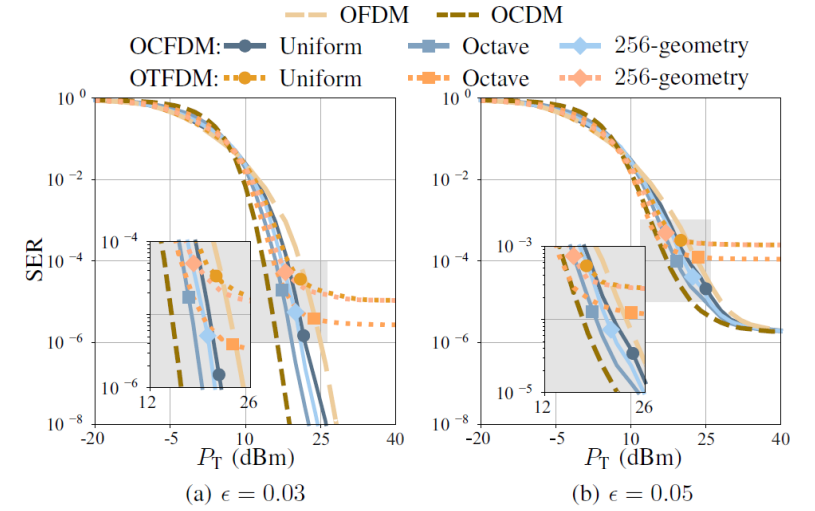
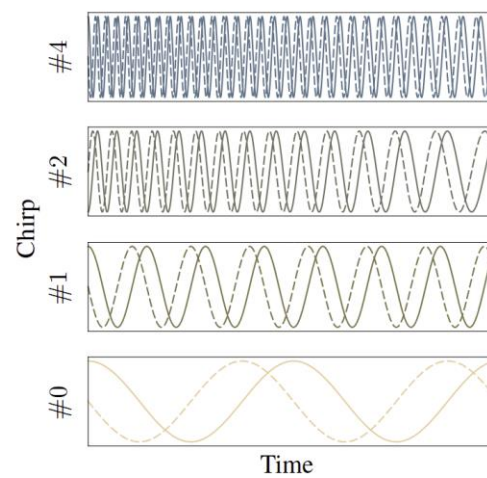
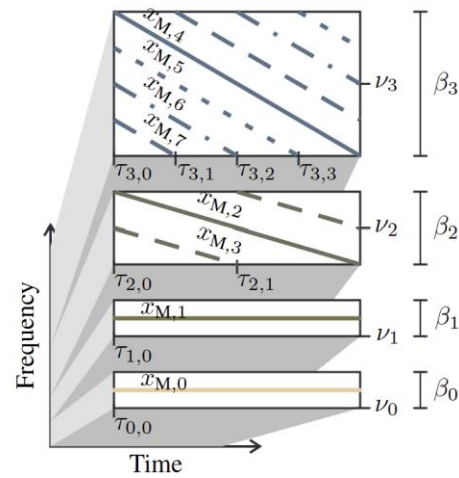
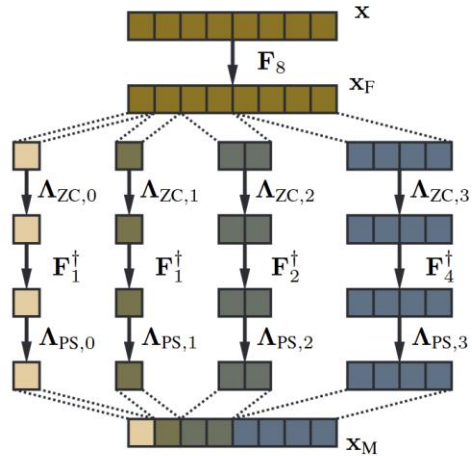
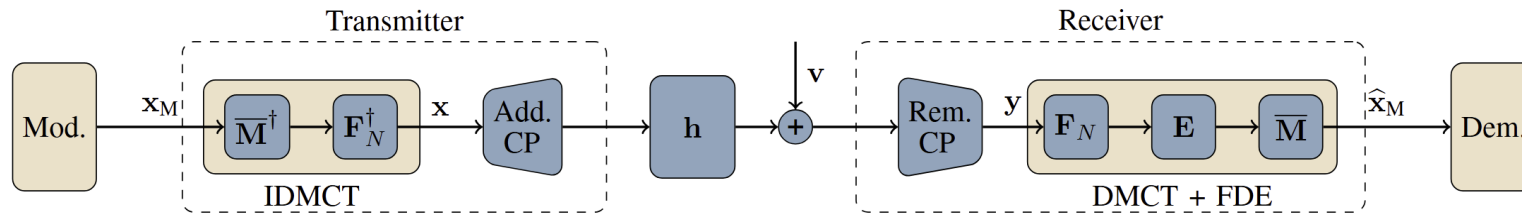


-  **Conectividade em Áreas Remotas**
Comunicação confiável onde não há infraestrutura terrestre e áreas isoladas e zonas de difícil acesso.
-  **Monitoramento em Tempo Real**
Telemetria e agilidade na detecção e resposta a falhas.
-  **Resiliência Cibernética e Operacional**
Redundância e continuidade em desastre ou sabotagem.
-  **Integração com Renováveis e Smart Grids**
Coordenação de sistemas distribuídos e suporte às REIs.
-  **Baixa Latência e Alta Disponibilidade**
LEO: ~30 ms (vs. GEO: ~600 ms). Adequado para comandos e proteção em tempo real.
-  **Escalabilidade e Cobertura Global**
Constelações com expansão rápida e menor dependência de infraestrutura física.

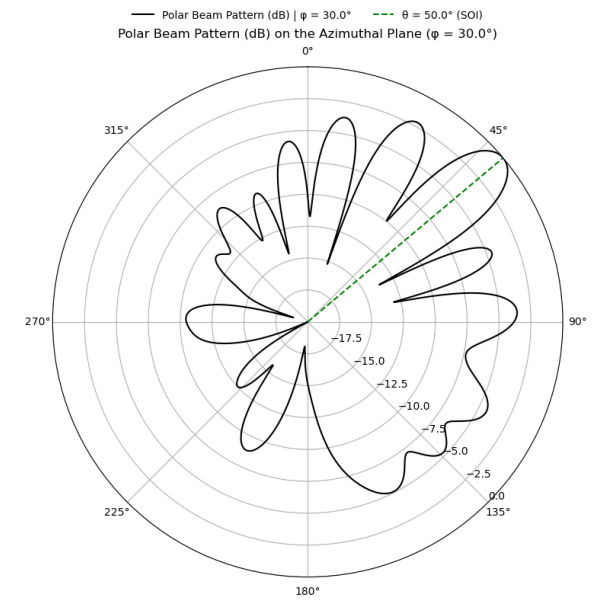
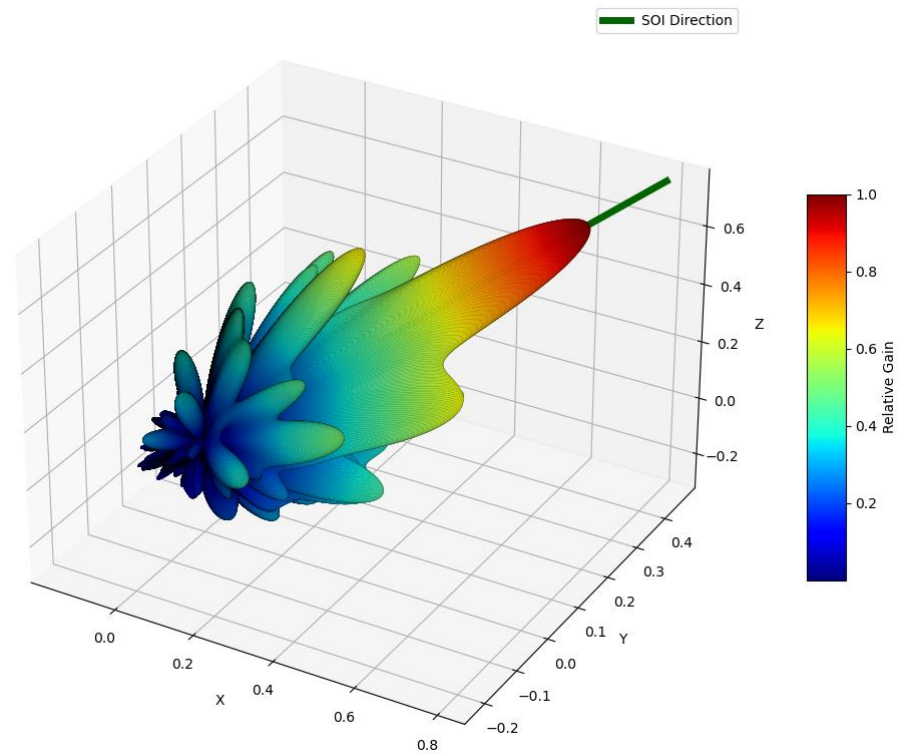
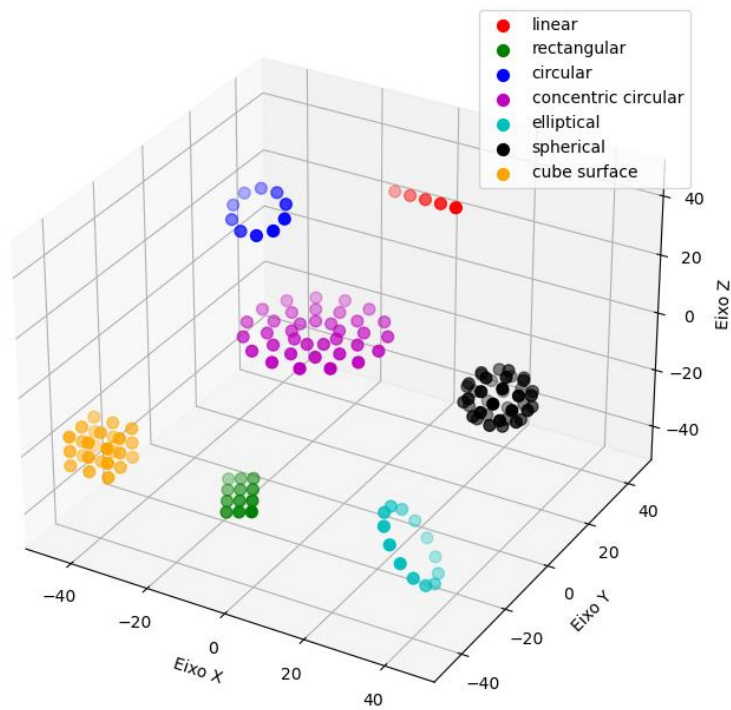
Soluções para o NewSpace: Camada Física em Comunicações por Satélite e Lançamento de Veículos Espaciais (SOLVE)

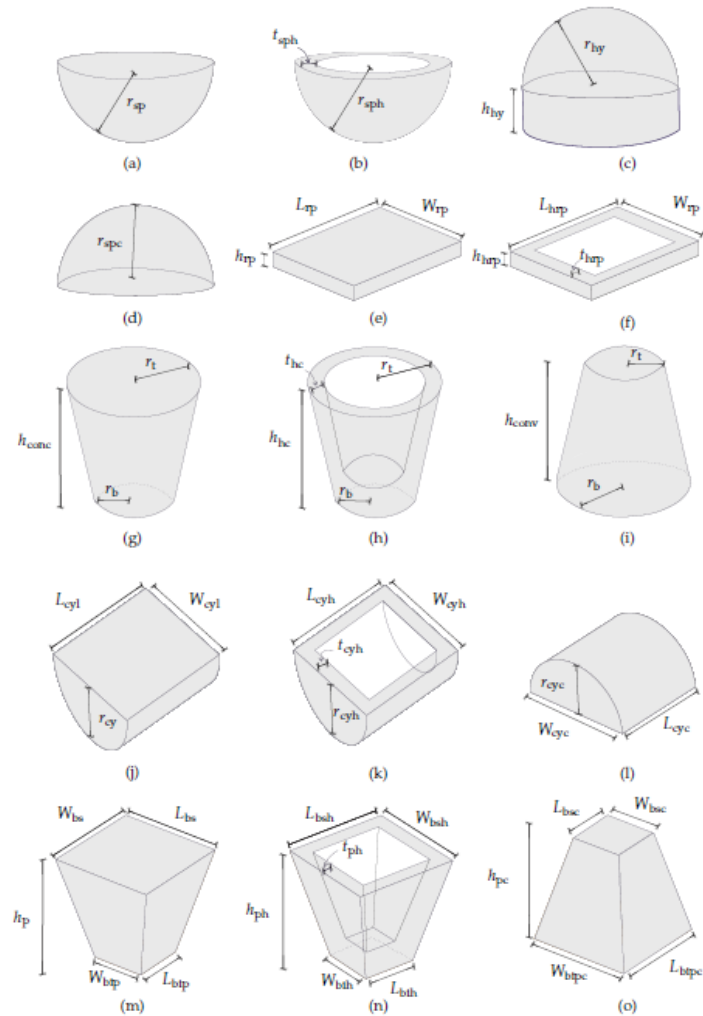
INSTITUIÇÃO: Universidade Federal de Juiz de Fora
COORDENAÇÃO: Prof. Moisés Vidal Ribeiro

Projeto de Forma de Onda



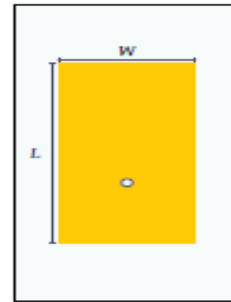
Array virtual de satélite para *beamforming* distribuído





Ressonadores para Antenas patch

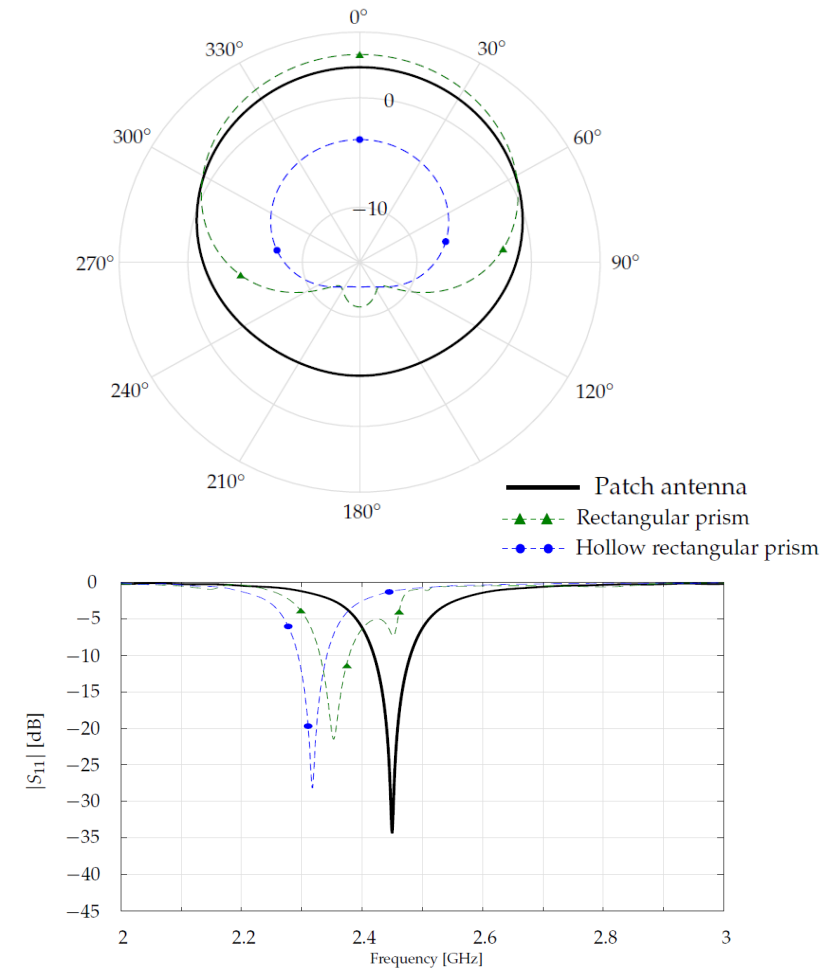
Antena Patch com um elemento



Tipos de Materiais

Material	ϵ_r	μ_r	σ (S/m)
Água Destilada	78.4	1	5.55μ
Glicerina	50	1	0
Grafite	12	1	100 k

Resultados com Glicerina



Power Line Communication

Comunicação sobre Infraestrutura Existente

Monitoramento em Tempo Real de Cabos

- Detecção de falhas, sobreaquecimento e degradação
- Sensoriamento distribuído e preciso ao longo dos condutores.

Aplicações Típicas

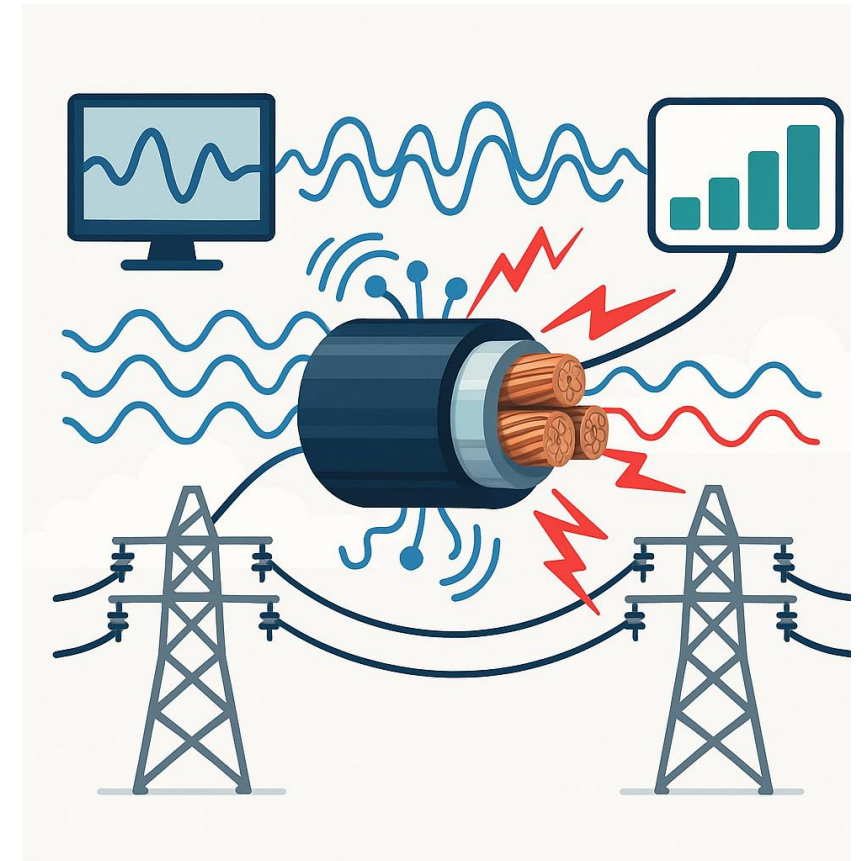
- Redes de distribuição transmissão
- Sistemas ferroviários e industriais

Vantagens Técnicas

- Custo reduzido de implantação
- Funciona em ambientes hostis (sem rádios/fibra)

Tecnologias

- Banda-estreita e banda-larga

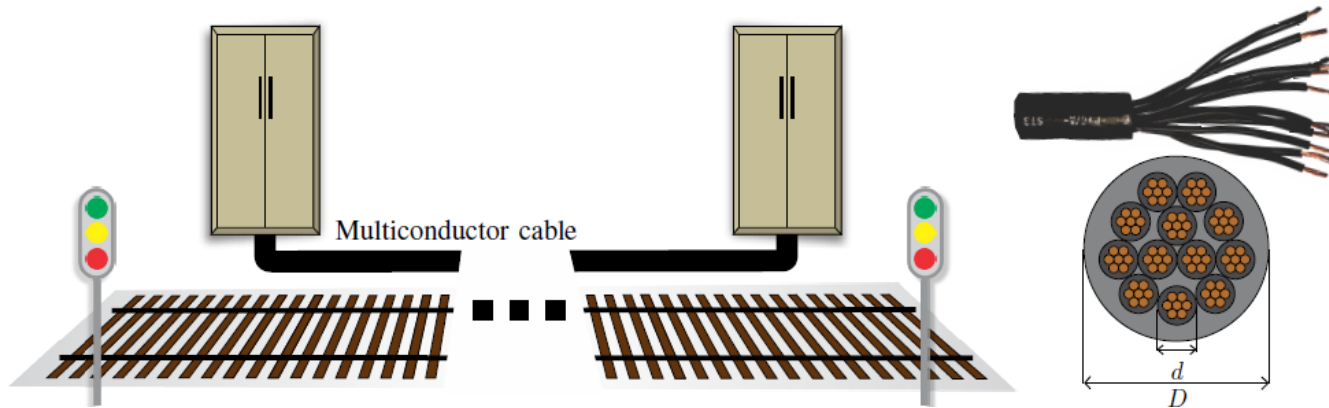


Sensoriamento de cabos de sinalização em vias ferroviárias

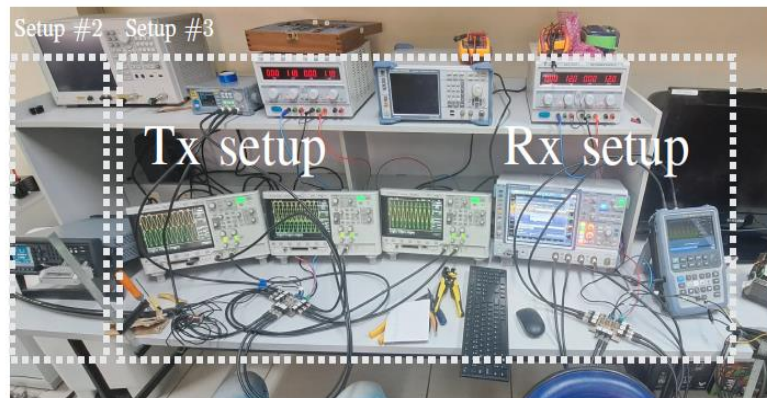
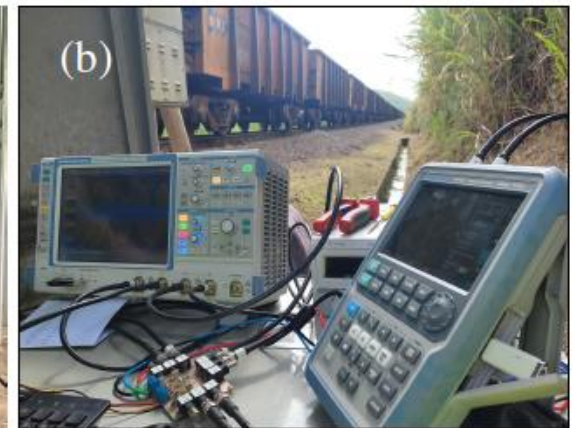
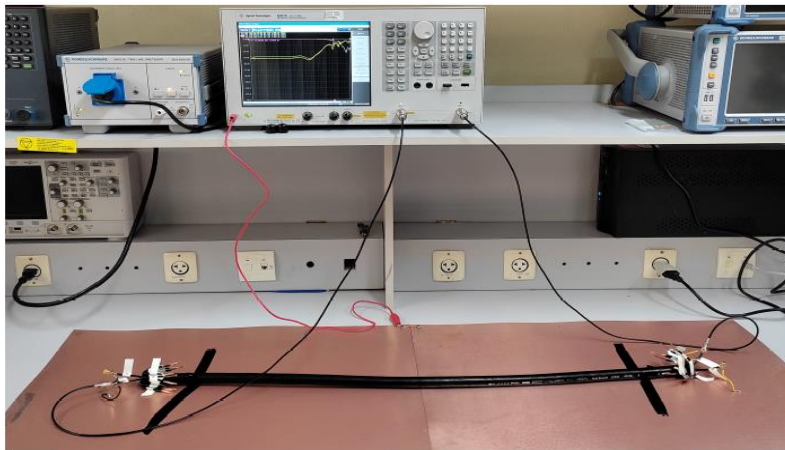
O monitoramento da degradação do cabos é realizado a cada 5 anos.

As falhas em cabos de sinalização resultam em perdas significativas para as operadoras ferroviárias.

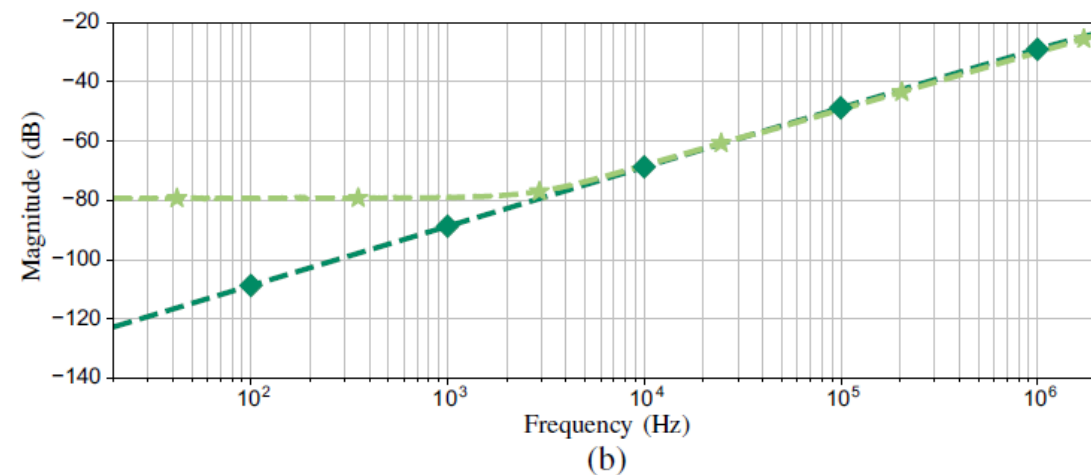
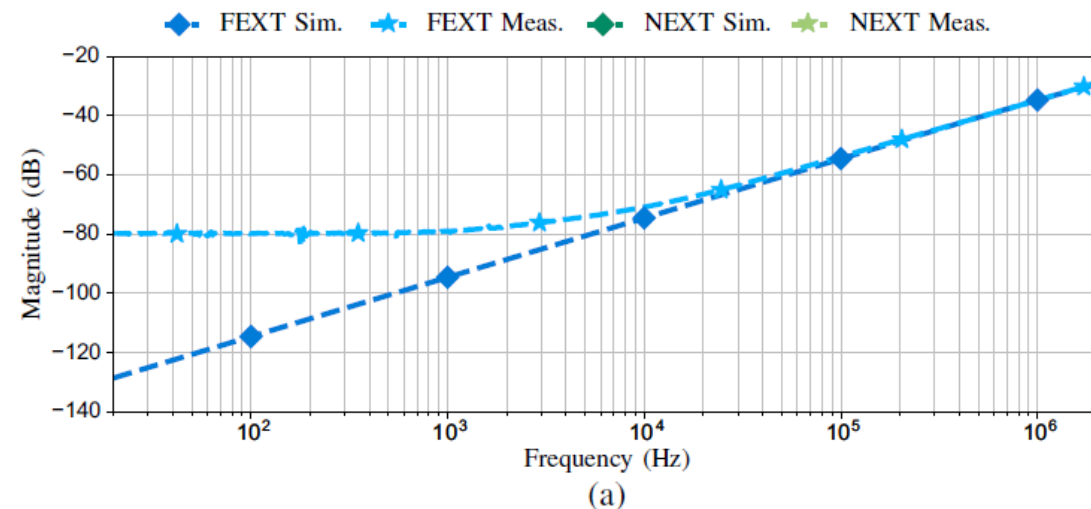
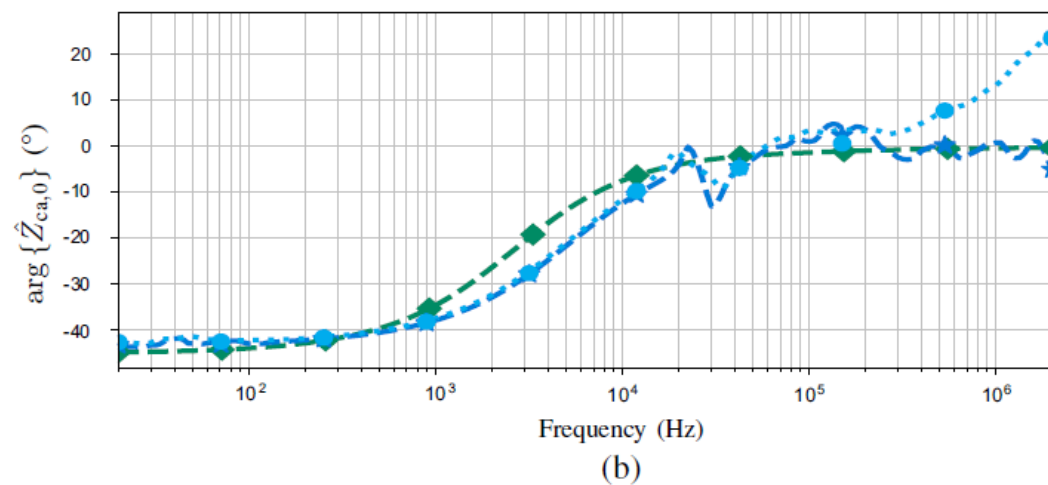
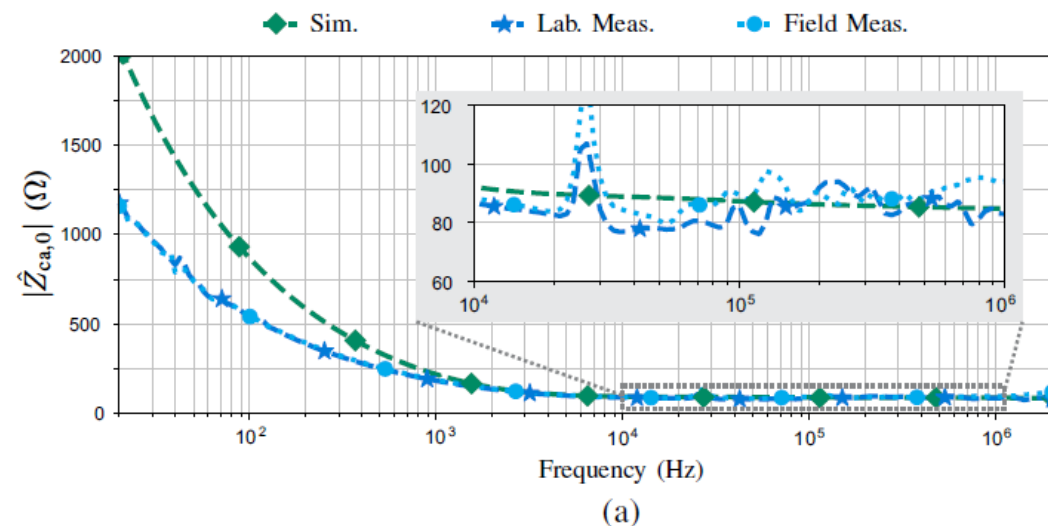
A localização das falhas não é fácil de ser realizada.



Experimentos no lab e campo

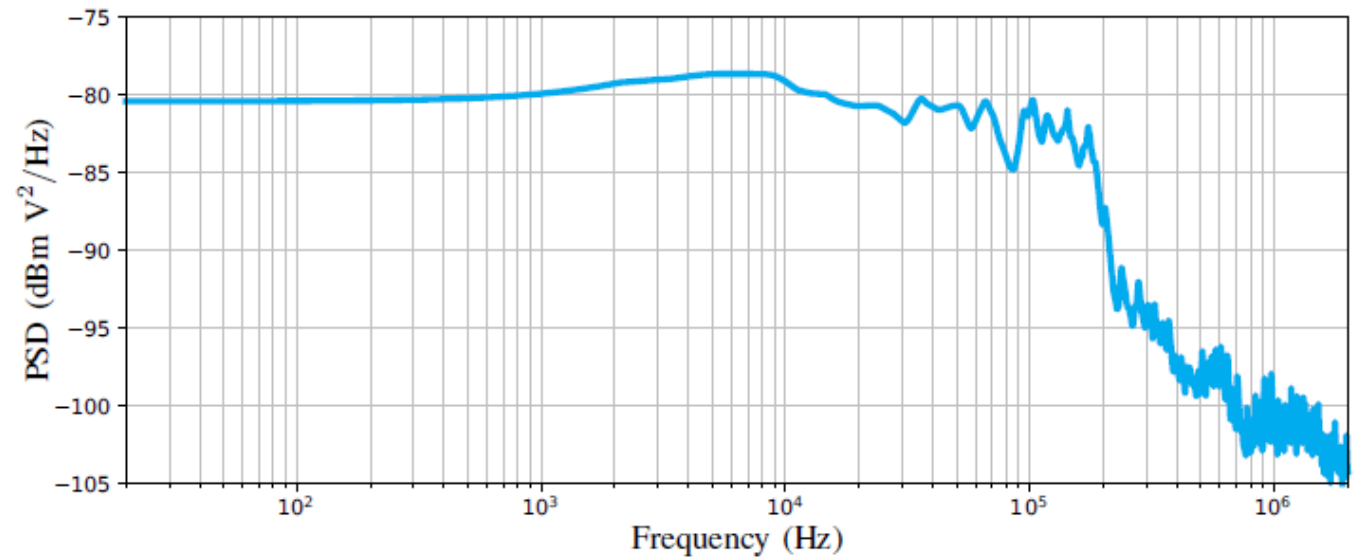
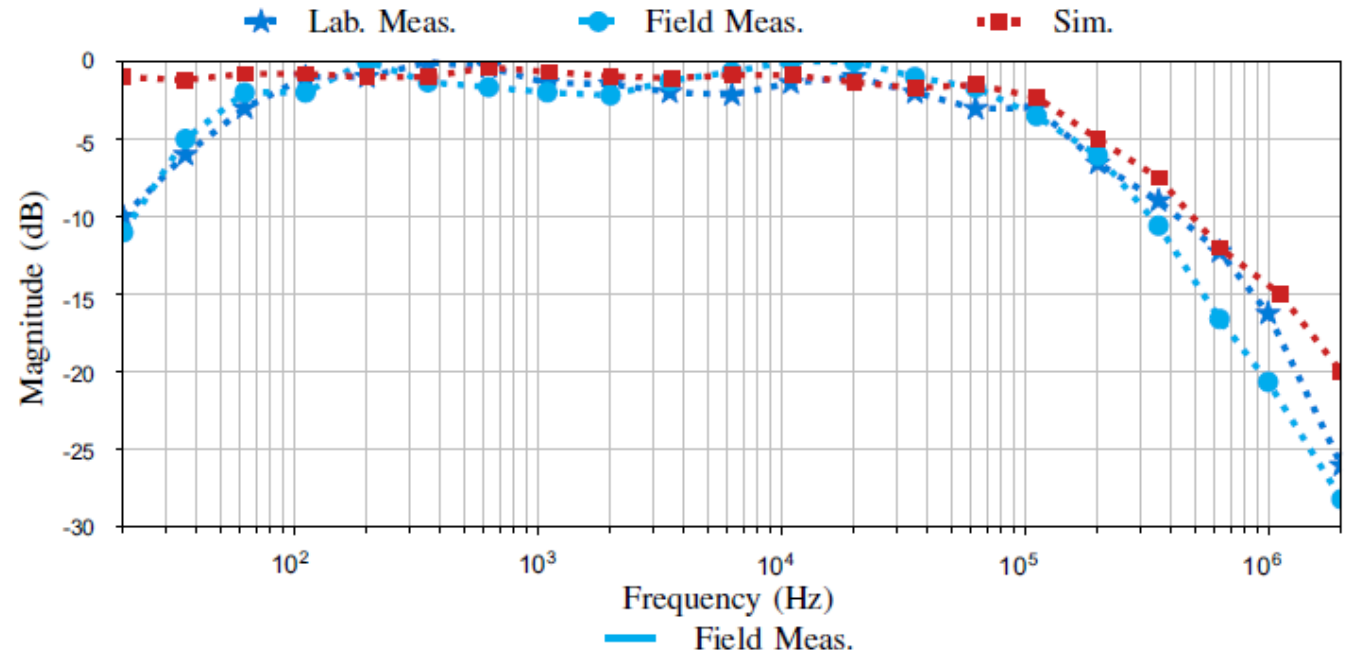


Alguns resultados experimentais



Alguns resultados experimentais

- Comparação entre as magnitudes obtidas com simulação, no laboratório e campo.
- Medição do ruído aditivo.



Conclusões

- O computador quântico é um desafio para a segurança e o setor elétrico deve se antecipar.
- As comunicações satelitais de baixa órbitas apresentam grande potencial para o setor elétrico de potência.
- Power line communication voltado para sensoramento de cabos é muito importante, principalmente, no processo de eletrificação.
- A integração entre criptografia pós-quântica, comunicações satelitais e power line communication é bastante interessante para prover comunicações seguras e sensoramento.

Obrigado

- moises.ribeiro@ufjf.br