

# Comunicação Quântica Analógica

V. F. Guedes, S. T. de Oliveira, J. P. da F. Neto, G. L. de Oliveira, J. B. R. Silva e R. V. Ramos

**Resumo** — Neste trabalho apresentamos a realização experimental de um protocolo de comunicação quântica segura direta de sinais analógicos, realizada na rede óptica instalada da cidade de Fortaleza.

**Palavras-Chave** — Comunicação quântica, óptica quântica, teorema de Whittaker-Nyquist-Shannon, redes ópticas.

**Abstract** — In this work we present the experimental realization of a quantum secure direct communication protocol of analog signals, realized in the installed optical network at Fortaleza city.

**Keywords** — Quantum communication, quantum optics, Whittaker-Nyquist-Shannon's theorem, optical networks.

## I. COMUNICAÇÃO QUÂNTICA SEGURA DIRETA DE SINAIS ANALÓGICOS

O objetivo do protocolo de comunicação quântica segura direta (QSDC) aqui proposto é permitir que os dois usuários legítimos da comunicação, Alice (transmissor) e Bob (receptor), identifiquem se mais alguém teve acesso à informação, um sinal analógico de áudio ou vídeo, por exemplo, enviada de Alice para Bob.

O esquema óptico proposto para implementar o protocolo de QSDC é mostrado na Fig. 1.

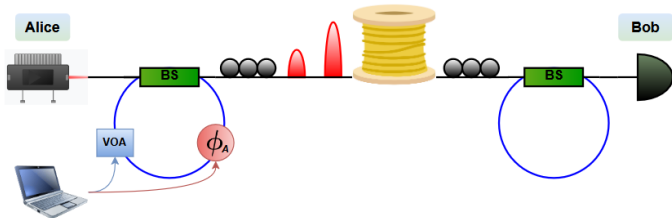


Fig. 1 – Esquema óptico para comunicação quântica segura direta de sinais analógicos. VOA – Atenuador óptico variável, BS – divisor de feixes,  $\phi_A$  – modulador de fase.

O protocolo de QSDC usando o esquema óptico da Fig. 1 funciona como descrito abaixo:

1) Alice alimenta seu modulador de fase com amostras do sinal contínuo  $s(t)$ , cuja maior componente espectral é  $f_{max}$ , ou com amostras de outro sinal contínuo  $r(t)$ , cuja maior componente espectral também é  $f_{max}$ . O sinal  $r(t)$  é um sinal isca.

2) Para cada pulso enviado por Alice, ela escolhe aleatoriamente, com igual probabilidade, se vai modular a fase do pulso fraco com uma amostra de  $s(t)$  ajustando o VOA para que o número médio de fótons do pulso fraco entrando no canal seja  $\mu_s$ , ou se vai modular a fase do pulso fraco com uma amostra de  $r(t)$  ajustando o VOA para que o número médio de fótons do pulso fraco entrando no canal seja  $\mu_r$ .

3) Bob mede os sinais enviados por Alice usando seu aparato óptico mostrado na Fig. 1.

4) Alice informa publicamente para Bob em quais slots de tempo ela escolheu  $s(t)$  (ou  $r(t)$ ). Ela também envia para Bob o sinal  $r(t)$  completo.

5) Bob compara o sinal  $r(t)$  que Alice enviou para ele com a versão de  $r(t)$  que ele construiu com as medições das amostras que Alice enviou para ele. Se Bob reconstruiu corretamente o sinal  $r(t)$ , a comunicação é abortada. Se Bob não consegue reconstruir corretamente o sinal  $s(t)$ , a comunicação também é abortada.

## II. ANÁLISE DE SEGURANÇA

A segurança do protocolo QSDC para sinais analógicos é baseada no teorema de amostragem de Whittaker–Nyquist–Shannon. Ele afirma que: se uma função  $x(t)$  não contém frequências maiores que  $B$  Hz, então  $x(t)$  pode ser completamente determinado a partir de suas amostras em uma sequência de pontos espaçadas por menos que  $1/(2B)$  segundos. Além disso, se um sinal contínuo de banda limitada  $s(t)$  é aleatoriamente amostrado com probabilidade  $p$ , então ele pode ser reconstruído a partir de suas amostras se a taxa de amostragem é maior que  $2f_{max}/p$ , sendo  $f_{max}$  a maior componente espectral de  $s(t)$ .

De uma forma breve pode-se entender a segurança da seguinte forma: Alice escolhe  $\mu_s > \mu_r$  (ou seja, Bob precisa de menos pulsos para reconstruir  $s(t)$  do que para reconstruir  $r(t)$ ) e  $T_p$  (período do trem de pulsos enviado por Alice) tal que, na ausência de espionagem, Bob consegue reconstruir  $s(t)$  mas não consegue reconstruir  $r(t)$ . Quando uma espia, Eva, implementa o ataque intercepta-reenvia, ela não sabe a priori o número médio de fótons dos pulsos enviados por Alice. Ao reenviá-los para Bob, Eva precisa escolher aleatoriamente o valor do número médio de fótons para cada pulso. Isso vai diminuir (aumentar) a média do número médio de fótons com informações de  $s(t)$  ( $r(t)$ ) que chegam em Bob, impedindo-o (habilitando-o) de reconstruir corretamente  $s(t)$  ( $r(t)$ ).

De forma semelhante, pode-se mostrar que o protocolo aqui descrito é resistente ao ataque por divisor de feixes se a transmissividade do canal for maior que 0,5, o que limita a distância entre Alice e Bob a cerca de 10 km [1].

### III. EXPERIMENTOS

Como prova de conceito, uma versão simplificada do protocolo (sem o sinal  $r(t)$ ) foi implementada. A Fig. 2 mostra a detecção em Bob, no laboratório, de um tom de 1,5 MHz (O modulador de fase de Alice foi alimentado com um sinal sinusoidal com frequência de 1,5 MHz). O número médio de fótons do pulso fraco era de  $\langle n \rangle \approx 0.6$  (1550 nm) na entrada do canal óptico, a transmissividade do canal foi de  $t_c \approx 0.6$  e a frequência do trem de pulsos ópticos de Alice foi de  $T_p^{-1} = 5$  MHz. O detector óptico usado por Bob foi o PDB465C da Thorlabs.

Por fim, usamos nosso protocolo de QSDC para transmitir a música *dois lados*, de Wesley Safadão, por um link de 5 km de fibra óptica instalada em Fortaleza, pertencente à empresa CLARO Telecom. A Fig. 3 mostra o link óptico utilizado no mapa de Fortaleza.

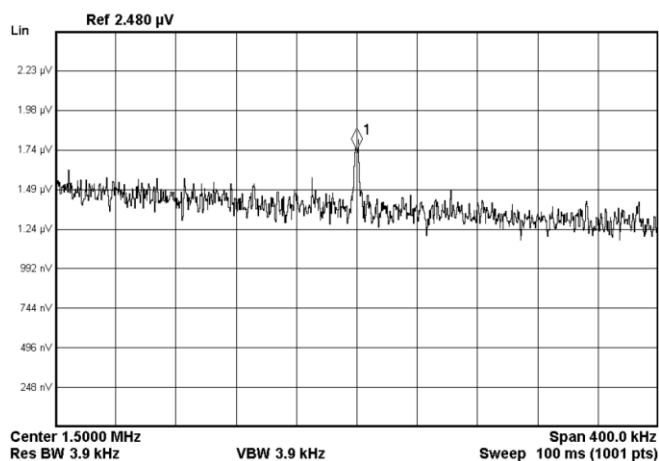


Fig. 2 – Detecção em Bob do tom de 1,5 MHz enviado por Alice.

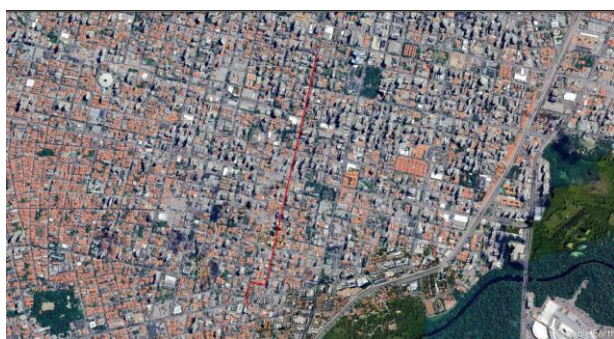


Fig. 3 – Enlace óptico subterrâneo utilizado na implementação de QSDC em Fortaleza.

Neste experimento, ligamos um amplificador de áudio e um autofalante diretamente na saída do PDB465C para ouvir a música transmitida, evidenciando a boa estabilidade do interferômetro mostrado na Fig. 1 e da detecção homódina realizada.

### IV. CONCLUSÕES

O protocolo de QSDC aqui apresentado traz duas novidades: 1) Ele permite a transmissão segura direta de sinais analógicos. 2) Sua segurança é baseada no teorema de Whittaker–Nyquist–Shannon. Adicionalmente, o protocolo aqui proposto pode ser facilmente implementado com componentes ópticos baratos e comumente encontrados, o que permite sua implementação massiva em redes ópticas instaladas.

#### AGRADECIMENTOS

Este trabalho foi parcialmente suportado pelas agências CNPq (304188/2025-5), CAPES (001) e FUNCAP (ITR-0214-00041.01.00/23). Este artigo também é parte do projeto Desenvolvimento e Inovação em Comunicações Quânticas (422316/2023-7). Por fim, gostaríamos de agradecer à CLARO Telecom por nos permitir utilizar sua infraestrutura de rede óptica instalada em Fortaleza.

#### REFERÊNCIAS

- [1] V. F. Guedes, S. T. de Oliveira, G. L. de Oliveira, J. B. R. Silva e R. V. Ramos, Quantum Secure Direct Communication of Continuous-Time Signals Using Whittaker-Nyquist-Shannon Theorem, ArXiv Quant-ph 2506.1737. Available on <https://arxiv.org/abs/2506.17377>.