Protocolos de Comunicação Quântica: Estudo de Caso Prévio para Implementação de Enlace Experimental

Emanuel M. Cabrera[2], João Victor C. Miranda[1], Akio N. Barbosa[1] e Regina M. Silveira[1]

[1]Escola Politécnica / [2]Instituto de Física
Universidade de São Paulo (USP) – São Paulo, SP – Brasil

emanuel01@usp.br

Abstract. *This article presents a preliminary study for the implementation of an experimental Quantum Key Distribution (QKD) link operating in free-space optical channels between the Physics Institute and the Polytechnic School of the University of São Paulo, which will be part of the São Paulo State Quantum Network. For the study of short-distance urban scenarios, the BB84, B92, and COW protocols were initially considered, evaluating various transmission characteristics in different scenarios. To make this possible, it was necessary to develop an extension of the SeQUeNCe simulator, with which it was possible to compare the performance of the three protocols, highlighting the superiority of BB84 in secret key rate.*

Resumo. *Este artigo apresenta um estudo prévio para a implementação de um enlace experimental de Distribuição Quântica de Chaves (QKD) operando em canais ópticos de espaço livre (free space) entre o Instituto de Física e a Escola Politécnica da Universidade de São Paulo, que fará parte da Rede Quântica do Estado de São Paulo. Para o estudo de cenários urbanos de curta distância foram considerados inicialmente os protocolos BB84, B92 e COW, avaliando diversas características de transmissão em diferentes cenários. Para que isso fosse possível foi necessário desenvolver uma extensão do simulador SeQUeNCe, com o qual foi possível comparar o desempenho dos três protocolos, evidenciando a superioridade do BB84 em taxa de chave secreta.*

1. Introdução

A criptografia quântica resolve o problema da distribuição de chaves sem depender da complexidade matemática de funções unidirecionais, protegendo as comunicações mesmo contra ataques de computadores quânticos, pois explora propriedades quânticas da não-clonagem e do entrelaçamento para garantir sigilo incondicional [Gisin et al. 2002]. Enlaces quânticos em espaço livre (*free space*) surgem como uma alternativa de baixo custo e alta flexibilidade em relação à fibra óptica, especialmente em áreas urbanas onde a instalação de cabos é dificultada pela geografia, geologia ou infraestrutura existente.

Para a implantação de uma rede de Distribuição Quântica de Chaves (QKD - Quantum Key Distribution), um aspecto relevante é a escolha do protocolo de comunicação a ser utilizado. Neste contexto, simulações computacionais são ferramentas indispensáveis para projetos de caracterização, validação e otimização dos protocolos de comunicação [Bel and Kiran 2025].

Por este motivo, este trabalho avalia e compara o desempenho dos protocolos BB84 [Mehic et al. 2020], B92 [Gandelman et al. 2025] e COW [Stucki et al. 2005] por meio de simulação, como estudo prévio à implementação de um enlace experimental QKD operando em canais ópticos de espaço livre entre o Instituto de Física da USP (IFUSP) e a Escola Politécnica da USP (EPUSP). Esse enlace fará parte da Rede Quântica do Estado de São Paulo (Projeto StruQT —- FAPESP). O foco desta etapa é comparativo: identificar tendências de desempenho, validar a extensão implementada no simulador e explicitar quais simplificações ainda precisam ser removidas antes de usar os resultados como base de decisão experimental.

Embora enlaces aéreos sofram com turbulência atmosférica, cintilação e luz de fundo, esses efeitos ainda não foram incorporados ao modelo desta versão. Optou-se por começar com um cenário controlado para isolar o comportamento intrínseco dos protocolos e validar a implementação no SeQUeNCe.

Este artigo é estruturado da seguinte maneira: na seção 2 apresentamos um breve levantamento dos protocolos mais utilizados; a seção 3 aborda simuladores disponíveis, suas limitações e a escolha do simulador para este projeto; na seção 4 é mostrado o estudo realizado para a comparação de 3 protocolos utilizando o simulador SeQUeNCe e a extensão desenvolvida por nós e finalmente, a seção 5 apresenta as considerações finais e os próximos passos.

2. Protocolos de Comunicação Quântica

Em um sistema QKD, os protocolos podem ser organizados em duas classes principais: preparação-e-medição e protocolos baseados em emaranhamento [Wolf 2021, ITU-T 2021]. No primeiro caso, Alice prepara estados quânticos e Bob os mede; no segundo, ambos compartilham correlações quânticas geradas por pares emaranhados. A segurança não decorre exclusivamente do emaranhamento: mesmo nos protocolos de preparação-e-medição, a tentativa de extração de informação por um espião introduz perturbações mensuráveis no sistema.

Nesta fase do projeto analisamos apenas protocolos de preparação-e-medição, considerando a maturidade tecnológica que apresentam. Os protocolos selecionados foram:

BB84. Utiliza dois conjuntos de bases conjugadas; neste trabalho, sua implementação é associada à codificação em polarização. Após a etapa de *sifting*, os usuários estimam a taxa de erro e executam o pós-processamento clássico.

B92. Emprega apenas dois estados não ortogonais, também modelados aqui em polarização. É um protocolo comparativamente mais simples que o BB84, porém mais sensível a perdas e a estratégias de discriminação sem ambiguidade (*unambiguous state discrimination*, USD), o que deve ser considerado em análises futuras.

COW. É um protocolo de codificação temporal com pulsos coerentes fracos. A informação é extraída principalmente pelo tempo de chegada na linha de dados, enquanto a segurança é monitorada pela visibilidade do interferômetro na linha de monitoramento [Stucki et al. 2005].

3. Simuladores para estudo da comunicação quântica

Diversos simuladores de comunicação quântica estão disponíveis na literatura [Abreu et al. 2024, Bel and Kiran 2025]. Neste trabalho escolhemos o SeQUeNCe [Wu et al. 2021] por quatro motivos: é *open-source*, opera com abstração em nível de fótons, tem manutenção ativa e possui arquitetura suficientemente modular para extensão dos protocolos de interesse. Não realizamos, nesta etapa, um *benchmark* quantitativo com outros simuladores; tal comparação exigiria a reimplementação homogênea dos mesmos cenários e foge ao escopo desta versão. Pelo mesmo motivo, também não foi desenvolvido um simulador próprio: a prioridade foi validar rapidamente cenários experimentais sobre uma base já consolidada.

3.1. Extensão do simulador e hipóteses adotadas

O código-base do SeQUeNCe foi estendido para suportar os protocolos B92 e COW, sendo disponibilizado em repositório público[1]. A fim de validar a extensão do simulador SeQUeNCe desenvolvida por nós, replicamos os experimentos com o protocolo B92, elaborados em [Gandelman et al. 2025], utilizando os mesmos cenários propostos pelos autores, ou seja, para tamanho de chave de 45 e 100 bits. Na replicação destes experimentos obtivemos a mesma taxa de bits úteis R_s e o mesmo QBER (Quantum Bit Error Rate), demonstrando a corretude da implementação.

Um dos pontos fortes do simulador SeQUeNCe é a ampla gama de parâmetros configuráveis, o que permite explorar diferentes cenários. No entanto, em nosso estudo, o cenário de teste simula o enlace quântico a ser implantado (StruQT-FAPESP) considerando um cenário simplificado, onde o objetivo é validar a implementação dos protocolos na extensão.

Assim, dos parâmetros de emissor (frequência do laser, número médio de fótons), canal (distância, atenuação) e detector (eficiência, *dark count*, resolução temporal), determinadas grandezas (número médio de fótons, atenuação, t_B, p_{Eve}) tiveram papel fundamental na simulação de ensaios de estresse. As métricas avaliadas são [Wolf 2021]: latência; QBER, isto é, a porcentagem de bits incorretos na chave bruta gerada; bits úteis por transmissão, correspondentes à taxa de bits remanescentes após a etapa de *sifting*; e a taxa de chave secreta (R_{sk}), correspondente à taxa de chaves secretas geradas após os processos de reconciliação da informação e amplificação de privacidade. Nota-se que, nesta simulação, a etapa de pós-processamento não é implementada, de modo que R_{sk} é estimada por meio de aproximações estatísticas.

Os parâmetros do emissor incluem: frequência de geração de fótons de $8\,\mathrm{MHz}$ e comprimento de onda de $780\,\mathrm{nm}$. Na simulação, o detector considera os parâmetros: eficiência $\eta = 65\%$, taxa de contagens escuras em $100\,\mathrm{Hz}$, taxa de contagem em $20\,\mathrm{MHz}$, resolução temporal de $1000\,\mathrm{ps}$. O canal quântico simulado adota os parâmetros: atenuação $\alpha = 2 \cdot 10^{-4}\,\mathrm{dB/m}$ e fidelidade de polarização $F = 97\%$ (para BB84 e B92). Cabe destacar que, para os protocolos BB84 e B92, simula-se uma fonte de fótons únicos, enquanto que no protocolo COW, utiliza-se de uma fonte de pulsos coerentes fracos.

A atual versão da simulação considerou a fibra óptica como meio utilizado, pois em um primeiro momento, considerou-se a validade da implementação dos protocolos

[1] `https://github.com/Manolo789/SeQUeNCe-QKDprotocols`

BB84, B92 e COW na simulação em detrimento da modelagem do canal, resultando em uma modelagem mais simples do que a implementada no enlace real, mas suficiente como forma de validar a implementação dos protocolos. A simulação com o modelo de canal quântico que considere o meio aéreo está em desenvolvimento[2].

Especificamente no protocolo COW, considera-se o número médio de fótons $\mu = 0{,}5$, o coeficiente de transmissão do divisor de feixe não equilibrado $t_B = 0{,}58$, o erro de fase do interferômetro $\sigma_{\text{int}} = 0{,}20\,\text{rad}$ e o coeficiente de ruído de fase $\sigma_\varphi = 0{,}01\,\text{rad}/\sqrt{\text{m}}$.

No cenário com ataque, Eve é posicionada na metade da distância do canal e emprega uma taxa de interceptação[3] $p_{\text{Eve}} = 0{,}9$, de forma a evidenciar a sensibilidade dos protocolos a uma interceptação maciça; esse valor não deve ser interpretado como cenário realista de operação. A análise foi desenvolvida em duas dimensões: variação da distância $d \in [1,\, 100]\,\text{km}$ com tamanho de chave fixo $k = 10000\,\text{bits}$, e variação do tamanho da chave $k \in \{20,\, 45,\, 50,\, 100,\, 200,\, 400,\, 800,\, 1600,\, 5000,\, 20000,\, 40000,\, 80000,\, 100000\}$ bits com distância fixa $d = 700\,\text{m}$.

4. Resultados e Discussão

Inicialmente consideramos o cenário sem ataque. A Figura 1 resume os resultados para variação da distância e do tamanho da chave. O BB84 mantém R_{sk} positivo em toda a faixa simulada, com QBER aproximadamente constante em torno de $1{,}5\%$. O B92 também apresenta R_{sk} positivo, porém menor, acompanhado de QBER ligeiramente superior ($\approx 3\%$). No COW, no cenário de variação da distância, R_{sk} cai a zero por volta de 10–11 km, o que, no modelo atual, decorre principalmente da degradação da visibilidade imposta pelos parâmetros de fase adotados.

Para os três protocolos, R_s decai com a distância de forma aproximadamente exponencial, acompanhando a transmitância do canal $T(d) = 10^{-\alpha d/10}$. Quando fixamos $d = 700\,\text{m}$ e variamos k, observa-se crescimento monotônico de R_{sk} até a saturação assintótica e comportamento análogo para R_s.

No cenário com ataque *intercept-resend*, a Figura 2 mostra a degradação esperada dos protocolos BB84 e B92. Para o BB84, a simulação fornece $\text{QBER} \approx 24{,}1\%$, em boa concordância com o valor teórico de 25% para esse tipo de ataque. Para o B92, obtemos $\text{QBER} \approx 32{,}5\%$, o que também torna nula a taxa secreta. Isso resulta da natureza básica dos protocolos QKD: com o aumento de QBER, R_{sk} cairá para valores negativos. Como $R_{sk} < 0$, então $\log_{10}(R_{sk})$ é indefinido. Como o caso $p_{\text{Eve}} = 0{,}9$ é deliberadamente extremo, ele deve ser interpretado apenas como ensaio de estresse e não como cenário de ameaça provável.

A taxa R_s permanece próxima à do cenário sem ataque, pois idealmente a presença de Eve não elimina a chegada de fótons a Bob; ela apenas corrompe a informação neles contida. No COW, a perturbação de Eve manifesta-se prioritariamente na visibilidade do interferômetro, e não diretamente na QBER da linha de dados [Stucki et al. 2005]. Isso se deve ao fato de que a linha de dados do protocolo COW realiza medição de tempo de chegada (time-of-arrival), insensível a erros ópticos na polarização. No entanto, apesar de este protocolo ter um sistema de medição insensível a erros ópticos na polarização,

[2] `https://github.com/Manolo789/SeQUeNCe-QKDprotocols/tree/QC-in-FS`

[3] Probabilidade de Eve interceptar um único fóton.

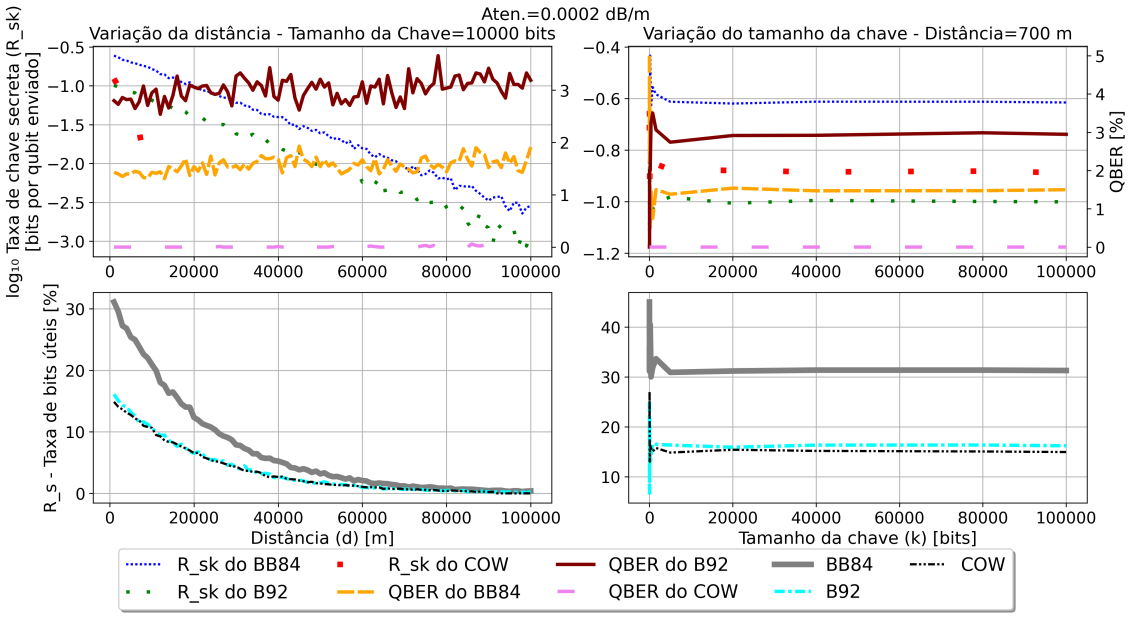

Figura 1. Desempenho dos protocolos no cenário ideal, considerando a variação da distância e do tamanho da chave.

observa-se que em sistemas reais há erros relacionados à fase do pulso e ao ruído térmico, resultando em uma taxa QBER não nula. Por este motivo, está previsto em nosso plano de trabalho a implementação de modelos de fontes ruidosas mais realistas na simulação do protocolo COW.

5. Conclusão

Este artigo apresentou uma comparação preliminar entre os protocolos BB84, B92 e COW para um futuro enlace QKD em espaço livre entre a EPUSP e o IFUSP. O desenvolvimento de uma extensão do simulador SeQUeNCe permitiu validar a implementação do B92 e incorporar o COW ao estudo comparativo.

Os experimentos demonstraram que o protocolo BB84 apresenta melhores resultados, o que justifica sua ampla utilização e maturidade tecnológica. Os resultados decorrentes das simulações realizadas com o SeQUeNCe poderão ser utilizados como valores de referência para uma situação idealizada, contribuindo para comparação futura com uma simulação que admita canal quântico em meio aéreo, como justificado na seção 3.1.

Como trabalho futuro será avaliada a possibilidade de implementar os protocolos BBM92 e E91 no simulador SeQUeNCe, de forma a enriquecer a análise ao ampliar a cobertura para o paradigma *device-independent*, evidenciando o contraste entre maturidade tecnológica e robustez teórica de segurança. Além disso, os resultados desta simulação e futuras simulações mais realistas serão validados experimentalmente no enlace quântico EPUSP–IFUSP do projeto StruQT–FAPESP.

Agradecimentos

O presente trabalho foi realizado com apoio da Pró-reitoria de Pesquisa da USP com o Programa Unificado de Bolsas de iniciação científica, da Coordenação de

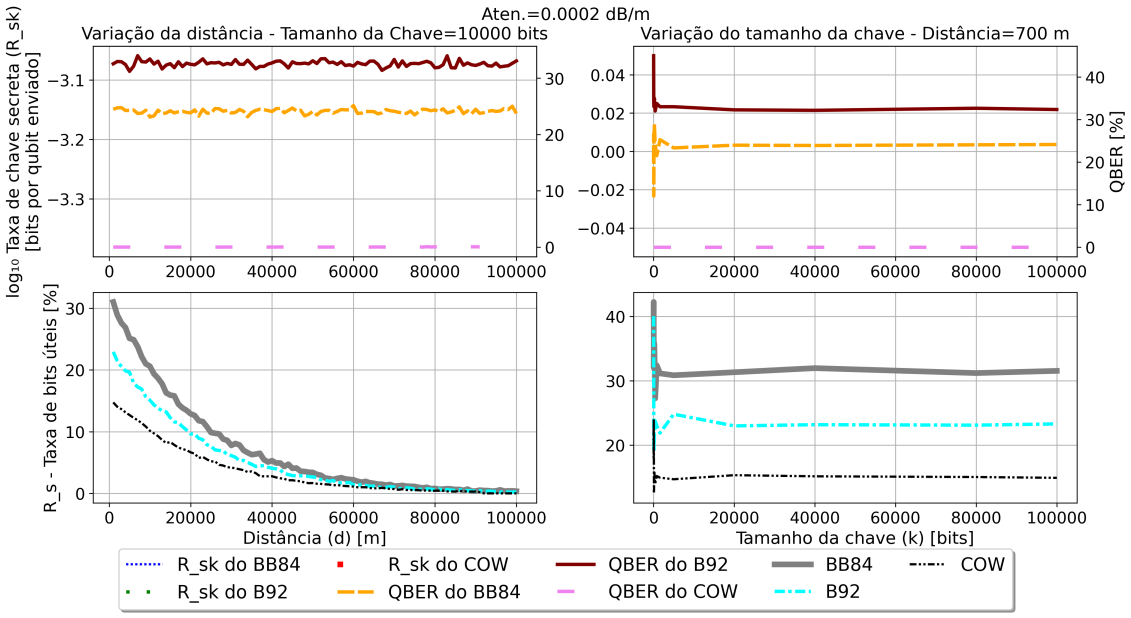

Figura 2. Desempenho dos protocolos no cenário com ataque *intercept-resend*, considerando a variação da distância e do tamanho da chave.

Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001 e da Fundação de Apoio à Pesquisa do Estado de São Paulo (FAPESP), projeto StruQT (Proc. 2024/08450-0).

Referências

Abreu, D. et al. (2024). Multipurpose quantum network simulators: A comparative study. In *Proceedings of WQuNets*. SBC.

Bel, O. and Kiran, M. (2025). Simulators for quantum network modeling: A comprehensive review. *Computer Networks*, 263:111204.

Gandelman et al. (2025). Hands-on quantum cryptography: Experimentation with the B92 protocol using pulsed lasers.

Gisin, N. et al. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195.

ITU-T (2021). Technical report on QKDN protocols: Quantum layer. D2.3-part 1: FG-QIT4N. Technical report, ITU, Geneva.

Mehic, M. et al. (2020). Quantum key distribution: A networking perspective. *ACM Computing Surveys*, 53(5):1–41.

Stucki, D. et al. (2005). Fast and simple one-way quantum key distribution. *Applied Physics Letters*, 87:194108.

Wolf, R. (2021). *Quantum Key Distribution: An Introduction with Exercises*. Springer.

Wu, X. et al. (2021). SeQUeNCe: A customizable discrete-event simulator of quantum networks. *Quantum Science and Technology*, 6(4):045027.