Rui Manuel Paiva de Morais Santos Ferreira

Distribuição de Chaves Quânticas Em Redes de Comunicação Para Redes Elétricas Inteligentes

Dissertação no âmbito do Mestrado Integrado em Engenharia Eletrotécnica e de Computadores, ramo de Telecomunicações sob a orientação da Professora Doutora Rita Cristina Girão Coelho da Silva, apresentada ao Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Fevereiro de 2022

Faculdade de Ciências e Tecnologia
da Universidade de Coimbra

1 2  9 0

UNIVERSIDADE D
COIMBRA

Distribuição de Chaves Quânticas Em Redes de Comunicação Para Redes Elétricas Inteligentes

Rui Manuel Paiva de Morais Santos Ferreira

Dissertação no âmbito do Mestrado Integrado em Engenharia Eletrotécnica e de Computadores, ramo de Telecomunicações sob a orientação da Professora Doutora Rita Cristina Girão Coelho da Silva, apresentada ao Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Ciências e Tecnologia da Universidade de Coimbra

Júri:

Prof. Doutora Rita Cristina Girão Coelho da Silva

Prof. Doutor Luís Alberto da Silva Cruz

Prof. Doutora Lúcia Maria dos Reis Albuquerque Martins

Fevereiro 2022

Agradecimentos

Gostava de agradecer em primeiro lugar à minha orientadora, Professora Rita Girão da Silva, por todo o apoio dado ao longo da realização deste projeto, pelos seus conselhos, a sua compreensão e a sua enorme disponibilidade para me auxiliar na realização do mesmo.

Não poderia deixar de agradecer a todos os meus colegas e amigos que me acompanharam neste percurso académico, em especial aqueles que se tornaram na minha segunda família, pois sem eles não teria sido a mesma coisa.

Por fim, e não menos importante, um grande agradecimento à minha família, não esquecendo os que não puderam ver a conclusão desta etapa da minha vida, por todo o apoio que me deram, por me terem proporcionado o melhor que lhes foi possível e por toda a paciência que, por vezes, lhes foi exigida.

O presente trabalho foi realizado e financiado no âmbito do Financiamento Plurianual de Unidades de I&D 2020-2023, da UI0308, com a referência UIDB/00308/2020, do Instituto de Engenharia de Sistemas e Computadores de Coimbra (INESC Coimbra), BI Refª UI0308 SG-Quantum.1/2020, com apoio financeiro da Fundação para a Ciência e a Tecnologia (FCT).

Resumo

Às redes elétricas inteligentes (*smart grids*) está associada, além do fluxo energético base, uma enorme quantidade de comunicações confidenciais. Tais comunicações dizem respeito a trocas de informação entre consumidores e centros de controlo e requerem elevada segurança e privacidade. Os métodos de distribuição de chaves quânticas (QKD) são uma opção de garantir encriptação de informação trocada entre os elementos destas redes energéticas com o grau de segurança requerido. Considera-se assim a possibilidade de utilização destas formas de distribuição de chaves seguras e eficientes, por forma a sustentarem métodos de encriptação de chave simétrica, cuja segurança não se prevê afetada pelo desenvolvimento tecnológico, em especial, pela utilização de computação quântica. Existem várias formas de implementar estes métodos de distribuição de chaves, cada um com os seus respetivos protocolos, todos com as suas limitações, características e requisitos para o seu bom funcionamento.

Esta Dissertação propõe-se analisar todo o funcionamento do método QKD Prepare-and-Measure, com encriptação de fotões segundo a sua polarização, para três protocolos já desenvolvidos e testados, BB84, SARG04 e KMB09, tendo por base o contexto de uma *smart grid*, em que cada medidor energético inteligente (*smart meter)* envia o seu consumo periodicamente. É tido em conta um vasto leque de fatores a considerar para uma possível implementação prática destes protocolos descritos na literatura consultada, sendo que, o objetivo da aplicação deste método é a codificação One-Time-Pad (OTP) das respetivas mensagens.

O trabalho é desenvolvido no *framework* de simulação MOSAIK, onde foi sobreposto uma solução QKD, de modo a distribuir chaves quânticas pelos dispositivos da *smart grid*. Apesar de não ser o primeiro simulador de QKD aplicado a este tipo de rede (Lardier et al. 2009), este trabalho propõe-se expandir a aplicabilidade destes métodos de distribuição de chave, contemplando mais características da rede e dos elementos que a constituem, como emissores, canais de transmissão e recetores. Pretende-se assim elaborar uma simulação o mais fiel possível à realidade, num contexto onde podem constar dois ataques distintos estudados: *intercept-and-resend* e *photon-number-splitting.*

Palavras-Chave: *smart grid*, *qubits*, *bits*, encriptação, chaves, protocolos, eficiência, segurança.

Abstract

In addition to the basic energy flow, smart grids are associated with a huge amount of confidential communications. Such communications concern exchanges of information between consumers and control centers and require high security and privacy. Methods of quantum key distribution (QKD) emerge as an option to ensure encryption of information exchanged between elements of these energy networks with the required degree of security. These forms of key distribution are secure and efficient, in order to support symmetric key encryption methods, whose security is not expected to be affected by technological development, especially by the use of quantum computing. There are several ways to implement these methods of key distribution, each with their respective protocols, all with their limitations, characteristics and requirements for their proper functioning.

This dissertation proposes to analyze the entire operation of the QKD Prepare-and Measure method, with encryption of photons according to their polarization, for three protocols already developed and tested, BB84, SARG04 and KMB09, based on the context of a smart grid, where each smart meter sends its reading periodically. A wide range of factors associated with a possible practical implementation of these protocols described in the consulted literature are taken into account, and the objective of the application of this method is the One-Time-Pad (OTP) encoding of the respective messages.

The work is developed in the MOSAIK simulation framework, where a QKD solution was superimposed, in order to distribute quantum keys to the smart grid devices. Despite not being the first QKD simulator applied to this type of network (Lardier et al. 2009), this work proposes to expand the applicability of these methods, contemplating more characteristics of the network and the elements that constitute it, such as transmitters, transmission channels and receivers. The goal is to elaborate a simulation as faithful as possible to reality, in a context where two different attacks studied can be included: intercept-and-resend and photon-number-splitting (PNS).

Keywords: smart grid, qubits, bits, encryption, keys, protocols, efficiency, security,

Lista de Acrónimos

AES Advanced Encryption Standard

CC Centro de Controlo

CV Continuous Variables

DI-QKD Device Independent - QKD

DoS Denial of Service

DV Discrete Variables

EB Entanglement Based

ENISA European Network and Information Security Agency

IEEE Institute of Electrical and Electronics Engineers

ITER Index transmission error

MDI-QKD Measurement Device Independent - QKD

MITM Man-in-the-Middle

NIST National Institute of Standards and Technology

OTP One-Time-Pad

PKI Public Key Infrastructure

PM Prepare-and-Measure

PNS Photon-Number Splitting

QBER Quantum Bit Error Rate

QKD Quantum Key Distribution

WDM wavelenghth-division multiplexing

WCP weak coherent pulse

Lista de Figuras

Lista de Tabelas

Lista de Símbolos

$\|\varphi\rangle$	Representação de um *qubit*
θ	Polarização dos *qubits* na representação de espaço de Hilbert
φ	Ângulo longitudinal da polarização do *qubit* na esfera de Bloch
$A+,+$	Estados anunciados por Alice no protocolo SARG04
μ	Intensidade média de fotões por *qubit*
n	Número de fotões que constituem um *qubit*
p_n	Probabilidade de um *qubit* ser constituído por n fotões
$R(L)$	Taxa de transmissão de *qubits* em função do comprimento do canal L
α	Atenuação média na fibra
L	Distância da ligação quântica
σ	Estado de polarização após despolarização
p	Probabilidade de um *qubit* ser despolarizado
ρ	Representação matricial de um estado de um *qubit*
R_{raw}	Probabilidade de leitura de um *qubit*
η_{det}	Eficiência do fotorrecetor
η_{δ}	Atenuação sofrida no canal quântico
L_j	Leitura de um *qubit* no estado j
E_i	Envio de um *qubit* no estado i
B_x	Utilização da base x na leitura
k_{err}	Número de *qubits* dos quais foi possível concluir um *bit*
k_{corr}	Número de *qubits* dos quais não foi possível concluir um *bit*
κ	Número de *bits* da chave gerada e consequente número de *qubits*
$\eta_{protocolo}$	Eficiência de leitura do protocolo QKD utilizado
ξ	Reta que representa o número máximo teórico de *bits* de teste possíveis em função de κ

Índice

1. Introdução

Uma *smart grid* consiste numa rede elétrica inteligente, suportada por diversos dispositivos para controlo da potência ao longo dessa rede, permitindo estabelecer regras para o uso da energia. Monitoriza assim a produção, transmissão, distribuição e consumo da energia elétrica ao longo de toda a rede [1]. Existe então a necessidade de garantir a segurança e a privacidade das comunicações entre os intervenientes da rede, sendo que para tal são aplicados métodos para a encriptação das mensagens. Os métodos de encriptação atuais baseiam-se na utilização de chaves simétricas e assimétricas, e apresentam um elevado grau de segurança atualmente, o que não é garantido no futuro, em especial com a utilização de computação quântica. Devido às suas propriedades intrínsecas, os métodos de encriptação com base em chaves quânticas permitem a deteção de ataques *Man-in-the-Middle* (MITM) tradicionais com elevada eficiência, dependendo do tamanho da chave gerada [2]. Desta forma, trata-se de um conceito promissor para infraestruturas críticas ao nível da segurança. Contudo, devido ao *hardware*, a implementação de tais métodos é extremamente cara, quer para o seu estudo ao nível académico, quer ao nível comercial.

Esta dissertação pretende analisar métodos de distribuição de chaves quânticas (QKD) aplicados a uma rede *smart grid*, sendo desenvolvido sobre o *framework* Mosaik, um simulador de ambiente de *smart grids*, elaborado na linguagem *python* [3]. O *software* permite simular um cenário de rede *smart grid* ao nível local, fazendo uso de vários simuladores de elementos da rede. O Mosaik permite também a integração de uma plataforma de distribuição de chaves quânticas, como por exemplo Quantum-Sim [2], de forma a encriptar comunicações entre os *smart meters* das várias casas da rede e um simulador de um controlador específico para o efeito, intitulado originalmente de *Control Center*.

Este trabalho está organizado do seguinte modo: no Capítulo 2 é descrita a motivação para a realização deste trabalho. No Capítulo 3 é feita uma revisão da literatura no âmbito de métodos de encriptação atuais, descrição de sistemas QKD, as características do *hardware* necessário à sua implementação, possíveis ataques, protocolos QKD utilizados e métodos de encriptação que os complementam. No Capítulo 4 são descritos os objetivos do trabalho realizado, no Capítulo 5 é explicado o contexto de simulação e no Capítulo 6 é elaborada a metodologia da realização do mesmo. No Capítulo 7 é feita uma análise dos resultados obtidos, seguida da discussão das potencialidades deste trabalho que poderão vir a ser desenvolvidas no futuro no Capítulo 8, e por último o Capítulo 9 consiste na conclusão do trabalho desenvolvido.

2. Motivação

Este projeto surgiu como uma oportunidade de estudo de um sistema de distribuição de chaves quânticas, para comunicações entre elementos de uma *smart grid*.

Uma *smart grid* requer um extenso desenvolvimento de sistemas de computação e comunicação entre todos os sensores, atuadores, dispositivos de armazenamento de dados, transformadores, geradores de energia renovável, baterias e contadores inteligentes (*smart meters)* da rede [4]. Tais comunicações dizem respeito ao controlo do fluxo energético e gestão de carga, sendo necessário garantir a privacidade dos intervenientes dos canais de comunicação. Entre os dados em causa estão por exemplo padrões de uso de eletricidade, que inclusive se podem traduzir em deduções sobre atividades específicas ou uso de equipamentos. Essas informações podem ter uso criminal ou podem ser usadas para concorrência a nível de negócios [5]. É então necessário garantir que estes dispositivos de controlo da rede são confiáveis, ou seja, que os dispositivos se encontram seguros, livres de ataques e que as trocas de dados garantem privacidade dos mesmos. Tal é atingido através da codificação da informação transmitida. De acordo com o *National Institute of Standards and Technology* (NIST) e com o *European Network and Information Security Agency* (ENISA), a confidencialidade, integridade, autenticidade, funcionalidade e disponibilidade, são os aspetos mais críticos de comunicação numa *smart grid* [4].

Com o objetivo de responder a estas questões, é então explorada a hipótese de aplicar QKD [6], de modo a serem atribuídas chaves como forma de segurança na *smart grid*, o que requer uma aplicação de protocolos quânticos para a atribuição das chaves entre o Centro de Controlo (CC) e os restantes dispositivos de controlo da *smart grid*. Estes métodos de distribuição de chaves apresentam diversas vantagens, tais como o facto de a sua segurança ser garantida mesmo utilizando processos computacionais avançados, o facto de serem práticos de implementar, uma vez que consistem essencialmente em fotões transmitidos por canais de fibra ótica e por último o nível elevado de segurança que apresentam, devido a propriedades de física quântica. Tais métodos de comunicação quântica foram reconhecidos como um tópico importante para as *smart grids* em IEEE *Smart Grid roadmap* para 2030, tal como referido em [2]. Contudo, estes métodos apresentam alguns desafios quando aplicados num contexto de rede, tais como a distância necessária para as ligações, a necessidade de ser aplicada em vários nós e a velocidade e quantidade das trocas de dados requeridas [4]. Além disso, estes novos sistemas trazem consigo novos tipos de ataques que necessitam de ser analisados, por forma a garantir a segurança das ligações da rede.

O teste de esquemas de comunicação baseados em protocolos quânticos é demasiado dispendioso, devido sobretudo ao *hardware* necessário para a sua implementação [2]. Deste modo, é de todo o interesse a criação de um método de co-simulação que contemple vários protocolos QKD, ataques e parâmetros intrínsecos à transmissão, como por exemplo, o ruído, aplicados ao cenário de *smart grid*. Assim, é possível analisar diversos cenários de QKD, de forma a determinar a viabilidade e segurança de cada um, facilitando a investigação na área.

3. Revisão de Literatura e Conceitos Chave

Neste capítulo, são analisados vários conceitos subjacentes ao trabalho desenvolvido. É feita uma descrição dos métodos de encriptação mais utilizados atualmente, das suas fragilidades e da forma como os métodos QKD podem representar uma solução para essas fragilidades. De seguida, descreve-se os sistemas QKD, as suas características e diversos protocolos. É ainda explorado o seu funcionamento geral, o *hardware* necessário à sua implementação e as suas especificidades e limitações, como por exemplo os vários tipos de ruído e possíveis ataques. Por último, são descritos os métodos de encriptação contemplados.

3.1. Métodos de Encriptação Atuais

De forma a garantir a confidencialidade das mensagens, é necessário encriptar a informação com uma chave, de forma que apenas os intervenientes na comunicação lhe tenham acesso. Atualmente, os esquemas de distribuição de chaves de encriptação estão divididos em duas categorias principais, *public key infrastructure* (PKI) e *symmetric key environment* [7].

Em PKI, ou *asymmetric key*, cada nó de uma ligação contém uma chave pública (*public key)* e uma chave privada (*private key)*. Como o nome indica, a chave pública de um nó pode ser disseminada pelos restantes elementos, enquanto a chave privada é apenas conhecida pelo nó em causa. Assim, com este método, um transmissor codifica uma mensagem com a chave pública do nó recetor, contudo, esta apenas pode ser desencriptada com a chave privada do recetor. Os métodos atuais de *public key* referidos baseiam-se no facto de que certos problemas matemáticos são extraordinariamente difíceis de solucionar com os recursos atuais e visam apenas tipos de ataques já conhecidos [8]. Tal deve-se ao facto de a segurança destes métodos se basear na complexidade de realizar fatorização de inteiros ou resolver problemas logarítmicos discretos, algo que poderá ser ultrapassado com computação quântica [4], [6].

Já num ambiente de chave simétrica, ambos os intervenientes da ligação usam a mesma chave para encriptar e desencriptar. Naturalmente, por questões de privacidade, esta deve ser apenas conhecida pelos intervenientes da ligação em causa. Dois exemplos de métodos deste tipo são a encriptação por One-Time-Pad (OTP) e Advanced Encryption Standard (AES), que serão explicados em detalhe no seguimento do texto. Para o funcionamento de um ambiente de chaves simétricas numa *smart grid*, é necessário que um dispositivo de controlo (*Control Center*) e dispositivos de controlo da rede concordem numa chave comum [9], [4], [6]. Estes métodos, apesar de serem relativamente seguros contra atacantes munidos de computação quântica, dependem da garantia de ambos os intervenientes da comunicação serem de confiança e da chave que ambos partilham não ser copiada por nenhum intruso.

Conclui-se então que nenhum destes métodos oferece total garantia de segurança no futuro. De acordo com a literatura, estes métodos apenas são 100% seguros caso a chave tenha o mesmo tamanho que a mensagem [10], encriptando-a usando o *standard* One-Time-Pad (OTP) [11]. A questão principal é saber como os intervenientes da ligação conseguem partilhar uma chave segura inicialmente, o que é designado de "problema de distribuição de chaves" [6].

3.2. Qubit

Por forma a compreender o funcionamento de sistemas QKD, é necessária, primeiro uma revisão ao quantum *bit* (*qubit*), que corresponde à unidade de informação quântica. Corresponde a um vetor unitário $|\varphi\rangle$ no espaço vetorial bidimensional [12], tratando-se assim de um objeto que se encontra simultaneamente numa conjugação de dois estados distintos até ao momento da medição, segundo o princípio de sobreposição. Esses estados correspondem a:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Cada *qubit* é dado pela fórmula $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, em que α e β podem ser reais ou imaginários, apenas necessitam de ser normalizados $|\alpha|^2 + |\beta|^2 = 1$, por forma a que cada *qubit* contenha apenas informação correspondente a um único *bit* clássico de informação.

Para melhor visualização do estado de um *qubit* é vulgarmente utilizada a representação em esfera de Bloch, em que cada um dos eixos é denominado de base:

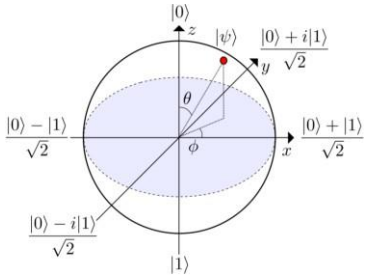


Figura 1: Representação de 6 estados distintos de qubits numa esfera de Bloch [13].

Os estados na Fig. 1 descritos por $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ e $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ são vulgarmente representados por $|+\rangle$ e $|-\rangle$, respetivamente. As rotações ao longo dos vários eixos são descritas por multiplicações do estado inicial pelas matrizes de Pauli, são elas:

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Contudo, para uma representação mais prática, é melhor a utilização em espaço de Hilbert, como na Figura 2, em duas dimensões, que corresponde a um mapeamento holomórfico da esfera de Bloch, onde cada *qubit* é descrito por $|\varphi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$. Nesta representação $|+\rangle$ e $|-\rangle$, correspondem aos valores de $\theta = 45^o$ e $\theta = 315^o$.

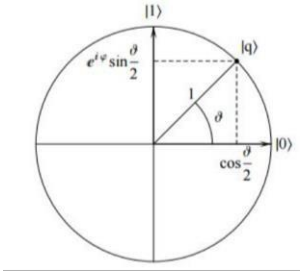


Figura 2: Representação de um qubit no espaço de Hilbert [14].

Devido à física quântica a que os *qubits* estão sujeitos, uma das suas particularidades é o facto do seu estado ser inevitavelmente alterado quando sujeito a uma leitura direta, pelo que não podem ser, por exemplo, copiados, o que é denominado por *no-clonning theorem* [15].

3.3. QKD

Os métodos QKD surgem como uma tentativa de obter sistemas de encriptação o mais seguros possível. Tal deve-se à necessidade de criar protocolos alternativos aos métodos clássicos de geração e distribuição de chaves secretas entre intervenientes numa comunicação sem a necessidade de um canal seguro para o efeito, de forma que essas chaves sejam utilizadas em criptografia de chave simétrica. A combinação de dois métodos, QKD e de encriptação OTP, é conhecida por ser em teoria, extremamente segura, garantindo a confidencialidade da informação, inclusive contra atacantes com recursos clássicos e quânticos ilimitados [4], [16].

Existem várias formas de implementar sistemas deste tipo, sendo que todas requerem o uso de dois tipos de canais, como ilustrado na Figura 3. O primeiro corresponde a um canal quântico, também designado de canal físico, e nele é transmitida informação quântica, entre o emissor e o recetor. O segundo é um canal de comunicação clássico autenticado, onde os intervenientes na distribuição da chave chegam a um consenso acerca da chave a utilizar na respetiva troca de informação que se sucede [17]. Neste último canal, são trocadas informações acerca da informação quântica enviada e recebida, bem como alguns *bits* de teste da chave resultante, o que permite fazer a deteção e correção de erros, bem como averiguar a presença de um potencial intruso (*eavesdropper*) no canal quântico.

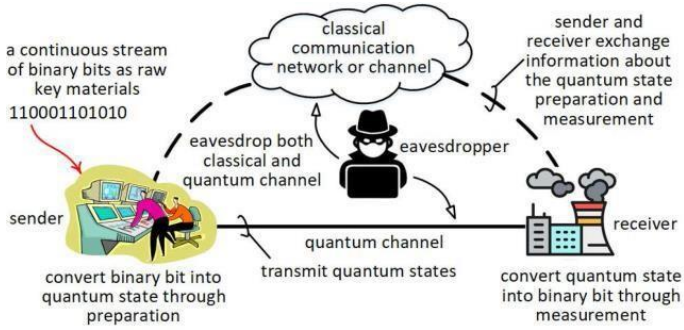


Figura 3: Representação de uma ligação QKD [4].

A maioria dos protocolos apresenta quatro fases de troca de informação. Primeiramente, em (1) *Distribution and Measurements*, o emissor, geralmente referido na literatura por Alice, gera uma chave que utilizará juntamente com o recetor, vulgarmente designado por Bob, na codificação e descodificação na troca da mensagem posterior. Alice codifica essa chave em informação quântica utilizando fotões, originando assim *qubits*. Os métodos de codificação possíveis e os graus de liberdade que cada fotão possui serão explicados de seguida. A leitura dum *qubit* é ambígua, pelo princípio da incerteza de Heisenberg, e tem uma dada probabilidade de ser feita de forma errada, o que depende do protocolo utilizado. Segue-se então a troca de informação no canal público como referido anteriormente, na fase (2) *Shifting and Parameter estimation*, onde são averiguados os *qubits* lidos corretamente, descartando os restantes, obtendo assim uma *raw key*. Na fase (3), *Advantage Distilation*, que é uma fase opcional presente em alguns protocolos, é feito um pós processamento da *raw key*, para aumentar a correlação entre as chaves de Alice e Bob, como por exemplo alteração de *bits* da *raw key*. Por último, na fase (4) *Information Reconciliation and Privacy Amplification*, Bob deteta e corrige os erros da sua *string* de bits [18].

Este método apresenta várias vantagens em relação aos métodos de distribuição de chaves tradicionais. Os protocolos QKD permitem que dispositivos numa *smart grid*, com energia limitada, possam evitar sobrecargas de computação e consumo energético, garantindo confiança e segurança, sendo pouco dispendiosa ao nível de *hardware* [2]. A segurança contra intrusos que intercetem o sinal quântico é outro ponto forte destes sistemas. A presença de um *eavesdropper*, vulgarmente denominado por Eve, que leia diretamente o canal quântico, resulta num erro quântico e numa taxa de erro de *bit* quântico (QBER) significativo, sob a forma de ruído, que pode ser detetado após troca de informação no canal público e de *bits* de teste [19], [20], [21]. Tal deve-se ao facto de a informação quântica estar sujeita ao princípio da incerteza e do *no-cloning theorem* e um *eavesdropper* não poder obter informação diretamente acerca do estado quântico sem o perturbar. Dessa forma, não pode também, por exemplo, duplicar o sinal quântico proveniente de Alice e efetuar um reencaminhamento de uma cópia perfeita para Bob [6],[22],[23],[24]. Outra vantagem corresponde à facilidade de implementação destes sistemas, sendo apenas necessário uma fonte e um recetor de fotões nos intervenientes da ligação quântica. O canal entre os dois pode ser de dois tipos, fibra ótica ou espaço livre e podem ainda coexistir com sistemas de comunicação com multiplexagem, como é o caso de sistemas *wavelenghth-division multiplexing (*WDM*)* [17], [20]. Acima de tudo, a segurança destes métodos de distribuição de chaves não incorre no risco de se tornarem obsoletos com o rápido avanço da tecnologia, comparativamente com os métodos tradicionais, como é o caso do esquema Diffie-Hellman [4].

3.4. Protocolos

Os protocolos QKD podem ser classificados conforme a modulação aplicada, codificação, descodificação e implementação física do canal quântico [20]. Estes são divididos em: Entanglement Based (EB), que faz uso das propriedades de emaranhamento de partículas quânticas e Prepare-and-Measure (PM), em que os fotões codificados são transmitidos de Alice até Bob [4]. Os protocolos quânticos podem ter ainda outra classificação possível, que é feita com base na forma como os fotões se encontram codificados. Nestes, a informação pode encontrar-se sob a forma de uma variável contínua (CV) ou discreta (DV) [6]. A classificação dos protocolos QKD está então organizada segundo a seguinte figura:

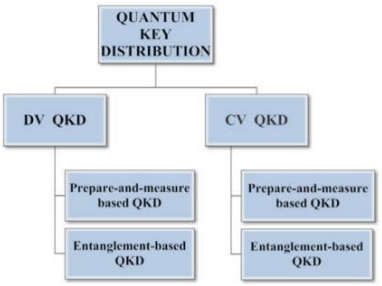


Figura 4: Classificação geral de métodos QKD [17].

Existem ainda mais dois tipos de protocolos, com base no *hardware* utilizado, que não serão considerados neste projeto. A saber, Device Independent (DI-QKD) e Measurement Device Independent (MDI-QKD), os quais surgem da necessidade de impedir ataques, ou *hacking*, devidos a imperfeições de *hardware*, especificamente ao nível dos emissores e dos recetores do sistema [6]. Os protocolos DI são do tipo EB e não pressupõem que, quer a fonte quer o detetor sejam confiáveis [16] e fazem uso de uma fonte única que envia *qubits* para ambos os intervenientes da ligação, que estão equipados com o seu respetivo recetor. Estes protocolos são imunes a ataques e a *hacking* quer na fonte quer no recetor. Contudo, a taxa de chaves atribuídas por unidade de tempo (*key rate*) resultante deste método é baixa mesmo para curtas distâncias e requer alta eficiência de deteção e medição [17]. Já os MDI são desenvolvidos para impedir ataques do lado da deteção e podem ser implementados com tecnologia atual [16], sem fazer uso das propriedades de *entanglement* dos fotões gerados. Estes são do tipo PM e requerem apenas um único detetor, como se encontra ilustrado na Figura 5.

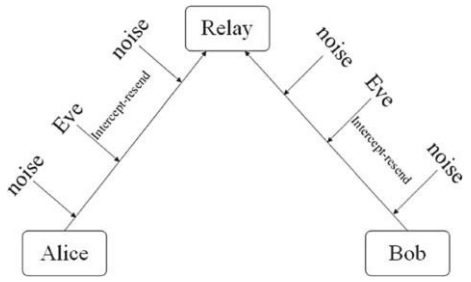


Figura 5: Diagrama de canal quântico de método MDI-QKD [25].

3.4.1. *Entanglement Based*

O primeiro protocolo QKD EB foi denominado de E91 e foi criado por Ekert em 1991 [26]. Este método consiste em produzir um par de fotões emaranhados para cada *bit*, com uso de uma fonte especial para o efeito, ou seja, um par de partículas cujas propriedades estão correlacionadas, ainda que distantes uma da outra. Para cada par gerado, o emissor (Alice) e o recetor (Bob) recebem um dos fotões, ficando cada um com um dos elementos do par. Alice escolhe uma base aleatória para interpretar o fotão e daí resulta um *bit* clássico. Esta medição afeta o elemento do par que se encontra em Bob, que escolhe uma base aleatória para a sua leitura, independente de Alice. De cada uma das leituras resulta um bit. Os dois *bits* obtidos podem não coincidir devido à aleatoriedade das bases, sendo que este método não abdica de nenhuma das fases de pós-processamento no canal público para averiguação dos *qubits* lidos com a mesma base por ambos os intervenientes e retificação de alguns *bits* de teste [4], [27].

3.4.2. *Prepare-and-Measure*

A alternativa ao método descrito consiste na transmissão de fotões sem uso das propriedades de *entanglement* da informação quântica. No método *prepare-and-measure*, Alice gera uma chave binária e codifica cada fotão de acordo com o bit gerado. Os *qubits* resultantes são enviados num meio quântico, ótico ou espaço livre, até Bob. À semelhança dos protocolos EB, após a geração e envio dos *qubits*, seguem-se as fases de pós-processamento. Comparativamente com os métodos EB, este tipo de protocolos atinge maiores valores de *key rate*, contudo, as distâncias operacionais são mais reduzidas [4].

3.4.3. *Continuous Variable*

Neste tipo de protocolos, a informação é codificada com base no campo eletromagnético dos fotões [6], [17]. Já a sua deteção é feita com base em técnicas de *homodyne and heterodyne*, dependendo do tipo de quadratura medido. É da leitura que advém o termo de variável contínua, uma vez que estas leituras projetam a fase e amplitude na quadratura do campo, originando assim valores de leitura contínuos. A interação de um Eve com o sinal quântico resulta em ruído gaussiano [20]. Estes protocolos atingem maiores *key rates* do que pelo método DV, mas apenas para distâncias pequenas. De facto, são até mais sensíveis a perdas no canal de transmissão, ou seja, possuem distâncias operacionais menores do que em DV-QKD. Contudo, apesar desta desvantagem, a sua implementação é mais fácil e barata do que para métodos de codificação discreta, uma vez que requerem componentes de comunicação convencionais [17].

3.4.4. *Discrete Variable*

Em DV-QKD, os fotões são tipicamente codificados na sua polarização, fase, ou tempo de chegada, assumindo valores conforme o valor do *bit* correspondente gerado inicialmente [6],[17]. A codificação é feita com o uso de bases aleatórias. Assim, como um potencial intruso não tem acesso às bases utilizadas pelo emissor, a leitura dos *qubits* traduz-se numa alteração dos que foram lidos utilizando uma base diferente, o que pode conduzir posteriormente à sua deteção. A medição dos *qubits* é feita também com recurso a bases aleatórias, pelo que não existe uma total correlação entre a informação dos dois intervenientes [20].

3.4.5. *Discrete Variable*

Este trabalho foca-se na simulação de protocolos do tipo *prepare-and-measure*, com utilização de codificação por variável discreta, mais especificamente, com codificação dos *qubits* com base em ângulos de polarização. Existem diversos protocolos deste tipo que resultam da conjugação destas duas classificações. Este trabalho focar-se-á concretamente em três em específico: BB84, SARG04 e KMB09. O funcionamento dos protocolos em questão será explicado de seguida.

3.4.5.1. BB84

Consiste na primeira classe de protocolos QKD, elaborado em 1984 por Charles Bennett e Gilles Brassard [12],[22],[28],[29]. A codificação dos *qubits* é feita num espaço bi-dimensional, que tanto pode ser obtida com o recurso à polarização dos mesmos ou no intervalo de tempo entre *qubits* sucedidos (*time-bin*) [19]. Contudo, como já foi mencionado anteriormente, neste trabalho considera-se apenas a codificação por via de polarização dos fotões transmitidos.

O transmissor codifica uma sequência de qubits por polarização de fotões, conforme a base diagonal ou retilínea, escolhida aleatoriamente para cada 0 ou 1. Tal polarização poder ser feita através da passagem de um feixe por, por exemplo, um filtro de polarização, ou um cristal de calcite. O feixe fica então polarizado conforme a orientação do aparelho usado. Neste protocolo, os fotões podem ser orientados segundo quatro direções, 0^o, 45^o, 90^o e 135^o, correspondentes a $|0\rangle$, $|+\rangle$ $|1\rangle$ e $|-\rangle$, respetivamente, em que o '0' digital corresponde a uma orientação de 0^o ou de 45^o e o '1' a 90^o ou a 135^o, como ilustrado na seguinte tabela:

Tabela 1: Polarização dos qubits segundo o protocolo BB84, considerando apenas representação em espaço de Hilbert com $\theta \in [0, \pi]$.

Tipo de Bases	0	1
+	→	↑
x	↗	↖

No canal público, na fase de *Shifting*, é então averiguado o conjunto de *qubits* que foram tratados com as mesmas bases de CC por cada casa, de modo a que só esses sejam considerados, seguido de uma retificação de alguns dos *bits* resultantes da leitura na fase de *Reconciliation* [10],[12]. Dado que a probabilidade de escolha de cada base é de $^1/_2$, em condições ideais, o número de *bits* obtidos no final do processo corresponde a cerca de $^1/_2$ do que foi gerado inicialmente por Alice. Um exemplo do funcionamento do protocolo nas várias fases do processo encontra-se esquematizado na figura seguinte:

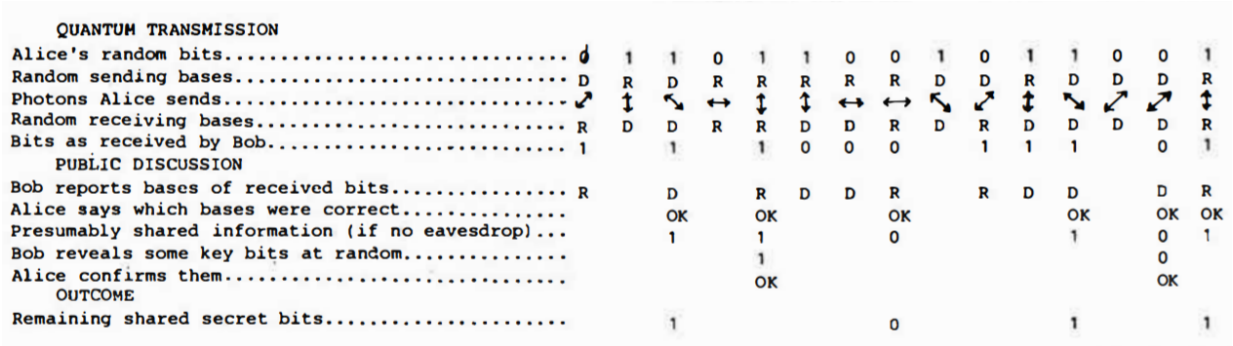


Figura 6: Exemplo das várias fases de QKD usando o protocolo BB84 *[10]*.

Na imagem do exemplo acima, após a confirmação das bases usadas e de Bob enviar alguns dos bits descodificados com as bases corretas, de forma a garantir que nenhum Eve intercetou a transmissão de fotões, Alice e Bob concluem que a chave a usar corresponde a 1011, presente na última linha da referida imagem.

Este protocolo serviu de base aos restantes protocolos mencionados neste trabalho e o seu protótipo foi desenvolvido com sucesso em 1989 por Bennet *et. al* [28]. A sua segurança foi demonstrada posteriormente, pois permite, pelo seu funcionamento detetar com elevada certeza a presença de um Eve no canal físico, uma vez que tal induz erros nas correlações entre as bases usadas na codificação e descodificação. Tem, contudo, algumas limitações físicas e não garante, por exemplo, a segurança perante outros tipos de ataque, como *photon-number splitting attack*, uma vez que na fase *shifting*, este protocolo partilha toda a informação necessária (bases) à obtenção da chave [24]. O funcionamento deste ataque em específico será desenvolvido em 3.5.

3.4.5.2. SARG04

Esta classe de protocolos é baseada em BB84, com algumas alterações na fase de pós processamento [24], [30]. São utilizados os mesmos estados quânticos, o que faz com que na prática, ao nível quântico os protocolos se comportem da mesma forma [31]. Os estados correspondem a $|\pm x\rangle$ e $|\pm z\rangle$ para 0's e 1's digitais, respetivamente. Após a receção dos fotões, é feita a leitura dos seus estados conforme a base escolhida pelo recetor, em que x e z correspondem aos eixos da esfera de Bloch, ilustrada na Figura 1. Assim, existem as seguintes equivalências das notações utilizadas neste protocolo com os estados descritos em 3.2: $|+z\rangle = |0\rangle$; $|-z\rangle = |1\rangle$; $|+x\rangle = |+\rangle$; $|-x\rangle = |-\rangle$.

Uma vez que utiliza os mesmos estados quânticos, é na fase de pós processamento que este protocolo se distancia de BB84, já que em vez dos intervenientes revelarem as bases usadas para cada bit (x ou z), o transmissor anuncia publicamente um dos quatro pares de estados não ortogonais, através do canal público, ou seja, representados por $A\pm,\pm$, que indicam o estados do *qubit* transmitido $\{|\pm x\rangle,|\pm z\rangle\}$. Por exemplo, se o transmissor anunciar $A+,+$ e o recetor tiver lido $|-z\rangle$, então este fica a saber que foi enviado $|+x\rangle$ e não descarta o *bit* correspondente da leitura do *qubit* em causa. Por outro lado, se a leitura do recetor coincidir com a base enviada, suponha-se uma leitura de $|+x\rangle$ ou $|+z\rangle$ e o par de bases enviada for de $A+,+$, nada pode concluir, e o bit é descartado. Com o procedimento descrito, a quantidade de bits que orecetor guarda tende para $1/4$, em vez de $1/2$ como em BB84. Este protocolo mostra-se mais robusto e especialmente resistente contra ataques, em especial contra *photon-number splitting attack* [24].

3.4.5.3. KMB09

Este protocolo foi desenvolvido por Khan *et. al.* em [19], onde se encontra toda a descrição do protocolo. Consiste em codificar cada bit com uma polarização de índice *i* arbitrário de entre as N polarizações possíveis, para '0' ou '1'. Alice deve codificar os fotões usando estados não ortogonais, ou variando aleatoriamente entre dois conjuntos de bases *e* e *f*, sendo que cada uma codifica os *bits* 0 e 1, respetivamente. Na figura seguinte encontram-se representadas as bases *e*, *f* e as bases que Eve deve utilizar para a sua leitura, *g*, para o caso N=2.

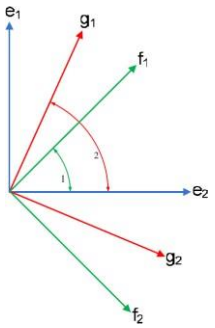


Figura 7: Bases utilizadas por Alice, Bob e Eve, para KMB09 utilizando um total de N=2 índices para cada base [19].

Retira-se da Fig.7 a equivalência entre os estados: $e_2 = |0\rangle$, $e_1 = |1\rangle$, $f_1 = |+\rangle$ e $f_2 = |-\rangle$.

Para maximizar o erro introduzido por Eve, Alice e Bob devem escolher uma base com um ângulo de polarização de $\varphi_1 = \pi/4$, o que induz uma taxa de erro de 25% independentemente da escolha de Eve para φ_2. É de notar que no caso N=2, o protocolo apresenta o mesmo funcionamento de SARG04 [21].

Após o envio de cada $|e_i\rangle$ ou $|f_i\rangle$, o recetor mede o estado de cada fotão variando arbitrariamente entre ambas as bases *e* e *f*. Para um dado *qubit*, o uso da mesma base que Alice resulta numa leitura correta, e o uso de uma base diferente resulta numa leitura errada, ambas associadas a um determinado índice lido. Na fase de pós processamento, no canal público, Alice partilha os índices *i* utilizados, de forma que Bob guarde os bits para os quais obteve um índice diferente, pois caso obtenha o mesmo índice, nada pode concluir. A seguinte tabela demonstra o modo como Bob obtém a *raw key* com base nas suas leituras e nos índices anunciados por Alice, para um total de índices possíveis de N=2.

Tabela 2: Interpretação de Bob com base na sua medição e índices anunciados por Alice, adaptado de [19].

Index announced by Alice	States measured by Bob			
	$\|e_1\rangle$	$\|e_2\rangle$	$\|f_1\rangle$	$\|f_2\rangle$
1	×	1	×	0
2	1	×	0	×

Na tabela acima, conforme a leitura de Bob e a receção dos índices utilizados, este pode concluir que Alice enviou '1', '0', ou nada pode concluir: 'x'. Para Bob obter um *bit* correto tem que utilizar uma base diferente da que foi usada por Alice e obter um índice diferente do que é anunciado. Após retificação, pela partilha de alguns *bits* de teste, é gerada a chave secreta a utilizar.

Neste protocolo, Eve introduz dois tipos de erros distintos [21]. Um dos métodos de deteção de um Eve no canal quântico deriva da medição de um *index transmission error* (ITER), que ocorre quando é preparado um fotão em $|e_i\rangle(|f_i\rangle)$ e Bob lê $|e_j\rangle(|f_j\rangle)$, com $i \neq j$. Selecionando e enviando os índices de fotões aleatórios que não resultaram na chave secreta, é possível que Bob obtenha os estados codificados por Alice e, com essa informação e com o resultado das suas medidas, calcule o valor de ITER da respetiva transmissão. Por exemplo, para N=2, o ITER mínimo correspondente é de 25%, para N=4 é de 37,5% e aumenta assim por diante com o incremento de N. Esta deteção pode também ser feita com

base no valor de *qubit error rate* (QBER). Para tal, executam um processode retificação semelhante ao que foi descrito anteriormente, comparando abertamente alguns bits da *raw key* obtida. Não existe correlação direta entre os valores de ITER e QBER, contudo alguns trabalhos já propuseram uma modificação no protocolo de modo que haja uma dependência linear entre os dois valores de erros [21].

Uma das grandes vantagens deste protocolo, além da elevada segurança perante alguns tipos de ataques MITM, que se traduz, no entanto, numa diminuição de eficiência, é a possibilidade de tolerar mais ruído no canal de transmissão do que os restantes protocolos mencionados anteriormente, e, como tal, permitir um aumento nas distâncias de comunicações possíveis [19].

3.5. Limitações dos Métodos QKD

Apesar de os métodos QKD serem bastante promissores, existem algumas limitações nas suas implementações. Mesmo na ausência de um intruso, um sistema QKD está sujeito a certos níveis de ruído [18] e, na prática, tais limitações também desafiam a segurança destes métodos, teoricamente seguros, com o surgimento de novos tipos de ataques [6], que dizem respeito ao facto de nenhuma parte de *hardware* utilizado ser ideal e existirem várias imperfeições nos dispositivos [19], [11].

Neste trabalho consideram-se os casos práticos de imperfeições nas fontes de fotões, perdas e ruído no canal de transmissão e eficiência do recetor, que constituem os principais fatores de perdas de informação em sistemas QKD e consequente aumento do QBER das ligações [28].

3.5.1. Emissor

Os tipos de protocolos descritos acima em 3.4.5, requerem idealmente o uso de fontes de fotões únicos (*single photon sources*), em que a cada *qubit* corresponde um único fotão. Contudo, devido a limitações tecnológicas, a implementação deste tipo de fontes perfeitas ainda está longe de ser uma realidade. Em alternativa, experimentalmente, são utilizadas *heavy attenuated laser sources* [29]. Esta alternativa produz pulsos fracos coerentes (*weak coherent pulses* – WCP), descritos por estados coerentes conforme a polarização escolhida [30],[32]. Este tipo de fontes está longe de ser ideal e substituir completamente as fontes de fotões únicos ideais, visto que há uma grande probabilidade de existir menos de um fotão por pulso [7].

Em DV-QKD, com *qubits* gerados por codificação da polarização dos fotões, cada WCP encontra-se no estado simbolizado por $\sqrt{\mu}e^{i\theta}$. O número médio de fotões por pulso corresponde a μ (intensidade do pulso) e é dado por uma distribuição de Poisson [24]. A probabilidade de um pulso conter n fotões, dada uma média de μ fotões por pulso é de

$$p_n(\mu) = e^{-\mu} * \frac{\mu^n}{n!}$$

Ou seja, existe uma probabilidade p_0 de um pulso não conter nenhum fotão, p_1 de conter um único fotão e assim por diante. Desta forma, resulta que, para valores de μ inferiores a 1, a maior parte dos pulsos não é constituída por nenhum fotão, o que limita o funcionamento dos protocolos, especialmente quando se tem em conta as perdas no canal quântico [34]. Por outro lado, pelo facto de haver alguns pulsos com mais do que um fotão, um Eve pode efetuar ataques em que, ao invés de ler os *qubits*, retém parte deles, não estando assim limitado pelo *no-cloning theorem*, como é o caso do ataque PNS [24], [32]. Na figura seguinte encontram-se as várias probabilidades de ocorrência de fotões por pulsos conforme a média μ.

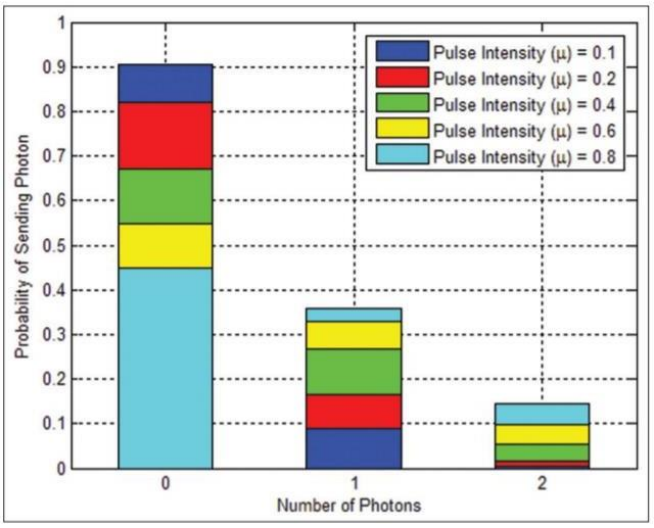


Figura 8: Relação entre a probabilidade de enviar 0, 1 ou 2 fotões por pulso com vários valores de μ [31].

3.5.2. Canal Quântico

O comprimento do canal quântico utilizado na distribuição de chaves é neste momento uma das grandes limitações destes métodos. À semelhança de todas as transferências de informação, este canal está sujeito a perdas e ruído, além de outros fatores como o *decoherence* que corresponde à perda de informação quântica devido por exemplo a variações no campo eletromagnético ou radiação. Assim, é dado um limite superior à quantidade de informação que pode ser transmitida de forma confiável ao longo de um canal quântico não ideal, no qual estes fenómenos ocorrem [35]. Este trabalho foca-se sobretudo na transmissão de *qubits* ao longo de um meio ótico, o mais indicado para um cenário de *smart grid*. Além de diminuir a probabilidade de sucesso dos esquemas implementados, o ruído pode também dar oportunidade a um potencial *eavesdropper* de disfarçar as perturbações da sua presença, ficando indistinguíveis do ruído na ligação, condicionando assim a segurança das implementações QKD [36].

3.5.2.1. Atenuação

Tipicamente, todos os sistemas QKD estão limitados ao nível da taxa de atribuição de chaves atingível, devido à distância possível nas ligações quânticas realizadas. Tal facto deve-se, entre outros fatores, ao decaimento espontâneo do sinal, devido à perda de fotões por absorção do meio, o que faz com que a informação se perca na transmissão. Em redes de fibras óticas, a atenuação da luz em fibras padrão, para um comprimento de onda de $1550\ nm$ é de $0.2\ dB/km$ ou $0.16\ dB/km$ em fibras de perdas ultrabaixas, recentemente desenvolvidas [6]. Em [37] é projetada uma rede QKD de acordo com o seguinte modelo de taxa de transmissão de *qubits* em função do comprimento do canal, L

$$R(L) = R_0 * 10^{-\alpha\frac{L}{10}}$$

onde $R_0 = 50\ kbit/s$ e α corresponde à atenuação média sofrida na transmissão pela fibra, que é considerada como $0.25\ dB/km$. Este modelo mostra que a informação transmitida decresce exponencialmente com a distância e assegura uma transmissão de *qubits* a uma taxa adequada até uma distância de 100 km. A partir desse patamar, $R(L)$ decresce acentuadamente [37].

O perfil típico da taxa de transmissão em função da distância encontra-se representado na seguinte figura:

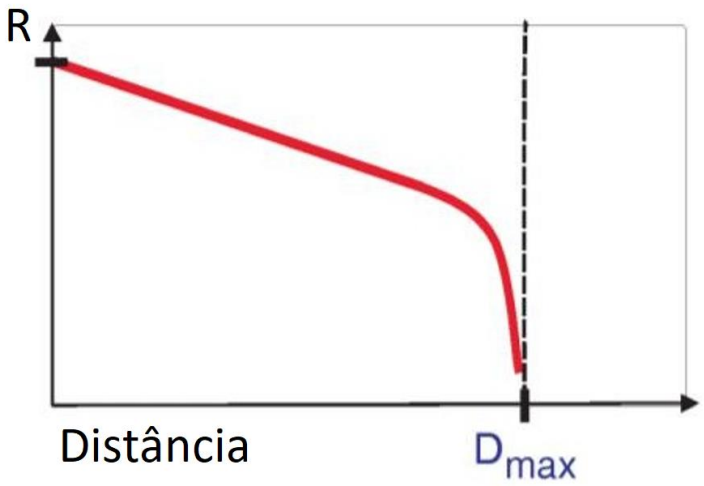


Figura 9: Perfil típico da taxa de transmissão de informação num canal quântico [38].

Esta limitação das ligações ponto a ponto numa rede QKD, pode ser contornada usando *quantum repeaters* [38], quantum *relays*, ou *ground-to-satellite* QKD [6], [20], que não serão contemplados neste trabalho. Em 3.5.3 será descrito um modelo matemático que calcula a probabilidade de um recetor ler um *qubit* recebido, contemplando as características da fibra, a distância da ligação e ainda a eficiência do recetor.

3.5.2.2. Ruído de Despolarização

Os estados de polarização dos *qubits* estão bem definidos num certo quadro de referência. Contudo, esses estados são facilmente alterados ao longo da transmissão por influência de flutuações térmicas, vibrações e imperfeições da fibra utilizada para a sua transmissão [30], [36], [39]. Resulta assim ruído de despolarização, também chamado de ruído de rotação, cuja consequência é os estados dos *qubits* transmitidos poderem não coincidir com os que são recebidos, o que leva a uma taxa de erro [22].

Existem vários modelos para descrever este fenómeno, como o de [29] em que o canal que provoca esta despolarização dos fotões, chamado canal de despolarização ou canal de Pauli, tem o funcionamento que se descreve de seguida: cada *qubit* é caracterizado por ter uma probabilidade p de ser alterado e a respetiva probabilidade $1 - p$ de se manter intacto [12]. Supondo que o estado inicial do *qubit* em causa é caracterizado pela matriz ρ, que o representa no espaço de Hilbert, então o seu estado à saída do canal de despolarização é dado pela seguinte expressão:

$$\sigma(\rho) = (1 - 3p)\rho + \rho(X\rho X + Y\rho Y + Z\rho Z)$$

onde X, Y e Z representam as matrizes de Pauli mencionadas em 3.2. Caso um *qubit* em causa seja sujeito a ruído suficiente, a sua polarização é alterada de tal forma que a sua leitura se traduz num *qubit* errado, um fenómeno denominado de *bit-flip*. Num canal de comunicação clássico, este é o único tipo de erro possível, o que pode levar à permutação de uma equivalência quântica de um *bit* de 0 para 1 e vice-versa. Contudo, em canais quânticos existe também o *phase-flip* em que um *qubit*, caracterizado por um operador bidimensional $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$, sofre uma alteração para $|\varphi'\rangle = \alpha|0\rangle - \beta|1\rangle$ [23].

Outro modelo possível é o de [25], que descreve um ruído constante a todos os *qubits* ao longo do tempo, denominado de ruído coletivo. O ruído coletivo é um fenómeno que se deve ao facto de, usualmente o tempo de intervalo entre fotões ser muito menor do que a variação de flutuação do ruído, pelo que vários fotões muito próximos espacialmente são afetados da mesma forma pelo mesmo ruído [36]. Os estados à saída do canal de despolarização são dados pela multiplicação das matrizes dos vários *qubits* pela seguinte matriz:

$$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

onde θ resulta da expressão $\varepsilon = sin^2(\theta) <=> \theta = \arcsin(\sqrt{\varepsilon})$ sendo ε um parâmetro independente com valores entre 0 e 1. Quando ocorre despolarização, as várias probabilidades de envio de um *qubit* e leitura nos vários estados, ignorando a base de leitura escolhida, dependem do parâmetro θ e encontram-se na seguinte tabela:

Tabela 3: Tabela com as probabilidades de leitura dos vários estados de polarização intercetada com a probabilidade de ser enviado um dado estado, dependendo dos valores de θ [25].

$A(B)/R$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	$\frac{\cos^2\theta}{8}$	$\frac{\sin^2\theta}{8}$	$\frac{1-\sin 2\theta}{16}$	$\frac{1+\sin 2\theta}{16}$
$\|1\rangle$	$\frac{\sin^2\theta}{8}$	$\frac{\cos^2\theta}{8}$	$\frac{1+\sin 2\theta}{16}$	$\frac{1-\sin 2\theta}{16}$
$\|+\rangle$	$\frac{1+\sin 2\theta}{16}$	$\frac{1-\sin 2\theta}{16}$	$\frac{\cos^2\theta}{8}$	$\frac{\sin^2\theta}{8}$
$\|-\rangle$	$\frac{1-\sin 2\theta}{16}$	$\frac{1+\sin 2\theta}{16}$	$\frac{\sin^2\theta}{8}$	$\frac{\cos^2\theta}{8}$

Ambos os modelos descritos, [25] e [29], só são possíveis para protocolos que utilizem *qubits* com quatro polarizações possíveis, devido às dimensões das matrizes de Pauli e da matriz U, respetivamente. Dessa forma, a sua aplicabilidade não é possível em protocolos como por exemplo KMB09 com N=4, pois tem um total de 8 estados de polarização. Contudo, estes protocolos com 6 ou até 8 estados já se mostraram mais robustos ao ruído [18].

Desde o primeiro método de correção de erros quânticos, desenvolvido por Shor em 1995 [35], vários esquemas já foram propostos para a correção destes e doutros tipos de erros. Como exemplo, códigos de correção de erros quânticos para ambas as situações descritas acima estão em [23], [29], entre outras formas de correção, que consideram ruído coletivo [22].

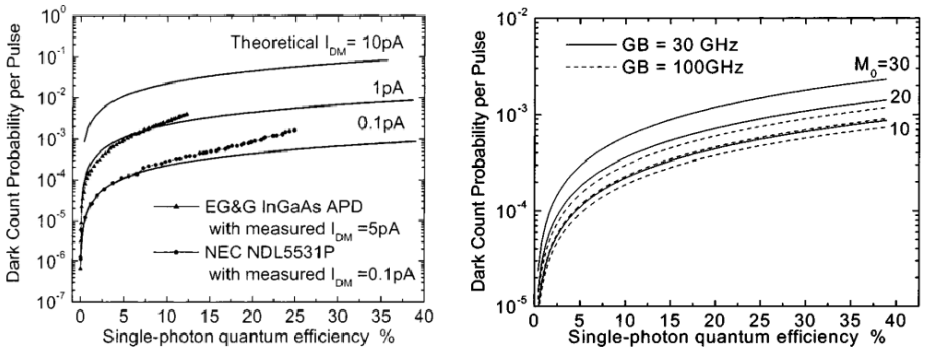
3.5.3. Recetor

Os dispositivos de deteção são os mais vulneráveis em relação a ataques num sistema QKD, uma vez que nenhum método de deteção dos protocolos *standard* é totalmente confiável devido a imperfeições e *hacking* [17]. A taxa de transmissão de *qubits* obtida, depende essencialmente do desempenho do detetor utilizado. Para atingir a taxa pretendida, é necessária uma alta eficiência e um intervalo de tempo de espera até ser possível detetar outra receção (*dead time*) curto [6]. Neste trabalho foi utilizado um modelo para calcular a taxa de *raw detection*, ou seja, a probabilidade de o recetor detetar pelo menos um fotão por pulso enviado, utilizando pulsos fracos, descrita em [24].

$$R_{raw}(\delta) = \sum_{n \geq 1} p_n(1 - (1 - \eta_{det}\eta_\delta)^n) \cong \eta_{det}\eta_\delta\mu$$

em que: η_{det} corresponde à eficiência do recetor, tipicamente 10% nos comprimentos de ondas de telecomunicações *standard* utilizados; η_δ é a atenuação devido a perdas na fibra de comprimento l, dada por $\eta_\delta = 10^{-\frac{\delta}{10}}$, em que $\delta = \alpha l$, sendo α a atenuação média da fibra dada em dB/km; μ é a intensidade média do pulso; p_n é a probabilidade de ocorrerem n fotões por pulso, ambos descritos em 3.5.1. A aproximação da expressão acima só é válida caso $\eta_{det}\eta_\delta\, p_n n \ll 1$, para qualquer valor de n, o que se verifica sempre no contexto de pulsos fracos.

Outro fenómeno que caracteriza o bom funcionamento dos detetores é a ocorrência de uma baixa probabilidade de *dark counts*, por unidade de tempo, na ausência de um sinal. Um *dark count* vulgarmente ocorre quando um dado fotorrecetor fornece uma leitura na presença de um pulso vazio. Este fenómeno ocorre, entre outros aspetos, devido a flutuações térmicas internas ou externas ao detetor e podem induzir uma taxa de erro considerável [7], [33] e está muito relacionado com o valor de corrente nas células de receção na ausência de estímulo, com a eficiência e ganho do fotorrecetor. A ocorrência deste fenómeno está muito ligada à eficiência do fotorrecetor utilizado, como ilustra a seguinte figura, para vários valores de *dark current* primária e de ganho, em função da eficiência de leitura, para recetores de fotão único:



(a) *(b)*

Figura 10: Probabilidade de ocorrência de um dark count na receção, para diferentes valores de (a) dark current e (b) ganho, em função da eficiência do fotorrecetor [40].

3.6. Ataques

Como já foi mencionado ao longo deste trabalho, QKD é um método bastante seguro de distribuição de chaves que, aliado a um método de encriptação de chaves simétricas, proporciona trocas de informação teoricamente seguras. Contudo, apesar da leitura do canal quântico por parte de Eve ser relativamente fácil de detetar, surgem vários tipos de ataques que os protocolos, metodologias e topologias de rede devem contemplar, por forma a manter este método seguro. Existem vários tipos de ataques quânticos, entre os quais *Intercept-and-resend attack*, *photon-number-splitting attack* (PNS), *Trojan horse attack*, *phase-remapping attack*, *partially random phase attack*, *on the source and detector-efficiency-mismatch based attack*, *detector control attack*, *side channel attack*, *denial of service*, entre outros [41].

Uma forma de evitar totalmente ataques do tipo man-in-the-middle, é a utilização de uma chave pré estabelecida para troca de informação do canal clássico utilizado pelo sistema QKD entre os dois intervenientes, Alice e Bob [42]. Tal pode ser feito utilizando um código de autenticação Wegman- Carter message authentication code (MAC), que constitui o método tradicional de autenticação em QKD [43]. Estes métodos de autenticação consistem em associar um pequeno conjunto de bits de retificação à mensagem transmitida, cuja autenticidade é verificada no recetor através de um algoritmo [44].

3.6.1. *Intercept-and-Resend*

Trata-se do mais simples tipo de ataque *Man-in-the-Middle* ao canal quântico. O seu funcionamento baseia-se, resumidamente em Eve ler os fotões enviados por Alice, escolhendo para tal uma base aleatória e encaminhar o resultado dessa leitura para Bob, simulando que foram enviados diretamente por Alice e que a comunicação ocorreu normalmente [19],[42]. Para obter conhecimento dos *qubits*, Eve deverá utilizar o mesmo procedimento que Bob para a leitura dos mesmos [12]. O facto de Eve fazer esta leitura direta dos *qubits* no canal quântico pode induzir um erro na mensagem transmitida. À semelhança do recetor Bob, caso Eve utilize a base correta na leitura de um dado *qubit*, este é lido de forma correta e consequentemente, é retransmitido para Bob um *qubit* igual ao que foi envidado por Alice. Se porventura a base utilizada por Eve não for a correta, é introduzido um erro na mensagem que Bob recebe. Este erro introduzido, fisicamente, é diferente do que ocorre devido à presença de ruído [28].

O método mais simples de deteção de ataques *intercept-and-resend* em sistemas QKD com quatro estados é através da medição da percentagem de erros da chave obtida, através do cálculo do QBER resultante da análise dos *bits* de teste trocados [11]. O QBER aceitável do resultado deste ataque, em condições ideais, deve em teoria ser menor que 25%, por forma a detetar o ataque. Um Eve pode atingir um QBER baixo, atacando apenas uma fração dos *qubits* enviados [31].

3.6.2. *Photon-Number Splitting*

Este é o ataque potencialmente mais letal, pois é caracterizado pelo facto de Eve não ler diretamente os *qubits* enviados. Em vez disso, começa por contar o número de fotões de cada *qubit*, sendo que, dos n fotões que constituem o *qubit* enviado por Alice, Eve isola um. Esse fotão é então armazenado em memória quântica e fica concluída a parte quântica do ataque. De seguida Eve necessita de aceder à troca de informação no canal público, por forma a saber como elaborar a correta leitura dos *qubits.* No caso de DV-QKD com uso de polarização dos fotões, Eve deve aguardar pela divulgação das bases utilizadas, ou pela correção das bases utilizadas por Bob, conforme o protocolo utilizado, pois só assim consegue garantir que poderá fazer a leitura correta da polarização dos fotõesarmazenados. Desta forma, Eve fica a conhecer vários elementos da chave sem introduzir nenhum erro na mensagem recebida por Bob. Contudo, na prática, Eve deve de alguma forma garantir que a taxa média de fotões recebidos por Bob não se afasta da gama dos valores esperados, pois tal pode ser monitorizado para a deteção deste tipo de ataque [24], [32]. Para obter uma maior resiliência à obtenção de *bits* por Eve na presença deste ataque, uma possível opção é o uso de *decoy states*, que corresponde a uma codificação que também faz uso de valores de amplitude [25], [34], [35]. Já com SARG04 e KMB09 tal não é necessário, pois devido à informação que é partilhada no canal público, verifica-se que um atacante obtém menos *bits* do total de *qubits* transmitidos.

3.6.3. *Denial of Service*

No contexto de ligações QKD o objetivo de um ataque do tipo *Denial of Service* é impedir o seu funcionamento e consequente atribuição de chaves. Uma das formas de o fazer é por introdução de erros no canal de transmissão quântico, de forma que o número de erros aumente para valores intoleráveis, e como tal, não seja possível a atribuição de chaves, que consequentemente, impede a troca de mensagens. Estes erros podem ser introduzidos por duas formas, devido a um *eavesdropper* no canal quântico ou devido a ruído. Por motivos de segurança devem ser sempre considerados consequência de *eavesdropping*, uma vez que são indistinguíveis [25]. Para tal, Eve necessita de acessofísico ao canal de transmissão quântico, o que é detetável. O efeito deste ataque numa rede de larga escala pode ser mitigado caso as transmissões afetadas sejam redirecionadas. Outro método, que não será considerado, consiste em Eve iniciar uma ligação de elevado ruído e consequente taxa de troca de chaves baixa, ao ponto de não ser possível a atribuição de chave. Enquanto esta sessão estiver ativa, um utilizador legitimo não pode receber nenhuma chave proveniente de Alice, constituindo assim um Denial of Service [43].

3.7. Encriptação

A atribuição de chaves para posterior encriptação de mensagens é o objetivo final das ligações QKD, como já foi mencionado, deforma que apenas utilizadores autorizados possam aceder à informação trocada. Nesta secção serão explicados os dois principais tipos de encriptação que podem constituir uma solução ao nível de segurança numa *smart grid*. Como foi explicado em 3.2, tais métodos de encriptação resultantes de métodos QKD são do tipo chave simétrica, pelo que serão estudados os métodos Advanced Encryption Standard (AES) e One-Time-Pad (OTP), sendo que existem muitos outros.

3.7.1. *Advanced Encryption Standards* (AES)

Corresponde ao método de encriptação simétrica mais utilizado atualmente. É baseado num sistema de rondas sucessivas, com substituições e permutações dos *bits* da mensagem em causa, que funciona em blocos com variações no seu tamanho de 128, 192 e 256 *bits*. O seu funcionamento consiste inicialmente em dividir toda a mensagem binária em blocos de 128, 192 ou 256 *bits*, conforme o tipo de AES utilizado. Cada bloco está sujeito a sucessivas rondas com quatro operações, são elas: (i) subtração não linear de cada *byte*, segundo uma tabela definida (S-Box), (ii) alteração da posição das linhas dos blocos, (iii) multiplicação de cada coluna por uma matriz pré-definida, e finalmente (iv) em que é feita uma operação de XOR entre o bloco resultante das três operações anteriores e a chave do mesmo, em que a chave utilizada consiste no resultado da codificação do bloco anterior [46].

Para os sistemas de encriptação que usam QKD, AES pode constituir uma solução mais viável para codificação de mensagens, pelo facto de utilizarem a chave atribuída de uma forma mais eficiente. Dessa forma, requerem um menor número de *bits* na chave resultante utilizada na encriptação, comparativamente com OTP, o que possibilita taxa de *qubits* mais baixas [43]. Contudo, apesar de utilizar menos *bits* na sua chave, é possível atingir uma elevada segurança utilizando QKD com este tipo de codificação, quer em ligações ponto a ponto quer num ambiente de rede [38].

3.7.2. *One-Time Pad* (OTP)

A elevada segurança deste método advém do facto de não reutilizar parte ou a totalidade da chave para diferentes mensagens enviadas, chaves essas que têm o mesmo comprimento, em *bits*, que a própria mensagem [4],[11]. Como já foi referido ao longo deste trabalho, este é o método considerado como preferencial num cenário de codificação por chave simétrica numa rede *smart grid*, em virtude da sua simplicidade computacional e elevado grau de segurança. Contudo, como foi referido em 3.7.1, requer a utilização de chaves com um maior número de *bits*, o que implica uma maior eficiência do protocolo de atribuição de chaves utilizado.

4. Objetivo do Projeto

Este trabalho tem como objetivo a simulação de métodos PM DV-QKD com uso de estados de polarização de fotões como método de codificação dos *qubits* transmitidos. O simulador elaborado procura sobretudo avaliar a segurança e eficiência deste método QKD para três protocolos distintos, BB84, SARG04 e KMB09, com quatro e oito estados, todos descritos anteriormente. Funciona num contexto específico de rede *smart grid* de uma zona, com nós estáticos, que será descrito de seguida em 5.3. Para simular o cenário em questão faz-se uso do *framework* Mosaik [47], onde é sobreposta a comunicação na rede entre cada casa e o Centro de Controlo (CC), baseado no método utilizado em Quantum-Sim [2]. Para tal simula-se um ambiente de envio de leituras de *smart meters*, alocados em cada casa da rede, codificadas por chaves atribuídas por QKD. A atribuição de chaves ocorre na presença de dois tipos de ataques: *intercept-and-resend*, os ataques mais comuns e que, segundo a literatura, contra os quais estes protocolos são bastantes eficazes, bem como ataques PNS, considerados como os ataques mais promissores contra estes métodos no futuro. O objetivo final de cada simulação é enviar as várias leituras de *smart meter* encriptadas pelo método OTP, utilizando a chave resultante do processo QKD. Para uma simulação mais elaborada, tudo isto é avaliado não só em condições ideais, mas também na presença das limitações práticas que estes métodos têm que ultrapassar no seu funcionamento, também descritas no Capítulo 3. Considerando todos estes fenómenos, é então necessário avaliar os resultados obtidos com o objetivo de obter os requisitos impostos aos vários elementos do canal quântico, necessários ao bom funcionamento dos protocolos e à sua resiliência à presença destes ataques. Tais requerimentos dizem respeito ao tamanho mínimo de chave para cada protocolo, número de *bits* de teste possíveis, percentagem de *bits* de teste incorretos aceitáveis nadeteção de um erro, parâmetros de ruído aceitáveis e intensidade média dos fotões transmitidos, por forma a maximizar a eficiência do método sem comprometer a segurança perante ataques PNS. Em última análise, pretende-se fazer uma avaliação da viabilidade deste método QKD, perante todos os fenómenos mencionados, no contexto de rede simulado e os modelos matemáticos considerados, que serão elaborados em 5.3.

5. Contexto do Trabalho

Nesta secção é descrito o contexto de simulação utilizado. Começa-se por uma breve menção ao *framework* utilizado bem como ao programa que inspirou este projeto e no qual este se baseou, seguido de uma explicação da rede considerada no programa. Além disso, é descrito o funcionamento do método QKD considerado, as várias características consideradas nas ligações quânticas e os parâmetros de simulação utilizados para a obtenção de resultados.

5.1. Mosaik

O Mosaik é um simulador de ambiente de *smart grids*, elaborado na linguagem *python* [3]. O *software* permite a criação de um cenário de rede ao nível local, onde são associados vários simuladores de elementos de *smart grid*, tais como uma fonte, casas e painéis fotovoltaicos, bem como a interação entre os mesmos, sob a forma de eventos discretos. Permite também o uso de um simulador que proporciona uma visualização *web* da rede e respetivos parâmetros de potência nos vários nós e elementos da rede. O Mosaik permite também a integração de mecanismos de controlo sob a forma de atuadores e controladores de supervisão, bem como a adição de eventuais simuladores [47]. É neste ambiente que são adicionadas todas as ações necessárias para implementar QKD para a implementação de encriptação das comunicações entre as casas e o Centro de Controlo (CC) da rede, para além de todas as funcionalidades de simulação de fluxo energético que já o constituem.

5.2. Quantum-Sim

A solução criada é baseada no funcionamento do Quantum-Sim, um simulador de distribuição de chaves quânticas em cenário de *smart grid* desenvolvido por Lardier et. al. (2019) [2]. Este simulador de distribuição de chaves quânticas *open-source* é baseado em *python* e funciona sob a forma de eventos discretos sobre o *framework* Mosaik, seguindo a arquitetura representada na imagem seguinte:

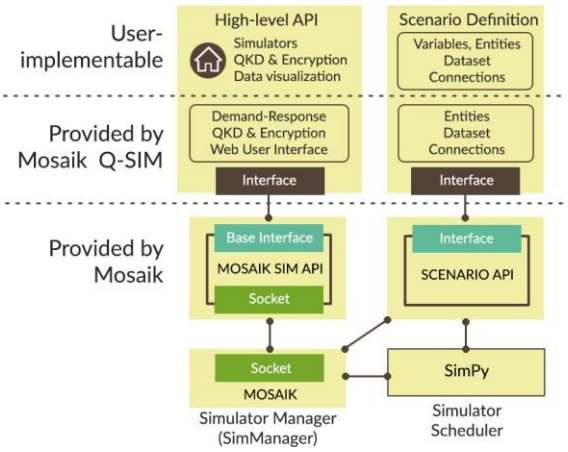


Figura 11: Arquitetura Quantum-Sim [2].

Consiste então numa plataforma de co-simulação para uma rede elétrica local de reduzida voltagem que simula a distribuição de chaves quânticas por parte de um CC às várias casas da rede, que a cada pedido enviam o seu consumo codificado com as chaves quânticas atribuídas. Contempla a implementação de três protocolos QKD distintos: BB84, SARG04 e KMB09, bem como dois métodos de encriptação das mensagens.

O Quantum-Sim serviu de inspiração para a elaboração deste trabalho, originalmente planeado como uma continuação do mesmo. No entanto, rapidamente se verificou que tal não era possível. Foi desenvolvido um simulador de um cenário de QKD aplicado a uma *smart grid*, tendo como ponto de partida a arquitetura desenvolvida em [2]. Para tal elaborou-se todo o código relativo à simulação dos métodos de atribuições de chaves, tais como as fases de funcionamento dos protocolos considerados, simulação de ataques e das consequências das limitações ao nível do *hardware* utilizado em implementações práticas do tipo de QKD considerado.

5.3. Contexto de Rede Utilizado

A rede utilizada consiste em 37 nós, dispostos em 4 ramos distintos, cada um com ligação a uma casa. Considera-se que cada casa contém um medidor inteligente (*smart meter)* que comunica a um CC o seu próprio consumo periodicamente, em intervalos de 15 minutos. O CC encontra-se a uma distância entre 1 e 9 km da zona residencial e está encarregue de distribuir chaves quânticas pelas casas, de modo que estas possam encriptar o valor dos seus consumos e transmiti-los de forma segura. A figura seguinte consiste na topologia da rede ilustrada no visualizador Web da plataforma Mosaik. Por motivos inerentes ao programa Quantum-Sim, uma das casas que constitui a rede não está presente no processo QKD sendo que uma das casas não inicia troca de mensagens, um erro que não foi corrigido, pois não foi considerado uma prioridade.

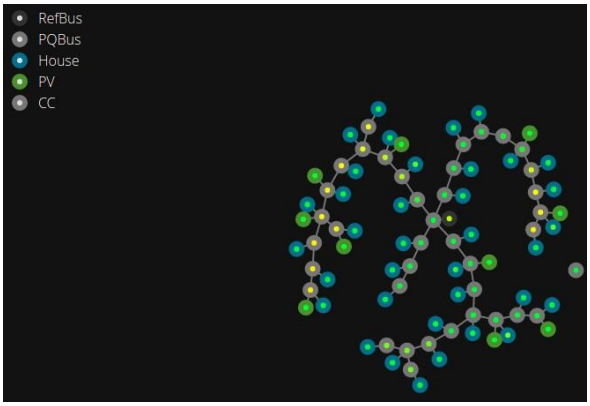


Figura 12: Representação da rede considerada na simulação.

Na figura acima, como o CC não faz parte da rede de energia, encontra-se separado da mesma, uma vez que o visualizador Web do Mosaik não contempla as comunicações na rede. Na rede contemplada existe também a hipótese de haver vários painéis solares ligados arbitrariamente a cada casa. Tais painéis em nada afetam o funcionamento da simulação do canal de comunicação da rede e servem apenas para a simulação da rede elétrica no Mosaik.

A forma como a rede se encontra disposta não afeta diretamente o funcionamento da distribuição de chaves quânticas, uma vez que, aos olhos do simulador, cada casa se encontra ligada diretamente ao CC. Em condições reais, a topologia da rede afeta a *key rate* possível para cada casa [37], na medida em que a taxa máxima de informação em cadaligação depende da forma como os elementos da rede estão organizados. No entanto, nesta simulação, a informação não é reencaminhada pelos vários nós até atingir o destinatário, além de que não foi possível alterar a quantidade de informação transmitida nos canais entre cada casa e o CC, em função do tempo.

Até à data, o uso de ligações QKD está um pouco limitado a estas ligações *end-to-end*, apesar de serem pouco práticas e mais dispendiosas, especialmente com a escalabilidade da rede em causa [38]. No entanto, num contexto objetivo de simulação de cada ligação simples dos vários canais quânticos de uma rede de pequena escala, é o mais indicado. Também no contexto do funcionamento do Mosaik é mais prático. Além disso, tal representaria, numa possível implementação real desta rede, uma melhoria na segurança da mesma, uma vez que o número de locais onde é possível efetuar um ataque é reduzido, uma vez que não é necessário garantir que todos os nós da rede são confiáveis, o que diminuiria não só o tipo de tipo de ataques possíveis como a probabilidade de ocorrerem. Além disso, um ataque numa ligação só afeta o canal atacado, enquanto num contexto clássico de rede, tal forneceria informação acerca das comunicações de todas as casas que partilhariam essa ligação em causa. Os contextos dos dois ataques simulados são idênticos no que se refere à sua localização, que é considerada como adjacente ao CC.

6. Metodologia

Como mencionado no Capítulo 4, foi elaborada uma simulação do processo de QKD utilizando codificação DV por polarização dos fotões em quatro e oito estados e método PM. O canal corresponde a uma fibra ótica convencional. Para este método, a implementação com mais sucesso é com uso de encriptação de *qubits* através das fases dos mesmos [45]. Embora em [17] se conclua que para a implementação de QKD em *smart grids,* o método mais indicado é MDI-QKD, neste trabalho não são considerados ataques no *hardware,* quer do emissor quer do recetor. Dessa forma, optou-se pelo método PM direto entre os intervenientes, ao contrário do esquema da Fig. 5, que reduz a complexidade e o número de cenários possíveis.

A distribuição de chaves quânticas está dividida em vários passos, descritos como estados de funcionamento, descritos em pormenor na Tabela 4, executados a cada passo do simulador das casas da rede, HouseHoldSim, e do Control Center. O processo pode ser simulado utilizando os três protocolos mencionados, para um número variável de *bits* por chave gerada ao longo de várias horas de simulação. Cada demanda de chaves ocorre por omissão a cada 15 minutos e é inicializada em bloco pelas casas, ao enviarem todas para o Control Center o valor 1, que sinaliza o pedido de atribuição de chaves. O centro de controlo recebe o pedido, gera uma chave binária aleatória e codifica-a conforme o protocolo utilizado, originando assim *qubits*.

Os *qubits* enviados através de canais quânticos às respetivas casas são representados conforme a polarização dos fotões de acordo com o protocolo utilizado. Cada casa recebe o sinal quântico e descodifica-o, utilizando bases aleatórias independentes das que foram utilizadas pelo Centro de Controlo. Segue-se então a simulação da fase de pós-processamento, realizada no canal público, que difere conforme o protocolo utilizado. Dos passos do processo QKD mencionado em 3.2, apenas a fase de Destilação não é simulada neste trabalho. Após troca de um valor fixo de bits obtidos para retificação de erros ou ataques na transmissão quântica, por parte do CC, a ligação é validada ou não. No caso de a taxa de bits de teste errados ultrapassar um dado *threshold*, a ligação é cancelada e o consumo da casa em questão não é enviado nessa demanda. Caso seja validado, a casa encripta o seu respetivo consumo utilizando a chave restante do processo utilizando codificação OTP. A mensagem codificada é transmitida para o CC, que a descodifica com uma chave que em princípio será igual à que foi utilizada na sua codificação. Caso a chave não coincida, a mensagem obtida também não irá coincidir com um valor possível de uma leitura, diga-se um número decimal e tal é detetado. Todo o processo é repetido na próxima procura, que ocorre no instante de tempo definido como *target date*.

Caso, por qualquer motivo, uma casa não envie a sua leitura na demanda atual, o valor é guardado e acrescentado na próxima leitura. Existe a possibilidade de que, dadas as circunstâncias, a meio do processo uma casa não obtenha nenhum *bit* da chave resultante, uma vez que necessita de enviar um certo número de *bits* de teste pré-definido. Neste caso em específico, a codificação da casa em causa não ocorre na demanda atual. Existe também a hipótese de que a chave obtida seja menor do que o valor do consumo em binário, o que não permite encriptação OTP. Nesse caso, a chave final é repetida n vezes até atingir ou ultrapassar o tamanho do consumo, uma situação que também se pretende evitar ao máximo, por motivos de segurança. Em binário, os valores de consumos variam em valores entre os 40 e 48 *bits*, contudo, estes valores podem aumentar na presença de erros sucessivos na transmissão de uma dada casa, uma vez que cada um incrementa o valor da leitura da próxima demanda.

De forma a elaborar uma simulação o mais fiel possível com a descrição teórica dos protocolos referidos, todas os estados e bases diagonais ou retangulares são representados com a nomenclatura descrita nos artigos em que foram apresentados. Para BB84, os *bits* são codificados com bases representadas por $'+'$ e $'x'$, resultando assim, *qubits* com 4 estados possíveis, representados pelo grau da sua polarização 0^o 45^o para representação de 0 binário e 90^o 135^o para 1. Em SARG04, para cada *qubit* é utilizado um par de bases polarizadas possíveis, representadas pelas bases $'x'$ e $'z'$ e seus respetivos estados aleatórios $'+'$ e $'-'$, resultando assim os quatro estados de polarização possíveis, $\pm x$ e $\pm z$.

Finalmente, em KMB09, cada *qubit* é codificado com as bases identificadas por $'e'$ e $'f'$, e seus respetivos índices $i = 1, \dots N$ escolhidos aleatoriamente para cada base. Resultam assim os estados $e_1, \dots, e_N$ que codificam cada *bit* 0 da chave e $f_1, \dots, f_N$, que correspondem a cada *bit* de valor 1. No código utilizado, optou-se por representar todos os elementos dos quais nada se pode concluir pelo símbolo '*'. Tal diz respeito a *qubits* não lidos ou sobre os quais nada se pode concluir, bem como os *bits* de teste da chave abdicados para deteção de erros.

Na prática, cada *qubit* transmitido representa uma sobreposição de dois estados que conduzem à ambiguidade da leitura. Contudo, neste trabalho a informação transmitida no canal quântico é objetiva, representando apenas um só estado conforme a base utilizada na codificação elaborada pelo CC. Por forma a que o processo se assemelhe à realidade, a ambiguidade é simulada no código referente à leitura do *qubit* por parte de cada casa. Tal não afeta o funcionamento dos protocolos, como se irá observar posteriormente nos resultados, pela avaliação da eficiência dos protocolos em condições ideais.

Os três protocolos diferem ligeiramente na fase de *Shifting and Parameter estimation*. Tal deve-se ao simples facto de que, sendo fiel à literatura consultada dos respetivos criadores dos protocolos, em BB84 é o recetor quem anuncia as bases utilizadas na leitura dos *qubits* recebidos. Já nos restantes dois protocolos, é o emissor quem anuncia as características utilizadas na codificação, são elas os estados e os índices utilizados, para cada *bit* da chave, respetivamente em SARG04 e KMB09. O caso específico do uso de KMB09 com quatro estados, ou seja, dois índices por estado (N=2) não será muito explorado, uma vez que na prática tem um funcionamento análogo a SARG04 e, portanto, os resultados de ambos são redundantes. Contudo, é de todo o interesse estudar o funcionamento de KMB09 com N=4, pois corresponde ao único protocolo com oito estados estudado neste trabalho. Os passos do processo de QKD que foi simulado estão na tabela que se segue. Mais detalhes sobre a implementação de cada um destes passos estão no Anexo A.

Tabela 4: Passos do processo QKD simulado.

STATE	Casa	CC
0	Aguarda por *target date* para nova demanda.	Aguarda Pedido de Demanda.
	Faz pedido de atribuição de chave	Recebe pedido de atribuição de chave, gera chave binária para cada casa, codifica conforme o protocolo e envia *qubits* para cada casa.
1	Receção e descodificação dos *qubits.*	
2	Para BB84: Envia bases utilizadas na descodificação de *qubits*.	Para BB84: Retifica bases utilizadas pela casa e envia retificação.
	Para os restantes protocolos aguarda receção de bases utilizadas por CC.	Para os restantes protocolos: Envia bases utilizadas.
3	Averigua quais os bits possíveis de obter e comunica a sua posição.	Atualiza chave com a resposta da casa.
4	Envia um certo número de bits de teste.	Avalia se bits de teste correspondem aos gerados. Retorna ACK ou NACK

5	Caso receba confirmação positiva, codifica o consumo com a chave resultante.	Recebe e descodifica a mensagem recebida. Comunica se a receção foi correta
6	Recebe ACK ou NACK de CC conforme a correta receção da mensagem enviada. Retorna a STATE 0	Retorna a STATE 0

Neste trabalho, por forma a simular o pior caso possível dos ataques, considera-se que ambos (*intercept-and-resend* e *photon number splitting*) são efetuados no canal quântico junto ao Centro de Controlo, como já foi mencionado. Desta forma, não são afetados por atenuação ou ruído, apenas pelo número de fotões que constituem cada *qubit*. Além disso, considera-se também que têm tecnologia hipoteticamente em condições ideias, quer ao nível quântico quer ao nível de leitura dos *qubits* transmitidos, como por exemplo 100% de eficiência do fotorrecetor utilizado em *intercept-and-resend* e memória quântica, utilizada em PNS. Por último, uma vez que não é simulada qualquer encriptação no canal público, considera-se que após efetuado um ataque num dado canal quântico, Eve tem acesso à totalidade de informação transmitida no canal público pelos intervenientes da ligação atacada, por forma este possa ser bem sucedido.

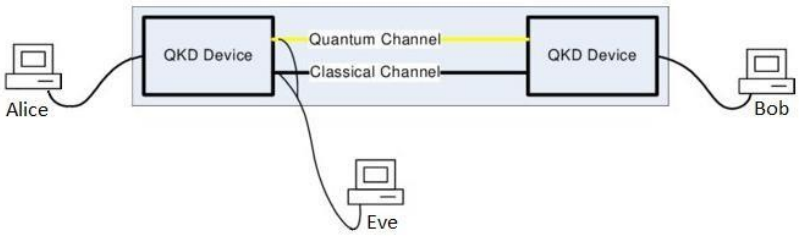


Figura 13: Representação esquemática da ligação QKD utilizada, adaptada de [48].

Um ataque considera-se bem sucedido quando Eve obtém no início da sua chave, os primeiros w *bits* da chave que é utilizada pela casa, em que w corresponde ao número de *bits* do valor do consumo a transmitir, em binário. Por outras palavras, se a chave utilizada pela casa com a ligação atacada for igual à chave do atacante, ou nela estiver contida, o ataque é assumido pelo simulador como válido. Para *intercept-and-resend* é considerada a hipótese de deteção de ataque com base nos *bits* de teste transmitidos, sendo possível que o ataque seja bem sucedido, mas fique sem efeito, uma vez que a casa da ligação intercetada não chega a enviar o seu consumo para o CC. Para PNS não foi implementado qualquer método de deteção de ataques. Os *bits* de teste analisados são selecionados aleatoriamente, dentro do conjunto de *bits* cuja leitura dos respetivos *qubits* foi conclusiva por parte de cada casa. Já para PNS, não foi implementado qualquer tipo de deteção de ataque.

No que se refere aos elementos da ligação quântica, o programa simula separadamente ou em conjunto as várias características de transmissão e leitura já mencionadas, correspondendo ao modelo de Poisson da fonte de pulsos coerentes fracos (*weak coherent pulses* – WCP), descrito em [24] e [31] e à probabilidade de leitura, com base na percentagem de receção devido à fonte, atenuação do canal e eficiência do recetor, descrito em [24]. Apenas se considera até um máximo de 4 fotões por pulso, valor cuja probabilidade de ocorrência já é bastante reduzida. É de notar que, se um *qubit* for constituído por 2 ou mais *qubits*, o seu valor exato não afeta em nada o funcionamento de nenhum dos fenómenos simulados. Este modelo, explicado em 3.4.3, é possível apenas para as situações em que a aproximação $\eta_{det}\eta_{\delta}p_n n \ll 1$ se verifica para qualquer valor de n, o que acontece para quase todos os valores possíveis de η_{det}, n, mesmo no pior caso $\mu = 1$, para um valor de $\eta_{\delta} = 10^{-\frac{0.2*1}{10}} \approx 0.955$.

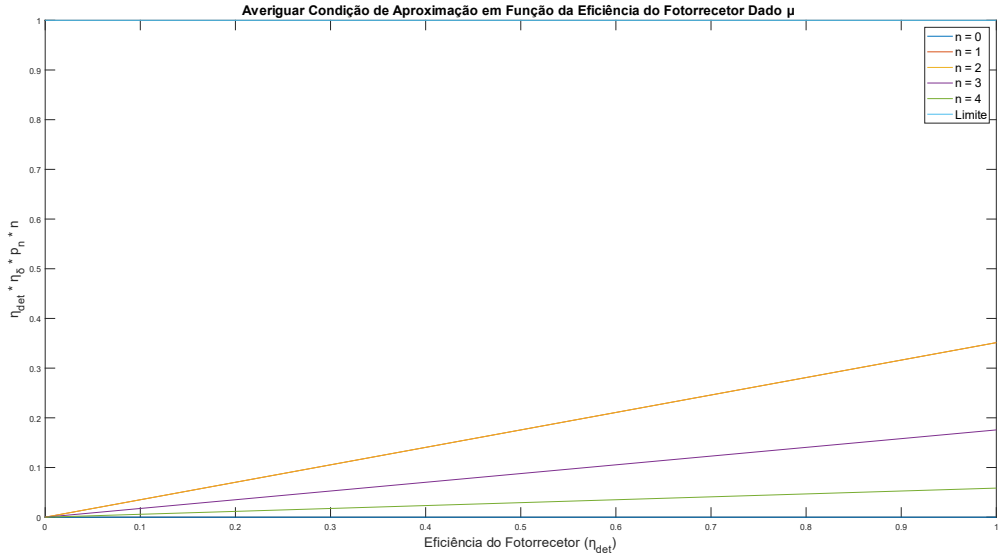


Figura 14: Resultados do produto $\eta_{det}\eta_{\delta}p_n n$, com $\mu = 1$, para vários valores de n, em função de η_{det}.

Aliado a isso, é possível simular um ambiente em que ocorre ruído de despolarização coletivo, conforme as probabilidades de leitura de estados do modelo de [25], pois corresponde ao modelo mais dinâmico estudado, que melhor se adequa à simulação e que apenas não é válido para protocolos que usem quatro estados quânticos, ou seja, não é válido para KMB09 com N=4.

As várias probabilidades de leitura dos estados dos *qubits* da Tabela 3, são explicadas e desenvolvidas de seguida. A tabela mencionada contém os valores de probabilidades das várias interceções de leitura de valor j (L_j) e envio de i (E_i), $P(L_j \cap E_i)$. Sendo que o pretendido é avaliar as probabilidades condicionadas da leitura num estado de polarização $j = \{0, 90, 45, 315\}$, sabendo que foi enviado um estado i e que foi escolhida a base de leitura (B_g), $g = \{x, +\}$, uma vez que o simulador precisa de lidar caso a caso, tendo i e g definido para cada *qubit*. Uma vez que na prática, para todos os protocolos contemplados por este modelo, os seus estados têm as mesmas polarizações e são lidos com bases análogas, utilizou-se a nomenclatura descrita em BB84 para condensar o funcionamento da simulação de ruído de despolarização. Inicialmente, pretendeu-se analisar

$$P(L_j/E_i) = \frac{P(L_j \cap E_i)}{P(E_i)}.$$

Uma vez que $P(E_i) = \frac{1}{4}, \forall\, i \in i = \{0; 90; 45; 315\}$, então, $P(L_j/E_i) = 4P(L_j \cap E_i)$ e obtém-se a seguinte tabela de probabilidades condicionadas.

Tabela 5: Probabilidade de leitura de qubit com estado j, sabendo que foi enviado estado i.

	$P(L_j / E_i)$			
Enviado	L_0	L_{90}	L_{45}	L_{315}
0	$\frac{cos^2(\theta)}{2}$	$\frac{sen^2(\theta)}{2}$	$\frac{1 - sen(2\theta)}{4}$	$\frac{1 + sen(2\theta)}{4}$
90	$\frac{sen^2(\theta)}{2}$	$\frac{cos^2(\theta)}{2}$	$\frac{1 + sen(2\theta)}{4}$	$\frac{1 - sen(2\theta)}{4}$
45	$\frac{1 + sen(2\theta)}{4}$	$\frac{1 - sen(2\theta)}{4}$	$\frac{cos^2(\theta)}{2}$	$\frac{sen^2(\theta)}{2}$
315	$\frac{1 - sen(2\theta)}{4}$	$\frac{1 + sen(2\theta)}{4}$	$\frac{sen^2(\theta)}{2}$	$\frac{cos^2(\theta)}{2}$

Fixando o valor de i, $\sum_j P(L_j\ /E_i) = 1$, bem como $\sum_i\ P(Lj\ /Ei) = 1$, quando fixado o valor de j. Contudo, estas probabilidades não contemplam a base escolhida para a leitura do dado *qubit* enviado com polarização i. É de notar que a base escolhida, B_x, influencia L_j, na medida em que escolhida a base $+$, é impossível obter $j = \{45;\ 315\}$, bem como, escolhido x, é impossível $j = \{0;\ 90\}$. Ou seja, $P(((L_0 \cup L_{90})/\ E_i) \cap B_x) = 0$ e $P(((L_{45} \cup L_{315})/\ E_i) \cap B_+) = 0$. Atendendo a estes conjuntos vazios, é possível concluir:

$$P((L_0/E_i) \cap (B_+)) = P(L_0/E_i)$$
$$P((L_0/E_i) \cap (B_x)) = 0$$
$$P((L_{90}\ /E_i) \cap (B_+)) = P(L_{90}/E_i)$$
$$P((L_{90}\ /E_i) \cap (B_x)) = 0$$
$$P((L_{45}\ /E_i) \cap (B_x)) = P(L_{45}/E_i)$$
$$P((L_{45}\ /E_i) \cap (B_+)) = 0$$
$$P((L_{315}\ /E_i) \cap (B_x)) = P(L_{315}/E_i)$$
$$P((L_{315}\ /E_i) \cap (B_+)) = 0$$

Perante estes cálculos, obtém-se a seguinte tabela:

Tabela 6: Probabilidade de leitura de qubit no estado j, sabendo que foi enviado no estado i e que foi escolhida base g para a sua leitura.

	$P(L_j\ /E_i \cap B_g)$							
Enviado/Leitura	B_+				B_x			
	L_0	L_{90}	45	315	0	90	L_{45}	L_{315}
0	$\frac{cos^2(\theta)}{2}$	$\frac{sen^2(\theta)}{2}$	0	0	0	0	$\frac{1 - sen(2\theta)}{4}$	$\frac{1 + sen(2\theta)}{4}$
90	$\frac{sen^2(\theta)}{2}$	$\frac{cos^2(\theta)}{2}$	0	0	0	0	$\frac{1 + sen(2\theta)}{4}$	$\frac{1 - sen(2\theta)}{4}$
45	$\frac{1 + sen(2\theta)}{4}$	$\frac{1 - sen(2\theta)}{4}$	0	0	0	0	$\frac{cos^2(\theta)}{2}$	$\frac{sen^2(\theta)}{2}$
315	$\frac{1 - sen(2\theta)}{4}$	$\frac{1 + sen(2\theta)}{4}$	0	0	0	0	$\frac{sen^2(\theta)}{2}$	$\frac{cos^2(\theta)}{2}$

É com base nos valores desta última tabela que o simulador se rege por forma a contar o número de *qubits* enviado no estado i e determinar quantos são lidos em cada um dos estados j, pelo produto entre $\sum E_i$ de uma dada chave e $P\ (L_j\ /\ E_i\ )$, alterações que ocorrem conforme a base g escolhida para a sua leitura. Serão então analisados os valores possíveis de $\varepsilon = sin^2(\theta)$, que caracterizam o ruído de despolarização, por forma a calcular os seus efeitos e os valores aceitáveis ao funcionamento do sistema, segundo o modelo utilizado.

Com base em todos estes fenómenos mencionados, é obtido um número abrangente de diferentes *outputs* por forma a avaliar o impacto das várias situações de simulação. São elas:

(i) funcionamento em condições ideais;

(ii) impacto de uma fonte imperfeita em conjunto com atenuação e eficiência do fotorrecetor utilizado, para vários valores de intensidade média por pulso, atenuação por km de transmissão, eficiência do fotorrecetor e distância de ligação, considerando diferentes números de *bits* de teste possíveis;

(iii) impacto duma fonte de transmissão imperfeita para várias intensidades médias por pulso;

(iv) funcionamento e resultados do ataque *intercept-and-resend* ao nível do número de bits descobertos por Eve;

(v) sucesso do ataque *intercept-and-resend* para vários valores de *bits* de teste e taxa máxima de *bits* de teste incorretos;

(vi) avaliação de ataques PNS para várias intensidades médias de pulsos transmitidos;

(vii) presença de um ataque PNS;

(viii) efeitos de ruído de despolarização no canal quântico e parâmetros aceitáveis de ruído;

(ix) impacto do ruído de despolarização na presença de um ataque *intercept-and-resend*.

Os vários parâmetros de simulação são os seguintes:

(i) Distância de ligação no canal quântico: $L \in [1; 9]\ km$.

(ii) Atenuação típica de atenuação por km de fibra α, que varia entre os valores de 0.20 e 0.16 dB/km[6], [45], respetivamente.

(iii) Eficiência do fotorrecetor $\eta_{det} \in [0\%; 80\%]$, sendo os valores típicos considerados por volta dos 10% [24], [45].

(iv) Intensidade média de fotões por *qubit* (ou de fotões por pulso, uma vez que é enviado um fotão por pulso) $\mu \in [0; 0{,}8]$, sendo os valores considerados típicos $\mu = 0.1$ [24], [45]. O valor de intensidade aqui considerado é de $\mu = 0.2$, uma vez que, pelo modelo de [24], era de interesse que $R_{raw} = \cong \eta_{det}\eta_{\delta}\mu$ ultrapassasse o valor de 1%, visto que $R_{raw} \cong 0.1 * 10^{-\frac{0.2}{10}} * 0.1 = 0.95\%$. Tal podia ser feito com o aumento da eficiência do fotorrecetor, como já foi explicado pela Fig. 10, o que conduziria, na prática, a um aumento do número de *dark counts* no recetor. A questão mais importante com esta escolha é averiguar se o uso deste valor médio de intensidade compromete a segurança contra ataques PNS, em prol da eficiência. Todos estes casos serão estudados na secção seguinte deste trabalho.

O método de obtenção de todos os *outputs* seguidamente apresentados corresponde a executar a simulação quatro vezes, ou seja, ao longo de uma hora, para um certo tamanho de chave gerada e um certo valor do parâmetro a simular. Nos gráficos gerados considera-se a média aritmética dos valores de cada conjunto de quatro valores nas mesmas condições e os resultados são apresentados como as médias das 36 casas da rede que estão presentes no processo QKD.

7. Resultados

7.1. Condições Ideais

É de interesse começar por avaliar o funcionamento dos protocolos implementados nas condições ideais de simulação. Nestas condições, as eficiências de leitura dos protocolos simulados, ao nível de leitura de *qubits* estão bem documentadas na literatura consultada. É sabido que é suposto que com BB84, a taxa de *qubits* cuja leitura é validada pelo CC, corresponda a 50%, o que corresponde à percentagem de *qubits* lidos com a base correta. Já com SARG04, conforme descrito na revisão de literatura, Bob só consegue, em média, obter informação acerca de 25% dos *qubits* da chave. Para o caso de KMB09, para N=2, como já foi explicado, o seu funcionamento é análogo a SARG04, uma vez que o ITER corresponde a 25%. Por último para N=4, utilizando KMB09, é expectável um ITER de 37.5%.

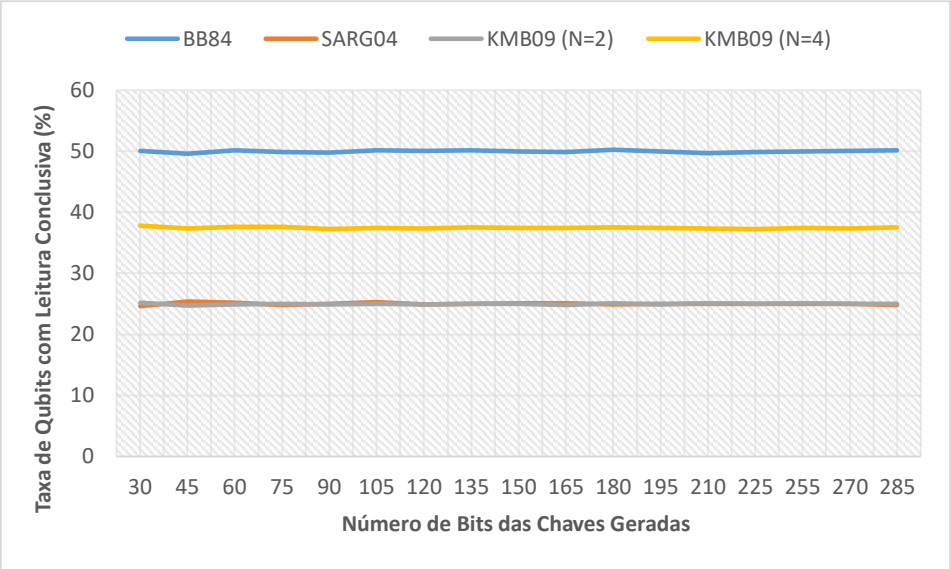


Figura 15: Taxas de leituras de qubits conclusivas em condições de simulação ideais, utilizando quatro protocolos distintos, em função do número de bits de cada chave gerada.

As eficiências de leitura dos protocolos dependem apenas da aleatoriedade associada à codificação e leitura dos qubits recebidos, pelo que, em média se mantêm inalteráveis, exceto em certos casos de ruído ou ataque externo. Correspondem assim, à percentagem de *qubits* lidos, dos quais foi possível extrair um bit. Por questões de simplificação, este parâmetro será referido como $\eta_{protocolo}$. Nestas simulações foi utilizado apenas um único bit de teste, pois nestas condições é o suficiente para detetar um potencial erro e, como era expectável, não ocorreu nenhum erro ao longo das simulações. O QBER de cada processo QKD é calculado pela fórmula: $QBER = \frac{\kappa_{err}}{\kappa} = \frac{\kappa - k_{corr}}{\kappa}$ em que κ_{err} consiste no número de *qubits* cujo *bit* correspondente não consta na chave resultante, incluindo o bit de teste utilizado e κ_{corr} ao número de *qubits* conclusivos que resultam na chave resultante utilizada para codificação. Num cenário em que todos os *qubits* transmitidos são lidos, $QBER = \frac{\kappa - \kappa * \eta_{protocolo} + número\ de\ bits\ de\ teste}{\kappa} = 1 - \eta_{protocolo} + \frac{número\ de\ bits\ de\ teste}{\kappa}$. Resulta assim que, nestas condições, o valor do QBER corresponde aproximadamente às taxas de leituras inconclusivas de *qubits*, complementares aos valores da figura acima, ou seja, 50%, 75% e 62.5%, para BB84, SARG04 e KMB09(N=4), respetivamente. Esta taxa de *qubits* que não resultam em nenhum *bit* na chave resultante é derivada da percentagem de leituras conclusivas, intrínsecas a cada protocolo. Já a taxa de *bits* lidos incorretamente corresponde exclusivamente à percentagem de *qubits* lidos com a base diferente da que foi utilizada na sua codificação, ou seja, 50% para todos os protocolos. É de notar que, nos protocolos SARG04 e KMB09, o recetor apenas pode obter *bits* a partir de uma parte dos *qubits* que leu incorretamente.

Nestas condições, todas as casas obtêm constantemente chaves resultantes não nulas, ou seja, constituídas por pelo menos um único *bit*, independentemente do protocolo utilizado. Contudo, existem casos em que o número de *bits* das chaves resultantes não é suficiente para a codificação OTP dos respetivos consumos energéticos. A taxa média de casas cuja chave resultante com *bits* insuficientes para codificação OTP, em função do tamanho da chave gerada por CC (κ) e do protocolo utilizado, encontra-se na Figura 16.

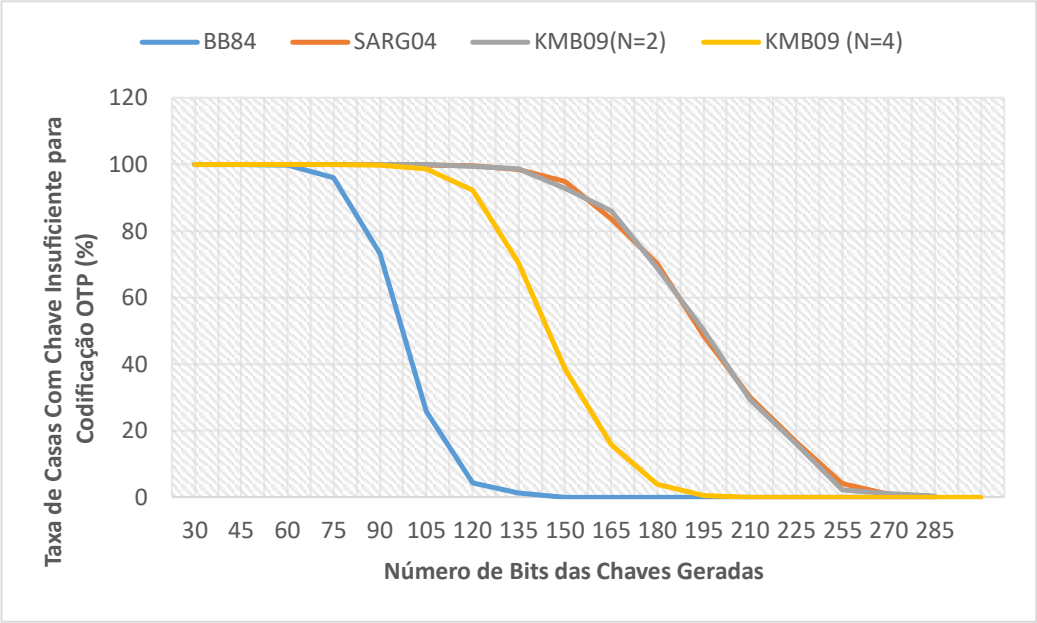


Figura 16: Taxas de casas com chave resultante insuficiente para codificação OTP, em condições ideais, para os vários protocolos simulados, em função do número de bits de cada chave gerada.

Conclui-se assim que, para condições ideais, os valores mínimos de κ que conferem uma taxa média de casas com chave insuficiente para codificação OTP nula são 150 para BB84, 210 para KMB09(N=4) e 285 para KMB09(N=2) e SARG04.

7.2. Funcionamento em Condições Reais na Ausência de Ataques

Após uma rápida observação do bom funcionamento dos protocolos implementados e suas características em condições ideais, é então feita uma análise ao seu desempenho considerando as limitações práticas que o sistema deve conseguir ultrapassar. Previamente, foi necessário fixar o número de *bits* de teste que devem ser utilizados no processo QKD, dado que, na prática, apenas uma pequena percentagem dos *qubits* é lida. Considerando o caso estipulado neste trabalho: $\mu = 0.2$, $\eta_{det} = 10\%$, $\alpha = 0.20\ dB/km$, para uma distância de $L = 1\ km$, a uma probabilidade de leitura corresponde a: $Rraw = 0.1 * 10^{-\frac{0.2}{10}} * 0.2 = 0.0191 = 1.91\%$.

Considerando, por exemplo, o protocolo BB84, é feita uma estimativa teórica do total de *bits* resultantes do processo QKD, por forma a analisar o número máximo teórico de *bits* de teste possíveis de utilizar na averiguação de erros. Atendendo ao tamanho típico das mensagens, entre 42 e 48 *bits*, para os cálculos, foi estipulado para os cálculos teóricos que o número de *bits* mínimo da chave resultante corresponde a 50.

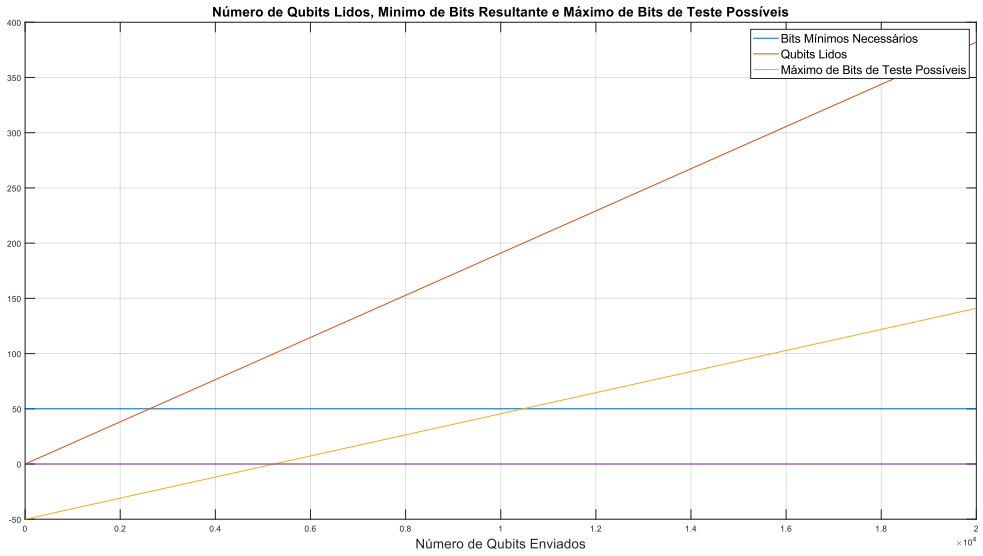


Figura 17: Valores teóricos de número de qubits lidos, bits mínimos requeridos para OTP, número máximo de bits deteste, em função do número de qubits transmitidos, evidenciando o número mínimo de qubits a partir do qual é possível enviar um bit de teste.

Conclui-se na figura acima que, por forma a obter uma chave com no mínimo 50 *bits*, dada a probabilidade R_{raw} e a taxa média de *qubits* lidos corretamente no protocolo em causa, só é possível o envio de um único *bit* de teste caso as chaves geradas tenham tamanho superior a 5341 *bits*. Para as mesmas circunstâncias, alterando o protocolo, para SARG04 ou KMB09 (N=2), cuja taxa de *bits* obtidos/*qubit* é metade, este valor aumenta para o dobro, 10681. Para o caso de KMB09 (N=4), este valor é de 7121 *bits*. Além de averiguar o tamanho mínimo da chave gerada pelo CC para ser possível o funcionamento dos métodos QKD, é também necessário estipular a proporção de *bits* de teste utilizados dado o tamanho da mesma (κ), o que é exequível usando apenas a probabilidade de leitura, eficiência do protocolo e o número de *bits* resultantes imposto:

$$bits\ de\ teste\ max = \kappa * R_{raw} * \eta_{protocolo} - tamanho\ da\ chave\ final\ minima$$

$$<=> bits\ de\ teste\ max = \kappa * \eta_{det}\eta_{\delta}\mu * \eta_{protocolo} - tamanho\ da\ chave\ final\ minima$$

Obtém-se que para BB84, a reta que relaciona o valor máximo de *bits* de teste utilizado com κ, garantindo um mínimo de 50 *bits* resultantes, é $\xi_{BB84} = 0.0095 * \kappa - 50$, para SARG04 e KMB09 (N=2) corresponde a $\xi_{SARG04} = \xi_{KMB09(N=2)} = 0.0048 * \kappa - 50$ e KMB09 (N=4) é $\xi_{KMB09(N=4)} = 0.0072 * \kappa - 50$. Porém na prática, o uso destes valores traduz-se numa grande taxa de casas com uma chave insuficiente para codificação OTP dos respetivos consumos. Tal é possível constatar nos seguintes resultados, contabilizando a taxa de casas cuja chave resultante é insuficiente para a codificação OTP de 50 *bits*, nas condições de distância, atenuação e eficiência referidas.

O gráfico seguinte ilustra esse resultado, com uso do protocolo BB84, para vários valores de $\mu = \{0; 0.2; 0.4; 0.6; 0.8\}$, em função de κ, com valores acima do mínimo requerido para o uso de *bits* de teste:

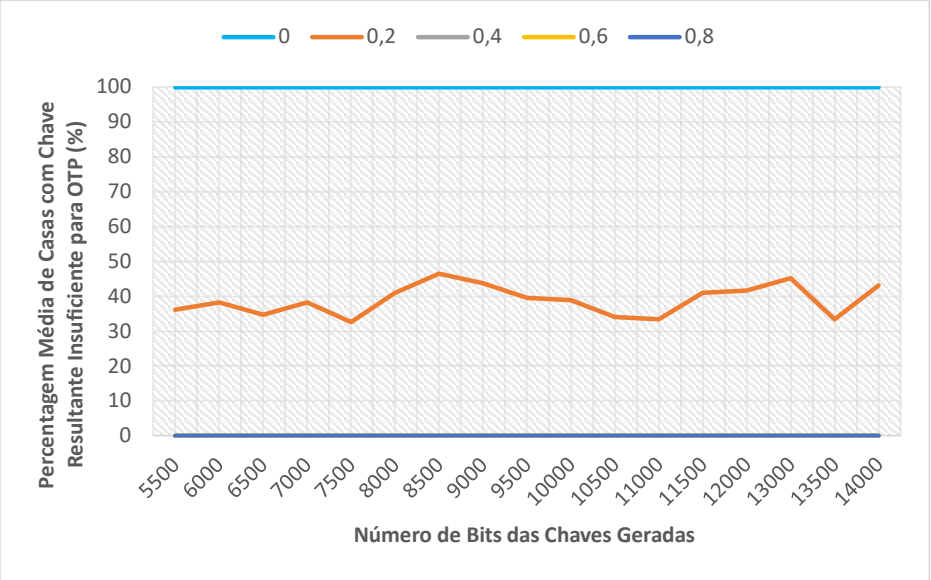


Figura 18: Percentagem de casas com chave resultante insuficiente para OTP, com protocolo BB84, utilizando o número máximo teórico de bits de teste nas condições mencionadas como padrão.

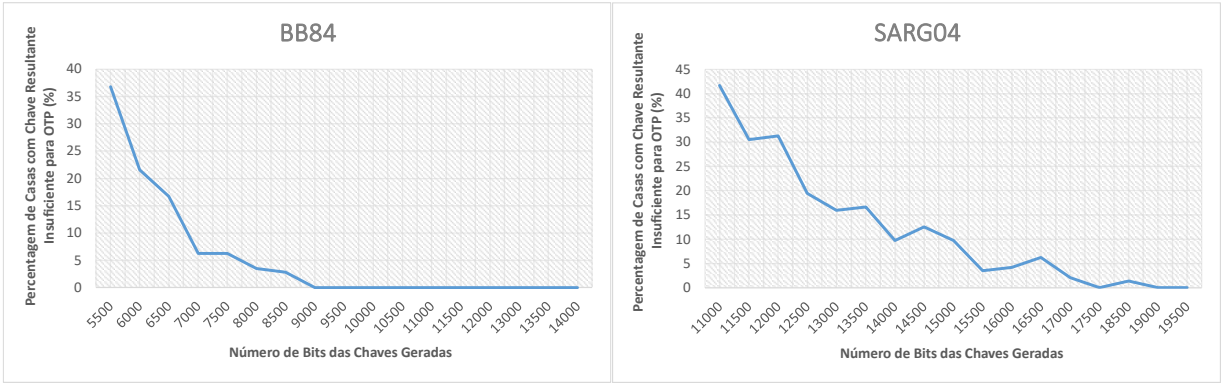
Como se pode observar, para valores de intensidade média por pulso de $\mu = 0.2$, a taxa de casas com uma chave resultante com um número de *bits* insuficiente para codificação OTP é aproximadamente de 40%, uma vez que nestas condições limite, corresponde às vezes em que a eficiência média de leitura do protocolo está abaixo do valor teórico. Note-se também que, para valores de μ iguais ou superiores a 0.4, a taxa de casas com *bits* de chave resultante insuficientes para a codificação OTP do consumo é nulo e os gráficos destes valores estão sobrepostos. Contudo, como foi estipulado o objetivo de não aumentar os valores de μ acima de 0.2, devido a ataques PNS, a opção tomada foi utilizar os valores $\frac{\xi_{BB84}}{2}$, $\frac{\xi_{SARG04}}{2}$ e $\frac{\xi_{KMB09\ N\_4}}{2}$, mencionadas anteriormente, utilizando assim metade do máximo teórico de *bits* de teste possíveis em função de κ, por forma a garantir assim uma margem nas eficiências de leitura.

Concluiu-se então, que a relação entre *bits* de teste e κ utilizada, seria a que se apresenta na tabela seguinte:

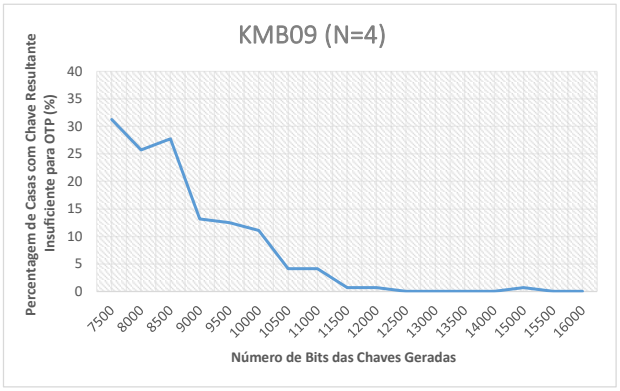
Tabela 7: Relação entre o número de bits de teste utilizados em função do número de bits da chave gerada escolhida para os diversos protocolos.

Protocolo	Número *Bits* de Teste
BB84	$\kappa * 0.00475 - 25$
SARG04	$\kappa * 0.00238 - 25$
KMB09 (N=2)	$\kappa * 0.00238 - 25$
KMB09 (N=4)	$\kappa * 0.0036 - 25$

Perante as conclusões teóricas e assumidos os valores de *bits* de teste usados, é então necessário avaliar para que valores de κ se garante uma taxa de casas com chaves resultantes suficientes para OTP de 100%, para os vários parâmetros de simulação. Inicialmente realizou-se uma análise dos resultados para valores fixos de atenuação média do canal quântico (0.2 dB/km), distância (1 km), eficiência do recetor (10%) e média de intensidade de fotões por *qubit* transmitido (0.2). Os resultados de taxa média de casas com número insuficiente de *bits* resultantes do processo para aplicarem codificação OTP dos respetivos consumos encontram-se na Figura 19, para os vários protocolos:



(a) *(b)*



(c)

Figura 19: Taxas de casas com chave resultante insuficiente para codificação OTP com 50 bits, com $\eta_{det} = 10\%, \mu = 0.2,$ *e* $l = 1$*, para os vários protocolos (a) BB84, (b) SARG04 e (c) KMB09 (N=4), em função do número de bits de cada chave gerada.*

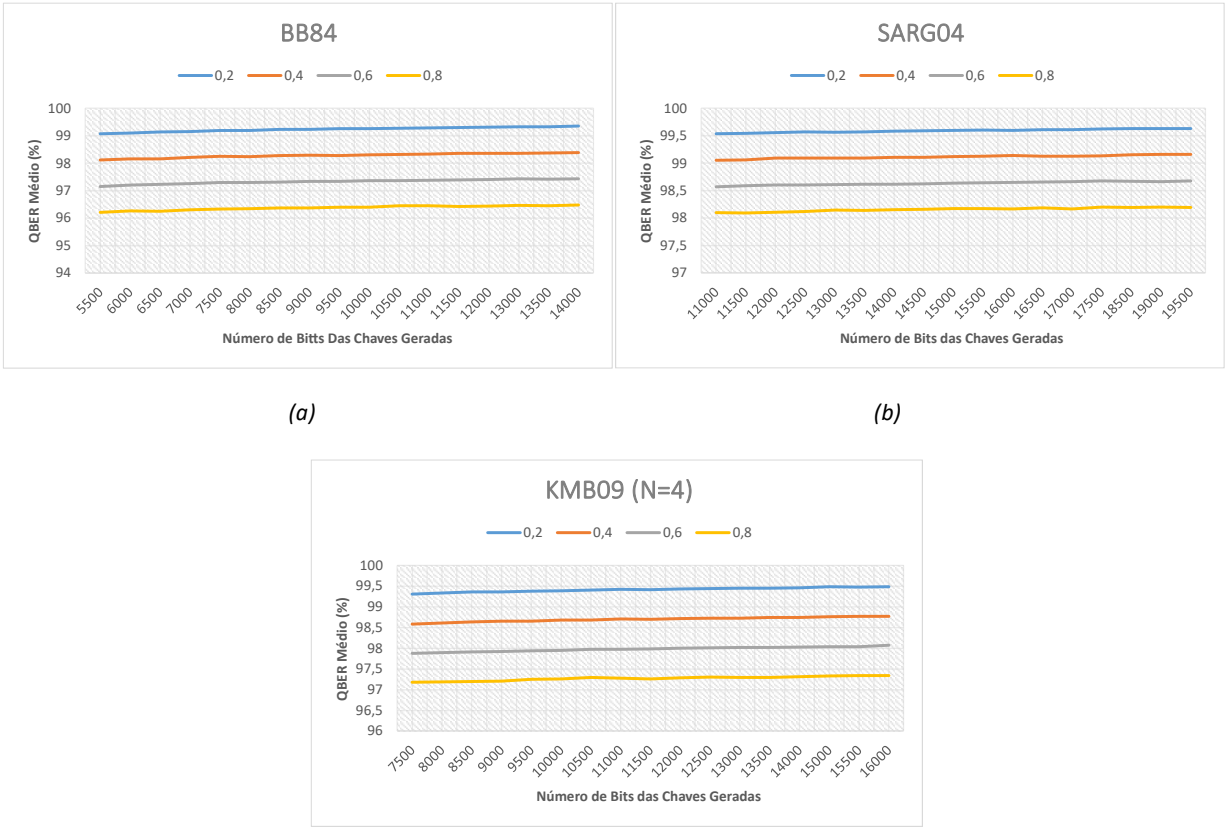
Desta fórmula, conclui-se que, para a proporção de número de *bits* de teste considerados, relativamente ao número de *bits* da chave gerada (κ), nas condições de probabilidade de leitura de *qubits* consideradas, por forma a garantir a fiabilidade mínima do sistema, são necessários os seguintes tamanhos mínimos de κ para alcançar o objetivo estipulado de *bits* da chave resultante suficientes para codificação OTP dos respetivos consumos.

Tabela 8: Número de bits mínimos de chave gerada para os diversos protocolos, utilizando a proporção de bits de teste determinada e simulando μ=0.2, α=0.2, ηdet*= 0.1 e* l*=1.*

Protocolo	Número mínimo de κ
BB84	9500
SARG04	19500
KMB09 (N=2)	19500
KMB09 (N=4)	13000

Como se pode observar, num cenário não ideal de percentagem de leitura de *qubits*, os valores mínimos de κ que conferem uma taxa média de casas com chave resultantes insuficiente para OTP nula é em média de 65 vezes superior ao que foi obtido na simulação de 7.1, para os protocolos utilizados. É de notar que na Fig. 19c) se verifica uma ocorrência em que uma das casas não obteve uma chave de tamanho suficiente, para $\kappa = 15000$. Contudo, a média de *bits* resultantes do processo pelas casas da rede, nesse valor específico, foi de 78.06.

É de interesse avaliar o impacto que a intensidade média de fotões por pulso tem no QBER, para $\eta_{det} = 10\%$, $\alpha = 0.20\ dB/km$ e $l = 1\ km$. Nestes resultados não foram utilizados os valores da Tabela 8, mas tal não tem influência uma vez que κ tem pouco impacto no QBER resultante.



(a) *(b)*

(c)

Figura 20: Taxas de QBER dos protocolos (a)BB84 (b)SARG04 e (c)KMB09(N=4), com $\eta_{det} = 10\%$, $\alpha = 0.20\ dB/km$ e $l = 1\ km$, para vários valores de intensidade média de fotões por pulso, em função do número de bits de cada chave gerada.

Os valores médios de QBER, resultantes da simulação, são extremamente altos comparativamente com o que é obtido em condições ideais. Tal deve-se ao facto de, além de ser afetado por $\eta_{protocolo}$, apenas são lidos $R_{raw}(\%)$ dos *qubits* transmitidos. O QBER nestas condições de leitura é dado por $QBER = \frac{\kappa - \kappa * R_{raw} * \eta_{protocolo} + número\ de\ bits\ de\ teste}{\kappa} = 1 - R_{raw} * \eta_{protocolo} + \frac{número\ de\ bits\ de\ teste}{\kappa}$. Dado que $R_{raw} = 0.0191$ nas condições consideradas, aliado ao facto de o número de *bits* de testes ser superior a um único *bit*, é normal este aumento substancial nos valores de QBER, para qualquer valor de μ.

Como se pode verificar, aumentar μ com um incremento de 0.2 diminui o QBER de forma absoluta por aproximadamente 1% em BB84, sendo que estas variações são ainda menos expressivas para os restantes protocolos considerados. Aliado a esta baixa melhoria na taxa de QBER, aumentar μ provoca o aumento da probabilidade de um *qubit* ser constituído por mais do que 1 único fotão, seguindo a distribuição de Poisson desse valor, como demonstra a Figura 21.

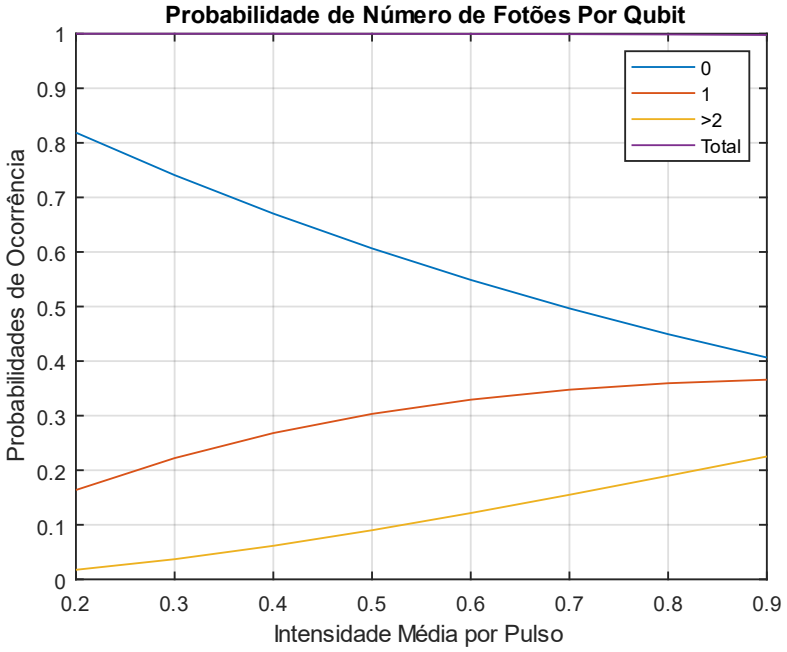
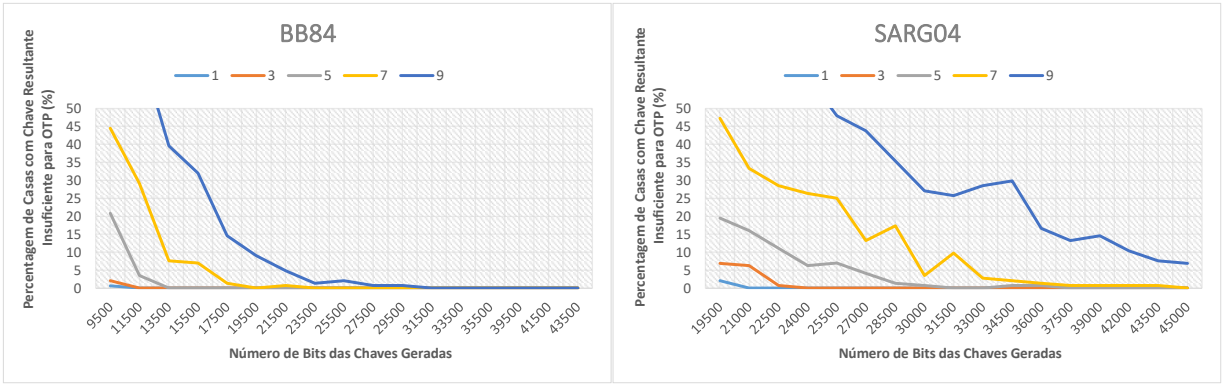


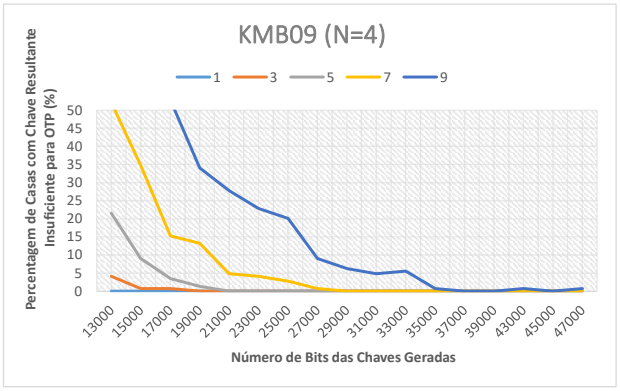
Figura 21: Probabilidade de um qubit ser constituído por 0, 1, ou mais do que 1 fotão, em função da média da distribuição de Poisson.

Uma variação da eficiência do fotorrecetor (η_{det}) tem um efeito análogo à variação de intensidade média por pulso, uma vez que têm exatamente o mesmo peso em R_{raw}, logo estudar a variação dos seus efeitos é redundante.

Segue-se uma análise do impacto da distância média entre as casas e o CC na eficiência do processo de atribuição de chaves, simulada para distâncias $L = \{1; 3; 5; 7; 9\}\ km$, mantendo $\eta_{det} = 10\%$, $\alpha = 0.20\ dB$, partindo dos valores mínimos de κ determinados na Tabela 8.



(a) *(b)*



(c)

Figura 22: Taxas de casas com chave insuficiente para OTP dos protocolos (a)BB84 (b)SARG04 e (c)KMB09(N=4), com $\eta_{det} = 10\%$, $\alpha = 0.20\ dB/km$, $\mu = 0.2$, para vários valores de distância (km), em função do número de bits de cada chave gerada.

Infelizmente, não é possível executar a simulação para valores de κ superiores a 50000, devido a limitações do *framework* Mosaik, na análise do tamanho mínimo da chave requerido nas condições estipuladas para SARG04 e KMB09. Contudo, é notável que o aumento da distância é muito limitante no que se refere ao tamanho de *bits* obtidos na chave final de codificação, em especial com os mínimos que são requeridos neste trabalho para garantir a viabilidade da codificação OTP.

Segue-se então uma análise dos mesmos resultados, aumentando a eficiência do fotorrecetor para $\eta_{det} = 12\%$, novamente para valores de distância L = {1; 3; 5; 7; 9}km, mantendo a intensidade média dos pulsos $\mu = 0.2$ e a atenuação média na fibra $\alpha = 0.2\ dB/km$.

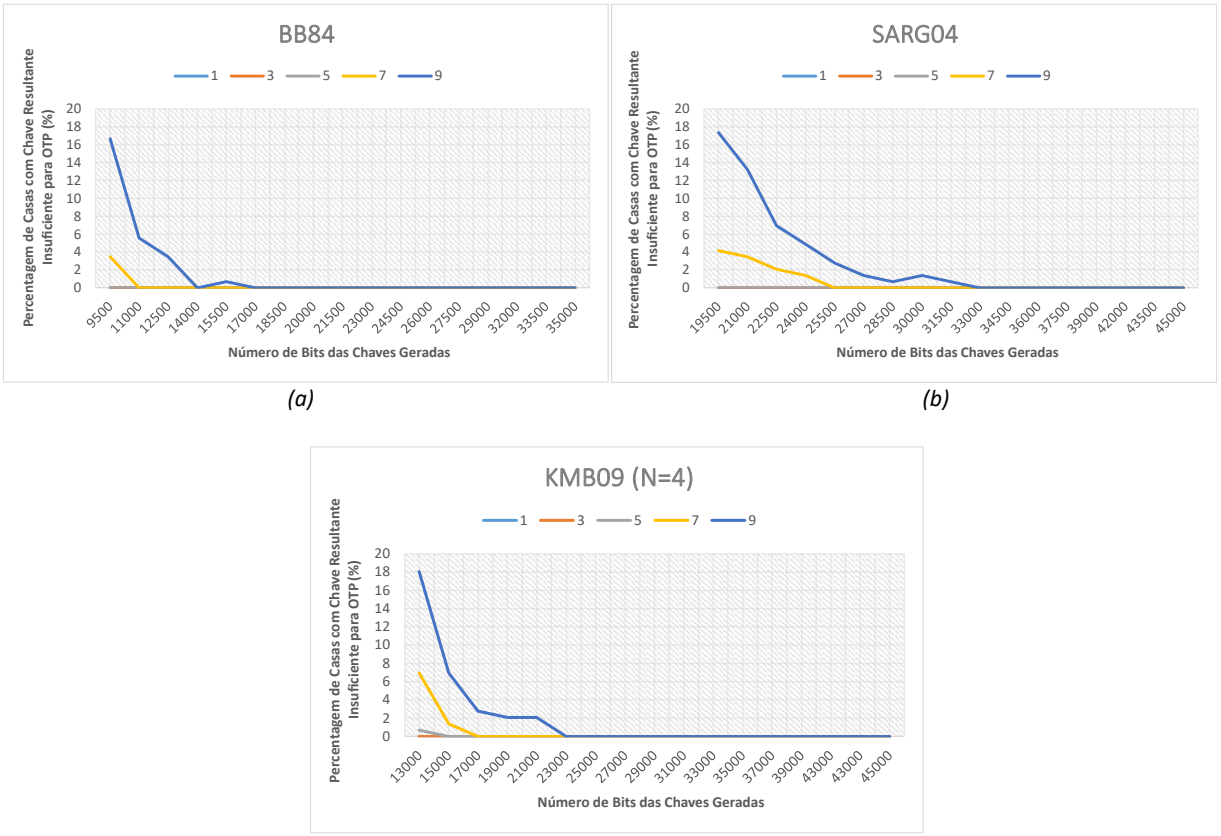


Figura 23: Taxas de casas com chave insuficiente para OTP dos protocolos (a)BB84 (b)SARG04 e (c)KMB09(N=4), com $\eta_{det} = 12\%$, $\alpha = 0.20\ dB/km$, $\mu = 0.2$, para vários valores de distância (km), em função do número de bits de cada chave gerada.

Conclui-se assim que aumentar a eficiência do fotorrecetor para $\eta_{det} = 12\%$ já constitui uma solução viável para este cenário de QKD com distâncias de 7 e 9 km pois baixa drasticamente o número de *bits* da chave gerada para que o número de *bits* da chave resultante seja consistentemente igual ou superior ao número de *bits* do consumo de cada casa.

Resta assim repetir a simulação, fazendo uma análise do impacto da atenuação média na fibra quando o valor desta é de $\alpha = 0.16\ dB/km$ na eficiência do sistema, com $\eta_{det} = 10\%$, $\mu = 0.2$, para os mesmos valores de L ao longo de κ. Os resultados encontram-se na Figura 24.

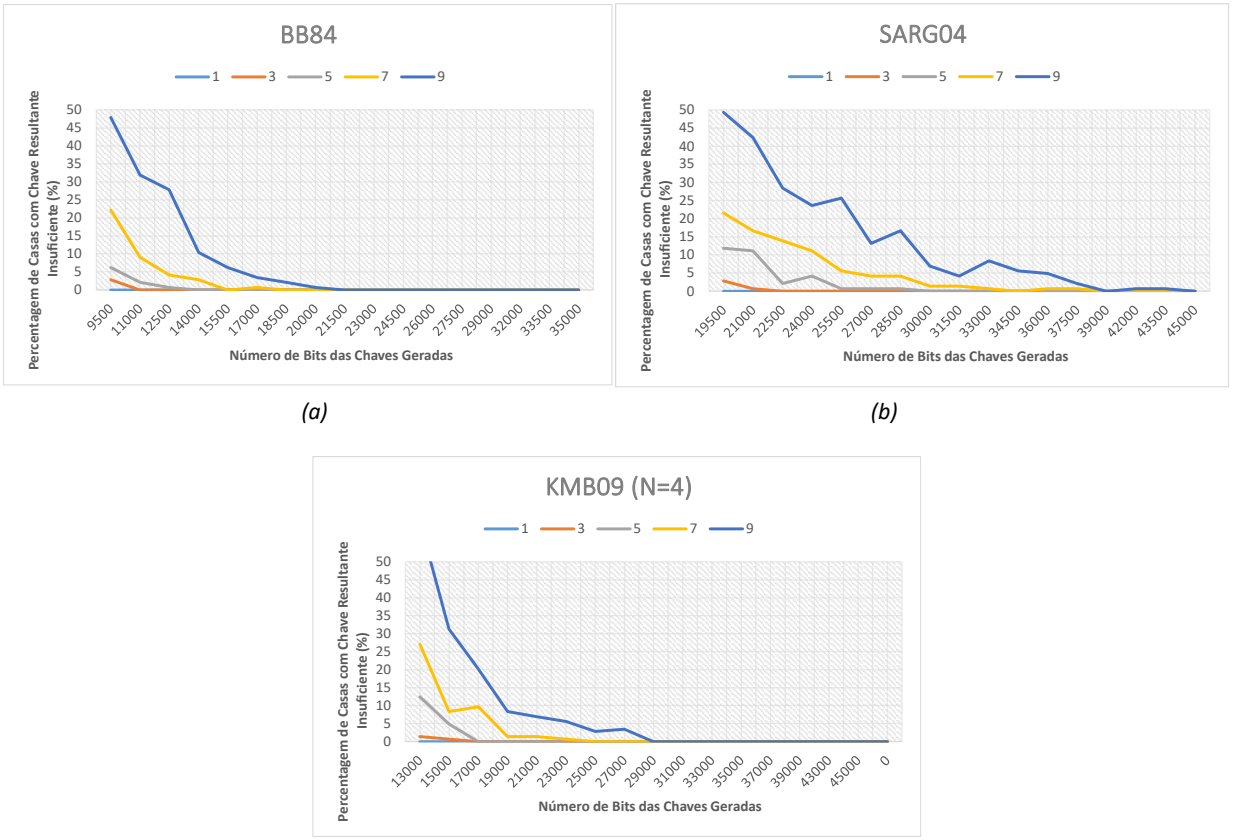
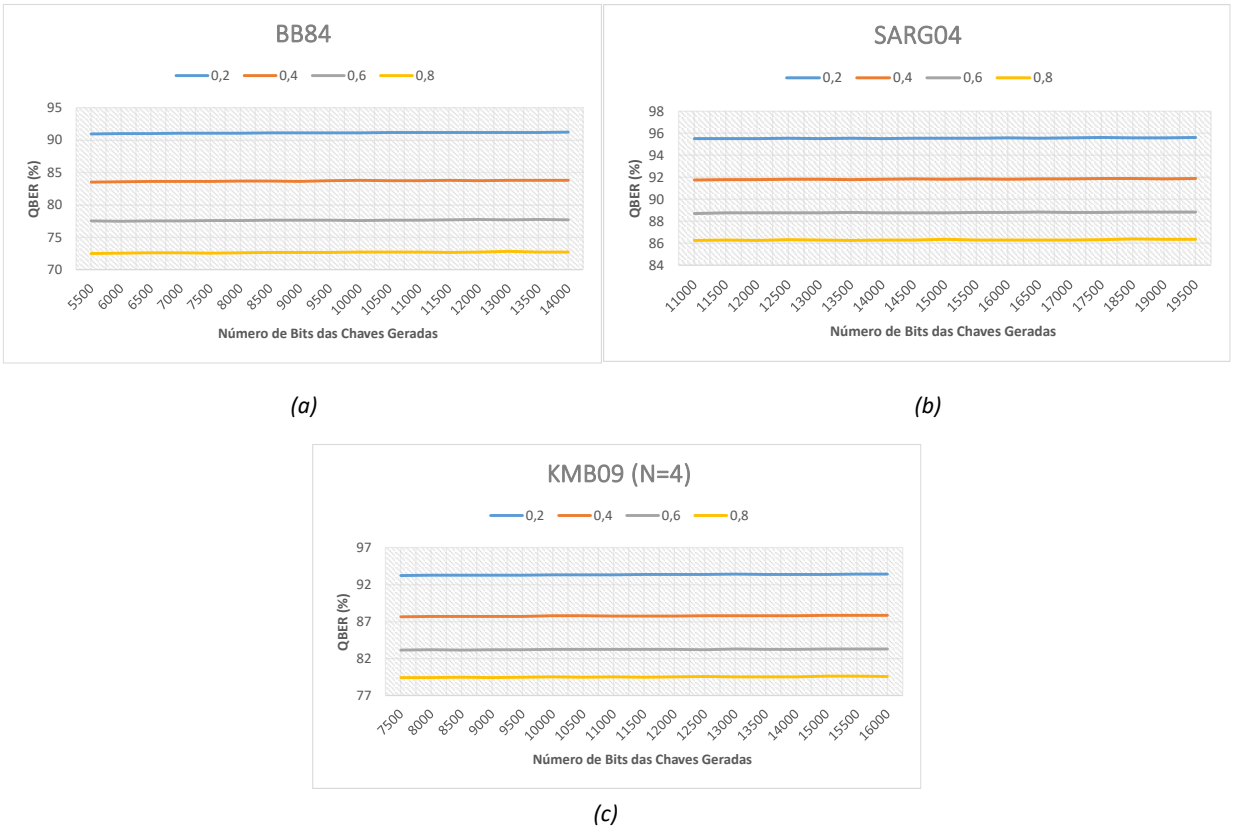


Figura 24: Taxas de casas com chave insuficiente para OTP dos protocolos (a)BB84 (b)SARG04 e (c)KMB09(N=4), com $\eta_{det} = 12\%$, $\alpha = 0.16\ dB/km$, $\mu = 0.2$, para vários valores de distância (km), em função do número de bits de cada chave gerada.

Conclui-se por comparação entre a Fig. 23 e Fig. 24, que, para uma implementação deste método num contexto em que as distâncias se aproximam dos 10 km, é mais viável aumentar a eficiência do fotorrecetor para 12% do que investir em fibras com perdas ultrabaixas, cujos efeitos não se manifestam nas distâncias que caracterizam uma rede local.

7.3. Fonte de Pulsos Coerentes Fracos com Canal e Recetor Ideais

Estas são as características de simulação pelas quais se rege Eve num ataque *intercept-and-resend*, estando, obviamente numa posição de vantagem sobre as casas da ligação, o que é visível pelo QBER obtido nestas condições, ilustrados na Figura 25.



(a) *(b)*

(c)

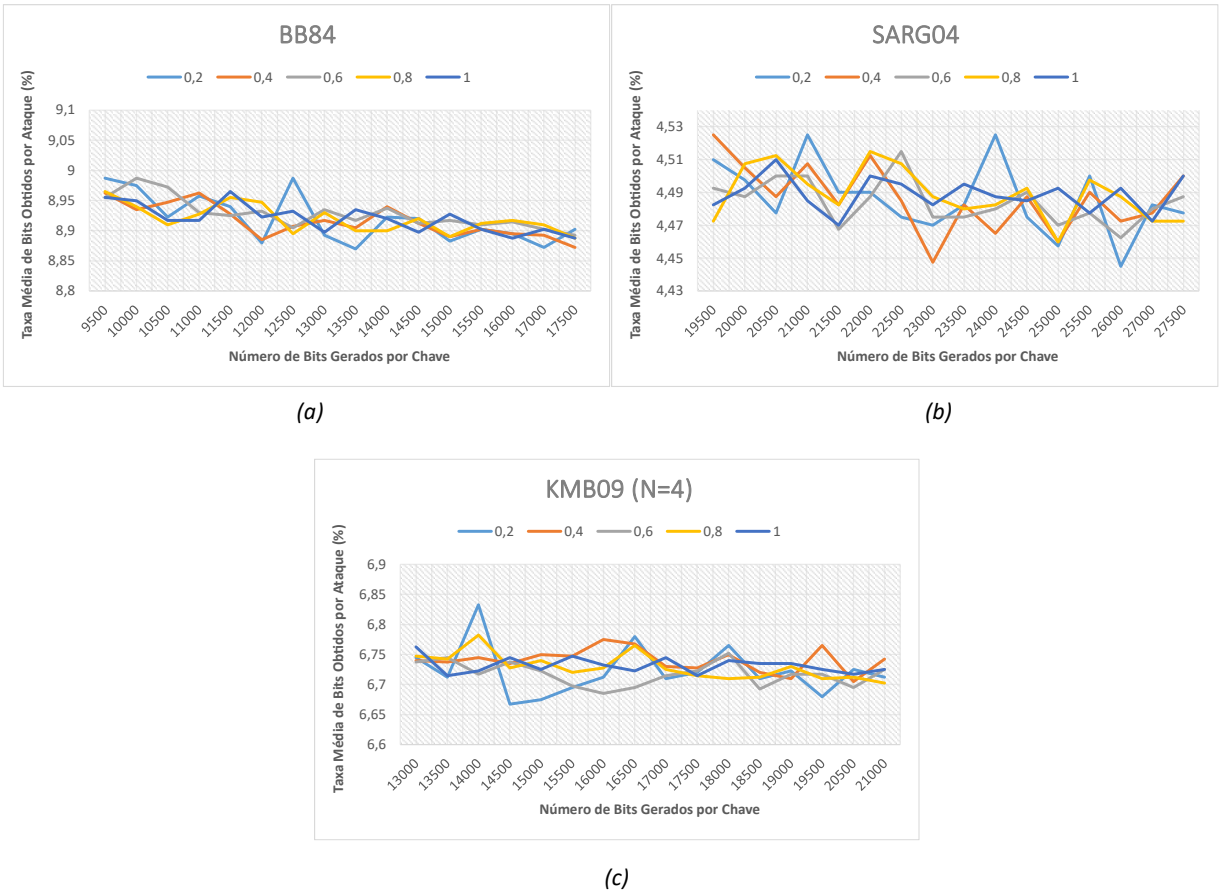
Figura 25: Taxas de QBER dos protocolos (a)BB84 (b)SARG04 e (c)KMB09(N=4), considerando apenas fontes de pulsos coerentes fracos que seguem distribuição de Poisson, para vários valores de intensidade média de fotões porpulso, em função do número de bits de cada chave gerada.

Comparando os valores de QBER obtidos nestas condições com os que foram obtidos na Fig. 20, é percetível que Eve obtenha substancialmente mais *bits* na sua chave resultante do que a casa correspondente à ligação onde efetuou o ataque, quando se trata de um *intercept-and-resend*, especialmente tendo em conta num contexto em que o número de *qubits* transmitidos são superiores aos da Tabela 8. Os resultados e impactos de um ataque deste tipo serão analisados de seguida.

7.4. Presença de Ataques *Intercept-and-Resend*

Considera-se nestas simulações as condições base estipuladas de leitura de *qubits* por parte das casas: $\mu = 0.2$, $\alpha = 0.2\ dB/km$, $\eta_{det} = 10\%$ a partir dos valores mínimos de κ, identificados na Tabela 8.

Inicialmente é averiguada a eficiência destes tipos de ataques ao nível da taxa média de *bits* obtidos na chave resultante de Eve, em relação à totalidade da chave quântica transmitida. As simulações são realizadas para várias probabilidades de ataque nas ligações quânticas da rede: 0.2, 0.4, 0.6, 0.8 e 1, para vários tamanhos de chaves geradas.

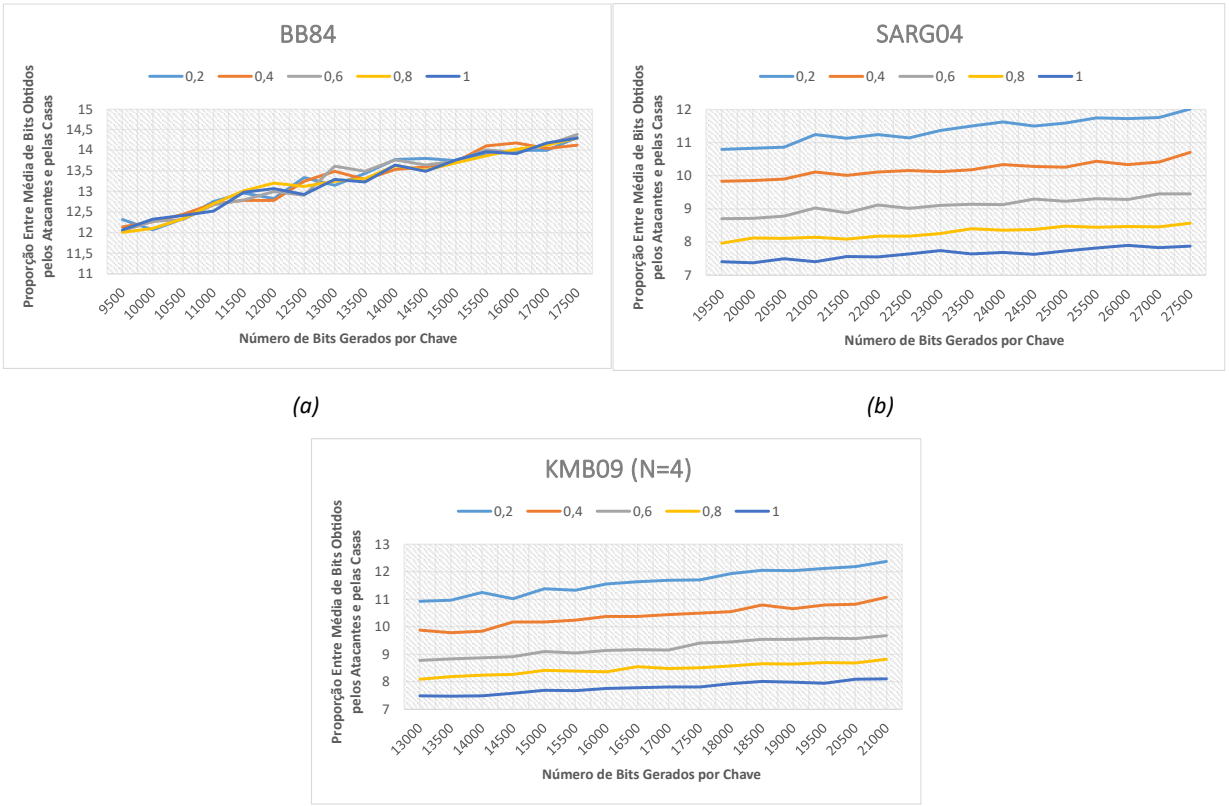


(a) *(b)*

(c)

Figura 26: Taxa da chave quântica gerada que é decifrada por Eve num ataque intercept-and-resend utilizando os vários protocolos (a)BB84 (b)SARG04 e (c)KMB09(N=4), para $\mu = 0.2$ e para várias probabilidades deocorrência de ataque numa ligação, em função do número de bits de cada chave gerada.

É visível nos gráficos da Fig. 26 que a taxa média de *bits* obtida por Eve neste ataque é proporcional à eficiência de leitura de cada protocolo, na medida em que a eficiência de leitura de KMB09(N=4) é 1.5 vezes superior à de SARG04, que por sua vez é metade da de BB84, como está ilustrado na Fig.15. Na Figura 27, que mostra a proporção entre o número médio de *bits* obtidos por Eve e as respetivas casas, cujo canal quântico foi atacado é possível observar que o número médio de *bits* obtidos por Eve é muito superior ao número médio de *bits* obtidos por cada casa na rede, para os mesmos valores de probabilidades de ataque da figura anterior, simulado ao longo de vários tamanhos de chaves geradas.

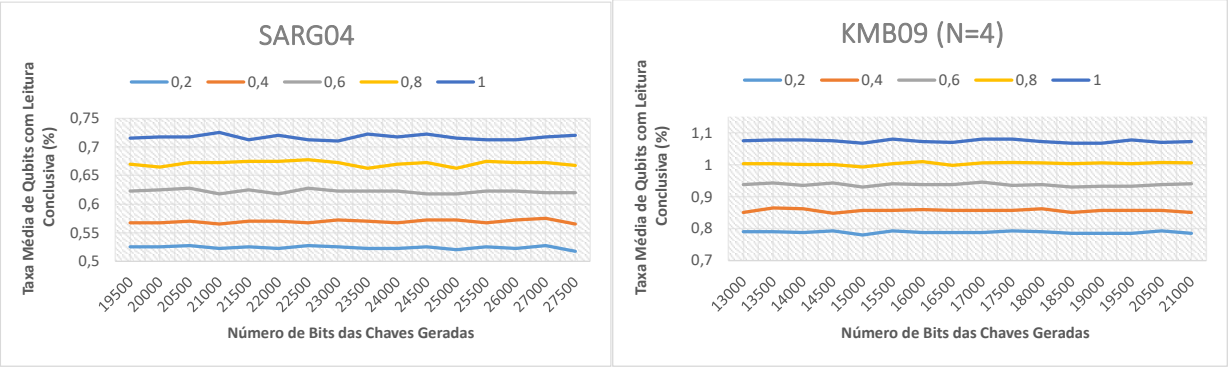


(a) *(b)*

(c)

Figura 27: Proporção entre a média de bits obtidos por Eve num ataque e a média de bits obtidos pelas casas, ambos nas condições de leitura mencionadas, para várias probabilidades de ataque numa ligação, em função do número de bits de cada chave gerada.

O facto das proporções entre o número de *bits* das chaves resultantes de Eve e das casas aumentar com κ, é explicado em virtude da probabilidade de leitura de Eve ser sempre superior à casa que sofre o ataque. Já o facto de, para SARG04 e KMB09, estas proporções das médias de *bits* obtidos dependerem da probabilidade de ataque, advém do facto da presença de um ataque conferir mais *qubits* conclusivos à casa que sofre o ataque. Dessa forma, quanto maior o número de ataques na rede, maior o valor da média de *bits* nela obtidos, ainda que esse excesso de *bits* resultantes, se traduza exclusivamente em *bits* errados. A taxa média de *qubits* de leitura conclusiva na rede, seguindo as mesmas probabilidades de ataque *intercept-and-resend*, para vários valores de κ, para estes dois protocolos encontra-se na Figura 28. É de notar que os valores de taxa média de *qubits* com leitura conclusiva são afetados pela probabilidade de leitura de um *qubit*, resultante do modelo de receção utilizado.

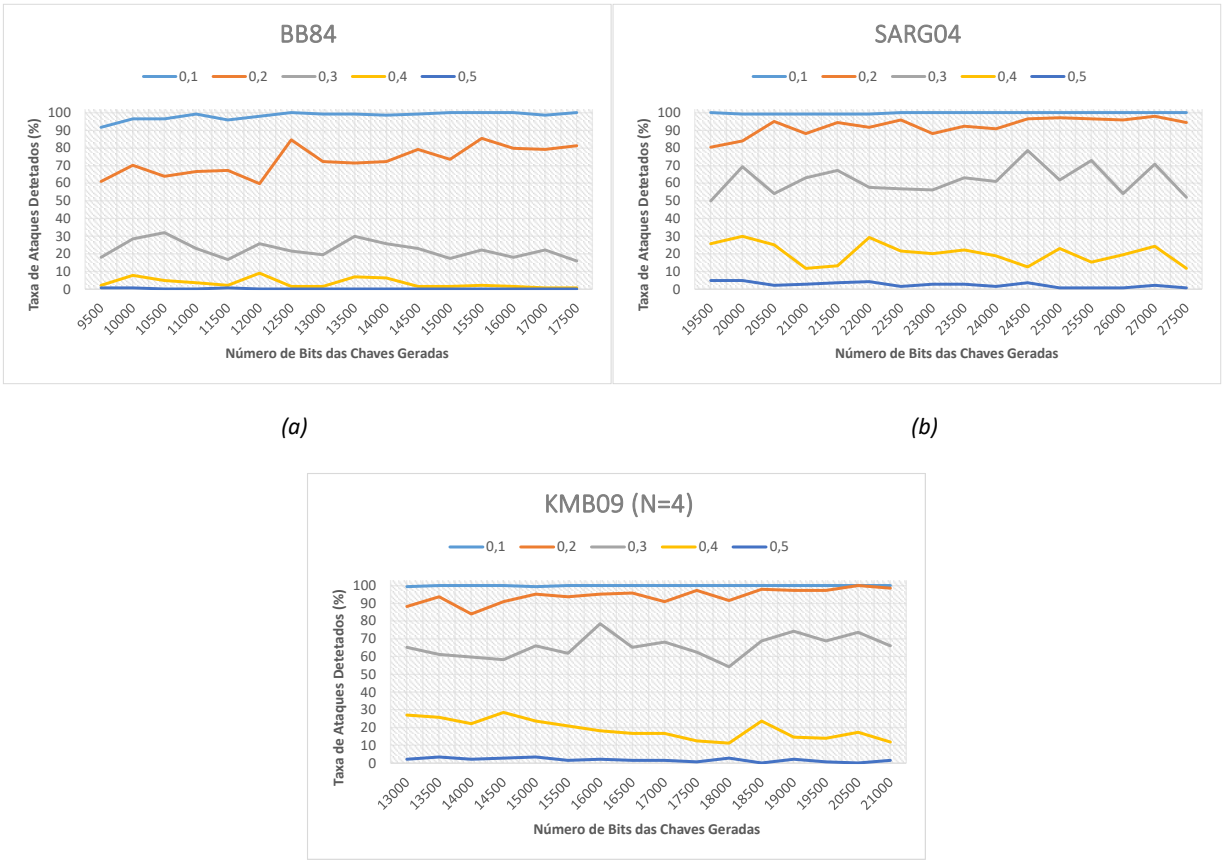


(a) *(b)*

Figura 28: Taxa de qubits da chave gerada cuja leitura foi conclusiva nos protocolos (a) SARG04 e (b) KMB09(N=4) nas condições de leitura mencionadas, para várias probabilidades de ataque a cada ligação da rede, em função do número de bits de cada chave gerada.

Este fenómeno pouco expectável e não descrito na literatura consultada, ocorre devido às propriedades do funcionamento da fase de pós processamento no canal público destes dois protocolos, em que cada recetor só pode concluir algo acerca dos *bits* que foram lidos incorretamente, como descrito em 3.4.5.2 e 3.4.5.3. O facto de Eve alterar a mensagem quântica permite que haja mais *qubits* com leitura conclusiva, ainda que estes estejam errados. Já no caso de BB84, em que o pós processamento corresponde simplesmente ao envio das bases utilizadas por parte das casas, em que o CC apenas indica quais as que foram utilizadas corretamente, a presença de um atacante em nada influencia o número de leituras conclusivas.

Apesar deste fenómeno poder representar uma forma complementar de deteção de erro, este trabalho deteta a presença de um Eve por análise de um certo número de *bits* de teste, proporcional ao número de *bits* da chave gerada por CC (κ). A análise é feita calculando a taxa de *bits* de teste errados e comparando esse valor com um limiar aceitável estabelecido. A análise da taxa de erros detetados é ilustrada na Figura 29, sendo que, na ausência de ruído, todos os erros existentes se devem a ataque. A probabilidade de ataque é fixada a 1, ou seja, todas as ligações da rede sofrem ataque, por forma a manter o número de erros constante. A análise é feita para vários limiares máximos de *bits* de teste errados aceites: 10% , 20% , 30% , 40% e 50% , para vários tamanhos de κ, para os diversos protocolos.

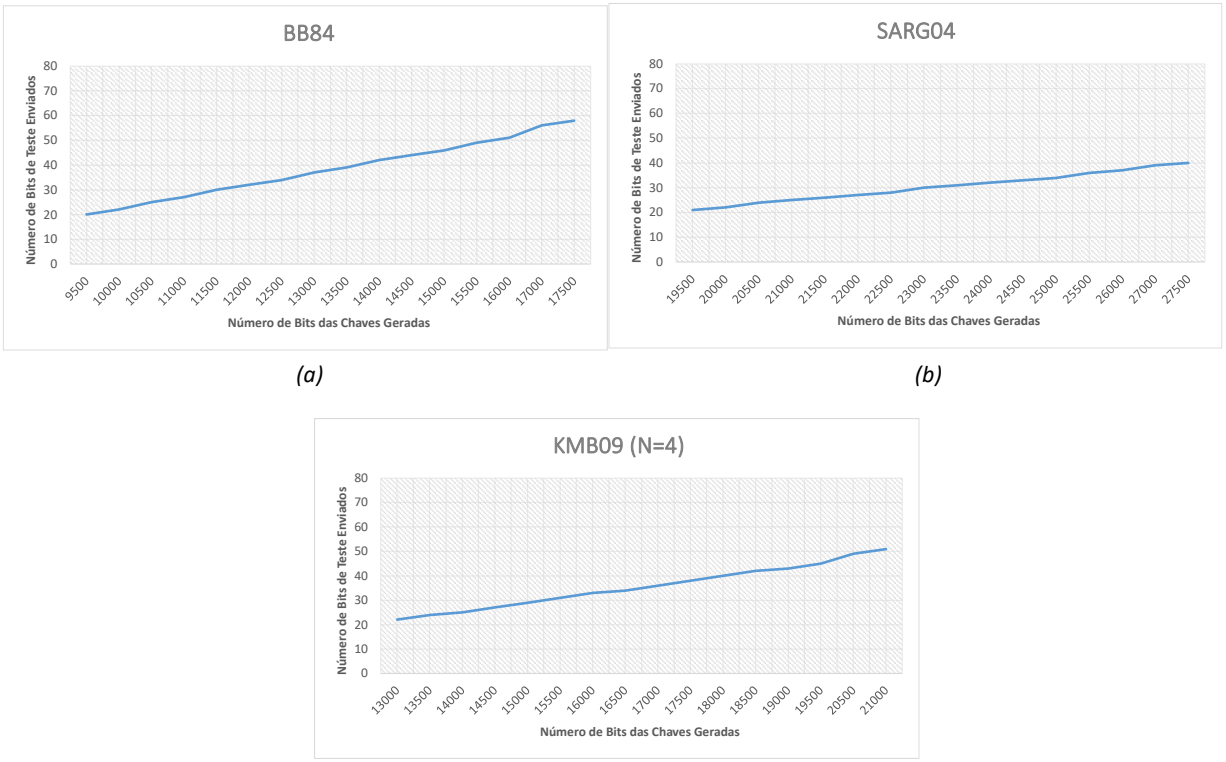


(a) *(b)*

(c)

Figura 29: Taxa de erros detetados num cenário em que todas as ligações entre CC e as respetivas casas sofrem um ataque, para vários valores de limiares de percentagem de máximo de bits de teste errados, em função do número de bits de cada chave gerada.

Conclui-se assim que, para um limiar máximo de 10% de *bits* de teste errados aceitáveis, a probabilidade de deteção de ataque é bastante elevada. Contudo, se esse limiar for de 20% ou mais, não se garante deteção de um ataque *intercept-and-resend*, principalmente para o protocolo BB84. Portanto, conclui-se que a taxa de *bits* de teste errados aceitável afeta a deteção de ataques de forma diferente nos vários protocolos, sendo que BB84 requer limiares máximos de taxas de *bits* de teste errados mais baixos, o que acontece apesar dos *bits* de teste partirem do mesmo valor (cerca de 20 nos três protocolos).



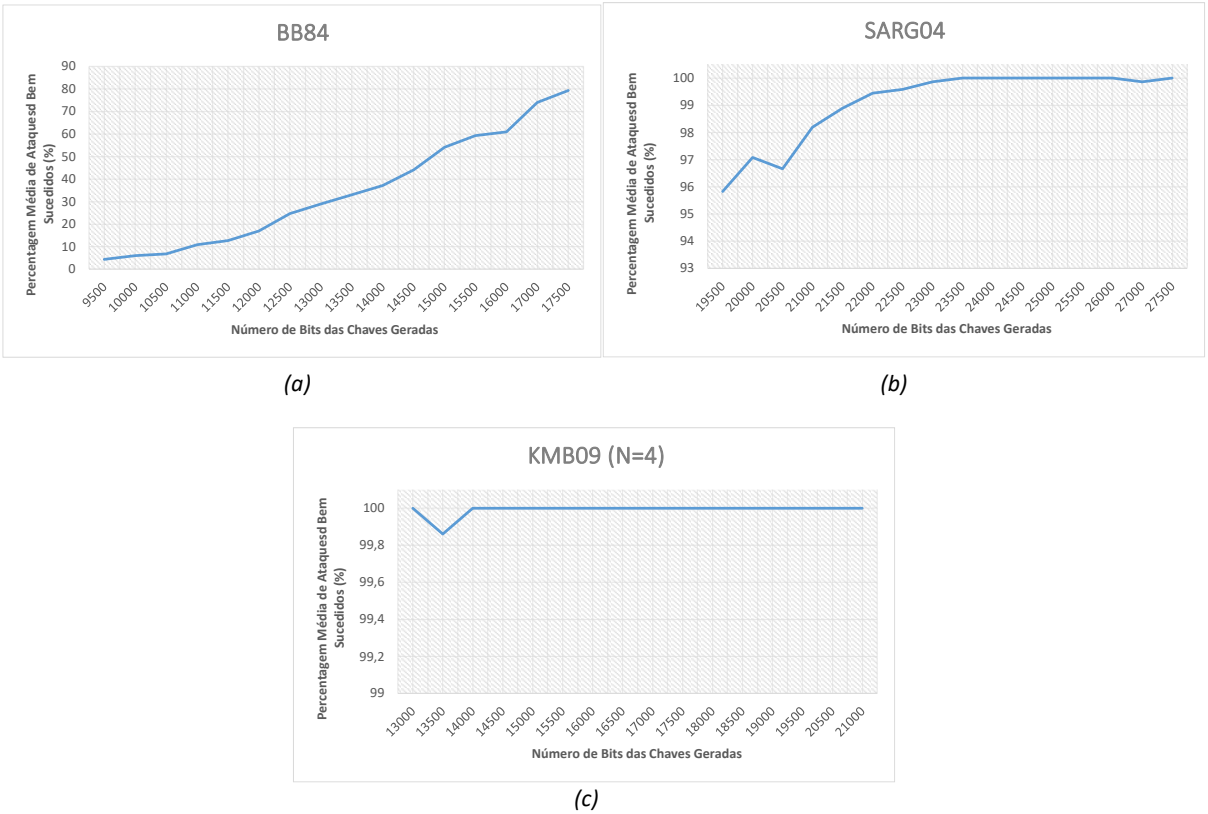
(a) *(b)*

(c)

Figura 30: Número de bits de teste enviados para os protocolos (a)BB84, (b)SARG04 e (c)KMB09(N=4), em função dos valores de κ simulados.

Contudo, em todas as simulações realizadas na presença de ataques *intercept-and-resend* nos 3 protocolos distintos, contabilizando um total de 2040 simulações para vários valores de κ, probabilidades de ataque e limiares de deteção de erros, não foi detetada uma única ocorrência de um ataque bem sucedido nestas condições. Tal pode ocorrer devido ao facto de Eve obter bastantes mais *bits* do que a casa atacada, o que origina chaves não correspondentes entre os dois quando comparadas. Conferindo alguma seletividade à chave obtida por Eve, descartando os *bits* nas posições em que a casa atacada nada pode concluir, conduz a que Eve obtenha uma menor percentagem de *bits* no ataque, porém, aumenta a probabilidade de obter a mesma chave que é usada pela casa atacada. Isto é possível uma vez que cada casa necessita de comunicar as posições dos *bits* obtidos ao CC, por forma a que ambos obtenham a mesma chave resultante.

A simulação anterior foi repetida, porém, agora Eve descarta os *bits* que obteve nas posições em que a casa nada pôde concluir. As taxas de ataques bem sucedidos que ocorreram na rede, para uma probabilidade de ataque de 1 nos canais quânticos da rede foram os seguintes:

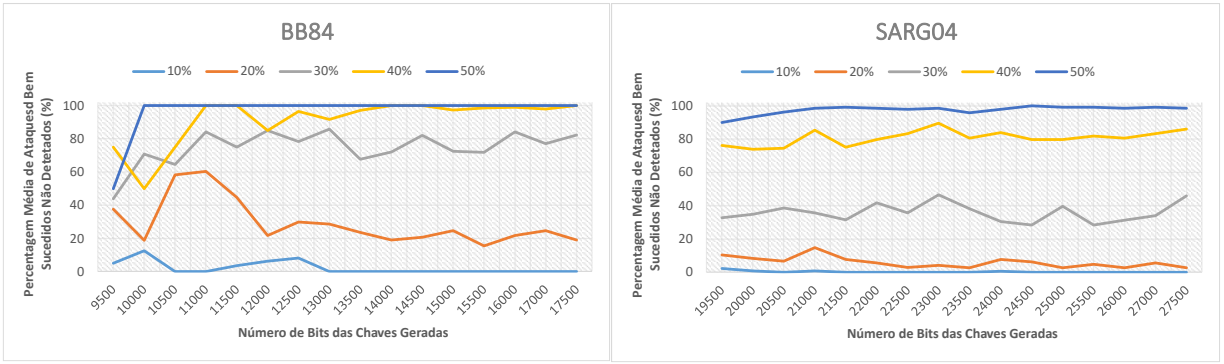


(a) *(b)*

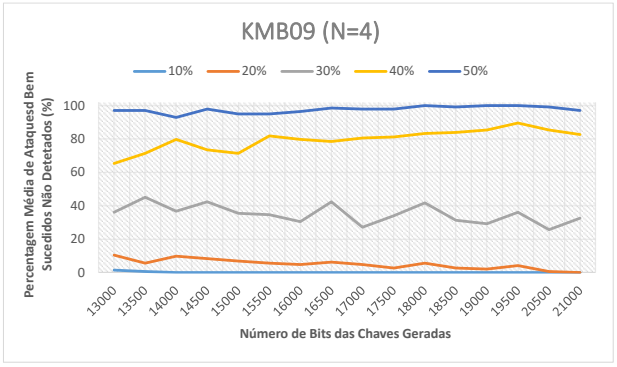
(c)

Figura 31: Taxa média de ataques bem sucedidos, para os protocolos (a)BB84, (b)SARG04 e (c)KMB09(N=4), num cenário em que Eve descarta os bits não obtidos pela casa atacada, em função do tamanho das chaves geradas.

Contudo, estas ocorrências de ataques bem sucedidos por parte de Eve, estão sujeitas a deteção pelo CC, portanto, é necessário averiguar quantos desses ataques passaram despercebidos, conforme os limiares de deteção utilizados: 10% , 20% , 30% , 40% e 50%.



(a) *(b)*



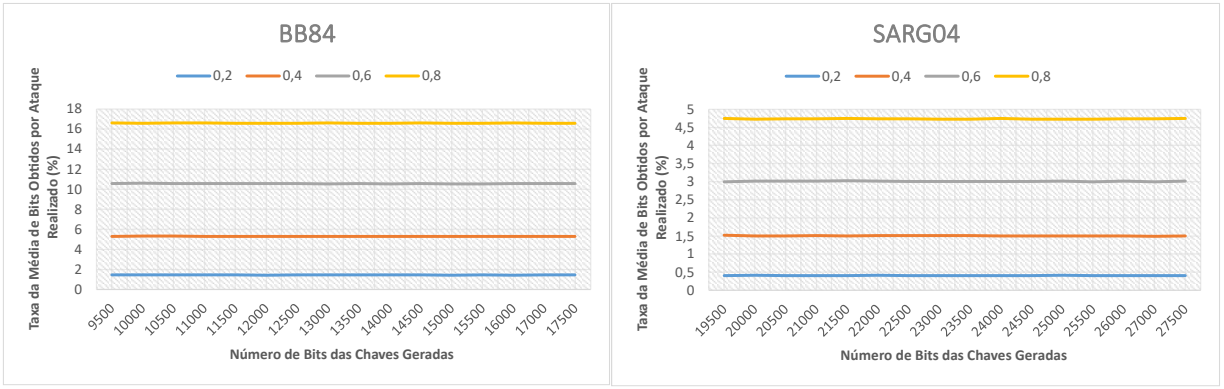
(c)

Figura 32: Taxa média de ataques bem sucedidos não detetados por CC aquando da troca de bits de teste, para os protocolos (a)BB84, (b)SARG04 e (c)KMB09(N=4), em função do número de bits das chaves geradas.

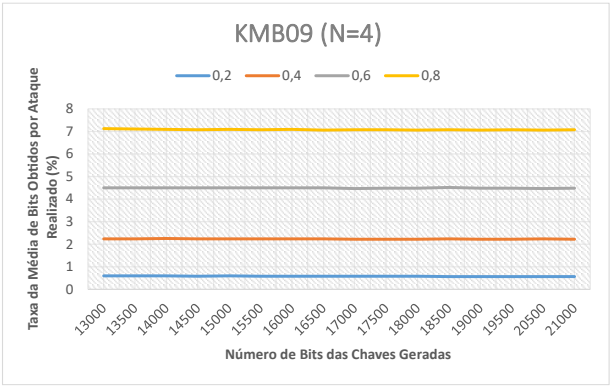
Conclui-se que, para garantir a segurança do sistema perante ataques *intercept-and-resend* é imperativo um limiar aceitável de *bits* de teste errados inferior a 10%, caso contrário, a percentagem de ataques bem sucedidos não detetados pode comprometer o funcionamento de QKD na rede em causa, especialmente para o protocolo BB84.

7.5. Presença de Ataques *Photon-Number Splitting*

O ataque PNS é simulado nas mesmas condições que *intercept-and-resend*. Inicialmente, é analisada a percentagem de *bits* que este ataque confere ao atacante nos diversos protocolos, para vários valores de μ = 0.2, 0.4, 0.6 e 0.8, para valores de κ, num cenário em que todas as casas darede sofrem um ataque deste tipo.



(a) *(b)*

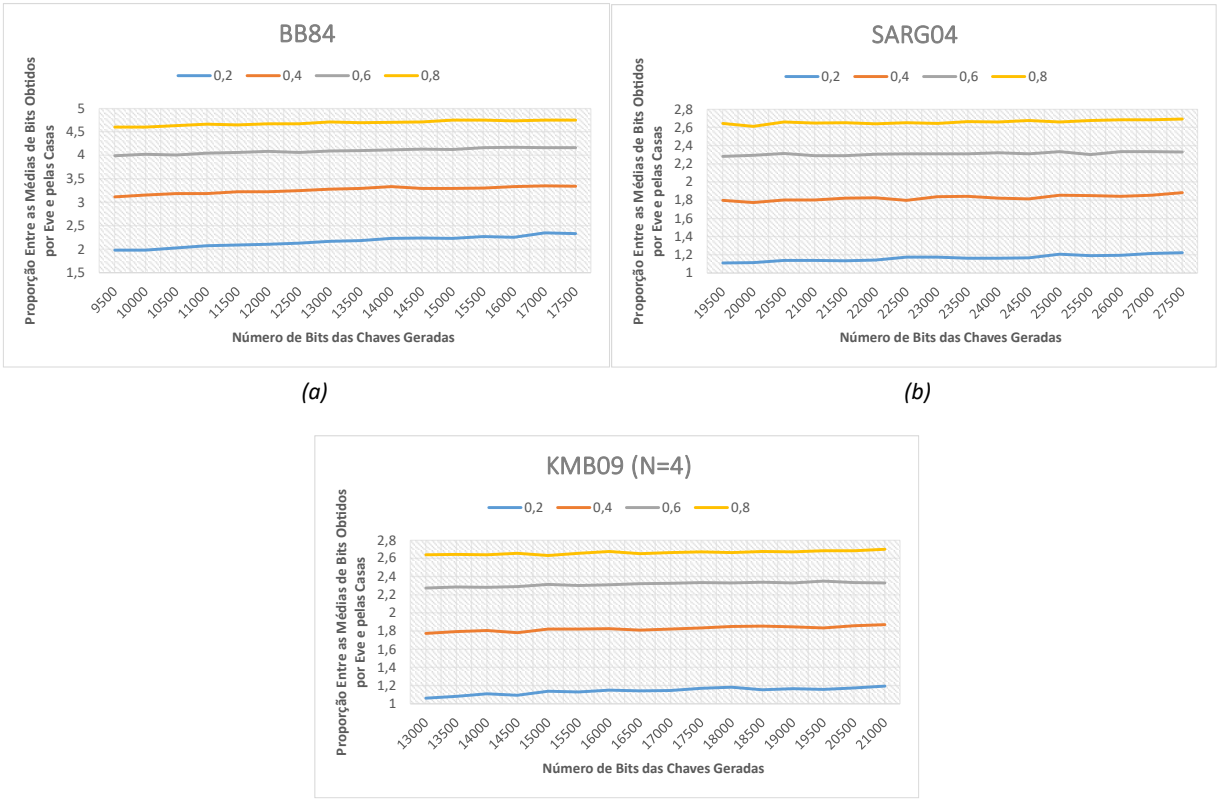


(c)

Figura 33: Taxa da chave quântica gerada que é decifrada por Eve num ataque PNS, utilizando os vários protocolos (a)BB84 (b)SARG04 e (c)KMB09(N=4), para vários valores de μ, em função do número de bits de cada chave gerada.

Comparando os valores das figuras acima com as taxas de *bits* obtidos pelo ataque *intercept-and-resend*, na Fig. 26, conclui-se que um Eve num ataque PNS apenas consegue atingir esses valores quando o sistema utiliza uma intensidade média de fotões por pulso alta.

A proporção média entre os *bits* obtidos por Eve num ataque e pela casa que sofre o ataque PNS encontra-se ilustrada na Figura 34.

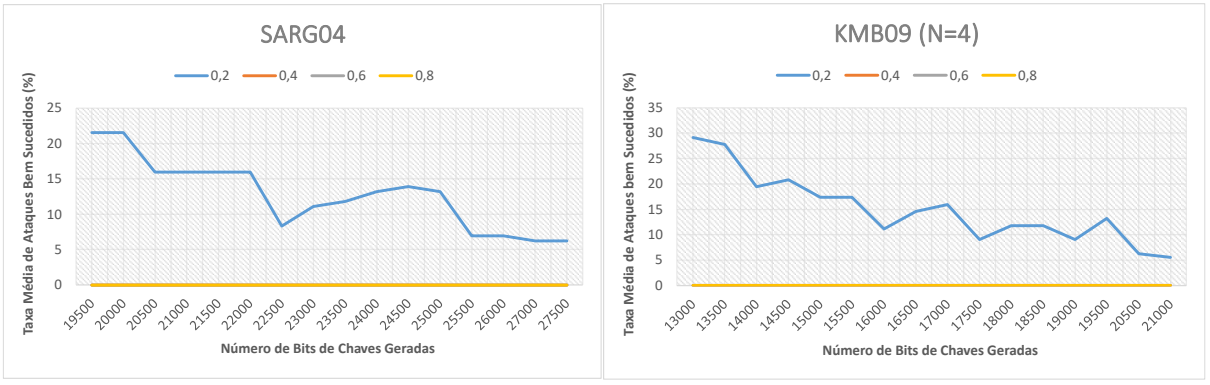


(a) *(b)*

(c)

Figura 34: Proporção entre a média de bits obtidos por Eve num ataque PNS e a média de bits obtidos pelas casas, nos 3 protocolos simulados (a) BB84, (b) SARG04 e (c) KMB09 (N=4), para várias intensidades médias por pulso μ, em função do número de bits de cada chave gerada.

As médias de *bits* obtidos entre os 3 diferentes protocolos estão de acordo com a literatura, na qual, para BB84, todos os *qubits* constituídos por mais do que um fotão, são conclusivos, enquanto esse número é diminuído em SARG04 e KMB09, uma vez que não partilham toda a informação necessária no canal público. Existem casos em que Eve, nestas condições, obtém a mesma chave que a casa atacada precisamente nestes últimos dois protocolos, enquanto para BB84 não foi registado nenhum ataque bem sucedido.

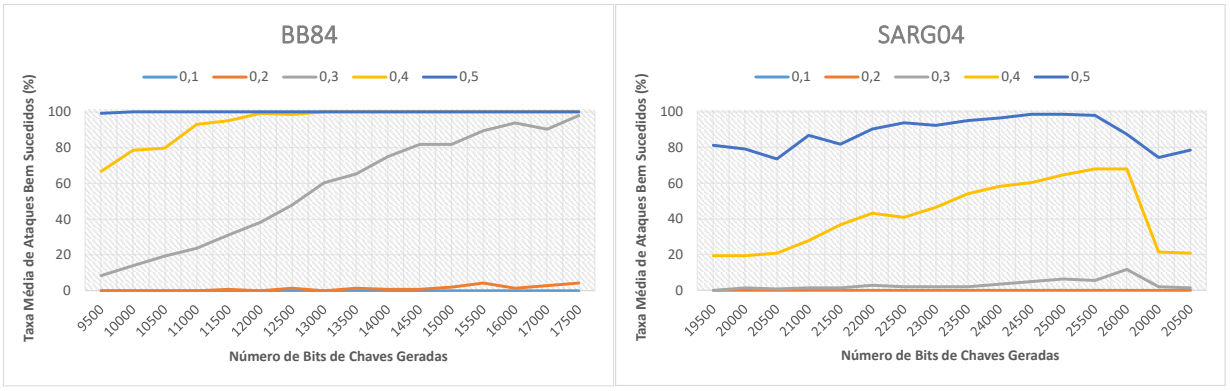


(a) *(b)*

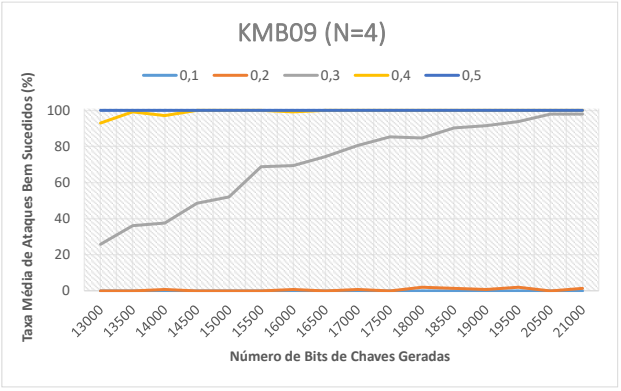
Figura 35: Taxa de ataques PNS bem-sucedidos, para vários valores de μ, em função do número de bits de cada chave gerada, para os dois protocolos SARG04(a) e KMB09(N=4)(b).

Como se pode observar na Figura 35, apenas para $\mu = 0.2$, Eve consegue obter uma boa percentagem das chaves resultantes, uma vez que os restantes valores de μ se encontram sobrepostos em zero, relembrando que a rede simulada é constituída por apenas 36 casas que executam processos de QKD. Tal não foi registado para outros valores de μ nestes protocolos, em que o número de *bits* obtidos por Eve é bastante superior nesta ordem de valores de κ, nem para nenhum valor de μ quando se utilizou BB84. Estas incongruências nos resultados de ataques bem-sucedidos em ataques PNS devem-se a dois fatores distintos. Primeiro, o número de fotões por *qubit* é calculado com recurso ao produto das probabilidades p_n (descritas em 3.5.1) e o valor de κ, resultando assim o número de frequência absoluta de cada valor n. O número de fotões ao longo de cada*qubit* da mensagem quântica é depois atribuído segundo uma variável pseudoaleatória. Assim, os casos menos comuns ocorrem maioritariamente no início da chave quântica transmitida, enquanto o final da mesma é constituído principalmente por *qubits* nulos. O outro fator que pode conduzir a estes resultados é, à semelhança do que se verificou com o ataque *intercept-and-resend*, o facto de neste ataque Eve também obter bastantes mais *bits* na sua chave resultante do que a casa atacada, o que provoca uma discrepância quando comparadas ambas as chaves. Dessa forma, é normal que as condições em que a proporção de *bits* resultantes entre atacante e atacado sejam aproximadamente 1, correspondam à ocorrência de casos em que as chaves finais de ambos possam ser iguais.

A simulação é então repetida, porém, Eve agora ignora os *qubits* nas posições em que a casa nada concluiu acerca da chave quântica transmitida. As taxas médias de ataques PNS bem sucedidos encontram-se na Figura 36.



(a) *(b)*



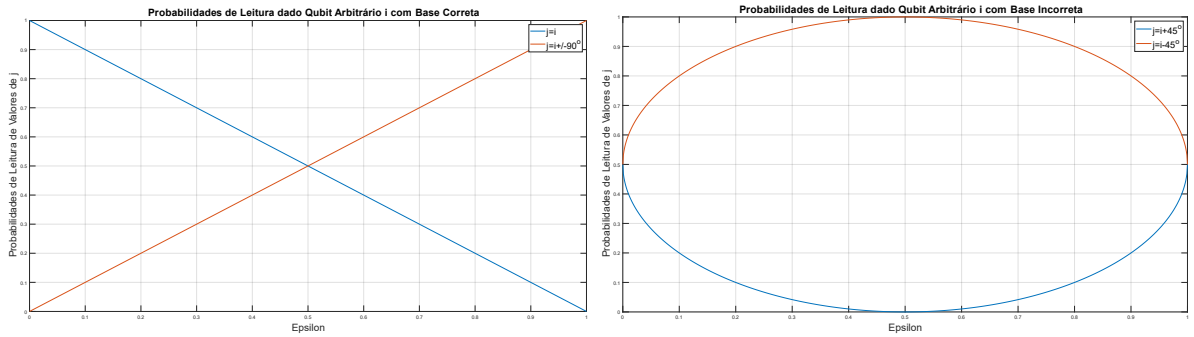
(c)

Figura 36: Taxa média de ataques PNS bem-sucedidos, para vários valores de μ, para os protocolos (a)BB84, (b)SARG04 e (c)KMB09(N=4), em função do número de bits de cada chave gerada.

O facto de Eve ignorar as posições da chave resultante, em que a casa não concluiu nenhum *bit*, resulta numa taxa de ataques bem sucedidos ao longo da rede muito mais realista. Como era expectável, pela literatura consultada, o protocolo SARG04 mostra-se bastante mais resiliente perante este ataque, em comparação com os restantes protocolos. Outra conclusão importante é que, quando Eve executa apenas este tratamento à sua chave obtida, as taxas médias de ataques bem sucedidos são bastantes reduzidas para μ = 0.2. De notar que, na Fig. 35, a taxa média de ataques para este valor de μ é superior, provavelmente devido a obtenções da mesma chave que a casa por mera coincidência, uma vez que não são comparados *bits* diferentes em posições diferentes entre os dois.

7.6. Impacto de Ruído de Despolarização

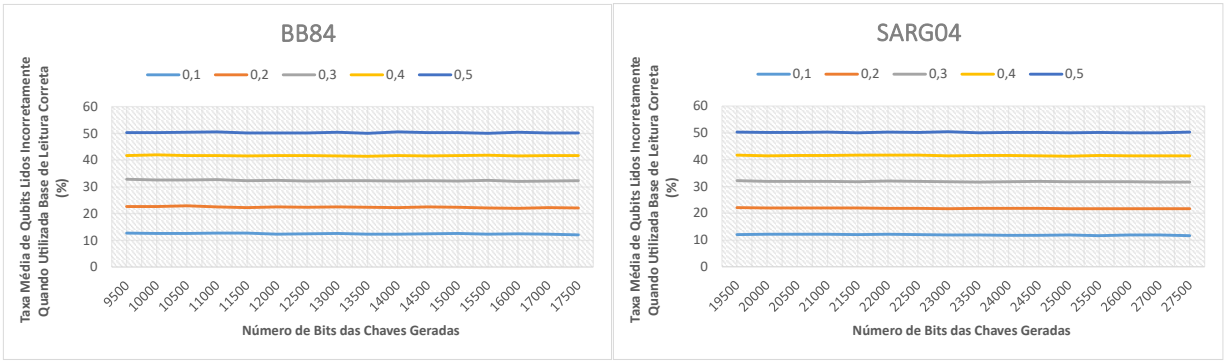
Primeiramente, é necessária uma análise da Tabela 6 que demonstra as consequências das probabilidades de leitura de um dado estado em função do estado enviado e da base utilizada, para vários valores de θ, que depende de $\varepsilon \in [0,1]$. Da tabela é retirado que, independentemente do estado enviado, utilizando a base correta de leitura (a mesma base utilizada na codificação do *qubit* nesse estado) é $cos^2(\theta)$, enquanto a leitura do estado errado nas mesmas condições é de $sen^2(\theta)$. Também se pode concluir que a probabilidade de leitura de um *qubit* num estado que corresponde a $+45^o$ do que foi enviado é de $\frac{1-sen(2\theta}{2}$ por exemplo enviado $i = 45^o$ e leitura de $j = 90^o$, enquanto a probabilidade da leitura de um estado que corresponde a $j = i - 45^o$ é de $\frac{1+sen(2\theta)}{2}$. Dessa forma, é possível analisar as probabilidades de leitura de qualquer estado j dependendo se essa é ou não a mesma base utilizada na codificação desse *qubit*, ilustradas na figura:



(a) *(b)*

Figura 37: Probabilidades de leitura de um estado j quando enviado um dado estado i, com uso da mesma base utilizada na sua codificação (a) e com base diferente (b), em função do parâmetro de ruído ε.

Uma vez que a leitura de um *qubit* com uma base diferente da que foi utilizada na codificação do mesmo se traduz automaticamente numa leitura errada, o foco corresponde à probabilidade de leitura incorreta com uso de base correta. Na figura seguinte é ilustrada a taxa de leituras incorretas com utilização de base correta, tendo por base apenas os *qubits* lidos ao invés dos *qubits* emitidos. Para a análise dos efeitos de ruído de despolarização, são utilizadas as condições de leitura consideradas em 7.2 ($\mu = 0.2$, $\eta_{det} = 10\%$, $\alpha = 0.2\ dB/km$ e $L = 1\ km$). Como não foi possível obter uma relação entre L e ε, foram simulados valores de $\varepsilon = \{0.1; 0.2; 0.3; 0.4; 0.5\}$, em função do valor de κ.

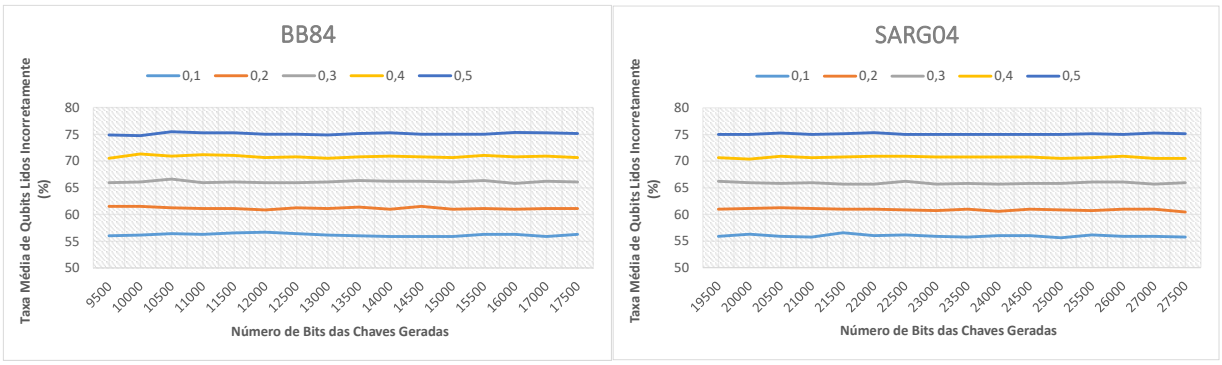


(a) *(b)*

Figura 38: Taxa média de qubits lidos incorretamente quando utilizada a base de leitura correta, considerando apenas os qubits lidos, para ambos os protocolos (a) BB84 e (b)SARG04, nas condições de leitura e transmissão mencionadas, para vários valores de ε, em função do número de bits das chaves geradas.

Como se pode verificar, o ruído tem um efeito análogo ao erro de leitura quando utilizada uma base correta. Os valores divergem ligeiramente dos teóricos, num máximo de 2.5% para todas as simulações, devido à pseudoaleatoriedade de acontecimentos e arredondamentos do produto da probabilidade de cada leitura com o número de *qubits* num dado estado. Contudo, este desvio é desprezável, dado o número médio de *qubits* lidos em cada simulação.

A taxa média de *qubits* lidos de forma errada também afeta ambos os protocolos de forma semelhante, como ilustra a Figura 39.

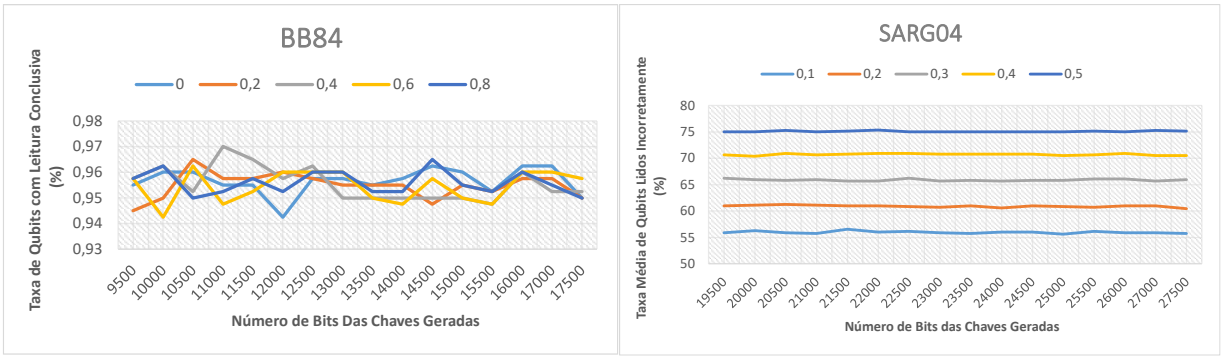


(a) *(b)*

Figura 39: Taxa média de qubits lidos incorretamente, considerando apenas os qubits lidos, para ambos os protocolos (a) BB84 e (b)SARG04, nas condições de leitura e transmissão mencionadas, para vários valores de ε, em função do número de bits das chaves geradas.

Após analise dos resultados da taxa de erros detetados, qualquer valor de ε utilizado nesta simulação corresponde a uma taxa de deteção de erro de $\cong$ 100%, quando se utiliza o limiar máximo escolhido nas conclusões da Fig. 32, ou seja, 10% de *bits* de teste errados na retificação.

Contudo, quando se utiliza o SARG04, à semelhança da presença de ataques *intercept-and-resend*, o número médio de *qubits* alterados no canal quântico, contribui para que a taxa média de *qubits* de leitura conclusiva aumente proporcionalmente ao valor de ε , algo que não ocorre quando utilizado BB84, como justificado em 7.3. De notar que os seguintes resultados de taxas médias de *qubits* conclusivos foram calculados com base na totalidade de *qubits* transmitidos.



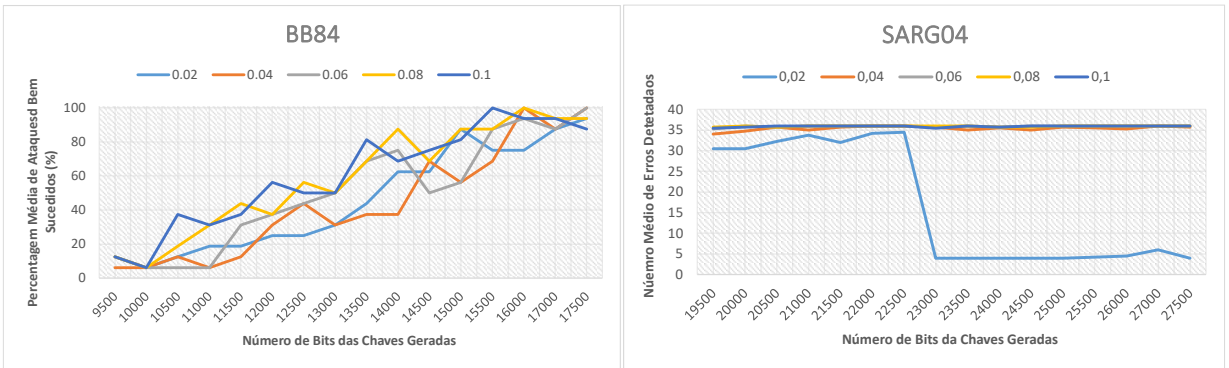
(a) *(b)*

Figura 40: Taxa de qubits da chave gerada cuja leitura foi conclusiva nos protocolos (a) BB84 e (b) SARG04, nas condições de leitura mencionadas, para vários valores de ε, em função do número de bits de cada chave gerada.

Contudo, à semelhança do que acontecia em *intercept-and-resend*, este aumento de *qubits* conclusivos traduz-se exclusivamente em *bits* errados na chave resultante.

7.7. Impacto de Ruído de Despolarização na Presença de Ataques *Intercept-and-Resend*

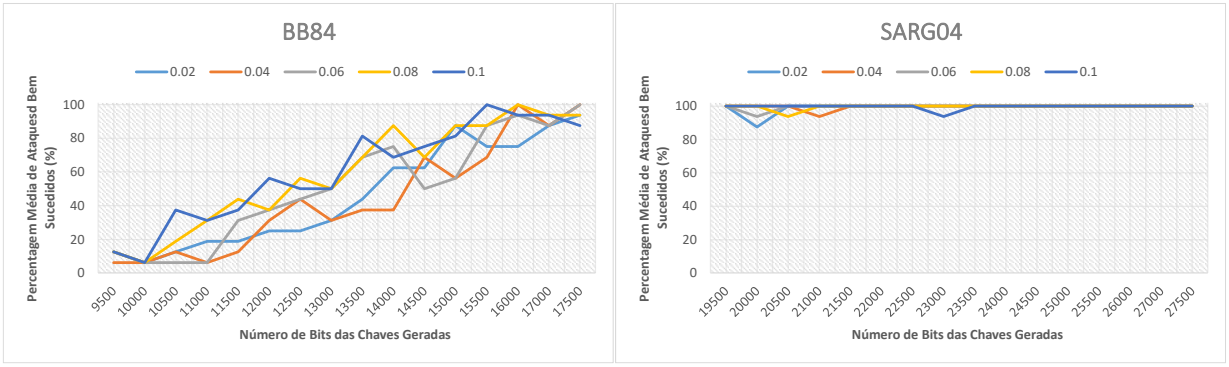
Pretende-se, por último, averiguar o impacto que o ruído de despolarização tem na deteção de ataques *intercept-and-resend*, uma vez que na prática ambos têm o mesmo efeito na retificação dos *bits* de teste. Nas simulações feitas, considerou-se uma probabilidade de ataque fixa de 0.1, que provoca um total de 4 ataques em toda a rede. As condições de leitura correspondem às que foram vulgarmente utilizadas nas simulações ($\mu = 0.2$, $\eta_{det} = 10\%$, $\alpha = 0.2\ dB/km$ e $L = 1\ km$), e os parâmetros de ruído analisados são de $\varepsilon = \{0.02; 0.04; 0.06; 0.08; 0.1\}$, uma vez que as ligações em causa são de curta distância, e como tal, não são afetadas por elevados níveis de ruído. Além disso, como mencionado em 7.6, valores de ε superiores a 0.1, traduzem-se automaticamente numa taxa de erros detetados na rede de 100%, para o limite máximo de *bits* de teste errados utilizado. Na Figura 40 é analisado o número de erros detetados, tendo em conta que apenas são efetuados quatro ataques em toda a rede, considerando que a percentagem máxima de *bits* de teste errados aceite é de 10%, como concluído em 7.4.



(a) *(b)*

Figura 41: Número de erros detetados nos protocolos BB84 (a) e SARG04 (b), nas condições de leitura mencionadas, para vários valores de ε, com uma deteção baseada num limiar máximo de bits de teste errados de 10%, em funçãodo número de bits de cada chave gerada.

Como se pode verificar na figura acima, o limiar máximo de bits de teste errados aceitável escolhido torna o sistema bastante intolerante ao ruído. Conclui-se por observação dos gráficos que apenas é exequível para valores de $\varepsilon \leq 0.02$, e para um valor de $\kappa \geq 14000$ e $\kappa \geq 23000$, para BB84 e SARG04, respetivamente. É, conveniente salientar que, apesar da maioria dos quatro ataques na rede serem bem sucedidos, como mostra a Figura 42, não houve uma única verificação de um ataque bem sucedido não detetado, para ambos os protocolos.



(a) *(b)*

Figura 42: Taxa média de ataques bem sucedidos nos protocolos BB84 (a) e SARG04 (b), nas condições de leitura mencionadas, para vários valores de ε, com uma deteção baseada num limiar máximo de bits de teste errados de10%, em função do número de bits de cada chave gerada.

Ainda que a variação entre os valores de ε utilizados seja pouca, é notório que, para BB84, as taxas de ataques bem sucedidos são relativamente superiores para $\varepsilon = 0.1$, enquanto que para SARG04, em praticamente todas as simulações, os quatro ataques realizados foram bem sucedidos.

8 Trabalho Futuro

Apesar de a simulação ser satisfatória, uma vez que o método de QKD desenvolvido contempla inúmeros fenómenos presentes nos sistemas, aplicados num cenário de *smart grid*, existem várias melhorias possíveis ao código já criado, bem como novas implementações que permitirão tornar a plataforma mais realista. As melhorias mencionadas dizem respeito a:

1. A pseudoaleatoriedade utilizada neste programa não é perfeita ao nível do número de fotões por *qubit* emitido pelo CC, *qubits* suprimidos por atenuação e *qubits* cuja polarização é alterada. Contudo, garante uma boa aproximação de todos os fenómenos simulados numa potencial implementação prática destes sistemas. Desta forma, é de interesse o uso de uma aleatoriedade mais realista em todos estes fenómenos mencionados por forma a obter resultados que se aproximam mais da realidade.
2. As simulações podem ter um ataque bem sucedido ou não, por comparação direta das chaves. No funcionamento do BB84, é possível adicionar complexidade ao obter a percentagem correta pelo atacante, que implica o conhecimento da posição dos *bits* que obteve relativamente à da chave da casa atacada. Tal permitiria averiguar quantas combinações de valores de *bits* desconhecidos teria Eve que fazer por forma a obter a chave utilizada na codificação da mensagem transmitida.

Além destas melhorias, existem também vários fatores que não puderam ser abordados neste trabalho e que iriam incrementar o nível de complexidade e realismo deste simulador. Segue-se uma descrição do que se considera serem os primeiros passos nesse sentido:

1. Os ataques PNS são assumidos como bem sucedidos, uma vez que não foi simulado nenhum método de deteção destes ataques. Tal poderia ser implementado por exemplo com base na análise estatística do número de fotões recebidos. Esse aspeto poderia ser útil para obter conclusões acerca de valores mínimos de fotões recebidos por chave quântica aceitáveis, dadas diversas combinações de fatores de atenuação e valores de μ.
2. Incorporar fenómenos de transmissão de informação quântica não abordados neste programa, como o de efeito de *Decoherence*.
3. Neste trabalho, o ruído de despolarização é tratado exclusivamente como ruído coletivo. Uma melhor análise desse fenómeno seria torná-lo dinâmico ao longo de cada mensagem quântica.
4. O modelo coletivo do ruído de despolarização apenas é aplicável para protocolos quânticos que fazem uso de quatro estados possíveis. Uma possível melhoria seria estender a aplicação do ruído de despolarização a protocolos quânticos que não contemplam outros números de estados de polarização possíveis.
5. Implementação de erros derivados de *dark counts* e estudo dos seus efeitos e métodos de correção de erros necessários, mediante o tipo de fotorrecetor utilizado.
6. Incluir a opção de encriptação AES, por forma a averiguar qual dos métodos é o mais apto para este cenário de rede.

9 Conclusão

Neste trabalho foi proposta uma análise ao impacto de diversos fatores e ataques numa solução QKD com os protocolos BB84, SARG04 e KMB09, funcionando sobre uma *smart grid* ao nível residencial, cujas casas necessitam de atribuição de chaves para codificação OTP dos seus consumos, cujo tamanho médio é de cerca de 45 *bits*. O método criado para o efeito considera-se bem sucedido, uma vez que os resultados obtidos não só vão ao encontro do que é afirmado na literatura consultada, como permitiram retirar algumas conclusões acerca de uma possível implementação prática nos diversos cenários simulados.

Provou-se o funcionamento consistentemente correto dos protocolos simulados, através dos resultados obtidos num cenário de utilização de *hardware* ideal em toda a rede, na ausência de ataques.

Para condições de transmissão reais, considerando as várias limitações do *hardware* requerido ao longo da rede e tendo em conta os parâmetros simulados $\mu = 0.2, \eta_{det} = 10\%, \alpha = 0.2\ dB/km$ e $L = 1\ km$, foi estabelecida uma possível relação entre os *bits de* teste enviados e o tamanho da chave gerada pelo CC, presentes na Tabela 7, obtida por forma a garantir chaves resultantes de tamanho suficiente para codificação OTP dos consumos. Verificou-se também que essas condições de transmissão de *qubits* entre o CC e cada casa da rede, provocam um aumento substancial no QBER médio da rede, em comparação com um cenário de condições ideais, provocado pela baixa probabilidade de leitura de *qubits*. Tal representa um problema, uma vez que diminui o número de *bits* das chaves resultante, sendo que, é requerido que corresponda ao mesmo número de *bits* do consumo a transmitir. A solução mais fácil para o problema consiste simplesmente em aumentar o tamanho das chaves geradas pelo CC, por forma a aumentar o número de *qubits* lidos e consequentemente o número de *bits* obtidos (ainda que na prática tal resultaria numa redução da taxa de atribuição de chaves, o que não foi considerado neste programa). A tabela com os tamanhos mínimos de chave gerada pelo CC, por forma a que, nestas condições, todas as casas da rede obtenham *bits* resultantes suficientes para a codificação dos seus consumos, encontra-se na Tabela 8. Como era expectável, o incremento da distância mostrou-se uma grande limitação quando se simulou a utilização de *hardware* convencional, pelo que o simples aumento dos tamanhos das chaves geradas não constitui uma solução. Esta limitação é acentuada para protocolos cuja eficiência de leitura é menor, em especial, o caso de SARG04. Assim, para cenários nestas condições em que são necessárias distâncias superiores entre as casas e o CC, conclui-se que a solução mais viável seria equipar cada casa com um fotorrecetor cuja eficiência fosse ligeiramente maior. É de notar que no método QKD simulado, o recurso a fotorrecetores com 12% de eficiência de leitura, ao invés de 10%, mitigou substancialmente o número de casas com chave resultante insuficiente para OTP, para distâncias até 9 km.

As simulações na presença de ambos os ataques foram propositadamente feitas de forma a analisar o pior cenário possível para a rede, em que Eves apenas são afetados pelo número de fotões que constituem cada *qubit* da chave, não considerando a atenuação e ruído de despolarização no canal, de forma a conferir mais *bits* resultantes a Eve do que à casa que sofre o ataque. Verificou-se que a presença de ataques *intercept-and-resend* nas ligações da rede aumenta a taxa média de *qubits* cuja leitura é conclusiva e resulta num *bit* da *raw key*, para os protocolos SARG04 e KMB09. O sucesso deste ataque mostrou-se promissor, contudo, facilmente detetável, quando considerado um limite máximo aceitável de 10% de *bits* de teste errados, para os três protocolos considerados. No caso de ataque PNS, o simulador não prevê a sua deteção. Contudo, para μ=0.2, praticamente só é bem sucedido caso Eve não descarte os *bits* da sua chave resultante nas posições em que a casa atacada nada pôde concluir, originando assim chaves iguais entre eles meramente devido ao acaso. Caso Eve apenas considere na sua chave resultante os i-ésimos *bits* também obtidos pela casa que sofre o ataque, a utilização de μ=0.2 mostra-se bastante segura, sendo que, como eraexpectável, SARG04 é o protocolo mais resiliente contra este tipo de ataque.

O último parâmetro analisado neste trabalho foi o efeito do ruído de despolarização, considerado coletivo. Conclui-se que afeta os dois protocolos constituídos por quatro estados de igual forma, o que era expectável dado que são idênticos ao nível quântico. Conclui-se que, de modo a poder aplicar um limiar máximo aceitável de 10% de *bits* de teste errados, nestas condições, é necessário um

ruído dado apenas por $\varepsilon = 0.02$, caso contrário, todas as ligações quânticas da rede resultam num erro. Conclui-se também que um aumento do parâmetro de ruído conduz a uma maior eficácia de um ataque *intercept-and-resend.* Verificou-se assim, que é possível garantir segurança numa rede *smart grid* local, num cenário em que é conferido a Eve toda a tecnologia idealizável para efetuar um ataque *intercept-and-resend* sob uma enorme vantagem de obtenção de chave, desde a quantidade de *qubits* lidos, até ao total acesso ao canal público da ligação QKD. O único protocolo em que tal não se verificou, foi no caso de BB84, em que as taxas de limiar de deteção têm de ser inferiores a 10%, o que provavelmente requer um canal quântico ideal ao nível de ruído de despolarização, mesmo para as curtas distâncias em que decorrem as simulações. Além disso, mostrou-se que é possível usar um sistema QKD na rede em causa, mesmo quando a codificação utilizada em cada casa requer uma chave com dezenas de *bits*.

10 Bibliografia

[1] Borges, Fábio, Raqueline AM Santos, and Franklin L. Marquezino. "Preserving privacy in a smart grid scenario using quantum mechanics." Security and communication networks 8.12 (2015):2061-2069.

[2] Lardier, William, Quentin Varo, and Jun Yan. "Quantum-sim: An open-source co-simulation platform for quantum key distribution-based smart grid communications." 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm). IEEE, 2019.

[3] Mosaik - Mosaik is a flexible Smart Grid co-simulation framework. Disponível em: https://mosaik.offis.de/

[4] Kong, Peng-Yong. "A review of quantum key distribution protocols in the perspective of smart grid communication security." IEEE Systems Journal (2020).

[5] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," IEEE Security Privacy, vol. 8, no. 1 Jan./Feb. (2010): 81–85,

[6] Diamanti, E., Lo, HK., Qi, B. *et al*. Practical challenges in quantum key distribution. *npj Quantum Inf*

[7] Brassard, Gilles, et al. "Limitations on practical quantum cryptography." Physical Review Letters 85.6 (2000): 1330.

[8] Yoshino, Ken-ichiro, et al. "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days." Optics Express 21.25 (2013): 31395-31401.

[9] Singh, Hitesh, Dharmendra Lal Gupta, and Ashish Kumar Singh. "Quantum key distribution protocols: a review." *Journal of Computer Engineering* 16.2 (2014): 1-9.

[10] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. Computer Systems and Signal Processing., Bangalore, India, 1984,pp. 175-179.

[11] Mogos, Gabriela. "Quantum Key Distribution Protocol with Four-State Systems–Software Implementation." Procedia Computer Science 54 (2015): 65-72.

[12] Pereszlenyi, Attila. "Simulation of quantum key distribution with noisy channels." Proceedings of the 8th International Conference on Telecommunications, 2005. ConTEL 2005.. Vol. 1. IEEE, 2005.

[13] Kockum, Anton Frisk. Quantum optics with artificial atoms. Chalmers Tekniska Hogskola(Sweden), 2014.

[14] Ekert, Artur, and Chiara Macchiavello. An overview of quantum computing. Springer-Verlag, Singapore, 1998.

[15] Bužek, Vladimir, and Mark Hillery. "Quantum copying: Beyond the no-cloning theorem." Physical Review A 54.3 (1996): 1844.

[16] Pang, Xiao-Ling, et al. "Hacking quantum key distribution via injection locking." Physical Review Applied 13.3 (2020): 034008.

[17] Bebrov, Georgi, Rozalina Dimova, and Evelina Pencheva. "Quantum approach to the information privacy in smart grid." 2017 International Conference on Optimization of Electrical

and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP). IEEE, 2017.

[18] Murta, Gláucia, et al. "Key rates for quantum key distribution protocols with asymmetric noise." Physical Review A 101.6 (2020): 062321.

[19] Khan, Muhammad Mubashir, Michael Murphy, and Almut Beige. "High error-rate quantum key distribution for long-distance communication." New Journal of Physics 11.6 (2009): 063043.

[20] Gyöngyösi, László, Laszlo Bacsardi, and Sandor Imre. "A survey on quantum key distribution." Infocommunications journal 11.2 (2019): 14-21.

[21] Khan, Muhammad Mubashir, Jie Xu, and Almut Beige. "Improved Eavesdropping Detection in Quantum Key Distribution." International Journal of Computer Science and Information Security 15.1 (2017): 536.

[22] Guo, Peng-Liang, et al. "Efficient quantum key distribution against collective noise using polarization and transverse spatial mode of photons." Optics Express 28.4 (2020): 4611-4624.

[23] Lidar, Daniel A., and Todd A. Brun, eds. Quantum error correction. Cambridge University Press, 2013.

[24] Scarani, Valerio, et al. "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations." Physical Review Letters 92.5 (2004): 057901.

[25] Li, Na, et al. "Security analysis of measurement-device-independent quantum key distribution in collective-rotation noisy environment." International Journal of Theoretical Physics 57.1 (2018):83-94.

[26] Ribordy, Grégoire, et al. "Long-distance entanglement-based quantum key distribution." Physical Review A 63.1 (2000): 012309.

[27] Ursin, Rupert, et al. "Entanglement-based quantum communication over 144 km." Nature Physics 3.7 (2007): 481-486.

[28] Ez-Zahraouy, Hamid, and Abdelilah Benyoussef. "Quantum key distribution with several intercepts and resend attacks." International Journal of Modern Physics B 23.23 (2009): 4755-4765.

[29] Qiao, Hui, and Xiao-yu Chen. "Simulation of BB84 Quantum Key Distribution in depolarizing channel." Proceedings of 14th Youth Conference on Communication. 2009.

[30] Jeong, Y-C., Y-S. Kim, and Y-H. Kim. "Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols." Laser Physics 21.8 (2011): 1438-1442.

[31] Yousif, Ali H., et al. "Intercept-Resend Attack on SARG04 Protocol: An Extended Work." Polytechnic Journal 10.1 (2020): 88-92.

[32] Lütkenhaus, Norbert, and Mika Jahma. "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack." New Journal of Physics 4.1 (2002): 44.

[33] Boileau, J-C., J. Batuwantudawe, and R. Laflamme. "Higher-security thresholds for quantum key distribution by improved analysis of dark counts." Physical Review A 72.3 (2005): 032321.

[34] Koashi, Masato. "Security of quantum key distribution with discrete rotational symmetry." arXiv preprint quant-ph/0507154 (2005).

[35] Lloyd, Seth. "Capacity of the noisy quantum channel." Physical Review A 55.3 (1997): 1613.

[36] Li, Xi-Han, Fu-Guo Deng, and Hong-Yu Zhou. "Efficient quantum key distribution over acollective noise channel." Physical Review A 78.2 (2008): 022321.

[37] Gunkel, Matthias, Felix Wissel, and Andreas Poppe. "Designing a Quantum Key Distribution Network-Methodology and Challenges." Photonic Networks; 20th ITG-Symposium. VDE, 2019.

[38] Salvail, Louis, et al. "Security of trusted repeater quantum key distribution networks." Journal of Computer Security 18.1 (2010): 61-87.

[39] Kaminow, Ivanp. "Polarization in optical fibers." IEEE Journal of Quantum Electronics 17.1(1981): 15-22.

[40] Kang, Yooli, et al. "Dark count probability and quantum efficiency of avalanche photodiodes for single-photon detection." Applied Physics Letters 83.14 (2003): 2955-2957.

[41] Fei, Yang-Yang, et al. "Quantum man-in-the-middle attack on the calibration process ofquantum key distribution." Scientific reports 8.1 (2018): 1-10.

[42] Pacher, Christoph, et al. "Attacks on quantum key distribution protocols that employ non-ITS authentication." Quantum Information Processing 15.1 (2016): 327-362.

[43] Price, Alasdair B., John G. Rarity, and Chris Erven. "A quantum key distribution protocol forrapid denial of service detection." EPJ Quantum Technology 7.1 (2020): 8.

[44] Ghosh, Sebati, and Palash Sarkar. "Variants of Wegman-Carter message authentication code supporting variable tag lengths." Designs, Codes and Cryptography 89.4 (2021): 709-736.

[45] Gobby, C., Z. L. Yuan, and A. J. Shields. "Quantum key distribution over 122 km of standardtelecom fiber." Applied Physics Letters 84.19 (2004): 3762-3764.

[46] Guy-Cedric, Toa Bi Irie. Suchithra R.,“A Comparative Study on AES 128 BIT AND AES 256 BIT”. International Journal of Scientific Research in Computing Science and Engineering 6.4 (2018): 30-33.

[47] Schütte, Steffen, Stefan Scherfke, and Martin Tröschel. "Mosaik: A framework for modularsimulation of active components in smart grids." 2011 IEEE First International Workshop onSmart Grid Modeling and Simulation (SGMS). IEEE, 2011.

[48] Alléaume, R., et al. "Secoqc white paper on quantum key distribution and cryptography (January 2007)." (2007)

Anexo A

Neste anexo é descrito o que ocorre nas várias fases do funcionamento do programa, nos simuladores das casas e do CC, suportadas pelo código utilizado na sua implementação.

- STATE 0 - Casa:

```
if date == target_date:

    # Found target date, cache results:
    values = list(map(float, values))

    #CONSUMO INSTANTÂNEO
    self._cache = [values[i % self.num_profiles] for i, _ in enumerate(self.houses)]

    #CONSUMO TOTAL ATÉ DATE
    for i, house in enumerate(self.houses):
        consumption[i] += ((self._cache[i])) #+ random.randint(0,100) ###############
        consumption[i] = round(consumption[i],2)

    #ENVIO DO CONSUMO DE CADA CASA
    for i, house in enumerate(self.houses):
        house['hhrequest'] = 1
        print("Pedido de mensagem de" ,house['node_id'], ":" ,consumption[i])

    self.STATE = 1
    self._last_date = date
```

Envia ‘1’ a cada *target date* para sinalizar pedido de atribuição de chave.

- STATE 0 - CC:

```
for key, value in input.items():
    for key2, value2 in value.items():
        for key3, value3 in value2.items():

            if value3 != 0:
                self.debug_print("\nVALOR RECEBIDO:" ,value3)

            #STATE == 0 -> PEDIDO DE MENSAGEM ##################################
            if value3 == 1:
                print("PEDIDO DE QK RECEBIDO DE:" ,key3)
```

Recebido valor ‘1’, início do processo QKD.

```
#CRIAR UMA CHAVE PARA CADA PEDIDO E ARMAZENA
bin_key = self.generate_random_bits(self.N)
bin_key_dict.append(bin_key)

#CODIFICAR A CHAVE GERADA CONFORME PROTOCOLO
if self.protocol["qkd"] == 'BB84':
    q_key,bases = self.generate_BB84_QK(bin_key)

elif self.protocol["qkd"] == 'SARG04':
    q_key,bases = self.generate_SARG04_QK(bin_key)

elif self.protocol["qkd"] == 'KMB09':
    q_key,bases = self.generate_KMB09_QK(bin_key,self.index)
```

Gerar chave binária e codificar os *qubits* correspondentes.

- STATE 1 - Casa:

```
#PHOTON ##########################################################################
photon_number = self.det_photon_number(self.N,self.mean_photons_per_pulse,qk)
#REAL SOURCE - Qubit's photon number folllows a poissonic distribution
if self.real_source == True:
    # Some qubits may no have any photon to it as it is impossible to read it
    qk = self.photon_number_qubit_update(photon_number,qk)
```

Aplicar número de fotões a cada *qubit*.

```
#PHOTON NUMBER SPLIPPING ATTACK ###################################################################
if self.pns_eve == True:
    pns_attack = self.det_mitm_PNS_attack(self.I)

    if pns_attack == True:
        pns_eve_qubit_read = self.eve_pns_read_qk(qk,photon_number)
        pns_eve_qubit_read_dict.append(pns_eve_qubit_read)

    else:
        pns_eve_qubit_read_dict.append(None)
```

Aplicar ataques PNS.

```
# STRAIGTH FORWARD MITM ############################################################################
if self.sf_mitm_eve == True:
    attack = self.det_mitm_ir_attack(self.I)

    if attack == True:
        if self.qkd == 'BB84':
            sf_eve_qubits_read, sf_eve_bases, sf_eve_key_read = self.eve_ir_read_qk_BB84(qk)
        if self.qkd == 'SARG04':
            sf_eve_qubits_read, sf_eve_bases, sf_eve_key_read = self.eve_ir_read_qk_SARG04(qk)
        if self.qkd == 'KMB09':
            sf_eve_qubits_read, sf_eve_bases, sf_eve_key_read = self.eve_ir_read_qk_KMB09(qk,self.index)
```

Aplicar ataques *Intercept-and-Resend*.

```
# QUBITS DETECTON ##################################################################################
if self.real_detection == True:
    qk_received = self.detection(qk,photon_number)
```

Determinar quais os *qubits* que são lidos.

```
# RUÍDO DE DEPOLARIZAÇÃO ##############################################################################
if self.polarization_noise == True:

    qk_converted = self.states_degrees_conversion(qk_received) #qk_received
    qubit_read, bases, key_read = self.read_depolarization_noise(qk_converted,self.noise_parameter[self.I])

else:
# LEITURA DAS CHAVES (SEM RUÍDO DE POLARIZAÇÃO) ########################################################
    if self.qkd =='BB84':
        qubit_read, bases, key_read = self.read_qk_BB84(qk_received)

    if self.qkd =='SARG04':
        qubit_read, bases, key_read = self.read_qk_SARG04(qk_received)

    if self.qkd =='KMB09':
        qubit_read, bases, key_read = self.read_qk_KMB09(qk_received,self.index)
```

Efetuar leitura com ou sem ruído de despolarização.

- STATE 1 - CC:

Aguarda

- STATE 2 - Casa:

```
if self.qkd =='BB84':
    #TRANSMITING USED BASES
    for i, house in enumerate(self.houses):
        house['hhrequest'] = bases_dict[self.I]
        self.reponseReceived += 1
        self.I += 1
```

Envia bases caso o protocolo seja BB84.

- STATE 2 - CC:

```
if self.protocol["qkd"] == 'BB84':
    received_bases = value3
    used_bases = bases_dict[self.I]

    #RETIFY BASES
    key,bases = self.rectify_bases_BB84(received_bases,used_bases,bin_key_dict[self.I])
```

Retifica bases caso se utilize o protocolo BB84.

```
qkd = {self.eid+'.': {key3: {'response': bases_dict[self.I]}}}
yield self.mosaik.set_data(qkd)
```

Envia bases retificadas/estados de polarização/índices, conforme o protocolo utilizado.

- STATE 3 - Casa:

```
# PNS MITM ATTACK ##########################################################################################################################
if self.pns_eve == True:
    if pns_eve_qubit_read_dict[self.I] != None:
        if self.qkd == "BB84":
            pns_eve_key_read_dict.append(self.eve_pns_get_bin_key_BB84(qk,bases_dict[self.I],pns_eve_qubit_read_dict[self.I]))
        if self.qkd == "SARG04":
            pns_eve_key_read_dict.append(self.eve_pns_get_bin_key_SARG04(qk,pns_eve_qubit_read_dict[self.I]))
        if self.qkd == "KMB09":
            pns_eve_key_read_dict.append(self.eve_pns_get_bin_key_KMB09(qk,pns_eve_qubit_read_dict[self.I],self.index))
    else:
        pns_eve_key_read_dict.append(None)
```

Eve tem acesso às bases retificadas/estados de polarização/índices, conforme o protocolo utilizado, num ataque PNS.

```
# STRAIGHT FORWARD MITM ATTACK ##############################################################################################################
if self.sf_mitm_eve == True:
    if sf_eve_qubit_read_dict[self.I] != None:
        #print("Dict:",sf_eve_qubit_read_dict)
        if self.qkd =='BB84':
            sf_eve_key_read_dict[self.I]=self.eve_ir_update_bin_key_BB84(sf_eve_bases_dict[self.I],qk,bases_dict[self.I],sf_eve_key_read_dict[self.I])
        if self.qkd == 'SARG04':
            sf_eve_key_read_dict[self.I]=self.eve_ir_update_bin_key_SARG04(sf_eve_qubit_read_dict[self.I],qk,sf_eve_key_read_dict[self.I])
        if self.qkd == 'KMB09':
            sf_eve_key_read_dict[self.I]=self.eve_ir_update_bin_key_KMB09(sf_eve_qubit_read_dict[self.I],qk,sf_eve_key_read_dict[self.I],self.index)
```

Eve tem acesso às bases retificadas/estados de polarização/índices, conforme o protocolo utilizado, num ataque Intercept-and-Resend.

```
# GETTING RAW KEY ###########################################################################################################################
if self.qkd =='BB84':
    key_read_dict[self.I] = self.update_bin_key_BB84(qk,key_read_dict[self.I])

if self.qkd =='SARG04':
    key_read_dict[self.I] = self.update_bin_key_SARG04(qubit_read_dict[self.I],qk,key_read_dict[self.I])

if self.qkd =='KMB09':
    key_read_dict[self.I] = self.update_bin_key_KMB09(qubit_read_dict[self.I],qk,key_read_dict[self.I],self.index)
```

A casa atualiza a sua chave.

```
# VALIDATED QUBITS POSITIONS
correct_bits = self.det_correct_bits(key_read_dict[self.I])
```

Averigua as posições dos *qubits* para as quais a casa pôde concluir o respetivo *bit* e envia essa informação ao CC.

- STATE 3 - CC:

```
house_update = value3
bin_key_dict[self.I] = self.update_bin_key(bin_key_dict[self.I],house_update)
```

Atualiza a chave conforme o que foi enviado pela casa neste estado de funcionamento.

- STATE 4 - Casa:

```
for i, house in enumerate(self.houses):
    self.debug_print("\nID:" ,house['node_id'])

    bits_sended, key_read_dict[self.I] = self.select_bit_to_send(key_read_dict[self.I],self.NUM_BITS_SENDED)
    bits_sended_dict.append(bits_sended)

    house['hhrequest'] = bits_sended_dict[self.I]
```

Determina os *bits* de teste e envia-os.

```
# UPDATE KEY
key_read_dict[self.I] = self.delete_non_bits(key_read_dict[self.I],0,0)
```

Atualiza a chave resultante.

```
if self.sf_mitm_eve == True:
    sf_eve_key_read_dict[self.I] = self.eve_ir_delete_test_bits(bits_sended_dict[self.I],sf_eve_key_read_dict[self.I])
    self.ir_compare_eve_house_keys(key_read_dict[self.I],sf_eve_key_read_dict[self.I],consumption[i])

if self.pns_eve == True:
    pns_eve_key_read_dict[self.I] = self.eve_pns_delete_test_bits(bits_sended_dict[self.I],pns_eve_key_read_dict[self.I])
    self.pns_compare_eve_house_keys(key_read_dict[self.I],pns_eve_key_read_dict[self.I],consumption[i])
```

Atacantes eliminam da sua chave resultante os *bits* de teste enviados.

- STATE 4 - CC:

```
correct, bin_key_dict[self.I] = self.confirm_bits_sended(bin_key_dict[self.I],house_bits)

bin_key_dict[self.I] = self.delete_non_bits(bin_key_dict[self.I])

qkd = {self.eid+'.': {key3: {'response': correct}}}
```

Confirma os *bits* de teste recebidos, elimina-os da chave e emite uma confirmação acerca dos mesmos.

- STATE 5 - Casa:

```
if qk == False:
    house['hhrequest'] = 'NA'
```

Caso CC não tenha validado os *bits* de teste enviados, nada acontece.

```
elif qk == True:

    #CHACK UNDETECTED EVE
    if self.sf_mitm_eve == True:
        self.update_ir_cracked_key(sf_eve_craked_key_dict[self.I])
```

Na presença de uma resposta positiva é averiguada a existência de ataques não detetados.

```
#ENCRIPTION
encrypted_message = self.encryption(consumption[i],key_read_dict[self.I])
encrypted_message_dict.append(encrypted_message)
house['hhrequest'] = encrypted_message
```

Seguiu-se da encriptação e o envio do consumo.

- STATE 5 - CC:

```
if received_encrypted_message == 'NA':
    response = 0

# CHECKS ERRORS
else:
    received_message = self.decryption(received_encrypted_message,bin_key_dict[self.I])
    response = self.update_undetected_error(received_message)
```

Para cada valor diferente de 'NA' recebido, procede à desencriptação e averigua se existem erros que não foram detetados.

```
qkd = {self.eid+'.': {key3: {'response': response}}}
yield self.mosaik.set_data(qkd)
```

Comunica a cada casa se existiu algum erro não detetado.

- STATE 6 - Casa:

```
# CHECK CC RESPONSE
if qk == 1:
    print("CC RESPONSE: CORRECT")

elif qk == 0:
    print(house["node_id"],"NÃO ENVIOU CONSUMO")
    consumption_not_sended[i] = self._cache

house['hhrequest'] = 0
```

Recebe verificação de erro não detetado por parte de CC. Na presença de um erro, a casa torna a enviar o consumo atual no próximo *target date.*